Sun Java System Directory Server Enterprise Edition 6.2 Troubleshooting Guide

Contents

Preface

This *Troubleshooting Guide* shows you how to troubleshoot problems with Sun Java™ System Directory Server Enterprise Edition.

Who Should Use This Book

This guide is intended for advanced administrative users who are troubleshooting problems with Directory Server Enterprise Edition.

Before using this guide, you must be familiar with the following:

- Directory Server functionality
- Specifications for LDAP and related protocols, such as DSML v2
- Internet and World Wide Web technologies

Before You Read This Book

Review pertinent information in the *Sun Java System Directory Server Enterprise Edition 6.2 Release Notes*.

How This Book Is Organized

Chapter 1, "Overview of Troubleshooting Directory Server Enterprise Edition" describes how to approach troubleshooting problems in Directory Server Enterprise Edition, including how to define the scope of the problem, generic data collection, troubleshooting tools, and a where to get more information.

Chapter 2, "Troubleshooting Installation and Migration Problems" provides information to help you troubleshoot installation and migration problems.

Chapter 3, "Troubleshooting Replication" provides information to help you troubleshoot problems with replication and contains a procedure to help you reinitialize your entire topology.

Chapter 4, "Troubleshooting Directory Proxy Server" provides information to help you troubleshoot problems with Directory Proxy Server.

Chapter 5, "Troubleshooting Directory Server Problems" provides information about how to troubleshoot general problems with Directory Server, including a crash, an unresponsive process, database problems, and memory leaks.

Chapter 6, "Troubleshooting Data Management Problems" provides information to help you troubleshoot data management problems, include operation failures and SSL problems.

Chapter 7, "Troubleshooting Identity Synchronization for Windows" provides information to help you troubleshoot problems you may encounter while using Identity Synchronization for Windows.

Chapter 8, "Troubleshooting DSCC and 5.x Console Problems" contains information to help you troubleshoot problems with the DSCC.

Chapter 9, "Directory Server Error Log Message Reference" lists messages logged by Directory Server that can serve as a good starting point for resolving common problems.

Examples Used in This Guide

For consistency reasons, the same example data is used throughout this guide. Replace these values with the appropriate values for your system.

TABLE P–1 Default Values Used in Examples

Variable	Values used in examples
Suffix (SUFFIX_DN)	dc=example,dc=com
Instance path (INSTANCE_PATH)	For Directory Server: /local/ds/
	For Directory Proxy Server: /local/dps/
Hostnames (HOST)	host1, host2, host3
Port (PORT)	LDAP: Default for root: 389. Default for non-root: 1389
	SSL default: Default for root: 636. Default for non-root: 1636

Directory Server Enterprise Edition Documentation Set

This Directory Server Enterprise Edition documentation set explains how to use Sun Java System Directory Server Enterprise Edition to evaluate, design, deploy, and administer directory services. In addition, it shows how to develop client applications for Directory Server Enterprise Edition. The Directory Server Enterprise Edition documentation set is available at http://docs.sun.com/coll/1224.3.

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

TABLE P–2   Directory Server Enterprise Edition Documentation

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.2 Release Notes	Contains the latest information about Directory Server Enterprise Edition, including known problems.
Sun Java System Directory Server Enterprise Edition 6.2 Documentation Center	Contains links to key areas of the documentation set.
Sun Java System Directory Server Enterprise Edition 6.2 Evaluation Guide	Introduces the key features of this release. Demonstrates how these features work and what they offer in the context of a fictional deployment that you can implement on a single system.
Sun Java System Directory Server Enterprise Edition 6.2 Deployment Planning Guide	Explains how to plan and design highly available, highly scalable directory services based on Directory Server Enterprise Edition. Presents the basic concepts and principles of deployment planning and design. Discusses the solution life cycle, and provides high-level examples and strategies to use when planning solutions based on Directory Server Enterprise Edition.
Sun Java System Directory Server Enterprise Edition 6.2 Installation Guide	Explains how to install the Directory Server Enterprise Edition software. Shows how to select which components to install, configure those components after installation, and verify that the configured components function properly.
	For instructions on installing Directory Editor, go to `http://docs.sun.com/coll/DirEdit_05q1`.
	Make sure you read the information in *Sun Java System Directory Server Enterprise Edition 6.2 Release Notes* related to Directory Editor before you install Directory Editor.
Sun Java System Directory Server Enterprise Edition 6.2 Migration Guide	Provides instructions for upgrading components from earlier versions of Directory Server, Directory Proxy Server, and Identity Synchronization for Windows.
Sun Java System Directory Server Enterprise Edition 6.2 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 about administering Directory Editor, go to `http://docs.sun.com/coll/DirEdit_05q1`.
	For instructions about installing and configuring Identity Synchronization for Windows, see Part II, "Installing Identity Synchronization for Windows," in *Sun Java System Directory Server Enterprise Edition 6.2 Installation Guide*.

TABLE P–2   Directory Server Enterprise Edition Documentation   *(Continued)*

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.2 Developer's Guide	Provides instructions for developing 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 6.2 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 6.2 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 6.2 Troubleshooting Guide	Provides information for defining the scope of the problem, gathering data, and troubleshooting the problem areas using various tools.
Sun Java System Identity Synchronization for Windows 6.0 Deployment Planning Guide	Provides general guidelines and best practices for planning and deploying Identity Synchronization for Windows.

Related Reading

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

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

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

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

Identity Synchronization for Windows works with Microsoft Windows password policies.

- Information about password policies for Windows 2003 is available in the Microsoft documentation online.

- Information about changing passwords, and about group policies in Windows 2003 is available in the Microsoft documentation online.

- Information about the Microsoft Certificate Services Enterprise Root certificate authority is available in the Microsoft support documentation online.

- Information about configuring LDAP over SSL on Microsoft systems is available in the Microsoft support documentation online.

Redistributable Files

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

Default Paths and Command Locations

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

Default Paths

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

- Chapter 14, Directory Server File Reference
- Chapter 25, Directory Proxy Server File Reference
- Appendix A, Directory Server Resource Kit File Reference

TABLE P–3 Default Paths

Placeholder	Description	Default Value
install-path	Represents the base installation directory for Directory Server Enterprise Edition software. The software is installed in directories below this base *install-path*. For example, Directory Server software is installed in *install-path*/ds6/.	When you install from a zip distribution using dsee_deploy(1M), the default *install-path* is the current directory. You can set the *install-path* using the -i option of the dsee_deploy command. When you install from a native package distribution, such as you would using the Java Enterprise System installer, the default *install-path* is one of the following locations: ■ Solaris systems - /opt/SUNWdsee/. ■ Red Hat systems - /opt/sun/. ■ Windows systems - C:\Program Files\Sun\JavaES5\DSEE.
instance-path	Represents the full path to an instance of Directory Server or Directory Proxy Server. The documentation uses /local/ds/ for Directory Server and /local/dps/ for Directory Proxy Server.	No default path exists. Instance paths must nevertheless always be found on a *local* file system. The following directories are recommended: /var on Solaris systems /global if you are using Sun Cluster
serverroot	Represents the parent directory of the Identity Synchronization for Windows installation location	Depends on your installation. Note the concept of a *serverroot* no longer exists for Directory Server.
isw-*hostname*	Represents the Identity Synchronization for Windows instance directory	Depends on your installation
/path/to/cert8.db	Represents the default path and file name of the client's certificate database for Identity Synchronization for Windows	*current-working-dir*/cert8.db
serverroot/isw-*hostname*/logs/	Represents the default path to the Identity Synchronization for Windows local logs for the System Manager, each connector, and the Central Logger	Depends on your installation
serverroot/isw-*hostname*/logs/central/	Represents the default path to the Identity Synchronization for Windows central logs	Depends on your installation

Command Locations

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

TABLE P–4   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- *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 Red Hat- /opt/sun/private/bin/certutil	*install-path*/dsee6/bin/certutil
dpadm(1M)	*install-path*/dps6/bin/dpadm	*install-path*/dps6/bin/dpadm
dpconf(1M)	*install-path*/dps6/bin/dpconf	*install-path*/dps6/bin/dpconf
dsadm(1M)	*install-path*/ds6/bin/dsadm	*install-path*/ds6/bin/dsadm
dsccmon(1M)	*install-path*/dscc6/bin/dsccmon	*install-path*/dscc6/bin/dsccmon
dsccreg(1M)	*install-path*/dscc6/bin/dsccreg	*install-path*/dscc6/bin/dsccreg
dsccsetup(1M)	*install-path*/dscc6/bin/dsccsetup	*install-path*/dscc6/bin/dsccsetup
dsconf(1M)	*install-path*/ds6/bin/dsconf	*install-path*/ds6/bin/dsconf
dsee_deploy(1M)	Not provided	*install-path*/dsee6/bin/dsee_deploy
dsmig(1M)	*install-path*/ds6/bin/dsmig	*install-path*/ds6/bin/dsmig
entrycmp(1)	*install-path*/ds6/bin/entrycmp	*install-path*/ds6/bin/entrycmp
fildif(1)	*install-path*/ds6/bin/fildif	*install-path*/ds6/bin/fildif
idsktune(1M)	Not provided	At the root of the unzipped zip distribution

TABLE P–4 Command Locations *(Continued)*

Command	Java ES, Native Package Distribution	Zip Distribution
insync(1)	*install-path*/ds6/bin/insync	*install-path*/ds6/bin/insync
ns-accountstatus(1M)	*install-path*/ds6/bin/ns-accountstatus	*install-path*/ds6/bin/ns-accountstatus
ns-activate(1M)	*install-path*/ds6/bin/ns-activate	*install-path*/ds6/bin/ns-activate
ns-inactivate(1M)	*install-path*/ds6/bin/ns-inactivate	*install-path*/ds6/bin/ns-inactivate
repldisc(1)	*install-path*/ds6/bin/repldisc	*install-path*/ds6/bin/repldisc
schema_push(1M)	*install-path*/ds6/bin/schema_push	*install-path*/ds6/bin/schema_push
smcwebserver	Solaris and Linux- /usr/sbin/smcwebserver Windows - *install-path*\share\ webconsole\bin\smcwebserver	This command pertains only to DSCC when it is installed using native packages distribution.
wcadmin	Solaris and Linux- /usr/sbin/wcadmin Windows - *install-path*\share\ webconsole\bin\wcadmin	This command pertains only to DSCC when it is installed using native packages distribution.

Typographic Conventions

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

TABLE P–5 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*.

TABLE P–5 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
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–6 Shell Prompts

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

Symbol Conventions

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

TABLE P–7 Symbol Conventions

Symbol	Description	Example	Meaning
`[ ]`	Contains optional arguments and command options.	`ls [-l]`	The `-l` option is not required.
`{	}`	Contains a set of choices for a required command option.	`-d {y|n}`	The `-d` option requires that you use either the y argument or the n argument.
`${ }`	Indicates a variable reference.	`${com.sun.javaRoot}`	References the value of the `com.sun.javaRoot` variable.
`-`	Joins simultaneous multiple keystrokes.	Control-A	Press the Control key while you press the A key.

	TABLE P–7	Symbol Conventions	*(Continued)*	
Symbol	**Description**		**Example**	**Meaning**
+	Joins consecutive multiple keystrokes.		Ctrl+A+N	Press the Control key, release it, and then press the subsequent keys.
→	Indicates menu item selection in a graphical user interface.		File → New → Templates	From the File menu, choose New. From the New submenu, choose Templates.

Documentation, Support, and Training

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

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

Searching Sun Product Documentation

Besides searching Sun product documentation from the docs.sun.com^{SM} web site, you can use a search engine by typing the following syntax in the search field:

search-term site:docs.sun.com

For example, to search for "broker," type the following:

broker site:docs.sun.com

To include other Sun web sites in your search (for example, java.sun.com, www.sun.com, and developers.sun.com), use sun.com in place of docs.sun.com in the search field.

Third-Party Web Site References

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

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

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 820-2496.

1

Overview of Troubleshooting Directory Server Enterprise Edition

This chapter describes how to approach troubleshooting problems in Directory Server Enterprise Edition. It includes the following sections:

Defining the Scope of Your Problem

Before you begin troubleshooting a problem, you must first define the scope of your problem. When defining the scope , you need to identify what is working and what is not working. Sometimes it is useful to identify another machine that is working as you expect. Comparing the server that is experiencing a problem with a server that is working correctly simplifies troubleshooting and can help you arrive at a solution more quickly.

For example, you are checking email at work and are suddenly unable to read or write new email. If you can not resolve the problem quickly, you might go to a colleague and see if they are experiencing the same problem. If your colleague is experiencing the same problem, you feel relieved and decide that the problem is a bigger network issue. If your colleague says no, email is working as expected, you might look at your colleague's proxy settings and see if yours are configured the same.

You can help define the scope of your problem by asking questions about what is working and what isn't working, such as the following:

- On which servers is the problem being observed?
- On which servers is the problem not being observed?
- For which types of operations is the problem occurring?
- For which types of operations is the problem not occurring?

- On the failing server, which plug-ins or components are experiencing the problem? For example, replicated updates, local updates, UID uniqueness, ACIs, roles, CoS, password policy, or all of the above.
- On the failing server, which plug-ins or components are not experiencing the problem?
- Is the problem permanent or transient?
- Where could the problem be permanent or transient, but is not?
- Is the problem still growing, decreasing or stable?
- Where could the problem be growing but is not?

On each of the servers where the problem is observed, determine the first time the problem was observed, including the date and time. Identify any changes that were made to your system immediately before this date, such as changes to the configuration, upgrades, and installations.

Collecting Generic Data

No matter the type of problem you are encountering, there is a minimum set of data that needs to be collected and, if necessary, provided to Sun Support. If your problem occurs across your topology, you need to provide this generic data for all instances of Directory Server or Directory Proxy Server inside the topology.

The generic data for Directory Server that you collect must include the following:

- Collect the Directory Server version information:

  ```
  # install-path/bin/slapd/server/ns-slapd -D instance-dir -V
  ```

- Collect the Directory Server access and errors logs that contain the time since the problem started. By default, you find these logs in the following locations:

  ```
  instance-dir/logs/access
  instance-dir/logs/errors
  ```

- Provide information about the computers involved, including their IP addresses, operating system version, disk partitions, swap space, installed patches, hard disk space, and file systems used.
- Collect the Directory Server configuration file, install-path/slapd-serverID/config/dse.ldif.

For more information about generic data, collection, refer to "To Collect Required Debug Data For Any Directory Server Problem" in *Sun Gathering Debug Data for Sun Java System Directory Server 5*.

The generic data for includes the generic data collected for Directory Server and the following Directory Proxy Server information:

- Collect the Directory Proxy Server version information:

  # *install-path*/bin/dps/server/bin/ldapfwd -v

- Collect the Directory Proxy Server access and errors logs that contain the time since the problem started. By default, you find these logs in the following locations:

  instance-dir/logs/

- Collect the Directory Proxy Server configuration file using the dpconf info command.

Using Troubleshooting Tools

Several tools are available that you can use to collect general information for troubleshooting purposes. This section provides information about the following troubleshooting tools:

Using the idsktune Command

The idsktune command provides information about system parameters, patch level, and tuning recommendations. You can use the output of this command to detect problems in thread libraries or patches that are missing. For more information about the idsktune command, see idsktune(1M)

Run the idsktune command as follows:

./idsktune

Note – The idsktune command is delivered next to the dsee_deploy command with zip distribution software only.

Using the pkg_app Script on Solaris

The Solaris pkg_app script packages an executable and all of its shared libraries into one compressed tar file. You provide the process ID of the application and, optionally, the name of the core file to be opened.

You can download this script from http://kaneda.central.sun.com/pkg_app/. This script retrieves the correct version of the binary of the running process or from the core and works with 32 and 64 bit libraries.

The files are stripped of their directory paths, and are stored under a relative directory named /app with their names only, allowing them to be unpacked in one directory. On Solaris 9 and

Solaris 10, the list of files output by the pkg_app script is derived from the core file rather than the process image, if it is specified. You must still provide the process ID of the running application to assist in path resolution.

As superuser, run the pkg_app script as follows:

```
# pkg_app server-pid core-file
```

Note – You can also run the pkg_app script without a core file. This reduces the size of the pkg_app output. You need to later set the variable to the correct location of the core file.

Using the dirtracer **Script**

The dirtracer tool is a shell script that gathers debugging information about a running, hung, or stopped Directory Server process. This information can be used by Sun Support to diagnose a problem. The scripts collects information about the operating system configuration, the Directory Server configuration, and the runtime data elements, as well as log files, databases, cores, gcores, and pstack output. The type of information gathered depends upon the type of problem you are experiencing.

The dirtracer script is available from BigAdmin at
http://www.sun.com/bigadmin/scripts/.

As superuser, run the dirtracer script as follows:

```
#./ dirtracer -f ./dirtracer.config
```

The dirtracer.config file contains the configuration parameters used by the dirtracer script to generate its output. The dirtracer script comes with a tool to generate this configuration file called the configurator. This interactive shell script automatically creates a configuration file that addresses the type of problem you are experiencing. The configurator set the parameters for log gathering, core collection, as well as many other parameters.

Where to Go For More Information

If you are a Sun Service Plan customer, you have access to a number of exclusive online resources, including the following:

- Sun support web site
- SunSolve Online Knowledgebase

  Search the knowledgebase for information that correspond to the problem you are experiencing.

- Sun Gathering Debug Data

  The Sun GDD tools provide best practices to help you gather the required debug data needed for further problem analysis.

- Sun Online Support Center

  If you are a SunSpectrum Support member, you can use the resources available to you in the Online Support Center, including submitting a new service request.

- Patches and upgrades

  Get patches, diagnostic tools, and software updates from the Sun Update Connection.

- Security resources

  Provides access to Security Sun Alerts, Solaris Fingerprint Database, Security T-Patches, and more.

- Visit support forums

  You can browse the forums as a guest or login and post your own questions.

- Join the System Admin Community

  Find helpful system administration resources, join and discuss issues with other system administrators worldwide.

For questions regarding your Sun Service Plan, contact your local Sun sales representative.

2

Troubleshooting Installation and Migration Problems

This chapter provides information to help you troubleshoot problems with installation and migration. It includes the following topics:

Possible Causes of an Installation Problem

A problem installing Directory Server Enterprise Edition could be caused by one of the following:

- Incorrect patches installed
- Installing a patch that does not correspond to your architecture
- During installation of the Directory Server Enterprise Edition zip distribution, specifying a common agent container port that is already in use
- Permissions problems
- Specifying an LDAP port that is already in use
- The presence of a previous installation
- The list of packages being installed is incomplete
- Shared components version does not match the JES version

If you encounter a problem doing an upgrade, confirm that you are installing the same type of software distribution as you installed previously. For example, if you installed before using the zip distribution, any upgrade you make must also use the zip distribution.

If you are installing a SunAlert patch, confirm in the read me that you are installing the patch number that applies to your type of distribution.

Troubleshooting Java ES Installation Problems

This section describes how to troubleshoot problems installing the Java Enterprise System software distribution on Solaris and Linux operating systems.

Note – If the problem concerns a general installation failure for Java Enterprise System, first check the installation troubleshooting chapter in the *Installation Guide* for your version of Java Enterprise System.

General Recommendations

Before you begin troubleshooting your Java ES installation, be certain that you have done your installation using the Java ES installer. You must install the Java ES distribution using this installer. The installer installs a large number of component packages.

Troubleshooting Java ES Installations on Solaris

This section provides information to help you troubleshoot problems installing Directory Server Enterprise Edition on Solaris using the Java ES distribution.

Collecting and Analyzing Data

Review the installation errors logs for information about what occurred during the installation failure. On Solaris, search for error messages in the `/var/sadm/install/logs` directory. On Red Hat and HP-UX systems, installations logs are located in the `/var/opt/sun/install/logs` directory. On Windows systems, installation logs are located in the `C:\Docuemnts and Settings\`*current-user*`\Local Settings\Temp` directory.

The logs directory contains the following log files:

- `Java_Enterprise_System_5_install.B04251905`
- `Java_Enterprise_System_5_install.A04251905`
- `JavaES_Install_log.45487014`
- `Java_Enterprise_System_5_Summary_Report_install.04250719`

Information about the installed components, including Directory Server, are included in these log files.

Contacting Sun Support

If you cannot complete Directory Server Enterprise Edition installation using the Java ES distribution on Solaris and are unable to troubleshoot your problem, collect the following data. This data can help the Sun Support Center resolve your problem.

- Identify the step-by-step procedure used for the installation
- Send a copy of the log files located in the `/var/sadm/install/logs` directory.
- Send a copy of the `/var/sadm/install/contents` file.
- Send the output of `showrev -p`.

In addition to the data described here, see "To Collect Required Debug Data For Directory Server Installation Problems" in *Sun Gathering Debug Data for Sun Java System Directory Server 5*.

Troubleshooting Java ES Installations on Linux

If you installed the Java Enterprise System distribution manually, meaning you installed only the packages you thought were required, restart a clean installation using the installer.

▼ To Do a Clean Reinstall of Java ES on Linux

1 Stop all of the Java ES processes.

2 Remove everything under the *install-path* **that you specified during the configuration phase.**

To help you locate this path, run the following:

```
# grep location /var/tmp/productregistery
```

3 Remove the `/var/tmp/productregistry` **file and the** `/var/opt/sun/install/productregistry` **file.**

These product registry files contain a description of what packages have been installed for Java ES and where they were installed.

4 Uninstall the Directory Server Enterprise Edition RPM packages.

Locate all of the installed Directory Server Enterprise Edition RPM packages as follows:

```
# rpm -qa | grep 'sun-ldap-(shared|directory|proxy|console)'
```

Remove all of the RPM packages you locate as follows:

```
# rpm -e list-of-rpm-packages
```

5 Install the package again using the Java ES installer

Resolving a Java ES Permissions Problem

If after performing a clean install you still cannot launch the installer, you may be experiencing a problem with permissions. This problem typically occurs on Linux because of an incorrect default umask value. This problem arises when you install as one user, such as root, then use a regular LDAP user for Directory Server. When you launch Directory Server as the LDAP user, it fails because this user does not have access to files that have been installed as root because of a umask value that is too restrictive.

For example, you can reset the permissions using a simple script as follows:

```
# cd /opt/sun
# for i in 'find . -perm 750'
do
chmod $i 755 $i
done
# for i in 'find. -perm 640'
do
chmod $i 644 $i
done
# cd instance-directory
# for i in 'find . -perm 750'
do
chmod $i 755 $i
done
# for i in 'find . -perm 640'
do
chmod $i 644 $i
done
```

Contacting Sun Support

If you cannot complete Directory Server Enterprise Edition installation using the Java ES distribution on Linux and are unable to troubleshoot your problem, collect the following data. This data can help the Sun Support Center resolve your problem.

- Identify the step-by-step procedure used for the installation
- Get the errors log for Directory Server.
- Send a copy of the log files located in the /var/opt/install/logs directory.
- Get the output of rpm -qalv command.
- Send a copy of the /var/opt/sun/install/productregistry file

In addition to the data described here, see "To Collect Required Debug Data For Directory Server Installation Problems" in *Sun Gathering Debug Data for Sun Java System Directory Server 5*.

Troubleshooting Zip Installation Problems

This section provides information to help you troubleshoot problems using the zip distribution for Directory Server Enterprise Edition installation.

If you are installing Directory Server Enterprise Edition on a host machine that already contains an installation of the Java Enterprise System, then the common agent container port may already be in use. To provide an alternate port for the common agent container, use the `dsee_deploy -p` *port* command.

If you cannot complete Directory Server Enterprise Edition installation using the zip distribution, collect and analyze the following data. If the source of the error is not apparent, send this data to the Sun Support Center for help resolving your problem.

- Identify the step-by-step procedure used for the installation
- Get the output of the `dsee_deploy` command.
- Get the output of the `showrev -p` command.
- Get the output of the `idsktune` command. Search the output yourself for critical errors.
- Collect installation output showing system calls using the `truss` command on Solaris OS or other similar tools on other operating systems. For more information about collecting the output of the command that is displayed during installation, see "To Collect Required Debug Data For Directory Server Installation Problems" in *Sun Gathering Debug Data for Sun Java System Directory Server 5*.

Troubleshooting Migration Problems

If you encounter problems during a Directory Server Enterprise Edition migration, collect and analyze the following data. If the source of the error is not apparent, send this data to the Sun Support Center for help resolving your problem.

- Provide the exact version from which you are migrating using the `ns-slapd -V` command.
- Identify the step-by-step procedure used for the migration.
- Provide the exact directory paths for the old and new servers.
- Provide the migration script used for the migration and a `cksum`.
- Provide the migration output log. These logs are typically found in the *instance-dir*/`logs/Migration_`*date_time*`.log` file.

Troubleshooting Problems Installing Directory Server 5.2

Review the installation errors logs for information about what occurred during the installation failure. On Solaris, search for error messages in the `/var/sadm/install/logs` directory. On Red Hat and HP-UX systems, installations logs are located in the `/var/opt/sun/install/logs` directory. On Windows systems, installation logs are located in the `C:\Docuemnts and Settings\`*current-user*`\Local Settings\Temp` directory.

The `Directory_Server_install.A`*timestamp* log file records installation summary information and the `Directory_Server_install.B`*timestamp* log file contains more detailed log messages. For example, the detailed log file for a Directory Server installation that failed on December 16 at 3:32 p.m. would have a name like `Directory_Server_install.B12161532`.

To use the log files for troubleshooting, attempt to isolate the first problem that occurred. Often, the first problem leads to successive problems. Review the logs as follows:

1. Review the installation summary log file (A), which provides a high-level description of what was installed and configured. If a problem occurred, see what component caused the problem. If multiple problems occurred, isolate the first.

2. Review the detailed log file (B). Look for the first error warning that occurred and attempt to resolve it. Sometimes resolving one error resolves a number of seemingly unrelated errors that follow.

   Find the name of the component or package that caused the problem.

The log files can give you clues that determine your next steps. For example, if there was a configuration problem, look at the configuration summary to examine the settings you used. If there was a directory conflict, check that you did not specify a directory that is reserved by a different component product.

3

Troubleshooting Replication

This chapter provides information to help you troubleshoot problems with replication. It also contains a procedure to help you reinitialize your entire topology. It includes the following sections:

- "Analyzing Replication Problems" on page 33
- "Troubleshooting a Replication Halt or Replication Divergence" on page 41
- "Reinitializing a Topology" on page 48

Analyzing Replication Problems

This section guides you through the general process of analyzing replication problems. It provides information about how replication works and tools you can use to collect replication data.

About Replication

Replication is a topology wide feature that always involves more than one participant. For this reason, when you troubleshoot problems with replication, you need to detect from exactly what point in the topology replication stopped working and which replication agreements are broken.

Replication works as follows:

1. A master receives a change. Once the change has been applied to the entry in the database, then because the server is a master, it stores the change in the change log database.

2. The master updates the Replica Update Vector (RUV) in memory.

3. The master notifies the replication threads that a new change has been recorded in the change log.

4. These replication threads contact replication partners to propagate the information.

For example, Master 1 receives a change, applies it to the entry and updates its change log. When the threads on master 1 contact the consumer, the consumer shows that master replica its RUV. The master looks at the RUV and compares it with the RUV it contains in memory to see if it contains more recent changes than the consumer. If, for example, it sees that the consumer contains a higher RUV, it does not send changes. If it contains a more recent change, it sends another request to the consumer asking for a lock on replica ID 1 so that it can make updates. If the lock is unavailable, the update will be made later. If the lock is available, then the master can proceed to make the change.

About Change Sequence Numbers (CSNs)

Replication is sequential, meaning that entries are replicated in an orderly way. Because replication is orderly, any change generated by a master is labeled by a change sequence number (CSN) that is unique for any change inside a multi-master topology. The CSN is a hexadecimal that appears in the logs as follows:

41e6ee93000e00640000

The first 8 hexa-digits represent the time when the change was generated in the master. The time is represented in seconds since January 1, 1970.

The next four digits are the sequence number, or the order in the current second in which the change occurred. For example, multiple changes occur in second 41e6ee93. The sequence number tells us at which point in this second the change occurred.

The next four digits specify the replica ID of the master that received the change in the first place.

The last four digits are always 0000.

CSNs are generated only when local traffic introduces a new change to a replica. So only masters that receive updates generate CSNs. Consumers always refer to masters, because all the updates they receive are through replication.

During troubleshooting, try to find the CSN or CSNs that are at the origin of the delay. To find the CSN associated with the delay, you need to use replica update vectors (RUVs). RUVs are described in the next section.

About Replica Update Vectors (RUVs)

Any replica in a replication topology stores its current replication state in a replica update vector (RUV). The RUV is stored in memory by a process that is running and provides the exact knowledge this replica has of itself and every other participant in the replication topology. The RUV entry on a given server contains a line for each master participating in a replication

topology. Each line contains an identifier of one of the masters, the URL of the replica, and the CSN of the first and last changes made on the server. The CSN records only the first and last changes known by the server, not necessarily the most recent changes made by the master.

The state of the RUV entry is physically updated every 30 seconds in the following entry:

nsuniqueid=ffffffff-ffffffff-ffffffff-ffffffff,*suffix-name*

The RUV is also stored in memory and accessed using `ldapsearch` on the `cn=replica,cn=`*suffix*`,cn=mapping tree,cn=config` entry. For example, an `ldapsearch` for the `ou=people` suffix might yield the following results:

```
# ldapsearch -h host1 -p 1389 -D cn=Directory Manager -w secret \
-b cn=replica,
cn=ou=people,cn=mapping tree,cn=config -s base objectclass=* nsds50ruv
nsds50ruv: {replicageneration} 45e8296c000000010000
nsds50ruv: {replica 1 ldap://server1:1389} 45ed8751000000010000 4600f252000000010000
nsds50ruv: {replica 2 ldap://server1:2389} 45eec0e1000000020000 45f03214000000020000
```

For clarity, we will simplify the RUV syntax to CSN*change-number*-*replica-id*. The *change-number* shows which change the RUV corresponds to in the successive changes that occurred on the master. For example, `45ed8751000000010000` can be written as `CSN05-1`. In the previous illustration, master 1 contains the following RUVs:

```
replica 1: CSN05-1 CSN43-1
replica 2: CSN05-2 CSN40-2
```

The first line provides information about the first change and the last change that this replica knows about from itself, master 1, as indicated by the replica ID 1. The second line provides information about the first change and the last change that it knows about from master 2. The information that is most interesting to us is the last change. In normal operations, master 1 should know more about the updates it received than master 2. We confirm this by looking at the RUV for master 2:

```
replica 2: CSN05-2 CSN50-2
replica 1: CSN01-1 CSN35-1
```

Looking at the last change, we see that master 2 knows more about the last change it received (`CSN50-2`) than master 1 (which shows the last change as having occurred at `CSN40-2`). By contrast, master 1 knows more about its last change (`CSN43-1`) than master 2 (`CSN35-1`).

When troubleshooting problems with replication, the CSNs can be useful in identifying the problem. Master 1 should always know at least as much about its own replica ID as any other participant in the replication topology because the change was first applied on master 1 and then replicated. So, `CSN43-1` should be the highest value attributed to replica ID 1 in the topology.

A problem is identified if, for example, after 30 minutes the RUV on master 1 is still `CSN40-2` but on master 2 the RUV has increased significantly to `CSN67-2`. This indicates that replication is not happening from master 2 to master 1.

If a failure occurs and you need to reinitialize the topology while saving as much data as possible, you can use the RUV picture to determine which machine contains the most recent changes. For example, in the replication topology described previously you have a hub that contains the following RUV:

```
2: CSN05-2 CSN50-2
1: CSN05-1 CSN43-1
```

In this case, hub 1 seems like a good candidate for providing the most recent changes.

Using the `nsds50ruv` Attribute to Troubleshoot 5.x Replication Problems

When a server stops, the `nsds50ruv` attribute is not stored in the `cn=replica` entry. At least every 30 seconds, it is stored in the `nsuniqueid=ffffffff-ffffffff-ffffffff-ffffffff,`*suffix-name* entry as described above, as an LDAP subentry. This information is stored in the suffix instead of the configuration file because this is the only way to export this information into a file. When you initialize a topology, this occurs when the servers are off line. The data is exported into an LDIF file then reimported. If this attribute was not stored in the exported file, then the new replica would not have the correct information after an import.

Whenever you use the `db2ldif -r` command, the `nsuniqueid=ffffffff-ffffffff-ffffffff-ffffffff,`*suffix-name* entry is included.

Using the `nsds50ruv` and `ds6ruv` Attributes to Troubleshoot 6.x Replication Problems

In 6.0 and later versions of Directory Server, you can also use the `nsds50ruv` attribute to see the internal state of the consumer, as described in the previous section. If you are using the replication priority feature, you can use the `ds6ruv` attribute, which contains information about the priority operations. When replication priority is configured, you create replication rules to specify that certain changes, such as updating the user password, are replicated with high priority, For example, the RUV appears as follows:

```
nsds50ruv: {replicageneration} 4405697d000000010000
nsds50ruv: {replica 2 ldap://server1:2389}
nsds50ruv: {replica 1 ldap://server1:1390} 440569aa000000010000 44056a23000200010000
ds6ruv: {PRIO 2 ldap://server1:2389}
ds6ruv: {PRIO 1 ldap://server1:1390} 440569b6000100010000 44056a30000800010000
```

To see the replication information, export the following file:

```
# dsadm export instance-path suffix-dn [suffix-dn] ldif-file
```

Overview of Replication Data Collection

You need to collect a minimum of data from your replication topology when a replication error occurs.

Setting the Replication Logging Level

You need to collect information from the access, errors, and, if available, audit logs. Before you collect errors logs, adjust the log level to keep replication information. To set the error log level to include replication, use the following command:

```
# dsconf set-log-prop ERROR level:err-replication
```

Note – In Directory Server 5.x, use the console to set the error log level.

Using the `insync` Command

The `insync` command provides information about the state of synchronization between a supplier replica and one or more consumer replicas. This command compares the RUVs of replicas and displays the time difference or delay, in seconds, between the servers.

For example, the following command shows the state every 30 seconds:

```
$ insync -D cn=admin,cn=Administrators,cn=config -w mypword \
 -s portugal:1389 30

ReplicaDn          Consumer                Supplier        Delay

dc=example,dc=com france.example.com:2389 portugal:1389   0

dc=example,dc=com france.example.com:2389 portugal:1389   10

dc=example,dc=com france.example.com:2389 portugal:1389   0
```

You analyze the output for the points at which the replication delay stops being zero. In the above example, we see that there may be a replication problem between the consumer `france.example.com` and the supplier, `portugal`, because the replication delay changes to 10, indicating that the consumer is 10 seconds behind the supplier. We should continue to watching the evolution of this delay. If it stays more or less stable or decreases, we can conclude there is not a problem. However, a replication halt is probable when the delay increases over time.

For more information about the `insync` command, see `insync(1)`.

Using the `repldisc` **Command**

The `repldisc` command displays the replication topology, building a graph of all known replicas using the RUVs. It then prints an adjacency matrix that describes the topology. Because the output of this command shows the machine names and their connections, you can use it to help you read the output of the `insync` tool. You run this command on 6.0 and later versions of Directory Server as follows:

```
# /opt/SUNWdsee/ds6/bin/repldisc -D cn=Directory Manager -w password -b replica-root -s host:port
```

You run this command on 5.x versions of Directory Server as follows:

```
# install-root /shared/bin/repldisc -D cn=Directory Manager -w password -b replica-root -s host:port
```

The following command show an example of the output of the `repldisc` command:

```
$ repldisc -D cn=admin,cn=Administrators,cn=config -w pwd \
  -b o=rtest -s portugal:1389

Topology for suffix: o=rtest

Legend:
^ : Host on row sends to host on column.
v : Host on row receives from host on column.
x : Host on row and host on column are in MM mode.
H1 : france.example.com:1389
H2 : spain:1389
H3 : portugal:389

     | H1 | H2 | H3 |
  ===+==============
H1 |    | ^  |    |
---+--------------
H2 | v  |    | ^  |
---+--------------
H3 |    | v  |    |
---+--------------
```

Example: Troubleshooting a Replication Problem Using RUVs and CSNs

In this example, two masters replicate to two hosts, which in turn replicate to five consumers:
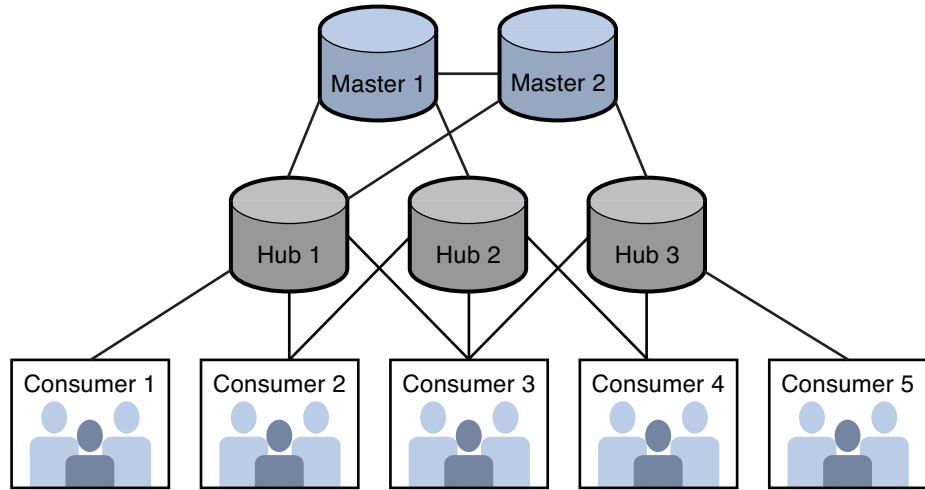
Replication is not working, and fatal errors appear in the log on consumer 4.

However, because replication is a topology wide feature, we look to see if other consumers in the topology are also experiencing a problem, and we see that consumers 3 and 5 also have fatal errors in their error logs. Using this information, we see that potential participants in the problem are consumers 3, 4, and 5, hubs 2 and 3, and masters 1 and 2. We can safely assume that consumers 1 and 2 and hub 2 are not involved.

To debug this problem, we need to collect at least the following information from the following replication participants:

- Topology wide data, using the output of the insync and repldisc commands.
- Information about the CSN or CSNs that are blocking, using the RUV of masters 1 and 2 and consumer 4.
- Information for each potential participant in the problem, including dse.ldif, nsslapd -V, access and errors log (with replication enabled) related to the date when the blocking CSN was created.
- Information about the replication participants that are functioning correctly and most likely not involved in the problem, including dse.ldif, nsslapd -V, and the access and errors log (with replication enabled).

