

**Red Hat Directory Server 8.0**

**8.0**

# **Configuration, Command, and File Reference**

**ISBN: N/A**

**Publication date:**

## Red Hat Directory Server 8.0

---

This Reference documents the server configuration and command-line utilities provided with Red Hat Directory Server 8.0.



---

# Red Hat Directory Server 8.0: Configuration, Command, and File Reference

Copyright © 2008 Red Hat, Inc.

Copyright © You need to override this in your local ent file Red Hat. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later with the restrictions noted below (the latest version of the OPL is presently available at <http://www.opencontent.org/openpub/>).

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive  
Raleigh, NC 27606-2072  
USA  
Phone: +1 919 754 3700  
Phone: 888 733 4281  
Fax: +1 919 754 3701  
PO Box 13588  
Research Triangle Park, NC 27709  
USA

---



---

About This Reference .....	vii
1. Directory Server Overview .....	vii
2. Other Reading .....	vii
3. Document Conventions .....	viii
4. We Need Feedback! .....	x
1. Introduction .....	1
1. Directory Server Configuration .....	1
2. Directory Server Instance File Reference .....	1
3. Using Directory Server Command-Line Utilities .....	1
4. Using Directory Server Command-Line Scripts .....	1
2. Core Server Configuration Reference .....	3
1. Server Configuration - Overview .....	3
2. Accessing and Modifying Server Configuration .....	8
3. Core Server Configuration Attributes Reference .....	11
3. Plug-in Implemented Server Functionality Reference .....	107
1. Server Plug-in Functionality Reference .....	107
2. List of Attributes Common to All Plug-ins .....	127
3. Attributes Allowed by Certain Plug-ins .....	129
4. Database Plug-in Attributes .....	131
5. Database Link Plug-in Attributes (Chaining Attributes) .....	158
6. Retro Changelog Plug-in Attributes .....	167
4. Server Instance File Reference .....	171
1. Overview of Directory Server Files .....	171
2. Backup Files .....	173
3. Configuration Files .....	173
4. Database Files .....	173
5. LDIF Files .....	175
6. Lock Files .....	176
7. Log Files .....	176
8. PID Files .....	177
9. Tools .....	177
10. Scripts .....	178
5. Access Log and Connection Code Reference .....	179
1. Access Log Content .....	179
2. Common Connection Codes .....	191
3. LDAP Result Codes .....	192
6. Command-Line Utilities .....	195
1. Finding and Executing Command-Line Utilities .....	195
2. Using Special Characters .....	195
3. Command-Line Utilities Quick Reference .....	196
4. Idapsearch .....	197
5. Idapmodify .....	214
6. Idapdelete .....	221
7. Idappasswd .....	227
8. Idif .....	234
9. dbscan .....	235

- 7. Command-Line Scripts .....241
  - 1. Finding and Executing Command-Line Scripts .....241
  - 2. Command-Line Scripts Quick Reference .....241
  - 3. Shell Scripts .....243
  - 4. Perl Scripts .....259
- A. Using the ns-slapd Command-Line Utilities .....277
  - 1. Overview of ns-slapd .....277
  - 2. Finding and Executing the ns-slapd Command-Line Utilities .....277
  - 3. Utilities for Exporting Databases: db2ldif .....277
  - 4. Utilities for Restoring and Backing up Databases: ldif2db .....279
  - 5. Utilities for Restoring and Backing up Databases: archive2db .....281
  - 6. Utilities for Restoring and Backing up Databases: db2archive .....282
  - 7. Utilities for Creating and Regenerating Indexes: db2index .....282
- B. Revision History .....285
- Glossary .....287
- Index .....305

---

## About This Reference

Red Hat Directory Server (Directory Server) is a powerful and scalable distributed directory server based on the industry-standard Lightweight Directory Access Protocol (LDAP). Directory Server is the cornerstone for building a centralized and distributed data repository that can be used in an intranet, over an extranet with trading partners, or over the public Internet to reach customers.

This reference covers the server configuration and the command-line utilities. It is designed primarily for directory administrators and experienced directory users who want to use the command-line to access the directory. After configuring the server, use this reference to help maintain it.

The Directory Server can also be managed through the Directory Server Console, a graphical user interface. The *Red Hat Directory Server Administration Guide* describes how to do this and explains individual administration tasks more fully.

## 1. Directory Server Overview

The major components of Directory Server include:

- An LDAP server – The LDAP v3-compliant network daemon.
- Directory Server Console – A graphical management console that dramatically reduces the effort of setting up and maintaining your directory service.
- SNMP agent – Can monitor the Directory Server using the Simple Network Management Protocol (SNMP).
- Directory Gateway – A web application which allows users to search for information in the Directory Server, in addition to providing self service access to their own information, including password changes, to reduce user support costs.
- Org Chart – A web application which shows a graphical view of the structure of your organization.

## 2. Other Reading

This reference does not describe many of the basic directory and architectural concepts to design, implement, and administer the directory service successfully. Those concepts are described in the *Red Hat Directory Server Administration Guide*. Read that book before continuing with this reference.

After becoming familiar with Directory Server concepts and doing some preliminary planning for the directory service, install the Directory Server. The instructions for installing the Directory Server components are contained in the *Red Hat Directory Server Installation Guide*.

This book is a reference guide for the server configuration and the command-line utilities. It is

designed primarily for directory administrators and experienced directory users who want to use the command line to access the directory. After configuring the server, use this reference guide to maintain it.

The document set for Directory Server also contains the following guides:

- *Red Hat Directory Server Release Notes* - Contains important information on new features, fixed bugs, known issues and work arounds, and other important deployment information for this specific version of Directory Server.
- *Red Hat Directory Server Installation Guide*. Contains procedures for installing Directory Server as well as procedures for migrating the Directory Server.
- *Red Hat Directory Server Administration Guide*. Contains procedures for the day-to-day maintenance of the directory service. Includes information on configuring server-side plug-ins.

For the latest information about Directory Server, including current release notes, complete product documentation, technical notes, and deployment information, see the Red Hat Directory Server documentation main page at <http://www.redhat.com/docs/manuals/dir-server/>.

### 3. Document Conventions

Certain words in this manual are represented in different fonts, styles, and weights. This highlighting indicates that the word is part of a specific category. The categories include the following:

Courier font

Courier font represents `commands`, `file names` and `paths`, and `prompts`.

When shown as below, it indicates computer output:

```
Desktop      about.html    logs          paulwesterberg.png
Mail         backupfiles  mail          reports
```

**Courier font**

**Courier font** represents text that you are to type, such as: `service jonas start`

If you have to run a command as root, the root prompt (`#`) precedes the command:

```
# gconftool-2
```

*italic Courier font*

Italic Courier font represents a variable, such as an installation directory:

```
install_dir/bin/
```

### bold font

Bold font represents **application programs** and **text found on a graphical interface**.

When shown like this: **OK** , it indicates a button on a graphical application interface.

Additionally, the manual uses different strategies to draw your attention to pieces of information. In order of how critical the information is to you, these items are marked as follows:



### Note

A note is typically information that you need to understand the behavior of the system.



### Tip

A tip is typically an alternative way of performing a task.



### Important

Important information is necessary, but possibly unexpected, such as a configuration change that will not persist after a reboot.



### Caution

A caution indicates an act that would violate your support agreement, such as recompiling the kernel.



### Warning

A warning indicates potential data loss, as may happen when tuning hardware for maximum performance.

## 4. We Need Feedback!

If you find a typographical error in this manual, or if you have thought of a way to make this manual better, we would love to hear from you! Please submit a report in Bugzilla: <http://bugzilla.redhat.com/bugzilla/> against the product **Red Hat Directory Server**.

When submitting a bug report, be sure to mention the manual's identifier: *Red Hat Directory Server 8.0*

If you have a suggestion for improving the documentation, try to be as specific as possible when describing it. If you have found an error, please include the section number and some of the surrounding text so we can find it easily.

# Introduction

Directory Server is based on an open-systems server protocol called the Lightweight Directory Access Protocol (LDAP). The Directory Server is a robust, scalable server designed to manage large scale directories to support an enterprise-wide directory of users and resources, extranets, and e-commerce applications over the Internet. The Directory Server runs as the `ns-slapd` process or service on the machine. The server manages the directory databases and responds to client requests.

This reference deals with the other methods of managing the Directory Server by altering the server configuration attributes using the command line and using command-line utilities and scripts.

## 1. Directory Server Configuration

The format and method for storing configuration information for Directory Server and a listing for all server attributes are found in two chapters, [Chapter 2, Core Server Configuration Reference](#) and [Chapter 3, Plug-in Implemented Server Functionality Reference](#).

## 2. Directory Server Instance File Reference

[Chapter 4, Server Instance File Reference](#) has an overview of the files and configuration information stored in each instance of Directory Server. This is useful reference to help administrators understand the changes or absence of changes in the course of directory activity. From a security standpoint, this also helps users detect errors and intrusion by highlighting normal changes and abnormal behavior.

## 3. Using Directory Server Command-Line Utilities

Directory Server comes with a set of configurable command-line utilities that can search and modify entries in the directory and administer the server. [Chapter 6, Command-Line Utilities](#) describes these command-line utilities and contains information on where the utilities are stored and how to access them. In addition to these command-line utilities, Directory Server also provides `ns-slapd` command-line utilities for performing directory operations, as described in [Appendix A, Using the ns-slapd Command-Line Utilities](#).

## 4. Using Directory Server Command-Line Scripts

In addition to command-line utilities, several non-configurable scripts are provided with the Directory Server that make it quick and easy to perform routine server administration tasks from the command-line. [Chapter 7, Command-Line Scripts](#) lists the most frequently used scripts and contains information on where the scripts are stored and how to access them.



# Core Server Configuration Reference

The configuration information for Red Hat Directory Server is stored as LDAP entries within the directory itself. Therefore, changes to the server configuration must be implemented through the use of the server itself rather than by simply editing configuration files. The principal advantage of this method of configuration storage is that it allows a directory administrator to reconfigure the server using LDAP while it is still running, thus avoiding the need to shut the server down for most configuration changes.

This chapter gives details on how the configuration is organized and how to alter it. The chapter also provides an alphabetical reference for all attributes.

## 1. Server Configuration - Overview

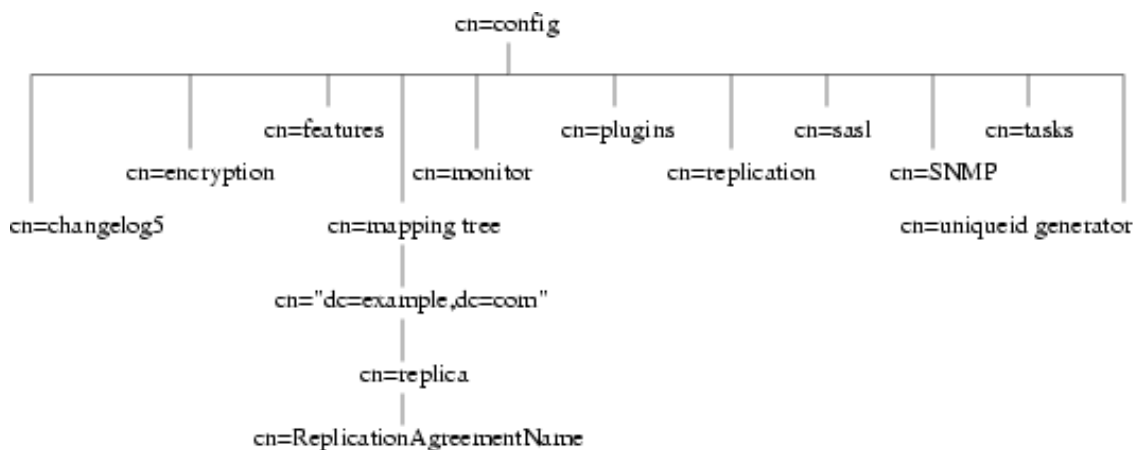
When the Directory Server is set up, its default configuration is stored as a series of LDAP entries within the directory, under the subtree `cn=config`. When the server is started, the contents of the `cn=config` subtree are read from a file (`dse.ldif`) in LDIF format. This `dse.ldif` file contains all of the server configuration information. The latest version of this file is called `dse.ldif`, the version prior to the last modification is called `dse.ldif.bak`, and the latest file with which the server successfully started is called `dse.ldif.startOK`.

Many of the features of the Directory Server are designed as discrete modules that plug into the core server. The details of the internal configuration for each plug-in are contained in separate entries under `cn=plugins,cn=config`. For example, the configuration of the Telephone Syntax Plug-in is contained in this entry:

```
cn=Telephone Syntax,cn=plugins,cn=config
```

Similarly, database-specific configuration is stored under `cn=ldbm` `database,cn=plugins,cn=config` for local databases and `cn=chaining` `database,cn=plugins,cn=config` for database links.

The following diagram illustrates how the configuration data fits within the `cn=config` directory information tree.



**Figure 2.1. Directory Information Tree Showing Configuration Data**

### 1.1. LDIF and Schema Configuration Files

The Directory Server configuration data is automatically output to files in LDIF format that are located in the `/var/lib/dirsrv/slapd-instance_name/ldif` directory on Red Hat Enterprise Linux and Solaris and `/var/opt/dirsrv/slapd-serverID/ldif` on HP-UX. Thus, if a server identifier is `phonebook`, then for a Directory Server on Red Hat Enterprise Linux 5, the configuration LDIF files are all stored under `/var/lib/dirsrv/slapd-phonebook/ldif`.

This directory also contains other server instance-specific configuration files.

Schema configuration is also stored in LDIF format, and these files are located in `/etc/dirsrv/slapd-instance_name/schema`.

The following table lists all of the configuration files that are supplied with the Directory Server, including those for the schema of other compatible servers. Each file is preceded by a number which indicates the order in which they should be loaded (in ascending numerical and then alphabetical order).

Configuration Filename	Purpose
dse.ldif	Contains front-end Directory Specific Entries created by the directory at server startup. These include the Root DSE (" ") and the contents of <code>cn=config</code> and <code>cn=monitor</code> (acis only).
00core.ldif	Contains only those schema definitions necessary for starting the server with the bare minimum feature set (no user schema, no schema for any non-core features). The rest of the schema used by users, features, and applications is found in <code>01common.ldif</code> and the other schema files. Do not modify this file.

Configuration Filename	Purpose
01common.ldif	Contains LDAPv3 standard operational schema, such as <code>subschemaSubentry</code> , LDAPv3 standard user and organization schema defined in RFC 2256 (based on X.520/X.521), <code>inetOrgPerson</code> and other widely-used attributes, and the operational attributes used by Directory Server configuration. Modifying this file causes interoperability problems. User-defined attributes should be added through the Directory Server Console.
05rfc2247.ldif	Schema from RFC 2247 and related pilot schema, from "Using Domains in LDAP/X500 Distinguished Names."
05rfc2927.ldif	Schema from RFC 2927, "MIME Directory Profile for LDAP Schema." Contains the <code>ldapSchemas</code> operational attribute required for the attribute to show up in the <code>subschema</code> subentry.
10presence.ldif	Legacy. Schema for instant messaging presence (online) information; the file lists the default object classes with the allowed attributes that must be added to a user's entry in order for instant-messaging presence information to be available for that user.
10rfc2307.ldif	Schema from RFC 2307, "An Approach for Using LDAP as a Network Information Service." This may be superseded by <code>10rfc2307bis</code> , the new version of <code>rfc2307</code> , when that schema becomes available.
20subscriber.ldif	Contains new schema elements and the Nortel subscriber interoperability specification. Also contains the <code>adminRole</code> and <code>memberOf</code> attributes and <code>inetAdmin</code> object class, previously stored in the <code>50ns-delegated-admin.ldif</code> file.
25java-object.ldif	Schema from RFC 2713, "Schema for Representing Java® Objects in an LDAP Directory."
28pilot.ldif	Contains pilot directory schema from RFC 1274, which is no longer recommended for new deployments. Future RFCs which succeed RFC 1274 may deprecate some or

Configuration Filename	Purpose
	all of <code>28pilot.ldif</code> attribute types and classes.
<code>30ns-common.ldif</code>	Schema that contains objects classes and attributes common to the Directory Server Console framework.
<code>50ns-admin.ldif</code>	Schema used by Red Hat Administration Server.
<code>50ns-certificate.ldif</code>	Schema for Red Hat Certificate Management System.
<code>50ns-directory.ldif</code>	Contains additional configuration schema used by Directory Server 4.12 and earlier versions of the directory, which is no longer applicable to current releases of Directory Server. This schema is required for replicating between Directory Server 4.12 and current releases.
<code>50ns-mail.ldif</code>	Schema used by Netscape Messaging Server to define mail users and mail groups.
<code>50ns-value.ldif</code>	Schema for servers' value item attributes.
<code>50ns-web.ldif</code>	Schema for Netscape Web Server.
<code>60pam-plugin.ldif</code>	Reserved for future use.
<code>99user.ldif</code>	User-defined schema maintained by Directory Server replication consumers which contains the attributes and object classes from the suppliers.

**Table 2.1. Directory Server LDIF Configuration Files**

### 1.2. How the Server Configuration Is Organized

The `dse.ldif` file contains all configuration information including directory-specific entries created by the directory at server startup, such as entries related to the database. The file includes the root Directory Server entry (or DSE, named by `" "`) and the contents of `cn=config` and `cn=monitor`.

When the server generates the `dse.ldif` file, it lists the entries in hierarchical order in the order that the entries appear in the directory under `cn=config`, which is usually the same order in which an LDAP search of subtree scope for base `cn=config` returns the entries.

`dse.ldif` also contains the `cn=monitor` entry, which is mostly read-only, but can have ACIs set on it.



### NOTE

The `dse.ldif` file does not contain every attribute in `cn=config`. If the attribute has not been set by the administrator and has a default value, the server will not write it to `dse.ldif`. To see every attribute in `cn=config`, use `ldapsearch`.

### 1.2.1. Configuration Attributes

Within a configuration entry, each attribute is represented as an attribute name. The value of the attribute corresponds to the attribute's configuration.

The following code sample is an example of part of the `dse.ldif` file for a Directory Server. The example shows, among other things, that schema checking has been enabled; this is represented by the attribute `nsslapd-schemacheck`, which takes the value `on`.

```
dn: cn=config
objectclass: top
objectclass: extensibleObject
objectclass: nsslapdConfig
nsslapd-accesslog-logging-enabled: on
nsslapd-enquote-sup-oc: off
nsslapd-localhost: phonebook.example.com
nsslapd-schemacheck: on
nsslapd-port: 389
nsslapd-localuser: nobody
...
```

### 1.2.2. Configuration of Plug-in Functionality

The configuration for each part of Directory Server plug-in functionality has its own separate entry and set of attributes under the subtree `cn=plugins,cn=config`. The following code sample is an example of the configuration entry for an example plug-in, the Telephone Syntax plug-in.

```
dn: cn=Telephone Syntax,cn=plugins,cn=config
objectclass: top
objectclass: nsSlapdPlugin
objectclass: extensibleObject
cn: Telephone Syntax
nsslapd-pluginType: syntax
nsslapd-pluginEnabled: on
```

Some of these attributes are common to all plug-ins, and some may be particular to a specific plug-in. Check which attributes are currently being used by a given plug-in by performing an

ldapsearch on the `cn=config` subtree.

For a list of plug-ins supported by Directory Server, general plug-in configuration information, the plug-in configuration attribute reference, and a list of plug-ins requiring restart for configuration changes, see [Chapter 3, Plug-in Implemented Server Functionality Reference](#).

### 1.2.3. Configuration of Databases

The `cn=NetscapeRoot` and `cn=UserRoot` subtrees under the database plug-in entry contain configuration data for the databases containing the `o=NetscapeRoot` suffix and the default suffix created during setup, such as `dc=example,dc=com`.

These entries and their children have many attributes used to configure different database settings, like the cache sizes, the paths to the index files and transaction logs, entries and attributes for monitoring and statistics; and database indexes.

### 1.2.4. Configuration of Indexes

Configuration information for indexing is stored as entries in the Directory Server under the following information-tree nodes:

- `cn=index,cn=NetscapeRoot,cn=ldb database,cn=plugins,cn=config`
- `cn=index,cn=UserRoot,cn=ldb database,cn=plugins,cn=config`
- `cn=default indexes,cn=config,cn=ldb database,cn=plugins,cn=config`

For more information about indexes in general, see the *Directory Server Administration Guide*. For information about the index configuration attributes, see [Section 4.1, “Database Attributes under `cn=config`, `cn=ldb database`, `cn=plugins`, `cn=config`”](#).

## 2. Accessing and Modifying Server Configuration

This section discusses access control for configuration entries and describes the various ways in which the server configuration can be viewed and modified. It also covers restrictions to the kinds of modification that can be made and discusses attributes that require the server to be restarted for changes to take effect.

### 2.1. Access Control for Configuration Entries

When the Directory Server is installed, a default set of access control instructions (ACIs) is implemented for all entries under `cn=config`. The following code sample is an example of these default ACIs.

```
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrators
Group"; allow (all)
    groupdn = "ldap:///cn=Configuration Administrators,u=Groups,
ou=TopologyManagement, o=NetscapeRoot";)
```

```
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator";
allow (all)
    userdn = "ldap:///uid=admin, ou=Administrators, ou=TopologyManagement,
o=NetscapeRoot");
aci: (targetattr = "*")(version 3.0; acl "Local Directory Administrators
Group"; allow (all)
    groupdn = "ldap:///ou=Directory Administrators, dc=example,dc=com");
aci: (targetattr = "*")(version 3.0; acl "SIE Group"; allow(all)
    groupdn = "ldap:///cn=slapd-phonebook, cn=Red Hat Directory Server,
cn=Server Group, cn=phonebook.example.com, dc=example,dc=com,
o=NetscapeRoot");
```

These default ACIs allow all LDAP operations to be carried out on all configuration attributes by the following users:

- Members of the Configuration Administrators group.
- The user acting as the administrator, the `admin` account that was configured at setup. By default, this is the same user account which is logged into the Console.
- Members of local Directory Administrators group.
- The SIE (Server Instance Entry) group, usually assigned using the **Set Access Permissions** process the main console.

For more information on access control, see the *Directory Server Administration Guide*.

## 2.2. Changing Configuration Attributes

Server attributes can be viewed and changed in one of three ways: through the Directory Server Console, by performing `ldapsearch` and `ldapmodify` commands, or by manually editing the `dse.ldif` file.



### NOTE

Before editing the `dse.ldif` file, the server *must* be stopped; otherwise, the changes are lost. Editing the `dse.ldif` file is recommended only for changes to attributes which cannot be altered dynamically. See [Section 2.2.3, “Configuration Changes Requiring Server Restart”](#) for further information.

The following sections describe how to modify entries using LDAP (both by using Directory Server Console and by using the command line), the restrictions that apply to modifying entries, the restrictions that apply to modifying attributes, and the configuration changes requiring restart.

### 2.2.1. Modifying Configuration Entries Using LDAP

The configuration entries in the directory can be searched and modified using LDAP either via the Directory Server Console or by performing `ldapsearch` and `ldapmodify` operations in the same way as other directory entries. The advantage of using LDAP to modify entries is changes can be made while the server is running.

For further information, see the "Creating Directory Entries" chapter in the *Directory Server Administration Guide*. However, certain changes do require the server to be restarted before they are taken into account. See [Section 2.2.3, "Configuration Changes Requiring Server Restart"](#) for further information.



#### NOTE

As with any set of configuration files, care should be taken when changing or deleting nodes in the `cn=config` subtree as this risks affecting Directory Server functionality.

The entire configuration, including attributes that always take default values, can be viewed by performing an `ldapsearch` operation on the `cn=config` subtree:

```
ldapsearch -b cn=config -D bindDN -w password
```

- `bindDN` is the DN chosen for the Directory Manager when the server was installed (`cn=Directory Manager` by default).
- `password` is the password chosen for the Directory Manager.

For more information on using `ldapsearch`, see [Section 4, "ldapsearch"](#).

To disable a plug-in, use `ldapmodify` to edit the `nsslapd-pluginEnabled` attribute:

```
ldapmodify -D cn="directory manager" -w password
dn: cn=Telephone Syntax,cn=plugins,cn=config
changetype: modify
replace: nsslapd-pluginEnabled
nsslapd-pluginEnabled: off
```

### 2.2.2. Restrictions to Modifying Configuration Entries and Attributes

Certain restrictions apply when modifying server entries and attributes:

- The `cn=monitor` entry and its child entries are read-only and cannot be modified, except to manage ACIs.
- If an attribute is added to `cn=config`, the server ignores it.
- If an invalid value is entered for an attribute, the server ignores it.
- Because `ldapdelete` is used for deleting an entire entry, use `ldapmodify` to remove an attribute from an entry.

### 2.2.3. Configuration Changes Requiring Server Restart

Some configuration attributes cannot be altered while the server is running. In these cases, for the changes to take effect, the server needs to be shut down and restarted. The modifications should be made either through the Directory Server Console or by manually editing the `dse.ldif` file. Some of the attributes that require a server restart for any changes to take effect are listed below. This list is not exhaustive; to see a complete list, run `ldapsearch` and search for the `nsslapd-requiresrestart` attribute. For example:

```
ldapsearch -p 389 -D "cn=directory manager" -w password -s sub -b
"cn=config"
  "(objectclass=*)" | grep nsslapd-requiresrestart
```

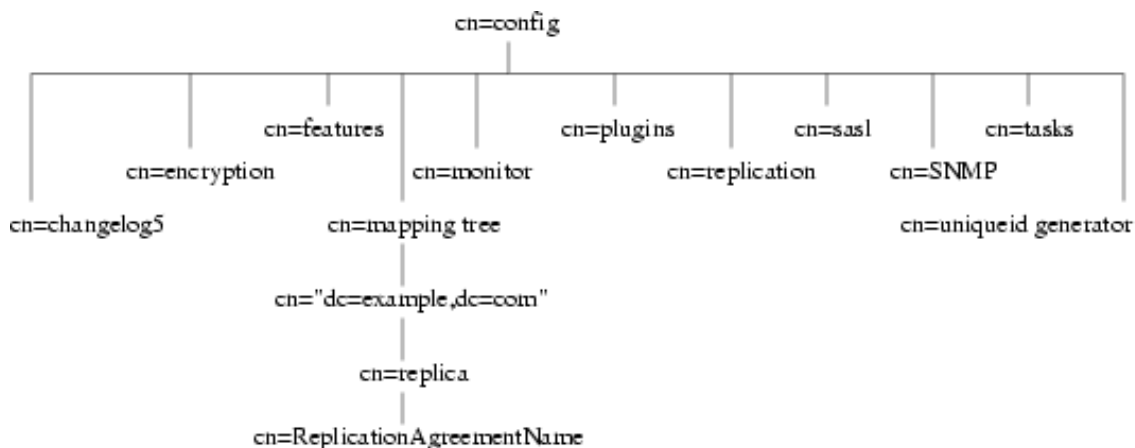
<code>nsslapd-cachesize</code>	<code>nsslapd-certdir</code>
<code>nsslapd-dbcachesize</code>	<code>nsslapd-dbncache</code>
<code>nsslapd-plugin</code>	<code>nsslapd-changelogdir</code>
<code>nsslapd-changelogmaxage</code>	<code>nsslapd-changelogmaxentries</code>
<code>nsslapd-port</code>	<code>nsslapd-schemadir</code>
<code>nsslapd-saslpath</code>	<code>nsslapd-secureport</code>
<code>nsslapd-tmpdir</code>	<code>nsSSL2</code>
<code>nsSSL3</code>	<code>nsSSLclientauth</code>
<code>nsSSLSessionTimeout</code>	<code>nsslapd-conntablesizesize</code>
<code>nsslapd-lockdir</code>	<code>nsslapd-maxdescriptors</code>
<code>nsslapd-reservedescriptors</code>	<code>nsslapd-listenhost</code>
<code>nsslapd-schema-ignore-trailing-spaces</code>	<code>nsslapd-securelistenhost</code>
<code>nsslapd-workingdir</code>	<code>nsslapd-return-exact-case</code>

## 3. Core Server Configuration Attributes Reference

This section contains reference information on the configuration attributes that are relevant to the core server functionality. For information on changing server configuration, see [Section 2, “Accessing and Modifying Server Configuration”](#). For a list of server features that are

implemented as plug-ins, see [Section 1, “Server Plug-in Functionality Reference”](#). For help with implementing custom server functionality, contact Directory Server support.

The configuration information stored in the `dse.ldif` file is organized as an information tree under the general configuration entry `cn=config`, as shown in the following diagram.



**Figure 2.2. Directory Information Tree Showing Configuration Data**

Most of these configuration tree nodes are covered in the following sections.

The `cn=plugins` node is covered in [Chapter 3, Plug-in Implemented Server Functionality Reference](#). The description of each attribute contains details such as the DN of its directory entry, its default value, the valid range of values, and an example of its use.



### NOTE

Some of the entries and attributes described in this chapter may change in future releases of the product.

## 3.1. cn=config

General configuration entries are stored in the `cn=config` entry. The `cn=config` entry is an instance of the `nsslapdConfig` object class, which in turn inherits from `extensibleObject` object class.

### 3.1.1. nsslapd-accesslog (Access Log)

This attribute specifies the path and filename of the log used to record each LDAP access. The following information is recorded by default in the log file:

- IP address of the client machine that accessed the database.

- Operations performed (for example, search, add, and modify).
- Result of the access (for example, the number of entries returned or an error code).

For more information on turning access logging off, see the "Monitoring Server and Database Activity" chapter in the *Directory Server Administration Guide*.

For access logging to be enabled, this attribute must have a valid path and parameter, and the `nsslapd-accesslog-logging-enabled` configuration attribute must be switched to `on`. The table lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of access logging.

Attribute	Value	Logging enabled or disabled
<code>nsslapd-accesslog-logging-enabled</code>	<code>off</code>	Disabled
<code>nsslapd-accesslog</code>	empty string	
<code>nsslapd-accesslog-logging-enabled</code>	<code>on</code>	Enabled
<code>nsslapd-accesslog</code>	<i>filename</i>	
<code>nsslapd-accesslog-logging-enabled</code>	<code>off</code>	Disabled
<code>nsslapd-accesslog</code>	empty string	
<code>nsslapd-accesslog-logging-enabled</code>	<code>on</code>	Disabled
<code>nsslapd-accesslog</code>	<i>filename</i>	

**Table 2.2. dse.ldif File Attributes**

Parameter	Description
Entry DN	<code>cn=config</code>
Valid Values	Any valid filename.
Default Value	<code>/var/log/dirsrv/slapd-<i>instance_name</i>/access</code>
Syntax	DirectoryString
Example	<code>nsslapd-accesslog: /var/log/dirsrv/slapd-<i>instance_name</i>/access</code>

### 3.1.2. nsslapd-accesslog-level

This attribute controls what is logged to the access log.

Parameter	Description
Entry DN	cn=config
Valid Values	<ul style="list-style-type: none"> <li>• 0 - No access logging</li> <li>• 4 - Logging for internal access operations</li> <li>• 256 - Logging for connections, operations, and results</li> <li>• 512 - Logging for access to an entry and referrals</li> <li>• 131072 - Provides microsecond operation timing</li> <li>• These values can be added together to provide the exact type of logging required; for example, 516 (4 + 512) to obtain internal access operation, entry access, and referral logging.</li> </ul>
Default Value	256
Syntax	Integer
Example	nsslapd-accesslog-level: 256

### 3.1.3. nsslapd-accesslog-list

This read-only attribute, which cannot be set, provides a list of access log files used in access log rotation.

Parameter	Description
Entry DN	cn=config
Valid Values	
Default Value	None
Syntax	DirectoryString
Example	nsslapd-accesslog-list: accesslog2,accesslog3

### 3.1.4. nsslapd-accesslog-logbuffering (Log Buffering)

When set to `off`, the server writes all access log entries directly to disk. Buffering allows the server to use access logging even when under a heavy load without impacting performance.

However, when debugging, it is sometimes useful to disable buffering in order to see the operations and their results right away instead of having to wait for the log entries to be flushed to the file. Disabling log buffering can severely impact performance in heavily loaded servers.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-accesslog-logbuffering: off

### 3.1.5. nsslapd-accesslog-logexpirationtime (Access Log Expiration Time)

This attribute specifies the maximum age that a log file is allowed to reach before it is deleted. This attribute supplies only the number of units. The units are provided by the *nsslapd-accesslog-logexpirationtimeunit* attribute.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	1
Syntax	Integer
Example	nsslapd-accesslog-logexpirationtime: 2

### 3.1.6. nsslapd-accesslog-logexpirationtimeunit (Access Log Expiration Time Unit)

This attribute specifies the units for *nsslapd-accesslog-logexpirationtime* attribute. If the unit is unknown by the server, then the log never expires.

Parameter	Description
Entry DN	cn=config
Valid Values	month   week   day
Default Value	month
Syntax	DirectoryString
Example	nsslapd-accesslog-logexpirationtimeunit: week

### 3.1.7. nsslapd-accesslog-logging-enabled (Access Log Enable Logging)

Disables and enables accesslog logging but only in conjunction with the *nsslapd-accesslog* attribute that specifies the path and parameter of the log used to record each database access.

For access logging to be enabled, this attribute must be switched to *on*, and the *nsslapd-accesslog* configuration attribute must have a valid path and parameter. The table lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of access logging.

Attribute	Value	Logging Enabled or Disabled
nsslapd-accesslog-logging-enabled	<i>off</i>	Disabled
nsslapd-accesslog	empty string	
nsslapd-accesslog-logging-enabled	<i>on</i>	Enabled
nsslapd-accesslog	<i>filename</i>	
nsslapd-accesslog-logging-enabled	<i>off</i>	Disabled
nsslapd-accesslog	empty string	
nsslapd-accesslog-logging-enabled	<i>on</i>	Disabled
nsslapd-accesslog	<i>filename</i>	

**Table 2.3. dse.ldif Attributes**

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-accesslog-logging-enabled: off

### 3.1.8. nsslapd-accesslog-logmaxdiskspace (Access Log Maximum Disk Space)

This attribute specifies the maximum amount of disk space in megabytes that the access logs are allowed to consume. If this value is exceeded, the oldest access log is deleted.

When setting a maximum disk space, consider the total number of log files that can be created due to log file rotation. Also, remember that there are three different log files (access log, audit log, and error log) maintained by the Directory Server, each of which consumes disk space. Compare these considerations to the total amount of disk space for the access log.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means that the disk space allowed to the access log is unlimited in size.
Default Value	500
Syntax	Integer
Example	nsslapd-accesslog-logmaxdiskpace: 200

### 3.1.9. nsslapd-accesslog-logminfreediskspace (Access Log Minimum Free Disk Space)

This attribute sets the minimum allowed free disk space in megabytes. When the amount of free disk space falls below the value specified on this attribute, the oldest access logs are deleted until enough disk space is freed to satisfy this attribute.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	5
Syntax	Integer
Example	nsslapd-accesslog-logminfreediskspace: 4

### 3.1.10. nsslapd-accesslog-logrotationsync-enabled (Access Log Rotation Sync Enabled)

This attribute sets whether access log rotation is to be synchronized with a particular time of the day. Synchronizing log rotation this way can generate log files at a specified time during a day, such as midnight to midnight every day. This makes analysis of the log files much easier because they then map directly to the calendar.

For access log rotation to be synchronized with time-of-day, this attribute must be enabled with the *nsslapd-accesslog-logrotationsynchour* and *nsslapd-accesslog-logrotationsyncmin* attribute values set to the hour and minute of the day for rotating log files.

For example, to rotate access log files every day at midnight, enable this attribute by setting its value to `on`, and then set the values of the `nsslapd-accesslog-logrotationsynchour` and `nsslapd-accesslog-logrotationsyncmin` attributes to `0`.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-accesslog-logrotationsync-enabled: on

### 3.1.11. nsslapd-accesslog-logrotationsynchour (Access Log Rotation Sync Hour)

This attribute sets the hour of the day for rotating access logs. This attribute must be used in conjunction with `nsslapd-accesslog-logrotationsync-enabled` and `nsslapd-accesslog-logrotationsyncmin` attributes.

Parameter	Description
Entry DN	cn=config
Valid Range	0 through 23
Default Value	0
Syntax	Integer
Example	nsslapd-accesslog-logrotationsynchour: 23

### 3.1.12. nsslapd-accesslog-logrotationsyncmin (Access Log Rotation Sync Minute)

This attribute sets the minute of the day for rotating access logs. This attribute must be used in conjunction with `nsslapd-accesslog-logrotationsync-enabled` and `nsslapd-accesslog-logrotationsynchour` attributes.

Parameter	Description
Entry DN	cn=config
Valid Range	0 through 59
Default Value	0
Syntax	Integer
Example	nsslapd-accesslog-logrotationsyncmin: 30

### 3.1.13. nsslapd-accesslog-logrotationtime (Access Log Rotation Time)

This attribute sets the time between access log file rotations. The access log is rotated when this time interval is up, regardless of the current size of the access log. This attribute supplies only the number of units. The units (day, week, month, and so forth) are given by the *nsslapd-accesslog-logrotationtimeunit* attribute.

Although it is not recommended for performance reasons to specify no log rotation since the log grows indefinitely, there are two ways of specifying this. Either set the *nsslapd-accesslog-maxlogsperdir* attribute value to 1 or set the *nsslapd-accesslog-logrotationtime* attribute to -1. The server checks the *nsslapd-accesslog-maxlogsperdir* attribute first, and, if this attribute value is larger than 1, the server then checks the *nsslapd-accesslog-logrotationtime* attribute. See [Section 3.1.16, “nsslapd-accesslog-maxlogsperdir \(Access Log Maximum Number of Log Files\)”](#) for more information.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means that the time between access log file rotation is unlimited.
Default Value	1
Syntax	Integer
Example	nsslapd-accesslog-logrotationtime: 100

### 3.1.14. nsslapd-accesslog-logrotationtimeunit (Access Log Rotation Time Unit)

This attribute sets the units for the *nsslapd-accesslog-logrotationtime* attribute.

Parameter	Description
Entry DN	cn=config
Valid Values	month   week   day   hour   minute
Default Value	day
Syntax	DirectoryString
Example	nsslapd-accesslog-logrotationtimeunit: week

### 3.1.15. nsslapd-accesslog-maxlogsize (Access Log Maximum Log Size)

This attribute sets the maximum access log size in megabytes. When this value is reached, the access log is rotated. That means the server starts writing log information to a new log file. If the `nsslapd-accesslog-maxlogsperdir` attribute is set to `1`, the server ignores this attribute.

When setting a maximum log size, consider the total number of log files that can be created due to log file rotation. Also, remember that there are three different log files (access log, audit log, and error log) maintained by the Directory Server, each of which consumes disk space.

Compare these considerations to the total amount of disk space for the access log.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means the log file is unlimited in size.
Default Value	100
Syntax	Integer
Example	nsslapd-accesslog-maxlogsize: 100

### 3.1.16. nsslapd-accesslog-maxlogsperdir (Access Log Maximum Number of Log Files)

This attribute sets the total number of access logs that can be contained in the directory where the access log is stored. Each time the access log is rotated, a new log file is created. When the number of files contained in the access log directory exceeds the value stored in this attribute, then the oldest version of the log file is deleted. For performance reasons, Red Hat recommends *not* setting this value to `1` because the server does not rotate the log, and it grows indefinitely.

If the value for this attribute is higher than `1`, then check the `nsslapd-accesslog-logrotationtime` attribute to establish whether log rotation is specified. If the `nsslapd-accesslog-logrotationtime` attribute has a value of `-1`, then there is no log rotation. See [Section 3.1.13, “nsslapd-accesslog-logrotationtime \(Access Log Rotation Time\)”](#) for more information.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	10
Syntax	Integer
Example	nsslapd-accesslog-maxlogsperdir: 10

### 3.1.17. nsslapd-accesslog-mode (Access Log File Permission)

This attribute sets the access mode or file permission with which access log files are to be created. The valid values are any combination of 000 to 777 (these mirror the numbered or absolute UNIX file permissions). The value must be a 3-digit number, the digits varying from 0 through 7:

- 0 - None
- 1 - Execute only
- 2 - Write only
- 3 - Write and execute
- 4 - Read only
- 5 - Read and execute
- 6 - Read and write
- 7 - Read, write, and execute

In the 3-digit number, the first digit represents the owner's permissions, the second digit represents the group's permissions, and the third digit represents everyone's permissions. When changing the default value, remember that 000 does not allow access to the logs and that allowing write permissions to everyone can result in the logs being overwritten or deleted by anyone.

The newly configured access mode only affects new logs that are created; the mode is set when the log rotates to a new file.

Parameter	Description
Entry DN	cn=config
Valid Range	000 through 777
Default Value	600
Syntax	Integer
Example	nsslapd-accesslog-mode: 600

### 3.1.18. nsslapd-attribute-name-exceptions

This attribute allows non-standard characters in attribute names to be used for backwards compatibility with older servers, such as "\_" in schema-defined attributes.

Parameter	Description
Entry DN	cn=config

Parameter	Description
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-attribute-name-exceptions: on

### 3.1.19. nsslapd-auditlog (Audit Log)

This attribute sets the path and filename of the log used to record changes made to each database.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid filename
Default Value	/var/log/dirsrv/slapd- <i>instance_name</i> /audit
Syntax	DirectoryString
Example	nsslapd-auditlog: /var/log/dirsrv/slapd- <i>instance_name</i> /audit

For audit logging to be enabled, this attribute must have a valid path and parameter, and the *nsslapd-auditlog-logging-enabled* configuration attribute must be switched to `on`. The table lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of audit logging.

Attributes in dse.ldif	Value	Logging enabled or disabled
nsslapd-auditlog-logging-enabledn nsslapd-auditlog	empty string	Disabled
nsslapd-auditlog-logging-enabledn nsslapd-auditlog	<i>filename</i>	Enabled
nsslapd-auditlog-logging-enabledff nsslapd-auditlog	empty string	Disabled
nsslapd-auditlog-logging-enabledff nsslapd-auditlog	<i>filename</i>	Disabled

**Table 2.4. Possible Combinations for nsslapd-auditlog****3.1.20. nsslapd-auditlog-list**

Provides a list of audit log files.

Parameter	Description
Entry DN	cn=config
Valid Values	
Default Value	None
Syntax	DirectoryString
Example	nsslapd-auditlog-list: auditlog2,auditlog3

**3.1.21. nsslapd-auditlog-logexpirationtime (Audit Log Expiration Time)**

This attribute sets the maximum age that a log file is allowed to be before it is deleted. This attribute supplies only the number of units. The units (day, week, month, and so forth) are given by the *nsslapd-auditlog-logexpirationtimeunit* attribute.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	1
Syntax	Integer
Example	nsslapd-auditlog-logexpirationtime: 1

**3.1.22. nsslapd-auditlog-logexpirationtimeunit (Audit Log Expiration Time Unit)**

This attribute sets the units for the *nsslapd-auditlog-logexpirationtime* attribute. If the unit is unknown by the server, then the log never expires.

Parameter	Description
Entry DN	cn=config
Valid Values	month   week   day
Default Value	week
Syntax	DirectoryString

Parameter	Description
Example	nsslapd-auditlog-logexpirationtimeunit: day

### 3.1.23. nsslapd-auditlog-logging-enabled (Audit Log Enable Logging)

Turns audit logging on and off.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-auditlog-logging-enabled: off

For audit logging to be enabled, this attribute must have a valid path and parameter and the *nsslapd-auditlog-logging-enabled* configuration attribute must be switched to `on`. The table lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of audit logging.

Attribute	Value	Logging enabled or disabled
nsslapd-auditlog-logging-enabledn nsslapd-auditlog	empty string	Disabled
nsslapd-auditlog-logging-enabledn nsslapd-auditlog	<i>filename</i>	Enabled
nsslapd-auditlog-logging-enabledff nsslapd-auditlog	empty string	Disabled
nsslapd-auditlog-logging-enabledff nsslapd-auditlog	<i>filename</i>	Disabled

**Table 2.5. Possible combinations for nsslapd-auditlog and nsslapd-auditlog-logging-enabled**

### 3.1.24. nsslapd-auditlog-logmaxdiskspace (Audit Log Maximum Disk

## Space)

This attribute sets the maximum amount of disk space in megabytes that the audit logs are allowed to consume. If this value is exceeded, the oldest audit log is deleted.

When setting a maximum disk space, consider the total number of log files that can be created due to log file rotation. Also remember that there are three different log files (access log, audit log, and error log) maintained by the Directory Server, each of which consumes disk space. Compare these considerations with the total amount of disk space for the audit log.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means that the disk space allowed to the audit log is unlimited in size.
Default Value	500
Syntax	Integer
Example	nsslapd-auditlog-logmaxdiskspace: 500

### 3.1.25. nsslapd-auditlog-logminfreediskspace (Audit Log Minimum Free Disk Space)

This attribute sets the minimum permissible free disk space in megabytes. When the amount of free disk space falls below the value specified by this attribute, the oldest audit logs are deleted until enough disk space is freed to satisfy this attribute.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	5
Syntax	Integer
Example	nsslapd-auditlog-logminfreediskspace: 3

### 3.1.26. nsslapd-auditlog-logrotationsync-enabled (Audit Log Rotation Sync Enabled)

This attribute sets whether audit log rotation is to be synchronized with a particular time of the day. Synchronizing log rotation this way can generate log files at a specified time during a day, such as midnight to midnight every day. This makes analysis of the log files much easier because they then map directly to the calendar.

For audit log rotation to be synchronized with time-of-day, this attribute must be enabled with the *nsslapd-auditlog-logrotationsynchour* and *nsslapd-auditlog-logrotationsyncmin* attribute values set to the hour and minute of the day for rotating log files.

For example, to rotate audit log files every day at midnight, enable this attribute by setting its value to `on`, and then set the values of the *nsslapd-auditlog-logrotationsynchour* and *nsslapd-auditlog-logrotationsyncmin* attributes to `0`.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-auditlog-logrotationsync-enabled: on

### 3.1.27. nsslapd-auditlog-logrotationsynchour (Audit Log Rotation Sync Hour)

This attribute sets the hour of the day for rotating audit logs. This attribute must be used in conjunction with *nsslapd-auditlog-logrotationsync-enabled* and *nsslapd-auditlog-logrotationsyncmin* attributes.

Parameter	Description
Entry DN	cn=config
Valid Range	0 through 23
Default Value	None (because <i>nsslapd-auditlog-logrotationsync-enabled</i> is off)
Syntax	Integer
Example	nsslapd-auditlog-logrotationsynchour: 23

### 3.1.28. nsslapd-auditlog-logrotationsyncmin (Audit Log Rotation Sync Minute)

This attribute sets the minute of the day for rotating audit logs. This attribute must be used in conjunction with *nsslapd-auditlog-logrotationsync-enabled* and *nsslapd-auditlog-logrotationsynchour* attributes.

Parameter	Description
Entry DN	cn=config
Valid Range	0 through 59

Parameter	Description
Default Value	None (because <i>nsslapd-auditlog-logrotationsync-enabled</i> is off)
Syntax	Integer
Example	<i>nsslapd-auditlog-logrotationsyncmin</i> : 30

### 3.1.29. *nsslapd-auditlog-logrotationtime* (Audit Log Rotation Time)

This attribute sets the time between audit log file rotations. The audit log is rotated when this time interval is up, regardless of the current size of the audit log. This attribute supplies only the number of units. The units (day, week, month, and so forth) are given by the *nsslapd-auditlog-logrotationtimeunit* attribute. If the *nsslapd-auditlog-maxlogsperdir* attribute is set to 1, the server ignores this attribute.

Although it is not recommended for performance reasons to specify no log rotation, as the log grows indefinitely, there are two ways of specifying this. Either set the *nsslapd-auditlog-maxlogsperdir* attribute value to 1 or set the *nsslapd-auditlog-logrotationtime* attribute to -1. The server checks the *nsslapd-auditlog-maxlogsperdir* attribute first, and, if this attribute value is larger than 1, the server then checks the *nsslapd-auditlog-logrotationtime* attribute. See [Section 3.1.32, “\*nsslapd-auditlog-maxlogsperdir\* \(Audit Log Maximum Number of Log Files\)”](#) for more information.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means that the time between audit log file rotation is unlimited.
Default Value	1
Syntax	Integer
Example	<i>nsslapd-auditlog-logrotationtime</i> : 100

### 3.1.30. *nsslapd-auditlog-logrotationtimeunit* (Audit Log Rotation Time Unit)

This attribute sets the units for the *nsslapd-auditlog-logrotationtime* attribute.

Parameter	Description
Entry DN	cn=config
Valid Values	month   week   day   hour   minute

Parameter	Description
Default Value	week
Syntax	DirectoryString
Example	nsslapd-auditlog-logrotationtimeunit: day

### 3.1.31. nsslapd-auditlog-maxlogsize (Audit Log Maximum Log Size)

This attribute sets the maximum audit log size in megabytes. When this value is reached, the audit log is rotated. That means the server starts writing log information to a new log file. If *nsslapd-auditlog-maxlogsperdir* to 1, the server ignores this attribute.

When setting a maximum log size, consider the total number of log files that can be created due to log file rotation. Also, remember that there are three different log files (access log, audit log, and error log) maintained by the Directory Server, each of which consumes disk space. Compare these considerations to the total amount of disk space for the audit log.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means the log file is unlimited in size.
Default Value	100
Syntax	Integer
Example	nsslapd-auditlog-maxlogsize: 50

### 3.1.32. nsslapd-auditlog-maxlogsperdir (Audit Log Maximum Number of Log Files)

This attribute sets the total number of audit logs that can be contained in the directory where the audit log is stored. Each time the audit log is rotated, a new log file is created. When the number of files contained in the audit log directory exceeds the value stored on this attribute, then the oldest version of the log file is deleted. The default is 1 log. If this default is accepted, the server will not rotate the log, and it grows indefinitely.

If the value for this attribute is higher than 1, then check the *nsslapd-auditlog-logrotationtime* attribute to establish whether log rotation is specified. If the *nsslapd-auditlog-logrotationtime* attribute has a value of -1, then there is no log rotation. See [Section 3.1.29, “nsslapd-auditlog-logrotationtime \(Audit Log Rotation Time\)”](#) for more information.

Parameter	Description
Entry DN	cn=config

Parameter	Description
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	1
Syntax	Integer
Example	nsslapd-auditlog-maxlogspdir: 10

### 3.1.33. nsslapd-auditlog-mode (Audit Log File Permission)

This attribute sets the access mode or file permissions with which audit log files are to be created. The valid values are any combination of 000 to 777 since they mirror numbered or absolute UNIX file permissions. The value must be a combination of a 3-digit number, the digits varying from 0 through 7:

- 0 - None
- 1 - Execute only
- 2 - Write only
- 3 - Write and execute
- 4 - Read only
- 5 - Read and execute
- 6 - Read and write
- 7 - Read, write, and execute

In the 3-digit number, the first digit represents the owner's permissions, the second digit represents the group's permissions, and the third digit represents everyone's permissions. When changing the default value, remember that 000 does not allow access to the logs and that allowing write permissions to everyone can result in the logs being overwritten or deleted by anyone.

The newly configured access mode only affects new logs that are created; the mode is set when the log rotates to a new file.

Parameter	Description
Entry DN	cn=config
Valid Range	000 through 777
Default Value	600
Syntax	Integer

Parameter	Description
Example	nsslapd-auditlog-mode: 600

### 3.1.34. nsslapd-certdir (Certificate and Key Database Directory)

This is the full path to the directory holding the certificate and key databases for a Directory Server instance. This directory must contain only the certificate and key databases for this instance and no other instances. This directory must be owned and allow read-write access for the server user ID. No other user should have read-right access to this directory. The default location is the configuration file directory, `/etc/dirsrv/slapd-instance_name`.

Changes to this value will not take effect until the server is restarted.

Parameter	Description
Entry DN	cn=config
Valid Values	Absolute path to any directory which is owned by the server user ID and only allows read and write access to the server user ID
Default Value	<code>/etc/dirsrv/slapd-<i>instance_name</i></code>
Syntax	DirectoryString
Example	<code>/etc/dirsrv/slapd-phonebook</code>

### 3.1.35. nsslapd-certmap-basedn (Certificate Map Search Base)

This attribute can be used when client authentication is performed using SSL certificates in order to avoid limitations of the security subsystem certificate mapping, configured in the `certmap.conf` file. Depending on the `certmap.conf` configuration, the certificate mapping may be done using a directory subtree search based at the root DN. If the search is based at the root DN, then the `nsslapd-certmap-basedn` attribute may force the search to be based at some entry other than the root. The valid value for this attribute is the DN of the suffix or subtree to use for certificate mapping. For further information on configuring for SSL, see the "Managing SSL" chapter in the *Directory Server Administration Guide*.

### 3.1.36. nsslapd-config

This read-only attribute is the config DN.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid configuration DN
Default Value	
Syntax	DirectoryString

Parameter	Description
Example	nsslapd-config: cn=config

### 3.1.37. nsslapd-conntablesize

This attribute sets the connection table size, which determines the total number of connections supported by the server.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config
Valid Values	Operating-system dependent
Default Value	The default value is the system's max descriptors, which can be configured using the <a href="#">Section 3.1.67, "nsslapd-maxdescriptors (Maximum File Descriptors)"</a> attribute.
Syntax	Integer
Example	nsslapd-conntablesize: 4093

Increase the value of this attribute if Directory Server is refusing connections because it is out of connection slots. When this occurs, the Directory Server's error log file records the message `Not listening for new connections -- too many fds open.`

A server restart is required for the change to take effect.

It may be necessary to increase the operating system limits for the number of open files and number of open files per process, and it may be necessary to increase the `ulimit` for the number of open files (`ulimit -n`) in the shell that starts the Directory Server. See [Section 3.1.67, "nsslapd-maxdescriptors \(Maximum File Descriptors\)"](#) for more information.

### 3.1.38. nsslapd-csnlogging

This attribute sets whether change sequence numbers (CSNs), when available, are to be logged in the access log. By default, CSN logging is turned on.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-csnlogging: on

### 3.1.39. nsslapd-ds4-compatible-schema

Makes the schema in `cn=schema` compatible with 4.x versions of Directory Server.

Parameter	Description
Entry DN	<code>cn=config</code>
Valid Values	<code>on</code>   <code>off</code>
Default Value	<code>off</code>
Syntax	DirectoryString
Example	<code>nsslapd-ds4-compatible-schema: off</code>

### 3.1.40. nsslapd-enquote-sup-oc (Enable Superior Object Class Enquoting)

This attribute is deprecated and will be removed in a future version of Directory Server.

This attribute controls whether quoting in the `objectclass` attributes contained in the `cn=schema` entry conforms to the quoting specified by Internet draft RFC 2252. By default, the Directory Server conforms to RFC 2252, which indicates that this value should not be quoted. Only very old clients need this value set to `on`, so leave it `off`.

Turning this attribute on or off does not affect Directory Server Console.

Parameter	Description
Entry DN	<code>cn=config</code>
Valid Values	<code>on</code>   <code>off</code>
Default Value	<code>off</code>
Syntax	DirectoryString
Example	<code>nsslapd-enquote-sup-oc: off</code>

### 3.1.41. nsslapd-errorlog (Error Log)

This attribute sets the path and filename of the log used to record error messages generated by the Directory Server. These messages can describe error conditions, but more often they contain informative conditions, such as:

- Server startup and shutdown times.
- The port number that the server uses.

This log contains differing amounts of information depending on the current setting of the Log Level attribute. See [Section 3.1.42, “nsslapd-errorlog-level \(Error Log Level\)”](#) for more

information.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid filename
Default Value	/var/log/dirsrv/slaped- <i>instance_name</i> /errors
Syntax	DirectoryString
Example	nsslapd-errorlog: /var/log/dirsrv/slaped- <i>instance_name</i> /errors

For error logging to be enabled, this attribute must have a valid path and filename, and the *nsslapd-errorlog-logging-enabled* configuration attribute must be switched to `on`. The table lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of error logging.

Attributes in dse.ldif	Value	Logging enabled or disabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	on empty string	Disabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	on <i>filename</i>	Enabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	off empty string	Disabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	off <i>filename</i>	Disabled

**Table 2.6. Possible Combinations for nsslapd-errorlog Configuration Attributes**

### 3.1.42. nsslapd-errorlog-level (Error Log Level)

This attribute sets the level of logging for the Directory Server. The log level is additive; that is, specifying a value of 3 includes both levels 1 and 2.

The default value for *nsslapd-errorlog-level* is 16384.

Parameter	Description
Entry DN	cn=config
Valid Values	<ul style="list-style-type: none"> <li>• 1 — Trace function calls. Logs a message when the server enters and exits a function.</li> <li>• 2 — Debug packet handling.</li> <li>• 4 — Heavy trace output debugging.</li> <li>• 8 — Connection management.</li> <li>• 16 — Print out packets sent/received.</li> <li>• 32 — Search filter processing.</li> <li>• 64 — Config file processing.</li> <li>• 128 — Access control list processing.</li> <li>• 2048 — Log entry parsing debugging.</li> <li>• 4096 — Housekeeping thread debugging.</li> <li>• 8192 — Replication debugging.</li> <li>• 16384 — Default level of logging used for critical errors and other messages that are always written to the error log; for example, server startup messages. Messages at this level are always included in the error log, regardless of the log level setting.</li> <li>• 32768 — Database cache debugging.</li> <li>• 65536 — Server plug-in debugging. It writes an entry to the log file when a server plug-in calls <code>slapi-log-error</code>.</li> <li>• 131072 — Microsecond resolution for timestamps instead of the default seconds.</li> <li>• 262144 — Access control summary information, much less verbose than level 128. This value is recommended for use when a summary of access control processing is needed. Use 128 for very detailed processing messages.</li> </ul>

Parameter	Description
Default Value	16384
Syntax	Integer
Example	nsslapd-errorlog-level: 8192

### 3.1.43. nsslapd-errorlog-list

This read-only attribute provides a list of error log files.

Parameter	Description
Entry DN	cn=config
Valid Values	
Default Value	None
Syntax	DirectoryString
Example	nsslapd-errorlog-list: errorlog2,errorlog3

### 3.1.44. nsslapd-errorlog-logexpirationtime (Error Log Expiration Time)

This attribute sets the maximum age that a log file is allowed to reach before it is deleted. This attribute supplies only the number of units. The units (day, week, month, and so forth) are given by the *nsslapd-errorlog-logexpirationtimeunit* attribute.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	1
Syntax	Integer
Example	nsslapd-errorlog-logexpirationtime: 1

### 3.1.45. nsslapd-errorlog-logexpirationtimeunit (Error Log Expiration Time Unit)

This attribute sets the units for the *nsslapd-errorlog-logexpirationtime* attribute. If the unit is unknown by the server, then the log never expires.

Parameter	Description
Entry DN	cn=config
Valid Values	month   week   day

Parameter	Description
Default Value	month
Syntax	DirectoryString
Example	nsslapd-errorlog-logexpirationtimeunit: week

### 3.1.46. nsslapd-errorlog-logging-enabled (Enable Error Logging)

Turns error logging on and off.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-errorlog-logging-enabled: on

### 3.1.47. nsslapd-errorlog-logmaxdiskpace (Error Log Maximum Disk Space)

This attribute sets the maximum amount of disk space in megabytes that the error logs are allowed to consume. If this value is exceeded, the oldest error log is deleted.

When setting a maximum disk space, consider the total number of log files that can be created due to log file rotation. Also, remember that there are three different log files (access log, audit log, and error log) maintained by the Directory Server, each of which consumes disk space. Compare these considerations to the total amount of disk space for the error log.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means that the disk space allowed to the error log is unlimited in size.
Default Value	500
Syntax	Integer
Example	nsslapd-errorlog-logmaxdiskpace: 500

### 3.1.48. nsslapd-errorlog-logminfreediskpace (Error Log Minimum Free Disk Space)

This attribute sets the minimum allowed free disk space in megabytes. When the amount of free disk space falls below the value specified on this attribute, the oldest error log is deleted until enough disk space is freed to satisfy this attribute.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	5
Syntax	Integer
Example	nsslapd-errorlog-logminfreediskspace: 5

### 3.1.49. nsslapd-errorlog-logrotationsync-enabled (Error Log Rotation Sync Enabled)

This attribute sets whether error log rotation is to be synchronized with a particular time of the day. Synchronizing log rotation this way can generate log files at a specified time during a day, such as midnight to midnight every day. This makes analysis of the log files much easier because they then map directly to the calendar.

For error log rotation to be synchronized with time-of-day, this attribute must be enabled with the *nsslapd-errorlog-logrotationsynchour* and *nsslapd-errorlog-logrotationsyncmin* attribute values set to the hour and minute of the day for rotating log files.

For example, to rotate error log files every day at midnight, enable this attribute by setting its value to *on*, and then set the values of the *nsslapd-errorlog-logrotationsynchour* and *nsslapd-errorlog-logrotationsyncmin* attributes to 0.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-errorlog-logrotationsync-enabled: on

### 3.1.50. nsslapd-errorlog-logrotationsynchour (Error Log Rotation Sync Hour)

This attribute sets the hour of the day for rotating error logs. This attribute must be used in conjunction with *nsslapd-errorlog-logrotationsync-enabled* and *nsslapd-errorlog-logrotationsyncmin* attributes.

Parameter	Description
Entry DN	cn=config
Valid Range	0 through 23
Default Value	0
Syntax	Integer
Example	nsslapd-errorlog-logrotationsynchour: 23

### 3.1.51. nsslapd-errorlog-logrotationsyncmin (Error Log Rotation Sync Minute)

This attribute sets the minute of the day for rotating error logs. This attribute must be used in conjunction with *nsslapd-errorlog-logrotationsync-enabled* and *nsslapd-errorlog-logrotationsynchour* attributes.

Parameter	Description
Entry DN	cn=config
Valid Range	0 through 59
Default Value	0
Syntax	Integer
Example	nsslapd-errorlog-logrotationsyncmin: 30

### 3.1.52. nsslapd-errorlog-logrotationtime (Error Log Rotation Time)

This attribute sets the time between error log file rotations. The error log is rotated when this time interval is up, regardless of the current size of the error log. This attribute supplies only the number of units. The units (day, week, month, and so forth) are given by the *nsslapd-errorlog-logrotationtimeunit* (Error Log Rotation Time Unit) attribute.

Although it is not recommended for performance reasons to specify no log rotation, as the log grows indefinitely, there are two ways of specifying this. Either set the *nsslapd-errorlog-maxlogsperdir* attribute value to 1 or set the *nsslapd-errorlog-logrotationtime* attribute to -1. The server checks the *nsslapd-errorlog-maxlogsperdir* attribute first, and, if this attribute value is larger than 1, the server then checks the *nsslapd-errorlog-logrotationtime* attribute. See [Section 3.1.55, “nsslapd-errorlog-maxlogsperdir \(Maximum Number of Error Log Files\)”](#) for more information.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647), where a value of -1 means that the time between error log file rotation is unlimited).

Parameter	Description
Default Value	1
Syntax	Integer
Example	nsslapd-errorlog-logrotationtime: 100

### 3.1.53. nsslapd-errorlog-logrotationtimeunit (Error Log Rotation Time Unit)

This attribute sets the units for *nsslapd-errorlog-logrotationtime* (Error Log Rotation Time). If the unit is unknown by the server, then the log never expires.

Parameter	Description
Entry DN	cn=config
Valid Values	month   week   day   hour   minute
Default Value	week
Syntax	DirectoryString
Example	nsslapd-errorlog-logrotationtimeunit: day

### 3.1.54. nsslapd-errorlog-maxlogsize (Maximum Error Log Size)

This attribute sets the maximum error log size in megabytes. When this value is reached, the error log is rotated, and the server starts writing log information to a new log file. If *nsslapd-errorlog-maxlogspedir* is set to 1, the server ignores this attribute.

When setting a maximum log size, consider the total number of log files that can be created due to log file rotation. Also, remember that there are three different log files (access log, audit log, and error log) maintained by the Directory Server, each of which consumes disk space. Compare these considerations to the total amount of disk space for the error log.

Parameter	Description
Entry DN	cn=config
Valid Range	-1   1 to the maximum 32 bit integer value (2147483647) where a value of -1 means the log file is unlimited in size.
Default Value	100
Syntax	Integer
Example	nsslapd-errorlog-maxlogsize: 100

### 3.1.55. nsslapd-errorlog-maxlogspedir (Maximum Number of Error Log Files)

This attribute sets the total number of error logs that can be contained in the directory where the error log is stored. Each time the error log is rotated, a new log file is created. When the number of files contained in the error log directory exceeds the value stored on this attribute, then the oldest version of the log file is deleted. The default is 1 log. If this default is accepted, the server does not rotate the log, and it grows indefinitely.

If the value for this attribute is higher than 1, then check the *nsslapd-errorlog-logrotationtime* attribute to establish whether log rotation is specified. If the *nsslapd-errorlog-logrotationtime* attribute has a value of -1, then there is no log rotation. See [Section 3.1.52, “nsslapd-errorlog-logrotationtime \(Error Log Rotation Time\)”](#) for more information.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647)
Default Value	1
Syntax	Integer
Example	nsslapd-errorlog-maxlogspedir: 10

### 3.1.56. nsslapd-errorlog-mode (Error Log File Permission)

This attribute sets the access mode or file permissions with which error log files are to be created. The valid values are any combination of 000 to 777 since they mirror numbered or absolute UNIX file permissions. That is, the value must be a combination of a 3-digit number, the digits varying from 0 through 7:

- 0 - None
- 1 - Execute only
- 2 - Write only
- 3 - Write and execute
- 4 - Read only
- 5 - Read and execute
- 6 - Read and write
- 7 - Read, write, and execute

In the 3-digit number, the first digit represents the owner's permissions, the second digit represents the group's permissions, and the third digit represents everyone's permissions. When changing the default value, remember that 000 does not allow access to the logs and that

allowing write permissions to everyone can result in the logs being overwritten or deleted by anyone.

The newly configured access mode only affects new logs that are created; the mode is set when the log rotates to a new file.

Parameter	Description
Entry DN	cn=config
Valid Range	000 through 777
Default Value	600
Syntax	Integer
Example	nsslapd-errorlog-mode: 600

### 3.1.57. nsslapd-groupevalnestlevel

This attribute is deprecated, and documented here only for historical purposes.

The Access Control Plug-in does not use the value specified by the *nsslapd-groupevalnestlevel* attribute to set the number of levels of nesting that access control performs for group evaluation. Instead, the number of levels of nesting is hardcoded as 5.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 5
Default Value	5
Syntax	Integer
Example	nsslapd-groupevalnestlevel: 5

### 3.1.58. nsslapd-idletimeout (Default Idle Timeout)

This attribute sets the amount of time in seconds after which an idle LDAP client connection is closed by the server. A value of 0 means that the server never closes idle connections. This setting applies to all connections and all users. Idle timeout is enforced when the connection table is walked, when `poll()` does not return zero. Therefore, a server with a single connection never enforces the idle timeout.

Use the *nsIdleTimeout* operational attribute, which can be added to user entries, to override the value assigned to this attribute. For details, see the "Setting Resource Limits Based on the Bind DN" section in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config

Parameter	Description
Valid Range	0 to the maximum 32 bit integer value (2147483647)
Default Value	0
Syntax	Integer
Example	nsslapd-idletimeout: 0

### 3.1.59. nsslapd-instancedir (Instance Directory)

This attribute is deprecated. There are now separate configuration parameters for instance-specific paths, such as *nsslapd-certdir* and *nsslapd-lockdir*. See the documentation for the specific directory path that is set.

### 3.1.60. nsslapd-ioblocktimeout (IO Block Time Out)

This attribute sets the amount of time in milliseconds after which the connection to a stalled LDAP client is closed. An LDAP client is considered to be stalled when it has not made any I/O progress for read or write operations.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to the maximum 32 bit integer value (2147483647) in ticks
Default Value	1800000
Syntax	Integer
Example	nsslapd-ioblocktimeout: 1800000

### 3.1.61. nsslapd-lastmod (Track Modification Time)

This attribute sets whether the Directory Server maintains the modification attributes for Directory Server entries. These are operational attributes. These attributes include:

- `modifiersname` - The distinguished name of the person who last modified the entry.
- `modifytimestamp` - The timestamp, in GMT format, for when the entry was last modified.
- `creatorsname` - The distinguished name of the person who initially created the entry.
- `createtimestamp` - The timestamp for when the entry was created in GMT format.

Parameter	Description
Entry DN	cn=config

Parameter	Description
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-lastmod: on



## WARNING

This attribute should never be turned off. If the `nsslapd-lastmod` is set to `off`, then generating `nsUniqueIDS` is also disabled, replication does not work, and other issues may arise.

If for some reason this attribute were set to `off`, the solution is to export the database to `ldif` (`db2ldif` or `db2ldif.pl` or from the console), set the value to `on`, and import the data. The import process assigns each entry a unique id.

### 3.1.62. nsslapd-listenhost (Listen to IP Address)

This attribute allows multiple Directory Server instances to run on a multihomed machine (or makes it possible to limit listening to one interface of a multihomed machine). There can be multiple IP addresses associated with a single hostname, and these IP addresses can be a mix of both IPv4 and IPv6. This parameter can be used to restrict the Directory Server instance to a single IP interface.

If a hostname is given as the `nsslapd-listenhost` value, then the Directory Server responds to requests for every interface associated with the hostname. If a single IP interface (either IPv4 or IPv6) is given as the `nsslapd-listenhost` value, Directory Server only responds to requests sent to that specific interface. Either an IPv4 or IPv6 address can be used.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config
Valid Values	Any local hostname, IPv4 or IPv6 address
Default Value	
Syntax	DirectoryString
Example	nsslapd-listenhost: ldap.example.com

**NOTE**

On HP-UX the hostname value can be a relocatable IP address.

### 3.1.63. nsslapd-localhost (Local Host)

This attribute specifies the host machine on which the Directory Server runs. This attribute is used to create the referral URL that forms part of the MMR protocol. In a high-availability configuration with failover nodes, that referral should point to the virtual name of the cluster, not the local hostname.

Parameter	Description
Entry DN	cn=config
Valid Values	Any fully qualified hostname.
Default Value	Hostname of installed machine.
Syntax	DirectoryString
Example	nsslapd-localhost: phonebook.example.com

### 3.1.64. nsslapd-localuser (Local User)

This attribute sets the user as whom the Directory Server runs. The group as which the user runs is derived from this attribute by examining the user's primary group. Should the user change, then all of the instance-specific files and directories for this instance need to be changed to be owned by the new user, using a tool such as `chown`.

The value for the `nsslapd-localuser` is set initially when the server instance is configured.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid user
Default Value	
Syntax	DirectoryString
Example	nsslapd-localuser: nobody

### 3.1.65. nsslapd-lockdir (Server Lock File Directory)

This is the full path to the directory the server uses for lock files. The default value is `/var/lock/dirsrv/slapd-instance_name`. Changes to this value will not take effect until the server is restarted.

Parameter	Description
Entry DN	cn=config
Valid Values	Absolute path to a directory owned by the server user ID with write access to the server ID
Default Value	<code>/var/lock/dirsrv/slapd-<i>instance_name</i></code>
Syntax	DirectoryString
Example	nsslapd-lockdir: <code>/var/lock/dirsrv/slapd-<i>instance_name</i></code>

### 3.1.66. nsslapd-maxbersize (Maximum Message Size)

Defines the maximum size in bytes allowed for an incoming message. This limits the size of LDAP requests that can be handled by the Directory Server. Limiting the size of requests prevents some kinds of denial of service attacks.

The limit applies to the total size of the LDAP request. For example, if the request is to add an entry and if the entry in the request is larger than two megabytes, then the add request is denied. Be cautious before changing this attribute, and Red Hat recommends contacting Directory Server support first.