With this data we can now identify where the delays start. Looking at the output of the insync command, we see delays from hub 2 of 3500 seconds, so this is likely where the problem originates. Now, using the RUV in the nsds50ruv attribute, we can find the operation that is at the origin of the delay. We look at the RUVs across the topology to see the last CSN to appear on a consumer. In our example, master 1 has the following RUV:

```
replica 1: CSN05-1 CSN91-1
replica 2: CSN05-2 CSN50-2
```

Master 2 contains the following RUV:

```
replica 2: CSN05-2 CSN50-2
replica 1: CSN05-1 CSN91-1
```

They appear to be perfectly synchronized. Now we look at the RUV on consumer 4:

```
replica 1: CSN05-1 CSN35-1
replica 2: CSN05-2 CSN50-2
```

The problem appears to be related to the change that is next to the change associated with CSN 35 on master 1. The change associated with CSN 35 corresponds to the oldest CSN ever replicated to consumer 4. By using the grep command on the access logs of the replicas on CSN35–01, we can find the time around which the problem started. Troubleshooting should begin from this particular point in time.

As discussed in "Defining the Scope of Your Problem" on page 21, it can be helpful to have information from a system that is working to help identify where the trouble occurs. So we collect data from hub 1 and consumer 1, which are functioning as expected. Comparing the data from the servers that are functioning, focusing on the time when the trouble started, we can identify differences. For example, maybe the hub is being replicated from a different master or a different subnet, or maybe it contains a different change just before the change at which the replication problem occurred.

Possible Symptoms of a Replication Problem and How to Proceed

Depending on the symptoms of your problem, your troubleshooting actions will be different.

For example, if you see nothing in the access logs of the consumers, a network problem may be the cause of the replication failure. Reinitialization is not required.

If the error log shows that is can not find a particular entry in the change log, the master's change log is not up-to-date. You may or may not need to reinitialize your topology, depending upon whether you can locate an up-to-date change log somewhere in your replication topology (for example, on a hub or other master).

If the consumer has problems, for example experiences processing loops or aborts locks, look in the access log for a large number of retries for a particular CSN. Run the replck tool to locate the CSN at the root of the replication halt and to repair this entry in the change log.

Troubleshooting a Replication Halt or Replication Divergence

This section describes how to troubleshoot a replication halt and replication divergence. It includes the following topics:

Possible Causes of a Replication Halt

The replication halt could be caused by one of the following:

- Replication agreement disabled or nonexistent

- Supplier missing the change record in its change log

- Supplier change log cache corrupted

- Replication manager using invalid credentials

- Replication sending a thread in a halted state

- Schema conflicts

- Unallowed operation on the consumer due to Update Resolution Protocol (URP) conflicts

- Network disconnection

- Consumer state locked down by an unavailable supplier

- Consumer out of disk

- RUVs contain meaningless information, such as `ffff, cleanruv`

Possible Causes of a Replication Divergence

Replication divergence could be caused by one of the following:

- Consumer power lower than the supplier
- Consumer disks getting to their upper read/write limits
- Intermittent network and packet dropping issues
- Change log in-memory cache not being used

Collecting Data About a Replication Halt or Replication Divergence

This section describes how to collect information to help you troubleshoot a replication halt or replication divergence.

Collecting 6.x Error and Change Logs

Collect errors logs from the consumer that is not getting the changes as well as the supplier of this consumer. By default, the errors logs are located in the following directory:

install-path/logs/errors

If the errors log is not in the default location, find the path to the log using the dsconf command as follows:

```
# dsconf get-log-prop -h host -p port ERROR path
```

The errors log must have the replication logging level enabled. You can use the DSCC to enable the replication logging level or enable it using the command line as follows:

```
# dsconf set-log-prop -h host -p port ERROR level:err-replication
```

You should also provide a listing of the supplier's change log , which is located in the same directory as the database. To find the path to your database, use the dsconf command as follows:

```
# dsconf get-suffix-prop -h host -p port suffix-dn db-path
```

Use the following command to provide a listing of the supplier's change log directory:

```
# ls -la /db-path/c15*
```

Collecting 5.x Errors and Change Logs

The errors log in 5.x and earlier versions of Directory Server are located in the following directory:

install-path/slapd-*serverID*/logs/errors

If the error log file is not in the default location, examine the Directory Server configuration file, *install-path*/slapd-*serverID*/config/dse.ldif, to find the path to the logs. The path is specified as the value of the nsslapd-errorlog attribute.

Provide a listing of the supplier's change log directory as follows:

```
# ls -la changelog-dir
```

If the change log file is not in the default location, examine the Directory Server configuration file, *install-path*/slapd-*serverID*/config/dse.ldif, to find the path to the logs. The path is specified as the value of the nsslapd-changelogdir attribute.

Collecting Data Using the insync and repldisc Commands

Use the output of the insync and repldisc commands to help troubleshoot your replication divergence.

The insync command indicates the state of synchronization between a master replica and one or more consumer replicas and can help you identify bottlenecks. If you are troubleshooting a problem with replication divergence, this data must be periodic. For more information, see "Using the insync Command" on page 37.

If you identify a bottleneck using the insync command, for example a bottleneck that results from an increasing delay as reported by the tool, it is helpful to start collecting nsds50ruv and ds6ruv attribute data. This data can help you identify when and where the potential halt is taking place. For more information about the nsds50ruv and ds6ruv attributes, see "About Replica Update Vectors (RUVs)" on page 34.

The repldisc command displays the replication topology, building a graph of all known replicas, then showing the results as a matrix. For more information, see "Using the repldisc Command" on page 38.

Collecting Information About the Network and Disk Usage

Try to determine if the replication halt is network related using the netstat command on both the consumer and supplier as follows:

```
# netstat -an | grep port
```

A replication halt may be the result of the network if a consumer is not receiving information despite the fact that access logs show that the supplier is sending updates. Running the ping and traceroute commands can also help you determine if network latency is responsible for the problem.

Collect swap information to see if you are running out of memory. Memory may be your problem if the output of the swap command is small.

Solaris	swap -l
HP-UX	swapinfo
Linux	free

Windows	Already provided in `C:\report.txt`

Try to determine if the disk controllers are fully loaded and if input/output is the cause of your replication problems. To determine if your problem is disk related, use the `iostat` tool as follows:

```
# iostat -xnMCz -T d 10
```

The `iostat` command iteratively reports terminal, disk, and tape input/output activity and can be helpful in determining if a replication divergence event results from a saturated disk on the consumer side.

Analyzing Replication Halt Data

Use the data you collected to determine if the replication halt is the result of a problem on the supplier or the consumer.

Use the `nsds50ruv` attribute output that you collected to determine the last CSN that was replicated to a particular consumer. Then, use the consumer's access and errors logs, with the logs set to collect replication level output, to determine the last CSN that was replicated. From this CSN, you can determine the next CSN that the replication process is failing to provide. For example, replication may be failing because the supplier is not replicating the CSN, because the network is blocking the CSN, or because the consumer is refusing to accept the update.

Maybe the CSN cannot be updated on the consumer. Try to `grep` the CSN that the supplier can not update on the consumer as follows:

```
grep csn=xxxxxxxx  consumer-access-log
```

If you do not find the CSN, try searching for the previous successful CSN committed to the supplier and consumer that are currently failing. Using CSNs, you can narrow your search for the error.

By using the `grep` command to search for CSNs in the access and errors logs, you can determine if an error is only transient. Always match the error messages in the errors log with its corresponding access log activity.

If analysis proves that replication is always looping in the same CSN with an `etime=0` and an `err=32` or `err=16`, the replication halt is likely to be a critical error. If the replication halt arises from a problem on the consumer, you can run the `replck` tool to fix the problem by patching the contents of the looping entry in the physical database.

If instead analysis proves that replication is not providing any report of the CSN in the consumer logs, then the problem is likely the result of something on the supplier side or

network. If the problem originates with the supplier, you can sometimes restart replication by forcing the replication agreement to send updates to the remote replica or by restarting the supplier. Otherwise, a reinitialization may be required.

To force updates to the remote replica from the local suffix, use the following command:

```
# dsconf update-repl-dest-now -h host -p port suffix-DN host:port
```

Resolving a Problem With the Schema

If the error log contains messages indicating a problem with the schema, then collect further schema related information. Before changes are sent from a supplier to a consumer, the supplier verifies that the change adheres to the schema. When an entry does not comply to the schema and the supplier tries to update this entry, a loop can occur.

To remedy a problem that arises because of the schema, get a single supplier that can act as the master reference for schema. Take the contents of its /*install-path*/config/schema directory. Tar the directory as follows:

```
# tar -cvs schema schema.tar
```

Use FTP to export this tar file to all of the other suppliers and consumers in your topology. Remove the /*install-path*/config/schema directory on each of the servers and replace it with the tar file you created on the master schema reference.

Analyzing Replication Divergence Data

Try to determine if the replication divergence is a result of low disk performance on the consumer using the output of the iostat tool. For more information about diagnosing disk performance problems, see .

Replication divergence is typically the result of one of the following:

- The supplier is not fast enough when sending the data to the consumer. For example, the supplier's changelog has low in-memory cache settings. Confirm these settings by looking at the nsslapd-cachememsize and nsslapd-cachesize attribute values in the cn=changelog5,cn=config entry.

  The nsslapd-cachememsize attribute specifies the changelog, or database, cache size in terms of the available memory space. The nsslapd-cachesize attribute specifies the replication changelog, or database, cache size in terms of the number of entries it can hold.

- The network's capacity is not large enough to guarantee transport speed at the rate that updates are generated. The network capacity may the problem when operating over a very low bandwidth.

- On Directory Server 5.1, the network latency is too large to guarantee transport speed at the rate that updates are generated. Network latency can cause problems with Directory Server 5.1 because the replication transport protocol is synchronous.

- Consumer not fast enough to apply the changes is receives. For example, consumer speed can be an issue when disk usage is saturated or when a problem occurs when replication is happening in parallel (unindexed searches, for example).

Analysis on Earlier Versions of Directory Server

If you are working on the 5.1 version of Directory Server and are experiencing replication divergence, it may be a result of protocol limits. Replication in 5.1 is synchronous, and therefore is not supported over a WAN. If you are replicating over a WAN, you must upgrade.

If replicating over a LAN, verify the network latency between the supplier and consumers using the ping command. In the 5.1 version of Directory Server, a supplier can only send changes once it receives an acknowledgement from the consumer. This results in consumer downtime that may resemble a halt when in fact the exchange is only slow. For example, you may update a password, but the new password does not go into effect immediately, giving you the impression that you are experiencing a replication divergence. Analyze the access log of the supplier and see how many updates are received, second by second. For example, the supplier access log should show varied traffic for each second, such as:

```
13:07:04  14
13:07:05  10
13:07:06  15
13:07:07   5
```

Next, look in the access log of the consumer. It may show continuous updates, suggesting a bottleneck:

```
13:07:04   8
13:07:05   8
13:07:06   8
13:07:07   8
```

If you are experiencing a problem of this kind, it may be the result of your method of network access, bandwidth, or small links.

Advanced Topic: Using the `replcheck` Tool to Diagnose and Repair Replication Halts

Advanced users can use the `replcheck` tool to check and repair replication on Directory Server 6.x. We strongly recommend that you use this tool with the guidance of Sun Support. The tool collects valuable information that Sun Support can use during problem diagnosis and can

repair several types of replication halt directly. This tool is located in the *install-path*/ds6/support_tools/bin/ directory.

Note – A earlier version of the replcheck tool is available for Directory Server 5.x. Contact Sun Support for more information.

For more information about the replcheck command, seereplcheck(1M)

Diagnosing Problems with replcheck

When run in diagnosis mode, the replcheck tool diagnoses the cause of the replication breakage and summarizes the proposed repair actions. It compares the RUVs for each of the servers in your replication topology to determine if the masters are synchronized. If the search results show that all of the consumer replica in-memory RUVs are evolving on time or not evolving but equal to those on the supplier replicas, the tool will conclude that a replication halt is not occurring.

To diagnose a replication problem, run the replcheck tool as follows:

```
replcheck diagnose topology-file
```

The *topology-file* specifies the path to a file that contains one record for each line in the following format: *hostname*:*port*:*suffix_dn*[:*label*]. The optional *label* field provides a name that appears in any messages that are displayed or logged. If you do not specify a *label*, the *hostname*:*port* are used instead.

For example, the following topology file describes a replication topology consisting of two hosts:

```
host1:389:dc=example,dc=com:Paris
host2:489:dc=example,dc=com:New York
```

Repairing Replication Failures With replcheck

If the replcheck diagnose command determines that a replication halt is occurring, then you can launch the replcheck fix subcommand to repair the replication halt. For example, the command determines that replication is blocked on the entry associated with CSN 24 if a supplier has a CSN of 40, while the consumer has a CSN of 23 that does not evolve at all over time.

To repair a replication halt, run the replcheck fix command as follows:

```
replcheck fix TOPOLOGY_FILE
```

Reinitializing a Topology

This section describes how to analyze your topology to determine which systems need to be reinitialized. It also describes the methods you can use to reinitialize your replication topology.

Note – When a replica has been reinitialized, all of its consumer replicas must also be reinitialized.

Determining What to Reinitialize

When you reinitialize your topology, you take a good copy of the data from a supplier and overwrite the bad data on the consumers in the topology. Before you reinitialize your topology, determine which systems are unsynchronized and need to reinitialized. This critical step can prevent your from wasting time by overwriting data that is already synchronized.

For example, the following figure illustrates a topology where replication is broken on hub 1.
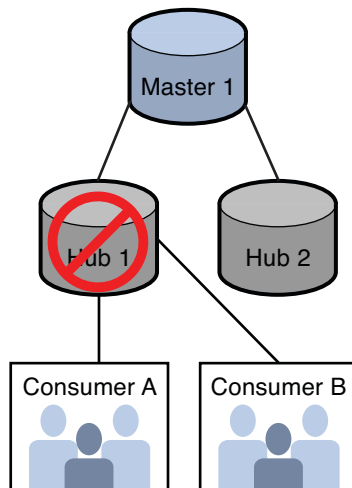
Because hub 1 provided data to consumers A and B, you need to reinitialize hub 1, consumer A, and consumer B.

In the following example, consumers A and B also receive updates from hub 2.
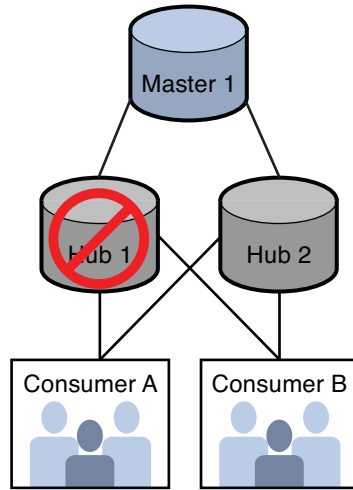
Consumers A and B may be synchronized with the supplier of the reinitialized replica because they receive updates from both hubs. Their status depends on which replica you select to reinitialize your topology. If you use RUVs to ensure that you have the latest changes, then these replicas may be up-to-date and you may not need to reinitialize consumers A and B.

Overview of Reinitialization Methods

You can use the following methods to reinitialize your topology:

- Using the DSCC. This method is best if you are reinitializing only a single server or several small databases.

  For more information about using the DSCC to reinitialize your topology, see "To Reinitialize a Suffix Using the DSCC" on page 51

  Note – You can not use earlier versions of the console to reinitialize replication on Directory Server 5.x.

- Using an import and export operation.

  You can reinitialize a suffix by exporting the data and then importing it everywhere else in your topology. This method is appropriate for a big system and only applies to one suffix.

  For information about reinitializing replication using an import and export, see "Replica Initialization From LDIF" in *Sun Java System Directory Server Enterprise Edition 6.2 Administration Guide*.

- Using a binary copy.

A binary copy enables you to clone an entire server by using the binary backup files from one server to restore the identical directory contents onto another server. You can use a binary copy to reinitialize any server from the binary copy of a master or hub server, or a consumer from the binary copy of another consumer server. This method is available in Directory Server 5.2 and later. This method is the fastest, though poses some restriction on 5.x and earlier versions of Directory Server.

For information about reinitializing replication using a binary copy, see "Initializing a Replicated Suffix by Using Binary Copy" in *Sun Java System Directory Server Enterprise Edition 6.2 Administration Guide*.

Doing a Clean Reinitialization

All of the reinitialization methods copy unnecessary data, for example data that contains values that were deleted or that maintain state information or other historical data. This unnecessary data makes the entry larger in disk. Also, the entry state information may need to be purged. If the root cause of the replication problem is related to this state information, the data is still present in the database and can cause another replication error. To avoid importing this unnecessary and potentially problematic data, you can do a clean reinitialization of your topology.

When you do a clean reinitialization, you create a clean master copy of the data that contains smaller databases, indexes, and empty change logs. A clean reinitialization uses less disk space and takes less time because it does not make backup copies of the database files. It also reduces index fragmentation, which can reduce performance. However, it requires you to stop the server that is being cloned to ensure that the database files are in a coherent state.

▼ To Create Clean Master Data in a 6.2 Version of Directory Server

1   **Stop the master server.**

2   **Export the database contents using the** dsadm **command.**
    Specify the -Q option so that replication information is not included in the export.
    ```
    # dsadm export -Q instance-path suffix-DN  /tmp/clean-export.ldif
    ```

3   **Reimport the exported data to the same master server using the** dsadm **command.**
    ```
    # dsadm import instance-path /tmp/clean-export.ldif suffix-DN
    ```

4   **Restart the master server.**
    The master server now contains clean data, meaning it contains smaller databases, indexes, and empty change logs.

5 Import the clean master data, to all of the other servers in your system.

Use one of the three methods described in "Overview of Reinitialization Methods" on page 49.

▼ To Create Clean Data in a 5.x Version of Directory Server

1 Stop the master server.

2 Export the database contents using the db2ldif **script without the** -r **option.**

```
# db2ldif -n database1 -a /tmp/clean-export.ldif
```

3 Reimport the exported data to the same master server using the ldif2db **script.**

```
# ldif2db -n database1 -i /tmp/clean-export.ldif
```

4 Restart the master server.

The master server now contains clean data, meaning it contains smaller databases, indexes, and empty change logs.

5 Import the clean master data, to all of the other servers in your system.

Use one of the three methods described in "Overview of Reinitialization Methods" on page 49.

▼ To Reinitialize a Suffix Using the DSCC

This method requires a replication agreement between the supplier and the consumers suffixes. Use this method to reinitialize a single suffix or to reinitialize many small suffixes.

Note – If you are using an earlier version of the Directory Server console, go to the Configuration panel and select the Replication node. Select the suffix you want to initialize in the consumer. Select the replication agreement to the consumer. Right click the agreements and select Initialize consumer now.

---

1 On the supplier server, log in to DSCC.

2 Click the Directory Servers tab, then click the Suffixes tab.

3 In the Suffixes tab, select the suffix or suffixes that you need to reinitialize.

Select Initialize Suffix from Data from the drop-down menu.

4 In Step 1, select Initialize Using Existing Replication Agreements.

5 In Step 2, specify the supplier suffix from which you want to copy the data.

6   Verify that the import is complete by checking the errors log of the consumers.

4

Troubleshooting Directory Proxy Server

This chapter describes how to troubleshoot problem you encounter with Directory Proxy Server. It contains the following sections:

- "Collecting Generic Directory Proxy Server Data" on page 53
- "Troubleshooting Directory Proxy Server Installation Problems" on page 55
- "Troubleshooting Problems With the Directory Proxy Server Process" on page 56

Collecting Generic Directory Proxy Server Data

No matter the type of problem you are encountering, there is a minimum set of data that needs to be collected and, if necessary, provided to Sun Support.

Collecting Version Information for Directory Proxy Server

The following sections describe how to collect configuration information on current and previous versions of Directory Proxy Server.

Collecting Directory Proxy Server 6.2 Version Information

Collect the Directory Proxy Server 6.2 version information. This information is available in the *instance-dir*/logs/error file. For example, the error log displays the version information as follows:

```
[21/May/2007:18:01:27 +0200] - STARTUP    - INFO  - \
Sun-Java(tm)-System-Directory-Proxy-Server/6.1 B2007.134.2156 started \
on host server1 in directory /local/dps.3333
```

Collecting Directory Proxy Server 5.x Version Information

If you are using migrated Directory Proxy Server 5.x instances, collect the version information as follows:

```
# install-path/bin/dps/server/bin/ldapfwd -v
```

On UNIX and Linux systems, you might see the following error:

```
ld.so.1: ldapfwd: fatal: libnss3.so: open failed: No such file or directory
```

If you see this error, set the LD_LIBRARY_PATH to include Directory Proxy Server libraries in your load path. For example, if you use sh, use the following command:

```
# export LD_LIBRARY_PATH=install-path/lib
```

Running the dpadm Command in Verbose Mode

Running the dpadm command in verbose mode will provide information to help troubleshoot problems that occur during instance creation or deletion, data backup, and so on. Run the dpadm is verbose mode as follows:

```
# dpadm -v
```

Collecting Directory Proxy Server Configuration Information

The following sections describe how to collect configuration information on current and previous versions of Directory Proxy Server.

Collecting Configuration Information on Directory Proxy Server 6.2

Collect the Directory Proxy Server 6.2 configuration information. This information is available in the *instance-dir*/logs/error file. For example, the error log displays the configuration information as follows:

```
user@server1 local]$ more dps.3333/logs/errors
[21/May/2007:18:01:27 +0200] - STARTUP    - INFO - Global log level INFO (from config)
[21/May/2007:18:01:27 +0200] - STARTUP    - INFO - Logging Service configured
[21/May/2007:18:01:27 +0200] - STARTUP    - INFO - Java Version: 1.5.0_09 (Java Home: \
/local/jre)
[21/May/2007:18:01:27 +0200] - STARTUP    - INFO - Java Heap Space: Total Memory (-Xms) \
= 246MB, Max Memory (-Xmx) = 246MB
[21/May/2007:18:01:27 +0200] - STARTUP    - INFO - Operating System: \
Linux/i386 2.6.17-1.2139_FC5smp
```

Collecting Configuration Information on Directory Proxy Server 5.x

Collect the Directory Proxy Server 5.x configuration information as follows:

```
# cd install-path/bin/dps_utilities
# ./dpsconfig2ldif -t install-path/dps-name/etc/tailor.txt.backup \
-o /tmp/DPS_tailor_Config.ldif
```

The `DPS_tailor_Config.ldif` file contains configuration information formatted as follows:

```
Begin configuration_url:file:///server-root/instance/
etc/tailor.ldif#cn=dps-instance1,cn=Sun ONE Directory Proxy Server,
cn=ServerGroup (1),cn=instance1.example.com,ou=example.com,
o=NetscapeRoot End
```

Collecting Directory Proxy Server Log Information

Collect the Directory Proxy Server logs. By default, the logs are stored in the following directory:

instance-path/`logs`

If you are providing this information to Sun Support, you should also include the generic Directory Server data from the various Directory Servers involved. This generic data includes the Directory Server version and the Directory Server access, error, and audit logs. For more information about collecting the Directory Server generic information, see "Collecting Generic Data" on page 22.

Include generic information about any other backend servers you may be using, such as JDBC backends, a SQL database, or an Oracle database.

Troubleshooting Directory Proxy Server Installation Problems

This section describes procedures to help you debug problems installing Directory Proxy Server. It includes the following:

Troubleshooting Directory Proxy Server 5.2 Installation Failures

Installation may fail if the password contains a dollar sign ($) character, such as pa$$word. For example, you might get the following error message:

```
[4] stderr > Can't read "word" no such variable
```

When the installer parses the password it interprets the text after the dollar sign, $*word*, as a variable, and this variable does not exist.

Change the password to not include the dollar sign character.

Troubleshooting Problems Starting Directory Proxy Server 5.2 on Windows

If Directory Proxy Server 5.2 fails to start on Windows, check the following:

1. Check that no keys remain in the registry, such as `dps`, `sunOne`, `idar`, `dar` and `iplanet`.

2. Remove the product registry file located in the `C:\WINNT\System32` directory.

3. Reboot your machine.

   Try to reinstall Directory Proxy Server

You may also need to manually remove the `Localmachine->system->controlset001->services->admin52` entry. This entry may be causing your problem if you receive the following error in the Admin server install log:

```
Error: Writing Administration Server service keys to the Windows registry... failed.
```

Troubleshooting Problems With the Directory Proxy Server Process

This section describes procedures for the following:

- "Overview of Process Troubleshooting Tools" on page 56
- "Troubleshooting a Hung or Unresponsive Directory Proxy Server Process" on page 58
- "Troubleshooting a Crashed Directory Proxy Server Process" on page 60

Overview of Process Troubleshooting Tools

Some tools are provided with Solaris and Java which may help you troubleshoot process issues. The following sections provide an overview of some of the most useful tools

Using Java Tools With Directory Proxy Server 6.2

As Directory Proxy Server 6.2 is a pure Java application, you can use the Java tools that are delivered with the JDK 1.5 to help troubleshoot problems. These tools include the following:

- jstack. This tool provides information about the Directory Proxy Server thread stack.
- jmap. This tool provides information about memory. For example, running jmap –histo *PID* prints a histogram of the heap.
- jinfo. This tool provides you with information about the JVM environment.
- jstat. This tool displays performance statistics for a JVM.

On Solaris, you can find these tools in the following location:

```
/usr/lang/JAVA/jdk1.5.0_03/solaris-sparc/bin
```

The JVM also includes a graphical tool for monitoring the Java virtual machine called the Java Monitoring and Management Console (JConsole) tool. This tool uses the Java virtual machine to provide information on performance and resource consumption of applications running on the Java platform using Java Management Extension (JMX) technology. JConsole can be used to observe information about an application running on the Java platform. The JConsole provides information and charts about memory use, thread use, class loading, and JVM parameters

On Unix platforms, if the kill -QUIT process-id command is used to get thread dump and it does not work, use jstack.

Using Solaris Tools With Directory Proxy Server 5.x

Solaris includes a collection of process tools to help you collect more information about process problems, such as a hung process, crashed process, or memory usage problems. These tools include the following:

- pmap — shows the process map, which includes a list of virtual addresses, where the dynamic libraries are loaded, and where the variables are declared.
- pstack — shows the process stack. For each thread in the process, it describes the exact stack of instruction the thread was executing at the moment when the process died or when the pstack command was executed.
- pfiles— reports information about all open files in each process.
- pldd — list the dynamic libraries linked into each process.

Troubleshooting a Hung or Unresponsive Directory Proxy Server Process

This section describes how to troubleshoot a unresponsive or hung Directory Proxy Server process. A totally unresponsive process is called a hang. The remainder of this section describes how to collect and analyze data about a hang.

Collecting Data About a Directory Proxy Server 6.2 Hang on Solaris

The jstat tool tells you the amount of CPU being used for each thread. If you collect a thread stack using the jstack utility at the same time you run the jstat tool, you can then use the jstack output to see what the thread was doing when it had trouble. If you run the jstack and jstat tools simultaneously several times, you can see over time if the same thread was causing the problem and if it was encountering the problem during the same function call.

To get the process ID of the running Directory Proxy Server, use the jps command. For example, the command is run as follows on Solaris:

```
# jps
8393 DistributionServerMain
2115 ContainerPrivate
21535 startup.jar
16672 Jps
13953 swupna.jar
```

Collect usage information as follows:

```
# ./scp DPS-PID
```

The *DPS-PID* field specifies the PID of the unresponsive process.

On Solaris and other UNIX platforms, show system calls that occur during the crash using the truss command as follows:

```
truss -o /tmp/trace.txt -ealf -rall -wall -vall -p 21362
```

The value 21362 corresponds to the PID of the unresponsive process.

Collecting and Analyzing Data About a Directory Proxy Server 5.x Hang on Solaris

The prstat tool tells you the amount of CPU being used for each thread. If you collect a process stack using the pstack utility at the same time you run the prstat tool, you can then use the pstack output to see what the thread was doing when it had trouble. If you run the prstat and pstack tools simultaneously several times, then you can see over time if the same thread was causing the problem and if it was encountering the problem during the same function call.

Note – On Linux, use the `lsstack` or `pstack` commands instead of the Solaris `pstack` utility.

The following script automates the process of running these tools:

```
cat scp
#!/bin/sh

i=0
while [ "$i" -lt "10" ]
do
        echo "$i\n"
        date='date "+%y%m%d:%H%M%S"'
        prstat -L -p $1 0 1 > /tmp/prstat.$date
        pstack $1 > /tmp/pstack.$date
        i='expr $i + 1';
        sleep 1
done
```

The value `10` in the `[ "$i" -lt "10" ]` line can be increased or decreased to suit the time during which the problem you are troubleshooting occurs. This adjustment allows to you collect a full set of process data to help troubleshoot the issue. Thus enabling a full process data set to be captured around the issue.

Collect usage information as follows:

```
# ./scp DPS-PID
```

The *DPS-PID* field specifies the PID of the unresponsive process.

On Solaris and other UNIX platforms, show system calls that occur during the crash using the `truss` command as follows:

```
truss -o /tmp/trace.txt -ealf -rall -wall -vall -p 21362
```

The value 21362 corresponds to the PID of the unresponsive `ldapfwd` process.

Analyzing Data About a Hang

Whenever the Directory Proxy Server crashes, it generates a core. With this core file and the process stack of the core file you obtained, you can analyze the problem. For information about analyzing a core file, see "Examining a Core File on Solaris" on page 68. However, rather than running the utility from the ns-slapd binary directory, you must run it from the

For example, the output of the `truss` command shows that no systems calls have been made at the time of the crash, suggesting a passive hang. Looking at the core file and the `jstack` or

`pstack` information, you can identify several threads that are waiting for a lock to be freed to continue processing. By comparing the out put of the various tools you can safely guess that the cause of the problem is a deadlock. With this information, Sun Support can better help you resolve your problem in a timely fashion.

Troubleshooting a Crashed Directory Proxy Server Process

Core file and crash dumps are generated when a process or application terminate abnormally. Analyzing these files can help you identify the cause of your problem.

This section includes the following topics:

- "Getting the Core and Shared Libraries" on page 60
- "Analyzing the Directory Proxy Server 6.2 Core Data on Solaris" on page 60
- "Analyzing the Directory Proxy Server 5.x Core Data on Solaris" on page 61
- "Analyzing the Directory Proxy Server 5.x Core Data on Linux" on page 63
- "Analyzing the Directory Proxy Server 5.x Core Data on HP-UX " on page 63
- "Analyzing the Directory Proxy Server 5.x Core Data on Windows" on page 64

Getting the Core and Shared Libraries

Get all the libraries and binaries associated with the Directory Proxy Server process for core file analysis. You must configure your system to allows Directory Proxy Server to generate a core file if the server crashes. For more information about generating a core file, see "Generating a Core File" on page 66.

Collect the libraries using the `pkg_app` script . The `pkg_app` script packages an executable and all of its shared libraries into one compressed tar file. You provide the process ID of the application and, optionally, the name of the core file to be opened. For more information about the `pkg_app` script see "Using the `pkg_app` Script on Solaris" on page 23.

As `superuser`, run the `pkg_app` script as follows:

```
# pkg_app pid core-file
```

Note – You can also run the `pkg_app` script without a core file. This reduces the size of the script output. You need to later set the variable to the correct location of the core file.

Analyzing the Directory Proxy Server 6.2 Core Data on Solaris

Once you have obtained a core file, run the `jstack` and `jpmap` Java tools on the file.

Run the `jstack` utility as follows:

```
# jstack process-ID
```

For example, the jstack utility creates the following output:

```
# jstack 8393
Attaching to process ID 8393, please wait...
Debugger attached successfully.
Server compiler detected.
JVM version is 1.5.0_03-b07
Thread t@1: (state = BLOCKED)

Thread t@42: (state = IN_NATIVE)
 - sun.nio.ch.ServerSocketChannelImpl.accept0(java.io.FileDescriptor, java.io.FileDescriptor, \
java.net.InetSocketAddress[]) (Interpreted frame)
 - sun.nio.ch.ServerSocketChannelImpl.accept0(java.io.FileDescriptor, java.io.FileDescriptor, \
java.net.InetSocketAddress[]) (Interpreted frame)
 - sun.nio.ch.ServerSocketChannelImpl.accept() @bci=130, line=145 (Interpreted frame)
 - com.sun.directory.proxy.extensions.ExtendedTCPClientListener.run() @bci=267, \
line=190 (Interpreted frame)

Thread t@41: (state = IN_NATIVE)
 - sun.nio.ch.ServerSocketChannelImpl.accept0(java.io.FileDescriptor, java.io.FileDescriptor, \
java.net.InetSocketAddress[]) (Interpreted frame)
 - sun.nio.ch.ServerSocketChannelImpl.accept0(java.io.FileDescriptor, java.io.FileDescriptor, \
java.net.InetSocketAddress[]) (Interpreted frame)
 - sun.nio.ch.ServerSocketChannelImpl.accept() @bci=130, line=145 (Interpreted frame)
 - com.sun.directory.proxy.extensions.ExtendedTCPClientListener.run() @bci=267, \
line=190 (Interpreted frame)
```

Analyzing the Directory Proxy Server 5.x Core Data on Solaris

Once you have obtained a core file, run the pstack and pmap Solaris utilities on the file.

Run the pstack utility as follows:

```
# pstack core-file > /tmp/pstack.txt
```

For example, the pstack utility creates the following output:

```
core '/var/core/core_dps-dr-zone1_ldapfwd_0_0_1156942096_3167' of 3167: ./ldapfwd
-t /var/opt/mps/serverroot/dps-dps-dr-zone1/etc/tailor.txt
----------------  lwp# 1 / thread# 1  --------------------
 fedc0b6c __pollsys (ffbff680, 2, ffbff610, 0, 0, 1770) + 8
 fed5cea8 poll     (ffbff680, 2, 1770, 10624c00, 0, 0) + 7c
 ff19c610 _pr_poll_with_poll (1770, ffbff680, 927c0, ffbff91c, 2, 1) + 42c
 00039504 __1cLCAI_LF_CmgrDrun6F_v_ (75, 115d74, 11202c, 2, 88c00, 116510) + 1a8
 00062070 ldapfwdMain (0, ffbffa84, c, 9952c, feb60740, feb60780) + 1c
 0002f968 _start   (0, 0, 0, 0, 0, 0) + 108
```

```
---------------- lwp# 3 / thread# 3 --------------------
 fedc0b6c __pollsys (fea19b70, 3, fea19b00, 0, 0, 3e8) + 8
 fed5cea8 poll     (fea19b70, 3, 3e8, 10624c00, 0, 0) + 7c
 ff19c610 _pr_poll_with_poll (3e8, fea19b70, 186a0, fea19e8c, 3, 2) + 42c
 0005de38 __1cIidarPollEwait6MI_i_ (fea19e6c, 186a0, 16e360, 1, 0, 1) + 20
 000639ec __1cJHeartbeatJheartbeat6Fpv_1_ (158f40, 1, 14da70, faa36, 16e360, faa5d) + 114
 fedbfd9c _lwp_start (0, 0, 0, 0, 0, 0)
---------------- lwp# 136734 / thread# 136734 --------------------
 fedbfe40 __lwp_park (0, 0, 116710, 0, 0, 1) + 14
 00076548 __1cMCAI_LF_MutexHacquire6M_v_ (116708, fd2bc, 0, 46, fea24800, 1000) + 34
 00076158 __1cPCAI_LF_RefCountGAddRef6M_v_ (116708, 156510, 2400, 26dc, 11667c, 800) + 24
 0006ddb0 __1cVCAI_LF_ReferralServer2t5B6MpnPCAI_LF_ConnPair_pnVCAI_LF_RequestMessage_pnNCAI_LF_Server
_ipcibbi_v_ (197198, fe7790d8, 1541c0, 156510, 185, 1565b8) + 50
 00046324 __1cPCAI_LF_ConnPairYstart_referral_operation6MipCpnNCAI_LF_Server_i_i_ (fe7790d8, 1, 1565b8
, 156510, 1, 197198) + 26c
 0004f2a0 __1cPCAI_LF_ConnPairLsend_result6MrnOCAI_LF_Message_rnVCAI_LF_RequestMessage__v_ (fe7790d8,
156eb8, 1541c0, 2400, 0, 0) + 354
 00044758 __1cPCAI_LF_ConnPairOinner_activity6MpnOCAI_LF_Message__v_ (fe7790d8, 156eb8, 11202c, f4f27,
fe7790f8, 1) + 114c
 00045c24 __1cPCAI_LF_ConnPairDrun6M_v_ (fe7797c8, 198383, 170c78, fe7790d8, fe779e54, fe779740) + 6cc
 00046cd0 CAI_LF_StartFunction (157500, 11202c, 1, 0, 46ab4, 1) + 21c
 fedbfd9c _lwp_start (0, 0, 0, 0, 0, 0)
---------------- lwp# 136735 / thread# 136735 --------------------
 fedc0b6c __pollsys (fe9e8d98, 3, fe9e8d28, 0, 0, 1d4c0) + 8
 fed5cea8 poll     (fe9e8d98, 3, 1d4c0, 10624c00, 0, 0) + 7c
 ff19c610 _pr_poll_with_poll (1d4c0, fe9e8d98, b71b00, fe9e9e74, 3, 2) + 42c
 0005de38 __1cIidarPollEwait6MI_i_ (fe9e9e54, b71b00, 1, f4f27, fe9e90f8, 12d8d0) + 20
 00045cbc __1cPCAI_LF_ConnPairDrun6M_v_ (fe9e97c8, 17bb43, 130ff8, fe9e90d8, fe9e9e54, fe9e9740) + 764
 00046cd0 CAI_LF_StartFunction (157500, 11202c, 1, 0, 46ab4, 1) + 21c
 fedbfd9c _lwp_start (0, 0, 0, 0, 0, 0)
---------------- lwp# 136738 / thread# 136738 --------------------
 fedc0b6c __pollsys (fe9a8d98, 3, fe9a8d28, 0, 0, 1d4c0) + 8
 fed5cea8 poll     (fe9a8d98, 3, 1d4c0, 10624c00, 0, 0) + 7c
 ff19c610 _pr_poll_with_poll (1d4c0, fe9a8d98, b71b00, fe9a9e74, 3, 2) + 42c
 0005de38 __1cIidarPollEwait6MI_i_ (fe9a9e54, b71b00, 1, f4f27, fe9a90f8, 0) + 20
 00045cbc __1cPCAI_LF_ConnPairDrun6M_v_ (fe9a97c8, 198123, 130fd8, fe9a90d8, fe9a9e54, fe9a9740) + 764
 00046cd0 CAI_LF_StartFunction (157500, 11202c, 1, 0, 46ab4, 1) + 21c
 fedbfd9c _lwp_start (0, 0, 0, 0, 0, 0)
---------------- lwp# 136788 / thread# 136788 --------------------
 00197d68 ???????? (116708, 1, 156510, 0, 0, 1000)
 0006dee4 __1cVCAI_LF_ReferralServer2T6M_v_ (155780, 1000, fedecbc0, fea25c00, fe779780, 0) + 34
 000707c4 __SLIP.DELETER__A (155780, 1, 4, a6c, 1, 2400) + 4
 00046a94 CAI_LF_ReferralStartFunction (155780, fe6da000, 0, 0, 46a64, 1) + 30
 fedbfd9c _lwp_start (0, 0, 0, 0, 0, 0)
```

You can also use the mdb or adb command instead of the pstack command to show the stack of the core. The mdb command is a modular debugger and the adb command is a general purpose debugger that is part of Solaris. Run the mdb command as follows:

```
# mdb $path-to-executable $path-to-core
$C to show the core stack
$q to quit
```

The output of the mdb and the pstack commands provide helpful information about the process stack at the time of the crash. The mdb $C command output provides the exact thread that was executing at the time of the crash.

On Solaris 8 and 9, the first thread of the pstack output often contains the thread responsible for the crash. On Solaris 10, use mdb to find the crashing thread or, if using the pstack command, analyze the stack by looking for threads that do not contain lwp-park, poll, and pollsys.

On Solaris, you can also use the Solaris dbx symbolic debugger, which is a developer tool available free from http://sun.com/. The dbx tool provides symbolic debugging, and includes variables that can be manipulated. For example, the dbx debugger produces the following output:

```
current thread: t@2482121
=>[1] 0x0(0x156138, 0x0, 0xff000000, 0xfedefad4, 0x2, 0x2), at 0xffffffffffffffff
  [2] CAI_LF_RefCount::Release(0x116708, 0x1, 0x156138, 0x0, 0x0, 0x1000), at 0x7629c
  [3] CAI_LF_ReferralServer::~CAI_LF_ReferralServer(0x241270, 0x1000, 0xfedecbc0, 0xfe097c00,
0xfe8d9780, 0x0), at 0x6dee4
  [4] __SLIP.DELETER__A(0x241270, 0x1, 0x4, 0xa6c, 0x1, 0x2400), at 0x707c4
  [5] CAI_LF_ReferralStartFunction(0x241270, 0xfe81a000, 0x0, 0x0, 0x46a64, 0x1), at 0x46a94
```

Analyzing the Directory Proxy Server 5.x Core Data on Linux

On Linux, use the lsstack or pstack commands instead of the Solaris pstack utility. For example, run the lsstack command as follows:

```
# lsstack /tmp/core-file
```

You can also use the GNU project debugger, gdb, to see what is happening at the time of the crash. Run this debugger as follows:

```
# gdb ./ldapfwd /tmp/core-file
```

For more information about the useful commands available with the gdb tool, see the gdb man page.

Analyzing the Directory Proxy Server 5.x Core Data on HP-UX

As for Linux, on HP-UX you can also use the GNU project debugger to see what is happening at the time of the crash. Run this debugger as follows:

```
# gdb ./ldapfwd /tmp/core-file
```

For more information about the useful commands available with the `gdb` tool, see the `gdb` man page.

Analyzing the Directory Proxy Server 5.x Core Data on Windows

On Windows, you can use the `WinDbg` debugger, which provides a UI for kernel and NT debugging. It can function both as a kernel-mode and user-mode debugger. You run this debugger on a Windows crash dump file.

Troubleshooting Directory Server Problems

This chapter describes how to troubleshoot general problems with Directory Server. It includes information about the following topics:

Troubleshooting a Crash

This section describe how to begin troubleshooting a crashed Directory Server process. It describes possible causes of a crash, what pieces of information you need to collect to help identify the problem, and how to analyze the information you collect.

Possible Causes of a Crash

A crash could be caused by one or more of the following:

- Buffer overflows
- Out of resources, such as memory, disk, or file descriptors
- Memory allocation problems, such as double frees or free unallocated memory
- NULL de-referencing
- Other programmatic errors

If a Directory Server process crashes, you need to open a service request with the Sun Support Center.

Collecting Data About a Crash

This section describes the data you need to collect when the server crashes. The most critical data to collect is the core file.

Note – If you contact the Sun Support Center about a crashed Directory Server process, you must provide a core file and logs.

Generating a Core File

Core file and crash dumps are generated when a process or application terminates abnormally. You must configure your system to allow Directory Server to generate a core file if the server crashes. The core file contains a snapshot of the Directory Server process at the time of the crash, and can be indispensable in determining what led to the crash. Core files are written to the same directory as the errors logs, by default, *instance-path*/logs/. Core files can be quite large, as they include the entry cache.

If a core file was not generated automatically, you can configure your operating system to allow core dumping by using the commands described in the following table and then waiting for the next crash to retrieve the data.

Solaris	`coreadm`
	
	or
	
	`ulimit -c unlimited`
	`ulimit -H -c unlimited`

Linux	`ulimit -c unlimited` `ulimit -H -c unlimited`
HPUX/AIX	`ulimit -c`
Windows	`Windows crashdump`

For example, on Solaris OS, you enable applications to generate core files using the following command:

```
# coreadm -g /path-to-file/%f.%n.%p.core -e global -e process \
 -e global-setid -e proc-setid -e log
```

The *path-to-file* specifies the full path to the core file you want to generate. The file will be named using the executable file name (%f), the system node name (%n), and the process ID (%p).

If after enabling core file generation your system still does not create a core file, you may need to change the file-size writing limits set by your operating system. Use the `ulimit` command to change the maximum core file size and maximum stack segment size as follows:

```
# ulimit -c unlimited
# ulimit -s unlimited
```

Check that the limits are set correctly using the -a option as follows:

```
# ulimit -a
time(seconds)        unlimited
file(blocks)         unlimited
data(kbytes)         unlimited
stack(kbytes)        unlimited
coredump(blocks)     unlimited
nofiles(descriptors) 256
vmemory(kbytes)      unlimited
```

For information about configuring core file generate on Red Hat Linux and Windows, see "Configuring the Operating System to Generate Core Files" in *Sun Gathering Debug Data for Sun Java System Directory Server 5*.

Next, verify that applications can generate core files using the kill -11 *process-id* command. The cores should be generated in either the specified directory or in the default *instance-name*/logs directory.

```
# cd /var/cores
# sleep 100000 &
[1] process-id
# kill -11 process-id
# ls
```

Getting the Core and Shared Libraries

Get all the libraries and binaries associated with the slapd process for core file analysis. Collect the libraries using the pkg_app script . The pkg_app script packages an executable and all of its shared libraries into one compressed tar file. You provide the process ID of the application and, optionally, the name of the core file to be opened. For more information about the pkg_app script see "Using the pkg_app Script on Solaris" on page 23.

As superuser, run the pkg_app script as follows:

```
# pkg_app server-pid core-file
```

Note – You can also run the pkg_app script without a core file. This reduces the size of the script's output. You need to later set the variable to the correct location of the core file.

Additional Information

To look at the log files created at the time the problem occurred, check the following files:

```
# install-path/instance-name/logs/errors*
# install-path/instance-name/logs/access*
```

If the crash is related to the operating system running out of disk or memory, retrieve the system logs. For example, on Solaris OS check the /var/adm/messages file and the /var/log/syslogs file for hardware or memory failures.

To get complete version output, use the following commands:

```
# cd install-path/bin/slapd/server
# ./ns-slapd -D install-path/instance-name -V
```

Analyzing Crash Data

Whenever the Directory Server crashes, it generates a core. With this core file and the process stack of the core file you obtained from the ns-slapd binary directory, you can analyze the problem.

This section describes how to analyze the core file crash data on a Solaris OS.

Examining a Core File on Solaris

Once you have obtained a core file, run the pstack and pmap Solaris utilities on the file. The pmap utility shows the process map, which includes a list of virtual addresses, where the dynamic libraries are loaded, and where the variables are declared. The pstack utility shows the process stack. For each thread in the process, it describes the exact stack of instruction the thread was executing at the moment when the process died or when the pstack command was executed.

These utilities must be run from the directory that contains the ns-slapd binary, root-dir/bin/slapd/server. Run the utilities as follows:

```
# pstack core-file
```

```
# pmap core-file
```

If the results of the pstack utility are almost empty, all of the lines in the output look as follows:

```
0002c3cc ???????? (1354ea0, f3400, 1354ea0, 868, 2fc, 1353ff8)
```

If your pstack output looks like this, confirm that you are running the utilities from the ns-slapd binary directory. If you did not run the utility from the ns-slapd binary directory, then go to the directory and rerun the utility.

You can also use the mdb command instead of the pstack command to know the stack of the core. Run the mdb command as follows:

```
# mdb $path-to-executable $path-to-core
$C to show the core stack
$q to quit
```

The output of the mdb and the pstack commands provide helpful information about the process stack at the time of the crash. The mdb $C command output provides the exact thread that caused the crash.

On Solaris 8 and 9, the first thread of the pstack output often contains the thread responsible for the crash. On Solaris 10, use mdb to find the crashing thread or, if using the pstack command, analyze the stack by looking for threads that do not contain lwp-park, poll, and pollsys.

For example, the following core process stack occurs during the call of a plug-in function:

```
core '../../../slapd-psvmrr3-27/logs/core' of 18301:    ./ns-slapd \
-D /opt/iplanet/servers/slapd-psvmrr3-27
-i /opt/iplanet/se
----------------  lwp# 13 / thread# 25  -------------------
 ff2b3148 strlen  (0, fde599fb, 0, fbed1, 706d2d75, fde488a8) + 1c
 ff307ef8 sprintf (7fffffff, fde488a0, fde599d8, fde599ec, 706d2d75, fde599fc) + 3c
 fde47cf8 ???????? (1354ea0, 850338, fde59260, e50243, 923098, 302e3800) + f8
 fde429cc ???????? (1354ea0, 3, 440298, 154290, 345c10, 154290) + 614
 ff164018 plugin_call_exop_plugins (1354ea0, 8462a0, d0c, ff1e7c70, ff202a94, 1353ff8) + d0
 0002c3cc ???????? (1354ea0, f3400, 1354ea0, 868, 2fc, 1353ff8)
 00025e08 ???????? (0, 1353ff8, fdd02a68, f3400, f3000, fbc00)
 fef47d18 _pt_root (362298, fe003d10, 0, 5, 1, fe401000) + a4
 fed5b728 _thread_start (362298, 0, 0, 0, 0, 0) + 40
```

When analyzing process stacks from cores, concentrate on the operations in the middle of the thread. Processes at the bottom are too general and processes at the top are too specific. The commands in the middle of the thread are specific to the Directory Server and can thus help you identify at which point during processing the operation failed. In the above example, we see the plugin_call_exop_plugins process call indicates a problem calling an external operation in the custom plug-in.

If the problem is related to the Directory Server, you can use the function call that seems like the most likely cause of the problem to search on SunSolve for known problems associated with this function call. SunSolve is located at http://sunsolve.sun.com/.

If you do locate a problem related to the one you are experiencing, confirm that it applies to the version of Directory Server that you are running. To get information about the version you are running, use the following command:

```
# ns-slapd -V
```

If after doing a basic analysis of your core files you cannot identify the problem, collect the binaries and libraries using the pkg_app script and contact the Sun Support Center.

Troubleshooting an Unresponsive Process

The type of performance problem you are experiencing depends on the level of CPU available as described in the following table. The first step in troubleshooting a Directory Server that is still running but no longer responding to client application requests is to identify which of the three types of performance issue it corresponds to.

TABLE 5–1 CPU Level Associated With Performance Problems

CPU Level	Problem Description
CPU = 0%	Passive hang, the server is completely unresponsive
CPU > 10% CPU < 90%	Performance drop, the server is operating but not at the expected rate
CPU = 100%	Active hang, the server is completely unresponsive

The remainder of this section describes the following troubleshooting procedures:

- "Symptoms of an Unresponsive Process" on page 70
- "Collecting Data About an Unresponsive Process" on page 70
- "Analyzing Data About a Unresponsive Process: an Example" on page 71
- "Troubleshooting Drops in Performance" on page 73
- "Troubleshooting Process Hangs" on page 77

Symptoms of an Unresponsive Process

If your error log contains errors about not being able to open file descriptors, this is usually a symptom of an unresponsive process. For example, the error log may contain a message such as the following:

```
[17/Jan/2007:01:41:13 +0000] - ERROR<12293> - Connection  - conn=-1
op=-1 msgId=-1 - fd limit exceeded Too many open file descriptors - not listening
on new connection
```

Other symptoms of an unresponsive process include LDAP connections that do not answer or that hang, no messages in the error or access logs, or an access log that is never updated.

Collecting Data About an Unresponsive Process

The prstat tool tells you the amount of CPU being used for each thread. If you collect a process stack using the pstack utility at the same time you run the prstat tool, you can then use the pstack output to see what the thread was doing when it had trouble. If you run the prstat and

pstack simultaneously several times, then you can see over time if the same thread was causing the problem and if it was encountering the problem during the same function call. If you are experiencing a performance drop, then run the commands simultaneously every 2 seconds. If you are experiencing a passive or active hang, run the commands with a slightly longer delay, for example every 10 seconds or so.

Analyzing Data About a Unresponsive Process: an Example

For example, you try running an ldapsearch on your Directory Server as follows:

```
# ldapsearch -p 5389 -D "cn=Directory Manager" -w secret
-b"o=test" description=*
```

This command generates a 40 second search with no results. To analyze why the process in unresponsive, first get the process ID using the following command:

```
# ps -aef | grep slapd | grep slapd-server1
   mares 15013 24159  0 13:06:20 pts/32   0:00 grep slapd-server1
   mares 14993     1  1 13:05:36 ?        0:04 ./ns-slapd -D
/u1/SUNWdsee/user1/52/slapd-server1 -i /u1/SUNWdsee/user1/52/slapd-s
```

Next, rerun the search and during the search run the prstat and pstack commands simultaneously for the Directory Server process, which in the output above has a process ID of 14993.

```
prstat -L -p 14993 0 1 > prstat.output ; pstack 14993 > pstack.output
```

We rerun the commands three times, with an interval of two seconds between each consecutive run.

The output of the first prstat command appears as follows:

```
   PID USERNAME  SIZE   RSS STATE  PRI NICE     TIME  CPU PROCESS/LWPID
 14993 mares     128M  110M cpu0    59    0  0:00.02 3.0% ns-slapd/51
 14993 mares     128M  110M sleep   59    0  0:00.49 1.3% ns-slapd/32
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/16
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/15
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/14
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/13
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/12
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/11
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/10
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/9
 14993 mares     128M  110M sleep   59    0  0:00.00 0.0% ns-slapd/8
```

```
14993 mares      128M  110M sleep   59    0    0:00.00 0.0% ns-slapd/6
14993 mares      128M  110M sleep   59    0    0:00.00 0.0% ns-slapd/5
14993 mares      128M  110M sleep   59    0    0:00.00 0.0% ns-slapd/4
14993 mares      128M  110M sleep   59    0    0:00.00 0.0% ns-slapd/3
Total: 1 processes, 51 lwps, load averages: 0.36, 0.29, 0.17
```

The problem appears to be occurring in thread 51. Next, we look for thread 51 in the output of
the first pstack command and it appears as follows:

```
---------------- lwp# 51 / thread# 51  -------------------
 ffffffff7eb55a78 ???????? (1, 102183a10, ffffffff70c1d340, 1001c5390, 0,
ffffffff7ecea248)
 ffffffff77925fe0 id2entry (1002b7610, 1a09, 0, ffffffff70c1e7f4, 0, ffffffff77a6faa8)
+ 3e8
 ffffffff7795ed20 ldbm_back_next_search_entry_ext (101cfcb90, 10190fd60, 0, 101b877b0,
1a08, 45b4aa34) + 300
 ffffffff7ebaf6f8 ???????? (101cfcb90, 1002b7610, 1, ffffffff70c1eaf4, 0, 0)
 ffffffff7ebafbc4 ???????? (101cfcb90, 1, ffffffff70c1eaf4, 0, 10190fd60,
ffffffff70c1e980)
 ffffffff7ebaf170 op_shared_search (101cfcb90, 0, 1015ad240, 0, ffffffffffffffff,
ffffffff7ecea248) + 8c0
 ffffffff7e92efcc search_core_pb (101cfcb90, 2, 1000, 4000, ffffffff7ea4c810,
ffffffff7ea56088) + 6c4
 ffffffff7e93a710 dispatch_operation_core_pb (101cfcb90, 101cfcb90, c00,
ffffffff7ea4c810, 0, d10) + cc
 ffffffff7e926420 ???????? (101f3fe80, 102fd3250, 2, 63, 2, 200000)
 ffffffff7e92672c ldap_frontend_main_using_core_api (101f3fe80, 102fd3250, 2,
101da1218, 10133db10, 0) + fc
 ffffffff7e927764 ???????? (220, 101c97310, ffffffffffffffff, 800, 958, 101f3fe80)
 ffffffff7d036a7c _pt_root (101c97310, ffffffff70b00000, 0, 0, 20000, ffffffff70c1ff48)
+ d4
 ffffffff7c1173bc _lwp_start (0, 0, 0, 0, 0, 0)
```

Note – The ends of the lines in this example have been wrapped so that they fit on the page.

The output of the second and third pstack command show the same results, with thread 51
doing the same types of operation.

All three pstack outputs taken at two second intervals show thread 51 doing the same search
operations. The first parameter of the op_shared_search function contains the address of the
operations taking place, which is 101cfcb90. The same operation occurs in each of the three
stacks, meaning that the same search is taking place during the four seconds that elapsed
between the first and the last pstack run. Moreover, the prstat output always shows thread 51
as the thread taking the highest amount of CPU.

If you check the access log for the result of the search operations at the time the hang was observed, we find that it is a result of the search on the unindexed description entry. By creating a description index, this hang will be avoided.

Troubleshooting Drops in Performance

This section describes how to begin troubleshooting a drop in performance. It describes possible causes of performance drops, describes the information you need to consult if you experience a performance drop, and how to analyze this information.

Possible Causes of a Drop in Performance

Make certain that you have not mistaken an active or passive hang for a performance drop. If you are experiencing a performance drop, it could be for one of the following reasons:

- Other processes are affecting CPU or disk access
- Network problems
- High input/ouput rate
- Memory swapping
- Unindexed searches, such as when an index is missing or when a "!" filter is used
- Complex searches, such as searches on static groups, class of service, and roles
- Complex updates, such as to static groups, class of service, and roles
- Sub-optimum hardware
- Sub-optimum system settings, such as `fds` or `keepalive`
- Directory Server tuned incorrectly

Collecting Data About a Drop in Performance

Collect information about disk, CPU, memory, and process stack use during the period in which performance is dropping.

Collecting Disk, CPU, and Memory Statistics

If your CPU is very low (at or around 10%), try to determine if the problem is network related using the `netstat` command as follows:

```
# netstat -an | grep port
```

A performance drop may be the result of the network if a client is not receiving information despite the fact that access logs show that results work sent immediately. Running the `ping` and `traceroute` commands can help you determine if network latency is responsible for the problem.

Collect swap information to see if you are running out of memory. Memory may be your problem if the output of the swap command is small.

Solaris	`swap -l`
HP-UX	`swapinfo`
Linux	`free`
Windows	Already provided in `C:\report.txt`

On Solaris, use the output of the `prstat` command to identify if other processes could be impacting the system performance. On Linux and HP-UX, use the `top` command.

Collecting Consecutive Process Stacks on Solaris

Collect consecutive `pstack` and `prstat` output of the Directory Server during the period when the performance drops as described in "Analyzing Data About a Unresponsive Process: an Example" on page 71. For example, you could use the following script on Solaris to gather `pstack` and `prstat` information:

```
#!/bin/sh

i=0
while [ "$i" -lt "10" ]
do
        echo "$i/n"
        date= 'date"+%y%m%d:%H%M%S"
        prstate -L -p $1 0 1 > /tmp/prstate.$date
        pstack $1 > /tmp/pstack.$date
        i='expr $i + 1'
        sleep 1
done
```

Using the `idsktune` Command

The `idsktune` command provides information about system parameters, patch level, and tuning recommendations. You can use the output of this command to detect problems in thread libraries or patches that are missing. For more information about the `idsktune` command, see idsktune(1M).

Analyzing Data Collected About a Performance Problem

In general, look through your data for patterns and commonalities in the errors encountered. For example, if all operation problems are associated with searches to static groups, modifies to static groups, and searches on roles, this indicates that Directory Server is not properly tuned to

handle these expensive operations. For example, the nsslapd-search-tune attribute is not configured correctly for static group related searches, or maybe the uniqueMember attribute indexed in a substring affects the group related updates. If you notice that problems are associated with unrelated operations but all at a particular time, this might indicate a memory access problem or a disk access problem.

You can take information culled from you pstacks to SunSolve and search for them along with the phrase unresponsive events to see if anything similar to your problem has already been encountered and solved. SunSolve is located at
http://sunsolve.sun.com/pub-cgi/show.pl?target=tous

The remainder of this section provides additional tips to help you analyze the data you collected in the previous steps.

Analyzing the Access Log Using the logconv Command

You can use the logconv command to analyze the Directory Server access logs. This command extracts usage statistics and counts the occurrences of significant events. For more information about this tool, see logconv(1).

For example, run the logconv command as follows:

```
# logconv -s 50 -efcibaltnxgju access > analysis.access
```

Check the output file for the following:

- Unindexed searches (notes=U)

  If unindexed searches are present, search for the associated indexes using the dsconf list-indexes command. If the index exists, then you may be reaching the limit of your all-ids-threshold property. This property defines the maximum number of values per index key in an index list. Increase the all-ids-threshold and reindex.

  If the index does not exist, then you need to create the index and then reindex. For information about creating an index, see "To Create Indexes" in *Sun Java System Directory Server Enterprise Edition 6.2 Administration Guide*.

- High file descriptor consumption

  To manage a problem with file descriptor consumption you may need to request to increase the file descriptors available at the system level. You may want to reduce the number of persistent searches (notes=persistent), modify the client applications that do not disconnect, or reduce the idle time-out value set by the nsslapd-idletimeout property.

- Searches with long etimes or that return many entries

  For example. if the etime is 344, grep the access log for etime 344. The access log tells you the connection and operation. You can use this information to see what the operation was doing when the performance drop occurred, when the connection was opened, and who was

the binding user. If all of the same operations have long etimes, that points to a problem with a particular operation. If the same binding user is always associated with a long etime, this suggests an ACI issue.

If you suspect an ACI problem with the binding user, prove it by running the same operation with the Directory Manager user, who is not subject to ACIs.

- Searches on the uniquemember attribute or on the wrong filters.

  Look on SunSolve for static group performance hot patches. Run your search by specifying the nsslapd-search-tune attribute.

- Long ADDand MOD operations

Identifying Capacity Limitations: an Exercise

Often a capacity limitation manifests itself as a performance issue. To differentiate between performance and capacity, performance might be defined as "How fast the system is going" while capacity is "the maximum performance of the system or an individual component."

If your CPU is very low (at or around 10%), try to determine if the disk controllers are fully loaded and if input/output is the cause. To determine if your problem is disk related, use the iostat tool as follows:

```
# iostat -xnMCz -T d 10
```

For example, a directory is available on the internet. Their customers submit searches from multiple sites and the Service Level Agreement (SLA) was no more than 5% of requests with response times of over 3 seconds. Currently 15% of request take more than 3 seconds, which puts the business in a penalty situation. The system is a 6800 with 12x900MHz CPUs.

The vmstat output looks as follows:

```
procs     memory            page            disk          faults      cpu
 r b w   swap   free  re  mf pi po fr de sr m0 m1 m1 m1   in   sy   cs us sy id
 0 2 0 8948920 5015176 374 642 10 12 13 0 2 1  2  1  2  132 2694 1315 14  3 83
 0 19 0 4089432 188224 466 474 50 276 278 0 55 5 5  4  3 7033 6191 2198 19  4 77
 0 19 0 4089232 188304 430 529 91 211 211 0 34 8 6  5  4 6956 9611 2377 16  5 79
 0 18 0 4085680 188168 556 758 96 218 217 0 40 12 4 6  4 6979 7659 2354 18  6 77
 0 18 0 4077656 188128 520 501 75 217 216 0 46 9 3  5  2 7044 8044 2188 17  5 78
```

We look at the right 3 columns, us=user, sy=system and id=idle, which show that over 50% of the CPU is idle and available for the performance problem. One way to detect a memory problem is to look at the sr, or scan rate, column of the vmstat output. If the page scanner ever starts running, or the scan rate gets over 0, then we need to look more closely at the memory system. The odd part of this display is that the blocked queue on the left of the display has 18 or 19 processes in it but there are no processes in the run queue. This suggests that the process is blocking somewhere in Solaris without using all of the available CPU.

Next, we look at the I/O subsystem. With Solaris 8, the `iostat` command has a switch, `-C`, which will aggregate I/Os at the controller level. We run the `iostat` command as follows:

```
#  iostat -xnMCz -T d
                    extended device statistics
    r/s    w/s   Mr/s   Mw/s wait actv wsvc_t asvc_t  %w  %b device
  396.4   10.7    6.6    0.1  0.0 20.3    0.0   49.9   0 199 c1
  400.2    8.8    6.7    0.0  0.0 20.2    0.0   49.4   0 199 c3
  199.3    6.0    3.3    0.0  0.0 10.1    0.0   49.4   0  99 c1t0d0
  197.1    4.7    3.3    0.0  0.0 10.2    0.0   50.4   0 100 c1t1d0
  198.2    3.7    3.4    0.0  0.0  9.4    0.0   46.3   0  99 c3t0d0
  202.0    5.1    3.3    0.0  0.0 10.8    0.0   52.4   0 100 c3t1d0
```

On controller 1 we are doing 396 reads per second and on controller 3 we are doing 400 reads per second. On the right side of the data, we see that the output shows the controller is almost 200% busy. So the individual disks are doing almost 200 reads per second and the output shows the disks as 100% busy. That leads us to a rule of thumb that individual disks perform at approximately 150 I/Os per second. This does not apply to LUNs or LDEVs from the big disk arrays. So our examination of the numbers leads us to suggest adding 2 disks to each controller and relaying out the data.

In this exercise we looked at all the numbers and attempted to locate the precise nature of the problem. Do not assume adding CPUs and memory will fix all performance problems. In this case, the search programs were exceeding the capacity of the disk drives which manifested itself as a performance problem of transactions with extreme response times. All those CPUs were waiting on the disk drives.

Troubleshooting Process Hangs

This section describes how to troubleshoot a totally unresponsive Directory Server process. A totally unresponsive process is called a hang, and there are two types of hang you might experience:

- Active hang, when the CPU level is at 100%. For example, the process encounters an infinite loop meaning it waits forever waiting for and servicing a request.

- Passive hang, when the CPU level is at 0%. For example, the process encounters a deadlock where two or more threads of a process are waiting for the other to finish, and thus neither ever does.

The remainder of this section describes how to troubleshoot each of these types of process hang.

Troubleshooting an Active Hang

A hang is active if the `top` or `vmstat 1` output show CPU levels of over 95%.

This section describes the causes of an active hang, how to collect information about an active hang, and out to analyze this data.

Possible Causes of an Active Hang

Possible causes of an active hang include the following:

- An infinite loop
- Retry of an unsuccessful operation, such as a replication operation or a bad commit

Collecting and Analyzing Data About an Active Hang

On a Solaris system, collect several traces of the Directory Server process stack that is hanging using the Solaris pstack utility. Run the command from the *root-dir*/bin/slapd/server directory. You should also collect statistics about the active process using the Solaris prstat utility. You must collect this information while the server is hanging.

The consecutive pstack and prstat data should be collected every second.

Troubleshooting a Passive Hang

A hang is passive if the top or vmstat 1 output show low CPU levels.

Possible Causes of a Passive Hang

Possible causes of a passive hang include the following:

- A deadlock resulting from locks or conditional variables
- A defunct thread

Collecting and Analyzing Data About a Passive Hang

On a Solaris system, collect several traces of the Directory Server process stack that is hanging using the Solaris pstack utility. Run the command from the *root-dir*/bin/slapd/server directory. You must collect this information while the server is hanging. The consecutive pstack data should be collected every three seconds.

Collect several core files that show the state of the server threads while the server is hanging. Do this by generating a core file using the gcore command, changing the name of the core file, waiting 30 seconds, and generating another core file. Repeat the process as least once to get a minimum of three sets of core files and related data.

For more information about generating a core file, see "Generating a Core File" on page 66.

Troubleshooting Database Problems

This section describes how to troubleshoot an inaccessible database

Possible Causes of Database Problems

The Directory Server database may be inaccessible for one of the following reasons:

- Database corruption
- index corruption
- Shared region file corruption
- Missing change log
- Corrupted change log
- Database offline, for example it is being reimported
- Missing transaction log

▼ To Troubleshoot a Database Problem

1 **If the server refuses to start, remove the guardian file and all shared memory files while the server is offline and then retry a new start.**

   # *install-path*/*instance-name*/db/guardian
   # *install-path*/*instance-name*/db/_db.00*

   If the start succeeds and the database still cannot be loaded, continue with this procedure.

2 **Backup up all database file stored in the** db/ **directory.**

3 **Collect error and access log files from the time during which the database was inaccessible.**

   # *install-path*/*instance-name*/logs/errors*
   # *install-path*/*instance-name*/access*

Troubleshooting Memory Leaks

This section describes how to troubleshoot a memory leak.

Possible Causes of a Memory Leak

Memory leaks are caused by problems allocating memory, either in Directory Server itself or in custom plug-ins. Troubleshooting these problems can be very difficult, particularly in the case of custom plug-ins.

Collecting Data About a Memory Leak

It is important to do the following before collecting data about your memory leak:

- Disable any custom plug-ins
- Reduce the cache setting to very low values
- Enable the audit log

One you have done the above, run a test that proves your memory leak. During the life of the test run, gather output from the pmonitor utility as follows:

The pmonitor utility is a process monitor.

Collect the generic Directory Server data, as described in "Collecting Generic Data" on page 22. This data includes the version of Directory Server that you are running, logs from the test run, in particular the audit log, and the Directory Server configuration file.

With the data you collected, you can now contact the Sun Support Center for assistance with your problem.

Analyzing Memory Leaks Using the libumem Library

On Solaris systems, the libumem library is a memory agent library that tracks all of the address allocated into the process memory footprint. Usually it is not used in a production environment because it is much slower. However, it is helpful for analyzing the cause of a memory leak. For more information about the libumem library, see the technical article at the following location:
http://access1.sun.com/techarticles/libumem.html

Restart the Directory Server using the following command:

```
# SUN_SUPPORT_SLAPD_NOSH=true LD_PRELOAD=libumem.so \
UMEM_DEBUG=contents,audit=40,guards UMEM_LOGGING=transaction ./start-slapd
```

The libumem library is now loaded before the Directory Server starts, instead of using SmartHeap.

Next, run the gcore command several times, once before the memory use started to grow and once after. The gcore command provides a list of addresses and pointers. Use these to read the libumem library.

```
# cd install-root/bin/slapd/server
gcore -o /tmp/directory-core process-id
```

Finally, use the mdb and splitrec tools to analyze the results. The splitrec tool compares the results to see the complete stack of the leak.

```
# cd install-root/bin/slapd/server
echo "::umausers -e" | mdb ./ns-slapd path_gcore1 > res.1
eacho "::umausers -e" | mdb ./ns-slapd path_gcore2 > res.2
splitrec -1 res.1 res.2
```

The splitrec tool is available through Sun Support. This tool provides a summary of the stacks that have been identified as responsible for leaking allocation stacks. Sun Support can use the contents of these stacks to identify known memory leaks in the SunSolve database. Sometimes the splitrec tool does not provide any output because by default it is configured to report leaks only for stacks that have been identified as leaking more than 100 times. Configure this limit to a lower value using the splitrec -l option.

6

Troubleshooting Data Management Problems

This chapter provides information to help you troubleshoot Directory Server and Directory Proxy Serverdata management problems.

This chapter contains the following sections:

Troubleshooting LDAP Operation Failures

This section describes how to troubleshoot LDAP operation failures. It describes the possible causes of the operation failures, the information to collect to help you troubleshoot the problem, and how to analyze this information.

Possible Causes of an Operation Failure

An operation may fail for the following reasons:

- ACIs are in place that do not allow the operation
- Referrals are being followed to a different server
- Updates can not proceed because a database has been set to referrals on updates
- Database being reimported
- Unallowed online configuration

Collecting and Analyzing Data About Operation Failures

To determine if ACIs are the source of your problem, gather information about all of the ACIs from the suffix level to the entry you are trying to access. Gather this data using the ldapsearch operation as follows:

```
# ldapsearch -D cn=Directory Manager -b base-suffix dn aci
```

Collect the access and errors log files that contain the operation. Be sure to enable the ACI logging level. Enable the ACI logging level for the errors log file as follows:

```
# dsconf set-log-prop errors level:err-acl
```

Enable the ACI logging level for the access log file as follows:

```
# dsconf set-log-prop access level:acc-internal
```

To view the contents of the error log, use the dsadm command as follows:

```
dsadm show-error-log -A duration [-L last-lines] install-path
```

The -A option specifies the maximum age of lines to be returned from the log. For example, to search for all entries younger than 24 hours, use -A 24h. The -L option specifies the number of lines to be returned from the log. For example, to return the last 50 lines, use -L 50. By default, 20 lines are returned.

To view the access log, use the dsadm command as follows:

```
dsadm show-access-log -A duration [-L last-lines] install-path
```

The log files themselves are located in the following directories:

instance-path/logs/errors*
instance-path/logs/access*

If you are unable to troubleshoot your problem yourself, collect the error and access log files from the time during which the database was inaccessible and send them to Sun Support for analysis. By default, the log files are located in the *instance-path*/logs directory. To find the path to your error and access logs, use the following command:

```
# dsconf get-log-prop ERROR path
```

or

```
# dsconf get-log-prop ACCESS path
```

Troubleshooting SSL Problems

This section helps you troubleshoot when an SSL connection fails. It includes the following sections:

This chapter contains the following sections:

For information about troubleshooting SSL problems with Identity Synchronization for Windows, see

Overview of Important SSL Concepts

This section describes concepts to help you troubleshoot problems using SSL for Directory Server multi-master replication. Problems with SSL always appear on the supplier side. The error log will contain security related messages such as "SSL init failed." or "Certificate not accepted."

SSL connections always involve two participants:

- The SSL client, which is the LDAP client sending the LDAP requests or the Directory Server sending the replication updates (the supplier).
- The SSL server, which is the Directory Server accepting the LDAP requests (the consumer).

The SSL client initiates requests and the SSL server always receives the requests. During this exchange, the SSL server must provide credentials. Any SSL server needs to verify the credentials sent by the SSL client. In order to make this verification, the certificate database on the peer must contain the CA certificate of the certificate sent by the other peer.

In replication, SSL must be enabled in all replicas, even master replicas that only accept non-SSL operations. For example, a master server communicates with a hub server using SSL. The hub must listen on the SSL port. The master does not need listen on the SSL port because it is an SSL client. However, it must still define an SSL port, otherwise Directory Server can not initiate SSL certificate exchange for communication with the host server.

By default, SSL is enabled on all Directory Server 6.x instances. For a detailed explanation of how SSL works, see "Secure Sockets Layer (SSL)" in *Sun Java System Directory Server Enterprise Edition 6.2 Reference*.

Possible Causes of SSL Problems

Failure of an SSL connection could be the result of one of the following:

- Wrong security libraries patch family applied
- Server not configured to accept SSL
- SSL port not open
- CA certificate not found
- CA certificate not appropriate or expired
- SSL client not sending certificate when required
- SSL server certificate not imported

Collecting and Analyzing SSL Data

This section provides information about collecting and analyzing data to help you troubleshoot SSL problem, including problems replicating over SSL.

About the `certutil` and `ssltap` Tools

The Mozilla website provides NSS Security Tools that are helpful for debugging and troubleshooting SSL problems. You can obtain the source-code of these tools from `http://www.mozilla.org/projects/security/pki/nss/tools`. This toolbox contains two tools, `certutil` and `ssltap`.

The `certutil` tool can be used to display all certificates stored in a certificate database and to display a single certificate in detail. Because it is possible to change or delete data in the certificates database when using this program, we recommend running the `certutil` tool on a copy of the original certificates database.

Note – To use the `certutil` tool, you need to provide a password. However, the `dsadm create` command generates a default certificate database password that can not be retrieved. To use the `certutil` tool, change the certificate database password using the `dsadm set-flags` *instance-path* `cert-pwd-prompt=on` command.

The `ssltap` tool can capture the SSL communications between two systems. You must place the `ssltap` program between the connection from a Directory Server and an LDAP client. The program behaves like a Directory Server when it communicates with the LDAP client and behaves like the LDAP client when communicating with the Directory Server.

Verifying the Certificates Using `dsadm`

The certificates database resides *instance-path*/`alias` directory. Get the contents of this directory for each server involved in the problem.

For example, to see a list of the certificates that can be used as ns-slapd certificates (certificates with a u,, trust flags) use the dsadm command as follows:

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

The command lists the certificates, such as defaultCert, the date from which it is valid, the date it expires, whether it is self-signed, who issued it, and to whom it is issued.

To see information about valid and trusted CA certificates (certificates with CT,, trust flags) use the dsadm command as follows:

```
dsadm list-certs --ca instance-path
```

This command provides the certificate alias, its dates of validity and expiration, whether it is built in, who issued it, and to whom it was issued. Verify that the SSL server and client certificates are generated by a certificate authorities that appear in the output of this command.

For detailed information about a particular certificate, use the dsadm command as follows:

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

For example, the output of this command appears as follows:

```
server1 [/var/dsee/instances]> dsadm show-cert ds1 defaultCert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            00:85:8b:13:ef
        Signature Algorithm: PKCS #1 MD5 With RSA Encryption
        Issuer:
            "CN=server1,CN=Directory Server,O=example.com"
        Validity:
            Not Before: Fri Mar 23 14:10:51 2007
            Not After : Sat Jun 23 14:10:51 2007
        Subject:
            "CN=server1,CN=Directory Server,O=example.com"
        Subject Public Key Info:
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    9a:c9:52:bd:ec:32:43:1a:39:96:90:02:f5:7e:18:45:
                    78:37:ca:8d:8f:c4:cc:6f:d1:7e:6c:38:d1:a1:53:41:
                    96:67:07:c7:c8:56:78:d1:f2:24:df:1f:eb:b2:07:5d:
                    6e:1f:58:fa:7a:f2:00:e4:95:d1:57:97:37:9d:22:31:
                    1c:b7:99:29:df:a3:8a:2a:87:e1:8b:54:ea:1f:7c:b7:
                    28:23:ce:be:7e:73:b3:87:f5:32:88:56:4e:58:68:f6:
                    f6:01:2c:51:ca:07:00:40:ca:b3:9e:33:40:e8:f2:18:
```

```
                    bc:16:d4:ac:ae:69:a7:c9:d7:g5:34:d4:87:11:2c:b1
            Exponent: 65537 (0x10001)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
        29:76:4f:9f:ca:00:09:7b:05:ac:0f:26:6f:d1:93:aa:
        a8:c0:eb:a9:2a:39:e2:6e:08:0a:90:41:e5:7f:18:4a:
        17:05:03:04:9b:ee:0a:dc:3c:ef:ee:aa:fc:ea:85:bf:
        f9:05:32:65:35:2c:e8:1f:32:9d:d6:a7:aa:68:a4:7a:
        e8:d9:4a:a0:a6:bc:fd:36:ba:d3:80:8a:1b:d3:81:8a:
        68:1a:73:cc:36:7a:92:dc:eb:ec:af:02:6b:14:c7:77:
        e3:7d:95:19:e7:17:9d:d2:35:67:60:6b:9f:9b:d9:af:
        01:f2:55:7f:5f:ce:23:a0:49:67:01:cd:30:38:8b:d2
    Fingerprint (MD5):
        B8:34:27:AA:02:F6:07:FC:8F:D1:4A:AD:38:29:09
    Fingerprint (SHA1):
        3C:3B:BD:15:E8:1F:68:2E::E8:EJ:02:63:CD:8F:39:BE:DD:70


    Certificate Trust Flags:
        SSL Flags:
            Valid CA
            Trusted CA
            User
            Trusted Client CA
        Email Flags:
            User
        Object Signing Flags:
            User
```

Confirm the validity of the certificate. Also, confirm that the issuer of the certificate is a valid and trusted certificate authority.