Parameter	Description
Entry DN	cn=config
Valid Range	0 - 2 gigabytes (2,147,483,647 bytes)  Zero 0 means that the default value should be used.
Default Value	2097152
Syntax	Integer
Example	nsslapd-maxbersize: 2097152

### 3.1.67. nsslapd-maxdescriptors (Maximum File Descriptors)

This attribute sets the maximum, platform-dependent number of file descriptors that the Directory Server tries to use. A file descriptor is used whenever a client connects to the server and also for some server activities, such as index maintenance. File descriptors are also used by access logs, error logs, audit logs, database files (indexes and transaction logs), and as sockets for outgoing connections to other servers for replication and chaining.

The number of descriptors available for TCP/IP to serve client connections is determined by `nsslapd-conntablesizes`, and is equal to the `nsslapd-maxdescriptors` attribute minus the number of file descriptors used by the server as specified in the `nsslapd-reservedescriptors`

attribute for non-client connections, such as index management and managing replication. The `nsslapd-reservedescriptors` attribute is the number of file descriptors available for other uses as described above. See [Section 3.1.78, “nsslapd-reservedescriptors \(Reserved File Descriptors\)”](#).

The number given here should not be greater than the total number of file descriptors that the operating system allows the `ns-slapd` process to use. This number differs depending on the operating system.

If this value is set too high, the Directory Server queries the operating system for the maximum allowable value, and then use that value. It also issues a warning in the error log. If this value is set to an invalid value remotely, by using the Directory Server Console or `ldapmodify`, the server rejects the new value, keep the old value, and respond with an error.

Some operating systems let users configure the number of file descriptors available to a process. See the operating system documentation for details on file descriptor limits and configuration. The `dsktune` program (explained in the *Directory Server Installation Guide*) can be used to suggest changes to the system kernel or TCP/IP tuning attributes, including increasing the number of file descriptors if necessary. Increased the value on this attribute if the Directory Server is refusing connections because it is out of file descriptors. When this occurs, the following message is written to the Directory Server's error log file:

```
Not listening for new connections -- too many fds open
```

See [Section 3.1.37, “nsslapd-conntablesz”](#) for more information about increasing the number of incoming connections.



### NOTE

UNIX shells usually have configurable limits on the number of file descriptors. See the operating system documentation for further information about `limit` and `ulimit`, as these limits can often cause problems.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to 65535
Default Value	1024
Syntax	Integer
Example	nsslapd-maxdescriptors: 1024

### 3.1.68. nsslapd-maxthreadsperconn (Maximum Threads per Connection)

Defines the maximum number of threads that a connection should use. For normal operations where a client binds and only performs one or two operations before unbinding, use the default value. For situations where a client binds and simultaneously issues many requests, increase this value to allow each connection enough resources to perform all the operations. This attribute is not available from the server console.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to maximum threadnumber
Default Value	5
Syntax	Integer
Example	nsslapd-maxthreadsperconn: 5

### 3.1.69. nsslapd-nagle

When the value of this attribute is `off`, the `TCP_NODELAY` option is set so that LDAP responses (such as entries or result messages) are sent back to a client immediately. When the attribute is turned on, default TCP behavior applies; specifically, sending data is delayed so that additional data can be grouped into one packet of the underlying network MTU size, typically 1500 bytes for Ethernet.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-nagle: off

### 3.1.70. nsslapd-outbound-ldap-io-timeout

This attribute limits the I/O wait time for all outbound LDAP connections. The default is 300000 milliseconds (5 minutes). A value of 0 means that the server does not impose a limit on I/O wait time.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to the maximum 32 bit integer value (2147483647)

Parameter	Description
Default Value	300000
Syntax	DirectoryString
Example	nsslapd-outbound-ldap-io-timeout: 300000

### 3.1.71. nsslapd-plug-in

This read-only attribute lists the DNs of the plug-in entries for the syntax and matching rule plug-ins loaded by the server.

### 3.1.72. nsslapd-port (Port Number)

This attribute gives the TCP/IP port number used for standard LDAP communications. To run SSL/TLS over this port, use the Start TLS extended operation. This selected port must be unique on the host system; make sure no other application is attempting to use the same port number. Specifying a port number of less than 1024 means the Directory Server has to be started as `root`.

The server sets its `uid` to the `nsslapd-localuser` value after startup. When changing the port number for a configuration directory, the corresponding server instance entry in the configuration directory must be updated.

The server has to be restarted for the port number change to be taken into account.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to 65535
Default Value	389
Syntax	Integer
Example	nsslapd-port: 389



#### NOTE

Set the port number to zero (0) to disable the LDAP port if the LDAPS port is enabled.

### 3.1.73. nsslapd-privatenamespaces

This read-only attribute contains the list of the private naming contexts `cn=config`, `cn=schema`, and `cn=monitor`.

Parameter	Description
Entry DN	cn=config
Valid Values	cn=config, cn=schema, and cn=monitor
Default Value	
Syntax	DirectoryString
Example	nsslapd-privatenamespaces: cn=config

### 3.1.74. nsslapd-pwpolicy-local (Enable Subtree- and User-Level Password Policy)

Turns fine-grained (subtree- and user-level) password policy on and off.

If this attribute has a value of `off`, all entries (except for `cn=Directory Manager`) in the directory is subjected to the global ord policy; the server ignores any defined subtree/user level password policy.

If this attribute has a value of `on`, the server checks for password policies at the subtree- and user-level and enforce those policies.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-pwpolicy-local: off

### 3.1.75. nsslapd-readonly (Read Only)

This attribute sets whether the whole server is in read-only mode, meaning that neither data in the databases nor configuration information can be modified. Any attempt to modify a database in read-only mode returns an error indicating that the server is unwilling to perform the operation.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-readonly: off

### 3.1.76. nsslapd-referral (Referral)

This multi-valued attribute specifies the LDAP URLs to be returned by the suffix when the server receives a request for an entry not belonging to the local tree; that is, an entry whose suffix does not match the value specified on any of the suffix attributes. For example, assume the server contains only entries:

```
ou=People,dc=example,dc=com
```

but the request is for this entry:

```
ou=Groups,dc=example,dc=com
```

In this case, the referral would be passed back to the client in an attempt to allow the LDAP client to locate a server that contains the requested entry. Although only one referral is allowed per Directory Server instance, this referral can have multiple values.



#### NOTE

To use SSL and TLS communications, the referral attribute should be in the form `ldaps://server-location`.

Start TLS does not support referrals.

For more information on managing referrals, see the "Configuring Directory Databases" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid LDAP URL in the form <code>ldap://server-location</code>
Default Value	
Syntax	DirectoryString
Example	<code>nsslapd-referral: ldap://dap.example.com</code>

### 3.1.77. nsslapd-referralmode (Referral Mode)

When set, this attribute sends back the referral for any request on any suffix.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid LDAP URL in the form >ldap:// <i>server-location</i>
Default Value	
Syntax	DirectoryString
Example	nsslapd-referralmode: ldap://ldap.example.com

### 3.1.78. nsslapd-reservedescriptors (Reserved File Descriptors)

This attribute specifies the number of file descriptors that Directory Server reserves for managing non-client connections, such as index management and managing replication. The number of file descriptors that the server reserves for this purpose subtracts from the total number of file descriptors available for servicing LDAP client connections (See [Section 3.1.67](#), “*nsslapd-maxdescriptors (Maximum File Descriptors)*”).

Most installations of Directory Server should never need to change this attribute. However, consider increasing the value on this attribute if all of the following are true:

- The server is replicating to a large number of consumer servers (more than 10), and/or the server is maintaining a large number of index files (more than 30).
- The server is servicing a large number of LDAP connections.
- There are error messages reporting that the server is unable to open file descriptors (the actual error message differs depending on the operation that the server is attempting to perform), but these error messages are *not* related to managing client LDAP connections.

Increasing the value on this attribute may result in more LDAP clients being unable to access the directory. Therefore, the value on this attribute is increased, also increase the value on the *nsslapd-maxdescriptors* attribute. It may not be possible to increase the *nsslapd-maxdescriptors* value if the server is already using the maximum number of file descriptors that the operating system allows a process to use; see the operating system documentation for details. If this is the case, then reduce the load on the server by causing LDAP clients to search alternative directory replicas. See [Section 3.1.37](#), “*nsslapd-conntablesizes*” for information about file descriptor usage for incoming connections.

To assist in computing the number of file descriptors set for this attribute, use the following formula:

```
nsslapd-reservedescriptor = 20 + (NldbmBackends * 4) + NglobalIndex
+ ReplicationDescriptor + ChainingBackendDescriptors + PTADescriptors +
SSLDescriptors
```

- *NldbBackend*s is the number of ldbm databases.
- *NgloballIndex* is the total number of configured indexes for all databases including system indexes. (By default 8 system indexes and 17 additional indexes per database).
- *ReplicationDescriptor* is eight (8) plus the number of replicas in the server that can act as a supplier or hub (*NSupplierReplica*).
- *ChainingBackendDescriptors* is *NchainingBackend* times the *nsOperationConnectionsLimit* (a chaining or database link configuration attribute; 10 by default).
- *PTADescriptors* is 3 if PTA is configured and 0 if PTA is not configured.
- *SSLDescriptors* is 5 (4 files + 1 listensocket) if SSL is configured and 0 if SSL is not configured.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to 65535
Default Value	64
Syntax	Integer
Example	nsslapd-reservedescriptors: 64

### 3.1.79. nsslapd-return-exact-case (Return Exact Case)

Returns the exact case of attribute type names as requested by the client. Although LDAPv3-compliant clients must ignore the case of attribute names, some client applications require attribute names to match exactly the case of the attribute as it is listed in the schema when the attribute is returned by the Directory Server as the result of a search or modify operation. However, most client applications ignore the case of attributes; therefore, by default, this attribute is disabled. Do not modify it unless there are legacy clients that can check the case of attribute names in results returned from the server.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString

Parameter	Description
Example	nsslapd-return-exact-case: off

### 3.1.80. nsslapd-rewrite-rfc1274

This attribute is deprecated and will be removed in a later version.

This attribute is used only for LDAPv2 clients that require attribute types to be returned with their RFC 1274 names. Set the value to `on` for those clients. The default is `off`.

### 3.1.81. nsslapd-rootdn (Manager DN)

This attribute sets the distinguished name (DN) of an entry that is not subject to access control restrictions, administrative limit restrictions for operations on the directory, or resource limits in general. There does not have to be an entry corresponding to this DN, and by default there is not an entry for this DN, thus values like `cn=Directory Manager` are acceptable.

For information on changing the root DN, see the "Creating Directory Entries" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid distinguished name
Default Value	
Syntax	DN
Example	nsslapd-rootdn: cn=Directory Manager

### 3.1.82. nsslapd-rootpw (Root Password)

This attribute sets the password associated with the Manager DN. When the root password is provided, it is encrypted according to the encryption method selected for the `nsslapd-rootpwstoragescheme` attribute. When viewed from the server console, this attribute shows the value `*****`. When viewed from the `dse.ldif` file, this attribute shows the encryption method followed by the encrypted string of the password. The example shows the password as displayed in the `dse.ldif` file, not the actual password.



#### CAUTION

When the root DN is configured at server setup, a root password is required. However, it is possible for the root password to be deleted from `dse.ldif` by directly editing the file. In this situation, the root DN can only obtain the same access to the directory is allowed for anonymous access. Always make sure that a root password is defined in `dse.ldif` when a root DN is configured for the

database. The `pwdhash` command-line utility can create a new root password. For more information, see [Section 3.9, “pwdhash \(Prints Encrypted Passwords\)”](#).

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid password encrypted by any one of the encryption methods which are described in <a href="#">Section 3.1.123, “passwordStorageScheme (Password Storage Scheme)”</a> .
Default Value	
Syntax	DirectoryString { <i>encryption_method</i> } <i>encrypted_Password</i>
Example	nsslapd-rootpw: {SSHA}9Eko69APCJfF

### 3.1.83. nsslapd-rootpwstoragescheme (Root Password Storage Scheme)

This attribute sets the encryption method used for the root password.

Parameter	Description
Entry DN	cn=config
Valid Values	Any encryption method as described in <a href="#">Section 3.1.123, “passwordStorageScheme (Password Storage Scheme)”</a> .
Default Value	SSHA
Syntax	DirectoryString
Example	nsslapd-rootpwstoragescheme: SSHA

### 3.1.84. nsslapd-saslpath

Sets the absolute path to the directory containing the Cyrus-SASL SASL2 plug-ins. On HP-UX and Solaris systems, the Directory Server cannot use the system SASL libraries because they are either not provided or are not the correct version. Setting this attribute allows the server to use custom or non-standard SASL plug-in libraries. This is usually set correctly during installation, and Red Hat strongly recommends not changing this attribute. If the attribute is not present or the value is empty, this means the Directory Server is using the system provided SASL plug-in libraries which are the correct version.

If this parameter is set, the server uses the specified path for loading SASL plugins. If this parameter is not set, the server uses the `SASL_PATH` environment variable. If neither

`nsslapd-saslp` or `SASL_PATH` are set, the server attempts to load SASL plugins from the default location, `/usr/lib/sasl2`.

Changes made to this attribute will not take effect until the server is restarted.

Parameter	Description
Entry DN	cn=config
Valid Values	Path to plugins directory.
Default Value	Platform dependent
Syntax	DirectoryString
Example	nsslapd-saslp: /usr/lib/sasl2

### 3.1.85. nsslapd-schema-ignore-trailing-spaces (Ignore Trailing Spaces in Object Class Names)

Ignores trailing spaces in object class names. By default, the attribute is turned off. If the directory contains entries with object class values that end in one or more spaces, turn this attribute on. It is preferable to remove the trailing spaces because the LDAP standards do not allow them.

For performance reasons, server restart is required for changes to take effect.

An error is returned by default when object classes that include trailing spaces are added to an entry. Additionally, during operations such as add, modify, and import (when object classes are expanded and missing superiors are added) trailing spaces are ignored, if appropriate. This means that even when `nsslapd-schema-ignore-trailing-spaces` is on, a value such as `top` is not added if `top` is already there. An error message is logged and returned to the client if an object class is not found and it contains trailing spaces.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-schema-ignore-trailing-spaces: on

### 3.1.86. nsslapd-schemacheck (Schema Checking)

This attribute sets whether the database schema is enforced when entries are added or modified. When this attribute has a value of `on`, Directory Server will not check the schema of existing entries until they are modified. The database schema defines the type of information allowed in the database. The default schema can be extended using the object classes and attribute types. For information on how to extend the schema using the Directory Server

Console, see the "Extending the Directory Schema" chapter in the *Directory Server Administration Guide*.



### CAUTION

Red Hat strongly discourages turning off schema checking. This can lead to severe interoperability problems. This is typically used for very old or non-standard LDAP data that must be imported into the Directory Server. If there are not a lot of entries that have this problem, consider using the `extensibleObject` object class in those entries to disable schema checking on a per entry basis.



### NOTE

Schema checking works by default when database modifications are made using an LDAP client, such as `ldapmodify`, the Directory Server Gateway, or when importing a database from LDIF using `ldif2db`. If schema checking is turned off, every entry has to be verified manually to see that they conform to the schema. If schema checking is turned on, the server sends an error message listing the entries which do not match the schema. Ensure that the attributes and object classes created in the LDIF statements are both spelled correctly and identified in `dse.ldif`. Either create an LDIF file in the schema directory or add the elements to `99user.ldif`.

Parameter	Description
Entry DN	<code>cn=config</code>
Valid Values	<code>on   off</code>
Default Value	<code>on</code>
Syntax	<code>DirectoryString</code>
Example	<code>nsslapd-schemacheck: on</code>

### 3.1.87. `nsslapd-schemadir`

This is the absolute path to the directory containing the Directory Server instance-specific schema files. When the server starts up, it reads the schema files from this directory, and when the schema is modified through LDAP tools, the schema files in this directory are updated. This directory must be owned by the server user ID, and that user must have read and write permissions to the directory. The default value is the schema subdirectory of the Directory Server instance-specific configuration directory, `/etc/dirsrv/slapd-instance_name/schema`.

Changes made to this attribute will not take effect until the server is restarted.

### 3.1.88. nsslapd-schemareplace

Determines whether modify operations that replace attribute values are allowed on the `cn=schema` entry.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off   replication-only
Default Value	replication-only
Syntax	DirectoryString
Example	nsslapd-schemareplace: replication-only

### 3.1.89. nsslapd-securelistenhost

This attribute allows multiple Directory Server instances to run on a multihomed machine (or makes it possible to limit listening to one interface of a multihomed machine). There can be multiple IP addresses associated with a single hostname, and these IP addresses can be a mix of both IPv4 and IPv6. This parameter can be used to restrict the Directory Server instance to a single IP interface; this parameter also specifically sets what interface to use for SSL/TLS traffic rather than regular LDAP connections.

If a hostname is given as the `nsslapd-securelistenhost` value, then the Directory Server responds to requests for every interface associated with the hostname. If a single IP interface (either IPv4 or IPv6) is given as the `nsslapd-securelistenhost` value, Directory Server only responds to requests sent to that specific interface. Either an IPv4 or IPv6 address can be used.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config
Valid Values	Any secure hostname, IPv4 or IPv6 address
Default Value	
Syntax	DirectoryString
Example	nsslapd-securelistenhost: ldaps.example.com

### 3.1.90. nsslapd-securePort (Encrypted Port Number)

This attribute sets the TCP/IP port number used for SSL/TLS communications. This selected port must be unique on the host system; make sure no other application is attempting to use the same port number. Specifying a port number of less than 1024 requires that Directory Server be started as `root`. The server sets its `uid` to the `nsslapd-localuser` value after startup.

The server only listens to this port if it has been configured with a private key and a certificate,

and `nsslapd-security` is set to `on`; otherwise, it does not listen on this port.

The server has to be restarted for the port number change to be taken into account.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to 65535
Default Value	636
Syntax	Integer
Example	nsslapd-securePort: 636

### 3.1.91. nsslapd-security (Security)

This attribute sets whether the Directory Server is to accept SSL/TLS communications on its encrypted port. This attribute should be set to `on` for secure connections. To run with security `on`, the server must be configured with a private key and server certificate in addition to the other SSL/TLS configuration.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-security: off

### 3.1.92. nsslapd-sizelimit (Size Limit)

This attribute sets the maximum number of entries to return from a search operation. If this limit is reached, `ns-slapd` returns any entries it has located that match the search request, as well as an exceeded size limit error.

When no limit is set, `ns-slapd` returns every matching entry to the client regardless of the number found. To set a no limit value whereby the Directory Server waits indefinitely for the search to complete, specify a value of `-1` for this attribute in the `dse.ldif` file.

This limit applies to everyone, regardless of their organization.



#### NOTE

A value of `-1` on this attribute in `dse.ldif` file is the same as leaving the attribute blank in the server console, in that it causes no limit to be used. This cannot have a null value in `dse.ldif` file, as it is not a valid integer. It is possible to set it

to 0, which returns `size limit exceeded` for every search.

Parameter	Description
Entry DN	cn=config
Valid Range	-1 to the maximum 32 bit integer value (2147483647)
Default Value	2000
Syntax	Integer
Example	nsslapd-sizelimit: 2000

### 3.1.93. nsslapd-ssl-check-hostname (Verify Hostname for Outbound Connections)

This attribute sets whether an SSL-enabled Directory Server should verify authenticity of a request by matching the hostname against the value assigned to the common name (*cn*) attribute of the subject name (*subjectDN* field) in the certificate being presented. By default, the attribute is set to *on*. If it is *on* and if the hostname does not match the *cn* attribute of the certificate, appropriate error and audit messages are logged.

For example, in a replicated environment, messages similar to the following are logged in the supplier server's log files if it finds that the peer server's hostname does not match the name specified in its certificate:

```
[DATE] - SSL alert: ldap_sasl_bind("",LDAP_SASL_EXTERNAL) 81 (Netscape
runtime error -12276 -
    Unable to communicate securely with peer: requested domain name
does not
    match the server's certificate.)

[DATE] NSMMReplicationPlugin - agmt="cn=SSL Replication Agreement to host1"
(host1.example.com:636):
Replication bind with SSL client authentication failed:
LDAP error 81 (Can't contact LDAP server)
```

Red Hat recommends turning this attribute on to protect Directory Server's outbound SSL connections against a man in the middle (MITM) attack.



#### NOTE>

DNS and reverse DNS must be set up correctly in order for this to work; otherwise, the server cannot resolve the peer IP address to the hostname in the

subject DN in the certificate.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-ssl-check-hostname: on

### 3.1.94. nsslapd-threadnumber (Thread Number)

Defines the number of operation threads that the Directory Server creates at startup. The *nsslapd-threadnumber* value should be increased if there are many directory clients performing time-consuming operations such as add or modify, as this ensures that there are other threads available for servicing short-lived operations such as simple searches. This value may also need increased if there are many replication agreements or chained backends (database links). This attribute is not available from the server console.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum number of threads supported by the system
Default Value	30
Syntax	Integer
Example	nsslapd-threadnumber: 60

### 3.1.95. nsslapd-timelimit (Time Limit)

This attribute sets the maximum number of seconds allocated for a search request. If this limit is reached, Directory Server returns any entries it has located that match the search request, as well as an exceeded time limit error.

When no limit is set, *ns-slapd* returns every matching entry to the client regardless of the time it takes. To set a no limit value whereby Directory Server waits indefinitely for the search to complete, specify a value of `-1` for this attribute in the *dse.ldif* file. A value of zero (0) causes no time to be allowed for searches. The smallest time limit is 1 second.

**NOTE**

A value of `-1` on this attribute in the `dse.ldif` is the same as leaving the attribute blank in the server console in that it causes no limit to be used. However, a negative integer cannot be set in this field in the server console, and a null value cannot be used in the `dse.ldif` entry, as it is not a valid integer.

Parameter	Description
Entry DN	cn=config
Valid Range	-1 to the maximum 32 bit integer value (2147483647) in seconds
Default Value	3600
Syntax	Integer
Example	nsslapd-timelimit: 3600

### 3.1.96. nsslapd-tmpdir

This is the absolute path of the directory the server uses for temporary files. The directory must be owned by the server user ID and the user must have read and write access. No other user ID should have read or write access to the directory. The default value is `/tmp`.

Changes made to this attribute will not take effect until the server is restarted.

### 3.1.97. nsslapd-versionstring

This attribute sets the server version number. The build data is automatically appended when the version string is displayed.

Parameter	Description
Entry DN	cn=config
Valid Values	Any valid server version number.
Default Value	
Syntax	DirectoryString
Example	nsslapd-versionstring: Red Hat-Directory/8.0

### 3.1.98. nsslapd-workingdir

This is the absolute path of the directory that the server uses as its current working directory after startup. This is the value that the server would return as the value of the `getcwd()` function, and the value that the system process table shows as its current working directory.

This is the directory a core file is generated in. The server user ID must have read and write access to the directory, and no other user ID should have read or write access to it. The default value for this attribute is the same directory containing the error log, which is usually `/var/log/dirsrv/slaped-instance_name`.

Changes made to this attribute will not take effect until the server is restarted.

### 3.1.99. passwordChange (Password Change)

Indicates whether users may change their passwords.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	passwordChange: on

### 3.1.100. passwordCheckSyntax (Check Password Syntax)

This attribute sets whether the password syntax is checked before the password is saved. The password syntax checking mechanism checks that the password meets or exceeds the password minimum length requirement and that the string does not contain any trivial words, such as the user's name or user ID or any attribute value stored in the `uid`, `cn`, `sn`, `givenName`, `ou`, or `mail` attributes of the user's directory entry.

Password syntax includes several different categories for checking:

- Minimum number of digit characters (0-9)
- Minimum number of ASCII alphabetic characters, both upper- and lower-case
- Minimum number of uppercase ASCII alphabetic characters
- Minimum number of lowercase ASCII alphabetic characters
- Minimum number of special ASCII characters, such as `!@#$`
- Minimum number of 8-bit characters
- Maximum number of times that the same character can be immediately repeated, such as `aaabbb`
- Minimum number of character categories required per password; a category can be upper- or

lower-case letters, special characters, digits, or 8-bit characters

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	passwordCheckSyntax off

### 3.1.101. passwordExp (Password Expiration)

Indicates whether user passwords expire after a given number of seconds. By default, user passwords do not expire. Once password expiration is enabled, set the number of seconds after which the password expires using the *passwordMaxAge* attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	passwordExp: on

### 3.1.102. passwordGraceLimit (Password Expiration)

This attribute is only applicable if password expiration is enabled. After the user's password has expired, the server allows the user to connect for the purpose of changing the password. This is called a *grace login*. The server allows only a certain number of attempts before completely locking out the user. This attribute is the number of grace logins allowed. A value of 0 means the server does not allow grace logins.

Parameter	Description
Entry DN	cn=config
Valid Values	0 (off) to any reasonable integer
Default Value	0
Syntax	Integer
Example	passwordGraceLimit: 3

### 3.1.103. passwordHistory (Password History)

Enables password history. Password history refers to whether users are allowed to reuse passwords. By default, password history is disabled, and users can reuse passwords. If this attribute is set to `on`, the directory stores a given number of old passwords and prevents users from reusing any of the stored passwords. Set the number of old passwords the Directory Server stores using the `passwordInHistory` attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	passwordHistory: on

### 3.1.104. passwordInHistory (Number of Passwords to Remember)

Indicates the number of passwords the Directory Server stores in history. Passwords that are stored in history cannot be reused by users. By default, the password history feature is disabled, meaning that the Directory Server does not store any old passwords, and so users can reuse passwords. Enable password history using the `passwordHistory` attribute.

To prevent users from rapidly cycling through the number of passwords that are tracked, use the `passwordMinAge` attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	2 to 24 passwords
Default Value	6
Syntax	Integer
Example	passwordInHistory: 7

### 3.1.105. passwordsGlobalPolicy (Password Policy and Replication)

This attribute controls whether password policy attributes are replicated.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	passwordIsGlobalPolicy: off

### 3.1.106. passwordLockout (Account Lockout)

Indicates whether users are locked out of the directory after a given number of failed bind attempts. By default, users are not locked out of the directory after a series of failed bind attempts. If account lockout is enabled, set the number of failed bind attempts after which the user is locked out using the *passwordMaxFailure* attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	passwordLockout: off

### 3.1.107. passwordLockoutDuration (Lockout Duration)

Indicates the amount of time in seconds during which users are locked out of the directory after an account lockout. The account lockout feature protects against hackers who try to break into the directory by repeatedly trying to guess a user's password. Enable and disable the account lockout feature using the *passwordLockout* attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647) in seconds
Default Value	3600
Syntax	Integer
Example	passwordLockoutDuration: 3600

### 3.1.108. passwordMaxAge (Password Maximum Age)

Indicates the number of seconds after which user passwords expire. To use this attribute, password expiration has to be enabled using the `passwordExp` attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647) in seconds
Default Value	8640000 (100 days)
Syntax	Integer
Example	passwordMaxAge: 100

### 3.1.109. passwordMaxFailure (Maximum Password Failures)

Indicates the number of failed bind attempts after which a user is locked out of the directory. By default, account lockout is disabled. Enable account lockout by modifying the `passwordLockout` attribute.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to maximum integer bind failures
Default Value	3
Syntax	Integer
Example	passwordMaxFailure: 3

### 3.1.110. passwordMaxRepeats (Password Syntax)

Maximum number of times the same character can appear sequentially in the password. Zero (0) is off. Integer values reject any password which used a character more than that number of times; for example, 1 rejects characters that are used more than once (aa) and 2 rejects characters used more than twice (aaa).

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64

Parameter	Description
Default Value	0
Syntax	Integer
Example	passwordMaxRepeats: 1

### 3.1.111. passwordMin8Bit (Password Syntax)

This sets the minimum number of 8-bit characters the password must contain.



#### NOTE

The 7-bit checking for *userPassword* must be disabled to use this.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64
Default Value	0
Syntax	Integer
Example	passwordMin8Bit: 0

### 3.1.112. passwordMinAge (Password Minimum Age)

Indicates the number of seconds that must pass before a user can change their password. Use this attribute in conjunction with the *passwordInHistory* (number of passwords to remember) attribute to prevent users from quickly cycling through passwords so that they can use their old password again. A value of zero (0) means that the user can change the password immediately.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to valid maximum integer
Default Value	0
Syntax	Integer
Example	passwordMinAge: 150

### 3.1.113. passwordMinAlphas (Password Syntax)

This attribute sets the minimum number of alphabetic characters password must contain.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64
Default Value	0
Syntax	Integer
Example	passwordMinAlphas: 4

### 3.1.114. passwordMinCategories (Password Syntax)

This sets the minimum number of character categories that are represented in the password. The categories are lower, upper, digit, special, and 8-bit. For example, if the value of this attribute were set to 2, and the user tried to change the password to `aaaaa`, the server would reject the password because it contains only lower case characters, and therefore contains characters from only one category. A password of `aAaAaA` would pass because it contains characters from two categories, uppercase and lowercase. The default is 3, which means that if password syntax checking is enabled, valid passwords have to have three categories of characters.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 5
Default Value	0
Syntax	Integer
Example	passwordMinCategories: 2

### 3.1.115. PasswordMinDigits (Password Syntax)

This sets the minimum number of digits a password must contain.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64
Default Value	0
Syntax	Integer
Example	passwordMinDigits: 3

### 3.1.116. passwordMinLength (Password Minimum Length)

This attribute specifies the minimum number of characters that must be used in Directory Server user password attributes. In general, shorter passwords are easier to crack. Directory Server enforces a minimum password of eight characters. This is long enough to be difficult to crack but short enough that users can remember the password without writing it down.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	2 to 512 characters
Default Value	6
Syntax	Integer
Example	passwordMinLength: 6

### 3.1.117. PasswordMinLowers (Password Syntax)

This attribute sets the minimum number of lower case letters password must contain.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64
Default Value	0
Syntax	Integer
Example	passwordMinLowers: 1

### 3.1.118. PasswordMinSpecials (Password Syntax)

This attribute sets the minimum number of *special*, or not alphanumeric, characters a password must contain.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64
Default Value	0
Syntax	Integer
Example	passwordMinSpecials: 1

### 3.1.119. PasswordMinTokenLength (Password Syntax)

This attribute sets the smallest attribute value length that is used for *trivial* words checking. For

example, if the `PasswordMinTokenLength` is set to 3, then a `givenName` of DJ does not result in a policy that rejects DJ from being in the password, but the policy rejects a password containing the `givenName` of Bob.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to 64
Default Value	3
Syntax	Integer
Example	passwordMinTokenLength: 3

### 3.1.120. PasswordMinUppers (Password Syntax)

This sets the minimum number of uppercase letters password must contain.

Parameter	Description
Entry DN	cn=config
Valid Range	0 to 64
Default Value	0
Syntax	Integer
Example	passwordMinUppers: 2

### 3.1.121. passwordMustChange (Password Must Change)

Indicates whether users must change their passwords when they first bind to the Directory Server or when the password has been reset by the Manager DN.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	passwordMustChange: off

### 3.1.122. passwordResetFailureCount (Reset Password Failure Count After)

Indicates the amount of time in seconds after which the password failure counter resets. Each

time an invalid password is sent from the user's account, the password failure counter is incremented. If the `passwordLockout` attribute is set to `on`, users are locked out of the directory when the counter reaches the number of failures specified by the `passwordMaxFailure` attribute (within 600 seconds by default). After the amount of time specified by the `passwordLockoutDuration` attribute, the failure counter is reset to zero (0).

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647) in seconds
Default Value	600
Syntax	Integer
Example	passwordResetFailureCount: 600

### 3.1.123. passwordStorageScheme (Password Storage Scheme)

This attribute sets the type of encryption used to store Directory Server passwords.

The following encryption types are supported by the Directory Server:

- CLEAR means the password is stored in cleartext, with no hashing or encryption. This scheme must be used in order to use SASL DIGEST-MD5.
- SSHA (Salted Secure Hash Algorithm), the default, is the recommended method because it is the most secure. There are several bit sizes available: 140 bits (the default), 256, 384, and 512.
- SHA (Secure Hash Algorithm) is included only for backward compatibility with 4.x Directory Servers; do not use this algorithm.
- MD5 (Message Digest algorithm 5) is a commonly used standard hashing algorithm.
- CRYPT, the UNIX crypt algorithm, is provided for compatibility with UNIX passwords.



#### NOTE

Passwords cannot be encrypted using the NS-MTA-MD5 password storage scheme. The storage scheme is still present but only for reasons of backward compatibility.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

### 3.1.124. passwordUnlock (Unlock Account)

Indicates whether users are locked out of the directory for a specified amount of time or until the administrator resets the password after an account lockout. The account lockout feature protects against hackers who try to break into the directory by repeatedly trying to guess a user's password. If this `passwordUnlock` attribute is set to `off` and the operational attribute `accountUnlockTime` has a value of `0`, then the account is locked indefinitely.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	passwordUnlock: off

### 3.1.125. passwordWarning (Send Warning)

Indicates the number of seconds before a user's password is due to expire that the user receives a password expiration warning control on their next LDAP operation. Depending on the LDAP client, the user may also be prompted to change their password at the time the warning is sent.

For more information on password policies, see the "Managing Users and Passwords" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config
Valid Range	1 to the maximum 32 bit integer value (2147483647) in seconds
Default Value	86400 (1 day)
Syntax	Integer
Example	passwordWarning: 86400

## 3.2. cn=changelog5

Multi-master replication changelog configuration entries are stored under the `cn=changelog5` entry. The changelog behaves much like a database, and it has many of attributes also used by

the ldbm databases. The changelog entry supports the following attributes with the same meaning as for databases:

The default values for the cache-related memory parameters (tuned for a single backend replicated to a single consumer) are as follows:

- `nsslapd-cachesize`: 3000 (3000 entries)
- `nsslapd-cachememsize`: 10000000 (10 Mbyte)

When more backends are replicated or when one backend is replicated to more than one consumer, tune the parameters as below:

```
nsslapd-cachesize = 2000*#repl_agreements_initiated_from_this_server
nsslapd-cachememsize = 5000000*#repl_agreements_initiated_from_this_server
```

Also, the relationship between the values assigned to the `nsslapd-dbcachesize` and `nsslapd-cachememsize` parameters should be the same as the relationship that is described in the database-tuning section.

The `cn=changelog5,cn=config` entry is an instance of the `extensibleObject` object class.

It is worth noting that two different types of changelogs are maintained by Directory Server. The first type, which is stored here and referred to as the `changelog`, is used by multi-master replication; the second changelog, which is actually a plug-in and referred to as the `retro changelog`, is for compatibility with some legacy applications. See [Section 1.31, “Retro Changelog Plug-in”](#) for further information about the Retro Changelog Plug-in.

### 3.2.1. nsslapd-changelogdir

This required attribute specifies the name of the directory in which the changelog database is created. Whenever a changelog configuration entry is created, it must contain a valid directory; otherwise, the operation is rejected. The GUI proposes by default that this database be stored in `/var/lib/dirsrv/slapd-instance_name/changelogdb`.



#### CAUTION

If the `cn=changelog5` entry is removed, the directory specified in the `nsslapd-changelogdir` parameter, including any subdirectories, are removed, with all of their contents.



**NOTE**

For performance reasons, store this database on a different physical disk.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=changelog5,cn=config
Valid Values	Any valid path to the directory storing the changelog
Default Value	None
Syntax	DirectoryString
Example	nsslapd-changelogdir: /var/lib/dirsrv/slapd- <i>instance_name</i> /changelogdb

### 3.2.2. nsslapd-changelogmaxage (Max Changelog Age)

This attribute sets the maximum age of any entry in the changelog. The changelog contains a record for each directory modification and is used when synchronizing consumer servers. Each record contains a timestamp. Any record with a timestamp that is older than the value specified in this attribute is removed. If this attribute is absent, there is no age limit on changelog records. For information on the changelog, see [Section 3.2.1, “nsslapd-changelogdir”](#).

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=changelog5,cn=config
Valid Range	0 (meaning that entries are not removed according to their age) to maximum 32-bit integer (2147483647)
Default Value	0
Syntax	DirectoryString <i>IntegerAgeID</i> where <i>AgeID</i> is <i>s</i> for seconds, <i>m</i> for minutes, <i>h</i> for hours, <i>d</i> for days, and <i>w</i> for weeks
Example	nsslapd-changelogmaxage: 30d

### 3.2.3. nsslapd-changelogmaxentries (Max Changelog Records)

This attribute sets the maximum number of records the changelog may contain. If this attribute is absent, there is no maximum number of records the changelog can contain. For information

on the changelog, see [Section 3.2.1, “nsslapd-changelogdir”](#).