Verifying the Certificates Using `certutil` on Directory Server 5.x

If you are using migrated 5.x instances of Directory Server, you can verify the contents of the certificates database using the output of the Certificate Database Tool, or `certutil`. The `certutil` tool displays the contents of the certificate and key database files. For more information about this tool, go to
http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html.

Note – The `certutil` tool can be used by advanced users to populate the certificate database.

For example, run the `certutil` tool as follows:

```
# ./certutil -L -d /opt/SUNWdsee/alias -P slapd-

Test (SUBCA1) Internal CA    CT,C,C
```

```
Test (CMSENG) Internal CA    CT,C,C
ESD SubCA1 Certificate       u,,
```

The tool lists the certificates, such as Test (SUBCA2) Internal CA. and the trust flags associated with each certificates, such as CT,C,C. Very that the SSL server certificates are generated by a certificate authority that has a C,, flag. Verify that SSL client certificates are generated by a certificate authority with a T,, flag.

For example, you might have a certificate that works only as an SSL client, but you were trying to use it as a SSL server, which would not work. In replication, all Directory Server replicas need to have certificates signed by CT,, because they act as suppliers and consumers. Change the certificate trust flags to CT,, as follows:

```
# ./certutil -M -n cert-name -t CT,, -d /opt/SUNWdsee/alias -P slapd-
```

You can also run the certutil tool using the following options, to see the certificate authority that issued the certificate.

```
# ./certutil -L -n server-cert -d /opt/SUNWdsee/alias -P slapd-
```

Use this information to confirm that the certificate is present in the certificate database. You can also check the expiration date of the certificate to make sure that it has not expired.

Checking Client Authentication Settings

You can configure client authentication to be required or allowed. Verify the setting client authentication settings by using the DSCC or by using the dsconf get-server-prop ssl-client-auth-mode command.

Note – User's of migrated 5.x instances of Directory Server can verify the client authentication settings by checking the nsSSLClientAuth property in the dse.ldif file.

▼ To Verify Client Authentication Settings Using the DSCC

1 Go to the Directory Servers tab in the DSCC, and select the server from the table.

2 Click the Security tab and then the General tab.

3 In the Client Authentication section, go to LDAP Settings.

If you want only the SSL server to require the certificate, select Allow Certificate Based Client Authentication.

If you want both the SSL server and the SSL client to require a certificate, select Require Certificate Based Client Authentication.

Checking the Libraries

Get a list of all the dynamically loaded libraries to see which NSS/SSL and NSPR libraries are being loaded. To get the list of dynamically loaded libraries on Solaris Intel, Linux, or Windows, used the following command:

```
# cd install-path /ds6/lib; ldd ns-slapd
```

To get the list of dynamically loaded libraries on Solaris SPARC, Solaris AMD64 or HPUX, use the following command:

```
# cd install-path/ds6/lib/64;  ldd ns-slapd
```

The dynamically loaded libraries will be located in the following directory:

```
install-path/dsee6/private/lib
```

If you installed Directory Server using JES, verify that you have the correct libraries in the output of the pkginfo command.

Verify SSL Communications Using the ssltap Tool

You can use the ssltap tool to check if the hand shake is working on your system. The tool works like an SSL proxy, showing the communications between the LDAP client and the Directory Server and the packages being exchanged. For example, using this tool you might see where the server asks for a certificate but the client does not send the certificate or where the client proposes a cipher suite that the server does not support.

Since the SSL port 636 is hard-coded on the client side, the ssltap tool run on the Directory Server, where it must list on port 636 for incoming client requests. The SSL port of the Directory Server needs to be changed to a number other than 636 while running the ssltap tool.

For example, run ssltap as follows:

```
ssltap -vhfsxl -p 636 localhost:637 > output.html
```

After running some simple LDAP request on the client, such as ldaplist, the tool should have captures some SSL packets. Stop the tool by pressing CTRL-C and view the output file in a browser window. The output data is color coded so that data sent by the client is marked in blue and data sent by the server is marked in red.

7

Troubleshooting Identity Synchronization for Windows

This chapter provides information to help you troubleshoot problems you may encounter while using Identity Synchronization for Windows. It includes the following topics:

This chapter contains the following sections:

General Troubleshooting Guidelines

This section provide general guidelines to help you troubleshoot problems with Identity Synchronization for Windows. It includes the following sections:

Note – Before you begin troubleshooting your problem, be sure to check the Release Notes for explanations about known issues as well as information about patch requirements.

Configuring and Using the Logs

Some events are not included in a log file until you adjust the log level to FINE or higher. To adjust the log level, see "Configuring Your Log Files" in *Sun Java System Directory Server Enterprise Edition 6.2 Installation Guide*. The log level should be left as INFO during all idsync resync operations.

When troubleshooting a problem, look at the central error log located in the following directory:

`isw-`*hostname*`/logs/central/error.log`

Almost all errors will be reported in the central error log file. Additional information about the error may be available in the `audit.log` file. To simplify the correlation between related log entries, the `audit.log` file also contains the information found in the error log.

For the Windows NT SAM Change Detector subcomponent to be effective, you must turn on the NT audit log as follows:

1. From the Start menu, go to Programs, Administrative Tools, then User Manager.

2. Select Policies, then Audit Policies.

3. Select Audit These Events and check the Success and Failure check boxes for User and Group Management.

4. Select Event Log Settings in the Event Viewer, Event Log Wrapping menu. Next, select Overwrite Events as Needed.

Using the `idsync printstat` Command

The `idsync printstat`command displays the connector IDs and the status of each connector. The output also displays a list of the remaining steps you have to perform to complete the installation and configuration process. This status information can be useful for troubleshooting problems with Identity Synchronization for Windows.

For example, the command is run as follows:

```
# idsync printstat

Connector ID: CNN100
Type:    Active Directory
Manages: example.com (ldaps://host2.example.com:636)
State:   READY
Connector ID: CNN101
Type:    Sun Java System Directory
Manages: dc=example,dc=com
(ldap://host1.example.com:389)
State:    READY
Sun Java System
Message Queue Status:  Started
Checking the System Manager status over the Sun Java System
Message Queue.
System Manager Status:  Started SUCCESS
```

If the command lists connectors, then you know that your configuration was saved successfully.

Troubleshooting Quick Checklist

This checklist provides questions to help guide you in your troubleshooting process:

1. Was the Directory Server running during resource configuration?

2. Is the core, including the Message Queue and the System Manager, currently running? On Windows, check for the appropriate service name. On Solaris and Linux, check for the appropriate daemon name. Use the `idsync printstat` command to verify that the Message Queue and System Manager are active.

3. Was synchronization started from the Identity Synchronization for Windows console or from the command line?

4. Are the directory sources that are being synchronized currently running?

5. Use the Identity Synchronization for Windows console to verify that modifications and creates are synchronized in the expected direction.

6. If synchronizing users and groups that existed in only one directory source, were these users and groups created in the other directory source using the `idsync resync` command?

Note – You must run `idsync resync` whenever there are existing users and groups. If you do not resynchronize existing users, resynchronization behavior remains undefined.

---

7. If synchronizing users that existed in both directory sources, were these users linked using the `idsync resync` command?

8. If user creates fail from Active Directory or Windows NT to the Sun Java System Directory Server, verify that all mandatory attributes in the Directory Server object class are specified as creation attributes and values for the corresponding attributes are present in the original user entry.

9. If synchronizing creates from Directory Server to Windows NT and the user creation succeeded, but the account is unusable, verify that the user name does not violate Windows NT requirements.

   For example, if you specify a name that exceeds the maximum allowable length for Windows NT, the user will be created on NT but can not be used or edited until you rename the user (User → Rename).

10. Are the users that fail to synchronize within a Synchronization User List? For example, do they match the base DN and filter of a Synchronization User List? In deployments that include Active Directory, on-demand password synchronization fails silently if the Sun Java System Directory Server entry is not in any Synchronization User List. This most often occurs because the filter on the Synchronization User List is incorrect.

11. Were the synchronization settings changed? If the synchronization settings changed from only synchronizing users from Active Directory to the Sun Java System Directory Server to synchronizing users from the Directory Server to Active Directory, then the Active

Directory SSL CA certificate must be added to the connector's certificate database. The `idsync certinfo` command reports what SSL certificates must been installed based on the current SSL settings.

12. Are all host names properly specified and resolvable in DNS? The Active Directory domain controller should be DNS-resolvable from the machine where the Active Directory Connector is running and the machine where the Sun Java System Directory Server Plug-in is running.

13. Does the IP address of the Active Directory domain controller resolve to the same name that the connector uses to connect to it?

14. Are multiple Synchronization User Lists configured? If so, are these in conflict? More specific Synchronization User Lists should be ordered before less specific ones using the Console.

15. If flow is set to bidirectional or from Sun to Windows and there are Active Directory data sources in your deployment, are the connectors configured to use SSL communication?

16. If you are creating or editing the Sun Java System Directory source, and the Directory Server does not display in the Choose a known server drop-down list, check that the Directory Server is running. The Directory Server must be running to appear in the drop down list of available hosts.

If the server in question is down temporarily, type the host and port into the "Specify a server by providing a hostname and port" field.

Note – Identity Synchronization for Windows uses a short host name by default; however, the default host name may not work with your configuration. We recommend using a fully qualified name whenever you are asked to provide a host name.

Troubleshooting Problems with Identity Synchronization for Windows Installation

Confirm that you installation was performed on a clean machine. If you reinstall and the previous installation was not properly uninstalled, errors may occur. For information about uninstalling Identity Synchronization for Windows, see Chapter 10, "Removing the Software," in *Sun Java System Directory Server Enterprise Edition 6.2 Installation Guide*.

For information about whether the core installed correctly, see the log file in the following directory:

```
isw-hostname/logs/central/
```

If the connector installation failed, but the Identity Synchronization for Windows installation program thinks that the connector is installed, the installation program will not allow you to reinstall the connector.

Run the idsync resetconn command to reset the connector's state to UNINSTALLED. Next, reinstall the connector.

If you receive the following error while uninstalling the software, you need to increase the size of the swap file mounted at /tmp:

```
./runInstaller.sh
IOException while making /tmp/SolarisNativeToolkit_5.5.1_1
executable:java.io.IOException: Not enough space java.io.IOException: Not enough space
```

After installation, confirm that all of the subcomponents were installed. Directory Server and the Windows NT connectors require subcomponents to be installed after the connector installation. The Directory Server plug-in must be installed in each Directory Server replica.

The Directory Server must be restarted after the Directory Server plug-in is installed. The Windows NT Primary Domain Controller must be restarted after the Windows NT subcomponents are installed.

Troubleshooting Memory Problems

If memory problems are suspected on Solaris or Linux environments check the processes. To view which components are running as different processes, enter

```
/usr/ucb/ps -gauxwww | grep com.sun.directory.wps
```

The output gives the full details including the ID of connectors, system manager and central logger. This can be useful to see if any of the processes are consuming excessive memory.

Troubleshooting Problems With Connectors

Use the information in this section to troubleshoot problems with your connectors. This section contains the following topics:

This chapter contains the following sections:

General Connector Troubleshooting Tips

Confirm that all of the connectors are installed. One connector must be installed for each directory source being synchronized.

Confirm that the source connector detects the change to the user. Use the central audit log to determine if the connector for the directory source where the user was added or modified detects the modification.

Verify that all connectors are in the SYNCING state using the Identity Synchronization for Windows console or `idsync printstat` command.

Determine if the destination connector processes the modification.

Determining the ID of a Connector Managing a Directory Source

You can determine the connector ID by using the central logs or by using the `idsync printstat` command.

You can find the connector ID of the directory sources being synchronized by looking in the central audit log. At start up, the central logger logs the ID of each connector and the directory source that it manages. Look for the last instance of the startup banner for the most recent information.

For example, the following log entry contains two connector IDs:

- **CNN101** is a Directory Server connector that manages `dc=example,dc=com`
- **CNN100** is an Active Directory connector that manages the `example.com` domain

```
[2006/03/19 00:00:00.722 -0600] INFO    16
"System Component Information:
SysMgr_100 is the system manager (CORE);
console is the Product Console User Interface;
CNN101 is the connector that manages
[dc=example,dc=com (ldap://host1.example.com:389)];
CNN100 is the connector that manages
[example.com (ldaps://host2.example.com:636)];"
```

For information about using the `idsync printstat` command to determine the connector ID, see "Using the `idsync printstat` Command" on page 92

Getting and Managing the Current State of a Connector

You can determine the current state of the connectors involved in synchronization using the Status pane in the Identity Synchronization for Windows console, using the `idsync printstat` command , or by looking in the central audit log.

To use the audit log, search for the last message that reports the connector state. For example, the following audit log entry shows the connector CNN101 is in the READY state:

```
[2006/03/19 10:20:16.889 -0600]
 INFO    13 SysMgr_100 host1
  "Connector [CNN101] is now in state "READY"."
```

TABLE 7–1   Definition of the Connector States

State	Definition
UNINSTALLED	The connector has not been installed.
INSTALLED	The connector is installed, but is not configured.
READY	The connector is installed and configured, but is not synchronizing.
SYNCING	The connector is installed, configured, and in the process of synchronizing.

Troubleshooting a Connector in the UNINSTALLED State

If the connector is in an UNINSTALLED state, you need to install the connector.

Troubleshooting a Connector in the INSTALLED State

If a connector remains in the installed state for a long period of time, then might not be running or might be unable to communicate with the Message Queue.

On the machine where the connector is installed, look in the audit and error logs for potential errors. For example, if the connector can not connect to the Message Queue, then that error log will report the problem. If the connector can not connect to the Message Queue, see "Troubleshooting the Message Queue Component" on page 104 for possible causes.

If the most recent messages in the audit log are old, then the connector may not be running. See "Troubleshooting the Watchdog Process and Core Components" on page 99 for information about starting the connector.

Troubleshooting a Connector in the READY State

A connector remains in the READY state until synchronization begins all of the subcomponents connect to the connector. If synchronization has not started, then start it using the Identity Synchronization for Windows console or command-line utility.

If synchronization has started and the connector does not go to the SYNCING state, then you may have a problem with one of the subcomponent. See "Troubleshooting the Connector Subcomponents" on page 102 for more information.

Troubleshooting a Connector in the SYNCING State

If all connectors are in the SYNCING state but modifications are not being synchronized, then verify that the synchronization settings are correct.

Using the Identity Synchronization for Windows console, verify that modifications and creates are synchronized in the expected direction, for example, from Windows to the Directory Server. Also verify that the attribute being modified is a synchronized attribute. If created user entries are not being synchronized, then verify that user creation flow is enabled in the Identity Synchronization for Windows console.

Note – Passwords are always synchronized.

If you are still experiencing the problem, check if the source connector detects the change to the user. Use the central audit log to determine if the connector for the directory source where the user was added or modified detects the modification. Also verify that the destination connector processes the modification.

Troubleshooting Problems With the Active Directory Connector

If the Active Directory connector fails to contact Active Directory over SSL and the following error message displays, restart the Active Directory domain controller.

```
Failed to open connection to
ldaps://server.example.com:636,
error(91): Cannot connect to the LDAP server,
reason: SSL_ForceHandshake failed: (-5938)
Encountered end of file.
```

If detecting and applying change in Active Directory fails, it may be the result of insufficient permissions. If a non-administrator account is used for the Active Directory connector, then the default permissions for this user are not sufficient. Some operations, such as a resynchronization process from Active Directory to Directory Server, succeed while other operations, such as detecting and applying changes in Active Directory, fail abruptly. For example, if you synchronize the deletions from Active Directory to Directory Server, then even full permissions are insufficient. To resolve this problem, you must use a Domain Administrator account for the Active Directory connector.

Troubleshooting the Watchdog Process and Core Components

Use the information in this section to troubleshoot the Identity Synchronization for Windows Watchdog process and core components. The Watchdog process launches and monitors the central logger, system manager, and connectors. The core components include the configuration directory, command-line utilities, system manager, and the central logger. The information is provided for each operating system as follows:

This chapter contains the following sections:

Troubleshooting Processes on Solaris or Linux

The following command lists all of the Identity Synchronization for Windows processes that are currently running:

```
# /usr/ucb/ps -auxww | grep com.sun.directory.wps
```

The following table describes the processes that should be running.

TABLE 7–2   Identity Synchronization for Windows Processes

Java Process Class Name	Component	When it Should be Present
`com.sun.directory.wps.watchdog.server.WatchDog`	Watchdog Process	Always
`com.sun.directory.wps.centrallogger.CentralLoggerManager`	Central Logger	Only where Core is installed
`com.sun.directory.wps.manager.SystemManager`	System Manager	Only where Core is installed
`com.sun.directory.wps.controller.AgentHarness`	Connector	One for each connector installed

If the expected number of processes are not running, then issue the following commands to restart all Identity Synchronization for Windows processes.

```
# /etc/init.d/isw stop
# /etc/init.d/isw start
```

If the WatchDog process is running, but the expected number of `java.exe` processes are not running, then verify that all components were installed properly. For information about verifying the components, see "Examining the `WatchList.properties` File" on page 101.

Like other system components, the Directory Server plug-in sends log records over the bus that are managed by the central logger for end-user viewing. However, the plug-in also logs some messages that may not show up over the bus, such as messages that are written when the subcomponent cannot contact the connector. These log messages only appear in the plug-in's `logs` directory on the file system, which should look something like the following:

serverroot/`isw-`*hostname*/`logs/SUBC`*id*

Because the plug-in runs with the Directory Server process, there could potentially be a problem for the plug-in's ability to write into its `logs` directory. This happens if the Directory Server runs as a different user than the owner of the `logs` directory. If the Directory Server process runs as a different user, give the plug-in explicit permissions using native operating system commands.

Troubleshooting Processes on Windows

Using the Service control panel, check that the Sun Java System Identity Synchronization for Windows service is started. If it is not started, then Identity Synchronization for Windows must be started.

If the service is started, then use the Task Manager to verify that the Watchdog process, `pswwatchdog.exe`, is running and that the expected number of `java.exe` processes are running. You should have one `java.exe` process for each connector installed on the machine. If the core component is installed, you should also have a `java.exe` process for each of the following:

- One for the message queue broker
- One for the system manager
- One for the central logger

Note – Other active Java processes, such as the Directory Service Control Center, may be running.

If the Watchdog process is not running, then restart the Sun Java System Identity Synchronization for Windows service. If it is running but the expected number of `java.exe` processes are not running, then verify that all components were installed properly. For information about verifying the components, see "Examining the `WatchList.properties` File" on page 101.

Examining the `WatchList.properties` File

On each machine where a Identity Synchronization for Windows component is installed, the isw-*machine_name*/resources/WatchList.properties file enumerates the components that should run on that machine. The process.name[n] properties name the components that should be running.

On machines where the core component is installed, the WatchList.properties file includes entries for the Central Logger and the System Manager as follows:

```
process.name[1]=Central Logger
process.name[2]=System Manager
```

On machines where the connectors are installed, the WatchList.properties file includes a separate entry for each connector as follows. The process.name property is the connector ID.

```
process.name[3]=CNN100
process.name[4]=CNN101
```

If the entries in the WatchList.properties file and the actively running processes are not the same, then restart the Identity Synchronization for Windows daemon or service.

If the WatchList.properties file contains too few a number of entries, for example only one connector entry even though two were installed, then examine the installation logs for possible installation failures. The location of the installation logs vary depending on your operating system as follows:

- On Solaris, installation logs are written to /opt/SUNWisw
- On Linux, installation logs are written to /var/opt/sun/isw/logs
- On Windows, installation logs are written to the %TEMP% directory, which is a subdirectory of the Local Settings folder located under

  ```
  C:\Documents and Settings\Administrator
  ```

  On some Windows systems, such as Windows 2000 Advanced Server, the Local Settings folder is a hidden folder. The following procedures describes how to view hidden folders.

▼ To View Hidden Folders and the `Temp` Subdirectory on Windows

1 Open your Windows Explorer.

2 From the Tools menu, select Folder Options.

3 When the Folder Options dialog box is displayed, select the View tab.

4 Check the Show Hidden Files checkbox.

Troubleshooting the Connector Subcomponents

This section guides you through the steps you should take to troubleshoot problems with the connector subcomponents. Before you begin, confirm the following:

- Are the subcomponents running?
- Is the Directory Server where the plug-in was installed running? Is the primary domain controller where the change detector and password filter were installed running?

Verifying Subcomponent Installation

Verify that all of the subcomponents are installed. Subcomponent installation must be done after the connector is installed. The subcomponents installed depend upon the connectors used as follows:

- For Active Directory Connectors, no subcomponents are installed.
- For Directory Server Connectors, the Directory Server plug-in must be enabled on the Directory Server being synchronized.
- For Windows NT Connectors, the Windows change detector and password filter subcomponents must be installed on the primary domain controller for each Windows NT domain being synchronized. These subcomponents are installed after the Windows NT Connector is installed.

For the Windows NT SAM Change Detector subcomponent to be effective, you must turn on the Windows NT audit log. To turn on the audit log, use the following procedure and then select Policies → Audit Policies. Select Audit These Events and then both the Success and Failure boxes for User and Group Management.

▼ To Turn on the Windows NT Audit Log

1   In the Start menu, select Programs, then Administrative Tools and User Manager.

2   In the Event Viewer, select Event Log Settings and then Event Log Wrapping.

3   Select Overwrite Events as Needed.

Verifying Server Restart After Installation

After you have installed the subcomponents, ensure that the correct post-installation steps have been taken. For example, after the Directory Server plug-in has been installed, the server must be restarted. After the Windows NT change detector and password filter have been installed on the primary domain controller, the server must be restarted.

Verifying Network Connections

If your subcomponents are still causing problems, confirm that they have established a network connection with the connector. On the machine where the connector is running, verify that the connector is listening for the subcomponent's connection by running the following command:

```
# netstat -n -a
```

For example, the netstat command shows that the connector is listening for incoming connections on port 9999 and the subcomponent has successfully connected as follows:

```
# netstat -n -a | grep 9999
*.9999
*.*     0   0 65536    0 LISTEN
12.13.1.2.44397 12.13.1.2.9999
73620 0 73620     0 ESTABLISHED
12.13.1.2.9999
12.13.1.2.44397 73620 0 73620
0 ESTABLISHED
```

However, if the subcomponent has not connected, the netstat command instead shows the following:

```
# netstat -n -a | grep 9999
*.9999
*.*     0   0 65536    0 LISTEN
```

After verifying that the subcomponent is running, examine the subcomponent's local logs for potential problems.

Verify that the correct port number was specified. Verify that the connector is running and is in the READY state. Examine the connector's local logs for potential problems.

If the connector is not listening for incoming connections, then the output of the netstat command appears as follows:

```
# netstat -n -a | grep 9999
#
```

Troubleshooting the Message Queue Component

This section describes how to troubleshoot problems with the Message Queue component and its broker. It contains the following topics:

This chapter contains the following sections:

Using telnet to Verify That the Message Queue Broker is Running

Verify that the Message Queue broker is running. Using the telnet command to connect to the machine and port where the Message Queue broker is running returns a list of the active Message Queue services:

```
# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is \q^]\q.
101 psw-broker 3.0.1
cluster tcp CLUSTER 32914
admin tcp ADMIN 32912
portmapper tcp PORTMAPPER 7676
ssljms tls NORMAL 32913
jms tcp NORMAL 32911
Connection closed by foreign host.
```

If the ssljms tcp NORMAL service is not listed in the output, then examine the Message Queue logs for potential problems. The location of the log depends on the platform you are using as follows:

- On Solaris, the log is in the following location:
  /var/imq/instances/psw-broker/log/log.txt

- On Linux, the log is in the following location:
  /var/opt/sun/mq/instances/isw-broker/log/log.txt

- On Windows, the log is in the following location:
  installation_root**isw-***machine_name***imq****var****instances****isw-broker****log****log.txt**

  If the telnet command fails, then either the broker is not running or the wrong port was specified. Check the port number in the broker's log. For example, the log contains a line for the broker's port as follows:

```
[13/Mar/2003:18:17:09 CST] [B1004]:
'Starting the portmapper service using tcp
[ 7676, 50 ]
with min threads 1 and max threads of 1'
```

If the broker is not running, start it on Solaris and Linux by running the `/etc/init.d/imq start` command. On Windows, start the broker by starting the `iMQ Broker` Windows service.

If you install Message Queue on Solaris 8, and you run the `mquinstall` command to install all of the packages, be sure to set `IMQ_JAVAHOME` property *before* running the `mqinstall` command. This ensures that the software picks the correct version of Java.

If you have not yet installed the core component, you do not have to set the `IMQ_JAVAHOME` property because the Identity Synchronization for Windows installation program tells the Message Queue broker which version of Java to use.

Collecting Additional Information About the Message Queue Broker

You can run the broker with the debug log turned on to help collect additional information about your problem. To turn on the debug log level, use the following command:

```
# imqbrokerd -loglevel DEBUG
```

You can get a debug dump of the broker using the following command:

```
imqcmd dump bkr -edebug -u admin -o file=filename
```

Troubleshooting Communication Problems With Directory Server

The Message Queue broker authenticates clients with the Directory Server that stores the Identity Synchronization for Windows configuration. If the broker cannot connect to this Directory Server, no clients can connect to the Message Queue. The broker log will contain a `javax.naming` exception, such as "`javax.naming.CommunicationException` or `javax.naming.NameNotFoundException`.

If a `javax.naming` exception occurs, take the following steps:

- Verify that all `imq.user_repository.ldap` properties in the `/var/imq/instances/isw-broker/props/config.properties` file have the correct values. If any of the values are incorrect, stop the Message Queue broker. Correct the errors, save the file, and restart the broker. Note that machine running the Message Queue broker must be able to resolve the Directory Server host name.

- Verify that the `imq.user_repository.ldap.password` property in the `/etc/imq/passfile` file is correct.

- Sometimes, the broker can not search for entries if the root suffix contains spaces. Verify that the root suffix name does not contain spaces.

Troubleshooting Memory Problems

During normal operation, the Message Queue broker consumes a modest amount of memory. However, during `idsync resync` operations, the broker's memory requirements increase. If the broker reaches its memory limit, undelivered messages will accumulate, the `idsync resync` operations will slow down dramatically or even, and Identity Synchronization for Windows may be unresponsive.

When the broker enters a low-memory state, the following messages will appear in its log:

```
[03/Nov/2003:14:07:51 CST] [B1089]:
In low memory condition,
Broker is attempting to f
ree up resources [03/Nov/2003:14:07:51 CST] [B1088]:
Entering Memory State [B0024]:
RED  from previous state [B0023]:
ORANGE - current memory is 1829876K,
90% of total memory
```

To avoid a low memory state, take the following steps:

- Increase the broker's memory limit to 1 or 2 GB, as explained in *Sun Java System Directory Server Enterprise Edition 6.2 Release Notes*.

- During an `idsync resync` operation, keep the log level set to `INFO`. Changing the log level to `FINE` or higher increases the load of the broker as more log messages are sent to the central logger.

- Run the `idsync resync` command for one synchronization user list at a time.

▼ To Recover From a Message Queue Broker Low Memory Condition

1 Verify that the broker has a backlog of undelivered messages.

Examine the broker's persistent message store in the appropriate directory for your operating system:

- On Solaris: `/var/imq/instances/psw-broker/filestore/message/`

- On Linux: `/var/opt/sun/mq/instances/isw-broker/filestore/message/`

- On Windows:
  installation_root\isw-*machine_name*\imq\var\instances\isw-broker\filestore\message\

Each file in this directory contains a single undelivered message. If there are more than 10,000 files in this directory, then the broker has a backlog of messages. Otherwise, an undelivered message backlog is not causing the problem with the broker.

The message backlog usually contains log files related to an idsync resync operation and you can safely remove them.

2   **Stop the Message Queue broker.**

   For more information, see "Starting and Stopping Services" in *Sun Java System Directory Server Enterprise Edition 6.2 Installation Guide*.

3   **Remove all files in the persistent message store.**

   The easiest way to remove these files is by recursively removing the message/ directory and then recreating it.

4   **Restart the Message Queue broker.**

   To avoid running out of memory in the future, take the steps described earlier in this section.

Troubleshooting Problems With Identity Synchronization for Windows Over SSL

This section describes how to troubleshoot problems using Identity Synchronization for Windows over SSL. It contains the following topics:

This chapter contains the following sections:

- "Troubleshooting Problems With SSL Between Core Components" on page 107
- "Troubleshooting Problems With SSL Between Connectors and Directory Server or Active Directory" on page 108
- "Troubleshooting Problems With SSL Between the Directory Server and Active Directory" on page 108
- "Troubleshooting Problems With Certificates" on page 109

Troubleshooting Problems With SSL Between Core Components

The Identity Synchronization for Windows installation program cannot verify that the SSL port provided during core installation is correct. If you type the SSL port incorrectly during core installation, then the core components will not be able to communicate properly. You may not

notice a problem until you try to save your configuration for the first time. The Identity Synchronization for Windows Console displays the following warning:

```
The configuration was successfully saved,
however, the System Manager could not be
notified of the new configuration.
```

The system manager log contains the following entry:

```
[10/Nov/2003:10:24:35.137 -0600] WARNING 14
example  "Failed to connect
to the configuration directory because "Unable to connect: (-5981)
Connection refused by peer."
Will retry shortly."
```

If you receive these warning and error messages, uninstall the core and install it again with the correct SSL port number.

Troubleshooting Problems With SSL Between Connectors and Directory Server or Active Directory

If a connector is unable to connect over SSL to the Directory Server or Active Directory, then the following message appears in the central error log:

```
[06/Oct/2006:14:02:48.911 -0600]
WARNING 14  CNN100 host1
"failed to open connection
to ldaps://host2.example.com:636."
```

Open the Identity Synchronization for Windows Console and go to the Specifying Advanced Security Options panel. Confirm that the SSL port is correct.

Troubleshooting Problems With SSL Between the Directory Server and Active Directory

By default, Directory Server does not communicate with Active Directory over SSL when performing on-demand password synchronization. If the default is overridden to protect this communication with SSL, then the Active Directory CA certificate must be added to the Directory Server certificate database of each master replica as described in Chapter 4, "Understanding the Product," in *Sun Java System Directory Server Enterprise Edition 6.2 Installation Guide*.

If the Active Directory CA certificate is not added, users fail to bind to Directory Server with the error DSA is unwilling to perform. The plug-in's log, isw-*hostname* /logs/SUBC100/pluginwps_log_0.txt, reports the following:

```
[06/Nov/2006:15:56:16.310 -0600]
INFO    td=0x0376DD74 logCode=81
ADRepository.cpp:310
"unable to open connection to Active Directory server
at ldaps://host2.example.com:636, reason: "
```

If you receive these errors, you must add the Active Directory CA certificate to Directory Server's certificate database and restart Directory Server.

Troubleshooting Problems With Certificates

This section describes how to troubleshoot various problems using certificates with Identity Synchronization for Windows. It contains the following sections:

This chapter contains the following sections:

- "Untrusted Certificates" on page 109
- "Mismatched Hostnames" on page 110
- "Expired Certificates" on page 111

Untrusted Certificates

Go to the central audit log when you receive notice that the certificate is untrusted. For example, if the LDAP server's SSL certificate is not trusted, this message is logged as follows:

```
[06/Oct/2006:14:02:48.951 -0600] INFO
14  CNN100 host1  "failed to open connection to
ldaps://host2.example.com:636, error(91):
Cannot connect to the LDAP server,
reason: SSL_ForceHandshake failed:
(-8179) Peer's Certificate issuer
is not recognized."
```

When you receive this sort of error, it is usually because the CA certificate has not been added to the connector's certificate database. Run the certutil tool to see if the certificate has been added. For more information about this tool, see "About the certutil and ssltap Tools" on page 86.

In this example, the certificate database contains no certificates:

```
# /usr/sunone/servers/shared/bin/certutil
 -L -d /usr/sunone/servers/
 isw-host1/etc/CNN100
```

```
Certificate Name              Trust Attributes
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

In the following example, the certificate database contains only the Active Directory CA certificate:

```
# /usr/sunone/servers/shared/bin/certutil -L -d
/usr/sunone/servers/ isw-host1/etc/CNN100
Certificate Name                          Trust Attributes
example.com CA                             C,c,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

As shown here, the trust flags of the CA certificate must be C, , . If the certificate exists and the trust flags are set properly but the connector still can not connect, then verify that the connector was restarted after adding the certificate. Use the ldapsearch command to help diagnose the problem. If ldapsearch does not accept the certificate, then neither will the connector. For example, ldapsearch can reject certificates if they are not trusted as follows:

```
# /usr/sunone/servers/shared/bin/ldapsearch
-Z -P /usr/sunone/ servers/isw-host1/etc/CNN100
-h host2 -b "" -s base "(objectclass=*)
"ldap_search: Can't contact LDAP server
SSL error -8179
Peer's Certificate issuer is not recognized.)
```

The -P option directs ldapsearch to use the CNN100 connector's certificate database for SSL certificate validation. After the correct certificate is added to the connector's certificate database, verify that ldapsearch accepts the certificate, and then restart the connector.

Mismatched Hostnames

When Identity Synchronization for Windows tries to establish SSL connections, the connectors verify that the server's hostname matches the hostname in the certificate that is presented by the server during the SSL negotiation phase. If the hostnames do not match, the connector will refuse to establish the connection.

The directory source hostname in the Identity Synchronization for Windows configuration file must always match the hostname embedded in the certificate used by that directory source.

You can use ldapsearch to verify that the hostnames match as follows:

```
/var/mps/serverroot/shared/bin/ldapsearch.exe
-Z -P /var/opt/SUNWisw/etc/CNN100 -3
-h host2.example.com -p 636
-s base -b "" "(objectclass=*)"
```

If the hostname given in the ldapsearch command-line and the hostname embedded in the certificate are not the same, then the following error message is displayed:

```
ldap_search: Can't contact LDAP server
SSL error -12276
(Unable to communicate securely with peer: requested
do main name does not match
the server's certificate.)
```

If the hostnames match, the ldapsearch command is successful and displays the contents of the root DSE.

Expired Certificates

If the server's certificate has expired, the following message appears in the log:

```
[06/Oct/2006:14:06:47.130 -0600]
INFO    20  CNN100 host1
"failed to open connection to ldaps://host2.example.com:636,
error(91): Cannot connect to the LDAP server,
reason: SSL_ForceHandshake failed:
(-8181) Peer's Certificate has expired."
```

If you receive this message in your log file, the server must be issued a new certificate.

Troubleshooting Active Directory Domain Controller Problems

The Active Directory domain controller is a global catalog server that stores the objects from all domains in the forest. When you restore an Active Directory domain controller from backup files, some counters are not reset. To ensure all counters are reset appropriately, resynchronize all users after restoring an Active Directory domain controller.

8

Troubleshooting DSCC and 5.x Console Problems

This chapter contains information to help you troubleshoot problems with the Directory Service Control Center (DSCC) and the 5.x Console, It contains the following sections:

This chapter contains the following sections:

Possible Causes of DSCC Problems

The DSCC may fail for one of the following reasons:

- Sun Java Web Console is not running
- DSCC application not registered in the Sun Java Web Console
- DSCC registry has not been created
- The Application Server used for the DSCC WAR deployment is not running.

Collecting DSCC Troubleshooting Data

This section describes how to collect information about DSCC failures.

▼ To Collect DSCC Troubleshooting Data

1 **Verify that the Sun Java Web Console is running.**

```
# smcwebserver status
Sun Java(TM) Web Console is running
```

2   Verify the status of the DSCC.

/opt/SUNWdsee/dscc6/bin/dsccsetup status

If it is running correctly, this command should give the following output:

```
***
DSCC Application is registered in Sun Java (TM) Web Console
***
DSCC Agent is registered in Cacao
***
DSCC Registry has been created
Path of DSCC registry is /var/opt/sun/dscc6/dcc/ads
Port of DSCC registry is 3998
***
```

3   If the status says that the DSCC application is not registered, you need to reinitialize the DSCC.

When the DSCC application is not registered, the DSCC does not appear in the Sun Java Web Console. Reinitialize the DSCC using the following command:

dsccsetup console-reg

4   If the status says that the DSCC agent is not registered, reinitialize the agent.

When the DSCC agent is not registered, the local Directory Server and Directory Proxy Server instances can not be managed from a remote DSCC. Reinitialize the agent using the following command:

dsccsetup cacao-reg

5   If the status message states that the DSCC registry has not been created, initialize the DSCC registry.

When the registry does not exist, the DSCC application needs to be initialized. Initialize the registry using the following command:

dsccsetup ads-create

6   If the other actions do not help, run a clean setup for the DSCC.

Running a clean setup resets the DSCC but in the process you lose the DSCC registry.

Run each of the following commands:

/opt/SUNWdsee/dscc6/bin/dsccsetup dismantle
#/opt/SUNWdsee/dscc6/bin/dsccsetup initialize

These commands cleanup and reconfigure the DSCC and its agents.

Collecting and Analyzing 5.x Console Data

This section describes how to collect and then analyze data about failures with the 5.x Directory Server console.

The console may fail for one of the following reasons:

- Directory Server not running
- The user that is logged in is missing rights
- Wrong jar files
- Wrong version of Java

▼ Collecting 5.x Console Troubleshooting Data

1 Verify that the Admin Server is running.

```
# ps -ef | grep httpd
```

If yes, proceed to the next step.

2 Verify that Directory Server is running.

```
# ps -ef | grep slapd
```

If yes, proceed to the next step.

3 Collect the Admin Server logs.

4 Launch the startconsole **command in debugging mode as follows:**

```
# ./startconsole -D 9:all -f /tmp/console_trace
```

Now reproduce the problem. Check the console_trace file output by the startconsole command for errors, such as the Java version, paths to loaded jar files, Java exceptions.