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=changelog5,cn=config
Valid Range	0 (meaning that the only maximum limit is the disk size) to maximum 32-bit integer (2147483647)
Default Value	0
Syntax	Integer
Example	nsslapd-changelogmaxentries: 5000

### 3.3. cn=encryption

Encryption related attributes are stored under the `cn=encryption,cn=config` entry. The `cn=encryption,cn=config` entry is an instance of the `nsslapdEncryptionConfig` object class.

#### 3.3.1. nsslsessiontimeout

This attribute sets the lifetime duration of a TLS/SSL. The minimum timeout value is 5 seconds. If a smaller value is set, then it is automatically replaced by 5 seconds. A value greater than the maximum value in the valid range below is replaced by the maximum value in the range.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=encryption, cn=config
Valid Range	5 seconds to 24 hours
Default Value	0, which means use the maximum value in the valid range above.
Syntax	Integer
Example	nsslsessiontimeout: 5

#### 3.3.2. nsslclientauth

This attribute sets how clients may use certificates to authenticate to the Directory Server for SSL connections.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=encryption, cn=config
Valid Values	off   allowed   required  <i>off</i> means disallow certificate-based authentication <i>allowed</i> means clients may use certificates or other forms of authentication <i>required</i> means clients must use certificates for authentication
Default Value	allowed
Syntax	DirectoryString
Example	nssslclientauth: allowed

### 3.3.3. nsSSL2

Supports SSL version 2. SSLv2 is deprecated, and Red Hat strongly discourages using it.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=encryption, cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsssl2: off

### 3.3.4. nsSSL3

Supports SSL version 3.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=encryption, cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsssl3: on

### 3.3.5. nsssl3ciphers

This multi-valued attribute specifies the set of encryption ciphers the Directory Server uses during SSL communications. For more information on the ciphers supported by the Directory Server, see the "Managing SSL" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=encryption, cn=config
Valid Values	<p>For SSLv3:</p> <ul style="list-style-type: none"> <li>• rsa_null_md5</li> <li>• rsa_rc4_128_md5</li> <li>• rsa_rc4_40_md5</li> <li>• rsa_rc2_40_md5</li> <li>• rsa_des_sha</li> <li>• rsa_fips_des_sha</li> <li>• rsa_3des_sha</li> <li>• rsa_fips_3des_sha</li> </ul> <p>For TLS:</p> <ul style="list-style-type: none"> <li>• tls_rsa_export1024_with_rc4_56_sha</li> <li>• tls_rsa_export1024_with_des_cbc_sha</li> </ul>
Default Value	
Syntax	<p>DirectoryString</p> <p>Use the plus (+) symbol to enable or minus (-) symbol to disable, followed by the ciphers. Blank spaces are not allowed in the list of ciphers.</p> <p>To enable all ciphers — except <code>rsa_null_md5</code>, which must be specifically called — specify <code>+all</code>.</p>
Example	<pre>nsslapd-SSL3ciphers: +RSA_NULL_MD5,+RC4_56_SHA,-RC4_56_SHA</pre>

For more information, see the "Managing SSL" chapter in the *Directory Server Administration*

Guide

### 3.4. cn=features

There are not attributes for this entry. This entry is only used as a parent container entry. See the documentation on the child entries for more information.

### 3.5. cn=mapping tree

- Configuration attributes for suffixes, replication, and Windows synchronization are stored under `cn=mapping tree,cn=config`. Configuration attributes related to suffixes are found under the suffix subentry `cn=suffix,cn=mapping tree,cn=config`.

For example, a *suffix* is the root entry in the directory tree, such as `dc=example,dc=com`.

- Replication configuration attributes are stored under `cn=replica, cn=suffix, cn=mapping tree,cn=config`.
- Replication agreement attributes are stored under `cn=replicationAgreementName, cn=replica, cn=suffix,cn=mapping tree,cn=config`.
- Windows synchronization agreement attributes are stored under `cn=syncAgreementName, cn=replica, cn=suffix,cn=mapping tree,cn=config`.

### 3.6. Suffix Configuration Attributes under cn="suffixName"

Suffix configuration attributes are stored under the `cn=suffix` entry. The `cn=suffix` entry is an instance of the `nsMappingTree` object class which inherits from the `extensibleObject` object class. For suffix configuration attributes to be taken into account by the server, these object classes (in addition to the `top` object class) must be present in the entry.

The suffix DN should be quoted because the suffix DN contains characters such as equals signs (=), commas (,), and space characters that must be quoted or escaped to appear as a value in another DN.

#### 3.6.1. nsslapd-state

Determines how the suffix handles operations.

Parameter	Description
Entry DN	<code>cn=suffix, cn=mapping tree, cn=config</code>
Valid Values	<p><code>backend   disabled   referral   referral on update</code></p> <p><i>backend</i> means the backend (database) is used to process all operations.</p>

Parameter	Description
	<p><i>disabled</i> means the database is not available for processing operations. The server returns a "No such search object" error in response to requests made by client applications.</p> <p><i>referral</i> means a referral is returned for requests made to this suffix.</p> <p><i>referral on update</i> means the database is used for all operations except update requests, which receive a referral.</p>
Default Value	backend
Syntax	DirectoryString
Example	nsslapd-state: backend

### 3.6.2. nsslapd-backend

Gives the name of the database or database link used to process requests. This attribute can be multi-valued, with one database or database link per value. This attribute is required when the value of the `nsslapd-state` attribute is set to `backend` or `referral on update`. The value should be the name of the backend database entry instance under `cn=ldbm database,cn=plugins,cn=config`. For example:

```
cn=NetscapeRoot,cn=ldbm database,cn=plugins,cn=config.
```

Parameter	Description
Entry DN	<code>cn=suffix</code> , <code>cn=mapping tree</code> , <code>cn=config</code>
Valid Values	Any valid partition name
Default Value	None
Syntax	DirectoryString
Example	nsslapd-backend: userRoot

### 3.7. Replication Attributes under `cn=replica`, `cn="suffixDN"`, `cn=mapping tree`, `cn=config`

Replication configuration attributes are stored under `cn=replica`, `cn=suffix`, `cn=mapping tree`, `cn=config`. The `cn=replica` entry is an instance of the `nsDS5Replica` object class. For replication configuration attributes to be taken into account by the server, this object class (in addition to the `top` object class) must be present in the entry. For further information about

replication, see the "Managing Replication" chapter in the *Directory Server Administration Guide*.

### 3.7.1. nsDS5Flags

This attribute sets replica properties that were previously defined in flags. At present only one flag exists, which sets whether the log changes.

Parameter	Description
Entry DN	cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	0   1  0 means no changes are logged 1 means changes are logged
Default Value	0
Syntax	Integer
Example	nsDS5Flags: 0

### 3.7.2. nsDS5ReplicaBindDN

This multi-valued attribute specifies the DN to use when binding. Although there can be more than one value in this cn=replica entry, there can only be one supplier bind DN per replication agreement. Each value should be the DN of a local entry on the consumer server. If replication suppliers are using client certificate-based authentication to connect to the consumers, configure the certificate mapping on the consumer to map the subjectDN in the certificate to a local entry.

Parameter	Description
Entry DN	cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Any valid DN
Default Value	
Syntax	DirectoryString
Example	nsDS5ReplicaBindDN: cn=replication manager, cn=config

### 3.7.3. nsDS5ReplicaChangeCount

This read-only attribute shows the total number of entries in the changelog and whether they still remain to be replicated. When the changelog is purged, only the entries that are still to be replicated remain.

See [Section 3.7.7, "nsDS5ReplicaPurgeDelay"](#) and [Section 3.7.10,](#)

“[nsDS5ReplicaTombstonePurgeInterval](#)” for more information about purge operation properties.

Parameter	Description
Entry DN	cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Range	-1 to maximum 32-bit integer (2147483647)
Default Value	
Syntax	Integer
Example	nsDS5ReplicaChangeCount: 675

### 3.7.4. nsDS5ReplicaId

This attribute sets the unique ID for suppliers in a given replication environment.

Parameter	Description
Entry DN	cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Range	0 to 65534
Default Value	
Syntax	Integer
Example	nsDS5ReplicaId: 1

### 3.7.5. nsDS5ReplicaLegacyConsumer

If this attribute is absent or has a value of `false`, then it means that the replica is not a legacy consumer.

Parameter	Description
Entry DN	cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	true   false
Default Value	false
Syntax	DirectoryString
Example	nsDS5ReplicaLegacyConsumer: false

### 3.7.6. nsDS5ReplicaName

This attribute specifies the name of the replica with a unique identifier for internal operations. If it is not specified, this unique identifier is allocated by the server when the replica is created.



**NOTE**

It is recommended that the server be permitted to generate this name. However, in certain circumstances, for example, in replica role changes (master to hub etc.), this value needs to be specified. Otherwise, the server will not use the correct changelog database, and replication fails.

This attribute is destined for internal use only.

Parameter	Description
Entry DN	cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	
Default Value	
Syntax	DirectoryString (a UID identifies the replica)
Example	nsDS5ReplicaName: 66a2b699-1dd211b2-807fa9c3-a58714648

**3.7.7. nsDS5ReplicaPurgeDelay**

This attribute controls the maximum age of update operations and state information.

The Directory Server stores updates — operations like adds, modifies, and deletes — so that it can replay those updates to other replicas. It keeps those updates in the changelog and as state information in the main database as change sequence numbers (CSN) and tombstone entries for some period of time after they have been replayed, in case a replica needs to be brought up to date without having to do a full reinitialization. An internal Directory Server housekeeping operation periodically removes updates and state information older than the value of this attribute (in seconds). Not every update may be removed. The server may need to keep a small number of the latest updates to *prime* replication, even if they are older than the value of the attribute. This attribute specifies the period of time in seconds after which internal purge operations are performed on the changelog. When setting this attribute, ensure that the purge delay is longer than the longest replication cycle in the replication policy to avoid incurring conflict resolution problems and server divergence.

Parameter	Description
Entry DN	cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Range	0 (keep forever) to maximum 32-bit integer (2147483647)
Default Value	604800 [1 week (60x60x24x7)]

Parameter	Description
Syntax	Integer
Example	nsDS5ReplicaPurgeDelay: 604800

### 3.7.8. nsDS5ReplicaReferral

This multi-valued attribute specifies the user-defined referrals. This should only be defined on a consumer. User referrals are only returned when a client attempts to modify data on a read-only consumer. This optional referral overrides the referral that is automatically configured by the consumer by the replication protocol.

Parameter	Description
Entry DN	cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Any valid LDAP URL
Default Value	
Syntax	DirectoryString
Example	nsDS5ReplicaReferral: ldap://ldap.example.com

### 3.7.9. nsDS5ReplicaRoot

This attribute sets the DN at the root of a replicated area. This attribute must have the same value as the suffix of the database being replicated and cannot be modified.

Parameter	Description
Entry DN	cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Suffix of the database being replicated, which is the suffix DN
Default Value	
Syntax	DirectoryString
Example	nsDS5ReplicaRoot: "dc=example,dc=com"

### 3.7.10. nsDS5ReplicaTombstonePurgeInterval

This attribute specifies the time interval in seconds between purge operation cycles.

Periodically, the server runs an internal housekeeping operation to purge old update and state information from the changelog and the main database. See [Section 3.7.7](#), “*nsDS5ReplicaPurgeDelay*”.

When setting this attribute, remember that the purge operation is time-consuming, especially if the server handles many delete operations from clients and suppliers.

Parameter	Description
Entry DN	cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Range	0 to maximum 32-bit integer (2147483647) in seconds
Default Value	86400 (1 day)
Syntax	Integer
Example	nsDS5ReplicaTombstonePurgeInterval: 86400

### 3.7.11. nsDS5ReplicaType

Defines the type of replication relationship that exists between this replica and the others.

Parameter	Description
Entry DN	cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	0   1   2   3  0 means unknown 1 means primary (not yet used) 2 means consumer (read-only) 3 consumer/supplier (updateable)
Default Value	
Syntax	Integer
Example	nsDS5ReplicaType: 2

### 3.7.12. nsDS5ReplicaReapActive

This read-only attribute specifies whether the background task that removes old tombstones (deleted entries) from the database is active. See [Section 3.7.10](#), “*nsDS5ReplicaTombstonePurgeInterval*” for more information about this task. A value of 0 means that the task is inactive, and a value of 1 means that the task is active. The server ignores the modify request if this value is set manually.

Parameter	Description
Entry DN	cn=replica,cn="suffixDN",cn=mapping tree,cn=config
Valid Values	0   1

Parameter	Description
Default Value	
Syntax	Integer
Example	nsDS5ReplicaReapActive: 0

### 3.7.13. nsState

This attribute stores information on the state of the clock. It is designed only for internal use to ensure that the server cannot generate a change sequence number (*csn*) inferior to existing ones required for detecting backward clock errors.

### 3.7.14. nsDS5ReplConflict

Although this attribute is not in the *cn=replica* entry, it is used in conjunction with replication. This multi-valued attribute is included on entries that have a change conflict that cannot be resolved automatically by the synchronization process. To check for replication conflicts requiring administrator intervention, perform an LDAP search for (*nsDS5ReplConflict=\**). For example:

```
ldapsearch -D cn=directory manager -w password -s sub -b dc=example,dc=com
"(|(objectclass=nsTombstone)(nsDS5ReplConflict=*))" dn
nsDS5ReplConflict nsUniqueID
```

Using the search filter "(objectclass=nsTombstone)" also show tombstone (deleted) entries. The value of the *nsDS5ReplConflict* contains more information about which entries are in conflict, usually by referring to them by their *nsUniqueID*. It is possible to search for a tombstone entry by its *nsUniqueID*. For example:

```
ldapsearch -D cn=directory manager -w password -s sub -b dc=example,dc=com
"(|(objectclass=nsTombstone)(nsUniqueID=66a2b699-1dd211b2-807fa9c3-a58714648))"
```

## 3.8. Replication Attributes under cn=ReplicationAgreementName, cn=replica, cn="suffixName", cn=mapping tree, cn=config

The replication attributes that concern the replication agreement are stored under *cn=ReplicationAgreementName*, *cn=replica*, *cn=suffixDN*, *cn=mapping tree*, *cn=config*. The *cn=ReplicationAgreementName* entry is an instance of the *nsDS5ReplicationAgreement* object class. Replication agreements are configured only on supplier replicas.

### 3.8.1. cn

This attribute is used for naming. Once this attribute has been set, it cannot be modified. This

attribute is required for setting up a replication agreement.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Any valid <i>cn</i>
Default Value	
Syntax	DirectoryString
Example	<i>cn: MasterAtoMasterB</i>

### 3.8.2. description

Free form text description of the replication agreement. This attribute can be modified.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Any string
Default Value	
Syntax	DirectoryString
Example	<i>description: Replication Agreement between Server A and Server B.</i>

### 3.8.3. nsDS5ReplicaBindDN

This attribute sets the DN to use when binding to the consumer during replication. The value of this attribute must be the same as the one in *cn=replica* on the consumer replica. This may be empty if certificate-based authentication is used, in which case the DN used is the subject DN of the certificate, and the consumer must have appropriate client certificate mapping enabled. This can also be modified.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Any valid DN (can be empty if client certificates are used)
Default Value	
Syntax	DirectoryString
Example	<i>nsDS5ReplicaBindDN: cn=replication manager, cn=config</i>

### 3.8.4. nsDS5ReplicaBindMethod

This attribute sets the method to use for binding. This attribute can be modified.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	SIMPLE   SSLCLIENTAUTH  The <code>SIMPLE</code> bind method requires a DN and password.
Default Value	SIMPLE
Syntax	DirectoryString
Example	nsDS5ReplicaBindMethod: SIMPLE

### 3.8.5. nsDS5ReplicaBusyWaitTime

This attribute sets the amount of time in seconds a supplier should wait after a consumer sends back a busy response before making another attempt to acquire access. The default value is three (3) seconds. If the attribute is set to a negative value, Directory Server sends the client a message and an `LDAP_UNWILLING_TO_PERFORM` error code.

The *nsDS5ReplicaBusyWaitTime* attribute works in conjunction with the *nsDS5ReplicaSessionPauseTime* attribute. The two attributes are designed so that the *nsDS5ReplicaSessionPauseTime* interval is always at least one second longer than the interval specified for *nsDS5ReplicaBusyWaitTime*. The longer interval gives waiting suppliers a better chance to gain consumer access before the previous supplier can re-access the consumer.

Set the *nsDS5ReplicaBusyWaitTime* attribute at any time by using `changetype:modify` with the `replace` operation. The change takes effect for the next update session if one is already in progress.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Any valid integer
Default Value	3
Syntax	Integer
Example	nsDS5ReplicaBusyWaitTime: 3

### 3.8.6. nsDS5ReplicaChangesSentSinceStartup

This read-only attribute shows the number of changes sent to this replica since the server started.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Range	0 to maximum 32-bit integer (2147483647)
Default Value	
Syntax	Integer
Example	<i>nsDS5ReplicaChangesSentSinceStartup</i> : 647

### 3.8.7. nsDS5ReplicaCredentials

This attribute sets the credentials for the bind DN (specified in the *nsDS5ReplicaBindDN* attribute) on the remote server containing the consumer replica. The value for this attribute can be modified. When certificate-based authentication is used, this attribute may not have a value. The example shows the *dse.ldif* entry, not the actual password. If this value over LDAP or using the Console, set it to the cleartext credentials, and let the server encrypt the value.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Any valid password, which is then encrypted using the DES reversible password encryption schema.
Default Value	
Syntax	DirectoryString {DES} <i>encrypted_password</i>
Example	<i>nsDS5ReplicaCredentials</i> :{DES} 9Eko69APCJfF08A0aD0C

### 3.8.8. nsDS5ReplicaHost

This attribute sets the hostname for the remote server containing the consumer replica. Once this attribute has been set, it cannot be modified.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Any valid host server name
Default Value	
Syntax	DirectoryString

Parameter	Description
Example	nsDS5ReplicaHost: ldap2.example.com

### 3.8.9. nsDS5ReplicaLastInitEnd

This optional, read-only attribute states when the initialization of the consumer replica ended.

Parameter	Description
Entry DN	cn= <i>ReplicationAgreementName</i> , cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	YYYYMMDDhmmssZ is the date/time in Generalized Time form at which the connection was opened. This value gives the time in relation to Greenwich Mean Time. The hours are set with a 24-hour clock. The z at the end indicates that the time is relative to Greenwich Mean Time.
Default Value	
Syntax	GeneralizedTime
Example	nsDS5ReplicaLastInitEnd: 20070504121603Z

### 3.8.10. nsDS5ReplicaLastInitStart

This optional, read-only attribute states when the initialization of the consumer replica started.

Parameter	Description
Entry DN	cn= <i>ReplicationAgreementName</i> , cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	YYYYMMDDhmmssZ is the date/time in Generalized Time form at which the connection was opened. This value gives the time in relation to Greenwich Mean Time. The hours are set with a 24-hour clock. The z at the end indicates that the time is relative to Greenwich Mean Time.
Default Value	
Syntax	GeneralizedTime
Example	nsDS5ReplicaLastInitStart: 20070503030405

### 3.8.11. nsDS5ReplicaLastInitStatus

This optional, read-only attribute provides status for the initialization of the consumer. There is typically a numeric code followed by a short string explaining the status. Zero (0) means success.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	0 (Consumer Initialization Succeeded), followed by any other status message.
Default Value	
Syntax	String
Example	<code>nsDS5ReplicaLastUpdateStatus: 0 Total update succeeded</code>

### 3.8.12. nsDS5ReplicaLastUpdateEnd

This read-only attribute states when the most recent replication schedule update ended.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	<i>YYYYMMDDhhmmssZ</i> is the date/time in Generalized Time form at which the connection was opened. This value gives the time in relation to Greenwich Mean Time. The hours are set with a 24-hour clock. The <i>z</i> at the end indicates that the time is relative to Greenwich Mean Time.
Default Value	
Syntax	GeneralizedTime
Example	<code>nsDS5ReplicaLastUpdateEnd: 20070502175801Z</code>

### 3.8.13. nsDS5ReplicaLastUpdateStart

This read-only attribute states when the most recent replication schedule update started.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	<i>YYYYMMDDhhmmssZ</i> is the date/time in Generalized Time form at which the

Parameter	Description
	connection was opened. This value gives the time in relation to Greenwich Mean Time. The hours are set with a 24-hour clock. The z at the end indicates that the time is relative to Greenwich Mean Time.
Default Value	
Syntax	GeneralizedTime
Example	nsDS5ReplicaLastUpdateStart: 20070504122055Z

### 3.8.14. nsDS5ReplicaLastUpdateStatus

This read-only attribute provides the status for the most recent replication schedule updates. The format is a numeric code followed by a short string. Zero (0) means success.

Parameter	Description
Entry DN	cn= <i>ReplicationAgreementName</i> , cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	0 (no replication sessions started), followed by any other error or status message
Default Value	
Syntax	DirectoryString
Example	nsDS5ReplicaLastUpdateStatus: 0 replica acquired successfully

### 3.8.15. nsDS5ReplicaPort

This attribute sets the port number for the remote server containing the replica. Once this attribute has been set, it cannot be modified.

Parameter	Description
Entry DN	cn= <i>ReplicationAgreementName</i> , cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	Port number for the remote server containing the replica
Default Value	
Syntax	Integer
Example	nsDS5ReplicaPort:389

### 3.8.16. nsDS5ReplicaReapActive

This read-only attribute specifies whether the background task that removes old tombstones (deleted entries) from the database is active. See [Section 3.7.10](#), “*nsDS5ReplicaTombstonePurgeInterval*” for more information about this task. A value of zero (0) means that the task is inactive, and a value of 1 means that the task is active. If this value is set manually, the server ignores the modify request.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	0   1
Default Value	
Syntax	Integer
Example	nsDS5ReplicaReapActive: 0

### 3.8.17. nsDS5BeginReplicaRefresh

Initializes the replica. This attribute is absent by default. However, if this attribute is added with a value of `start`, then the server initializes the replica and removes the attribute value. To monitor the status of the initialization procedure, poll for this attribute. When initialization is finished, the attribute is removed from the entry, and the other monitoring attributes can be used for detailed status inquiries.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	stop   start
Default Value	
Syntax	DirectoryString
Example	nsDS5BeginReplicaRefresh: start

### 3.8.18. nsDS5ReplicaRoot

This attribute sets the DN at the root of a replicated area. This attribute must have the same value as the suffix of the database being replicated and cannot be modified.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	Suffix of the database being replicated - same as <i>suffixDN</i> above

Parameter	Description
Default Value	
Syntax	DirectoryString
Example	nsDS5ReplicaRoot: "dc=example,dc=com"

### 3.8.19. nsDS5ReplicaSessionPauseTime

This attribute sets the amount of time in seconds a supplier should wait between update sessions. The default value is 0. If the attribute is set to a negative value, Directory Server sends the client a message and an LDAP\_UNWILLING\_TO\_PERFORM error code.

The *nsDS5ReplicaSessionPauseTime* attribute works in conjunction with the *nsDS5ReplicaBusyWaitTime* attribute. The two attributes are designed so that the *nsDS5ReplicaSessionPauseTime* interval is always at least one second longer than the interval specified for *nsDS5ReplicaBusyWaitTime*. The longer interval gives waiting suppliers a better chance to gain consumer access before the previous supplier can re-access the consumer.

- If either attribute is specified but not both, *nsDS5ReplicaSessionPauseTime* is set automatically to 1 second more than *nsDS5ReplicaBusyWaitTime*.
- If both attributes are specified, but *nsDS5ReplicaSessionPauseTime* is less than or equal to *nsDS5ReplicaBusyWaitTime*, *nsDS5ReplicaSessionPauseTime* is set automatically to 1 second more than *nsDS5ReplicaBusyWaitTime*.

When setting the values, ensure that the *nsDS5ReplicaSessionPauseTime* interval is at least 1 second longer than the interval specified for *nsDS5ReplicaBusyWaitTime*. Increase the interval as needed until there is an acceptable distribution of consumer access among the suppliers.

Set the *nsDS5ReplicaSessionPauseTime* attribute at any time by using `changetype:modify` with the `replace` operation. The change takes effect for the next update session if one is already in progress.

If Directory Server has to reset the value of *nsDS5ReplicaSessionPauseTime* automatically, the value is changed internally only. The change is not visible to clients, and it is not saved to the configuration file. From an external viewpoint, the attribute value appears as originally set.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , cn=replica, cn= <i>suffixDN</i> , cn=mapping tree, cn=config
Valid Values	Any valid integer
Default Value	0
Syntax	Integer
Example	nsDS5ReplicaSessionPauseTime: 0

### 3.8.20. nsDS5ReplicatedAttributeList

This allowed attribute specifies any attributes that are *not* replicated to a consumer server. Fractional replication allows databases to be replicated across slow connections or to less secure consumers while still protecting sensitive information. By default, all attributes are replicated, and this attribute is not present. For more information on fractional replication, see the "Managing Replication" chapter in the *Directory Server Administration Guide*.



#### NOTE

To maintain data integrity, the consumer server must be a read-only server.

Parameter	Description
Entry DN	<code>cn=ReplicationAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config</code>
Valid Range	
Default Value	
Syntax	DirectoryString
Example	<code>nsDS5ReplicatedAttributeList: (objectclass=*) \$ EXCLUDE salary userPassword manager</code>

### 3.8.21. nsDS5ReplicaTimeout

This allowed attribute specifies the number of seconds outbound LDAP operations waits for a response from the remote replica before timing out and failing. If the server writes `warning: timed out waiting` messages in the error log file, then increase the value of this attribute.

Find out the amount of time the operation actually lasted by examining the access log on the remote machine, and then set the `nsDS5ReplicaTimeout` attribute accordingly to optimize performance.

Parameter	Description
Entry DN	<code>cn=ReplicationAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config</code>
Valid Range	0 to maximum 32-bit integer value (2147483647) in seconds
Default Value	600
Syntax	Integer
Example	<code>nsDS5ReplicaTimeout: 600 seconds</code>

### 3.8.22. nsDS5ReplicaTransportInfo

This attribute sets the type of transport used for transporting data to and from the replica. The attribute values can be either SSL, which means that the connection is established over SSL, or LDAP, which means that regular LDAP connections are used. If this attribute is absent, then regular LDAP connections are used. This attribute cannot be modified once it is set.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	SSL   LDAP
Default Value	absent
Syntax	DirectoryString
Example	nsDS5ReplicaTransportInfo: LDAP

### 3.8.23. nsDS5ReplicaUpdateInProgress

This read-only attribute states whether or not a replication update is in progress.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Values	true   false
Default Value	
Syntax	DirectoryString
Example	nsDS5ReplicaUpdateInProgress: true

### 3.8.24. nsDS5ReplicaUpdateSchedule

This multi-valued attribute specifies the replication schedule and can be modified. Changes made to this attribute take effect immediately. Modifying this value can be useful to pause replication and resume it later. For example, if this value is set to `0000-0001 0`, this in effect causes the server to stop sending updates for this replication agreement. The server continues to store them for replay later. If the value is later changed back to `0000-2359 0123456`, this makes replication immediately resume and sends all pending changes.

Parameter	Description
Entry DN	<i>cn=ReplicationAgreementName</i> , <i>cn=replica</i> , <i>cn=suffixDN</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
Valid Range	Time schedule presented as <i>XXXX-YYYY 0123456</i> , where <i>XXXX</i> is the starting hour, <i>YYYY</i> is the finishing hour, and the numbers

Parameter	Description
	0123456 are the days of the week starting with Sunday.
Default Value	0000-2359 0123456 (all the time)
Syntax	Integer
Example	nsDS5ReplicaUpdateSchedule: 0000-2359 0123456

### 3.8.25. nsDS50ruv

This attribute stores the last replica update vector (RUV) read from the consumer of this replication agreement. It is always present and must not be changed.

### 3.9. Synchronization Attributes under cn=syncAgreementName, cn=WindowsReplica,cn="suffixName", cn=mapping tree, cn=config

The synchronization attributes that concern the synchronization agreement are stored under `cn=syncAgreementName`, `cn=WindowsReplica`, `cn=suffixDN`, `cn=mapping tree`, `cn=config`. The `cn=syncAgreementName` entry is an instance of the `nsDSWindowsReplicationAgreement` object class. For synchronization agreement configuration attributes to be taken into account by the server, this object class (in addition to the `top` object class) must be present in the entry. Synchronization agreements are configured only on databases that are enabled to synchronize with Windows Active Directory servers.

Parameter	Description
cn	nsDS5ReplicaLastUpdateEnd
description	nsDS5ReplicaLastUpdateStart
nsDS5ReplicaBindDN (the Windows sync manager ID)	nsDS5ReplicaLastUpdateStatus
nsDS5ReplicaBindMethod	nsDS5ReplicaPort
nsDS5ReplicaBusyWaitTime	nsDS5ReplicaRoot
nsDS5ReplicaChangesSentSinceStartup	nsDS5ReplicaSessionPauseTime
nsDS5ReplicaCredentials (the Windows sync manager password)	nsDS5ReplicaTimeout
nsDS5ReplicaHost (the Windows host)	nsDS5ReplicaTransportInfo
nsDS5ReplicaLastInitEnd	nsDS5ReplicaUpdateInProgress
nsDS5ReplicaLastInitStart	nsDS5ReplicaUpdateSchedule
nsDS5ReplicaLastInitStatus	nsDS50ruv

**Table 2.7. List of attributes shared between replication and synchronization agreements**

### 3.9.1. nsds7DirectoryReplicaSubtree

The suffix or DN of the Directory Server subtree that is being synchronized.

Parameter	Description
Entry DN	cn=syncAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Any valid suffix or subsuffix
Default Value	
Syntax	DirectoryString
Example	nsDS7DirectoryReplicaSubtree: ou=People,dc=example,dc=com

### 3.9.2. nsds7DirsyncCookie

This string is created by Active Directory DirSync and gives the state of the Active Directory Server at the time of the last synchronization. The old cookie is sent to Active Directory with each Directory Server update; a new cookie is returned along with the Windows directory data. This means only entries which have changed since the last synchronization are retrieved.

Parameter	Description
Entry DN	cn=syncAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Any string
Default Value	
Syntax	DirectoryString
Example	nsDS7DirsyncCookie::khDKJFBZsjBDSCkjsdhIU74DJJBXDhfvjm

### 3.9.3. nsds7NewWinGroupSyncEnabled

This attribute sets whether a new group created in the Windows sync peer is automatically synchronized by creating a new group on the Directory Server.

Parameter	Description
Entry DN	cn=syncAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	on   off

Parameter	Description
Default Value	
Syntax	DirectoryString
Example	nsDS7NewWinGroupSyncEnabled: on

### 3.9.4. nsds7NewWinUserSyncEnabled

This attribute sets whether a new entry created in the Windows sync peer is automatically synchronized by creating a new entry on the Directory Server.

Parameter	Description
Entry DN	cn=syncAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	on   off
Default Value	
Syntax	DirectoryString
Example	nsDS7NewWinUserSyncEnabled: on

### 3.9.5. nsds7WindowsDomain

This attribute sets the name of the Windows domain to which the Windows sync peer belongs.

Parameter	Description
Entry DN	cn=syncAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Any valid domain name
Default Value	
Syntax	DirectoryString
Example	nsDS7WinndowsDomain: DOMAINWORLD

### 3.9.6. nsds7WindowsReplicaSubtree

The suffix or DN of the Windows subtree that is being synchronized.

Parameter	Description
Entry DN	cn=syncAgreementName, cn=replica, cn=suffixDN, cn=mapping tree, cn=config
Valid Values	Any valid suffix or subsuffix
Default Value	
Syntax	DirectoryString

Parameter	Description
Example	nsDS7WindowsReplicaSubtree: cn=Users, dc=domain, dc=com

### 3.10. cn=monitor

Information used to monitor the server is stored under `cn=monitor`. This entry and its children are read-only; clients cannot directly modify them. The server updates this information automatically. This section describes the `cn=monitor` attributes. The only attribute that can be changed by a user to set access control is the `aci` attribute.

#### connection.

This attribute lists open connections. These are given in the following format:

```
connection: A:YYYYMMDDhhmmssZ:B:C:D:E
```

For example:

```
connection: 31:20010201164808Z:45:45::cn=directory manager
```

- *A* is the connection number, which is the number of the slot in the connection table associated with this connection. This is the number logged as `slot=A` in the access log message when this connection was opened, and usually corresponds to the file descriptor associated with the connection. The attribute `dTableSize` shows the total size of the connection table.
- *YYYYMMDDhhmmssZ* is the date and time, in GeneralizedTime form, at which the connection was opened. This value gives the time in relation to Greenwich Mean Time.
- *B* is the number of operations received on this connection.
- *C* is the number of completed operations.
- *D* is `r` if the server is in the process of reading BER from the network, empty otherwise. This value is usually empty (as in the example).
- *E* this is the bind DN. This may be empty or have value of `NULLDN` for anonymous connections.

#### currentConnections.

This attribute shows the number of currently open and active Directory Server connections.

#### totalConnections.

This attribute shows the total number of Directory Server connections. This number includes connections that have been opened and closed since the server was last started in addition to the *currentConnections*.

### **dTableSize.**

This attribute shows the size of the Directory Server connection table. Each connection is associated with a slot in this table, and usually corresponds to the file descriptor used by this connection. See [Section 3.1.37, “nsslapd-conntablesize”](#) for more information.

### **readWaiters.**

This attribute shows the number of connections where some requests are pending and not currently being serviced by a thread in Directory Server.

### **opsInitiated.**

This attribute shows the number of Directory Server operations initiated.

### **opsCompleted.**

This attribute shows the number of Directory Server operations completed.

### **entriesSent.**

This attribute shows the number of entries sent by Directory Server.

### **bytesSent.**

This attribute shows the number of bytes sent by Directory Server.

### **currentTime.**

This attribute shows the current time, given in Greenwich Mean Time (indicated by *generalizedTime* syntax z notation; for example, 20070202131102Z).

### **startTime.**

This attribute shows the Directory Server start time given in Greenwich Mean Time, indicated by *generalizedTime* syntax z notation. For example, 20070202131102Z.

### **version.**

This attribute shows the Directory Server vendor, version, and build number. For example, Red Hat/8.0.1 B2007.274.08.

### **threads.**

This attribute shows the number of threads used by the Directory Server. This should correspond to *nsslapd-threadnumber* in *cn=config*.

**nbackEnds.**

This attribute shows the number of Directory Server database backends.

**backendMonitorDN.**

This attribute shows the DN for each Directory Server database backend. For further information on monitoring the database, see the following sections:

- [Section 4.8, “Database Attributes under cn=attributeName, cn=encrypted attributes, cn=database\\_name, cn=ldbm database, cn=plugins, cn=config”](#)
- [Section 4.4, “Database Attributes under cn=database, cn=monitor, cn=ldbm database, cn=plugins, cn=config”](#)
- [Section 4.6, “Database Attributes under cn=monitor, cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config”](#)
- [Section 5.4, “Database Link Attributes under cn=monitor, cn=database instance name, cn=chaining database, cn=plugins, cn=config”](#)

**3.11. cn=replication**

This entry has no attributes. When configuring legacy replication, these entries are stored under this `cn=replication` node, which serves as a placeholder.

**3.12. cn=SNMP**

SNMP configuration attributes are stored under `cn=SNMP, cn=config`. The `cn=SNMP` entry is an instance of the `nsSNMP` object class.

**3.12.1. nssnmpenabled**

This attribute sets whether SNMP is enabled.

Parameter	Description
Entry DN	<code>cn=SNMP, cn=config</code>
Valid Values	<code>on</code>   <code>off</code>
Default Value	<code>on</code>
Syntax	DirectoryString
Example	<code>nssnmpenabled: off</code>

**3.12.2. nssnmporganization**

This attribute sets the organization to which the Directory Server belongs.

Parameter	Description
Entry DN	cn=SNMP, cn=config
Valid Values	Organization name
Default Value	
Syntax	DirectoryString
Example	nssnmporganization: Red Hat, Inc.

### 3.12.3. nssnmplocation

This attribute sets the location within the company or organization where the Directory Server resides.

Parameter	Description
Entry DN	cn=SNMP, cn=config
Valid Values	Location
Default Value	
Syntax	DirectoryString
Example	nssnmplocation: B14

### 3.12.4. nssnmpcontact

This attribute sets the email address of the person responsible for maintaining the Directory Server.

Parameter	Description
Entry DN	cn=SNMP, cn=config
Valid Values	Contact email address
Default Value	
Syntax	DirectoryString
Example	nssnmpcontact: jerome@example.com

### 3.12.5. nssnmpdescription

Provides a unique description of the Directory Server instance.

Parameter	Description
Entry DN	cn=SNMP, cn=config
Valid Values	Description
Default Value	

Parameter	Description
Syntax	DirectoryString
Example	nssnmpdescription: Employee directory instance

### 3.12.6. nssnmpmasterhost

*nssnmpmasterhost* is deprecated. This attribute is deprecated with the introduction of *net-snmp*. The attribute still appears in *dse.ldif* but without a default value.

Parameter	Description
Entry DN	cn=SNMP, cn=config
Valid Values	machine hostname or localhost
Default Value	<blank>
Syntax	DirectoryString
Example	nssnmpmasterhost: localhost

### 3.12.7. nssnmpmasterport

The *nssnmpmasterport* attribute was deprecated with the introduction of *net-snmp*. The attribute still appears in *dse.ldif* but without a default value.

Parameter	Description
Entry DN	cn=SNMP, cn=config
Valid Values	Operating system dependent port number. See the operating system documentation for further information.
Default Value	<blank>
Syntax	Integer
Example	nssnmpmasterport: 199

## 3.13. SNMP Statistic Attributes

[Table 2.8, “SNMP Statistic Attributes”](#) contains read-only attributes which list the statistics available for LDAP and SNMP clients. Unless otherwise noted, the value for the given attribute is the number of requests received by the server or results returned by the server since startup. Some of these attributes are not used by or are not applicable to the Directory Server but are still required to be present by SNMP clients.

Attribute	Description
AnonymousBinds	This shows the number of anonymous bind

Attribute	Description
	requests.
UnAuthBinds	This shows the number of unauthenticated (anonymous) binds.
SimpleAuthBinds	This shows the number of LDAP simple bind requests (DN and password).
StrongAuthBinds	This shows the number of LDAP SASL bind requests, for all SASL mechanisms.
BindSecurityErrors	This shows the number of number of times an invalid password was given in a bind request.
InOps	This shows the total number of all requests received by the server.
ReadOps	Not used. This value is always 0.
CompareOps	This shows the number of LDAP compare requests.
AddEntryOps	This shows the number of LDAP add requests.
RemoveEntryOps	This shows the number of LDAP delete requests.
ModifyEntryOps	This shows the number of LDAP modify requests.
ModifyRDNops	This shows the number of LDAP modify RDN (modrdn) requests.
ListOps	Not used. This value is always 0.
SearchOps	This shows the number of LDAP search requests.
OneLevelSearchOps	This shows the number of one-level search operations.
WholeSubtreeSearchOps	This shows the number of subtree-level search operations.
Referrals	This shows the number of LDAP referrals returned.
Chainings	Not used. This value is always 0.
SecurityErrors	This shows the number of errors returned that were security related, such as invalid passwords, unknown or invalid authentication methods, or stronger authentication required.
Errors	This shows the number of errors returned.
Connections	This shows the number of currently open connections.

Attribute	Description
ConnectionSeq	This shows the total number of connections opened, including both currently open and closed connections.
BytesRecv	This shows the number of bytes received.
BytesSent	This shows the number of bytes sent.
EntriesReturned	This shows the number of entries returned as search results.
ReferralsReturned	This provides information on referrals returned as search results (continuation references).
MasterEntries	Not used. This value is always 0.
CopyEntries	Not used. This value is always 0.
CacheEntries <sup>a</sup>	If the server has only one database backend, this is the number of entries cached in the entry cache. If the server has more than one database backend, this value is 0, and see the monitor entry for each one for more information.
CacheHits <sup>a</sup>	If the server has only one database backend, this is the number of entries returned from the entry cache, rather than from the database, for search results. If the server has more than one database backend, this value is 0, and see the monitor entry for each one for more information.
SlaveHits	Not used. This value is always 0.

<sup>a</sup> *CacheEntries* and *CacheHits* are updated every ten (10) seconds. Red Hat strongly encourages using the database backend specific monitor entries for this and other database information.

## Table 2.8. SNMP Statistic Attributes

### 3.14. cn=tasks

This entry has no attributes and serves as the parent and container entry for the individual task entries.

### 3.15. cn=uniqueid generator

The unique ID generator configuration attributes are stored under `cn=uniqueid generator,cn=config`. The `cn=uniqueid generator` entry is an instance of the `extensibleObject` object class.

### **nsstate.**

This attribute saves the state of the unique ID generator across server restarts. This attribute is maintained by the server. Do not edit it.

Parameter	Description
Entry DN	cn=uniqueid generator, cn=config
Valid Values	
Default Value	
Syntax	DirectoryString
Example	nsstate: Abld0c3oMIDUntiLCyYNGgAAAAAAAAAA

# Plug-in Implemented Server Functionality Reference

This chapter contains reference information on Red Hat Directory Server plug-ins.

The configuration for each part of Directory Server plug-in functionality has its own separate entry and set of attributes under the subtree `cn=plugins, cn=config`.

```
dn: cn=Telephone Syntax, cn=plugins, cn=config
objectclass: top
objectclass: nsSlapdPlugin
objectclass: extensibleObject
cn: Telephone Syntax
nsslapd-pluginPath: libsyntax-plugin
nsslapd-pluginInitfunc: tel_init
nsslapd-pluginType: syntax
nsslapd-pluginEnabled: on
```

Some of these attributes are common to all plug-ins while others may be particular to a specific plug-in. Check which attributes are currently being used by a given plug-in by performing an `ldapsearch` on the `cn=config` subtree.

All plug-ins are instances of the `nsSlapdPlugin` object class, which in turn inherits from the `extensibleObject` object class. For plug-in configuration attributes to be taken into account by the server, both of these object classes (in addition to the `top` object class) must be present in the entry, as shown in the following example:

```
dn:cn=ACL Plugin, cn=plugins, cn=config
objectclass:top
objectclass:nsSlapdPlugin
objectclass:extensibleObject
```

## 1. Server Plug-in Functionality Reference

The following tables provide a quick overview of the plug-ins provided with Directory Server, along with their configurable options, configurable arguments, default setting, dependencies, general performance-related information, and further reading. These tables assist in weighing plug-in performance gains and costs and choose the optimal settings for the deployment. The *Further Information* section cross-references further reading, where this is available.

### 1.1. 7-bit Check Plug-in

Plug-in Parameter	Description
Plug-in Name	7-bit check (NS7bitAtt)
DN of Configuration Entry	cn=7-bit check, cn=plugins, cn=config

Plug-in Parameter	Description
Description	Checks certain attributes are 7-bit clean
Configurable Options	on   off
Default Setting	on
Configurable Arguments	List of attributes ( <code>uid mail userpassword</code> ) followed by "," and then suffixes on which the check is to occur.
Dependencies	None
Performance Related Information	None
Further Information	If the Directory Server uses non-ASCII characters, such as Japanese, turn this plug-in off.

### 1.2. ACL Plug-in

Plug-in Parameter	Description
Plug-in Name	ACL Plug-in
DN of Configuration Entry	<code>cn=ACL Plugin, cn=plugins, cn=config</code>
Description	ACL access check plug-in
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Access control incurs a minimal performance hit. Leave this plug-in enabled since it is the primary means of access control for the server.
Further Information	See the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i> .

### 1.3. ACL Preoperation Plug-in

Plug-in Parameter	Description
Plug-in Name	ACL Preoperation
DN of Configuration Entry	<code>cn=ACL preoperation, cn=plugins, cn=config</code>
Description	ACL access check plug-in
Configurable Options	on   off
Default Setting	on

Plug-in Parameter	Description
Configurable Arguments	None
Dependencies	Database
Performance Related Information	Access control incurs a minimal performance hit. Leave this plug-in enabled since it is the primary means of access control for the server.
Further Information	See the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i> .

## 1.4. Attribute Uniqueness Plug-in

Plug-in Parameter	Description
Plug-in Name	Attribute Uniqueness Plug-in
DN of Configuration Entry	cn=Attribute Uniqueness, cn=plugins, cn=config
Description	Checks that the values of specified attributes are unique each time a modification occurs on an entry. For example, most sites require that a user ID and email address be unique.
Configurable Options	on   off
Default Setting	off
Configurable Arguments	To check for UID attribute uniqueness in all listed subtrees, enter <code>uid "DN" "DN" . . .</code> . However, to check for UID attribute uniqueness when adding or updating entries with the <code>requiredObjectClass</code> , enter <code>attribute="uid" MarkerObjectclass = "ObjectClassName" and, optionally requiredObjectClass = "ObjectClassName"</code> . This starts checking for the required object classes from the parent entry containing the <code>ObjectClass</code> as defined by the <code>MarkerObjectClass</code> attribute.
Dependencies	Database
Performance Related Information	Directory Server provides the UID Uniqueness Plug-in by default. To ensure unique values for other attributes, create instances of the Attribute Uniqueness Plug-in for those attributes. See the "Using the Attribute Uniqueness Plug-in" in the <i>Directory</i>

Plug-in Parameter	Description
	<p><i>Server Administration Guide</i> for more information about the Attribute Uniqueness Plug-in.</p> <p>The UID Uniqueness Plug-in is off by default due to operation restrictions that need to be addressed before enabling the plug-in in a multi-master replication environment. Turning the plug-in on may slow down Directory Server performance.</p>
Further Information	See the "Using the Attribute Uniqueness Plug-in" in the <i>Directory Server Administration Guide</i> .

### 1.5. Binary Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Binary Syntax
DN of Configuration Entry	cn=Binary Syntax, cn=plugins, cn=config
Description	Syntax for handling binary data
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

### 1.6. Boolean Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Boolean Syntax
DN of Configuration Entry	cn=Boolean Syntax, cn=plugins, cn=config
Description	Syntax for handling booleans
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None

Plug-in Parameter	Description
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.7. Case Exact String Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Case Exact String Syntax
DN of Configuration Entry	cn=Case Exact String Syntax, cn=plugins, cn=config
Description	Syntax for handling case-sensitive strings
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.8. Case Ignore String Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Case Ignore String Syntax
DN of Configuration Entry	cn=Case Ignore String Syntax, cn=plugins, cn=config
Description	Syntax for handling case-insensitive strings
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.9. Chaining Database Plug-in

Plug-in Parameter	Description
Plug-in Name	Chaining Database
DN of Configuration Entry	cn=Chaining database, cn=plugins, cn=config
Description	Syntax for handling DNs
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	There are many performance related tuning parameters involved with the chaining database. See the "Maintaining Database Links" section in the <i>Directory Server Administration Guide</i> .
Further Information	A chaining database is also known as a <i>database link</i> . Database links are described in the "Configuring Directory Databases" chapter in the <i>Directory Server Administration Guide</i> .

## 1.10. Class of Service Plug-in

Plug-in Parameter	Description
Plug-in Name	Class of Service
DN of Configuration Entry	cn=Class of Service, cn=plugins, cn=config
Description	Allows for sharing of attributes between entries
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Leave this plug-in running at all times.
Further Information	See the "Advanced Entry Management" chapter in the <i>Directory Server Administration Guide</i> .

## 1.11. Country String Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Country String Syntax Plug-in
DN of Configuration Entry	cn=Country String Syntax, cn=plugins, cn=config
Description	Syntax for handling countries
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.12. Distinguished Name Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Distinguished Name Syntax
DN of Configuration Entry	cn=Distinguished Name Syntax, cn=plugins, cn=config
Description	Syntax for handling DNs
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.13. Generalized Time Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Generalized Time Syntax
DN of Configuration Entry	cn=Generalized Time Syntax, cn=plugins, cn=config
Description	Syntax for dealing with dates, times and time zones

Plug-in Parameter	Description
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	The Generalized Time String consists of a four digit year, two digit month (for example, 01 for January), two digit day, two digit hour, two digit minute, two digit second, an optional decimal part of a second, and a time zone indication. Red Hat strongly recommends using the Z time zone indication, which indicates Greenwich Mean Time.

### 1.14. HTTP Client Plug-in

Plug-in Parameter	Description
Plug-in Name	HTTP Client
DN of Configuration Entry	cn=HTTP Client, cn=plugins, cn=config
Description	HTTP client plug-in
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	Database
Performance Related Information	
Further Information	

### 1.15. Integer Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Integer Syntax
DN of Configuration Entry	cn=Integer Syntax, cn=plugins, cn=config
Description	Syntax for handling integers
Configurable Options	on   off
Default Setting	on

Plug-in Parameter	Description
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.16. Internationalization Plug-in

Plug-in Parameter	Description
Plug-in Name	Internationalization Plug-in
DN of Configuration Entry	cn=Internationalization Plugin, cn=plugins, cn=config
Description	Syntax for handling DN's
Configurable Options	on   off
Default Setting	on
Configurable Arguments	The Internationalization Plug-in has one argument, which must not be modified, which specifies the location of the <code>/etc/dirsrv/config/slapd-collations.conf</code> file. This file stores the collation orders and locales used by the Internationalization Plug-in.
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	See the "Internationalization" appendix and the section on "Searching an Internationalized Directory" in the "Finding Directory Entries" appendix in the <i>Directory Server Administration Guide</i> .

## 1.17. JPEG Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	JPEG Syntax Plug-in
DN of Configuration Entry	cn=JPEG Syntax,cn=plugins,cn=config
Description	Syntax for JPEG data.

Plug-in Parameter	Description
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

### 1.18. Idbm database Plug-in

Plug-in Parameter	Description
Plug-in Name	ldbm database Plug-in
DN of Configuration Entry	cn=ldbm database, cn=plugins, cn=config
Description	Implements local databases
Configurable Options	
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	See <a href="#">Section 4, "Database Plug-in Attributes"</a> for further information on database configuration.
Further Information	See the "Configuring Directory Databases" chapter in the <i>Directory Server Administration Guide</i> .

### 1.19. Legacy Replication Plug-in

Plug-in Parameter	Description
Plug-in Name	Legacy Replication Plug-in
DN of Configuration Entry	cn=Legacy Replication plug-in, cn=plugins, cn=config
Description	Enables a current version Directory Server to be a consumer of a 4.x supplier
Configurable Options	on   off
Default Setting	off
Configurable Arguments	None. This plug-in can be disabled if the

Plug-in Parameter	Description
	server is not (and never will be) a consumer of a 4.x server.
Dependencies	Database
Performance Related Information	None
Further Information	See the "Managing Replication" chapter in the <i>Directory Server Administration Guide</i> .

## 1.20. Multi-master Replication Plug-in

Plug-in Parameter	Description
Plug-in Name	Multi-master Replication Plug-in
DN of Configuration Entry	cn=Multimaster Replication plugin, cn=plugins, cn=config
Description	Enables replication between two current Directory Servers
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	Database
Performance Related Information	
Further Information	Turn this plug-in off if one server will never replicate. See the "Managing Replication" chapter in the <i>Directory Server Administration Guide</i> .

## 1.21. Octet String Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Octet String Syntax
DN of Configuration Entry	cn=Octet String Syntax, cn=plugins, cn=config
Description	Syntax for handling octet strings
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in.

Plug-in Parameter	Description
	Red Hat recommends leaving this plug-in running at all times.
Further Information	

### 1.22. OID Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	OID Syntax Plug-in
DN of Configuration Entry	cn=OID Syntax,cn=plugins,cn=config
Description	Syntax for object identifiers (OID).
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

### 1.23. CLEAR Password Storage Plug-in

Plug-in Parameter	Description
Plug-in Name	CLEAR
DN of Configuration Entry	cn=CLEAR, cn>Password Storage Schemes, cn=plugins, cn=config
Description	CLEAR password storage scheme used for password encryption
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	See the "User Account Management" chapter in the <i>Directory Server Administration Guide</i> .

## 1.24. CRYPT Password Storage Plug-in

Plug-in Parameter	Description
Plug-in Name	CRYPT
DN of Configuration Entry	cn=CRYPT, cn>Password Storage Schemes, cn=plugins, cn=config
Description	CRYPT password storage scheme used for password encryption
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	See the "User Account Management" chapter in the <i>Directory Server Administration Guide</i> .

## 1.25. NS-MTA-MD5 Password Storage Scheme Plug-in

Plug-in Parameter	Description
Plug-in Name	NS-MTA-MD5
DN of Configuration Entry	cn=NS-MTA-MD5, cn>Password Storage Schemes, cn=plugins, cn=config
Description	NS-MTA-MD5 password storage scheme for password encryption
Configurable Options	on   off
Default Setting	off
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	The NS-MTA-MD5 password storage scheme cannot be used to encrypt passwords. The storage scheme is still present but only for backward compatibility; that is, if the data in the directory still contains passwords encrypted with the NS-MTA-MD5 password storage scheme.

Plug-in Parameter	Description
	See the "User Account Management" chapter in the <i>Directory Server Administration Guide</i> .

## 1.26. SHA Password Storage Scheme Plug-in

Plug-in Parameter	Description
Plug-in Name	SHA
DN of Configuration Entry	cn=SHA, cn=Password Storage Schemes, cn=plugins, cn=config cn=SHA256, cn=Password Storage Schemes, cn=plugins, cn=config cn=SHA384, cn=Password Storage Schemes, cn=plugins, cn=config cn=SHA512, cn=Password Storage Schemes, cn=plugins, cn=config
Description	SHA password storage scheme for password encryption
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	If there are no passwords encrypted using the SHA password storage scheme, this plug-in can be turned off. To encrypt the password with the SHA password storage scheme, Red Hat recommends choosing SSHA instead, as SSHA is a far more secure option.
Further Information	See the "User Account Management" chapter in the <i>Directory Server Administration Guide</i> .

## 1.27. SSHA Password Storage Scheme Plug-in

Plug-in Parameter	Description
Plug-in Name	SSHA
DN of Configuration Entry	cn=SSHA, cn=Password Storage Schemes, cn=plugins, cn=config cn=SSHA256, cn=Password Storage Schemes, cn=plugins, cn=config

Plug-in Parameter	Description
	cn=SSHA384,cn=Password Storage Schemes,cn=plugins,cn=config cn=SSHA512,cn=Password Storage Schemes,cn=plugins,cn=config
Description	SSHA password storage scheme for password encryption
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	See the "User Account Management" chapter in the <i>Directory Server Administration Guide</i> .

## 1.28. Postal Address String Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Postal Address Syntax
DN of Configuration Entry	cn=Postal Address Syntax, cn=plugins, cn=config
Description	Syntax used for handling postal addresses
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 1.29. PTA Plug-in

Plug-in Parameter	Description
Plug-in Name	Pass-Through Authentication Plug-in
DN of Configuration Entry	cn=Pass Through Authentication, cn=plugins, cn=config

Plug-in Parameter	Description
Description	Enables <i>pass-through authentication</i> , the mechanism which allows one directory to consult another to authenticate bind requests.
Configurable Options	on   off
Default Setting	off
Configurable Arguments	ldap://example.com:389/o=example
Dependencies	None
Performance Related Information	Pass-through authentication slows down bind requests a little because they have to make an extra hop to the remote server. See the "Using Pass-through Authentication" chapter in the <i>Directory Server Administration Guide</i> .
Further Information	See the "Using the Pass-through Authentication Plug-in" chapter in the <i>Directory Server Administration Guide</i> .

### 1.30. Referential Integrity Postoperation Plug-in

Plug-in Parameter	Description
Plug-in Name	Referential Integrity Postoperation
DN of Configuration Entry	cn=Referential Integrity Postoperation, cn=plugins, cn=config
Description	Enables the server to ensure referential integrity
Configurable Options	All configuration and on   off
Default Setting	off
Configurable Arguments	<p>When enabled, the post-operation Referential Integrity Plug-in performs integrity updates on the <i>member</i>, <i>uniquemember</i>, <i>owner</i> and <i>seeAlso</i> attributes immediately after a delete or rename operation. The plug-in can be reconfigured to perform integrity checks on all other attributes:</p> <ul style="list-style-type: none"> <li>• Check for referential integrity.</li> </ul> <p>-1= no check for referential integrity                      0= check for referential integrity is performed immediately                      Positive integer= request for referential</p>

Plug-in Parameter	Description
	<p>integrity is queued and processed at a later stage. This positive integer serves as a wake-up call for the thread to process the request at intervals corresponding to the integer (number of seconds) specified.</p> <ul style="list-style-type: none"> <li>Log file for storing the change; for example <code>/var/log/dirsrv/slapd-<i>instance_name</i>/referint.</code></li> <li>All the additional attribute names to be checked for referential integrity.</li> </ul>
Dependencies	Database
Performance Related Information	The Referential Integrity Plug-in should be enabled only on one master in a multimaster replication environment to avoid conflict resolution loops. When enabling the plug-in on chained servers, be sure to analyze the performance resource and time needs as well as integrity needs; integrity checks can be time consuming and demanding on memory and CPU. All attributes specified must be indexed for both presence and equality.
Further Information	See the "Managing Indexes" chapter for information about how to index attributes used for referential integrity checking and the "Configuring Directory Databases" chapter in the <i>Directory Server Administration Guide</i> .

### 1.31. Retro Changelog Plug-in

Plug-in Parameter	Description
Plug-in Name	Retro Changelog Plug-in
DN of Configuration Entry	cn=Retro Changelog Plugin, cn=plugins, cn=config
Description	Used by LDAP clients for maintaining application compatibility with Directory Server 4.x versions. Maintains a log of all changes occurring in the Directory Server. The retro changelog offers the same functionality as the changelog in the 4.x versions of Directory Server. This plug-in exposes the <code>cn=changelog</code> suffix to clients, so that clients

Plug-in Parameter	Description
	can use this suffix with or without persistent search for simple sync applications.
Configurable Options	on   off
Default Setting	off
Configurable Arguments	See <a href="#">Section 6, "Retro Changelog Plug-in Attributes"</a> for further information on the two configuration attributes for this plug-in.
Dependencies	None
Performance Related Information	May slow down Directory Server update performance.
Further Information	See the "Managing Replication" chapter in the <i>Directory Server Administration Guide</i> .

### 1.32. Roles Plug-in

Plug-in Parameter	Description
Plug-in Name	Roles Plug-in
DN of Configuration Entry	cn=Roles Plugin, cn=plugins, cn=config
Description	Enables the use of roles in the Directory Server
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	Database
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	See the "Advanced Entry Management" chapter in the <i>Directory Server Administration Guide</i> .

### 1.33. Space Insensitive String Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Space Insensitive String Syntax
DN of Configuration Entry	cn=Space Insensitive String Syntax, cn=plugins, cn=config
Description	Syntax for handling space-insensitive values

Plug-in Parameter	Description
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	This plug-in enables the Directory Server to support <code>space</code> and <code>case insensitive</code> values. Applications can now search the directory using entries with ASCII space characters. For example, a search or compare operation that uses <code>jOHn Doe</code> will match entries that contain <code> johndoe</code> , <code>john doe</code> , and <code>John Doe</code> if the attribute's schema has been configured to use the space insensitive syntax. For more information about finding directory entries, refer to the "Finding Directory Entries" Appendix in the <i>Directory Server Administration Guide</i> .

### 1.34. State Change Plug-in

Plug-in Parameter	Description
Plug-in Name	State Change Plug-in
DN of Configuration Entry	cn=State Change Plugin, cn=plugins, cn=config
Description	Enables state-change-notification service
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	
Further Information	

### 1.35. Telephone Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	Telephone Syntax

Plug-in Parameter	Description
DN of Configuration Entry	cn=Telephone Syntax, cn=plugins, cn=config
Description	Syntax for handling telephone numbers
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

### 1.36. URI Syntax Plug-in

Plug-in Parameter	Description
Plug-in Name	URI Syntax
DN of Configuration Entry	cn=URI Syntax, cn=plugins, cn=config
Description	Syntax for handling URIs (Unique Resource Identifiers), including URLs (Unique Resource Locators)
Configurable Options	on   off
Default Setting	on
Configurable Arguments	None
Dependencies	None
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

### 1.37. Views Plug-in

Plug-in Parameter	Description
Plug-in Name	Views Plug-in
DN of Configuration Entry	cn=Views,cn=plugins,cn=config
Description	Enables the use of views in the Directory Server databases.
Configurable Options	on   off
Default Setting	on

Plug-in Parameter	Description
Configurable Arguments	None
Dependencies	Database
Performance Related Information	Do not modify the configuration of this plug-in. Red Hat recommends leaving this plug-in running at all times.
Further Information	

## 2. List of Attributes Common to All Plug-ins

This list provides a brief attribute description, the entry DN, valid range, default value, syntax, and an example for each attribute.

### 2.1. nsslapd-pluginPath

This attribute specifies the full path to the plug-in.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	Any valid path
Default Value	None
Syntax	DirectoryString
Example	nsslapd-pluginPath: uid-plugin

### 2.2. nsslapd-pluginInitfunc

This attribute specifies the plug-in function to be initiated.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	Any valid plug-in function
Default Value	None
Syntax	DirectoryString
Example	nsslapd-pluginInitfunc: NS7bitAttr_Init

### 2.3. nsslapd-pluginType

This attribute specifies the plug-in type. See [Section 3.3, “nsslapd-plugin-depends-on-type”](#) for further information.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	Any valid plug-in type
Default Value	None
Syntax	DirectoryString
Example	nsslapd-pluginType: preoperation

### 2.4. nsslapd-pluginEnabled

This attribute specifies whether the plug-in is enabled. This attribute can be changed over protocol but will only take effect when the server is next restarted.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-pluginEnabled: on

### 2.5. nsslapd-pluginId

This attribute specifies the plug-in ID.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	Any valid plug-in ID
Default Value	None
Syntax	DirectoryString
Example	nsslapd-pluginId: chaining database

### 2.6. nsslapd-pluginVersion

This attribute specifies the plug-in version.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	Any valid plug-in version

Plug-in Parameter	Description
Default Value	Product version number
Syntax	DirectoryString
Example	nsslapd-pluginVersion: 8.0

## 2.7. nsslapd-pluginVendor

This attribute specifies the vendor of the plug-in.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	Any approved plug-in vendor
Default Value	Red Hat, Inc.
Syntax	DirectoryString
Example	nsslapd-pluginVendor: Red Hat, Inc.

## 2.8. nsslapd-pluginDescription

This attribute provides a description of the plug-in.

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	
Default Value	None
Syntax	DirectoryString
Example	nsslapd-pluginDescription: acl access check plug-in

## 3. Attributes Allowed by Certain Plug-ins

### 3.1. nsslapd-pluginLoadNow

This attribute specifies whether to load all of the symbols used by a plug-in immediately (`true`), as well as all symbols references by those symbols, or to load the symbol the first time it is used (`false`).

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config

Plug-in Parameter	Description
Valid Values	true   false
Default Value	false
Syntax	DirectoryString
Example	nsslapd-pluginLoadNow: false

### 3.2. nsslapd-pluginLoadGlobal

This attribute specifies whether the symbols in dependent libraries are made visible locally (`false`) or to the executable and to all shared objects (`true`).

Plug-in Parameter	Description
Entry DN	cn=plug-in name, cn=plugins, cn=config
Valid Values	true   false
Default Value	false
Syntax	DirectoryString
Example	nsslapd-pluginLoadGlobal: false

### 3.3. nsslapd-plugin-depends-on-type

Multi-valued attribute used to ensure that plug-ins are called by the server in the correct order. Takes a value which corresponds to the type number of a plug-in, contained in the attribute `nsslapd-pluginType`. See [Section 2.3, “nsslapd-pluginType”](#) for further information. All plug-ins with a type value which matches one of the values in the following valid range will be started by the server prior to this plug-in. The following postoperation Referential Integrity Plug-in example shows that the database plug-in will be started prior to the postoperation Referential Integrity Plug-in.

Plug-in Parameter	Description
Entry DN	cn=referential integrity postoperation, cn=plugins, cn=config
Valid Values	database
Default Value	
Syntax	DirectoryString
Example	nsslapd-plugin-depends-on-type: database

### 3.4. nsslapd-plugin-depends-on-named

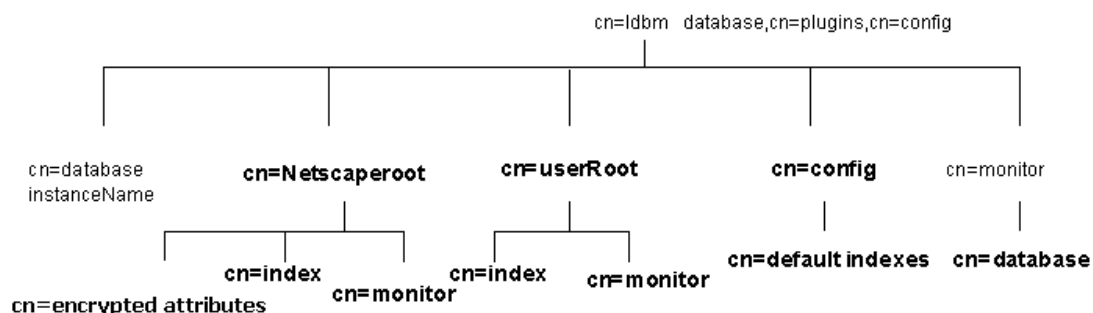
Multi-valued attribute used to ensure that plug-ins are called by the server in the correct order.

Takes a value which corresponds to the *cn* value of a plug-in. The plug-in with a *cn* value matching one of the following values will be started by the server prior to this plug-in. If the plug-in does not exist, the server fails to start. The following postoperation Referential Integrity Plug-in example shows that the Views plug-in is started before Roles. If Views is missing, the server is not going to start.

Plug-in Parameter	Description
Entry DN	cn=referential integrity postoperation, cn=plugins, cn=config
Valid Values	Class of Service
Default Value	
Syntax	DirectoryString
Example	nsslapd-plugin-depends-on-named: Views nsslapd-pluginId: roles

## 4. Database Plug-in Attributes

The database plug-in is also organized in an information tree, as shown in [Figure 3.1, "Database Plug-in"](#).



**Figure 3.1. Database Plug-in**

All plug-in technology used by the database instances is stored in the *cn=ldbm database* plug-in node. This section presents the additional attribute information for each of the nodes in bold in the *cn=ldbm database, cn=plugins, cn=config* information tree.

### 4.1. Database Attributes under **cn=config, cn=ldbm database, cn=plugins, cn=config**

This section covers global configuration attributes common to all instances are stored in the *cn=config, cn=ldbm database, cn=plugins, cn=config* tree node.

### 4.1.1. nsLookthroughLimit

This performance-related attribute specifies the maximum number of entries that the Directory Server will check when examining candidate entries in response to a search request. The Directory Manager DN, however, is, by default, unlimited and overrides any other settings specified here. It is worth noting that binder-based resource limits work for this limit, which means that if a value for the operational attribute `nsLookThroughLimit` is present in the entry as which a user binds, the default limit will be overridden. Attempting to set a value that is not a number or is too big for a 32-bit signed integer returns an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config
Valid Range	-1 to maximum 32-bit integer in entries (where -1 is unlimited)
Default Value	5000
Syntax	Integer
Example	nsLookthroughLimit: 5000

### 4.1.2. nsslapd-idlistscanlimit

This performance-related attribute, present by default, specifies the number of entry IDs that are searched during a search operation. Attempting to set a value that is not a number or is too big for a 32-bit signed integer returns an `LDAP_UNWILLING_TO_PERFORM` error message, with additional error information explaining the problem.

It is advisable to keep the default value to improve search performance. For a more detailed explanation of the effect of ID lists on search performance, refer to the "Managing Indexes" chapter in the *Directory Server Administration Guide*.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config
Valid Range	100 to the maximum 32-bit integer value (2147483647) entry IDs
Default Value	4000
Syntax	Integer
Example	nsslapd-idlistscanlimit: 4000

### 4.1.3. nsslapd-cache-autosize

This performance tuning-related attribute, which is turned off by default, specifies the percentage of free memory to use for all the combined caches. For example, if the value is set to 80, then 80 percent of the remaining free memory would be claimed for the cache. To run other servers on the machine, then set the value lower. Setting the value to 0 turns off the cache autosizing and uses the normal *nsslapd-cachememsize* and *nsslapd-dbcachesize* attributes.



#### NOTE

If the *nsslapd-cache-autosize* attribute and *nsslapd-cache-autosize-split* attribute are both set to high values, such as 100, then the Directory Server may fail to start and return an error message. To fix this issue, reset the *nsslapd-cache-autosize* and *nsslapd-cache-autosize-split* attributes to a more reasonable level. For example:

```
nsslapd-cache-autosize: 60
nsslapd-cache-autosize-split: 60
```

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	0 (turns cache autosizing off) to 100
Default Value	-1
Syntax	Integer
Example	nsslapd-cache-autosize: 80

### 4.1.4. nsslapd-cache-autosize-split

This performance tuning-related attribute specifies the percentage of cache space to allocate to the database cache. For example, setting this to 60 would give the database cache 60 percent of the cache space and split the remaining 40 percent between the backend entry caches. That is, if there were two databases, each of them would receive 20 percent. This attribute only applies when the *nsslapd-cache-autosize* attribute has a value of 0.



#### NOTE

If the *nsslapd-cache-autosize* attribute and *nsslapd-cache-autosize-split* attribute are both set to high values, such as 100, then the Directory Server may fail to start and return error message. To fix this issue, reset the

*nsslapd-cache-autosize* and *nsslapd-cache-autosize-split* attributes to a more reasonable level. For example:

```
nsslapd-cache-autosize: 60
nsslapd-cache-autosize-split: 60
```

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	0 to 99
Default Value	50 (This will not necessarily optimize operations.)
Syntax	Integer
Example	nsslapd-cache-autosize-split: 50

#### 4.1.5. nsslapd-dbcachesize

This performance tuning-related attribute specifies the database index cache size, and is one of the most important values for controlling how much physical RAM the directory server uses.

This is not the entry cache. This is the amount of memory the Berkeley database backend will use to cache the indexes (the `.db4` files) and other files. This value is passed to the Berkeley DB API function `set_cachesize`. If automatic cache resizing is activated, this attribute is overridden when the server replaces these values with its own guessed values at a later stage of the server startup. For more technical information on this attribute, see the cache size section of the Berkeley DB reference guide.

Attempting to set a value that is not a number or is too big for a 32-bit signed integer returns an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	500 kilobytes to 4 gigabytes for 32-bit platforms and 500 kilobytes to $2^{64}-1$ for 64-bit platforms
Default Value	10000000 bytes
Syntax	Integer

Parameter	Description
Example	nsslapd-dbcachesize: 10,000,000

**NOTE**

On Solaris, the `nsslapd-dbcachesize` attribute has no effect on performance because the disk/filesystem cache overrides it.

#### 4.1.6. nsslapd-db-checkpoint-interval

This sets the amount of time in seconds after which the Directory Server sends a checkpoint entry to the database transaction log. The database transaction log contains a sequential listing of all recent database operations and is used for database recovery only. A checkpoint entry indicates which database operations have been physically written to the directory database. The checkpoint entries are used to determine where in the database transaction log to begin recovery after a system failure. The `nsslapd-db-checkpoint-interval` attribute is absent from `dse.ldif`. To change the checkpoint interval, add the attribute to `dse.ldif`. This attribute can be dynamically modified using `ldapmodify`. For further information on modifying this attribute, see the "Tuning Directory Server Performance" chapter in the *Directory Server Administration Guide*.

This attribute is provided only for system modification/diagnostics and should be changed only with the guidance of Red Hat technical support or Red Hat professional services. Inconsistent settings of this attribute and other configuration attributes may cause the Directory Server to be unstable.