5 Match the exceptions in the console_trace **file with the contents of the errors log.**

Analyzing the Console Data

If you are using a 5.2 version of the Console, confirm that the correct jar files are being used.

Next, determine if a 5.1 installation of the Console existed previous to your installation of the 5.2 version. You can make this verification by running startconsole as follows:

```
# ./startconsole -D
```

If running this command does not work, use the following instead:

```
# /usr/sbin/directoryserver -u 5.2 startconsole
```

If running the command from the /usr/sbin/directoryserver directory works, then you hang is a result of a version compatibility issue. After you have installed the 5.2 version of Directory Server , run the following command to set the default version to 5.2.

```
/usr/sbin/directoryserver -d 5.2
```

Now you can use the various `directoryserver` commands with the 5.2 version of Directory Server.

You may need to confirm that the `/etc/ds` file contains the following settings as well:

```
5.1|//usr/iplanet/ds5/sbin/directoryserver|YES|YES
5.2|//usr/ds/v5.2/sbin/directoryserver|YES|NO
```

9

Directory Server Error Log Message Reference

This chapter lists messages logged by Directory Server. While this list is not exhaustive, the information presented in this chapter serves as a good starting point for resolving common problems.

This chapter includes the following sections:

- "Common Error Codes" on page 118
- "Common Warning Codes" on page 213
- "Verifying Plug-In Signatures" on page 228

Log messages are defined according to their severity.

Error   The error is severe. Immediate action should be taken to avoid the loss or
          corruption of directory data.

Warning   Action should be taken at some stage to prevent a severe error occurring in the
          future.

Info   An informative message, usually describing server activity. No action is necessary.

Note – When using the error log for debugging, increase the log level progressively until the debugging data you need becomes evident in the log. Do not enable error logging for all Directory Server components at once, especially on a production system, to avoid severely impacting performance.

In the case of internal errors, plug-in writers should check their parameters to `slapi_*()` functions first.

Common Error Codes

This section describes the error codes displayed in the *instance-path*/`logs/errors` log and the appropriate action to take should these errors occur.

`4104: No backend has been defined to do the import.`
Cause: The server cannot detect a backend to do the import. This is an internal error and should not occur under normal circumstances.

Solution: Contact Sun Technical Support.

`4105: Bulk import not supported by this backend.`
Cause: The backend will not accept wire import. This is an internal error and should not occur under normal circumstances.

Solution: Contact Sun Technical Support.

`4107: Ignoring extremely large value for configuration attribute` *attribute_name*.
Cause: The value of the specified configuration attribute is too large.

Solution: Change the value of the specified configuration attribute. Refer to the attribute description for the acceptable value range.

`4108: The given file` *filename* `could not be accessed.`
Cause: The server is unable to obtain any information on the specified configuration file.

Solution: Check that the file exists and that it has the appropriate access rights.

`4109: The given file` *filename* `could not be opened for reading.`
Cause: The server is unable to open the specified configuration file.

Solution: Check that the file exists and that it has the appropriate access rights.

`4110: Could only read` *value* `of` *value* `bytes from configuration file` *filename*.
Cause: The server is unable to read the specified configuration file.

Solution: Check that the file exists and that it has the appropriate access rights.

`4111: The default password storage scheme SSHA could not be read or was not found in the file` *filename*. `It is mandatory. Server exiting.`
Cause: The mandatory password storage scheme Salted Secure Hashing Algorithm (SSHA) could not be retrieved from the configuration file.

Solution: Check that the password storage scheme SSHA exists in the configuration file. If it is not present, add it.

4112: Skipping plugin *plugin* - no valid signature.
  Cause: The specified plug-in does not have a valid signature.

  Solution: Provide a valid signature for the plug-in or disable the plug-in.

4112: Unable to load plugin *plugin_name*.
  Cause: An error occurred while loading configuration information for the specified plug-in.

  Solution: Check that the configuration information for the specified plug-in is accurate. For more information, it may be useful to turn debugging on for SLAPI_DEBUG_PLUGIN. Change the configuration information as required and restart the server.

4119: No password storage scheme plug-ins defined in the configuration.
  Cause: No encoding scheme was found in the configuration file.

  Under normal circumstances, this error will not occur, because the server cannot start if the mandatory scheme SSHA is not present in the configuration file.

  Solution: Add a password storage scheme plug-in to the configuration file and restart the server.

4120: Invalid scheme to hash password: *scheme*. Valid values are: *scheme values*.
  Cause: The tag (algorithm) specified to hash the password is not defined in the configuration file.

  Solution: Add a password storage scheme to the configuration file, or change the specified scheme, and restart the server.

4121: Invalid scheme: *scheme*. No password storage scheme loaded.
  Cause: The tag (algorithm) specified to hash the password is defined but the server is unable to retrieve the associated information.

  Solution: Check the password storage scheme configuration and its installation and restart the server.

4122: The configuration files in *directory* directory could not be read or were not found. Please refer to the error log or output for more information.
  Cause: An error occurred reading the configuration files. The specific cause for the error is logged in the log files.

  Solution: Refer to the log files for more information.

4123: The configuration file dse.ldif in directory *directory* could not be read or was not found. Please refer to the error log or output for more information.
  Cause: An error occurred reading the Directory Server configuration file. The specific cause for the error is logged in the log files.

  Solution: Refer to the log files for more information.

4124: Unknown attribute *attribute_name* will be ignored
  Cause: An attempt was made to set an unknown attribute in the configuration file.

  Solution: Check and correct the attribute name.

4125: The configuration file *filename* was not restored from backup.
  Cause: The configuration file backup has failed. The reason for the failed backup is provided in the error message.

  Solution: Correct the error and back up the configuration file manually.

4126: Failed to create lock. Cannot register supported SASL mechanism. Server exiting.
  Cause: This indicates a resource problem on the machine.

  Solution: Restart the server.

4127: Failed to create lock. Cannot register supported extended operations. Server exiting.
  Cause: This indicates a resource problem on the machine.

  Solution: Restart the server.

4128: Could not load configuration file *filename*.
  Cause: An error occurred when attempting to load the specified configuration file.

  Solution: Check that the configuration file exists and that it has the appropriate access permissions. Refer to the error log for more details.

4129: Bad configuration file. Edit the configuration file to correct the reported problems and then restart the server. Server exiting.
  Cause: There is an error in the configuration file. Details of the error are reported in the error log.

  Solution: Edit the configuration file to correct the reported problems and restart the server.

4130: Cannot copy DSE file *filename* to *path*.
Cause: Several possible causes (file system full, incorrect permissions, etc.). Details of the error are reported in the error log.

Solution: Check that the configuration file exists and that it has the appropriate access permissions.

4131: The entry *entry_name* in file *filename* is invalid.
Cause: The server cannot read the specified entry. Details of the error are provided in the error message.

Solution: Check that the entry is valid and change as necessary.

4132: Cannot parse DSE entry *entry_name*.
Cause: The server cannot parse the specified entry. There is an error in the LDIF syntax of the entry.

Solution: Check that the entry is valid and change as necessary.

4133: Cannot write temporary DSE file *filename*.
Cause: System error (file system full, incorrect permissions, etc.)

Solution: Check the log file for more information and restart the server.

4134: Cannot backup DSE file *filename*.
Cause: The server cannot write to the specified DSE file.

Solution: Check the specified path and ensure that you have the appropriate write permissions.

4135: Cannot rename temporary DSE file *filename*.
Cause: The server cannot rename the specified DSE file.

Solution: Check the specified path and ensure that you have the appropriate write permissions.

4136: Invalid plugin action *plugin_name*.
Cause: The configuration file contains an invalid value for the specified plug-in.

Solution: Check the value in the configuration file and set a valid value.

4137: Attempting to delete a child entry whose existence is unknown to the parent. Deletion attempt ignored.
Cause: An attempt was made to delete a child entry for which there was no subcount on the parent.

Solution: This error should not occur under normal circumstances.

4138: Failed to start *plugin_name* plug-in.
Cause: Plug-in dependencies have not been configured correctly.

Solution: Check that the dependencies are valid and that they are enabled.

4139: Failed to resolve plug-in dependencies.
Cause: An error occurred while resolving dependencies (usually the consequence of an earlier problem such as a disabled plug-in, etc.)

Solution: Check that the dependencies are valid and that they are enabled.

4140: Could not load symbol *symbol_name* from library *library_name* for plug-in *plugin_nam*e.
Cause: This may be due to:

1. Incorrect configuration of the plug-in entry
2. A plug-in library missing or in the wrong location
3. The expected symbol corresponding to the init function not found in the plug-in library

Solution: Perform the following steps:

1. Check the plug-in configuration.
2. Check that the library path and the init function name are correct.

4152: Unknown plugin type *type*.
Cause: A plug-in configuration entry does not have a recognized plug-in type.

Solution: Check the configuration and correct the specified plug-in entry.

4153: Only one instance allowed for plugin type *type*.
Cause: Multiple plug-ins of the specified type have been defined in the configuration. Only a single plug-in of that type is allowed.

Solution: Correct the configuration so that there is only a single plug-in of the specified type.

4158: UNBIND
Cause: Invalid unbind PDU. This is an error in the client code.

Solution: Correct the error in the client code.

4159: Bad controls in the UNBIND.
   Cause: Invalid controls in an unbind PDU. The control is marked as critical and is unknown to the server or the control is badly encoded. This is an error in the client code.

   Solution: The client should not require critical controls on unbind. Correct the error in the client code.

4160: Cannot retrieve internal operation result for search operation ("*operation*" subtree *subtree*)
   Cause: While performing an internal search, Directory Server could not retrieve the operation from the parameter block.

   Solution: Contact Sun Technical Support.

4161: Cannot allocate pblock for an internal search ("*baseDN*" *scope filter*)
   Cause: While performing an internal search, Directory Server could not allocate space for the parameter block structure.

   Solution: Check that sufficient memory is available on the system.

4162: ldapu_get_cert_subject_dn_fails
   Cause: The server is unable to obtain the subject in the client certificate.

   Solution: Check the message in the error log for more information.

4163: ldapu_get_cert_issuer_dn_fails
   Cause: The server is unable to obtain the certificate issuer of the client certificate.

   Solution: Check the message in the error log for more information.

4164: Bad BER decoding of an attribute value assertion.
   Cause: An error occurred during the decoding of an attribute value assertion. The format of the attribute value assertion is incorrect.

   Solution: Check the client application making the request.

4165: BER decoding: found *id* instead of *id* for MessageId.
   Cause: The Message ID tag was not found in the LDAP request.

   Solution: The request is invalid. Check the application that created the request.

4166: BER decoding: ber_peek_tag returns no Operation tag.
   Cause: An error occurred while decoding the operation tag.

   Solution: The request is invalid. Check the application that created the request.

4167: Load library error.
Cause: An error occurred while loading the dynamic library. This may be because the library does not exist, the library requires another library that does not exist, or the library could not resolve a symbol.

Solution: Check that the library exists and is accessible.

4168: Compute hash of a node in a filter but the filter choice is not valid *type*
Cause: While attempting to calculate the hash for a filter node, Directory Server encountered an invalid type.

Solution: Contact Sun Technical Support.

4169: Compare two filters but the filter choice is not valid *type*
Cause: While attempting to compare two filters, Directory Server encountered an invalid type.

Solution: Contact Sun Technical Support.

4170: slapi_filter_test_ext: found unknown filter type *type*
Cause: While attempting to test whether an entry matches a filter, Directory Server encountered an invalid type.

Solution: Contact Sun Technical Support.

4171: slapi_vattr_filter_test_ext: found unknown filter type *type*
Cause: While attempting to test whether an entry matches a filter, Directory Server encountered an invalid type.

Solution: Contact Sun Technical Support.

4173: slapd_init: could not create one or more locks for communication purpose (operations connections...)
Cause: Directory Server could not create locks due to resource constraints.

Solution: Check that Directory Server is not having to contend for system resources with other applications.

Restart Directory Server.

4175: FrontendConfig_init: failed to initialize read-write lock structure.
Cause: Directory Server could not create locks due to resource constraints.

Solution: Check that Directory Server is not having to contend for system resources with other applications, and that sufficient memory is available on the system.

Restart Directory Server.

4176: config_set: the attribute *attribute* is read only; ignoring new value *value*
Cause: A read-only attribute value has been changed.

Solution: Do not change the attribute value.

4177: Could not open lockfile *filename* in write mode.
Cause: The specified lock file could not be opened.

Solution: Check that the lock file exists and is accessible.

4178: Could not open file *filename* in mode *mode*.
Cause: The specified file could not be opened.

Solution: Check that the file exists and is accessible.

4185: Cannot allocate lock and/or conditional variable to handle slapd_started variable.
Cause: Directory Server could not create locks or conditional variables due to resource constraints.

Solution: Check that Directory Server is not having to contend for system resources with other applications, and that sufficient memory is available on the system.

4186: *** DISK FULL *** Attempting to shut down gracefully.
Cause: One of the following:

- Directory Server ran out of disk space.
- Directory Server is not properly configured to access data in a backend.

Solution: Provide more local disk space to Directory Server, if necessary.

Check that nsslapd-backend is correctly set in the appropriate mapping tree entry under cn=config.

Check that the backend state is set correctly.

Check that the backend is not offline.

4187: Trying to get a block element but the element identifier *ID* is unknown.
Cause: Directory Server tried to access a parameter block field that does not exist.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

4188: Trying to set a block element but the element identifier *ID* is unknown.
Cause: Directory Server tried to modify a parameter block field that does not exist.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

4189: sequence error in error strings at item *index*. Error *error* (*string*) should come after error *error* (*string*)
Cause: Directory Server encountered a problem encoding an error.

Solution: Contact Sun Technical Support.

4190: Internal search base="*base*" scope=*scope* filter=*filter* Result: *code* (*message*)
Cause: An internal search used for authentication failed.

Solution: Check that the client credentials allow it to access the entry to be used for authentication.

4191: Failed to change user and group identity to that of *user*.
Cause: The server was unable to change the user and group identity to the specified user.

Solution: Check the user privileges and correct.

4197: MODRDN invalid new RDN ("*RDN*")
Cause: The modify RDN operation on the specified entry did not succeed.

Solution: Try again with a valid new RDN.

4197: MODRDN invalid new superior ("*DN*")
Cause: The modify RDN operation on the specified entry did not succeed.

Solution: Try again with a valid new parent entry.

4210: Protocol error Account Usable control MUST be marked critical
Cause: The account usability control was not marked critical.

Solution: Notify the maintainer of the client application.

4211: *error-code* occurred while changing state of backend *backend-name*. Resetting state.
Cause: An error occurred while putting backends off line.

Solution: Verify all backends are in a correct and functional state.

4212: `Server is already suspending all operations.`
Cause: An administrator tried to put the already frozen server in frozen mode.

Solution: None.

4213: `error-code while stopping databases. Please make sure suffixes are online.`
Cause: An error occurred while putting the server in frozen mode.

Solution: Check that all suffixes supported by the server respond to read and write operations then try again.

4612: `Unable to start slapd because it is already running as process process.`
Cause: Unable to start Directory Server because it is already running.

Solution: Stop the running server instance before launching a new server.

4613: `Unable to start slapd because the process process is importing the database`
Cause: Unable to start Directory Server because a process is currently importing the database.

Solution: Stop the running import process instance before launching a new server.

4614: `Unable to run db2ldif with the -r flag because the database is being used by another slapd process.`
Cause: Unable to run db2ldif with the -r flag because the database is being used by another Directory Server process.

Solution: If the other process is not an import process, run db2ldif.pl -r instead. If it is an import process, stop the running import process before launching db2ldif.

4615: `Unable to run db2ldif because the process process is importing the database`
Cause: Unable to run db2ldif because a process is currently importing the database.

Solution: Stop the running import process before launching db2ldif.

4616: `Unable to run db2bak because the process process is importing the database`
Cause: Unable to run db2bak because a process is importing the database.

Solution: Stop the running import process before launching db2bak.

4617: `Unable to import the database because it is being used by another slapd process`
Cause: Unable to import the database because it is being used by another slapd process.

Solution: Stop Directory Server before importing.

4618: Unable to create an index because the database is being used by another
slapd process
   Cause: Unable to create an index because the database is being used by another slapd process.

   Solution: Stop Directory Server before creating indexes.

4623: Pathname *path* too long.
   Cause: When trying to convert the absolute path, it was discovered that the pathname is too long.

   Solution: Change the relative path or the absolute path base so that the sum of their length is lower than the maximum allowed length.

4625: Cannot determine current directory.
   Cause: When trying to convert the absolute path, the server was unable to determine the current directory.

   Solution: Contact Sun Technical Support.

4626: slapi_add_internal: add_values for type *type* failed.
   Cause: Internal error when converting from a set of modifications to an entry.

   Solution: Contact Sun Technical Support.

4627: Unable to test the database because it is being used by another slapd
process
   Cause: Unable to test the database because it is being used by another Directory Server process.

   Solution: Stop the running process and retry.

4629: Unable to create directory.
   Cause: System error - the directory could not be created.

   Solution: Check that your file system is valid and retry.

4630: ref_array_init: new lock creation failed
   Cause: Directory Server could not create locks due to resource constraints.

   Solution: Check that Directory Server is not having to contend for system resources with other applications.

   Restart Directory Server.

4631: ref_adjust: referrals suppressed (could not get target DN operation or scope from pblock).
   Cause: Referrals have been suppressed. The server was unable to obtain the target DN and operation structure.

   Solution: Contact Sun Technical Support.

4633: Suffix to be imported contains encrypted attributes.
   Cause: No password for the key database has been supplied within the arguments configured for this suffix. The password is required to retrieve the key and proceed with encryption.

   Solution: Use the -Y *pwd* or -y *pwd-file* arguments when executing the ldif2db command.

4634: Security initialization for attribute encryption failed.
   Cause: The security initialization required by the attribute encryption feature failed.

   Solution: Make sure that the password supplied is correct and that the password file syntax is correct. Check that SSL has been configured correctly (certificate file ciphers.)

4737: Security Initialization failed: unable to read configuration from *dn*.
   Cause: Security initialization failed. The server was unable to read the configuration from the specified configuration DN.

   Solution: Check that the configuration DN is valid and retry.

4738: Security Initialization: Failed to retrieve SSL configuration attribute nscertfile from *filename*
   Cause: Security initialization error. The server was unable to retrieve the SSL configuration attribute nscertfile.

   Solution: Check that the value of the nscertfile attribute is correct and retry.

4739: Security Initialization: Failed to retrieve SSL configuration information (error *error*): nskeyfile: *filename* nscertfile: *filename*
   Cause: Security initialization error. The server was unable to retrieve one of the SSL configuration attributes, nscertfile or nskeyfile.

   Solution: Check that the value of the nscertfile and nskeyfile attributes are correct and retry.

4740: Security Initialization: NSS initialization failed (error *error*): path: *path* certdb prefix: *prefix* keydb prefix: *prefix*.
   Cause: Security initialization error. NSS initialization failed.

   Solution: Check the NSS configuration and retry.

4741: Security Initialization: NSS initialization failed (error *error*)
Cause: Security initialization error. NSS initialization failed.

Solution: Contact Sun Technical Support.

4742: Security Initialization: Failed to retrieve SSL configuration information
(error *error*): nssslSessionTimeout: variable
Cause: Security initialization error. The server was unable to retrieve the SSL configuration
attribute nssslSessionTimeout.

Solution: Check that the value of the nssslSessionTimeout attribute is correct and retry.

4744: Security Initialization: Unable to get token for variable cipher family
(error *error*)
Cause: Security initialization error. The server was unable to obtain the required token (from
the nsssltoken attribute).

Solution: Check that the nsssltoken attribute is present in the cipher family entry, and that it
has a valid value.

4745: Security Initialization: Unable to find slot for variable cipher family
(error *error*)
Cause: Security initialization error. The server was unable to find the required slot.

Solution: Make sure that the security token (external or internal) is accessible to the server.

4746: slapd_get_tmp_dir mkdir(variable) Error: *error*
Cause: System error. The server was unable to create a temporary directory.

Solution: Check that the current user has sufficient access rights to create the temporary
directory and try again.

4747: Security Initialization: Unable to set SSL export policy (error *error*)
Cause: Security initialization error. The server was unable to set the SSL export policy.

Solution: Contact Sun Technical Support.

4748: Security Initialization: Failed to set SSL cipher preference information:
cipher (error *code - message*)
Cause: Security initialization error. The server was unable to set SSL cipher preference
information.

Solution: Perform the following steps:

1. Check the syntax of the ciphers in the configuration.
2. Make sure that all the ciphers are supported by the server.

4749: Security Initialization: Failed to import NSPR fd into SSL (error *error*)
Cause: Security initialization error. The server was unable to import the NSPR file descriptor into SSL.

Solution: Contact Sun Technical Support.

4750: Security Initialization: Unable to get internal slot (error *error*)
Cause: Security initialization error. The server was unable to obtain the internal slot.

Solution: Contact Sun Technical Support.

4751: Security Initialization: Unable to authenticate (error *error*)
Cause: Security initialization error. The server was unable to authenticate.

Solution: Contact Sun Technical Support.

4756: None of the ciphers are valid.
Cause: The ciphers are invalid.

Solution: Check the ciphers and retry.

4757: Config of SSL session cache failed: out of disk space! Make more room in the temp directory and try again.
Cause: The configuration of the SSL session cache failed, due to a disk space problem.

Solution: Free space in the */tmp* directory and try again.

4758: Config of SSL session cache failed (error *error*).
Cause: The configuration of the SSL session cache failed.

Solution: Contact Sun Technical Support.

4759: Security Initialization: Failed to enable security on the imported socket (error *error*)
Cause: Security initialization error. The server could not enable security on the imported socket.

Solution: Contact Sun Technical Support.

4760: Security Initialization: Failed to enable SSLv3 on the imported socket (error *error*)
Cause: Security initialization error. The server could not enable SSLv3 on the imported socket.

Solution: Contact Sun Technical Support.

4761: Security Initialization: Failed to enable TLS on the imported socket
(error *error*)
   Cause: Security initialization error. The server could not enable TLS on the imported socket.

   Solution: Contact Sun Technical Support.

4766: Encryption alias not configured.
   Cause: The encryption alias has not been configured.

   Solution: Contact Sun Technical Support.

4769: Failed to set SSL client ready for client authentication: certificate db:
database returned code *return_code* (error *error*)
   Cause: The server was unable to set the SSL client ready for client authentication.

   Solution: Check that the certificate and key databases are accessible to the server (acting as an SSL client).

4772: SSL client authentication cannot be used (no password) (error *error*)
   Cause: SSL client authentication cannot be used because a password has not been defined.

   Solution: Make sure that the server receives the password for the security token, using a pin.txt file option with the start-slapd command.

4773: ldapssl_enable_clientauth (*variable*) (error *error*)
   Cause: SSL error - the server cannot enable client authentication.

   Solution: Check that the password given to the server is correct.

4774: ldap_simple_bind_s(*variable*) (error *error*)
   Cause: Simple bind over SSL failed. The password may be incorrect.

   Solution: Check that the password for the DN is correct.

4775: ldap_sasl_bind(LDAP_SASL_EXTERNAL) (error *error*)
   Cause: The bind attempt failed with the SASL EXTERNAL method. The server was unable to find any external credentials.

   Solution: Make sure that the client's certificate is received by the server before the bind attempt.

4776: sasl *error* message
   Cause: SASL error. The details of the error are logged in the error log.

   Solution: Check the error log for more information.

4779: Security initialization: Unable to create PinObj (error *error*.)
    Cause: Security initialization error. The server was unable to create the pin object.

    Solution: Make sure that the server receives the password for the security token, using a `pin.txt` file option with the `start-slapd` command.

4780: Security Initialization: Unable to authenticate to slot for *variable* cipher family (error *error*)
    Cause: Security initialization error. The server was unable to authenticate to the required slot.

    Solution: The password entered was incorrect. Check the correct password and retry.

4781: SSL is misconfigured. Client authentication is enabled but no certificate authority is trusted for SSL client authentication.
    Cause: The server is configured to allow or require client authentication for SSL. The database contains no CA certificates marked as trusted for issuing client certificates. The server cannot perform SSL client authentication.

    Solution: Install one or more CA certificates using Directory Service Control Center. Ensure that the trust attributes of CA certificates installed with `certutil` include the T trust attribute.

4782: Failed to create context for cipher operation.
    Cause: NSS context creation failed.

    Solution: Ensure that a valid certificate is available so that the key may be generated.

4783: Out of memory to create a buffer to hold the encrypted output (error *code - string*).
    Cause: Directory Server could not allocate memory needed to encrypt attributes.

    Solution: Make more memory available to Directory Server.

4784: Out of memory to create a buffer to hold the cleartext input (error *code - string*).
    Cause: Directory Server could not allocate memory needed to encrypt attributes.

    Solution: Make more memory available to Directory Server.

4785: Cipher operation failed.
    Cause: The server was unable to accomplish the cipher operation.

    Solution: It is likely that the context is incorrect. Restart the server.

4786: Crypto mechanism not supported by this server.
Cause: The cryptography mechanism is invalid or unsupported.

Solution: Generate a symmetric key for the cryptography mechanism or choose a supported mechanism.

4787: Out of memory to create a buffer to hold the cleartext output (error *code - string*).
Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4788: Out of memory to create a buffer to hold the encrypted input (error *code - string*).
Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4789: Out of memory to create a pwd item. (error *code - string*).
Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4790: Out of memory to create a buffer to hold the pwd item data (error *code - string*).
Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4791: Out of memory to create the salt (error *code - string*).
Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4792: Out of memory to create a buffer to hold the salt data (error *code - string*).
Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4793: Failed to generate symmetric key.
Cause: The server was unable to generate the symmetric key.

Solution: Check that a security token is available to the server (as a certificate.)

4794: Out of memory to create a buffer to hold the parameter data (error *code - string*).

Cause: Directory Server could not allocate memory needed to encrypt attributes.

Solution: Make more memory available to Directory Server.

4795: Failed to map key generation parameters into crypto operation ones.

Cause: The server was unable to map the key generation mechanism to the cryptography mechanism.

Solution: Restart the server.

4796: Unable to retrieve private key for certificate.

Cause: The server was unable to retrieve a private key from the certificate.

Solution: Ensure that the certificate has been imported into the database with both its private and public keys. (This is usually performed as part of the process beginning with a certificate request.)

4797: Signature failed.

Cause: The signature required for attribute encryption failed.

Solution: Restart the server.

4798: Key database password was rejected.

Cause: The password for the key database has been rejected.

Solution: Enter a new password and retry.

4799: Couldn't read key database password.

Cause: The server was unable to find the key database password. No password was provided, or the password syntax was incorrect.

Solution: Enter a non-null password or ensure that a valid password file, containing a valid password, is supplied.

4800: No key db password was specified.

Cause: No key database password was specified (either explicitly or via a password file.)

Solution: Supply a valid password or the path to a valid password file.

4801: Unable to read key password file from *directory*.

Cause: The server was unable to read the key database password from the password file.

Solution: Check the password file access rights and ensure that the file is of a reasonable size.

4802: Bad password file syntax: missing ":' preceding password.
   Cause: The syntax of the password file is incorrect. The colon, :, is missing.

   Solution: Supply a password file with the correct syntax.

4803: Bad token identifier: *token*.
   Cause: The token identifier in the password file does not match the open token.

   Solution: Supply a token identifier that is consistent with the nsSSLToken attribute value in the configuration.

4804: Missing security initialization required by attribute encryption.
   Cause: Security configuration has not been completed.

   Solution: Make sure certificate and key database security has been enabled, nsslapd-security: on.

4805: Failed to check whether attribute encryption is configured or not.
   Cause: An internal search for attribute encryption configuration elements failed.

   Solution: Make sure attribute encryption is properly configured, then restart Directory Server.

4807: Security Initialization: Unable to register PIN callback(error *code - message*)
   Cause: Security Initialization: Unable to register PIN callback

   Solution: NSS refused the operation: check library compatibility and requirements.

4808: Security Initialization: certificate database file name should look like 'slapd-[serverId-]cert'
   Cause: Security Initialization: badly formed certificate database name

   Solution: Check the value of the nsCertfile attribute on cn=encryption. It should be of the form nsCertfile: slapd-cert8.db.

4865: Detected virtual attribute loop in get on entry *entry* attribute *attribute*.
   Cause: A loop was detected while retrieving the virtual attributes of an entry.

   Solution: Check the virtual attributes configured for this entry and break the loop.

4866: Out of memory to duplicate a type name.
   Cause: There is insufficient memory for the server to allocate a service provider for the virtual attributes map insert.

Solution: Make more memory available to the server and restart the server.

4867: Detected virtual attribute loop in compare on entry *entry* attribute
attribute.
Cause: The server detected a virtual attribute loop when comparing virtual attribute service
providers.

Solution: Check the virtual attributes configured for this entry and break the loop.

4868: Out of memory to allocate a service provider.
Cause: There is insufficient memory for the server to allocate a service provider for the virtual
attributes register.

Solution: Make more memory available to the server and restart the server.

4869: Out of memory to allocate a service provider handle.
Cause: There is insufficient memory for the server to allocate a service provider handle.

Solution: Make more memory available to the server and restart the server.

4870: Out of memory to create a map for virtual attributes.
Cause: There is insufficient memory for the server to allocate a map for virtual attributes.

Solution: Make more memory available to the server and restart the server.

4871: Out of memory to create a new hash table.
Cause: There is insufficient memory for the server to allocate a new hash table for virtual
attributes.

Solution: Make more memory available to the server and restart the server.

4872: Failed to create a new lock for virtual attributes map insert.
Cause: The server was unable to create a new lock for virtual attribute map creation. This is
probably due to a memory error.

Solution: Make more memory available to the server and restart the server.

4994: Multiple backend instances are specified.
Cause: More than one backend instance has been specified for the attempted task.

Solution: Contact Sun Technical Support.

4995: Cannot perform an import with pre-V3 backend plugin.
Cause: You are using a version of the backend plug-in API that is no longer supported and
cannot perform the database import.

Solution: Upgrade to a newer version of the backend plug-in API (at least version 3), recompile, and add the import functionality.

4996: No ldif2db function defined for backend *backend*
Cause: No ldif2db function is defined for this backend. This kind of database is unable to perform an import.

Solution: Use a backend that has the import functionality.

4997: Unable to allocate new task for import.
Cause: The server is unable to allocated a new task for the import. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

4998: Cannot export - backend not found.
Cause: The database could not be exported because the specified backend could not be found.

Solution: Check the configuration file and make sure that the correct database and suffix are specified.

4999: ldbm2ldif: backend *backend* export failed (*error*)
Cause: The db2ldif function failed when attempting to export the database.

Solution: Refer to the error log for more information and contact Sun Technical Support.

5000: No backend instance names are specified.
Cause: The database could not be exported because no backend instance names were specified.

Solution: Contact Sun Technical Support.

5003: Cannot perform an import with pre-V3 backend plugin.
Cause: You are using a version of the backend plug-in API that is no longer supported and cannot perform the database import.

Solution: Upgrade to a newer version of the backend plug-in API (at least version 3), recompile, and add the import functionality.

5004: No ldif2db function defined for backend *backend*
Cause: No ldif2db function is defined for this backend. This kind of database is unable to perform an import.

Solution: Use a backend that has the import functionality.

5005: Unable to allocate new task.
Cause: The server is unable to allocated a new task for the export. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5006: Unable to create ldbm2ldif thread for export.
Cause: The server is unable to create a thread for the export. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5007: db2archive function failed when trying to backup (error *error*)
Cause: The db2archive function failed when attempting to backup.

Solution: Refer to the error log for more information and contact Sun Technical Support.

5008: Unable to process backup when no db2archive function defined
Cause: The database could not be backed up because the db2archive function was not defined.

Solution: None - this type of database cannot be backed up.

5009: Cannot perform a backup with pre-V3 backend plugin variable
Cause: You are using a version of the backend plug-in API that is no longer supported and cannot perform the database backup.

Solution: Upgrade to a newer version of the backend plug-in API (at least version 3), recompile, and add the backup functionality.

5010: Unable to allocate new task for backup.
Cause: The server is unable to allocated a new task for the backup. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5011: Unable to create backup thread.
Cause: The server is unable to create a backup thread. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5012: Restore failed (error *error*)
Cause: The restore process failed.

Solution: Refer to the error log for more information and contact Sun Technical Support.

5014: Cannot perform a restore with pre-V3 backend plugin variable
Cause: You are using a version of the backend plug-in API that is no longer supported and cannot perform the database restore.

Solution: Upgrade to a newer version of the backend plug-in API (at least version 3), recompile, and add the restore functionality.

5015: Unable to allocate new task for restore.
Cause: The server is unable to allocated a new task for the restore. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5016: Unable to create restore thread for restore.
Cause: The server is unable to create a restore thread. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5017: db2index function failed when trying to restore (error *error*)
Cause: The db2index function failed when attempting to restore the database.

Solution: Refer to the error log for more information and contact Sun Technical Support.

5019: No db2index function defined for backend *backend*.
Cause: The database could not be indexed because no db2index() function was defined for the backend.

Solution: Contact Sun Technical Support.

5020: Unable to allocate new task for index.
Cause: The server is unable to allocated a new task for the index. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5021: Unable to create index thread.
Cause: The server is unable to create an index thread. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5023: Cannot create task node (error *error*)
Cause: The server is unable to create a task node.

Solution: Refer to the error log for more information and contact Sun Technical Support.

5024: Unable to create global tasks lock.
Cause: The server is unable to create a global tasks lock. This is usually due to a resource problem.

Solution: Free up resources on the machine and restart the server.

5025: Cannot import. Lookup instance name by suffixes failed.
Cause: The database could not be imported because the server was unable to locate the instance name for the specified suffix.

Solution: Check that the suffix is specified correctly in the configuration.

5026: Cannot import. Could not find database for suffix.
Cause: The database could not be imported because the server was unable to locate the database for the specified suffix.

Solution: Check that the database and the suffix are specified correctly in the configuration.

5027: Cannot import. Backend not found.
Cause: The database could not be imported because the server was unable to locate the specified backend.

Solution: Check that the database and the suffix are specified correctly in the configuration.

5028: Cannot import - lookup instance names by suffix failed.
Cause: The database could not be imported due to a problem with the suffix configuration.

Solution: Check that the suffix is specified correctly in the configuration.

5029: Could not find database for suffix.
Cause: The database could not be exported because it could not be found.

Solution: Check that the database and the suffix are specified correctly in the configuration.

5030: No archive2db function defined.
Cause: The database could not be restored because the archive2db function was not defined.

Solution: None - this type of database cannot be restored.

5031: Cannot index - backend not found.
Cause: The server cannot index the database because the specified backend was not found.

Solution: Contact Sun Technical Support.

5034: Incompatible options nsExportReplica=true and dsDecryptAttrs=false:
cannot dump replica with encrypted attributes.
Cause: An export has been called with incompatible options nsExportReplica: true and
dsDecryptAttrs: false. It is not possible to dump a replica with encrypted attributes.

Solution: Avoid using both options at the same time. Ensure that attributes are decrypted,
dsDecryptAttrs: true, if you want to export the database for replication purposes.

5035: Unknown Password Compatibility task: *state*
Cause: Unknown password policy compatibility action.

Solution: Move the server to the correct compatibility state.

5036: Can not modify Password Policy compatibility state. Task aborted.
Cause: The server could not move to the specified compatibility state.

Solution: See additional information returned to the client application.

5036: Password Compatibility task and Password Policy state are incompatible.
Can not change Password Policy state.
Cause: The server could not move to the specified compatibility state.

Solution: See additional information returned to the client applicatin.

5037: Unable to allocate new task for changing password compatibility state !"
Cause: Unable to allocate new task for backup.

Solution: Make more resources available for the server and restart the server.

5038: Unable to create Password Policy compatibility task thread !
Cause: Unable to create backup thread.

Solution: Make more resources available to the server and try again.

5039: Password Policy compatibility state is already *state*. Task aborted.
Cause: Nothing to do as the action required would not change the compatibility state.

Solution: Change to a different compatibility state.

5040: `Unknown log rotate task: ` *`type`*`.`
   Cause: The server did not recognize the log type set for the log rotation attribute.

   Solution: Use a valid log type.

5041: `Unable to allocate new task for log rotation !`
   Cause: The server was unable to allocate a new task for log rotation.

   Solution: Make more system memory available by restarting the server.

5042: `Unable to create log rotation task thread!`
   Cause: The server was unable to allocate a new task for log rotation.

   Solution: Make more system memory available by restarting the server.

5121: `reslimit_init: slapi_register_object_extension() failed.`
   Cause: The server cannot register an object extension (during resource limit initialization).

   Solution: Contact Sun Technical Support.

5122: `PR_NewRWLock() failed for reslimit.`
   Cause: System error - the server cannot create a new lock for the resource limit.

   Solution: Contact Sun Technical Support.

5123: *`error`*`: Resource limit initialization failed.`
   Cause: Resource limit initialization failed. This is likely to be a resource issue.

   Solution: Check the error message in the log file and contact Sun Technical Support.

5124: *`error`*`: slapi_get_object_extension() returned NULL`
   Cause: The server could not obtain the object extension (for the resource limit).

   Solution: Contact Sun Technical Support.

5126: *`error`*`: parameter error (`*`attribute`* `already registered)`
   Cause: A parameter error occurred when registering a new resource to be tracked. The LDAP attribute type that can be consulted in the bound entry to determine the limit's value is already registered.

   Solution: Check that the attribute provided is registered only once.

5127: *`error`*`: parameter error`
   Cause: A parameter error occurred when registering a new resource to be tracked.

   Solution: Perform the following tasks:

1. Check that the type is SLAPI_RESLIMIT_TYPE_INT
2. Check that attrname is an LDAP attribute type that can be consulted in the bound entry to determine the limit's value.

5127: *error*: parameter error
Cause: Internal error. When retrieving the integer limit associated with a connection and a resource, a parameter with a NULL value was found.

Solution: Contact Sun Technical Support.

5128: error: unknown handle *handle*
Cause: Parameter error. The handle used to identify a resource is unknown.

Solution: Contact Sun Technical Support.

5129: Cannot malloc bytes.
Cause: An attempt is being made to allocate 0 or a negative number of bytes. This is likely to be a software issue.

Solution: Contact Sun Technical Support.

5130: malloc of *bytes* bytes failed; errno *error*.
Cause: Memory allocation has failed. This is probably because of a lack of available memory.

Solution: Increase the virtual memory available to your server, or reduce the size of the server's maximum entries in cache (cachesize) or maximum database cache size (dbcachesize) parameters.

5131: cannot realloc *number* bytes; trying to allocate 0 or a negative number of bytes is not portable and gives different results on different platforms. Please check the code and change it to avoid the attempt to allocate *number* bytes.
Cause: Memory reallocation of *number* bytes is not allowed.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5132: realloc of *bytes* bytes failed; errno *error*.
Cause: Memory reallocation has failed. This is probably because of a lack of available memory.

Solution: Increase the virtual memory available to your server, or reduce the size of the server's maximum entries in cache (cachesize) or maximum database cache size (dbcachesize) parameters.

5133: cannot calloc *number* bytes; trying to allocate 0 or a negative number of bytes is not portable and gives different results on different platforms. Please check the code and change it to avoid the attempt to allocate *number* bytes.
    Cause: Memory allocation of *number* bytes is not allowed.

    Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5134: cannot calloc *number* elements; trying to allocate 0 or a negative number of elements is not portable and gives different results on different platforms. Please check the code and change it to avoid the attempt to allocate *number* elements.
    Cause: Memory allocation of *number* elements is not allowed.

    Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5135: calloc of *bytes* bytes failed; errno *error*.
    Cause: Memory c-allocation has failed. This is probably because of a lack of available memory.

    Solution: Increase the virtual memory available to your server, or reduce the size of the server's maximum entries in cache (cachesize) or maximum database cache size (dbcachesize) parameters.

5136: strdup of *chars* chars failed; errno *error*.
    Cause: String duplication has failed. This is probably because of a lack of available memory.

    Solution: Increase the virtual memory available to your server, or reduce the size of the server's maximum entries in cache (cachesize) or maximum database cache size (dbcachesize) parameters.

5137: ber_bvdup of *bytes* bytes failed; errno *error*.
    Cause: BER value duplication has failed. This is probably because of a lack of available memory.

    Solution: Increase the virtual memory available to your server, or reduce the size of the server's maximum entries in cache (cachesize) or maximum database cache size (dbcachesize) parameters.

5249: The entry *entry* in the configfile *filename* was empty or could not be parsed.
    Cause: An entry in the configuration file was empty or could not be parsed.

    Solution: Check the entry syntax in the configuration file.

5250: Invalid value
Cause: The specified configuration attribute in the Directory Server configuration file has no value or the value is invalid.

Solution: Check that the value of the attribute under cn=config in the Directory Server configuration file is either on or off.

5251: Cannot set error log *filename*.
Cause: The error log filename could not be set, either because the filename was NULL or the path was invalid.

Solution: Check that the value of the attribute nsslapd-errorlog under cn=config is valid, and that the path exists.

5252: Undefined value for errorlog level.
Cause: The error log level could not be set because its value is undefined.

Solution: Check that the value of the attribute nsslapd-errorlog-level under cn=config is set, and is correct.

5253: Bad value for nsslapd-maxdescriptors.
Cause: The request to set the maximum number of file descriptors has failed. The value is either NULL, or out of the permitted range [1..*max*] where *max* is the maximum number of file descriptors that can be created by a process.

Solution: Check that the value of the attribute nsslapd-maxdescriptors in the Directory Server configuration is not higher than the RLIMIT_NOFILE parameter, and is not lower than 1.

5254: Ignoring *attribute* (since -d *option* was given on the command line) nsslapd-errorlog-level.
Cause: The attribute nsslapd-errorlog-level in the Directory Server configuration has been ignored, because the -d option was specified at the command line.

Solution: Do not specify the -d option at the command line if you want the value of this attribute in the configuration file to be taken into account.

5255: The plugin entry *entry* in the configfile *filename* was invalid.
Cause: Failed to load the specified plug-in because the configuration entry of the plug-in in the -d is invalid.

Solution: Check and correct the faulty plug-in configuration.

5256: *file*: *max_descriptors*: *error*
   Cause: The request to set the maximum number of connections failed either because the value was NULL or the value was not in the allowed range [1..*max*] where *max* is the maximum number of file descriptors a process may create.

   Solution: Check `nsslapd-maxconnections` on `cn=config` to ensure its value is not higher than the `SC_OPEN_MAX` system parameter, nor lower than 1.

5385: Convert LDIF entry into LDAP entry fast method. Error: entry has no dn.
   Cause: While attempting to convert an LDIF entry to an LDAP entry, the server found that the entry has no DN.

   Solution: Check the entry and make sure that it has a DN.

5390: str2entry_dupcheck: entry has no dn.
   Cause: While attempting to convert a string entry to an LDAP entry, the server found that the entry has no DN.

   Solution: Check the entry and make sure that it has a DN.

5392: Error occurs while removing attribute values. Possible existing duplicate value for attribute type *attribute* found in entry *entry*.
   Cause: An error occurred while attempting to remove attribute values. This may be due to a duplicate attribute value.

   Solution: Check the attribute values being removed.

5393: str2entry_dupcheck: unexpected failure constructing the value tree.
   Cause: The server failed to add a value to the value tree.

   Solution: Check the error log for more information.

5394: Error occurs while removing attribute values. Possible existing duplicate value for attribute type *type* found in entry *DN*
   Cause: The entry contains duplicate values for the attribute.

   Solution: Delete the attribute and add a new set of values.

5395: Attribute 'nscpEntryWSI' can only be computed by root user.
   Cause: The attribute nscpEntryWSI cannot be computed by a user who is not the Directory Manager.

   Solution: Check the client application making the request. The client must bind as root to be able to compute this attribute.

```
5396: Cannot compute 'nscpEntryWSI' attribute because there is no pblock in the
context
```
Cause: A required parameter block structure was not available.

Solution: Contact Sun Technical Support.

```
5397: Existing duplicate values found in attribute "type" of entry "DN"
```
Cause: The entry contains duplicate values for the attribute.

Solution: Delete the attribute and add a new set of values.

```
5398: Duplicate value addition in attribute "type" of entry "DN"
```
Cause: A client is trying to add duplicate values for the attribute.

Solution: Fix the client application.

```
5399: occurred while removing attribute values. Could not find value number for
attribute type (message).
```
Cause: Error occurs while trying to remove attribute values. The value could not be found.

Solution: Check the attribute values to remove.

```
5505: Registration of extension failed.
```
Cause: A plug-in has attempted to register a new extension to an object type, but the object type is in use, by at least one object.

Solution: Correct the plug-in code.

```
5506: Registration of extension extension by plug-in failed: number extensions
already registered (max is max_ext).
```
Cause: Directory Server tried to register too many object extensions.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

```
5507: Number of extension users for extension is negative number.
```
Cause: Directory Server encountered a negative number of object extensions.

Solution: Contact Sun Technical Support.

```
5508: Registration of type object type failed. There is no more free slot in
factory array for object type (current in use number max is number).
```
Cause: Directory Server tried to register an object type other than Connection, Operation, Entry, or Mapping Tree Node.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5509: Trying to get extension on unregistered object type (object type identifier *ID*).
Cause: Directory Server tried to extend an unregistered object type.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5510: Release extension on unregistered object type (object type identifier *ID*).
Cause: Directory Server tried to release an extension for an unregistered object type.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5511: Plugin *plug-in* tries to register extension for object type that does not exist *type*.
Cause: Directory Server tried to extend a nonexistent object type.

Solution: Unless you are developing a plug-in and broke this yourself, contact Sun Technical Support.

5635: Backend *backend* is already pointed to by another mapping tree node. Only one mapping tree node can point to a backend.
Cause: Errors exist in the mapping tree node configuration.

Solution: Check nsslapd-backend values in the mapping tree entry.

Check that the mapping tree node state has a legal value, and that nsslapd-referral is appropriately set if necessary.

5641: Could not find parent node for entry *entry*. Node parent is defaulting to root node.
Cause: The parent node for the current mapping tree node could not be located.

Solution: Check the nsslapd-parent-suffix attribute of the entry in the Directory Server configuration.

5642: Node *node* is either a 'backend' or 'referral on update' node therefore it must define a backend (attribute 'nsslapd-backend').
Cause: The new mapping tree node is either a "backend" or "referral on update" node but has no backend defined.

Solution: Check the `nsslapd-backend` attribute of the entry in the Directory Server configuration.

5643: Node *node* is either a 'referral' or 'referral on update' node therefore it must define a referral (attribute 'nsslapd-referral').
Cause: The new mapping tree node is either a "referral" or "referral on update" node but has no referral defined.

Solution: Check the `nsslapd-referral` attribute of the entry in the Directory Server configuration.

5644: Cannot load distribution plugin lib *library* for node *node*.
Cause: The distribution plug-in could not be loaded.

Solution: Check the error log for more information. The dynamic library may not be present, may be inaccessible, or may be using another library that is not present.

5645: Node *node* wants to define a distribution plugin but either 'nsslapd-distribution-plugin' or 'nsslapd-distribution-funct' attribute is missing in the configuration file (dse.ldif).
Cause: The entry is missing either the distribution plug-in or the distribution function name.

Solution: Check the values for the `nsslapd-distribution-plugin` and `nsslapd-distribution-func` attributes in the plug-in configuration entry.

5648: Could not create mapping tree node for entry *entry*.
Cause: The mapping tree node could not be created.

Solution: Check the error log for evidence of the failure, otherwise contact Sun Technical Support.

5650: Modify (add or replace) callback for mapping tree: could not find parent for mapping tree node *DN*
Cause: One of the following:

- The mapping tree parent is not a suffix of a mapping tree child.
- While modifying the CN or `nsslapd-parent-suffix`, Directory Server could not find the new parent.

Solution: If the modification originated in a client request, fix the client. Otherwise, contact Sun Technical Support.

5653: Distribution plugin returned wrong backend: backend index *index* (range
0..*max*) for entry *DN* at node DN
Cause: One of the following:

- No attribute value exists for `nsslapd-distribution-func`.
- The distribution plug-in returned a bad backend index value.

Solution: Perform the following steps:

- Check the configuration for the distribution plug-in.
- Fix the distribution plug-in.

  If neither remedy works, contact Sun Technical Support.

5654: Distribution plugin not configured for mapping tree node *DN*
Cause: Directory Server tried to use a distribution plug-in, but the distribution plug-in was
not appropriately configured.

Solution: Check the configuration for the distribution plug-in.

5659: Cannot find distribution function *function* in distribution plugin lib *library*
for node *node*.
Cause: The distribution function in the plug-in library could not be located.

Solution: Check the error log for more information. The dynamic library may not be present,
may be inaccessible, or may be using another library that is not present.

5889: Could not create lock for Schema DSE
Cause: Directory Server could not create a lock for the schema subentry.

Solution: Check that Directory Server is not having to contend for system resources with
other applications.

5890: No schema files were found in the directory *directory_name*.
Cause: No schema files are present in the schema directory.

Solution: Restore the default schema files from a backup or CD image.

5891: Could not add attribute type "objectClass" to the schema: *message*
Cause: Directory Server could not create the default `objectclass` schema definition.

Solution: Contact Sun Technical Support.

5892: Could not add attribute type "aci" to the schema: *message*
Cause: Directory Server could not create the default `aci` schema definition.

Solution: Contact Sun Technical Support.

5893: Entry *entry* required attribute *objectclass* is missing.
Cause: The specified entry was added without an `objectclass` attribute.

Solution: Check the application that added the entry.

5894: Entry *entry* has unknown objectclass.
Cause: The entry was added or modified with an unknown `objectclass`.

Solution: Check the application that added or modified the entry.

5895: Entry *entry* single-valued attribute has multiple values.
Cause: The entry that was added or modified is invalid. A single-valued attribute has multiple values.

Solution: Check the application that added or modified the entry.

5896: Entry *entry* attribute *attribute* required by objectclass *objectclass* is missing.
Cause: The entry that was added or modified is missing a required attribute.

Solution: Check the application that added or modified the entry.

5897: Entry *entry* attribute *attribute* is not allowed.
Cause: The entry that was added or modified contains an invalid attribute.

Solution: Check the application that added or modified the entry.

5898: No attribute types to iterate through internally
Cause: Directory Server got an empty attribute type list.

Solution: Contact Sun Technical Support.

5899: No OID found in schema for syntax *syntax*
Cause: Directory Server could not match the OID with any OID in the schema.

Solution: Fix the schema, or the client. If neither fix solves the problem, contact Sun Technical Support.

5900: Missing value for objectClasses attribute.
Cause: While parsing the schema LDIF file, no value was specified for the `objectClasses` attribute.

Solution: Check the schema LDIF file or the schema modification request.

5901: No name or OID specified for checking schema
    Cause: Internal error

    Solution: Contact Sun Technical Support.

5906: Value has invalid syntax (not *syntax*): *attr=value*
    Cause: Entry was added or modified with invalid attribute syntax.

    Solution: Check application that added or modified the entry.

8194: Replication session aborted for agreement *agreement_name* because consumer
replica is disabled.
    Cause: The consumer has returned a disabled error, that is, it is not in a state in which it can
    receive replication updates.

    Solution: Enable the consumer replica. It may also be necessary to initialize the consumer
    again.

8195: Pending changes: error *value*.
    Cause: Looping through the changelog failed.

    Solution: Ensure that replication is working correctly (using the insync utility and checking
    the replication agreement object).

    Check the error code in the error log for more information.

8196: Bad Window size value for agreement *agreement_name*.
    Cause: The value of the ds5ReplicaTransportWindowSize attribute is invalid.

    Solution: Check the Directory Server configuration defining the Replication Agreement.

    Solution: Check the modification operation attempted on the replication agreement.

8197: Bad Group size value for agreement *agreement_name*.
    Cause: The value of the ds5ReplicaTransportGroupSize attribute is invalid.

    Solution: Check the Directory Server configuration defining the Replication Agreement.

    Solution: Check the modifications attempted on the replication agreement.

8198: Bad Compression Level value for agreement *agreement_name*.
    Cause: The value of the ds5ReplicaTransportCompressionLevel attribute is invalid.

    Solution: Check the Directory Server configuration defining the Replication Agreement.

    Solution: Check the modifications attempted on the replication agreement.

8199: Modification of *attribute_name* `attribute is not allowed - agreement`
agreement_name.
   Cause: The user is not permitted to modify the specified replication agreement attribute.

   Solution: Check the Directory Server configuration defining the Replication Agreement.

   Solution: Check the modifications attempted on the replication agreement.

8200: Failed to update flag to force 5.1 Replication protocol for agreement
agreement_name.
   Cause: The replication agreement is being stopped.

   Solution: Wait until the agreement has been stopped and retry.

8201: Failed to update the state (enable/disable) of the agreement *agreement*
   Cause: Replication is stopping for this agreement.

   Solution: Wait until the agreement has stopped and try again.

8202: Unknown replication agreement
   Cause: A replication agreement with the specified DN could not be found.

   Solution: Check the specified DN and all replication agreements.

   Solution: Check that the error is not in the client application.

8203: Failed to update partial replication checksum for agreement *agreement*
   Cause: One of the following:

   1. The checksum value provided for partial replication was not valid.
   2. Replication is stopping for this agreement.

   Solution: Wait until the agreement has stopped and try again.

8204: Refusing to update partial replication checksum for agreement
agreement_name permission denied.
   Cause: The server received an update operation that is permitted for internal operations only.

   Solution: Check the client that sent the forbidden update operation.

8205: Failed to update Bind Method for agreement *agreement*
   Cause: The replication agreement is stopping.

   Solution: Wait until the agreement has stopped and try again.

8206: Failed to update Transport Information for agreement *agreement*
Cause: The replication agreement is stopping.

Solution: Wait until the agreement has stopped and try again.

8207: Failed to update Bind DN for agreement *agreement*
Cause: The replication agreement is stopping.

Solution: Wait until the agreement has stopped and try again.

8208: Failed to update TimeOut value for agreement *agreement*
Cause: One of the following:

1. A client attempted to set an invalid attribute type or value.
2. Replication is stopping for this agreement.

Solution: Perform the following steps:

1. Check the client application.
2. Wait until the agreement has stopped and try again.

8209: Failed to update Credentials for agreement *agreement*
Cause: One of the following:

1. A client attempted to set an invalid attribute type or value.
2. Replication is stopping for this agreement.

Solution: Perform the following steps:

1. Check the client application.
2. Wait until the agreement has stopped and try again.

8210: No value supplied for attr *attribute*
Cause: No value was supplied for the specified attribute.

Solution: Perform the following steps:

1. Check the client application.
2. Wait until the agreement has stopped and try again.

8211: Invalid value *value* supplied for attr *attribute*
Cause: The value supplied for the specified attribute is not a valid value.

Solution: Perform the following steps:

1. Check the client application.
2. Wait until the agreement has stopped and try again.

8212: Failed to update replication schedule for agreement *agreement_name*.
Cause: One of the following:

1. The replication schedule format is invalid.
2. The replication agreement is stopping.

Solution: Perform the following steps:

1. Check the client application.
2. Wait until the agreement has stopped and try again.

8213: Failed to update Partial Replication Configuration for agreement
agreement_name. The agreement needs to be disabled first.
Cause: An attempt was made to change the configuration for partial replication, on an enabled replication agreement

Solution: To change the partial replication configuration, disable the replication agreement first.

8215: Partial replication not started for agreement *agreement_name*.
Cause: Partial replication has not been started.

Solution: Check the configuration of this replication agreement (specifically partial configuration entries). Start the partial replication feature for this agreement in Directory Service Control Center.

8216: Partial replication pointed to by this *entry* has been modified. Please
update the current configuration on this supplier or re-initialize consumer
accordingly.
Cause: The partial replication configuration has been modified.

Solution: Update the current configuration on the supplier, or initialize the consumer again.

8218: Replication protocol v5.0 not supported for *consumer*.
Cause: The version 5 replication protocol is not supported for this consumer.

Solution: Check the version of Directory Server running on the specified consumer.

8219: Could not parse update vector for replica *replica_name*. The replica must be
reinitialized.
Cause: The server was unable to parse the update vector for the specified replica.

Solution: Check that the consumer sent the replica update vector (RUV) during the start request.

8220: Too much time skew between replicas for [*consumer*:*port*]
Cause: The time difference between the specified replicas is too great for replication to work correctly.

Solution: Ensure that the supplier and consumer machines have the same time and date. The use of the Network Time Protocol (NTP) is recommended.

8221: Failed and requires administrator action.
Cause: A fatal error occurred during an incremental update. Replication on this consumer will be disabled.

Solution: Check the error log on the consumer for more information. Restart replication by updating the replication agreement and reinitializing updates.

8222: search_in_ruv_storage_entry: replica ruv tombstone entry for replica *DN* not found
Cause: Directory Server could not read the replication update vector storage entry in the database for the suffix.

Solution: Initialize replication for the suffix again.

8223: Invalid value *value* supplied for attr *attribute*
Cause: The value supplied for the specified attribute is not a valid value.

Solution: Perform the following steps:

1. Check the client application.
2. Wait until the agreement has stopped and try again.

8225: Replica_write_partial_repl_checksum: failed to update partial repl checksum with value *value* for replica *replica*. LDAP error.
Cause: An error occurred while writing an attribute value in the replica entry.

Although harmless while the server is up and running, this error may lead to a replication malfunction the next time the server is restarted.

The error occurs when the value of an important replication configuration attribute cannot be stored persistently in the Directory Server configuration.

Solution: Stop the server immediately and check the cn=replica entry for this suffix in the Directory Server configuration. If the attribute dsfilterspconfigchecksum is present in the entry, set its value to the value included in the error log. If the attribute dsfilterspconfigchecksum is not present in the entry, add it and set its value to the value included in the error log. Restart the server.

8226: `replica_write_last_init_time: failed to update last init timestamp with value` *value* `for replica` *replica*`. LDAP error.`
Cause: An error occurred while writing an attribute value in the replica entry.

Although harmless while the server is up and running, this error may lead to a replication malfunction the next time the server is restarted.

The error occurs when the value of an important replication configuration attribute cannot be stored persistently in the Directory Server configuration.

Solution: Stop the server immediately and check the `cn=replica` entry for this suffix in the Directory Server configuration. If the attribute `lastInitTimeStamp` is present in the entry, set its value to the value included in the error log. If the attribute `lastInitTimeStamp` is not present in the entry, add it and set its value to the value included in the error log. Restart the server.

8227: `Unable to read user schema.`
Cause: The server was unable to access to its own internal schema entry.

Solution: Stop and restart the server. If this does not solve the problem, contact Sun Technical Support.

8228: `Bind error for agreement:` *.agreement*`.`
Cause: A replication protocol bind error has occurred.

Solution: Check that the consumer is up and running.

8229: `Failed to start a total update session.`
Cause: The server was unable to start a total replication update session.

Solution: Check that the consumer is up and running.

8230: `Failed to create directory for changelog` *changelog* `error` *error*`.`
Cause: The pathname is invalid, or there is unsufficient access to create the changelog directory.

Solution: Check that the path is valid and that there are sufficient access rights to create the directory.

8232: `Removal of changelog file` *filename* `failed.`
Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8234: Changelog is not initialized.
Cause: The changelog is not initialized, or an attempt has been made to configure the changelog cleanup parameters, when the changelog service is not started.

Solution: Ensure that the changelog service has been enabled.

8235: Failed to initialize the changelog *resource*, error *ID*
Cause: Directory Server could not initialize a critical resource.

Solution: Check that Directory Server is not having to contend for system resources with other applications.

Restart Directory Server.

8236: Failed to open changelog.
Cause: This is probably due to a database or file access problem.

Solution: Enable the replication logs and retry the operation to see if additional reasons are output to the error log.

8237: Changelog is in invalid state (*state* instead of *state*)
Cause: The changelog service has not stopped as expected.

Solution: Restart Directory Server.

8238: Failed to start changelog monitoring threads (*error*)
Cause: Directory Server could not start threads needed to manage the changelog.

Solution: Check that sufficient threads are available, and that Directory Server is not having to contend for system resources with other applications.

8239: Removal of changelog file *filename* failed, file not removed
Cause: Directory Server could not delete the file.

Solution: Restart Directory Server.

8240: allocation failed while converting entry to data (size *size*)
Cause: Directory Server could not allocate enough memory to convert a changelog entry to data.

Solution: Check that sufficient memory is available to Directory Server.

Restart Directory Server if it stops.

8241: Change record has an invalid data version
Cause: A change record in the database has an invalid version number.

Solution: Perform the following steps:

1. Disable and re-enable replication for this database.
2. Initialize the server again.
3. Contact Sun Technical Support.

8242: Change record has an invalid operation type.
Cause: There is an invalid change record in the changelog.

Solution: Ordinarily, this error should not occur. If it does, the changelog is likely to be corrupted. In this case, reset the changelog for this database by reloading the data or disabling/enabling replication. If this does not solve the problem, contact Sun Technical Support.

8243: Failed to begin transaction for trimming DB error.
Cause: A database error occurred while the transaction was starting. This is likely to be a resource problem.

Solution: Check the database error and take action based on the error code. Directory Server uses Sleepycat Software's Berkeley DB.

8244: Failed to abort transaction for trimming DB error.
Cause: A database error occurred while the transaction was being aborted. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8245: Failed to commit transaction for trimming DB error.
Cause: A database error occurred while the transaction was being committed. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8246: Failed to begin transaction for writing changelog *changelog* RUV DB error.
Cause: A database error occurred while the transaction was starting. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8247: Failed to abort transaction for writing changelog *changelog* RUV DB error.
Cause: A database error occurred. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8248: Failed to commit transaction for writing changelog *changelog* RUV DB error.
Cause: A database error occurred while the transaction was being aborted. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8249: Writing the changelog *changelog* RUV in the file *filename* failed DB error.
Cause: A database error occurred while the transaction was being committed. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8250: Failed to begin transaction for writing change count entry DB error.
Cause: A database error occurred. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8251: Failed to abort transaction for writing change count entry DB error.
Cause: A database error occurred. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8252: Failed to commit transaction for writing change count entry DB error.
Cause: A database error occurred. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8253: Failed to write change count entry to the file *filename* DB error.
Cause: A database error occurred. This is likely to be a resource problem.

Solution: Check the corresponding database error code, and take action according to the database problem.

8254: allocation failed while converting change to ldif (size *size*)
Cause: Directory Server could not allocate enough memory to convert a change record to LDIF.

Solution: Check that sufficient memory is available to Directory Server.

Restart Directory Server if it stops.

8255: Change record from LDIF has an invalid data format. Record rejected
Cause: Directory Server encountered invalid data while loading a changelog record from LDIF.

Solution: Check that the LDIF file is valid.

8256: Failed to begin transaction for writing change operation DB error.
Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8257: Failed to abort transaction for writing change operation DB error.
Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8258: Failed to commit transaction for writing change operation DB error.
Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8259: Failed to write change operation with CSN *number*. DB error.
Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8260: Failed to create cursor for retrieving first change DB error.
Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8261: Failed to retrieve first change DB error.
  Cause: A database error occurred.

  Solution: Check the corresponding database error code, and take action according to the database problem.

8262: Failed to retrieve the next change DB error.
  Cause: A database error occurred.

  Solution: Check the corresponding database error code, and take action according to the database problem.

8263: Failed to delete the current change DB error.
  Cause: A database error occurred.

  Solution: Check the corresponding database error code, and take action according to the database problem.

8264: Failed to position in db at CSN *number*. DB error.
  Cause: A database error occurred.

  Solution: Check the corresponding database error code, and take action according to the database problem.

8265: allocation failed while creating changelog file for replica *replica*
  Cause: Directory Server could not allocate enough memory to create the changelog file.

  Solution: Check that sufficient memory is available to Directory Server.

  Restart Directory Server if it stops.

8266: Failed to open changelog file for replica *replica*. DB error.
  Cause: An internal database error occurred.

  Solution: Check the corresponding database error code, and take action according to the database problem.

8267: Failed to retrieve change count from changelog for replica *replica*.
  Cause: The server was unable to retrieve the number of entries in the changelog.

  Solution: Enable replication logging and check the specific replication error code for more information.

8268: Failed to close changelog file *filename*. DB error.
  Cause: A database error occurred.

Solution: Check the corresponding database error code, and take action according to the database problem.

8269: Failed to write content of changelog file *filename* to ldif file
Cause: Directory Server failed to export the changelog.

Solution: Check disk space, then check the file system.

8270: Failed to retrieve change from changelog file *filename* while exporting to ldif error *code*
Cause: Internal error

Solution: Contact Sun Technical Support.

8271: Consumer replica *replica_name* has an invalid RUV.
Cause: The replication update vector returned by the consumer could not be parsed or caused a problem.

Solution: Check the consumer configuration. It may be necessary to initialize the consumer again.

8272: Replication session aborted for agreement *agreement_name* because consumer replica is disabled.
Cause: The consumer returned a disabled error, that is, it is not in a state to receive replication updates.

Solution: Enable the consumer replica. It may also be necessary to initialize the consumer again.

8276: Failed to start Replication Session for suffix *suffix_name*.
Cause: The replica is still being configured. The replication session cannot be accepted yet.

Solution: Wait until the configuration is complete and restart replication on the supplier.

8277: Failed to start Replication Session for suffix *suffix_name*.
Cause: The replication session cannot be accepted because no replica has been defined for the suffix.

Solution: Check that the supplier replication agreement is correct. Enable replication on the consumer.

8278: Failed to start Replication Session for suffix *suffix_name*.
Cause: The consumer is configured as a legacy replica and can therefore not accept multimaster replication.

Solution: Correct the replication topology.

8279: Failed to start Replication Session for suffix *suffix_name*.
Cause: The consumer is denying the right to replicate

Solution: Check that the replication identity is properly defined and matches the one that the supplier is using.

8280: Failed to start Replication Session for suffix *suffix_name*.
Cause: Internal error

Solution: Contact Sun Technical Support.

8281: Failed to start Replication Session for suffix *suffix_name*.
Cause: The consumer is not yet initialized and can therefore not accept changes.

Solution: Initialize the consumer, either online or offline.

8282: Failed to start Replication Session for suffix *suffix_name*.
Cause: The consumer appears to have the same replica ID as the supplier (both are masters).

Solution: Disable and re-enable replication, providing a different replica ID for one of the servers.

8283: Failed to start Replication Session for suffix *suffix_name*.
Cause: The consumer replica is already busy with a replication session.

Solution: Wait and try later. If this error persists, restart the server.

8284: Failed to start Replication Session for suffix *suffix_name*.
Cause: The consumer server is a master and can therefore not accept a partial replica.

Solution: Make the consumer a read-only server, or eliminate partial replication configuration in the replication agreement.

8285: Failed to start Replication Session for suffix *suffix_name*.
Cause: Directory Server encountered an invalid mapping tree state.

Solution: Check the mapping tree state.

8286: Abort Replication Session for suffix *suffix_name*.
Cause: Directory Server encountered a replication protocol violation.

Solution: Take action based on the full error message.

If necessary, contact Sun Technical Support.

8287: Bad Group Packet size value for agreement *agreement_name*.
Cause: The value of the attribute ds5ReplicaTransportGrpPktSize is invalid.

Solution: Check the Directory Server configuration defining the replication agreement.

Solution: Check the modifications attempted on the replication agreement.

8288: Bad Concurrency Level value for agreement *agreement_name*.
Cause: Value of attribute ds5ReplicaTransportConcurrencyLevel is invalid.

Solution: Check the Directory Server configuration defining the replication agreement.

Solution: Check the modifications attempted on the replication agreement.

8292: Total update of a consumer *consumer* with an empty database is not allowed.
Cause: Consumer initialization has been requested but the supplier database is empty.

Solution: Load data onto the supplier before attempting to initialize the consumer with that supplier.

8293: A fatal problem occurred on the consumer side: *consumer* with error *error*.
Cause: A fatal problem has occurred on the remote consumer.

Solution: Check the error log on the consumer for more information. Once the problem has been solved, you will need to update the replication agreement and initiate updates again.

8294: _cl5TrimFile: Removing changelog file **filename** as it belongs to an unexisting replica.
Cause: The changelog file contains data changes from a replica whose configuration has been removed.

Solution: No action is necessary - this is an informational message.

8296: [S] Unable to start a replication session with MODDN enabled. The consumer *name* does not support MODDN operations.
Cause: The modify DN must be supported by all servers in the replication topology in order for it to be used.

Solution: Upgrade the consumer server or do not activate the modify DN operation.

8297: [C] Start replication request: Unknown tag while decoding *tag*
Cause: An incorrectly encoded request caused a protocol error.

Solution: Contact Sun Technical Support.

8298: [C] Start replication request, failed to decode end of sequence
   Cause: An incorrectly encoded request caused a protocol error.

   Solution: Contact Sun Technical Support.

8299: Internal Error: [C] while decoding optional csn (partial or medium consistency replication)
   Cause: An incorrectly encoded request caused a protocol error.

   Solution: Contact Sun Technical Support.

8300: Internal Error: [C] while parsing optional CSN *CSN*
   Cause: An incorrectly encoded request caused a protocol error.

   Solution: Contact Sun Technical Support.

8301: Protocol Error: [C] while decoding optional csn, bad end of sequence
   Cause: An incorrectly encoded request caused a protocol error.

   Solution: Contact Sun Technical Support.

8302: Decoding replicate entry failed.
   Cause: A protocol error occurred. The entry was incorrectly encoded.

   Solution: Check the error code and contact Sun Technical Support.

8303: Failed with error code *error*.
   Cause: Schema replication failed locally on the consumer.

   Solution: Check error code and contact Sun Technical Support.

8304: Protocol Error: [C] Decoding replication control request failed
   Cause: An incorrectly encoded request caused a protocol error.

   Solution: Contact Sun Technical Support.

8305: Protocol Error: [C] Decoding replication control request failed to get control type
   Cause: An incorrectly encoded request caused a protocol error.

   Solution: Contact Sun Technical Support.

8306: Protocol Error: [C] Decoding database entries request failed
   Cause: An incorrectly encoded entry caused a protocol error.

   Solution: Contact Sun Technical Support.

8307: Failed to import database entry.
Cause: An internal error occurred while adding an entry to the import queue, or while acknowledging the entry to the supplier.

Solution: Check the error log for a disk space problem and initialize the database again. If the problem persists, contact Sun Technical Support.

8308: Invalid change_operation: entry_UUID *entry* CSN *CSN_value*.
Cause: A badly formed change was received.

Solution: Contact Sun Technical Support.

8309: [C] Pblock allocation failed while decoding replay changes request for *operation-code* operation on DN *DN*
Cause: The server could not allocate sufficient memory to complete the operation.

Solution: Make sure enough memory is available, and then restart the server.

8310: Protocol error: [C] Detected unsupported operation (*operation*) in replay changes request
Cause: The server received an operation that is not supported for this version.

Solution: Make sure that the servers in your replication topology use compatible versions of the replication protocol. You may be running a legacy version of the server that uses an outdated version of the replication protocol.

8311: Unexpected operation sequence number *value* (expecting *value*).
Cause: An internal error occurred in the sequencing of replicated operations.

Solution: Contact Sun Technical Support.

8312: Replay of pending changes failed returning.
Cause: The replicated change could not be applied on this consumer.

Solution: Check the error code. A delete operation may generate a return code of 32 - this error code is harmless (a dependency of changes between several masters).

If the error persists, contact Sun Technical Support.

8313: Internal Error: [C] Decoding of group of changes failed, returning *error-code*
Cause: An incorrectly encoded group of replication changes caused a protocol error.

Solution: Contact Sun Technical Support.

8314: Protocol error received a response instead of a request
Cause: A response was received when a request was expected.

Solution: Contact Sun Technical Support.

8315: [C] Failed to add op *op_num* csn *CSN* to the pending list (err=*code*)
Cause: One of the following:

- The configuration on the consumer is invalid.
- The consumer is not initialized.
- An attempt was made to write to a read-only replica.
- The change involved has already been applied.

Solution: Verify that the replica is of the proper type.

Solution: Check the configuration on the consumer replica. Initialize the consumer if necessary.

8318: [S] Bind failed with response: *error_code*.
Cause: Authentication failed. This may be due to an invalid host and port combination, an invalid identity, or the fact that the consumer is down.

Solution: Check the error code and fix the replication agreement. It may be necessary to restart the consumer.

8319: [S] Start Failed with response: *error_code*.
Cause: Replication was unable to start. This is likely to be caused by an error in the replication configuration.

Solution: Check the error log for more information. Also check the error logs on the consumers.

8320: [S] End Failed with response: *error_code*.
Cause: Replication was unable to end. This may be because a network outage has occurred, the consumer is down, or the consumer has already dropped the connection.

Solution: Check the error log for more information. Also check the error logs on the consumers.

8321: Failed to close old changelog file *file-name* DB error *error-code - error-message*
Cause: A database error occurred.

Solution: Depending on the database error specified, you may need to initialize the replica.

8322: DB error *error-code* - *error-message*
Cause: A database error occurred.

Solution: Depending on the database error specified, you may need to initialize the replica.

8323: DB error *error-code* - *error-message*
Cause: A database error occurred.

Solution: Depending on the database error specified, you may need to initialize the replica.

8324: [C] Consumer has decided to prioritize a total update regarding
incremental sessions
Cause: An initialization request has priority over other replication sessions.

Solution: None.

8325: replica_write_partial_repl_checksum: failed to update partial repl
checksum with value (*value*) (*error-message* LDAP error - *error-code*)
Cause: The server encountered a problem writing an attribute value inside the replica entry.

Solution: Although possibly harmless while the server is up and running, this might become a
serious error that could lead to a break in replication next time the server is restarted. This is
because the value of an important replication configuration attribute could not be stored
persistently in the Directory Server configuration. To try to work around this issue, stop the
server immediately and check the cn=replica entry for this suffix found in the Directory
Server configuration file. If the attribute dsfilterspconfigchecksum is already present in
the entry, then use the value included in the errors log. If dsfilterspconfigchecksum is not
present yet in the entry, use the value suggested in the errors log. Then restart the server.

8326: replica_write_partial_repl_checksum: failed to update last init timestamp
with value (*value*) (*error-message* LDAP error - *error-code*)
Cause: The server encountered a problem writing an attribute value inside the replica entry.

Solution: Although possibly harmless while the server is up and running, this might become a
serious error that could lead to a break in replication next time the server is restarted. This is
because the value of an important replication configuration attribute could not be stored
persistently in the Directory Server configuration. To try to work around this issue, stop the
server immediately and check the cn=replica entry for this suffix found in the Directory
Server configuration file. If the attribute dsfilterspconfigchecksum is already present in
the entry, then use the value included in the errors log. If dsfilterspconfigchecksum is not
present yet in the entry, then use the value suggested in the errors log. Then restart the
server.

8327: Changelog directory *error-code* could not be created
Cause: The server could not create the replication changelog directory on the file system.

Solution: Check that the server user has permission to create directories under the *instance-path*.

8328: invalid priority rule : *error-message*
Cause: The prioritized replication configuration is not valid.

Solution: Make sure you specify a valid replication priority as explained in the error message.

8328: Cannot Delete priority rule : *error-message*
Cause: The prioritized replication value could not be deleted.

Solution: Make sure you specify a valid replication priority as explained in the error message.

8329: Ignored invalid priority rule : *error-message*
Cause: The prioritized replication configuration is not valid.

Solution: Make sure you specify a valid replication priority as explained in the error message.

8330: Failed to write change operation with CSN *CSN* to database DB error
error-code - *error-message*
Cause: The server could not write to the replication changelog database.

Solution: Check the file system permissions and restart the server.

8331: Unable to demote a hub to a read-only replica if some replication
agreements are enabled
Cause: The server could not be demoted to a dedicated consumer role.

Solution: First eliminate the replication agreements that call for updates from the hub.

12289: PR_Accept() failed error variable (*variable*)
Cause: The problem depends on the *variable* and is based on the Netscape Portable Runtime (NSPR) error (http://www.mozilla.org/projects/nspr/reference/html/prerr.html) layer.

Solution: If you determine that the cause of the problem is that the TCP port to which you are attempting to bind is already in use, consider the following actions.

- Restart the server, using a different port.
- Stop the application bound to that port and restart the server.

12290: PR_GetIPNodeByName(*variable*) failed errno *error* (*message*)
Cause: There is an error in the naming service configuration.

Solution: Add listen host (*variable*) to the naming service.

12291: No port to listen on.
Cause: The LDAP port is missing from the configuration.

Solution: Add an LDAP port to the configuration file or use the command line.

12292: Unable to create time thread (variable - variable) - shutting down.
Cause: System error, probably due to a resource problem.

Solution: Free up resources on the machine and restart the server.

12293: Too many open file descriptors - not listening on new connection.
Cause: There is an error in the configuration file. See the reservedfd attribute.

Solution: Increase the maximum number of file descriptors (in the configuration file) by increasing the value of nsslapd-maxdescriptors. Otherwise, check the Directory Server configuration and reduce the resource usage (number of threads, and number of backends, for example.)

12294: Not enough descriptors to accept any additional connections.
Cause: There are insufficient file descriptors to accept new connections. This may be because:

1. the value of the maxdescriptors attribute is too small
2. the hard limit on descriptors is too small
3. the value of the reservedescriptors attribute is too large

Solution: Increase the number of file descriptors available to the slapd process.

The error log displays the number of file descriptors currently available to the slapd process, and the number of descriptors reserved for internal slapd use. The total number of file descriptors available to the process must be greater than variable

12295: Cannot initialize lock. The server is terminating
Cause: Probably due to a resource problem on the system.

Solution: Restart Directory Server.