For more information on database transaction logging, refer to the "Monitoring Server and Database Activity" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	10 to 300 seconds
Default Value	60
Syntax	Integer
Example	nsslapd-db-checkpoint-interval: 120

#### 4.1.7. nsslapd-db-circular-logging

This attribute specifies circular logging for the transaction log files. If this attribute is switched off, old transaction log files are not removed and are kept renamed as old log transaction files. Turning circular logging off can severely degrade server performance and, as such, should only

be modified with the guidance of Red Hat Technical Support or Red Hat Professional Services.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-db-circular-logging: on

### 4.1.8. nsslapd-db-debug

This attribute specifies whether additional error information is to be reported to Directory Server. To report error information, set the parameter to `on`. This parameter is meant for troubleshooting; enabling the parameter may slow down the Directory Server.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-db-debug: off

### 4.1.9. nsslapd-db-durable-transactions

This attribute sets whether database transaction log entries are immediately written to the disk. The database transaction log contains a sequential listing of all recent database operations and is used for database recovery only. With durable transactions enabled, every directory change will always be physically recorded in the log file and, therefore, able to be recovered in the event of a system failure. However, the durable transactions feature may also slow the performance of the Directory Server. When durable transactions is disabled, all transactions are logically written to the database transaction log but may not be physically written to disk immediately. If there were a system failure before a directory change was physically written to disk, that change would not be recoverable. The `nsslapd-db-durable-transactions` attribute is absent from `dse.ldif`. To disable durable transactions, add the attribute to `dse.ldif`.

This attribute is provided only for system modification/diagnostics and should be changed only with the guidance of Red Hat Technical Support or Red Hat Professional Services. Inconsistent settings of this attribute and other configuration attributes may cause the Directory Server to be unstable.

For more information on database transaction logging, refer to the "Monitoring Server and

Database Activity" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsslapd-db-durable-transactions: on

#### 4.1.10. nsslapd-db-home-directory

This is usually applicable to Solaris only, and is used to fix a situation in Solaris where the operating system endlessly flushes pages. This flushing can be so excessive that performance of the entire system is severely degraded.

For users of other systems, to move the database to another physical location for performance reasons, use this parameter to specify the home directory.

This situation will occur only for certain combinations of the database cache size, the size of physical memory, and kernel tuning attributes. In particular, this situation should not occur if the database cache size is less than 100 megabytes.

If the Solaris host seems excessively slow and the database cache size is around 100 megabytes or more, then use the `iostat` utility to diagnose the problem by monitoring the activity of the disk where the Directory Server's database files are stored. There are three conditions required before resetting the `nsslapd-db-home-directory` attribute:

- The disk is heavily used (more than 1 megabyte per second of data transfer).
- There is a long service time (more than 100ms).
- There is mostly write activity.

If these are all true, use the `nsslapd-db-home-directory` attribute to specify a subdirectory of a `tempfs` type filesystem.

The directory referenced by the `nsslapd-db-home-directory` attribute must be a subdirectory of a filesystem of type `tempfs` (such as `/tmp`). However, Directory Server does not create the subdirectory referenced by this attribute. This directory must be created either manually or by using a script. Failure to create the directory referenced by the `nsslapd-db-home-directory` attribute will result in Directory Server being unable to start.

Also, if there are multiple Directory Servers on the same machine, their `nsslapd-db-home-directory` attributes must be configured with different directories. Failure to

do so will result in the databases for both directories becoming corrupted.

The use of this attribute causes internal Directory Server database files to be moved to the directory referenced by the attribute. It is possible, but unlikely, that the server will no longer start after the files have been moved because not enough memory can be allocated. This is a symptom of an overly large database cache size being configured for the server. If this happens, reduce the size of the database cache size to a value where the server will start again.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid directory name in a tempfs filesystem, such as /tmp
Default Value	
Syntax	DirectoryString
Example	nsslapd-db-home-directory: /tmp/slapd-phonebook

### 4.1.11. nsslapd-db-idl-divisor

This attribute specifies the index block size in terms of the number of blocks per database page. The block size is calculated by dividing the database page size by the value of this attribute. A value of 1 makes the block size exactly equal to the page size. The default value of 0 sets the block size to the page size minus an estimated allowance for internal database overhead. For the majority of installations, the default value should not be changed unless there are specific tuning needs.

Before modifying the value of this attribute, export all databases using the `db2ldif` script. Once the modification has been made, reload the databases using the `ldif2db` script.



#### CAUTION

This parameter should only be used by very advanced users.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	0 to 8
Default Value	0
Syntax	Integer
Example	nsslapd-db-idl-divisor: 2

### 4.1.12. nsslapd-db-logbuf-size

This attribute specifies the log information buffer size. Log information is stored in memory until the buffer fills up or the transaction commit forces the buffer to be written to disk. Larger buffer sizes can significantly increase throughput in the presence of long running transactions, highly concurrent applications, or transactions producing large amounts of data. The log information buffer size is the transaction log size divided by four.

The *nsslapd-db-logbuf-size* attribute is only valid if the *nsslapd-db-durable-transactions* attribute is set to on.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	32K to maximum 32-bit integer (limited to the amount of memory available on the machine)
Default Value	32K
Syntax	Integer
Example	nsslapd-db-logbuf-size: 32K

### 4.1.13. nsslapd-db-logdirectory

This attribute specifies the path and directory name of the directory containing the database transaction log. The database transaction log contains a sequential listing of all recent database operations and is used for database recovery only. By default, the database transaction log is stored in the same directory as the directory entries themselves, */var/lib/dirsrv/slapd-instance\_name/db*. For fault-tolerance and performance reasons, move this log file to another physical disk. The *nsslapd-db-logdirectory* attribute is absent from *dse.ldif*. To change the location of the database transaction log, add the attribute to *dse.ldif*.

For more information on database transaction logging, refer to the "Monitoring Server and Database Activity" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid path and directory name
Default Value	
Syntax	DirectoryString
Example	nsslapd-db-logdirectory: /logs/txnlog

### 4.1.14. nsslapd-db-logfile-size

This attribute specifies the maximum size of a single file in the log in bytes. By default, or if the value is set to 0, a maximum size of 10 megabytes is used. The maximum size is an unsigned 4-byte value.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	0 to unsigned 4-byte integer
Default Value	10MB
Syntax	Integer
Example	nsslapd-db-logfile-size: 10 MB

### 4.1.15. nsslapd-db-page-size

This attribute specifies the size of the pages used to hold items in the database in bytes. The minimum size is 512 bytes, and the maximum size is 64 kilobytes. If the page size is not explicitly set, Directory Server defaults to a page size of 8 kilobytes. Changing this default value can have a significant performance impact. If the page size is too small, it results in extensive page splitting and copying, whereas if the page size is too large it can waste disk space.

Before modifying the value of this attribute, export all databases using the `db2ldif` script. Once the modification has been made, reload the databases using the `ldif2db` script.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	512 bytes to 64 kilobytes
Default Value	8KB
Syntax	Integer
Example	nsslapd-db-page-size: 8KB

### 4.1.16. nsslapd-db-spin-count

This attribute specifies the number of times that test-and-set mutexes should spin without blocking.



#### CAUTION

*Never touch this value unless you are very familiar with the inner workings of*

Berkeley DB or are specifically told to do so by Red Hat support.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config
Valid Range	0 to 2 <sup>31</sup> -1
Default Value	0
Syntax	Integer
Example	nsslapd-db-spin-count: 0

#### 4.1.17. nsslapd-db-transaction-batch-val

This attribute specifies how many transactions will be batched before being committed. This attribute can improve update performance when full transaction durability is not required. This attribute can be dynamically modified using `ldapmodify`. For further information on modifying this attribute, refer to the "Tuning Directory Server Performance" chapter in the *Directory Server Administration Guide*.



#### WARNING

Setting this value will reduce data consistency and may lead to loss of data. This is because if there is a power outage before the server can flush the batched transactions, those transactions in the batch will be lost.

Do not set this value unless specifically requested to do so by Red Hat support.

If this attribute is not defined or is set to a value of 0, transaction batching will be turned off, and it will be impossible to make remote modifications to this attribute via LDAP. However, setting this attribute to a value greater than 0 causes the server to delay committing transactions until the number of queued transactions is equal to the attribute value. A value greater than 0 also allows modifications to this attribute remotely via LDAP. A value of 1 for this attribute allows modifications to the attribute setting remotely via LDAP, but results in no batching behavior. A value of 1 at server startup is therefore useful for maintaining normal durability while also allowing transaction batching to be turned on and off remotely when desired. Remember that the value for this attribute may require modifying the `nsslapd-db-logbuf-size` attribute to ensure sufficient log buffer size for accommodating the batched transactions.



**NOTE**

The `nsslapd-db-transaction-batch-val` attribute is only valid if the `nsslapd-db-durable-transaction` attribute is set to `on`.

For more information on database transaction logging, refer to the "Monitoring Server and Database Activity" chapter in the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config
Valid Range	0 to 30
Default Value	0 (or turned off)
Syntax	Integer
Example	nsslapd-db-transaction-batch-val: 5

**4.1.18. nsslapd-db-trickle-percentage**

This attribute sets that at least the specified percentage of pages in the shared-memory pool are clean by writing dirty pages to their backing files. This is to ensure that a page is always available for reading in new information without having to wait for a write.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config
Valid Range	0 to 100
Default Value	40
Syntax	Integer
Example	nsslapd-db-trickle-percentage: 40

**4.1.19. nsslapd-db-verbose**

This attribute specifies whether to record additional informational and debugging messages when searching the log for checkpoints, doing deadlock detection, and performing recovery. This parameter is meant for troubleshooting, and enabling the parameter may slow down the Directory Server.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config

Parameter	Description
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-db-verbose: off

#### 4.1.20. nsslapd-dbncache

This attribute can split the LDBM cache into equally sized separate pieces of memory. It is possible to specify caches that are large enough so that they cannot be allocated contiguously on some architectures; for example, some releases of Solaris limit the amount of memory that may be allocated contiguously by a process. If *nsslapd-dbncache* is 0 or 1, the cache will be allocated contiguously in memory. If it is greater than 1, the cache will be broken up into *ncache*, equally sized separate pieces of memory.

To configure a dbcache size larger than 4 gigabytes, add the *nsslapd-dbncache* attribute to *cn=config*, *cn=ldbm database*, *cn=plugins*, *cn=config* between the *nsslapd-dbcachesize* and *nsslapd-db-logdirectory* attribute lines.

Set this value to an integer that is one-quarter (1/4) the amount of memory in gigabytes. For example, for a 12 gigabyte system, set the *nsslapd-dbncache* value to 3; for an 8 gigabyte system, set it to 2.

This attribute is provided only for system modification/diagnostics and should be changed only with the guidance of Red Hat technical support or Red Hat professional services. Inconsistent settings of this attribute and other configuration attributes may cause the Directory Server to be unstable.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	1 to 4
Default Value	1
Syntax	Integer
Example	nsslapd-dbncache: 1

#### 4.1.21. nsslapd-directory

This attribute specifies absolute path to database instance. If the database instance is manually created then this attribute must be included, something which is set by default (and modifiable) in the Directory Server Console. Once the database instance is created, do not modify this path

as any changes risk preventing the server from accessing data.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid absolute path to the database instance
Default Value	
Syntax	DirectoryString
Example	nsslapd-directory: /var/lib/dirsrv/slaped- <i>instance_name</i> /db

### 4.1.22. nsslapd-import-cachesize

This performance tuning-related attribute determines the size of the database cache used in the bulk import process. Setting this attribute value so that the maximum available system physical memory is used for the database cache during bulk importing optimizes bulk import speed. Attempting to set a value that is not a number or is too big for a 32-bit signed integer returns an LDAP\_UNWILLING\_TO\_PERFORM error message, with additional error information explaining the problem.



#### NOTE

A cache is created for each load that occurs. For example, if the user sets the *nsslapd-import-cachesize* attribute to 1 gigabyte, then 1 gigabyte is used when loading one database, 2 gigabytes is used when loading two databases, and so on. Ensure there is sufficient physical memory to prevent swapping from occurring, as this would result in performance degradation.

Parameter	Description
Entry DN	cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Range	500 kilobytes to 4 gigabytes for 32-bit platforms and 500 kilobytes to 2 <sup>64</sup> -1 for 64-bit platforms
Default Value	20 000 000
Syntax	Integer
Example	nsslapd-import-cachesize: 20 000 000

### 4.1.23. nsslapd-import-cache-autosize

This performance tuning-related attribute automatically sets the size of the import cache (`importCache`) to be used during the command-line-based import process of LDIF files to the database (the `ldif2db` operation).

In Directory Server, the import operation can be run as a server task or exclusively on the command-line. In the task mode, the import operation runs as a general Directory Server operation. The `nsslapd-import-cache-autosize` attribute enables the `importCache` to be set automatically to a predetermined size when the import operation is run on the command-line. The attribute can also be used by Directory Server during the task mode import for allocating a specified percentage of free memory for `importCache`.

By default, the `nsslapd-import-cache-autosize` attribute is enabled and is set to a value of `-1`. This value autosizes `importCache` for the `ldif2db` operation only, automatically allocating fifty percent (50%) of the free physical memory for `importCache`. The percentage value (50%) is hardcoded and cannot be changed.

Setting the attribute value to `50` (`nsslapd-import-cache-autosize: 50`) has the same effect on performance during an `ldif2db` operation. However, such a setting will have the same effect on performance when the import operation is run as a Directory Server task. The `-1` value autosizes `importCache` just for the `ldif2db` operation and not for any, including import, general Directory Server tasks.



## NOTE

The purpose of a `-1` setting is to enable the `ldif2db` operation to benefit from free physical memory but, at the same time, not compete for valuable memory with `entryCache`, which is used for general operations of the Directory Server.

Setting the `nsslapd-import-cache-autosize` attribute value to `0` turns off the `importCache` autosizing feature - that is, no autosizing occurs during either mode of the import operation. Instead, Directory Server uses the [Section 4.1.22, “nsslapd-import-cachesize”](#) attribute for import cache size, with a default of `20,000,000`.

There are three caches in the context of Directory Server: `dbCache`, `entryCache`, and `importCache`. `importCache` is only used during the import operation. The `nsslapd-cache-autosize` attribute, which is used for autosizing `entryCache` and `dbCache`, is used during the Directory Server operations only and not during the `ldif2db` command-line operation; the attribute value is the percentage of free physical memory to be allocated for `entryCache` and `dbCache`.

If both the autosizing attributes, `nsslapd-cache-autosize` and `nsslapd-import-cache-autosize`, are enabled, ensure that their sum is less than 100.

Parameter	Description
Entry DN	cn=config, cn=ldb database, cn=plugins, cn=config

Parameter	Description
Valid Range	-1, 0 (turns import cache autosizing off) to 100
Default Value	-1 (turns import cache autosizing on for <code>ldif2db</code> only and allocates 50% of the free physical memory to <code>importCache</code> )
Syntax	Integer
Example	<code>nsslapd-import-cache-autosize: -1</code>

#### 4.1.24. `nsslapd-mode`

This attribute specifies the permissions used for newly created index files.

Parameter	Description
Entry DN	<code>cn=config, cn=ldbm database, cn=plugins, cn=config</code>
Valid Values	Any four-digit octal number. However, mode <code>0600</code> is recommended. This allows read and write access for the owner of the index files (which is the user as whom the <code>ns-slapd</code> runs) and no access for other users.
Default Value	<code>600</code>
Syntax	Integer
Example	<code>nsslapd-mode: 0600</code>

#### 4.2. Database Attributes under `cn=monitor, cn=ldbm database, cn=plugins, cn=config`

Global read-only attributes containing database statistics for monitoring activity on the databases are stored in the `cn=monitor, cn=ldbm database, cn=plugins, cn=config` tree node. For more information on these entries, refer to the "Monitoring Server and Database Activity" chapter in the *Directory Server Administration Guide*.

##### **`dbcachehits.`**

This attribute shows the requested pages found in the database.

##### **`dbcachetries.`**

This attribute shows the total cache lookups.

##### **`dbcachehitratio.`**

This attribute shows the percentage of requested pages found in the database cache (hits/tries).

**dbcachepagein.**

This attribute shows the pages read into the database cache.

**dbcachepageout.**

This attribute shows the pages written from the database cache to the backing file.

**dbcacheroevict.**

This attribute shows the clean pages forced from the cache.

**dbcacherwevict.**

This attribute shows the dirty pages forced from the cache.

### 4.3. Database Attributes under cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config and cn=UserRoot, cn=ldbm database, cn=plugins, cn=config

The `cn=NetscapeRoot` and `cn=UserRoot` subtrees contain configuration data for, or the definition of, the databases containing the `o=NetscapeRoot` and `o=UserRoot` suffixes, respectively. The `cn=NetscapeRoot` subtree contains the configuration data used by the Administration Server for authentication and all actions that cannot be performed through LDAP (such as start/stop), and the `cn=UserRoot` subtree contains all the configuration data for the user-defined database.

The `cn=UserRoot` subtree is called *userRoot* by default. However, this is not hard-coded and, given the fact that there are going to be multiple database instances, this name is changed and defined by the user as and when new databases are added. The following attributes are common to both the `cn=NetscapeRoot`, `cn=ldbm database`, `cn=plugins`, `cn=config` and `cn=userRoot`, `cn=ldbm database`, `cn=plugins`, `cn=config` subtrees.

#### 4.3.1. nsslapd-cachesize

This performance tuning-related attribute specifies the cache size in terms of the entries it can hold. However, it is simpler to limit by memory size only (as in [Section 4.3.2](#), “*nsslapd-cachememsize*”). Attempting to set a value that is not a number or is too big for a 32-bit signed integer returns an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config or cn=UserRoot, cn=ldbm database, cn=plugins, cn=config

Parameter	Description
Valid Range	1 to 2,147,483,647 (or -1, which means limitless) entries
Default Value	-1
Syntax	Integer
Example	nsslapd-cachesize: -1

### 4.3.2. nsslapd-cachememsize

This performance tuning-related attribute specifies the cache size in terms of available memory space. The simplest method is limiting cache size in terms of memory occupied. Activating automatic cache resizing overrides this attribute, replacing these values with its own guessed values at a later stage of the server startup. Attempting to set a value that is not a number or is too big for a 32-bit signed integer returns an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

Parameter	Description
Entry DN	cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config or cn=UserRoot, cn=ldbm database, cn=plugins, cn=config
Valid Range	500 kilobytes to 4 gigabytes for 32-bit platforms and 500 kilobytes to $2^{64}-1$ for 64-bit platforms
Default Value	10,485,760 (10 megabytes)
Syntax	Integer
Example	nsslapd-cachememsize: 10485760

### 4.3.3. nsslapd-directory

This attribute specifies the path to the database instance. If it is a relative path, it starts from the path specified by `nsslapd-directory` in the global database entry `cn=config`, `cn=ldbm database`, `cn=plugins`, `cn=config`. The database instance directory is named after the instance name and located in the global database directory, by default. After the database instance has been created, do not modify this path, because any changes risk preventing the server from accessing data.

Parameter	Description
Entry DN	cn= <i>instance name</i> , cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid path to the database instance
Default Value	

Parameter	Description
Syntax	DirectoryString
Example	nsslapd-directory: /var/lib/dirsrv/slapd- <i>instance_name</i> /db/userRoot

#### 4.3.4. nsslapd-readonly

This attribute specifies read-only mode for a single back-end instance. If this attribute has a value of `off`, then users have all read, write, and execute permissions allowed by their access permissions.

Parameter	Description
Entry DN	cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config or cn=UserRoot, cn=ldbm database, cn=plugins, cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-readonly: off

#### 4.3.5. nsslapd-require-index

When switched to `on`, this attribute allows one to refuse unindexed searches. This performance-related attribute avoids saturating the server with erroneous searches.

Parameter	Description
Entry DN	cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config or cn=UserRoot, cn=ldbm database, cn=plugins, cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsslapd-require-index: off

#### 4.3.6. nsslapd-suffix

This attribute specifies the suffix of the *database link*. This is a single-valued attribute because each database instance can have only one suffix. Previously, it was possible to have more than one suffix on a single database instance, but this is no longer the case. As a result, this attribute is single-valued to enforce the fact that each database instance can only have one suffix entry. Any changes made to this attribute after the entry has been created take effect only after the

server containing the database link is restarted.

Parameter	Description
Entry DN	cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config or cn=UserRoot, cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid DN
Default Value	
Syntax	DirectoryString
Example	nsslapd-suffix: o=NetscapeRoot

### 4.4. Database Attributes under cn=database, cn=monitor, cn=ldbm database, cn=plugins, cn=config

The attributes in this tree node entry are all read-only, database performance counters. All of the values for these attributes are 32-bit integers.

#### **nsslapd-db-abort-rate.**

This attribute shows the number of transactions that have been aborted.

#### **nsslapd-db-active-txns.**

This attribute shows the number of transactions that are currently active.

#### **nsslapd-db-cache-hit.**

This attribute shows the requested pages found in the cache.

#### **nsslapd-db-cache-try.**

This attribute shows the total cache lookups.

#### **nsslapd-db-cache-region-wait-rate.**

This attribute shows the number of times that a thread of control was forced to wait before obtaining the region lock.

#### **nsslapd-db-cache-size-bytes.**

This attribute shows the total cache size in bytes.

#### **nsslapd-db-clean-pages.**

This attribute shows the clean pages currently in the cache.

#### **nsslapd-db-commit-rate.**

This attribute shows the number of transactions that have been committed.

**nsslapd-db-deadlock-rate.**

This attribute shows the number of deadlocks detected.

**nsslapd-db-dirty-pages.**

This attribute shows the dirty pages currently in the cache.

**nsslapd-db-hash-buckets.**

This attribute shows the number of hash buckets in buffer hash table.

**nsslapd-db-hash-elements-examine-rate.**

This attribute shows the total number of hash elements traversed during hash table lookups.

**nsslapd-db-hash-search-rate.**

This attribute shows the total number of buffer hash table lookups.

**nsslapd-db-lock-conflicts.**

This attribute shows the total number of locks not immediately available due to conflicts.

**nsslapd-db-lock-region-wait-rate.**

This attribute shows the number of times that a thread of control was forced to wait before obtaining the region lock.

**nsslapd-db-lock-request-rate.**

This attribute shows the total number of locks requested.

**nsslapd-db-lockers.**

This attribute shows the number of current lockers.

**nsslapd-db-log-bytes-since-checkpoint.**

This attribute shows the number of bytes written to this log since the last checkpoint.

**nsslapd-db-log-region-wait-rate.**

This attribute shows the number of times that a thread of control was forced to wait before obtaining the region lock.

**nsslapd-db-log-write-rate.**

This attribute shows the number of megabytes and bytes written to this log.

### **nsslapd-db-longest-chain-length.**

This attribute shows the longest chain ever encountered in buffer hash table lookups.

### **nsslapd-db-page-create-rate.**

This attribute shows the pages created in the cache.

### **nsslapd-db-page-read-rate.**

This attribute shows the pages read into the cache.

### **nsslapd-db-page-ro-evict-rate.**

This attribute shows the clean pages forced from the cache.

### **nsslapd-db-page-rw-evict-rate.**

This attribute shows the dirty pages forced from the cache.

### **nsslapd-db-page-trickle-rate.**

This attribute shows the dirty pages written using the `memp_trickle` interface.

### **nsslapd-db-page-write-rate.**

This attribute shows the pages read into the cache.

### **nsslapd-db-pages-in-use.**

This attribute shows all pages, clean or dirty, currently in use.

### **nsslapd-db-txn-region-wait-rate.**

This attribute shows the number of times that a thread of control was forced to wait before obtaining the region lock.

## **4.5. Database Attributes under `cn=default indexes`, `cn=config`, `cn=ldbm database`, `cn=plugins`, `cn=config`**

The set of default indexes is stored here. Default indexes are configured per backend in order to optimize Directory Server functionality for the majority of setup scenarios. All indexes, except system-essential ones, can be removed, but care should be taken so as not to cause unnecessary disruptions. For further information on indexes, refer to the "Managing Indexes" chapter in the *Directory Server Administration Guide*.

### **4.5.1. nsSystemIndex**

This mandatory attribute specifies whether the index is a *system index*, an index which is vital for Directory Server operations. If this attribute has a value of `true`, then it is system-essential.

System indexes should not be removed, as this will seriously disrupt server functionality.

Parameter	Description
Entry DN	cn=default indexes, cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	true   false
Default Value	
Syntax	DirectoryString
Example	nssystemindex: true

### 4.5.2. nsIndexType

This optional, multi-valued attribute specifies the type of index for Directory Server operations and takes the values of the attributes to be indexed. Each desired index type has to be entered on a separate line.

Parameter	Description
Entry DN	cn=default indexes, cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	<ul style="list-style-type: none"> <li>• pres = presence index</li> <li>• eq = equality index</li> <li>• approx = approximate index</li> <li>• sub = substring index</li> <li>• matching rule = international index</li> <li>• index browse = browsing index</li> </ul>
Default Value	
Syntax	DirectoryString
Example	nsindextype: eq

### 4.5.3. nsMatchingRule

This optional, multi-valued attribute specifies the ordering matching rule name or OID used to match values and to generate index keys for the attribute. This is most commonly used to ensure that equality and range searches work correctly for languages other than English (7-bit ASCII).

This is also used to allow range searches to work correctly for integer syntax attributes that do

not specify an ordering matching rule in their schema definition. *uidNumber* and *gidNumber* are two commonly used attributes that fall into this category.

For example, for a *uidNumber* that uses integer syntax, the rule attribute could be `nsMatchingRule: integerOrderingMatch`.



### NOTE

Any change to this attribute will not take effect until the change is saved and the index is rebuilt using `db2index`, which is described in more detail in the "Managing Indexes" chapter of the *Directory Server Administration Guide*.

Parameter	Description
Entry DN	cn=default indexes, cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid collation order object identifier (OID)
Default Value	None
Syntax	DirectoryString
Example	nsMatchingRule: 2.16.840.1.113730.3.3.2.3.1 (For Bulgarian)

### 4.5.4. cn

This attribute provides the name of the attribute to index.

Parameter	Description
Entry DN	cn=default indexes, cn=config, cn=ldbm database, cn=plugins, cn=config
Valid Values	Any valid index cn
Default Value	None
Syntax	DirectoryString
Example	cn: aci

### 4.5.5. description

This optional attribute provides a free-hand text description of what the index actually performs.

Parameter	Description
Entry DN	cn=default indexes, cn=config, cn=ldbm database, cn=plugins, cn=config

Parameter	Description
Valid Values	
Default Value	None
Syntax	DirectoryString
Example	description:substring index

## 4.6. Database Attributes under cn=monitor, cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config

This section covers global, read-only entries for monitoring activity on the `NetscapeRoot` database. The attributes containing database statistics are given for each file that makes up the database. For further information, see the "Monitoring Server and Database Activity" chapter in the *Directory Server Administration Guide*.

### **dbfilenamenumber.**

This attribute gives the name of the file and provides a sequential integer identifier (starting at 0) for the file. All associated statistics for the file are given this same numerical identifier.

### **dbfilecachehit.**

This attribute gives the number of times that a search requiring data from this file was performed and that the data were successfully obtained from the cache.

### **dbfilecachemiss.**

This attribute gives the number of times that a search requiring data from this file was performed and that the data could not be obtained from the cache.

### **dbfilepagein.**

This attribute gives the number of pages brought to the cache from this file.

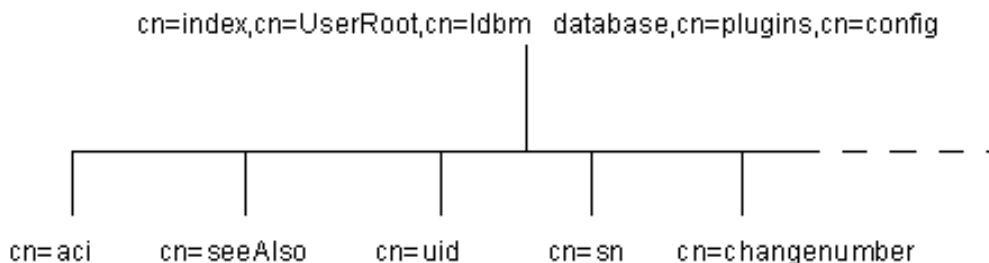
### **dbfilepageout.**

This attribute gives the number of pages for this file written from cache to disk.

## 4.7. Database Attributes under cn=index, cn=NetscapeRoot, cn=ldbm database, cn=plugins, cn=config and cn=index, cn=UserRoot, cn=ldbm database, cn=plugins, cn=config

In addition to the set of default indexes that are stored under `cn=default indexes`, `cn=config`, `cn=ldbm database`, `cn=plugins`, `cn=config`, custom indexes can be created for `o=NetscapeRoot`, `o=UserRoot`, and user-defined backend instances; these are stored under `cn=index,cn=database_name,cn=ldbm database, cn=plugins, cn=config`. Each indexed

attribute represents a subentry under the `cn=config` information tree nodes, as shown in the following diagram:



**Figure 3.2. Indexed Attribute Representing a Subentry**

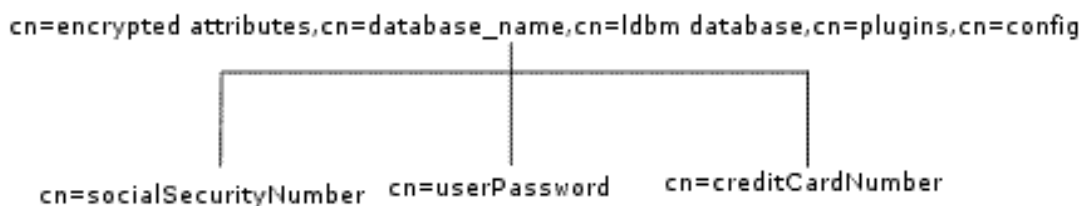
For example, the index file for the `aci` attribute under `o=UserRoot` appears in the Directory Server as follows:

```
dn:cn=aci, cn=index, cn=UserRoot, cn=ldbm database, cn=plugins, cn=config
objectclass:top
objectclass:nsIndex
cn:aci
nssystemindex:true
nsindextype:pres
```

For details regarding the five possible indexing attributes, see the section [Section 4.5, “Database Attributes under `cn=default indexes`, `cn=config`, `cn=ldbm database`, `cn=plugins`, `cn=config`”](#). For further information about indexes, refer to the “Managing Indexes” chapter in the *Directory Server Administration Guide*.

## 4.8. Database Attributes under `cn=attributeName`, `cn=encrypted attributes`, `cn=database_name`, `cn=ldbm database`, `cn=plugins`, `cn=config`

The `nsAttributeEncryption` object class allows selective encryption of attributes within a database. Extremely sensitive information such as credit card numbers and government identification numbers may not be protected enough by routine access control measures. Normally, these attribute values are stored in CLEAR within the database; encrypting them while they are stored adds another layer of protection. This object class has one attribute, `nsEncryptionAlgorithm`, which sets the encryption cipher used per attribute. Each encrypted attribute represents a subentry under the above `cn=config` information tree nodes, as shown in the following diagram:



**Figure 3.3. Encrypted Attributes under the cn=config Node**

For example, the database encryption file for the `userPassword` attribute under `o=UserRoot` appears in the Directory Server as follows:

```

dn:cn=userPassword, cn=encrypted attributes,o=UserRoot, cn=ldbm database,
cn=plugins, cn=config
objectclass:top
objectclass:nsAttributeEncryption
cn:userPassword
nsEncryptionAlgorithm:AES

```

To configure database encryption, see the "Database Encryption" section of the "Configuring Directory Databases" chapter in the *Directory Server Administration Guide*. For more information about indexes, refer to the "Managing Indexes" chapter in the *Directory Server Administration Guide*.

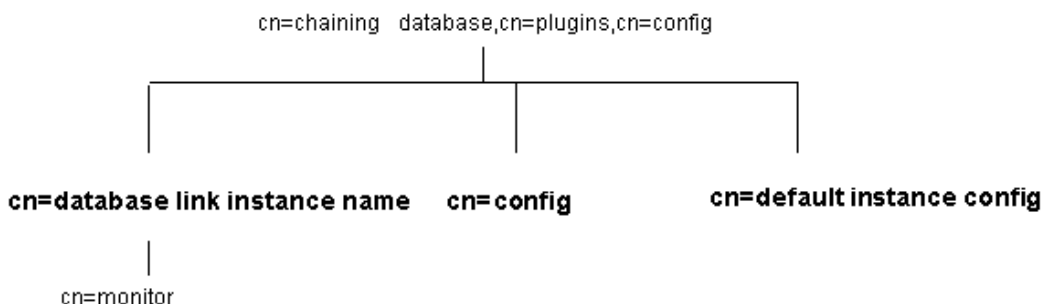
#### 4.8.1. nsEncryptionAlgorithm

`nsEncryptionAlgorithm` selects the cipher used by `nsAttributeEncryption`. The algorithm can be set per encrypted attribute.

Parameter	Description
Entry DN	cn=attributeName, cn=encrypted attributes, cn=databaseName, cn=ldbm database, cn=plugins, cn=config
Valid Values	The following are supported ciphers: <ul style="list-style-type: none"> <li>Advanced Encryption Standard Block Cipher (AES)</li> <li>Triple Data Encryption Standard Block Cipher (3DES)</li> </ul>
Default Value	
Syntax	DirectoryString
Example	nsEncryptionAlgorithm: AES

## 5. Database Link Plug-in Attributes (Chaining Attributes)

The database link plug-in attributes are also organized in an information tree, as shown in the following diagram:



**Figure 3.4. Database Link Plug-in**

All plug-in technology used by the database link instances is stored in the `cn=chaining database` plug-in node. This section presents the additional attribute information for the three nodes marked in bold in the `cn=chaining database, cn=plugins, cn=config` information tree in [Figure 3.4, “Database Link Plug-in”](#).

### 5.1. Database Link Attributes under `cn=config`, `cn=chaining database`, `cn=plugins`, `cn=config`

This section covers global configuration attributes common to all instances are stored in the `cn=config, cn=chaining database, cn=plugins, cn=config` tree node.

#### 5.1.1. `nsActiveChainingComponents`

This attribute lists the components using chaining. A component is any functional unit in the server. The value of this attribute overrides the value in the global configuration attribute. To disable chaining on a particular database instance, use the value `None`. This attribute also allows the components used to chain to be altered. By default, no components are allowed to chain, which explains why this attribute will probably not appear in a list of `cn=config, cn=chaining database, cn=config` attributes, as LDAP considers empty attributes to be non-existent.

Parameter	Description
Entry DN	<code>cn=config, cn=chaining database, cn=plugins, cn=config</code>
Valid Values	Any valid component entry

Parameter	Description
Default Value	None
Syntax	DirectoryString
Example	nsActiveChainingComponents: cn=uid uniqueness, cn=plugins, cn=config

### 5.1.2. nsMaxResponseDelay

This error detection, performance-related attribute specifies the maximum amount of time it can take a remote server to respond to an LDAP operation request made by a database link before an error is suspected. Once this delay period has been met, the database link tests the connection with the remote server.

Parameter	Description
Entry DN	cn=config, cn=chaining database, cn=plugins, cn=config
Valid Values	Any valid delay period in seconds
Default Value	60 seconds
Syntax	Integer
Example	nsMaxResponseDelay: 60

### 5.1.3. nsMaxTestResponseDelay

This error detection, performance-related attribute specifies the duration of the test issued by the database link to check whether the remote server is responding. If a response from the remote server is not returned before this period has passed, the database link assumes the remote server is down, and the connection is not used for subsequent operations.