12296: Cannot create lock. The server is terminating.
Cause: Probably due to a resource problem on the system.

Solution: Restart Directory Server.

12297: Cannot create condvar. The server is terminating.
Cause: Probably due to a resource problem on the system.

Solution: Restart Directory Server.

12298: PR_SetNetAddr(PR_IpAddrAny) failed errno *error*
   Cause: Internal error.

   Solution: Contact Sun Technical Support.

12299: PR_EnumerateHostEnt() failed.
   Cause: There is an error in the naming service configuration.

   Solution: Add the listen host variable to the naming service. Refer to your operating
   system documentation for more information.

12300: gethostname *host* failed error *error* (variable).
   Cause: There is an error in the naming service configuration.

   Solution: Add the listen host variable to the naming service. Refer to your operating
   system documentation for more information.

12301: NSS Initialization failed.
   Cause: The server was unable to initialize the security library.

   Solution: Contact Sun Technical Support.

12302: Shutting down due to possible conflicts with other slapd processes.
   Cause: More than one Directory Server is running.

   Solution: Stop Directory Servers that should not be running.

12304: Shutting down due to inability to find user in system account database.
   Cause: The server was unable to locate the specified user in the system account database.

   Solution: Add the user to the system account database and restart the server.

12308: ber encoding failed.
   Cause: This is an internal error, most likely to be related to a memory allocation problem.

   Solution: Increase the virtual memory of the machine and restart Directory Server.

12318: Call to _base64Decode fails.
   Cause: An error occurred during the base64 encoding of a value. This is an internal error
   with no specific cause. It may be due to a resource problem.

   Solution: Report the error to your administrator.

12319: connection_push_back_data has failed.
   Cause: The request has been aborted due to an internal error.

   Solution: Please contact Sun Technical Support.

12320: Invalid arguments: entry.
   Cause: Configuration error. The server failed to obtain the frontend configuration entry.

   Solution: Correct the frontend configuration entry and restart the server.

12321: Failure during frontend sanity check.
   Cause: Configuration error. The server failed the front end sanity check.

   Solution: Correct the front end declaration and restart the server.

12322: Start parse of DSML operation fails, operation aborted.
   Cause: Internal error occurred during the call to DsmlParser_startParse(). This error has no specific cause but may be related to a resource problem.

   Solution: Report the error to your administrator.

12323: Could not store worker context in Batch operation.
   Cause: This is an internal error with no specific cause. It may be related to a resource problem.

   Solution: Report the error to your administrator.

12324: Can't register HTTP port *port*.
   Cause: Internal error. The server failed to register the HTTP port.

   Solution: Check that the specified port is not currently in use and restart the server.

12325: Can't register HTTPS port *port*.
   Cause: Internal error. The server failed to register the HTTPS port.

   Solution: Check that the specified port is not currently in use and restart the server.

12326: Max size *value* of parser pool is lower than current size *value*.
   Cause: Configuration error: the maximum size of the parser pool is lower than the current size.

   Solution: In the Directory Server configuration, check that the value of the ds-hdsml-poolsize attribute is lower than the value of the ds-hdsml-maxpoolsize attribute.

12327: Cannot create XMLCh to UTF8 Transcoder.
Cause: An error occurred while trying to create an instance of a UTF8 transcoder. This is an internal error with no specific cause. It may be related to a resource problem.

Solution: Report the error to your administrator.

12328: Can't initialize DSML Worker.
Cause: Internal error. The server failed during the initialization of the DSML worker.

Solution: Please contact Sun Technical Support.

12329: Extra datacopy failed.
Cause: A request has not been processed due to a connection closure.

Solution: Check the connection and retry.

12330: Operation Key creation for HTTP context failed.
Cause: An internal memory management error has occurred.

Solution: Please contact Sun Technical Support.

12332: HTTP/DSML frontend initialization failed.
Cause: Initialization error. The server failed to set the plug-in functions.

Solution: Correct the front end configuration and restart the server.

12333: HTTP frontend instance creation failed.
Cause: Internal error. The server failed to instantiate the front end plug-in.

Solution: Please contact Sun Technical Support.

12334: Unknown internal error has been raised.
Cause: Unknown internal error.

Solution: Please contact Sun Technical Support.

12335: Error with config attribute *attribute*.
Cause: Configuration error. A configuration attribute is invalid.

Solution: Correct the specified attribute and restart the server.

12336: Invalid attribute syntax.
Cause: Configuration error. The syntax of a configuration attribute is invalid.

Solution: Correct the syntax of the specified attribute and restart the server.

12337: System I/O error.
Cause: Internal I/O error.

Solution: Please contact Sun Technical Support.

12338: Memory allocation error.
Cause: System error, probably due to insufficient resources (lack of memory).

Solution: Please contact Sun Technical Support.

12339: Memory usage error.
Cause: Memory management system error.

Solution: Please contact Sun Technical Support.

12340: DSML schema location is not defined.
Cause: Configuration error: DSML schema location is not defined. Under normal circumstances, the default value of the DSML schema location is hard coded. However, this default value can be overridden in the Directory Server configuration.

Solution: Correct the value of the `ds-hdsml-schemalocation` attribute in the Directory Server configuration, or remove this attribute from the Directory Server configuration.

12341: DSML schema URN is not defined.
Cause: Configuration error: DSML schema URN is not defined. Under normal circumstances, the default value of the DSML schema URN is hard coded. However, this default value can be overridden in the Directory Server configuration.

Solution: Correct the value of the `ds-hdsml-urn` attribute in the Directory Server configuration, or remove this attribute from the Directory Server configuration.

12342: SOAP schema location is not defined.
Cause: Configuration error. Under normal circumstances, the default value of the SOAP schema location is hard coded. If this error occurs, there is an internal problem.

Solution: Report the error to your administrator.

12343: SOAP schema URN is not defined.
Cause: Configuration error. Under normal circumstances, the default value of the SOAP schema URN is hard coded. If this error occurs, there is an internal problem.

Solution: Report the error to your administrator.

12344: Lock for concurrent access to _freeList does not exist.
Cause: Internal error: a lock for concurrent access to the specified list is missing. The lock should have been defined previously.

Solution: Report the error to your administrator.

12345: No more parser in the pool, operation aborted.
Cause: Internal error that occurs when the pool of parsers is empty and cannot be extended (all the parsers are in use).

Solution: Increase the value of the maximum pool size, specified by the ds-hdsml-poolmaxsize attribute in the Directory Server configuration.

12346: Bad Dsml request - *SOAP fault code*.
Cause: An error occurred during the call to DsmlParser_getNextRequest.

Solution: None - a SOAP fault is returned to the client with the reason for the failure.

12347: Error with secure identity method.
Cause: Configuration error. The secure identity method configuration parameter is invalid.

Solution: Correct this parameter and restart the server. Possible values for the secure identity method parameter are:

clientCertOnly clientCertFirst httpBasicOnly

12348: Exception raised when calling XMLString::transcode.
Cause: An exception was raised when calling XMLString::transcode. This is an internal error with no specific cause. It may be due to a resource issue.

Solution: Report the error to your administrator.

12352: Bad Dsml request - *SOAP error message*.
Cause: A SOAP/DSML error occurred during a call to DSMLParser_startParse().

Solution: None - a SOAP/DSML error message is returned to the client with the reason for the failure.

12353: Parse of fake request fails *error*.
Cause: This error occurs when a bad request is submitted to the parser. It should not occur in the case of the valid fake request. The DSML/SOAP schema URN and/or location may be invalid.

Solution: Check the error log for more information. If the schema URN and/or location are invalid, check the following attributes in the Directory Server configuration: `ds-hdsml-dsmlurn`, `ds-hdsml-dsmlschemalocation`.

12354: `Parse of fake request fails.`
Cause: This error occurs when a bad request is submitted to the parser. It should not occur in the case of the valid fake request. Cause unknown.

Solution: Please contact Sun Technical Support.

12355: `The XML schema file` *filename* `is missing.`
Cause: Configuration error: an XML schema is missing.

Solution: Insert the missing schema in the specified location and restart the server.

12356: `SOAPAction header is missing.`
Cause: The client must provide a `SOAPAction` header. If it is absent, the request is rejected.

Solution: Provide a `SOAPAction` header, the contents of which may be set to any value (including an empty value).

12362: `PR_Bind() on address` *host* `port` *port* `failed.`
Cause: It is likely that the port number configured for this server requires that the server be run as root.

Solution: Restart the server using a port that does not required root access or start the server as a user with root access.

12363: `Inconsistency: security is 'off' while there are attributes configured to be encrypted.`
Cause: Some attributes are configured to be encrypted, and attribute encryption requires that security be on. Yet Directory Server was started with security turned off.

Solution: Before performing any operation dealing with the encrypted attributes, switch security on, make sure certificate and key databases, certificate names, token name and token names are configured appropriately, and then restart Directory Server.

20490: `Database recovery process FAILED. The database is not recoverable.`
Cause: Database recovery has failed.

Solution: This is a serious database error. Please contact Sun Technical Support.

20492: `Failed to create thread (NSPR error).`
Cause: The Netscape Portable Runtime (NSPR) was unable to create one or more threads. This may be due to insufficient resources.

Solution: Perform the following steps:

1. Check that there is sufficient available memory and that a sufficient number of threads per process has been set up in the operating system configuration.

2. Check the error code that appears in the log against the NSPR error codes (refer to http://www.mozilla.org/projects/nspr/reference/html/prerr.html).

20494: Instance *instance_name* does not have the expected version *version_number*.
Cause: An attempt was made to open a database with a different database version. This is probably a migration issue.

Solution: Export the database from the old server and import it to the new server.

20499: dblayer_instance_start_fail: backend *instance_name* has no IDs left. Database must be rebuilt.
Cause: The internal NEXTID counter has reached the limit.

Solution: Rebuild the database.

20501: Serious failure in dblayer_txn_begin. Err=*value*.
Cause: The database has reported an error. If the printed value is positive, this is a system error. If the printed value is negative, the database has not been recognized or must be recovered.

Solution: This is a serious database error. Please contact Sun Technical Support.

20502: Serious failure in dblayer_txn_commit. Err=*value*.
Cause: The database has reported an error. If the printed value is positive, this is a system error. If the printed value is negative, the database has not been recognized or must be recovered.

Solution: This is a serious database error. Please contact Sun Technical Support

20503: Serious failure in dblayer_txn_abort. Err=*value*.
Cause: The database has reported an error. If the printed value is positive, this is a system error. If the printed value is negative, the database has not been recognized or must be recovered.

Solution: This is a serious database error. Please contact Sun Technical Support

20504: Serious failure in deadlock detect (aborted at *address*). Err=*value*.
Cause: The database has reported an error. If the printed value is positive, this is a system error. If the printed value is negative, the database has not been recognized or must be recovered.

Solution: This is a serious database error. Please contact Sun Technical Support

20505: Serious failure during database checkpointing. Err=*value*.
Cause: The database has reported an error other than an inability to write pages to the disk immediately. If the printed value is positive, this is a system error. If the printed value is negative, the database has not been recognized or must be recovered.

Solution: This is a serious database error. Please contact Sun Technical Support

20506: Serious failure during trickle. Err=*value*.
Cause: The database has reported an error. If the printed value is positive, this is a system error. If the printed value is negative, the database has not been recognized or must be recovered.

Solution: This is a serious database error. Please contact Sun Technical Support

20507: Failed to create guardian file. Database corruption possible.
Cause: This is a file system error. The server was unable to create the required guardian file.

Solution: Check that the user specified at installation has the appropriate permissions to write to the database directory.

20508: Database *database* is corrupt and being marked unavailable. Either re-import or delete the database.
Cause: The database is corrupt. This is most likely to be the result of a previously aborted database import.

Solution: Import from LDIF or delete the database.

20512: Failed to write guardian file. Database corruption possible.
Cause: This is a file system error. The server was unable to write to or close the guardian file.

Solution: Check that the user specified at installation has the appropriate permissions to write to the database directory. Ensure that the file system is not full.

20513: Failed to delete guardian file. Database corruption possible.
Cause: This is a file system error. The server was unable to delete the guardian file.

Solution: Check that the user specified at installation has the appropriate permissions to write to the database directory.

20517: open or creation of file: *filename* failed
Cause: Directory Server failed to create the specified file during backup.

Solution: Check disk space, then check permissions on the file system before attempting backup again.

20518: write to file: *filename* failed
Cause: Directory Server failed to write to the specified file during backup.

Solution: Check disk space, then check permissions on the file system before attempting backup again.

20519: open of file: *filename* failed
Cause: Directory Server failed to read from the specified file during restore.

Solution: Check permissions on the file system before attempting restore again.

20520: Wrong index definitions for backend *backend*: the index *index* is not part of backuped data
Cause: The index definitions in the backup do not match the current configuration.

Solution: Change the current configuration to match that of the backup before attempting to restore again.

20521: backend *backend* is included in backup but not in current configuration
Cause: A backend specified in the backup does not match the current configuration.

Solution: Add a backend to the current configuration with the same indexes configured as in the backup before attempting to restore again.

20522: backend *backend* is included in current configuration but not in backup
Cause: A backend specified in the current configuration does not match the backup.

Solution: Add a backend to the current configuration with the same indexes configured as in the backup before attempting to restore again.

20737: ldbm backend instance: nextid not initialized.
Cause: This is a software problem.

Solution: Please contact Sun Technical Support.

20738: ldbm backend instance: FATAL ERROR: backend name has no IDs left. DATABASE MUST BE REBUILT.
Cause: The limit for the database internal identifier has been reached. This is probably due to several adds and deletes being performed on the local database.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20739: ldbm backend instance: WARNING: backend *backend_name* may run out of IDs.
Cause: The limit for the database internal identifier is close to being reached. This is probably due to several adds and deletes being performed on the local database

Solution: If the limit has been reached, rebuild the database, using db2ldif, then ldif2db.

20740: Numsubordinates assertion failure.
Cause: The database is not coherent. There is a child entry that is unknown to the parent entry and the numsubordinates attribute is absent in the parent entry.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20745: ldbm_back_seq: id2entry err *error*.
Cause: An entry could not be located during an ldbm_back_seq operation. The database is incoherent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20746: ldbm_back_seq: could not open index file for attribute *attribute*.
Cause: An index file could not be located during an ldbm_back_seq operation. The database is incoherent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20747: compare_entries db err *error_number* while loading entry *entry*.
Cause: Certain entries were deleted while the server was attempting to sort them. This is probably due to a VLV or SORT control in a search.

Solution: Create a VLV index to avoid "on the fly" sorting.

20748: start : Resource limit registration failed.
Cause: The local database could not be started because the limit subsystem did not allow it to register.

Solution: Check the resource limit configuration and restart the server.

20749: start : Failed to init database err=*error*.
Cause: The local database could not be started because the underlying database component did not start.

Solution: Check that the database configuration is correct, and that there is enough disk space available.

20750: start : Failed to start databases err=*error*.
Cause: The local database instances could not be started.

Solution: Check that the database configuration is correct, and that there is enough disk space available.

20751: Database version mismatch (expecting *version* but found *version* in directory *directory*.)

Cause: The binary code for one version of Directory Server was started on a database with a different version.

Solution: Check the versions and ensure that the same binary and database versions are used.

20752: VLV : can't get index file *file* (err *error*).

Cause: The server could not locate the file used for the virtual list view (VLV) index during an update.

The database is inconsistent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20753: vlv_build_idl: can't follow db cursor (err *error*).

Cause: The database is incoherent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20754: nomem: wants *value* key *value* data.

Cause: The system is out of memory

Solution: Check the configuration.

20755: VLV : can't get index file *file* (err *error*).

Cause: The server could not locate the file used for virtual list view (VLV) indexes.

The database is inconsistent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20756: VLV : couldn't get cursor (err *error*).

Cause: The server could not locate a cursor used for virtual list view (VLV) indexes.

The database is inconsistent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20757: vlv_filter_candidates: Candidate *id* not found err=*error*.

Cause: The server could not locate an entry that is present in the virtual list view (VLV) index.

The database is inconsistent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20758: vlv_trim_candidates_byvalue: Candidate ID *id* not found err *error*.
Cause: The server could not locate an entry that is referenced in a virtual list view (VLV) index.

The database is inconsistent.

Solution: Rebuild the database, using db2ldif, then ldif2db.

20759: vlv find index: err *error*.
Cause: The server could not locate an index used in virtual list view (VLV).

Solution: Check the VLV configuration.

20760: Couldn't generate valid filename from Virtual List View Index Name name.
Need some alphabetical characters.
Cause: An LDAP client attempted to create a virtual list view (VLV) index with an invalid name. This should not harm Directory Server.

Solution: Change the LDAP client so that it uses a valid name.

20761: Add: maximum ID reached cannot add entry to backend *backend*.
Cause: The limit for the database internal identifier has been reached. This is probably because several adds and deletes have been performed on the local database.

Solution: Regenerate the database using ldif2db and db2ldif.

20762: Add: attempt to index *entry* failed.
Cause: The server was unable to index the entry being added.

Solution: Check the previous errors in the log for additional information.

20763: Retry count exceeded in add.
Cause: The acceptable number of add retry counts was exceeded without success. Another operation may be ongoing, resulting in a conflict when trying to access that part of the database.

Solution: Wait until other operations have ended and retry the add operation.

20764: Line *line_number*: Fatal Error: Failed to initialize attribute
structuring.
Cause: The server was unable to initialize the attribute structure. This is probably a memory error.

Solution: Check the available memory.

20765: Attempt to delete a non-tombstone entry *entry*.
Cause: An attempt was made to delete an entry that was not a tombstone entry.

Solution: Please contact Sun Technical Support.

20766: Attempt to tombstone again a tombstone entry *entry*.
Cause: An attempt was made to tombstone an entry that is already a tombstone entry.

Solution: Please contact Sun Technical Support.

20768: Retry count exceeded in delete.
Cause: The acceptable number of delete retry counts was exceeded without success. Another operation may be ongoing, resulting in a conflict when trying to access that part of the database.

Solution: Wait until other operations have ended and retry the delete operation.

20772: Retry count exceeded in modify.
Cause: The acceptable number of modify retry counts was exceeded without success. Another operation may be ongoing, resulting in a conflict when trying to access that part of the database.

Solution: Wait until other operations have ended and retry the modify operation.

20773: Retry count exceeded in modrdn.
Cause: The acceptable number of retry counts was exceeded without success. Another operation may be ongoing, resulting in a conflict when trying to access that part of the database.

Solution: Wait until other operations have ended and retry the modrdn operation.

20774: modrdn: could not add new value to index err=*error*
Cause: The server was unable to add a new value to the index.

Solution: Check the error log for more information and contact Sun Technical Support.

20775: Database error *error*.
Cause: A database error occurred while trying to build the list of possible candidate entries. The index files may be corrupt.

Solution: Re-index and try again.

20776: Null referral in *entry*.
   Cause: The candidate entry has a NULL referral.

   Solution: Update the referral in the entry or remove the ref attribute.

20777: Filter bypass error on entry *entry*.
   Cause: The server failed to bypass the filter test.

   Solution: Please contact Sun Technical Support.

20778: Unable to add config entries to the DSE.
   Cause: The server was unable to add configuration entries to the DSE.

   Solution: Ensure that there is no inconsistency within the entries.

20779: ERROR: ldbm plugin unable to read cn=config.
   Cause: The configuration information under cn=config could not be read.

   Solution: Please contact Sun Technical Support.

20780: ERROR: ldbm plugin unable to read attribute nsslapd-instancedir from
cn=config.
   Cause: The nsslapd-instancedir attribute under cn=config could not be read. The
   attribute may be missing.

   Solution: Ensure that the nsslapd-instancedir attribute is present and has an appropriate
   value.

20786: Invalid value for *attribute*. Must be between 0 and 100.
   Cause: An invalid value was provided for the nsslapd-db-trickle-percentage attribute.
   The value should be between 0 and 100.

   Solution: Check and correct the value provided for the nsslapd-db-trickle-percentage
   attribute

20787: *Attribute* can't be modified while the server is running.
   Cause: An attempt was made to modify a configuration attribute while the server was
   running. This attribute cannot be changed online.

   Solution: Stop the server before modifying the attribute.

20788: Value *value* for attribute *attribute* is not a number.
   Cause: The attribute value must be numerical.

   Solution: Ensure that the attribute has a numerical value.

20789: Value *value* for attribute *attribute* is greater than the maximum *value*.
   Cause: The value specified for the attribute is greater than the maximum permitted.

   Solution: Ensure that the attribute value is smaller than or equal to the maximum value.

20790: Value *value* for attribute *attribute* is less than the minimum *value*.
   Cause: The value specified for the attribute is smaller than the minimum permitted.

   Solution: Ensure that the attribute value is greater than or equal to the minimum value.

20791: Value *value* for attribute *attribute* is outside the range of representable values.
   Cause: The value specified for the attribute is outside the permissible range.

   Solution: Ensure that the attribute value is within the representable range.

20792: Could not set instance config attr *attribute* to *value*.
   Cause: The server failed to set the instance configuration attribute.

   Solution: Ensure that both the syntax and the value of the attribute are correct.

20793: Could not retrieve ldbm config info from DSE.
   Cause: The server was unable to access the ldbm configuration in the DSE.

   Solution: Check that the Directory Server configuration file has not been corrupted and restart the server.

20795: ldbm: instance instance does not exist!
   Cause: The specified instance was not found because no such instance exists.

   Solution: Verify that the instance name is correct and corresponds to an existing instance.

20796: ldbm: instance is in the middle of a task. Cancel the task or wait for it to finish then try again.
   Cause: The specified instance is currently processing a task.

   Solution: Cancel the current task or wait for it to finish and retry.

20797: ldbm: modify attempted to change the root suffix of a backend (which is not allowed).
   Cause: An attempt was made to change the suffix associated with an ldbm database.

   Solution: Do not modify the nsslapd-suffix attribute of an existing instance.

20806: System info mismatch (expecting *variable* but found *variable* in directory *directory_name*).
Cause: The system information from the backend's DBVERSION file did not match the server information.

Solution: Edit the backend's DBVERSION file to match the server information.

20807: Failed to read server system information
Cause: The server was unable to obtain the system information. This is possibly a permissions or NSPR compilation issue.

Solution: Check that the user specified at installation has the appropriate permissions.

20994: Disk full under *variable*.
Cause: The available space on a disk used by Directory Server has dropped below the value of the disk-full-threshold attribute.

Solution: Increase the available disk space.

20996: Cannot parse entry from database for id *id* string =*variable*.
Cause: The wrong file system permissions or ownership can prevent proper access to database files.

Solution: Verify that file system permissions and ownership allow read and write access for the user and group of the user who runs Directory Server. The directory containing the files should also allow access.

If your database is split across multiple locations, verify the access rights in each location.

Cause: The database may be corrupt.

Solution: Restore the database from a backup.

20997: Inconsistent database: entrydn for *entry* refers to id *id* missing from id2entry.
Cause: Database corruption.

Solution: Restore the database from a backup.

21005: Could not open index *index* for update.
Cause: An attribute index is configured but the corresponding database index file could not be opened.

Solution: Check whether the file exists and/or rebuild it using db2index.

21006: Could not open index *index* for range query.
Cause: An attribute index has been configured but the corresponding database index file could not be opened.

Solution: Check whether the file exists and/or rebuild it using db2index.

21008: Backend initialization failed: could not allocate a lock.
Cause: Insufficient system resources.

Solution: Check the available memory.

21009: Backend initialization failed: could not allocate a condition variable.
Cause: Insufficient system resources.

Solution: Check the available memory.

21010: Backend initialization failed: could not set plugin functions.
Cause: Insufficient system resources.

Solution: Check the available memory.

21011: Backend initialization failed on instance *instance*: could not allocate a lock.
Cause: Insufficient system resources.

Solution: Check the available memory.

21012: Backend initialization failed on instance *instance*: could not allocate a condition variable.
Cause: Insufficient system resources.

Solution: Check the available memory.

21016: Failed to create ancestorid index.
Cause: An index could not be created on the disk.

Solution: Check the error log for previous messages that should isolate the problem.

21017: Incomplete parentid index suspected (*value* extra keys in ancestorid)
Cause: Database corruption.

Solution: Rebuild the parentid index or restore the database from a backup.

21018: Entry cache initialization failed: could not allocate lock.
Cause: Insufficient system resources.

Solution: Check the system free memory.

21022: *variable* is configured to use more than the available physical memory.
Cause: The cache size as defined in the configuration file exceeds database limits.

Solution: Lower the value of the cachesize attribute in the configuration file.

21023: Index *index* is inconsistent.
Cause: Database corruption.

Solution: Rebuild the affected index or restore the database from a backup.

21024: ldbm be malloc fail: Unable to create db name
Cause: Insufficient system resources.

Solution: Check the system free memory, then restart Directory Server.

21249: Failed to encrypt some attribute inside the entry *entry* before writing it
to the database.
Cause: The server was unable to encrypt the specified attribute inside the entry.

Solution: Check the attribute encryption configuration.

21250: Failed to decrypt some attribute inside the entry *entry* when reading it
from the database.
Cause: The server was unable to decrypt the specified attribute inside the entry.

Solution: Check the attribute encryption configuration.

21251: Encrypted value's prefix doesn't match the corresponding algorithm
algorithm in the attribute encryption configuration.
Cause: The value is already encrypted or does not match the algorithm specified in the
configuration.

Solution: Check that the attribute encryption configuration is correct.

21252: Server didn't find plug-in for algorithm *algorithm*.
Cause: The server was unable to locate the plug-in for the specified algorithm.

Solution: Enable the encryption plug-in.

21253: Failed to encrypt index keys.
  Cause: The server was unable to encrypt the specified values.

  Solution: Check that the values are not already encrypted and that the cipher with which they are being encrypted match the configuration settings.

21254: Attribute encryption: failed to *encrypt/decrypt* attribute *attribute* with algorithm *algorithm*.
  Cause: The server was unable to encrypt/decrypt the attribute's values. The attribute may already be encrypted with an incorrect algorithm or the algorithm plug-in may be missing.

  Solution: Check for inconsistencies in the attribute encryption configuration.

21255: Encryption plugin (*plugin*): failed to encrypt.
  Cause: An error occurred during the plug-in's encryption function.

  Solution: Check the plug-in traces. Ensure that the plug-in itself has not been corrupted.

21256: Encryption plugin (*plugin*): failed to decrypt.
  Cause: An error occurred during the plug-in's decryption function.

  Solution: Check the plug-in traces. Ensure that the plug-in itself has not been corrupted.

24577: Bulk import process failed: state=*state*, error code=*error*.
  Cause: The bulk import has been aborted.

  Solution: Ensure that the bulk import is started or previously suspended before attempting an update or restart.

28673: filter_sp_replace_or_add_checksum: failed to update *attribute* attribute from *entry* entry; LDAP error - *errnum*.
  Cause: The attribute filterspconfchecksum could not be updated with a new value.

  Solution: Perform the following steps:

  1. Check whether the attribute already exists in the entry.
  2. Check whether the attribute is present in the Directory Server configuration.

32769: Unable to allocate memory. Cannot start Roles plugin.
  Cause: There is not enough memory to register the roles plug-in into the service provider broker.

  Solution: Restart the server.

32770: Unable to allocate memory. Cannot start Roles plugin.
Cause: There is not enough memory to register the nsrole attribute.

Solution: Restart the server.

32771: Unable to allocate memory. Cannot create Roles cache.
Cause: This error indicates a resource problem on the machine.

Solution: Restart the server.

32772: Lock creation failed. Cannot create Roles cache.
Cause: This error indicates a resource problem on the machine.

Solution: Restart the server.

32773: Conditional variable creation failed. Cannot create Roles cache.
Cause: This error indicates a resource problem on the machine.

Solution: Restart the server.

32774: Thread creation failed. Cannot create Roles cache.
Cause: This error indicates a resource problem on the machine.

Solution: Restart the server.

32775: Failed to get objectclass from *entry*.
Cause: The specified entry does not contain an objectclass.

Solution: Check the entry and add the required objectclass.

32776: Unsupported operation *operation*.
Cause: An unknown operation has been performed on the server and is triggering a role cache update.

Solution: Check that the specified operation is valid.

32778: Maximum number of nested roles exceeded (max *value* current *value*). Not retrieving roles from entry *entry*. Probable circular definition.
Cause: The maximum number of nested roles has been exceeded. This is probably due to a circular role definition.

Solution: Check the role definitions. The maximum number of nested roles permitted is defined by MAX_NESTED_ROLES.

32779: Nested role *entry* does not exist.
   Cause: The entry corresponding to the DN does not exist.

   Solution: Check the role definition.

32780: Cannot initialize Roles plugin.
   Cause: The server is unable to update the pblock parameters.

   Solution: Restart the server.

32781: Unknown role type *type*.
   Cause: The role type is unknown. Valid role types are : managed, filtered, or nested.

   Solution: Check the role definition and amend the type as necessary.

33025: Could not allocate PB.
   Cause: Internal error, probably due to insufficient available memory.

   Solution: Free up some memory. If the error continues, please contact Sun Technical Support.

33026: Internal PBG error.
   Cause: Internal error.

   Solution: Please contact Sun Technical Support.

33027: Internal search error in Attribute Uniqueness plugin.
   Cause: Internal error.

   Solution: Please contact Sun Technical Support.

33028: Internal PB error.
   Cause: Internal error.

   Solution: Please contact Sun Technical Support.

33029: Could not find plugin argument number.
   Cause: Memory corruption or invalid configuration.

   Solution: Check the plug-in configuration. If it is valid, please contact Sun Technical Support.

33030: Could not find plugin arguments.
   Cause: Memory corruption or invalid configuration.

   Solution: Check the plug-in configuration. If it is valid, please contact Sun Technical Support.

33031: Could not find a valid argument.
Cause: Configuration error.

Solution: Check the plug-in configuration parameters in the Directory Server configuration. Make sure that the syntax and values are correct.

33032: ADD/MOD/MODRDN: unable to get replication flag.
Cause: Internal error.

Solution: Please contact Sun Technical Support.

33033: ADD/MOD/MODRDN: unable to get target DN.
Cause: Internal error.

Solution: Please contact Sun Technical Support.

33034: Unable to get entry data.
Cause: Internal error.

Solution: Contact Sun Technical Support.

33035: Could not get MODIFY data.
Cause: Internal error.

Solution: Please contact Sun Technical Support.

33036: Error while retrieving mod values.
Cause: Internal error.

Solution: Please contact Sun Technical Support.

33037: Unable to get new superior DN.
Cause: The new superior DN does not exist.

Solution: Check the validity of the intended operation.

33038: Unable to get new DN.
Cause: The new DN is invalid or is not correctly specified.

Solution: Check the validity of the intended operation.

33039: Unable to allocate a new entry.
Cause: Internal error.

Solution: Please contact Sun Technical Support.

33040: ADD parameter untagged: *error*.
    Cause: Configuration error.

    Solution: Check the plug-in configuration parameters in the Directory Server configuration. Make sure that the syntax and values are correct.

33041: ADD result *result*.
    Cause: An error occurred during an internal search while performing an ADD operation.

    Solution: Ensure that the database is not corrupt and contact Sun Technical Support.

33042: MODIFY result *result*.
    Cause: An error occurred during an internal search while performing a MOD operation.

    Solution: Ensure that the database is not corrupt and contact Sun Technical Support.

33043: MODRDN bad rdn value=*value*.
    Cause: Internal error.

    Solution: Please contact Sun Technical Support.

33044: MODRDN result *result*
    Cause: An error occurred during an internal search while performing a modrdn operation.

    Solution: Ensure that the database is not corrupt and contact Sun Technical Support.

33045: NSUniqueAttr_Init Error: *error*
    Cause: Configuration error.

    Solution: Check the plug-in configuration parameters in the Directory Server configuration.

33046: Fatal error Initializing plugin. Disabling.
    Cause: A plug-in failed to initialize.

    Solution: Restart the server.

33059: Cannot get plugin identity.
    Cause: Plug-in identity information could not be determined.

    Solution: Restart the server.

33069: Sorry cannot do it but given the chance you just incurred in you may consider playing at the next lottery the number *number* successively reduced mod [your lottery maximum]

Cause: Your lucky number came up.

Solution: Contact Sun Technical Support.

33793: cos_cache_init: cannot create mutexes

Cause: The server was unable to allocate mutexes for the CoS plug-in. This is probably due to a memory problem.

Solution: Free up resources on the machine and restart the server.

33794: cos_cache_init: cannot register as service provider

Cause: The server was unable to register a virtual attribute service provider.

Solution: Free up resources on the machine and restart the server.

33795: cos_cache_init: PR_CreateThread failed

Cause: The server was unable to create a CoS thread.

Solution: Free up resources on the machine and restart the server.

33796: cos_cache_create: failed to cache the schema

Cause: The server was unable to create the CoS schema cache.

Solution: Follow these steps.

1. Free up resources on the machine.
2. "Touch" a CoS definition to trigger CoS cache building.
3. Restart the server.

33797: cos_cache_create: failed to index cache

Cause: The server was unable to index the CoS cache.

Solution: Follow these steps.

1. Free up resources on the machine.
2. "Touch" a CoS definition to trigger CoS cache building.
3. Restart the server.

33798: COS memory allocation failure: variable

Cause: The server was unable to allocate memory for the CoS cache.

Solution: Follow these steps.

1. Free up resources on the machine.

2. "Touch" a CoS definition to trigger CoS cache building.
3. Restart the server.

33799: `cos_cache_build_definition_list: failed to find suffixes in the rootDSE.`
Cause: The server was unable to read the suffix list from the rootDSE entry.

Solution: Restart the server.

33801: `COS Definition error` *error*
Cause: There is an error in the definition of the specified CoS.

Solution: Check and correct the CoS definition. Note that a definition cannot supply its own specifier. The DN of the CoS template may be incorrect.

33802: `cos_cache_add_dn_tmpls: could not cache cos template` *variable*
Cause: The server was unable to add the specified template to the CoS cache.

Solution: Follow these steps.

1. Free up resources on the machine.
2. "Touch" a CoS definition to trigger CoS cache building.
3. Restart the server.

33803: `cos_cache_query_atr: failed to get entry dn`
Cause: The server was unable to locate the dn of the target entry during a search operation. This error should not occur under normal circumstances.

Solution: Follow these steps.

1. Retry the search operation.
2. Restart the server.

33804: `COS failed to get objectclass from entry (`*entry*`)`
Cause: The server was unable to locate the `objectClass` of the target entry during a search or update operation. This error should not occur under normal circumstances.

Solution: Follow these steps.

1. Retry the search or update operation.
2. Restart the server.

33806: `cos_start: failed to initialise`
Cause: The server was unable to start the CoS plug-in. This is probably due to a memory problem.

Solution: Follow these steps.

1. Check the CoS plug-in configuration in the Directory Server configuration.
2. Check the CoS definitions and templates.
3. Check the error log for a more specific error message.
4. Restart the server.

33807: cos_init: failed to register plugin
Cause: The server was unable to register the CoS plug-in. This is probably due to a memory problem.

Solution: Follow these steps.

1. Check the CoS plug-in configuration in the Directory Server configuration.
2. Check the error log for a more specific error message.
3. Restart the server.

33808: COS Definition error (no DN)
Cause: There is an error in the definition of the specified CoS.

Solution: Check and correct the CoS definition.

33809: cos_cache_change_notify: failed to get dn of changed entry
Cause: The server was unable to obtain the dn of the target entry during an update operation. This error should not occur under normal circumstances.

Solution: Follow these steps.

1. Retry the update operation.
2. Restart the server.

34307: Request OID (*OID*) doesn't match Who Am I? Extended Op OID
Cause: Internal error

Solution: Contact Sun Technical Support.

34817: ACL library initialization failed.
Cause: The server is unable to initialize the ACL plug-in. This is usually an indication of memory problems.

Solution: Follow these steps.

1. Check the ACL plug-in configuration in the Directory Server configuration.
2. Check the error log for other, more specific error messages.
3. Restart the server.

34818: ACL failed to allocate locks.
Cause: The server is unable to allocate mutex or reader/writer locks for the ACL plug-in at initialization time.

Solution: Follow these steps.

1. Check the OS configuration and increase the file descriptors limit, if possible.
2. Check the Directory Server configuration and reduce the resource usage.

34819: ACL malloc fail: *error*.
Cause: The server is unable to allocate sufficient `aclpb` pool memory for the ACL plug-in.

Solution: Free up resources on the machine and restart the server.

34820: ACL internal error: *error*.
Cause: This is an internal error and should not occur under normal circumstances.

Solution: Perform the following steps:

1. Attempt the LDAP operation again.
2. Restart the server.
3. Copy the errors log file and contact Sun Technical Support.

34822: Unable to initialize the plugin: *plugin_name*
Cause: The server is unable to allocate sufficient ACL parameter block pool memory for the ACL plug-in.

Solution: Free up resources on the machine and restart the server.

34823: Error: ACIs not deleted from *entry*.
Cause: The server was unable to remove the specified ACIs from the entry. Refer to the error log for more information.

Solution: Attempt the modify operation again.

34824: ACL internal init fail: *error*.
Cause: Initialization error. The server was unable to register the specified attributes with `libaccess`. Refer to the error log for more information.

Solution: Verify the configuration and installation of the ACL plug-in.

34826: ACL error adding aci: *aci*.
Cause: There is an error (possibly invalid ACI syntax) in the ACI attribute being updated.

Solution: Correct the error in the ACI and attempt the ACI update operation again.

34827: ACL parsing error: *error*.
   Cause: ACL parsing error for a macro ACI. Refer to the log file for the exact cause of the error.

   Solution: Correct the error in the ACI and attempt the ACI update operation again.

34828: ACL parsing error: failed to make filter for string *string*.
   Cause: ACL parsing error. The server was unable to construct an LDAP filter for the specified string.

   Solution: Correct the error in the ACI and attempt the ACI update operation again.

34829: ACL PARSE ERR(rv=*error_code*): *aci*.
   Cause: ACL parsing error. Refer to the log file for the exact cause of the error.

   Solution: Correct the error in the ACI and attempt the ACI update operation again.

34830: Can't add the rest of the acls for entry: *entry* after delete.
   Cause: The server failed to update ACIs in the specified entry, when an ACI was deleted.

   Solution: Follow these steps.

   1. Attempt the update operation again.
   2. Restart the server.

34831: ACL failed to allocate locks.
   Cause: The server is unable to allocate mutex or reader/writer locks for the ACL plug-in at operation time.

   Solution: Follow these steps.

   1. Free up resources on the machine.
   2. Attempt the LDAP operation again.
   3. Restart the server.

34832: Operation extension allocation failed.
   Cause: The server is unable to get/create an operation extension structure at operation time.

   Solution: Follow these steps.

   1. Free up resources on the machine.
   2. Attempt the LDAP operation again.
   3. Restart the server.

34834: `acl_get_aclpb: Invalid aclpb type`
Cause: An invalid ACL operation extension was found. This is an internal error and should not occur under normal circumstances

Solution: Follow these steps.