Parameter	Description
Entry DN	cn=config, cn=chaining database, cn=plugins, cn=config
Valid Values	Any valid delay period in seconds
Default Value	15 seconds
Syntax	Integer
Example	nsMaxTestResponseDelay: 15

### 5.1.4. nsTransmittedControls

This attribute, which can be both a global (and thus dynamic) configuration or an instance (that is, `cn=database link instance, cn=chaining database, cn=plugins, cn=config`) configuration attribute, allows the controls the database link forwards to be altered. The

following controls are forwarded by default by the database link:

- Managed DSA (OID: 2.16.840.1.113730.3.4.2)
- Virtual list view (VLV) (OID: 2.16.840.1.113730.3.4.9)
- Server side sorting (OID: 1.2.840.113556.1.4.473)

Parameter	Description
Entry DN	cn=config, cn=chaining database, cn=plugins, cn=config
Valid Values	Any valid OID or the above listed controls forwarded by the database link
Default Value	None
Syntax	Integer
Example	nsTransmittedControls: 1.2.840.113556.1.4.473

### 5.2. Database Link Attributes under cn=default instance config, cn=chaining database, cn=plugins, cn=config

Default instance configuration attributes for instances are housed in the `cn=default instance config, cn=chaining database, cn=plugins, cn=config tree node`.

#### 5.2.1. nsAbandonedSearchCheckInterval

This attribute shows the number of seconds that pass before the server checks for abandoned operations.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	0 to maximum 32-bit integer (2147483647) seconds
Default Value	1
Syntax	Integer
Example	nsAbandonedSearchCheckInterval: 10

#### 5.2.2. nsBindConnectionsLimit

This attribute shows the maximum number of TCP connections the database link establishes with the remote server.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	1 to 50 connections
Default Value	3
Syntax	Integer
Example	nsBindConnectionsLimit: 3

### 5.2.3. nsBindRetryLimit

Contrary to what the name suggests, this attribute does not specify the number of times a database link *retries* to bind with the remote server but the number of times it *tries* to bind with the remote server. A value of 1 here indicates that the database link only attempts to bind once.



#### NOTE

Retries only occur for connection failures and not for other types of errors, such as invalid bind DNs or bad passwords.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	0 to 5
Default Value	3
Syntax	Integer
Example	nsBindRetryLimit: 3

### 5.2.4. nsBindTimeout

This attribute shows the amount of time before the bind attempt times out. There is no real valid range for this attribute, except reasonable patience limits.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	0 to 60 seconds
Default Value	15
Syntax	Integer
Example	nsBindTimeout: 15

### 5.2.5. nsCheckLocalACI

*Reserved for advanced use only.* This attribute controls whether ACIs are evaluated on the database link as well as the remote data server. Changes to this attribute only take effect once the server has been restarted.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsCheckLocalACI: on

### 5.2.6. nsConcurrentBindLimit

This attribute shows the maximum number of concurrent bind operations per TCP connection.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	1 to 25 binds
Default Value	10
Syntax	Integer
Example	nsConcurrentBindLimit: 10

### 5.2.7. nsConcurrentOperationsLimit

This attribute specifies the maximum number of concurrent operations allowed.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	1 to 50 operations
Default Value	2
Syntax	Integer
Example	nsConcurrentOperationsLimit: 5

### 5.2.8. nsConnectionLife

This attribute specifies connection lifetime. Connections between the database link and the remote server can be kept open for an unspecified time or closed after a specific period of time. It is faster to keep the connections open, but it uses more resources. When the value is 0 and a list of failover servers is provided in the *nsFarmServerURL* attribute, the main server is never contacted after failover to the alternate server.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	0 to limitless seconds (where 0 means forever)
Default Value	0
Syntax	Integer
Example	nsConnectionLife: 0

### 5.2.9. nsOperationConnectionsLimit

This attribute shows the maximum number of LDAP connections the database link establishes with the remote server.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	1 to n connections
Default Value	20
Syntax	Integer
Example	nsOperationConnectionsLimit: 10

### 5.2.10. nsProxiedAuthorization

*Reserved for advanced use only.* This attribute can disable proxied authorization with a value of `off`.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Values	on   off
Default Value	on
Syntax	DirectoryString
Example	nsProxiedAuthorization: on

### 5.2.11. nsReferralOnScopedSearch

This attribute controls whether referrals are returned by scoped searches. This attribute can be used to optimize the directory because returning referrals in response to scoped searches is more efficient. A referral is returned to all the configured farm servers.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Values	on   off
Default Value	off
Syntax	DirectoryString
Example	nsReferralOnScopedSearch: off

### 5.2.12. nsSizeLimit

This attribute specifies the default size limit for the database link in bytes.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	-1 (no limit) to maximum 32-bit integer (2147483647) entries
Default Value	2000
Syntax	Integer
Example	nsslapd-sizelimit: 2000

### 5.2.13. nsTimeLimit

This attribute specifies the default search time limit for the database link.

Parameter	Description
Entry DN	cn=default instance config, cn=chaining database, cn=plugins, cn=config
Valid Range	-1 to maximum 32-bit integer (2147483647) seconds
Default Value	3600
Syntax	Integer
Example	nsslapd-timelimit: 3600

### 5.3. Database Link Attributes under cn=database link instance name, cn=chaining database, cn=plugins, cn=config

This information node stores the attributes concerning the server containing the data. A *farm server* is a server which contains data on databases. This attribute can contain optional servers for failover, separated by spaces. For cascading chaining, this URL can point to another database link.

#### 5.3.1. nsFarmServerURL

This attribute gives the LDAP URL of the remote server. A farm server is a server containing data in one or more databases. This attribute can contain optional servers for failover, separated by spaces. If using cascading changing, this URL can point to another database link.

Parameter	Description
Entry DN	cn=database link instance name, cn=chaining database, cn=plugins, cn=config
Valid Values	Any valid remote server LDAP URL
Default Value	
Syntax	DirectoryString
Example	nsFarmServerURL: ldap://farm1.example.com:389 ldap://farm2.example.com:1389

#### 5.3.2. nsMultiplexorBindDN

This attribute gives the DN of the administrative entry used to communicate with the remote server. The *multiplexor* is the server that contains the database link and communicates with the farm server. This bind DN cannot be the Directory Manager, and, if this attribute is not specified, the database link binds as *anonymous*.

Parameter	Description
Entry DN	cn=database link instance name, cn=chaining database, cn=plugins, cn=config
Valid Values	
Default Value	DN of the multiplexor
Syntax	DirectoryString
Example	nsMultiplexerBindDN: cn=proxy manager

#### 5.3.3. nsMultiplexorCredentials

Password for the administrative user, given in plain text. If no password is provided, it means that users can bind as *anonymous*. The password is encrypted in the configuration file. The

example below is what is shown, not what is typed.

Parameter	Description
Entry DN	cn=database link instance name, cn=chaining database, cn=plugins, cn=config
Valid Values	Any valid password, which will then be encrypted using the DES reversible password encryption schema
Default Value	
Syntax	DirectoryString
Example	nsMultiplexerCredentials: {DES} 9Eko69APCJfF

### 5.3.4. nshoplimit

This attribute specifies the maximum number of times a database is allowed to chain; that is, the number of times a request can be forwarded from one database link to another.

Parameter	Description
Entry DN	cn=database link instance name, cn=chaining database, cn=plugins, cn=config
Valid Range	1 to an appropriate upper limit for the deployment
Default Value	10
Syntax	Integer
Example	nsHopLimit: 3

## 5.4. Database Link Attributes under cn=monitor, cn=database instance name, cn=chaining database, cn=plugins, cn=config

Attributes used for monitoring activity on the instances are stored in the `cn=monitor`, `cn=database instance name`, `cn=chaining database`, `cn=plugins`, `cn=config` information tree.

### **nsAddCount.**

This attribute gives the number of add operations received.

### **nsDeleteCount.**

This attribute gives the number of delete operations received.

### **nsModifyCount.**

This attribute gives the number of modify operations received.

**nsRenameCount.**

This attribute gives the number of rename operations received.

**nsSearchBaseCount.**

This attribute gives the number of base level searches received.

**nsSearchOneLevelCount.**

This attribute gives the number of one-level searches received.

**nsSearchSubtreeCount.**

This attribute gives the number of subtree searches received.

**nsAbandonCount.**

This attribute gives the number of abandon operations received.

**nsBindCount.**

This attribute gives the number of bind requests received.

**nsUnbindCount.**

This attribute gives the number of unbinds received.

**nsCompareCount.**

This attribute gives the number of compare operations received.

**nsOperationConnectionCount.**

This attribute gives the number of open connections for normal operations.

**nsBindConnectionCount.**

This attribute gives the number of open connections for bind operations.

## 6. Retro Changelog Plug-in Attributes

Two different types of changelogs are maintained by Directory Server. The first type, referred to as simply a *changelog*, is used by multi-master replication, and the second changelog, a plug-in referred to as the *retro changelog*, is intended for use by LDAP clients for maintaining application compatibility with Directory Server 4.x versions.

This Retro Changelog Plug-in is used to record modifications made to a supplier server. When the supplier server's directory is modified, an entry is written to the Retro Changelog that

contains both of the following:

- A number that uniquely identifies the modification. This number is sequential with respect to other entries in the changelog.
- The modification action; that is, exactly how the directory was modified.

It is through the Retro Changelog Plug-in that the changes performed to the Directory Server are accessed using searches to `cn=changelog` suffix.

### 6.1. nsslapd-changelogdir

This attribute specifies the name of the directory in which the changelog database is created the first time the plug-in is run. By default, the database is stored with all the other databases under `/var/lib/dirsrv/slapd-instance_name/changelogdb`.



#### NOTE

For performance reasons, store this database on a different physical disk.

The server has to be restarted for changes to this attribute to go into effect.

Parameter	Description
Entry DN	<code>cn=Retro Changelog Plugin, cn=plugins, cn=config</code>
Valid Values	Any valid path to the directory
Default Value	None
Syntax	DirectoryString
Example	<code>nsslapd-changelogdir: /var/lib/dirsrv/slapd-<i>instance_name</i>/changelogdb</code>

### 6.2. nsslapd-changelogmaxage (Max Changelog Age)

This attribute specifies the maximum age of any entry in the changelog. The changelog contains a record for each directory modification and is used when synchronizing consumer servers. Each record contains a timestamp. Any record with a timestamp that is older than the value specified in this attribute is removed. If this attribute is absent, there is no age limit on changelog records, which is the default behavior since this attribute is not present by default.

**NOTE**

Expired changelog records will not be removed if there is an agreement that has fallen behind further than the maximum age.

Parameter	Description
Entry DN	cn=Retro Changelog Plugin, cn=plugins, cn=config
Valid Range	0 (meaning that entries are not removed according to their age) to the maximum 32 bit integer value (2147483647)
Default Value	0
Syntax	DirectoryString Integer <i>AgeID</i> <i>AgeID</i> is <i>s</i> for seconds, <i>m</i> for minutes, <i>h</i> for hours, <i>d</i> for days, or <i>w</i> for weeks.
Example	nsslapd-changelogmaxage: 30d



# Server Instance File Reference

This chapter provides an overview of the files that are specific to an instance of Red Hat Directory Server (Directory Server) — the files stored in the `/usr/lib/dirsrv/slapd-instance_name` directory.<sup>1</sup> Having an overview of the files and configuration information stored in each instance of Directory Server helps with understanding the file changes (or lack of file changes) which occur in the course of directory activity. It can also help to detect errors and intrusion by indicating what kind of changes to expect and, as a result, what changes are abnormal.

## 1. Overview of Directory Server Files



### NOTE

In examples and sample code, paths assume that the Directory Server is installed on Red Hat Enterprise Linux, which has an instance directory of `/usr/lib/dirsrv/slapd-instance_name`. If the Directory Server is on a different platform, adjust the paths accordingly.

The files, tools, and scripts used by Directory Server are in the locations listed in the following directories.

File or Directory	Location
Backup files	<code>/var/lib/dirsrv/slapd-<i>instance_name</i>/bak</code>
Configuration files	<code>/etc/dirsrv/slapd-<i>instance_name</i></code>
Database files	<code>/var/lib/dirsrv/slapd-<i>instance_name</i>/db</code>
LDIF files	<code>/var/lib/dirsrv/slapd-<i>instance_name</i>/ldif</code>
Lock files	<code>/var/lock/dirsrv/slapd-<i>instance_name</i></code>
Log files	<code>/var/log/dirsrv/slapd-<i>instance_name</i></code>
PID files	<code>/var/run/dirsrv/slapd-<i>instance_name</i></code>
Tools	<code>/usr/bin</code> <code>/usr/sbin</code> <code>/usr/lib/mozldap6</code>
Instance directory	<code>/usr/lib/dirsrv/slapd-<i>instance_name</i></code>

<sup>1</sup> The `/lib` directory only applies to Red Hat Enterprise Linux 32-bit systems. On Red Hat Enterprise Linux 64-bit systems, the directory is `/lib64`, and on Solaris 64-bit systems, it is `/lib/sparcv9`.

**Table 4.1. Red Hat Enterprise Linux 4 and 5 (x86)**

File or Directory	Location
Backup files	/var/lib/dirsrv/slapd- <i>instance_name</i> /bak
Configuration files	/etc/dirsrv/slapd- <i>instance_name</i>
Database files	/var/lib/dirsrv/slapd- <i>instance_name</i> /db
LDIF files	/var/lib/dirsrv/slapd- <i>instance_name</i> /ldif
Lock file	/var/lock/dirsrv/slapd- <i>instance_name</i>
Log files	/var/log/dirsrv/slapd- <i>instance_name</i>
PID	/var/run/dirsrv/slapd- <i>instance_name</i>
Tools	/usr/bin /usr/sbin /usr/lib64/mozldap6
Instance directory	/usr/lib64/dirsrv/slapd- <i>instance</i>

**Table 4.2. Red Hat Enterprise Linux 4 and 5 (x86\_64)**

File or Directory	Location
Backup files	/var/lib/dirsrv/slapd- <i>instance_name</i> /bak
Configuration files	/etc/dirsrv/slapd- <i>instance_name</i>
Database files	/var/lib/dirsrv/slapd- <i>instance_name</i> /db
LDIF files	/var/lib/dirsrv/slapd- <i>instance_name</i> /ldif
Lock files	/var/lock/dirsrv/slapd- <i>instance_name</i>
Log files	/var/log/dirsrv/slapd- <i>instance_name</i>
PID	/var/run/dirsrv/slapd- <i>instance_name</i>
Tools	/usr/bin /usr/sbin /usr/lib/sparcv9/mozldap
Instance directory	/usr/lib/sparcv9/dirsrv/slapd- <i>instance</i>

**Table 4.3. Sun Solaris 9 (sparc)**

File or Directory	Location
Backup files	/var/opt/dirsrv/slapd- <i>instance</i> /bak
Configuration files	/etc/opt/dirsrv/slapd- <i>instance</i>

File or Directory	Location
Database files	<code>/var/opt/dirsrv/slapd-<i>instance</i>/db</code>
Runtime files	<code>/var/opt/dirsrv/<i>instance</i></code>
LDIF files	<code>/var/opt/dirsrv/slapd-<i>instance</i>/ldif</code>
Log files	<code>/var/opt/log/dirsrv/slapd-<i>instance</i></code>
Tools	<code>/opt/dirsrv/bin/ /opt/dirsrv/sbin/</code>
Instance directory	<code>/opt/dirsrv/slapd-<i>instance</i></code>
Libraries	<code>/opt/dirsrv/lib/</code>

**Table 4.4. HP-UX 11i (IA64)**

## 2. Backup Files

Each Directory Server instance contains the following directory and file for storing backup-related files:

- `/var/lib/dirsrv/slapd-instance_name/bak` — This contains a directory dated with the *instance\_name*, time and date of the database backup, such as `instance_name-2007_05_02_16_56_05/`, which in turn holds the database backup copy.
- `/etc/dirsrv/slapd-instance_name/dse_original.ldif` — This is a backup copy of the `dse.ldif` configuration file from the time of installation.

## 3. Configuration Files

Each Directory Server instance stores its configuration files in the `/etc/dirsrv/slapd-instance_name` directory. The configuration files in this directory are explained in [Section 1, “Server Configuration - Overview”](#).

## 4. Database Files

Each Directory Server instance contains the `/var/lib/dirsrv/slapd-instance_name/db` directory for storing all of the database files. The following is a sample listing of the `/var/lib/dirsrv/slapd-instance_name/db` directory contents.

```
__db.001  __db.003  __db.005  NetscapeRoot/
__db.002  __db.004  DBVERSION log.0000000007  userRoot/
```

### Example 4.1. Database Directory Contents

- `db.00x` files — Used internally by the database and should not be moved, deleted, or modified in any way.
- `log.xxxxxxxxxx` files — Used to store the transaction logs per database.
- `DBVERSION` — Used for storing the version of the database.
- `NetscapeRoot` — Stores the `o=NetscapeRoot` database created by default when the `setup-ds-admin.pl` script is run.
- `userRoot` — Stores the user-defined suffix (user-defined databases) created at setup; for example, `dc=example,dc=com`.



#### NOTE

If a new database is created (for example, `testRoot`) to store the directory tree under a new suffix, the directory named `testRoot` also appears in the `/var/lib/dirsrv/slapd-instance_name/db` directory.

The following is a sample listing of the `NetscapeRoot` directory contents.

```
./          entrydn.db4*      parentid.db4*
../         givenName.db4*     sn.db4*
DBVERSION* id2entry.db4*   uid.db4*
aci.db4*   nsUniqueId.db4*  uniquemember.db4*
ancestorid.db4* numsubordinates.db4*
cn.db4*    objectclass.db4*
```

### Example 4.2. NetscapeRoot Database Directory Contents

The `NetscapeRoot` subdirectories contain an `index_name.db4` file for every index currently defined in the database. In addition to these files, the `NetscapeRoot` and `userRoot` subdirectories contain the following files:

- `ancestorid.db4` — Contains a list of IDs to find the ID of the entry's ancestor.

- `entrydn.db4` — Contains a list of full DNs to find any ID.
- `id2entry.db4` — Contains the actual directory database entries. All other database files can be recreated from this one, if necessary.
- `nsuniqueid.db4` — Contains a list of unique IDs to find any ID.
- `numsubordinates.db4` — Contains IDs that have child entries.
- `objectclass.db4` — Contains a list of IDs which have a particular object class.
- `parentid.db4` — Contains a list of IDs to find the ID of the parent.

## 5. LDIF Files

Sample LDIF files are stored in the `/var/lib/dirsrv/slapd-instance_name/ldif` directory for storing LDIF-related files. [Example 4.3, “LDIF Directory Contents”](#) lists the `/ldif` directory contents.

```
European.ldif
Example.ldif
Example-roles.ldif
Example-views.ldif
```

### Example 4.3. LDIF Directory Contents

- `European.ldif` — Contains European character samples.
- `Example.ldif` — Is a sample LDIF file.
- `Example-roles.ldif` — Is a sample LDIF file similar to `Example.ldif`, except that it uses roles and class of service instead of groups for setting access control and resource limits for directory administrators.



#### NOTE

The LDIF files exported by `db2ldif` or `db2ldif.pl` scripts in the instance directory are stored in `/var/lib/dirsrv/slapd-instance_name/ldif`.

### 6. Lock Files

Each Directory Server instance contains a `/var/lock/dirsrv/slapd-instance_name` directory for storing lock-related files. The following is a sample listing of the `locks` directory contents.

```
exports/ imports/ server/
```

#### Example 4.4. Lock Directory Contents

The lock mechanisms stored in the `exports`, `imports`, and `server` subdirectories prevent multiple, simultaneous operations from conflicting with each other. The lock mechanisms allow for one server instance to run at a time, with possible multiple export jobs. They also permit one `ldif2db` import operation at a time (not `ldif2db.pl`, because multiple `ldif2db.pl` operations can be run at any time) to the exclusion of all export and `slapd` server operations.

If there are error messages indicating that the lock table is out of available locks (for example, `libdb: Lock table is out of available locks`), double the value of the `nsslapd-db-locks` attribute in the `cn=config,cn=ldb database,cn=plugins,cn=config` entry.

For example, if the current value is `10000`, set it to `20000`. If the problem persists, double the number again. To monitor the current and maximum number of locks, do a search on `cn=database, cn=monitor, cn=ldb database, cn=plugins, cn=config`. For example:

```
ldapsearch -h localhost -p 389 -D "cn=directory manager" -w password  
-b "cn=database,cn=monitor,cn=ldb database, cn=plugins,cn=config"  
objectclass=* | grep -- -locks: )
```

For more information on using LDAP utilities, see the *Directory Server Administration Guide*.

### 7. Log Files

Each Directory Server instance contains a `/var/log/dirsrv/slapd-instance_name` directory for storing log files. The following is a sample listing of the `/logs` directory contents.

```
access                access.20070228-171925  errors  
access.20070221-162824 access.rotationinfo    errors.20070221-162824  
access.20070223-171949 audit                  errors.rotationinfo  
access.20070227-171818 audit.rotationinfo    slapd.stats
```

#### Example 4.5. Log Directory Contents

- The content of the `access`, `audit`, and `error` log files is dependent on the log configuration.
- The `slapd.stats` file is a memory-mapped file which cannot be read by an editor. It contains data collected by the Directory Server SNMP data collection component. This data is read by the SNMP subagent in response to SNMP attribute queries and is communicated to the SNMP master agent responsible for handling Directory Server SNMP requests.

## 8. PID Files

`slapd-serverID.pid` and `slapd-serverID.startpid` files are created in the `/var/run/dirsrv/slapd-instance_name` directory when the server is up and running. Both files store the server's process ID.

## 9. Tools

Directory Server tools are stored in three directories on Red Hat Enterprise Linux:

- `/usr/bin`
- `/usr/sbin`
- `/usr/lib/mozldap6`

The contents of those directories are listed below. [Chapter 6, Command-Line Utilities](#) has more information on command-line scripts.

```
dbscan      ldif
dbscan-bin  ldif-bin
```

### Example 4.6. /bin Contents

```
ds_removal      migrate-ds-admin.pl  setup-ds-admin.pl
ds_unregister   register-ds-admin.pl setup-ds.pl
```

### Example 4.7. /sbin Contents

```
ldapcmp      ldapcompare-bin  ldapmodify      ldappasswd-bin
ldapcmp-bin  ldapdelete      ldapmodify-bin  ldapsearch
ldapcompare  ldapdelete-bin  ldappasswd     ldapsearch-bin
```

### Example 4.8. LDAP Tool Directory Contents

## 10. Scripts

Directory Server command-line scripts are stored in the `/usr/lib/dirsrv/slapd-instance_name` directory. The contents of the `/usr/lib/dirsrv/slapd-instance_name` directory are listed in [Example 4.9, “Instance Directory Contents”](#). [Chapter 7, Command-Line Scripts](#) has more information on command-line scripts.

```
bak2db      db2index.pl  ldif2db.pl      ns-inactivate.pl
start-slapd
bak2db.pl   db2ldif      ldif2ldap       ns-newpwpolicy.pl  stop-slapd
db2bak      db2ldif.pl   monitor         restart-slapd
suffix2instance
db2bak.pl   dbverify     ns-accountstatus.pl  restoreconfig
verify-db.pl
db2index    ldif2db      ns-activate.pl    saveconfig          vlvindex
```

### Example 4.9. Instance Directory Contents

# Access Log and Connection Code Reference

Red Hat Directory Server (Directory Server) provides logs to help monitor directory activity. Monitoring helps quickly detecting and remedying failures and, where done proactively, anticipating and resolving potential problems before they result in failure or poor performance. Part of monitoring the directory effectively is understanding the structure and content of the log files.

This chapter does not provide an exhaustive list of error messages. However, the information presented in this chapter serves as a good starting point for common problems.

## 1. Access Log Content

The Directory Server access log contains detailed information about client connections to the directory. A connection is a sequence of requests from the same client with the following structure:

- Connection record, which gives the connection index and the IP address of the client.
- Bind record.
- Bind result record.
- Sequence of operation request/operation result pairs of records (or individual records in the case of connection, closed, and abandon records).
- Unbind record.
- Closed record.

Every line begins with a timestamp — [21/Apr/2007:11:39:51 -0700] — the format of which may vary depending on the platform. -0700 indicates the time difference in relation to GMT. Apart from the connection, closed, and abandon records, which appear individually, all records appear in pairs, consisting of a request for service record followed by a result record. These two records frequently appear on adjacent lines, but this is not always the case.

This section presents the different levels of access logging available with Directory Server, then describes the default access logging content, and ends with a description of the additional access logging level content.

- [Section 1.1, “Access Logging Levels”](#)
- [Section 1.2, “Default Access Logging Content”](#)

- [Section 1.3, “Access Log Content for Additional Access Logging Levels”](#)



### NOTE

Directory Server provides a script which can analyze access logs to extract usage statistics and count the occurrences of significant events. For details about this script, see [Section 4.7, “logconv.pl \(Log Converter\)”](#).

## 1.1. Access Logging Levels

Different levels of access logging exist, and changing the value of the `nsslapd-accesslog-level` configuration attribute sets the exact type of logging required. See [Section 3.1.2, “nsslapd-accesslog-level”](#) for full details on access log levels.

## 1.2. Default Access Logging Content

This section describes the access log content in detail based on the default access logging level extract shown below.

```
[21/Apr/2007:11:39:51 -0700] conn=11 fd=608 slot=608 connection from
207.1.153.51 to 192.18.122.139
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 BIND dn="cn=Directory Manager"
method=128 version=3
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97 nentries=0
etime=0
[21/Apr/2007:11:39:51 -0700] conn=11 op=1 SRCH base="dc=example,dc=com"
scope=2 filter="(uid=bjensen)"
[21/Apr/2007:11:39:51 -0700] conn=11 op=1 RESULT err=0 tag=101 nentries=1
etime=1000 notes=U
[21/Apr/2007:11:39:51 -0700] conn=11 op=2 UNBIND
[21/Apr/2007:11:39:51 -0700] conn=11 op=2 fd=608 closed - U1
[21/Apr/2007:11:39:52 -0700] conn=12 fd=634 slot=634 connection from
207.1.153.51 to 192.18.122.139
[21/Apr/2007:11:39:52 -0700] conn=12 op=0 BIND dn="cn=Directory Manager"
method=128 version=3
[21/Apr/2007:11:39:52 -0700] conn=12 op=0 RESULT err=0 tag=97 nentries=0
etime=0
[21/Apr/2007:11:39:52 -0700] conn=12 op=1 SRCH base="dc=example,dc=com"
scope=2 filter="(uid=bjensen)"
[21/Apr/2007:11:39:52 -0700] conn=12 op=2 ABANDON targetop=1 msgid=2
nentries=0 etime=0
[21/Apr/2007:11:39:52 -0700] conn=12 op=3 UNBIND
[21/Apr/2007:11:39:52 -0700] conn=12 op=3 fd=634 closed - U1
[21/Apr/2007:11:39:53 -0700] conn=13 fd=659 slot=659 connection from
207.1.153.51 to 192.18.122.139
[21/Apr/2007:11:39:53 -0700] conn=13 op=0 BIND dn="cn=Directory Manager"
method=128 version=3
[21/Apr/2007:11:39:53 -0700] conn=13 op=0 RESULT err=0 tag=97 nentries=0
etime=0
[21/Apr/2007:11:39:53 -0700] conn=13 op=1 EXT oid="2.16.840.1.113730.3.5.3"
```

```
[21/Apr/2007:11:39:53 -0700] conn=13 op=1 RESULT err=0 tag=120 nentries=0
etime=0
[21/Apr/2007:11:39:53 -0700] conn=13 op=2 ADD dn="cn=Sat Apr 21 11:39:51 MET
DST 2007, dc=example,dc=com"
[21/Apr/2007:11:39:53 -0700] conn=13 op=2 RESULT err=0 tag=105 nentries=0
etime=0 csn=3b4c8cfb000000030000
[21/Apr/2007:11:39:53 -0700] conn=13 op=3 EXT oid="2.16.840.1.113730.3.5.5"
[21/Apr/2007:11:39:53 -0700] conn=13 op=3 RESULT err=0 tag=120 nentries=0
etime=0
[21/Apr/2007:11:39:53 -0700] conn=13 op=4 UNBIND
[21/Apr/2007:11:39:53 -0700] conn=13 op=4 fd=659 closed - U1
[21/Apr/2007:11:39:55 -0700] conn=14 fd=700 slot=700 connection from
207.1.153.51 to 192.18.122.139
[21/Apr/2007:11:39:55 -0700] conn=14 op=0 BIND dn="" method=saslversion=3
mech=DIGEST-MD5
[21/Apr/2007:11:39:55 -0700] conn=14 op=0 RESULT err=14 tag=97nentries=0
etime=0, SASL bind in progress
[21/Apr/2007:11:39:55 -0700] conn=14 op=1
BINDdn="uid=jdoe,dc=example,dc=com" method=sasl version=3
mech=DIGEST-MD5
[21/Apr/2007:11:39:55 -0700] conn=14 op=1 RESULT err=0 tag=97nentries=0
etime=0 dn="uid=jdoe,dc=
example,dc=com"
[21/Apr/2007:11:39:55 -0700] conn=14 op=2 UNBIND
[21/Apr/2007:11:39:53 -0700] conn=14 op=2 fd=700 closed - U1
```

## Example 5.1. Example Access Log

### 1.2.1. Connection Number

Every external LDAP request is listed with an incremental connection number, in this case `conn=11`, starting at `conn=0` immediately after server startup.

```
[21/Apr/2007:11:39:51 -0700] conn=11 fd=608 slot=608 connection from
207.1.153.51 to 192.18.122.139
```

Internal LDAP requests are not recorded in the access log by default. To activate the logging of internal access operations, specify access logging level 4 on the `nsslapd-accesslog-level` configuration attribute (see [Section 3.1.2, "nsslapd-accesslog-level"](#)).

### 1.2.2. File Descriptor

Every connection from an external LDAP client to Directory Server requires a file descriptor or socket descriptor from the operating system, in this case `fd=608`. `fd=608` indicates that it was file descriptor number 608 out of the total pool of available file descriptors which was used.

```
[21/Apr/2007:11:39:51 -0700] conn=11 fd=608 slot=608 connection from
207.1.153.51 to 192.18.122.139
```

### 1.2.3. Slot Number

The slot number, in this case `slot=608`, is a legacy part of the access log which has the same meaning as file descriptor. Ignore this part of the access log.

```
[21/Apr/2007:11:39:51 -0700] conn=11 fd=608 slot=608 connection from  
207.1.153.51 to 192.18.122.139
```

### 1.2.4. Operation Number

To process a given LDAP request, Directory Server will perform the required series of operations. For a given connection, all operation request and operation result pairs are given incremental operation numbers beginning with `op=0` to identify the distinct operations being performed.

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97 nentries=0  
etime=0
```

In [Section 1.2, “Default Access Logging Content”](#), we have `op=0` for the bind operation request and result pair, then `op=1` for the LDAP search request and result pair, and so on. The entry `op=-1` in the access log generally means that the LDAP request for this connection was not issued by an external LDAP client but, instead, initiated internally.

### 1.2.5. Method Type

The method number, in this case `method=128`, indicates which LDAPv3 bind method was used by the client.

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 BIND dn="cn=Directory Manager"  
method=128 version=3
```

There are three possible bind method values:

- 0 for authentication
- 128 for simple bind with user password
- `sasl` for SASL bind using external authentication mechanism

### 1.2.6. Version Number

The version number, in this case `version=3`, indicates the LDAP version number (either LDAPv2 or LDAPv3) that the LDAP client used to communicate with the LDAP server.

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 BIND dn="cn=Directory Manager"
method=128 version=3
```

### 1.2.7. Error Number

The error number, in this case `err=0`, provides the LDAP result code returned from the LDAP operation performed. The LDAP error number 0 means that the operation was successful. For a more comprehensive list of LDAP result codes, see [Section 3, "LDAP Result Codes"](#).

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97 nentries=0
etime=0
```

### 1.2.8. Tag Number

The tag number, in this case `tag=97`, indicates the type of result returned, which is almost always a reflection of the type of operation performed. The tags used are the BER tags from the LDAP protocol.

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97 nentries=0
etime=0
```

Tag	Description
tag=97	A result from a client bind operation.
tag=100	The actual entry being searched for.
tag=101	A result from a search operation.
tag=103	A result from a modify operation.
tag=105	A result from an add operation.
tag=107	A result from a delete operation.
tag=109	A result from a moddn operation.
tag=111	A result from a compare operation.
tag=115	A search reference when the entry on which the search was performed holds a referral to the required entry. Search references are expressed in terms of a referral.
tag=120	A result from an extended operation.

**Table 5.1. Commonly-Used Tags**



### NOTE

`tag=100` and `tag=115` are not result tags as such, and so it is unlikely that they will be recorded in the access log.

### 1.2.9. Number of Entries

`nentries` shows the number of entries, in this case `nentries=0`, that were found matching the LDAP client's request.

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97 nentries=0  
etime=0
```

### 1.2.10. Elapsed Time

`etime` shows the elapsed time, in this case `etime=1000`, or the amount of time (in seconds) that it took the Directory Server to perform the LDAP operation.

```
[21/Apr/2007:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97 nentries=0  
etime=0
```

An `etime` value of 0 means that the operation actually took milliseconds to perform. To have microsecond resolution for this item in the access log, enter a value of 131328 (256+131072) in the `nsslapd-accesslog-level` configuration attribute.

### 1.2.11. LDAP Request Type

The LDAP request type indicates the type of LDAP request being issued by the LDAP client. Possible values are:

- SRCH for search
- MOD for modify
- DEL for delete
- ADD for add
- MODDN for moddn
- EXT for extended operation
- ABANDON for abandon operation

If the LDAP request resulted in sorting of entries, then the message `SORT serialno` will be recorded in the log, followed by the number of candidate entries that were sorted. For example:

```
[04/May/2007:15:51:46 -0700] conn=114 op=68 SORT serialno (1)
```

The number enclosed in parentheses specifies the number of candidate entries that were sorted, which in this case is 1.

### 1.2.12. LDAP Response Type

The LDAP response type indicates the LDAP response being issued by the LDAP client. There are three possible values:

- `RESULT`
- `ENTRY`
- `REFERRAL`, an LDAP referral or search reference

### 1.2.13. Unindexed Search Indicator

The unindexed search indicator, `notes=U`, indicates that the search performed was unindexed, which means that the database itself had to be directly searched instead of the index file. Unindexed searches occur in three scenarios:

- When the `nsslapd-idlistscanlimit` was reached within the index file used for the search.
- When no index file existed.
- When the index file was not configured in the way required by the search.



#### NOTE

An unindexed search indicator is often accompanied by a large `etime` value, as unindexed searches are generally more time consuming.

### 1.2.14. VLV-Related Entries

When a search involves virtual list views (VLVs), appropriate entries are logged in the access log file. Similar to the other entries, VLV-specific entries show the request and response information side by side:

```
VLV RequestInformation ResponseInformation
```

*RequestInformation* has the following form:

```
beforeCount:afterCount:index:contentCount
```

If the client uses a position-by-value VLV request, the format for the first part, the request information would be *beforeCount*: *afterCount*: *value*.

*ResponseInformation* has the following form:

```
targetPosition:contentCount (resultCode)
```

The example below highlights the VLV-specific entries:

```
[07/May/2007:11:43:29 -0700] conn=877 op=8530 SRCH base="(ou=People)"
scope=2 filter="(uid=*)"
[07/May/2007:11:43:29 -0700] conn=877 op=8530 SORT uid
[07/May/2007:11:43:29 -0700] conn=877 op=8530 VLV 0:5:0210 10:5397 (0)
[07/May/2007:11:43:29 -0700] conn=877 op=8530 RESULT err=0 tag=101
nentries=1 etime=0
```

In the above example, the first part, 0:5:0210, is the VLV request information:

- The *beforeCount* is 0.
- The *afterCount* is 5.
- The *value* is 0210.

The second part, 10:5397 (0), is the VLV response information:

- The *targetPosition* is 10.
- The *contentCount* is 5397.
- The (*resultCode*) is (0).

### 1.2.15. Search Scope

The entry `scope=n` defines the scope of the search performed, and *n* can have a value of 0, 1, or 2.

- 0 for base search

- 1 for one-level search
- 2 for subtree search

For more information about search scopes, see "Using Ldapsearch" in Appendix B, "Finding Directory Entries", in the *Red Hat Directory Server Administration Guide*.

### 1.2.16. Extended Operation OID

An extended operation OID, in this case either `EXT oid="2.16.840.1.113730.3.5.3"` or `EXT oid="2.16.840.1.113730.3.5.5"`, provides the OID of the extended operation being performed. The following table provides a partial list of LDAPv3 extended operations and their OIDs supported in Directory Server.