1. Attempt the LDAP operation again.
2. Restart the server.
3. Copy the errors log file and contact Sun Technical Support.

34835: `ACLPB parameter` *parameter* `value` *value* `exceeded allowed value` *value*.
Cause: This is an internal error and should not occur under normal circumstances.

Solution: Follow these steps.

1. Attempt the LDAP operation again.
2. Restart the server.

34838: `ACL parent[ ] exceeded the levels limit` *max_limit*: *function*.
Cause: ACL parsing error: the parent keyword has been used with more than ten levels. Check the log file to see the type of ACI in which the keyword was used incorrectly.

Solution: Correct the error in the ACI and attempt the operation again.

34842: `getRightsControl: insufficient access`
Cause: User is not allowed to use the getRights control.

Solution: Check whether user should be granted access to get effective rights.

34844: `getRights control parsing:error parsing control paramters`
Cause: Directory Server found invalid request parameters in the request to get effective rights.

Solution: Check how the client is using the control. If necessary, contact Sun Technical Support.

34846: `ACL INTERNAL REFERENTIAL INTEGRITY ERR:` *message*
Cause: Not enough memory could be allocated to complete ACL processing.

Solution: Restart the server.

36865: `collation_unlock: PR_ExitMonitor (`*variable*`)=variable; collation_monitor =` *variable*
Cause: An error occurred while releasing the collation lock.

Solution: Restart the server.

36866: collation_init: PR_NewMonitor failed
  Cause: An error occurred while creating the collation lock.

  Solution: Restart the server.

36867: *variable*: line *line_no*: missing directory name in directory *directory*
(ignored)
  Cause: No argument was provided for the NLS parameter.

  Solution: Check the configuration variable.

36868: *variable*: line *line_no* ignored: only variable arguments (expected collation
language country variant strength decomposition oid...)
  Cause: Insufficient arguments were provided for the collation parameter.

  Solution: Check the configuration variable.

36869: *variable*: line *line_no*: strength *value* not supported (will use 2)
  Cause: An invalid value was specified for the collation strength.

  Solution: Check the configuration variable.

36870: *variable*: line *line_no*: decomposition *value* not supported (will use 2)
  Cause: An invalid value was specified for the collation decomposition.

  Solution: Check the configuration variable.

36871: Too many tokens (max *max_tokens*)
  Cause: Too many items have been specified on the configuration line.

  Solution: Check the configuration variable.

36872: Could not open config file *filename* - absolute path.
  Cause: The server was unable to open the collation configuration file.

  Solution: Check the path to the collation configuration file.

36873: *variable*: line *line_no*: bad config line (ignored)
  Cause: The server was unable to parse a line in the collation configuration file.

  Solution: Check the collation configuration file.

36874: Unable to retrieve slapd configuration pathname; using default.
  Cause: The location of the collation configuration file was not provided to the plug-in.

  Solution: Check the path to the collation configuration file.

36875: while reading configuration entry (*DN*) for Internationalization plugin,
error *code*
    Cause: Directory Server encountered an error while searching for the internationalization
    plug-in.

    Solution: Fix the Internationalization plug-in configuration entry, then restart Directory
    Server.

36876: Missing Internationalization plugin configuration entry *DN*
    Cause: Directory Server encountered an error while searching for the internationalization
    plug-in.

    Solution: Fix the Internationalization plug-in configuration entry, then restart Directory
    Server.

36877: Missing "Collation" attribute in Internationalization plugin
configuration entry *DN*
    Cause: Directory Server encountered an error while reading the configuration entry.

    Solution: Fix the Internationalization plug-in configuration entry, then restart Directory
    Server.

36878: *DN*: value *index*: bad collation config data (ignored)
    Cause: Directory Server encountered an error while reading the collation configuration file.

    Solution: Fix the Internationalization plug-in configuration entry, then restart Directory
    Server.

37121: Not enough pattern space.
    Cause: The regular expression being constructed for the DN substring filter could not be
    stored in the memory allocated.

    Solution: Check the DN substring filter being provided to the server.

37122: re_comp *filter* failed.
    Cause: The regular expression being constructed for the substring filter could not be
    compiled.

    Solution: Check the substring filter being provided to the server.

37123: dn_assertion2keys_ava: unknown ftype.
    Cause: A filter containing an unknown type was provided to the server.

    Solution: Check the filter being provided to the server.

37377: statechange_init: failed to register plugin.
   Cause: The state change plug-in could not be registered with the server.

   Solution: Restart the server.

37378: statechange: failed to create lock.
   Cause: The server was unable to create a mutex for the state change subsystem.

   Solution: Restart the server.

37379: statechange: failed to publish state change interface.
   Cause: The server was unable to publish the interface to the state change plug-in API.

   Solution: Restart the server.

37380: statechange_post_op: failed to get dn of changed entry.
   Cause: The server was unable to determine the DN of the modified entry.

   Solution: Restart the server.

37633: Only one pass through plugin instance can be used
   Cause: An attempt was made to configure multiple instances of the pass through authentication plug-in.

   Solution: Check the pass-through authentication plug-in configuration.

37634: No pass through servers found in configuration (at least one must be listed)
   Cause: An attempt was made to use the pass through authentication plug-in without specifying any remote servers.

   Solution: Check the pass-through authentication plug-in configuration.

37635: Server parameters should be in the form "maxconnections maxconcurrency timeout ldapversion connlifetime" (got "*error*")
   Cause: The set of parameters specified for the remote server was invalid.

   Solution: Check the pass-through authentication plug-in configuration.

37636: LDAP protocol version should be *version* or *version* (got *error*)
   Cause: The LDAP version specified for the remote server was invalid.

   Solution: Check the pass-through authentication plug-in configuration.

37637: Maximum connections must be greater than zero (got *error*)
Cause: The maximum number of connections to the remote server is specified as less than or equal to zero.

Solution: Check the pass-through authentication plug-in configuration.

37638: Maximum concurrency must be greater than zero (got *error*)
Cause: The maximum concurrency is specified as less than or equal to zero.

Solution: Check the pass-through authentication plug-in configuration.

37639: Unable to parse LDAP URL "*url*" (*error*)
Cause: An error occurred while parsing the LDAP URL.

Solution: Check the pass-through authentication plug-in configuration.

37640: Missing suffix in LDAP URL "*url*"
Cause: The pass-through suffix was not specified in the LDAP URL.

Solution: Check the pass-through authentication plug-in configuration.

37641: Unable to parse suffix string "*suffix*" within variable
Cause: An error occurred while splitting the list of suffixes for which authentication is to be passed through.

Solution: Check the pass-through authentication plug-in configuration.

37642: Suffix "*suffix*" is handled by a database backend and therefore will not be subject to pass through authentication
Cause: One of the suffixes for which pass-through authentication is configured exists in the local directory.

Solution: Check the pass-through authentication plug-in configuration.

37644: ldap_charray_add() failed when building suffix list
Cause: An error occurred while adding a suffix to the list of suffixes handled by backends in the server.

Solution: Restart the server.

37645: No active suffixes found
Cause: No active suffixes could be located in the local server.

Solution: Check the server configuration and/or restart the server.

37646: passthruauth_init failed
Cause: The pass-through authentication plug-in could not be registered.

Solution: Restart the server.

37647: Unable to get arguments
Cause: The server was unable to locate the list of arguments to the pass-through authentication plug-in.

Solution: Check the pass-through authentication plug-in configuration.

37648: configuration failed (variable)
Cause: The pass-through authentication plug-in could not be configured based on the arguments provided.

Solution: Check the pass-through authentication plug-in configuration.

37649: Operation not handled (unable to retrieve bind parameters)
Cause: The server was unable to determine the required information regarding the bind operation.

Solution: Check the bind request.

37650: *error*
Cause: The server was unable to retrieve the set of controls associated with the bind request.

Solution: Check the bind request.

37651: *error*
Cause: The server was unable to set the DN or authentication type associated with this connection.

Solution: Restart the server.

37889: referint_postop_init failed
Cause: A failure occurred while registering the referential integrity plug-in.

Solution: Restart the server.

37890: referint_postop_del: could not get parameters
Cause: The server was unable to retrieve the required information about a delete operation.

Solution: Check the delete request.

37891: referint_postop failed to get argc
   Cause: The server was unable to determine the number of parameters to the referential integrity plug-in.

   Solution: Restart the server.

37892: referint_postop failed to get argv
   Cause: The server was unable to retrieve the parameters associated with the referential integrity plug-in.

   Solution: Restart the server.

37893: referint_postop_del args are NULL
   Cause: No arguments were provided for the referential integrity plug-in.

   Solution: Check the configuration of the referential integrity plug-in.

37894: referint_postop insufficient arguments supplied
   Cause: Insufficient arguments were provided for the referential integrity plug-in.

   Solution: Check the configuration of the referential integrity plug-in.

37895: referint_postop_modrdn: could not get parameters
   Cause: The server was unable to retrieve the required information about a modrdn operation.

   Solution: Check the delete request.

37896: referint_postop failed to get argc
   Cause: The server was unable to determine the number of parameters to the referential integrity plug-in.

   Solution: Restart the server.

37897: referint_postop failed to get argv
   Cause: The server was unable to retrieve the parameters associated with the referential integrity plug-in.

   Solution: Restart the server.

37898: referint_postop_modrdn args are NULL
   Cause: No arguments were provided for the referential integrity plug-in.

   Solution: Check the configuration of the referential integrity plug-in.

37899: referint_postop_modrdn insufficient arguments supplied
Cause: Insufficient arguments were provided for the referential integrity plug-in.

Solution: Check the configuration of the referential integrity plug-in.

37900: update_integrity required config file arguments missing
Cause: No arguments were provided for the referential integrity plug-in.

Solution: Check the configuration of the referential integrity plug-in.

37901: referint_postop search (base=*base* filter=*filter*) returned error *error*.
Cause: An error occurred while searching for references to the deleted/renamed entry.

Solution: Follow these steps.

1. Check the error log for details of the error.
2. Restart the server.

37902: referint_postop failed to get argc
Cause: The server was unable to determine the number of parameters to the referential integrity plug-in.

Solution: Restart the server.

37903: referint_postop failed to get argv
Cause: The server was unable to retrieve the parameters associated with the referential integrity plug-in.

Solution: Restart the server.

37904: args were null in referint_postop_start
Cause: No arguments were provided for the referential integrity plug-in.

Solution: Check the configuration of the referential integrity plug-in.

37905: referint_postop_start PR_CreateThread failed.
Cause: The server was unable to create the thread to perform integrity updates.

Solution: Restart the server.

37906: referint_postop_start insufficient arguments supplied
Cause: Insufficient arguments were provided to the referential integrity plug-in to determine the update delay.

Solution: Check the configuration of the referential integrity plug-in.

37907: referint_thread_func could not get args
Cause: The server was unable to retrieve the parameters associated with the referential integrity plug-in.

Solution: Restart the server.

37908: referint_postop_close could not delete *filename*
Cause: The referential integrity log file could not be deleted.

Solution: Check the permissions on the specified file and restart the server.

37909: referint_postop could not open integrity log *filename*
Cause: The referential integrity log file could not be opened for writing.

Solution: Check the permissions on the specified file and restart the server.

37910: referint_postop could not write integrity log: line length exceeded. It will not be able to update references to the entry *entry*.
Cause: The change to be written to the integrity log file was longer than the maximum length allowed.

Solution: Check for references to the specified entry and update manually if necessary.

37911: writeintegritylog: PR_Write failed : The disk may be full or the file is unwritable :: NSPR error - *error*.
Cause: The server was unable to write data to the integrity log file.

Solution: Follow these steps.

1. Check the integrity log file.
2. Check the filesystem status.

37912: writeintegritylog: failed to close the file descriptor prfd; NSPR error - *error*.
Cause: An error occurred while closing the integrity log file.

Solution: Follow these steps.

1. Check the integrity log file.
2. Check the filesystem status.

38402: Invalid mapping: *DN*
Cause: The ID mapping configuration is invalid.

Solution: Check on the entry specified by *DN* in the error message that:

- dsSearchFilter and dsSearchBaseDN are not NULL

- dsSearchScope is either sub, base or onelevel
- dsMatching_regexp conforms to regular expression syntax
- dsMatching_pattern and dsMatching_regexp are either both are NULL or both not NULL

38403: *attribute* syntax error: *value* in mapping entry: *DN*
Cause: The ID mapping configuration is invalid as specified.

Solution: Fix the syntax error in the value of the attribute specified, keeping in mind the following issues.

If you refer to an input variable, use the syntax ${...}

If you refer to a sub-expression use $*i* where *i* is in [1..N]

The characters $, {, and } are reserved. Use their hexadecimal forms when using them as values.

38404: Identity Mapping configuration is missing
Cause: Directory Server could not find any ID mapping configuration entries.

Solution: Update the identity mapping configuration by doing the following.

- Adding protocol entries under cn=identity mapping, cn=config
- Adding identity mapping entries under protocol entries with DNs
  cn=*protocol*,cn=identity mapping, cn=config

38405: Authentication protocol name missing
Cause: Directory Server could not find the ID mapping protocol.

Solution: Update the CN attribute of the identity mapping entry.

38407: There are no identity mapping entries for authentication protocol:
protocol
Cause: Directory Server could not find any entries corresponding to the specified ID mapping protocol.

Solution: Add an ID mapping entry under at least one protocol entry, where the ID mapping DN is cn=*protocol*,cn=identity mapping, cn=config

38408: There are no valid identity mapping entries for authentication protocol:
protocol
Cause: Directory Server could not find any valid entries corresponding to the specified ID mapping protocol.

Solution: Check the syntax of the ID mapping entries for the protocol.

38409: There are no identity mapping configuration for authentication protocol:
protocol
    Cause: The ID mapping service does not support the specified authentication protocol.

    Solution: Follow these steps.

    1. Create a protocol entry under cn=identity mapping, cn=config

    2. Create an identity mapping entry under the protocol entries with DNs
        cn=*protocol*,cn=identity mapping, cn=config

38410: Can't add default identity mapping entry for authentication protocol:
protocol
    Cause: Internal error

    Solution: Check that sufficient memory is available. If adding memory does not solve the
    problem, contact Sun Technical Support.

38913: The default SASL configuration entry could not be read or was not found in
the dse.ldif file. It is mandatory.
    Cause: The mandatory SASL configuration entry, cn=SASL,cn=security,cn=config, could
    not be retrieved from the configuration file.

    Solution: Check the existence of this entry in the configuration file and add it if it is not
    present. The entry contains the dsSaslConfig object class.

38914: Out of memory to create the SASL configuration structure.
    Cause: Memory allocation problem.

    Solution: Increase the amount of memory available.

38915: The SASL mandatory attribute dsSaslPluginsPath is missing in the dse.ldif
file. Some SASL authentication mechanisms will not be available
    Cause: A required attribute is missing.

    Solution: Fix the configuration on cn=SASL, cn=security, cn=config, then restart
    Directory Server.

38916: The SASL mandatory attribute dsSaslPluginsEnable is missing in the
dse.ldif file. Some SASL authentication mechanisms will not be available
    Cause: A required attribute is missing.

    Solution: Fix the configuration on cn=SASL, cn=security, cn=config, then restart
    Directory Server.

38917: Can't find localhost name.
Cause: The local host name is absent from the naming service.

Solution: Add the local host name to the naming service.

38918: SASL initialization failed.
Cause: Incorrect or missing information in the SASL configuration entry in the Directory Server configuration under cn=sasl.

Solution: Follow these steps.

1. Check that the entry exists in the configuration file.
2. Check that the information in the configuration entry is valid. That is, that the authentication mechanism names are correct.

38919: SASL Layer encoding return error *error-code*
Cause: SASL Layer encode method failed.

Solution: Contact Sun Technical Support.

38920: Write with SASL security enabled failed with error *error-code*
Cause: A write operation failed with the SASL security layer enabled. This could be a network issue.

Solution: Verify that the problem was not due to network conditions or to the behavior of the client application.

38921: SASL Layer decoding return error *error-code*
Cause: SASL Layer decode method failed.

Solution: Contact Sun Technical Support.

38922: Read with SASL security enabled failed with error *error-code*
Cause: A read operation failed with the SASL security layer enabled. This could be a network issue.

Solution: Verify that the problem was not due to network conditions or to the behavior of the client application.

38923: Size of packet read with SASL security enabled (*size*) is larger than our buffersize (*size*)
Cause: The server encountered an encoded packet from a SASL client larger than the maximum buffer size value of dsSaslMaxBufSize.

Solution: Verify that the SASL client application can negotiate a buffer size no larger than the value of `dsSaslMaxBufSize`.

49153: Cannot initialize memberOf plugin.
Cause: Could not register the isMemberOf plug-in with the server.

Solution: Restart the server.

49154: Unable to allocate memory. Cannot start memberOf plugin.
Cause: The server could not allocate enough memory for the MemberOf plug-in to generate virtual attributes.

Solution: Restart the server.

49155: Unable to allocate memory. Cannot start memberOf plugin.
Cause: The server could not allocate enough memory for the MemberOf plug-in to generate virtual attributes.

Solution: Restart the server.

49156: Maximum number of nested groups exceeded (max *number* current *number*) not retrieving member from entry *DN* -- probable circular definition.
Cause: The MemberOf Plugin does not allow more than the specified number of levels of group nesting.

Solution: Make sure no groups are nested more than the specified number of levels deep.

49157: Unable to preload memberOf attributes for groups!
Cause: The server could not create a thread needed to build a cache for isMemberOf attribute values.

Solution: Make more resource available to the server and restart the server.

53516: Cannot initialize Monitoring plugin.
Cause: The monitoring plug-in parameter block could not be updated.

Solution: Restart the server.

Common Warning Codes

This section describes the warning codes displayed in the *instance-path*/`logs/errors` log and the appropriate action to take should these warnings occur.

4155: `Cannot modify password history error` *error-code* `on entry` *DN*
Cause: Cannot modify password history in the entry. An internal modify operation failed.

Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4157: `passwordPolicy modify error` *error-code* `on entry` *DN*
Cause: The password modifications could not be applied due to entry modify error. An internal modify operation failed.

Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4193: `Plugin '`*name*`' (`*op-type plug-in-type*`) signaled an error (`*error-code*`)`
Cause: An external or internal post-op plugin signaled an error.

Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4194: `Password value from history is being reused by Directory Manager for user` *DN*
Cause: Directory Manager set the user password to a value that was already in the user password history.

Solution: Have the user change the password.

4195: `Short password value set by Directory Manager for user` *DN*
Cause: Directory Manager set the user password to a value that is shorter than the minimum length specified in the password policy.

Solution: Have the user change the password.

4196: `Trivial password value set by Directory Manager for user` *DN*
Cause: The password value for Directory Manager is too easy to guess.

Solution: Use a stronger Directory Manager password.

4201: `Password already hashed. Cannot check quality.`
Cause: The client application provided a hashed password. The server cannot read the hashed password and so does not check the password quality.

Solution: None.

4202: Trivial password value set
    Cause: The password value used is too easy to guess.

    Solution: Use a stronger user password.

4214: Server is now [frozen|thawed].
    Cause: The server has been successfully placed in frozen mode or has returned from frozen mode.

    Solution: None.

4215: The default password policy object has not been initialized
    Cause: Internal error: No entry was supplied to mpp_init_policy.

    Solution: Contact Sun Technical Support.

4216: The default password policy object has not been initialized.
    Cause: Internal error: No default password policy object available to mpp_get_policy.

    Solution: Contact Sun Technical Support.

4217: (Password Policy: *migration-operation*) reports LDAP result (*error-code*) for suffix "dn=*DN*".
    Cause: Cannot migrate attributes in the password policy entry.

    Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4217: *ldap-error-msg* Entry "dn=*DN*".
    Cause: Cannot migrate attributes in the password policy entry. Attribute migration or internal modify has failed.

    Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4217: *ldap-error-msg* Rejecting add of entry "dn=*DN*".
    Cause: Cannot migrate attributes in the password policy entry.

    Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4217: *ldap-error-msg* Rejecting modify of entry "dn=*DN*".
    Cause: Cannot migrate attributes in the password policy update.

Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4219: *ldap-error-msg*. Entry "dn=*DN*". Value ignored; replaced by default.
Cause: Invalid password policy entry.

Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4219: *ldap-error-msg* Entry "dn=*DN*".
Cause: Invalid password policy entry discovered. Pre-migration validation of password policy entry failed. The server attempts entry migration attempted anyway.

Solution: If you cannot determine the cause and resolve the issue using information in the log files, contact Sun Technical Support.

4220: While a passwordExpirationTime far in the future implies "never expires" in previous versions of Directory Server, this DSA supports multiple password policies, and this feature *feature* should be used instead.
Cause: Password policy state attribute passwordExpirationTime migration would result in an invalid pwdChangedTime value.

Solution: If the passwordExpirationTime value was set far into the future with the intention of preventing the account from expiring, use a specialized password policy (subentry) for this purpose. Otherwise, change the account password to clean up the passwordExpirationTime value.

4221: Password policy migration: The entry "dn:*DN*" contains "passwordExpirationTime: *time*" , which results in a migrated pwdChangedTime value in the future. Setting pwdChangedTime to the current time, which will expire in *seconds* seconds.
Cause: Password policy state attribute passwordExpirationTime migration would result in a pwdChangedTime value far in the future.

Solution: If the passwordExpirationTime value was intended to prevent the account from expiring, use a specialized password policy (subentry) for this purpose. Otherwise, change the account password to clean up the passwordExpirationTime value.

4609: Unable to create *file*
Cause: Cannot create the process ID file for the instance.

Solution: Check the file system to make sure the file can be created under the instance directory.

4611: Couldn't set the ownership to *user* for *directory*
Cause: Cannot own the directory containing the process ID file for the instance.

Solution: Check the file system to make sure the user has the right to change the ownership of the directory.

4611: Couldn't set the ownership for *file*
Cause: Cannot own the process ID file for the instance.

Solution: Check the file system to make sure user has the right to take ownership of the process ID file.

4748: "Security Initialization: Failed to set SSL cipher preference information: *cipher* (error *error-code - error-message*)
Cause: Security Initialization: Failed to set SSL cipher preference information.

Solution: Check the syntax of the ciphers in the configuration. Make sure all ciphers are supported by the server.

4752: Security Initialization: Failed to parse cipher family information entry *DN* because at least one of the attributes nsSSLToken or nsSSLPersonalitySSL are absent.
Cause: Security Initialization: Failed to parse cipher family information entry.

Solution: Check the cipher family information entry and fix the configuration.

4753: Security Initialization: Can't find certificate (*name*) for family *family* (error *error-code - error-message*)
Cause: Security Initialization: Cannot find the certificate for the specified family.

Solution: Make sure the certificate exists within the certificate database. If not, use the correct certificate name in the configuration, or else import the certificate into the database and try again.

4754: Security Initialization: Unable to retrieve private key for cert *name* of family *family* (error *error-code - error-message*)
Cause: Security Initialization: Unable to retrieve private key from cert of family.

Solution: Make sure the certificate has been imported into the database with both its public and private keys. This is usually done as a result of a whole process beginning with your certificate request.

4755: ConfigSecureServer: Server key/certificate is bad for cert *name* of family
family (error *error-code - error-message*)
Cause: ConfigSecureServer: Server key/certificate is bad for cert of family.

Solution: Check the validity of the server key/certificate and retry.

4762: Security Initialization: Cannot get SSL Client Authentication status. No
nsslclientauth in *DN* (error *error-code - error-message*).
Cause: Security Initialization: Cannot get SSL Client Authentication property from the
configuration. nsslclientauth attribute missing.

Solution: Add nsslclientauth attribute to the configuration if you want something other
than the default value.

4763: Security Initialization: Cannot set SSL Client Authentication status to
"*status*" error (*error-message*). Supported values are "off" "allowed" and
"required". (error *error-code - error-message*).
Cause: Security Initialization: Cannot set SSL Client Authentication property. Probable
invalid value of nssslclientauth attribute.

Solution: Make sure nssslclientauth takes valid value.

4764: SSL_OptionSet(SSL_REQUIRE_CERTIFICATE PR_FALSE) *return-code* error *error-code*
(*error-message*)
Cause: Failed to set the Client Authentication Allowed property.

Solution: If you cannot determine the cause and resolve the issue using information in the log
files, contact Sun Technical Support.

4765: SSL_OptionSet(SSL_REQUEST_CERTIFICATE PR_TRUE) *return-code* error *error-code*
(*error-message*)
Cause: Failed to set the Client Authentication Required property.

Solution: If you cannot determine the cause and resolve the issue using information in the log
files, contact Sun Technical Support.

4767: Security Initialization: Cannot get SSL Server Authentication status. No
nsslserverauth in *DN* (error *error-code - error-message*).
Cause: Security Initialization: Cannot get SSL Server Authentication status. nsslserverauth
not found.

Solution: Add nsslserverauth attribute to the configuration if you want something other
than the default value.

4768: Security Initialization: Cannot set SSL Server Authentication status to
"*value*" error (*error-message*). Supported values are "weak" "cert" and "cncheck".
(error *error-code* - *error-message*).
   Cause: Security Initialization: Cannot set SSL Server Authentication status. Probable invalid
   value of nssslserverauth attribute.

   Solution: Make sure nssslserverauth has a valid value.

4770: Security Initialization: Failed to get cipher family information. Missing
nsssltoken or nssslpersonalityssl in *DN* (error *error-code* - *error-message*).
   Cause: Security Initialization: Failed to get cipher family information. Missing nsssltoken
   or nssslpersonalityssl attribute.

   Solution: Update your configuration information and try again.

4771: Security Initialization: Failed to get cipher family information. Missing
nsssltoken or nssslpersonalityssl in *DN* (error *error-code* - *error-message*).
   Cause: Security Initialization: Failed to get cipher family information. Missing nsssltoken
   or nssslpersonalityssl attribute.

   Solution: Update your configuration information and try again.

4993: Can't find task entry '*DN*'
   Cause: The entry related to that task is not found in the directory.

   Solution: Make sure that an entry exists for that task and try again.

5022: Can't modify task entry '*DN*'
   Cause: An error occurred when modifying the entry related to that task in order to update the
   task status.

   Solution: Check the task entry and try again.

5032: Entire cn=tasks tree not found.
   Cause: An error occurred when modifying the entry related to that task in order to update the
   task status.

   Solution: Check the task entry and try again.

5033: Entries in cn=tasks tree not found.
   Cause: An error occurred when modifying the entry related to that task in order to update the
   task status.

   Solution: Check the task entry and try again.

5125: *funtion-name*: `ignoring multiple values for` *attribute* `in entry` *DN*
Cause: Resource limit. Multiple values found when setting new limit.

Solution: Check that the entry used to set the limit contains only one value.

5902: `Removed option "`*option*`" from allowed attribute type "`*attribute*`" in object class "`*object-class*`"`
Cause: The specified schema definition has a problem.

Solution: Fix the schema definition.

5903: `Removed option "`*option*`" from required attribute type "`*attribute*`" in object class "`*object-class*`"`
Cause: The specified schema definition has a problem.

Solution: Fix the schema definition.

5904: `X-ORIGIN contains no value (`*schema-definition*`)`
Cause: The specified schema definition has a problem.

Solution: Fix the schema definition.

5905: `X-DS-USE contains no value (`*schema-definition*`)`
Cause: The specified schema definition has a problem.

Solution: Fix the schema definition.

8193: `ruv_to_values: NULL argument`
Cause: It is likely that either the replication configuration is broken or the consumer is not initialized.

Solution: Verify the replica object and the replication agreement.

10242: `Value` *value* `invalid (Range is 1..65535).`
Cause: The replication window size is incorrect.

Solution: Fix the configuration.

10243: `Value` *value* `invalid (Range is 1..255)`
Cause: The replication group size is incorrect.

Solution: Fix the configuration.

10244: Value *value* invalid (Range is 1..255)
   Cause: The replication compression level is incorrect.

   Solution: Fix the configuration.

10245: Deletion of the *name* attribute is not allowed
   Cause: The specified attribute cannot be deleted.

   Solution: None.

10246: Event *event* should not occur in state *state*; going to sleep
   Cause: The replica is waiting for a replication protocol window to open.

   Solution: None.

10246: Event *event* should not occur in state *state*
   Cause: The replica is waiting for a replication protocol window to open.

   Solution: None.

10247: Unable to replicate schema to host *host* port *number*. Closing this replication session.
   Cause: Replication is proceeding normally. A timeout temporarily prevented replication from continuing.

   Solution: None.

10250: Warning *number* during acquire for [*replica*]
   Cause: The consumer was busy when this supplier tried to perform replication.

   Solution: None.

10251: Failed to release the current replication session [*host*:*port*]
   Cause: The supplier could not release locked consumer replica IDs at this time.

   Solution: None.

10252: Failed to end the current replication session [*host*:*port*]
   Cause: The supplier failed to end a replication session at this time.

   Solution: None.

10252: Failed to end the current replication session (nothing to acquired)
[*host*:*port*]
   Cause: Replication is proceeding normally.

   Solution: None.

10252: Failed to end the current replication session (no lock acquired)
[*host*:*port*]
   Cause: The supplier could not lock consumer replica IDs at this time.

   Solution: None.

10258: Invalid parameter passed to cl5CreateReplayIterator while servicing
replication agreement "*DN*"
   Cause: An internal error occurred.

   Solution: Initialize the replica again.

10258: Unexpected format encountered in changelog database while servicing
replication agreement "*DN*"
   Cause: An internal error occurred.

   Solution: Initialize the replica again.

10258: Changelog database is in an incorrect state while servicing replication
agreement "*DN*" (cl5CreateReplayIterator)
   Cause: An internal error occurred.

   Solution: Initialize the replica again.

10258: Incorrect dbversion found in changelog database while servicing
replication agreement "*DN*"
   Cause: An internal error occurred.

   Solution: Initialize the replica again.

10258: A database error is encountered while servicing replication agreement
"*DN*"
   Cause: An internal error occurred.

   Solution: Initialize the replica again.

10258: Internal error (*error-code*) while servicing replication agreement "*DN*"
Cause: An internal error occurred.

Solution: Initialize the replica again.

10261: Deletion of the *name* attribute is not allowed
Cause: The specified attribute cannot be deleted.

Solution: None.

10263: overwrite referral flag is set for replica "*replica*" but no referral is
configured. Using default computed referrals
Cause: The nsDS5Flags is set to overwrite default referrals but no referral was configured.

Solution: Check the configuration.

10264: This server will be referring client updates for replica *name* during the
following *seconds* s
Cause: This supplier was recently initialized for this replica. As a preventive measure, it refers client updates to make sure that it is updated by all other masters in the topology with any missing changes before starting to accept updates.

Solution: No action needed. The server starts accepting client updates after the Referral Period specified in the warning message is elapsed. If you want your server to receive client updates from now on instead of waiting for the Referral Period to expire, set the ds5BeginReplicaAcceptUpdates attribute inside the cn=replica entry for this replica to the value start. Before making the change, verify that the server is up to date in terms of replication and that it has not missed any change previously originated in this server before it was initialized.

10265: This server will be referring client updates for replica *name*
indefinitely
Cause: This supplier was recently initialized for this replica. As a preventive measure, it refers client updates to make sure that it is updated by all other masters on the topology with any missing changes before starting to accept updates.

Solution: The server will not start accepting client updates until you add or replace the ds5BeginReplicaAcceptUpdates attribute inside the cn=replica entry for this replica with the value start. Before making the change, verify that the server is up to date in terms of replication and that it has not missed any change previously originated in this server before it was initialized.

10266: replica_write_ruv: failed to update RUV tombstone for replica (*name* LDAP error - *error-code*
> **Cause:** Problem writing an attribute value inside the replica update vector storage entry.

> **Solution:** If the problem persists, restart Directory Server.

10267: search_in_ruv_storage_entry: replica ruv tombstone entry for replica *name* not found
> **Cause:** Problem reading the RUV storage entry stored inside the suffix DB.

> **Solution:** If the replica is still participating in replication, initialize it again.

10268: The agreement *DN* was disabled the consumer has no more data
> **Cause:** A consumer initialization was ongoing while the replication agreement got aborted.

> **Solution:** restart the total update after enabling the replication agreement.

10273: Changelog was already opened
> **Cause:** The server tried to open the changelog though it was already open.

> **Solution:** None.

10274: Failed to parse ldif line
> **Cause:** The server could not read an LDIF entry.

> **Solution:** See the errors log for more information.

10278: Value *value* invalid (Range is 1..65535)
> **Cause:** The replication group packet size is incorrect.

> **Solution:** Fix the configuration.

10279: Value *value* invalid (Range is 0..3)
> **Cause:** The replication concurrency level is incorrect.

> **Solution:** Fix the configuration.

10280: An entry has been converted into a glue entry with DN *DN*
> **Cause:** An entry has been converted as part of multimaster replication conflict resolution.

> **Solution:** None.

10281: A tombstone entry has been resurrected as a glue entry with DN *DN*
> **Cause:** An entry has been resurrected as part of multimaster replication conflict resolution.

> **Solution:** None.

10282: [C] Invalid state of replication connection extension : Not started
Cause: The server noticed it tried to initiate a replication session without starting it.

Solution: None.

10282: [C] Invalid state of replication connection extension : Suspended
Cause: The server noticed it tried to initiate a replication session that was suspended.

Solution: None.

10283: [C] Session detected to be busy (state *state number* threads used *number* operations)
Cause: The server noticed the replication session was busy.

Solution: None.

10284: [C] Unable to release replica
Cause: The server was not able to release replica ID locks.

Solution: None.

10285: Replication already started for agreement "*DN*"
Cause: An attempt was made to start replication although replication had already been initialized.

Solution: None.

10286: Supplier has a new replication version (*version*) than us (*version*)
Cause: The supplier replica uses a more recent (but backward compatible) version of the replication protocol than the consumer.

Solution: None.

10287: [C] No extension data while cleaning session connection extension
Cause: The server found no data in the extension when closing the session.

Solution: None.

10288: csn *CSN* sequence number *number* ignoring it
Cause: The server found a change sequence number that does not affect its replication operation.

Solution: None.

10289: Removing dependency op=*number*
    Cause: The server is cleaning up dependencies left over from earlier replication sessions.

    Solution: None.

10306: Incremental update session aborted : Timeout while waiting for change
acknowledgement [*host*:*port*]
    Cause: Timeout while waiting for change acknowledgement.

    Solution: Check the consumer errors log for more information.

10307: DB ruv could not be recreated
    Cause: The server could not create the replication update vector from the database, and may reinitialize the changelog.

    Solution: None.

10308: Unable to reinitialize changelog file
    Cause: The changelog could not be reinitialized or removed.

    Solution: None.

10309: Fractional Replication configuration for *DN* can not define both include
and exclude attributes. Include attributes are taken into account by default.
    Cause: The fractional replication configuration is broken.

    Solution: Fix the configuration.

10309: Fractional Replication configuration for *replica* can not define both
include and exclude attributes.
    Cause: The fractional replication configuration is broken.

    Solution: Fix the configuration.

12303: SLAPI_DESTROY_CONTENT field obsolete.
    Cause: A plug-in uses the deprecated SLAPI_DESTROY_CONTENT field.

    Solution: Fix the plug-in.

33810: Failed to index classic cos scheme Def(*DN*) Template(*DN*) Attr(*name*)
reason(*message*)
    Cause: Failed to add the indicated classic COS template to a fast lookup hash table for the reason given.

Solution: Check the indicated COS definition and template for configuration errors. Check the syntax and value of the indicated attribute for errors.

33814: Definition *DN* and definition *DN* compete to provide attribute *'name'* at priority *number*
Cause: CoS processing is resolving competing definitions.

Solution: None.

33815: Definition *DN* and definition *DN* compete to provide attribute *'name'* at priority *number* Templates *'DN' 'DN'*
Cause: CoS processing is resolving competing definitions.

Solution: None.

34821: Error: This (*ACI*) ACL will not be considered for evaluation because of syntax errors.
Cause: Ignoring this access control instruction due to errors.

Solution: Try again with a correct aci.

34825: ACL internal db error detected: exiting acllist *list* evaluation at aci *ACI*
Cause: ACL detected internal database error.

Solution: None: server should recover itself and execute operation correctly.

34837: ACL syntax error: *operation* (*message*)
Cause: ACL parsing error: the reason and the string containing the error is logged.

Solution: Correct the error in the aci and try the aci update operation again.

34839: ACL internal db error detected: exiting userattr (*name*) evaluation at level *number*
Cause: ACL detected internal database error.

Solution: None: server should recover itself and execute operation correctly.

34840: ACL internal db error detected: exiting group evaluation (acllas_user_is_member_of_group) at group *DN*
Cause: ACL detected internal database error.

Solution: None: server should recover itself and execute operation correctly.

34841: ACL internal db error detected: exiting *ACI* evaluation
Cause: ACL detected internal database error.

Solution: None: server should recover itself and execute operation correctly.

37975: dictionary htable is full last *number* words not inserted
Cause: The server could not load the entire dictionary file used by the password check plug-in.

Solution: None.

37977: Invalid Policy Value. Setting to default
Cause: The value provided to the password check plug-in to specify the character set requirements is not correct.

Solution: Provide an acceptable value for pwd-strong-check-require-charset using the dsconf command.

38924: The value of SASL attribute dsSaslMinSSF in dse.ldif is not in the correct range. Default value of 0 will be used instead
Cause: Value for SASL attribute dsSaslMinSSF is not in the valid range.

Solution: Configure a value between 0 and 32767.

38925: The value of SASL attribute dsSaslMaxSSF in dse.ldif is not in the correct range. Default value of 32767 will be used instead
Cause: Value for SASL attribute dsSaslMaxSSF is not in the valid range.

Solution: Configure a value between 0 and 32767.

Verifying Plug-In Signatures

Plug-ins provided with Directory Server each have a digital signature which may be verified by the server at startup. By default, the server verifies plug-in signatures, but proceeds to load every plug-in regardless of the presence or validity of a signature.

Verifying signatures has the following advantages.

- A signature on a plug-in provided with Directory Server indicates that it has been rigorously tested and is officially supported.

- Using a checksum of the plug-in binary itself, the signature verification can detect whether the plug-in has been tampered with. Therefore the signature protects sensitive code that runs in the server itself.

- You may configure your server to load only the signed plug-ins, which may help detect problems with unsigned and unsupported plug-ins.

▼ To Force Directory Server to Verify Plug-Ins are Signed

1 **Set the** `ds-verify-plugin-signature` **in** `cn=config` **to** `on`**.**

2 **Restart Directory Server.**
The server logs an error message if any plug-in does not have a signature.

▼ To Force Directory Server to Validate Plug-In Signatures

1 **Set the** `ds-verify-plugin-signature` **in** `cn=config` **to** `on`**.**

2 **Set the** `ds-require-valid-plugin-signatures` **in** `cn=config` **to** `on`**.**

3 **Restart Directory Server.**
The server does not start if any plug-in is not signed or a signature is invalid.

Index