Extended Operation Name	Description	OID
Directory Server Start Replication Request	Sent by a replication initiator to indicate that a replication session is requested.	2.16.840.1.113730.3.5.3
Directory Server Replication Response	Sent by a replication responder in response to a Start Replication Request Extended Operation or an End Replication Request Extended Operation.	2.16.840.1.113730.3.5.4
Directory Server End Replication Request	Sent to indicate that a replication session is to be terminated.	2.16.840.1.113730.3.5.5
Directory Server Replication Entry Request	Carries an entry, along with its state information ( <i>csn</i> and <i>UniqueIdentifier</i> ) and is used to perform a replica initialization.	2.16.840.1.113730.3.5.6
Directory Server Bulk Import Start	Sent by the client to request a bulk import together with the suffix being imported to and sent by the server to indicate that the bulk import may begin.	2.16.840.1.113730.3.5.7
Directory Server Bulk Import Finished	Sent by the client to signal the end of a bulk import and sent by the server to acknowledge it.	2.16.840.1.113730.3.5.8

**Table 5.2. LDAPv3 Extended Operations Supported by Directory Server**

### 1.2.17. Change Sequence Number

The change sequence number, in this case `csn=3b4c8cfb00000030000`, is the replication change sequence number, indicating that replication is enabled on this particular naming context.

### 1.2.18. Abandon Message

The abandon message indicates that an operation has been aborted.

```
[21/Apr/2007:11:39:52 -0700] conn=12 op=2 ABANDON targetop=1 msgid=2
nentries=0 etime=0
```

`nentries=0` indicates the number of entries sent before the operation was aborted, `etime=0` value indicates how much time (in seconds) had elapsed, and `targetop=1` corresponds to an operation value from a previously initiated operation (that appears earlier in the access log).

There are two possible log `ABANDON` messages, depending on whether the message ID succeeds in locating which operation was to be aborted. If the message ID succeeds in locating the operation (the `targetop`) then the log will read as above. However, if the message ID does not succeed in locating the operation or if the operation had already finished prior to the `ABANDON` request being sent, then the log will read as follows:

```
[21/Apr/2007:11:39:52 -0700] conn=12 op=2 ABANDON targetop=NOTFOUND msgid=2
```

`targetop=NOTFOUND` indicates the operation to be aborted was either an unknown operation or already complete.

### 1.2.19. Message ID

The message ID, in this case `msgid=2`, is the LDAP operation identifier, as generated by the LDAP SDK client. The message ID may have a different value than the operation number but identifies the same operation. The message ID is used with an `ABANDON` operation and tells the user which client operation is being abandoned.

```
[21/Apr/2007:11:39:52 -0700] conn=12 op=2 ABANDON targetop=NOTFOUND msgid=2
```



#### NOTE

The Directory Server operation number starts counting at 0, and, in the majority of LDAP SDK/client implementations, the message ID number starts counting at 1, which explains why the message ID is frequently equal to the Directory Server operation number plus 1.

## 1.2.20. SASL Multi-Stage Bind Logging

In Directory Server, logging for multi-stage binds is explicit. Each stage in the bind process is logged, and, where appropriate, the progress statement `SASL bind in progress` is included.

In logging a SASL bind, the `sasl` method is followed by the LDAP version number (see [Section 1.2.6, "Version Number"](#)) and the SASL mechanism used, as shown below with the GSS-API mechanism.

```
[21/Apr/2007:12:57:14 -0700] conn=32 op=0 BIND dn="" method=sasl version=3
mech=GSSAPI
```



### NOTE

The authenticated DN (the DN used for access control decisions) is now logged in the BIND result line as opposed to the bind request line, as was previously the case:

```
[21/Apr/2007:11:39:55 -0700] conn=14 op=1 RESULT err=0 tag=97 nentries=0
etime=0
dn="uid=jdoe,dc=example,dc=com"
```

For SASL binds, the DN value displayed in the bind request line is not used by the server and, as a consequence, is not relevant. However, given that the authenticated DN is the DN which, for SASL binds, must be used for audit purposes, it is essential that this be clearly logged. Having this authenticated DN logged in the bind result line avoids any confusion as to which DN is which.

## 1.3. Access Log Content for Additional Access Logging Levels

This section presents the additional access logging levels available in the Directory Server access log. In the following example, access logging level 4, which logs internal operations, is enabled.

```
[12/Jul/2007:16:45:46 +0200] conn=Internal op=-1
SRCH base="cn=\22dc=example,dc=com\22,cn=mapping tree,cn=config"scope=0
filter="objectclass=nsMappingTree"attrs="nsslapd-referral"
options=persistent
[12/Jul/2007:16:45:46 +0200] conn=Internal op=-1 RESULT err=0 tag=48
nentries=1etime=0
[12/Jul/2007:16:45:46 +0200] conn=Internal op=-1
SRCH base="cn=\22dc=example,dc=com\22,cn=mapping tree,cn=config"scope=0
filter="objectclass=nsMappingTree" attrs="nsslapd-state"
[12/Jul/2007:16:45:46 +0200] conn=Internal op=-1 RESULT err=0 tag=48
nentries=1etime=0
```

Access log level 4 enables logging for internal operations, which log search base, scope, filter, and requested search attributes, in addition to the details of the search being performed.

In the following example, access logging level 768 is enabled (512 + 256), which logs access to entries and referrals. In this extract, six entries and one referral are returned in response to the search request, which is shown on the first line.

```
[12/Jul/2007:16:43:02 +0200] conn=306 fd=60 slot=60 connection from
127.0.0.1 to 127.0.0.1 \
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 SRCH base="dc=example,dc=com" \
    scope=2 filter="(description=*)" attrs=ALL
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 ENTRY dn="ou=Special
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=Accounting
Managers,ou=groups,dc=example,dc=com"
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=HR
Managers,ou=groups,dc=example,dc=com"
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=QA
Managers,ou=groups,dc=example,dc=com"
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=PD
Managers,ou=groups,dc=example,dc=com"
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 ENTRY dn="ou=Red Hat
Servers,dc=example,dc=com"
[12/Jul/2007:16:43:02 +0200] conn=306 op=0 REFERRAL
```

### 1.3.1. Connection Description

The connection description, in this case `conn=Internal`, indicates that the connection is an internal connection. The operation number `op=-1` also indicates that the operation was initiated internally.

```
[12/Jul/2007:16:45:46 +0200] conn=Internal op=-1
    ENTRY dn="cn=\22dc=example,dc=com\22, cn=mapping tree, cn=config"
```

### 1.3.2. Options Description

The options description, in this case `options=persistent`, indicates that a persistent search is being performed. Persistent searches can be used as a form of monitoring and configured to return changes to given configurations as changes occur.

```
[12/Jul/2007:16:45:46 +0200] conn=Internal op=-1
    SRCH base="cn=\22dc=example,dc=com\22,cn=mapping tree,cn=config"scope=0
    filter="objectclass=nsMappingTree"attrs="nsslapped-referral"
options=persistent
```

In this example, both access logging level 512 and 4 are enabled, which results in both internal

access operations and entry access and referrals being logged.

## 2. Common Connection Codes

A connection code is a code that is added to the `closed` log message to provide additional information related to the connection closure. Common connection codes include:

Connection Code	Description
A1	Client aborts the connection.
B1	Corrupt BER tag encountered. If BER tags, which encapsulate data being sent over the wire, are corrupt when they are received, a B1 connection code is logged to the access log. BER tags can be corrupted due to physical layer network problems or bad LDAP client operations, such as an LDAP client aborting before receiving all request results.
B2	BER tag is longer than the <code>nsslapd-maxbersize</code> attribute value. For further information about this configuration attribute, see <a href="#">Section 3.1.66, “nsslapd-maxbersize (Maximum Message Size)”</a> .
B3	Corrupt BER tag encountered.
B4	Server failed to flush data response back to client.
P2	Closed or corrupt connection has been detected.
T1	Client does not receive a result within the specified <code>idletimeout</code> period. For further information about this configuration attribute, see <a href="#">Section 3.1.58, “nsslapd-idletimeout (Default Idle Timeout)”</a> .
T2	Server closed connection after <code>ioblocktimeout</code> period was exceeded. For further information about this configuration attribute, see <a href="#">Section 3.1.60, “nsslapd-ioblocktimeout (IO Block Time Out)”</a> .
U1	Connection closed by server after client sends an unbind request. The server will always close the connection when it sees an unbind request.

Table 5.3. Common Connection Codes

### 3. LDAP Result Codes

LDAP has a set of result codes with which it is useful to be familiar.

Result Code	Defined Value	Result Code	Defined Value
0	SUCCESS	36	ALIAS_DEREFERENCING_PROBLEM
1	OPERATION_ERROR	48	INAPPROPRIATE_AUTHENTICATION
2	PROTOCOL_ERROR	49	INVALID_CREDENTIALS
3	TIME_LIMIT_EXCEEDED	50	INSUFFICIENT_ACCESS_RIGHTS
4	SIZE_LIMIT_EXCEEDED	51	BUSY
5	COMPARE_FALSE	52	UNAVAILABLE
6	COMPARE_TRUE	53	UNWILLING_TO_PERFORM
7	AUTH_METHOD_NOT_SUPPORTED	54	LOOP_DEFECT
8	STRONG_AUTH_REQUIRED	55	NAMING_VIOLATION
9	LDAP_PARTIAL_RESULT	65	OBJECT_CLASS_VIOLATION
10	REFERRAL (LDAP v3)	66	NOT_ALLOWED_ON_NONLEAF
11	ADMIN_LIMIT_EXCEEDED (LDAP v3)	67	NOT_ALLOWED_ON_RDN
12	UNAVAILABLE_CRITICAL_EXTENSION (LDAP v3)	68	ENTRY_ALREADY_EXISTS
13	CONFIDENTIALITY_REQUIRED (LDAP v3)	69	OBJECT_CLASS_MODS_PROHIBITED
14	SASL_BIND_IN_PROGRESS	75	AFFECTS_MULTIPLE_DSAS (LDAP v3)
16	NO_SUCH_ATTRIBUTE	80	OTHER
17	UNDEFINED_ATTRIBUTE_TYPE	81	SERVER_DOWN
18	INAPPROPRIATE_MATCHING	85	LDAP_TIMEOUT
19	CONSTRAINT_VIOLATION	89	PARAM_ERROR
20	ATTRIBUTE_OR_VALUE_EXISTS	91	CONNECT_ERROR
21	INVALID_ATTRIBUTE_SYNTAX	92	LDAP_NOT_SUPPORTED
32	NO_SUCH_OBJECT	93	CONTROL_NOT_FOUND
33	ALIAS_PROBLEM	94	NO_RESULTS_RETURNED
34	INVALID_DN_SYNTAX	95	MORE_RESULTS_TO_RETURN
35	IS_LEAF	96	CLIENT_LOOP

<b>Result Code</b>	<b>Defined Value</b>	<b>Result Code</b>	<b>Defined Value</b>
	97	REFERRAL_LIMIT_EXCEEDED	

**Table 5.4. LDAP Result Codes**



# Command-Line Utilities

This chapter contains reference information on command-line utilities used with Red Hat Directory Server (Directory Server). These command-line utilities make it easy to perform administration tasks on the Directory Server.

## 1. Finding and Executing Command-Line Utilities

The `ldapsearch`, `ldapmodify`, `ldapdelete`, and `ldappasswd` command-line utilities are provided as a separate package, called either `mozldap-tools` or `mozldap6-tools`, and the utilities are installed in `/usr/lib/mozldap` or `/usr/lib/mozldap6`, respectively. Depending on the package installed on the system, add the path to the `PATH` environment variable to use the command-line utilities.



### NOTE

For most Linux systems, OpenLDAP tools are already installed in the `/usr/bin/` directory. These OpenLDAP tools are not supported for Directory Server operations. For the best results with the Directory Server, make sure the path to the Mozilla LDAP tools comes first in the `PATH` or use the full path and file name for every LDAP operation. To use Mozilla LDAP tools, ensure that `/usr/lib/mozldap` or `/usr/lib/mozldap6` appears in the `PATH` variable before `/usr/bin`.

These OpenLDAP tools can be used for Directory Server operations with certain cautions:

- The output of the other tools may be different, so it may not look like the examples in the documentation.
- The OpenLDAP tools require a `-x` argument to disable SASL so that it can be used for a simple bind, meaning the `-D` and `-w` arguments or an anonymous bind.
- The OpenLDAP tools' arguments for using TLS/SSL and SASL are quite different than the Mozilla LDAP arguments. See the OpenLDAP documentation for instructions on those arguments.

The `ldif` and `dbscan` command-line utilities are stored in the `/usr/bin` directory.

## 2. Using Special Characters

When using the `ldapsearch` command-line utility, it may be necessary to specify values that

contain characters that have special meaning to the command-line interpreter, such as space ( ), asterisk (\*), and backslash (\). When this situation occurs, enclose the value in quotation marks (""). For example:

```
-D "cn=Barbara Jensen, ou=Product Development, dc=example,dc=com"
```

Depending on the command-line interpreter, use either single or double quotation marks for this purpose. See the operating system documentation for more information.

Additionally, commas in DN values must be escaped with a backslash. For example:

```
-D "cn=Patricia Fuentes, ou=people, dc=example,dc=Bolivia\, S.A."
```

### 3. Command-Line Utilities Quick Reference

The following table provides a summary of the command-line utilities provided for Directory Server.

Command-Line Utility	Description
ldapsearch	Searches the directory and returns search results in LDIF format. For details on this tool, see the "Finding Directory Entries" appendix in the <i>Directory Server Administration Guide</i> .
ldapmodify	Adds, deletes, modifies, or renames entries. All operations are specified using LDIF update statements. For details on this tool, see "Adding and Modifying Entries Using ldapmodify" in the "Creating Directory Entries" chapter in the <i>Directory Server Administration Guide</i> .
ldapdelete	Deletes entries in the directory. For information on using this utility, see "Deleting Entries Using ldapdelete" in the "Creating Directory Entries" chapter in the <i>Directory Server Administration Guide</i> .
ldappasswd	Changes users passwords with the password change extended operation. For more information on the password extended change operation, see the "Managing the Password Policy" section of the "Managing User Accounts and Passwords" chapter in the <i>Directory Server Administration Guide</i> .
ldif	Automatically formats LDIF files and creates base 64-encoded attribute values. For details

Command-Line Utility	Description
	on this tool, see appendix A in the <i>Directory Server Administration Guide</i> .
dbscan	Analyzes and extracts information from a Directory Server database file.

**Table 6.1. Commonly-Used Command-Line Utilities**

## 4. ldapsearch

ldapsearch is a configurable utility that locates and retrieves directory entries via LDAP. This utility opens a connection to the specified server using the specified distinguished name and password and locates entries based on a specified search filter. Search scopes can include a single entry, an entry's immediate subentries, or an entire tree or subtree. Search results are returned in LDIF format.

- [Syntax](#)
- [Commonly-Used ldapsearch Options](#)
- [SSL Options](#)
- [SASL Options](#)
- [Additional ldapsearch Options](#)

### Syntax.

```
ldapsearch [-b basedn ] [ optional_options ] [ filter ] [ optional_list_of_attributes ]
```

For any value that contains a space ( ), the value should be enclosed in double quotation marks. For example:

```
-b "ou=groups, dc=example,dc=com"
```

Option	Description
<i>optional_options</i>	A series of command-line options. These must be specified before the search filter, if used.
<i>filter</i>	An LDAP search filter as described in <i>Directory Server Administration Guide</i> . Do not specify a search filter if search filters are supplied in a file using the <code>-f</code> option.

Option	Description
<i>optional_list_of_attributes</i>	A list of space-separated attributes that reduce the scope of the attributes returned in the search results. This list of attributes must appear after the search filter. For a usage example, see the <i>Directory Server Administration Guide</i> . If a list of attributes is not specified, the search returns values for all attributes permitted by the access control set in the directory with the exception of operational attributes.

**Table 6.2. ldapsearch Syntax**

To return operational attributes as a result of a search operation, they must be explicitly specified in the search command. To retrieve regular attributes along with explicitly-specified operational attributes, specify an asterisk (\*) in addition to the operational attributes.

### Commonly-Used ldapsearch Options.

The following table lists the most commonly used `ldapsearch` command-line options.

Option	Description
<code>-b</code>	<p>Specifies the starting point for the search. The value specified here must be a distinguished name that currently exists in the database. This option is optional if the <code>LDAP_BASEDN</code> environment variable has been set to a base DN.</p> <p>The value specified in this option should be provided in double quotation marks. For example:</p> <pre>-b "cn=Barbara Jensen, ou=Product Development, dc=example,dc=com"</pre> <p>The root DSE entry is a special entry that contains a list of all the suffixes supported by the local directory. To search this entry, supply a search base of "", a search scope of <code>base</code>, and a filter of <code>"objectclass=*"</code>. For example:</p> <pre>-b "" -s base "objectclass=*"</pre>

Option	Description
-D	<p>Specifies the distinguished name with which to authenticate to the server. This option is optional if anonymous access is supported by the server. If specified, this value must be a DN recognized by the Directory Server, and it must also have the authority to search for the entries. For example:</p> <pre data-bbox="810 689 1359 752">-D "uid=bjensen, dc=example,dc=com"</pre>
-g	<p>Specifies that the password policy request control not be sent with the bind request. By default, the new LDAP password policy request control is sent with bind requests.</p> <p>The <code>ldapsearch</code> tool can parse and display information from the response control if it is returned by a server; that is, the tool will print an appropriate error or warning message when a server sends the password policy response control with the appropriate value.</p> <p>The criticality of the request control is set to <code>false</code> to ensure that all LDAPv3 servers that do not understand the control can ignore it. To suppress sending of the request control with the bind request, include <code>-g</code> on the command-line.</p>
-h	<p>Specifies the hostname or IP address of the machine on which the Directory Server is installed. If a host is not specified, <code>ldapsearch</code> uses the local host. For example:</p> <pre data-bbox="810 1657 1359 1720">-h mozilla</pre>
-l	<p>Specifies the maximum number of seconds to wait for a search request to complete. For example:</p> <pre data-bbox="810 1921 1359 1984">-l 300</pre>

Option	Description
	<p>Regardless of the value specified here, <code>ldapsearch</code> will never wait longer than is allowed by the server's <code>nsslapd-timelimit</code> attribute, unless the authenticated user is the Directory Manager. The default value for the <code>nsslapd-timelimit</code> attribute is 3600 seconds. See <a href="#">Section 3.1.95, “nsslapd-timelimit (Time Limit)”</a> for more information.</p>
-p	<p>Specifies the TCP port number that the Directory Server uses. For example:</p> <pre data-bbox="807 757 1390 824">-p 1049</pre> <p>The default is 389. If <code>-z</code> is used, the default is 636.</p>
-s	<p>Specifies the scope of the search. The scope can be one of the following:</p> <ul data-bbox="807 1115 1347 1615" style="list-style-type: none"> <li>• <code>base</code> searches only the entry specified in the <code>-b</code> option or defined by the <code>LDAP_BASEDN</code> environment variable.</li> <li>• <code>one</code> searches only the immediate children of the entry specified in the <code>-b</code> option. Only the children are searched; the actual entry specified in the <code>-b</code> option is not searched.</li> <li>• <code>sub</code> searches the entry specified in the <code>-b</code> option and all of its descendants. That is, perform a subtree search starting at the point identified in the <code>-b</code> option. This is the default.</li> </ul>
-w	<p>Specifies the password associated with the distinguished name that is specified in the <code>-D</code> option. For example:</p> <pre data-bbox="807 1800 1390 1868">-w diner892</pre> <p>If this option is not specified, anonymous access is used.</p>

Option	Description
	If a dash (-) is used as the password value, the utility prompts for the password after the command is entered. This avoids having the password on the command line.
-x	Specifies that the search results are sorted on the server rather than on the client. This is useful to sort according to a matching rule, as with an international search. In general, it is faster to sort on the server rather than on the client.
-z	<p>Specifies the maximum number of entries to return in response to a search request. For example:</p> <pre data-bbox="805 898 1358 965">-z 1000</pre> <p>Normally, regardless of the value specified here, <code>ldapsearch</code> never returns more entries than the number allowed by the server's <code>nsslapd-sizelimit</code> attribute, unless the authenticated user is the Directory Manager. However, this limitation can be overridden by binding as the root DN when using this command-line argument. This is because binding as the root DN causes this option to default to zero (0). The default value for the <code>nsslapd-sizelimit</code> attribute is 2000 entries. See <a href="#">Section 3.1.92, “nsslapd-sizelimit (Size Limit)”</a> for more information.</p>

**Table 6.3. Commonly-Used ldapsearch Options**

### SSL Options.

The following command-line options can be used to specify that `ldapsearch` use LDAPS when communicating with an SSL-enabled Directory Server or used for certificate-based authentication. These options are valid only when LDAPS has been turned on and configured for the Directory Server. For information on certificate-based authentication and creating a certificate database for use with LDAP clients, see the "Managing SSL" chapter in the *Directory Server Administration Guide*.

In addition to the standard `ldapsearch` options, to run an `ldapsearch` command using SSL,

specify the following:

```
ldapsearch { -Z, -ZZ, -ZZZ } [ -p secure_port ] [ -P certificate_database ] [ -N
certificate_name ] [ -K key_database ] [ -W key database password ]
```



### NOTE

To run `ldapsearch` over TLS/SSL, either the `-z` option is required (for SSL) or the `-zz` or `-zzz` option is required (for Start TLS).

Option	Description
-3	Specifies that hostnames should be checked in SSL certificates.
-I	Specifies the SSL key password <i>file</i> that contains the token:password pair.
-K	Specifies the absolute path, including the filename, of the private key database of the client.  The <code>-K</code> option must be specified when the key database has a different name than <code>key3.db</code> or when the key database is not under the same directory as the certificate database, the <code>cert8.db</code> file (the path which is specified with the <code>-P</code> option).
-m	Specifies the path to the security module database, such as <code>/etc/dirsrv/slapd-<i>instance_name</i>/secmod.db</code> . This option only need to be given if the security module database is in a different directory than the certificate database itself.
-N	Specifies the certificate name to use for certificate-based client authentication, such as <code>-N "Server-Cert"</code> . If this option is specified, then the <code>-z</code> , <code>-P</code> , and <code>-W</code> options are required. Also, if this option is specified, then the <code>-D</code> and <code>-w</code> options must <i>not</i> be specified, or certificate-based authentication will not occur, and the bind operation will use the authentication credentials specified on <code>-D</code> and <code>-w</code> .
-P	Specifies the absolute path, including the

Option	Description
	<p>option, of the certificate database of the client. This option is used only with the <code>-z</code> option.</p> <p>When used on a machine where an SSL-enabled web browser is configured, the path specified on this option can be that of the certificate database for the browser. For example:</p> <pre data-bbox="805 678 1390 741">-P /security/cert.db</pre> <p>The client security files can also be stored on the Directory Server in the <code>/etc/dirsrv/slapd-<i>instance_name</i></code> directory. In this case, the <code>-P</code> option would call out a path and filename similar to the following:</p> <pre data-bbox="805 1043 1390 1133">-P /etc/dirsrv/slapd-<i>instance_name</i>/client-cert.db</pre>
<p><code>-Q</code></p>	<p>Specifies the token and certificate name, which is separated by a semi-colon (;) for PKCS11.</p>
<p><code>-W</code></p>	<p>Specifies the password for the private key database identified in the <code>-P</code> option. For example:</p> <pre data-bbox="805 1435 1390 1498">-W serverpassword</pre> <p>If a dash (-) is used as the password value, the utility prompts for the password after the command is entered. This avoids having the password on the command line.</p>
<p><code>-z</code></p>	<p>Specifies that SSL is to be used for the search request.</p>
<p><code>-ZZ</code></p>	<p>Specifies the Start TLS request. Use this option to make a cleartext connection into a secure one. If the server does not support Start TLS, the command does not have to be aborted; it will continue in cleartext.</p>
<p><code>-ZZZ</code></p>	<p>Enforces the Start TLS request. The server</p>

Option	Description
	must respond that the request was successful. If the server does not support Start TLS, such as Start TLS is not enabled or the certificate information is incorrect, the command is aborted immediately.

**Table 6.4. Additional SSL Idapsearch Options**

**SASL Options.**

SASL mechanisms can be used to authenticate a user, using the `-o` the required SASL information.

To learn which SASL mechanisms are supported, search the root DSE. See the `-b` option in [Table 6.3, “Commonly-Used Idapsearch Options”](#).

Option	Description
<code>-o</code>	Specifies SASL options. The format is <code>-o sas/Option=value</code> . <i>sas/Option</i> can have one of six values: <ul style="list-style-type: none"> <li>• mech</li> <li>• authid</li> <li>• authzid</li> <li>• secProp</li> <li>• realm</li> <li>• flags</li> </ul> The expected values depend on the supported mechanism. The <code>-o</code> can be used multiple times to pass all of the required SASL information for the mechanism. For example: <pre style="background-color: #f0f0f0; padding: 5px;">-o "mech=DIGEST-MD5" -o "authzid=test_user" -o "authid=test_user"</pre>

**Table 6.5. SASL Options**

There are three SASL mechanisms supported in Red Hat Directory Server:

- CRAM-MD5, described in [Table 6.6, “Description of CRAM-MD5 Mechanism Options”](#)
- DIGEST-MD5, described in [Table 6.7, “Description of DIGEST-MD5 SASL Mechanism Options”](#)
- GSSAPI, described in [Table 6.8, “Description of GSSAPI SASL Mechanism Options”](#)

Required or Optional	Option	Description	Example
Required	<code>mech=CRAM-MD5</code>	Gives the SASL mechanism.	-o "mech=CRAM-MD5"
Required	<code>authid=authid_value</code>	Gives the ID used to authenticate to the server. <i>authid_value</i> can be the following: <ul style="list-style-type: none"> <li>• <i>UID</i>. For example, <code>msmith</code>.</li> <li>• <i>u: uid</i>. For example, <code>u:msmith</code>.</li> <li>• <i>dn: dn_value</i>. For example, <code>dn:uid=msmith,ou=People,o=example.com</code>.</li> </ul>	-o "authid=dn:uid=msmith,ou=People,o=example.com"
Optional	<code>secprop=value</code>	The <code>secprop</code> attribute sets the security properties for the connection. The <code>secprop</code> value can be any of the following: <ul style="list-style-type: none"> <li>• None</li> <li>• <i>noplain</i> — Do not permit mechanisms susceptible to simple passive attack.</li> <li>• <i>noactive</i> — Do not</li> </ul>	-o "secprop=noplain,minssf=1,maxbufsize=512"

Required or Optional	Option	Description	Example
		<p>permit mechanisms susceptible to active attacks.</p> <ul style="list-style-type: none"> <li>• <i>nodict</i> — Do not permit mechanisms susceptible to passive dictionary attacks.</li> <li>• <i>forwardsec</i> — Require forward secrecy.</li> <li>• <i>passcred</i> — Attempt to pass client credentials.</li> <li>• <i>noanonymous</i> — Do not permit mechanisms that allow anonymous access.</li> <li>• <i>minssf</i> — Require a minimum security strength; this option needs a numeric value specifying bits of encryption. A value of - 1 means integrity is provided without privacy.</li> <li>• <i>maxssf</i> — Require a maximum security strength; this option needs a numeric value specifying bits of encryption. A value of - 1 means integrity is provided without privacy.</li> </ul>	

Required or Optional	Option	Description	Example
		<ul style="list-style-type: none"> <li><i>maxbufsize</i> — Set the maximum receive buffer size the client will accept when using integrity or privacy settings.</li> </ul>	


**Table 6.6. Description of CRAM-MD5 Mechanism Options**

Required or Optional	Option	Description	Example
Required	<code>mech=DIGEST-MD5</code>	Gives the SASL mechanism.	-o "mech=DIGEST-MD5"
Required	<code>authid=<i>authid_value</i></code>	<p>Gives the ID used to authenticate to the server. <i>authid_value</i> can be the following:</p> <ul style="list-style-type: none"> <li><i>UID</i>. For example, <code>msmith</code>.</li> <li><i>u: uid</i>. For example, <code>u:msmith</code>.</li> <li><i>dn: dn_value</i>. For example, <code>dn:uid=msmith,ou=People,o=example.com</code>.</li> </ul>	-o "authid=dn:uid=msmith,ou=People,o=example.com"
Optional	<code>secprop=<i>value</i></code>	<p>The <code>secprop</code> attribute sets the security properties for the connection. The <code>secprop</code> value can be any of the following:</p> <ul style="list-style-type: none"> <li>None</li> <li><i>noplain</i> — Do not</li> </ul>	-o "secprop=noplain,noanonymous,maxssf=128,minssf=128"

Required or Optional	Option	Description	Example
		<p>permit mechanisms susceptible to simple passive attack.</p> <ul style="list-style-type: none"> <li>• <i>noanonymous</i> — Do not permit mechanisms that allow anonymous access.</li> <li>• <i>minssf</i> — Require a minimum security strength; this option needs a numeric value specifying bits of encryption. A value of - 1 means integrity is provided without privacy.</li> <li>• <i>maxssf</i> — Require a maximum security strength; this option needs a numeric value specifying bits of encryption. A value of - 1 means integrity is provided without privacy. The maximum value is 128.</li> </ul>	

**Table 6.7. Description of DIGEST-MD5 SASL Mechanism Options**

Required or Optional	Option	Description	Example
Required	mech=GSSAPI	Gives the SASL mechanism.	-o "mech=GSSAPI"

Required or Optional	Option	Description	Example
		<div data-bbox="805 369 1104 853" style="background-color: #333; color: white; padding: 10px;">  <p><b>NOTE</b> Have the Kerberos ticket before issuing a GSS-API request.</p> </div>	
Optional	secprop= <i>value</i>	<p>The <code>secprop</code> attribute sets the security properties for the connection. The <code>secprop</code> value can be any of the following:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• <i>noplain</i> — Do not permit mechanisms susceptible to simple passive attack.</li> <li>• <i>noanonymous</i> — Do not permit mechanisms that allow anonymous access.</li> <li>• <i>minssf</i> — Require a minimum security strength; this option needs a numeric value specifying bits of encryption. A value of <code>- 1</code> means integrity is provided</li> </ul>	<p>-o "secprop=noplain,noanonymous,maxssf=56,minssf=56"</p>

Required or Optional	Option	Description	Example
		<p>without privacy.</p> <ul style="list-style-type: none"> <li>• <i>maxssf</i> — Require a maximum security strength; this option needs a numeric value specifying bits of encryption. A value of - 1 means integrity is provided without privacy. The maximum value is 56.</li> </ul>	

Table 6.8. Description of GSSAPI SASL Mechanism Options

## Additional Idapsearch Options.

Option	Description
-A	Specifies that the search retrieve the attributes only, not the attribute values. This option is useful to determine if an attribute is present for an entry and the value is not important.
-a	Specifies how alias dereferencing is completed. Values can be <i>never</i> , <i>always</i> , <i>search</i> , or <i>find</i> . The default value is <i>never</i> .
-B	Print non-ASCII values using the old output format ( <i>attrName=attrValue</i> ).
-c	<p>Specifies the <code>getEffectiveRights</code> control <code>authzid</code>. For example:</p> <pre>dn:uid=bjensen,dc=example,dc=com</pre> <p>A value of "" means the authorization ID for the operation. A value of <code>dn:</code> means <code>anonymous</code></p>
-F	Specifies a different separator. This option allows a separator other than a colon (:) to

Option	Description
	<p>separate an attribute name from the corresponding value. For example:</p> <pre data-bbox="810 409 1359 477">-F +</pre>
-f	<p>Specifies the file containing the search filters to be used in the search. For example:</p> <pre data-bbox="810 633 1359 701">-f search_filters</pre> <p>option to supply a search filter directly to the command line.</p> <p>For more information about search filters, see Appendix B, "Finding Directory Entries", in the <i>Directory Server Administration Guide</i>.</p>
-G	<p>Conducts a virtual list view search. This option can set the number of entries before or after the search target and the index or value of the first entry returned.</p> <p>For example, a <i>value</i> operation that sorts by surname, <code>-G 20:30:johnson</code>, returns the first entry with a surname equal to or less than <code>johnson</code>, in addition to 20 entries that come before it and 30 entries that come after it. If there are fewer matching entries in the directory than the before or after number requested by the search, all available entries before/after the search target that match the search criteria are returned.</p> <p>An <i>index</i> operation which sorts by surname, <code>-G 20:30:100:0</code>, returns from the 80th through 130th entries sorted by <i>sn</i>. Use 0 as the fourth value for the count number unless you know how many entries the VLV index has.</p>
-i	<p>Specifies the character set to use for command-line input. The default is the character set specified in the <code>LANG</code> environment variable. Use this option to perform the conversion from the specified</p>

Option	Description
	<p>character set to UTF8, thus overriding the environment variable setting.</p> <p>This argument can input the bind DN, base DN, and the search filter pattern in the specified character set.</p> <p><code>ldapsearch</code> converts the input from these arguments before it processes the search request. For example, <code>-i no</code> indicates that the bind DN, base DN, and search filter are provided in Norwegian. This argument only affects the command-line input; that is, if a file containing a search filter (with the <code>-f</code> option) is specified, <code>ldapsearch</code> will not convert the data in the file.</p>
-J	<p>Send an arbitrary control. This option can be used in the following format to retrieve access control information on a specific entry:</p> <pre data-bbox="807 1039 1367 1133">-J control OID:boolean criticality:dn:AuthID</pre> <ul style="list-style-type: none"> <li>• <i>control OID</i> is the OID for the get effective rights control, <code>1.3.6.1.4.1.42.2.27.9.5.2</code>.</li> <li>• <i>boolean criticality</i> specifies whether the search operation should return an error if the server does not support this control (<code>true</code>) or if it should be ignored and let the search return as normal (<code>false</code>).</li> <li>• <i>AuthId</i> is the DN of the user whose rights to check.</li> </ul>
-k	Bypasses converting the password to UTF8.
-M	Manages smart referrals. This causes the server not to return the smart referral contained on the entry but, instead, to return the actual entry containing the referral. Use this option to search for entries that contain smart referrals. For more information about

Option	Description
	smart referrals, see the "Configuring Directory Databases" chapter in the <i>Directory Server Administration Guide</i> .
-n	Specifies that the search is not actually to be performed, but that <code>ldapsearch</code> is to show what it would do with the specified input.
-O	<p>Specifies the maximum number of referral hops <code>ldapsearch</code> should automatically follow. For example:</p> <pre data-bbox="807 692 1390 763">-O 2</pre>
-R	Specifies that referrals are not to be followed automatically. By default, referrals are followed automatically.
-S	<p>Specifies the attribute to use as the sort criteria. For example:</p> <pre data-bbox="807 1014 1390 1086">-S sn</pre> <p>Use multiple <code>-s</code> arguments to further define the sort order. In the following example, the search results will be sorted first by surname and then by given name:</p> <pre data-bbox="807 1279 1390 1350">-S sn -S givenname</pre> <p>The default is not to sort the returned entries.</p>
-T	Specifies that no line breaks should be used within individual values in the search results.
-t	Specifies that the results be written to a set of temporary files. With this option, each attribute value is placed in a separate file within the system temporary directory. No base-64 encoding is performed on the values, regardless of the content.
-u	Specifies that the user-friendly form of the distinguished name be used in the output.
-v	Specifies that the utility is to run in verbose mode.
-V	Specifies the LDAP version number to be used on the search. For example:

Option	Description
	<p><code>-V 2</code></p> <p>LDAPv3 is the default. An LDAPv3 search cannot be performed against a Directory Server that only supports LDAPv2.</p>
<code>-Y</code>	<p>Specifies the proxy DN to use for the search. This argument is provided for testing purposes. For more information about proxied authorization, see the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i>.</p>
<code>-X</code>	<p>Specifies the <code>getEffectiveRights</code> control specific attribute list, where attributes are separated by spaces. For example:</p> <p><code>"nsroledn userPassword"</code></p>

Table 6.9. Additional `ldapsearch` Options

## 5. `ldapmodify`

`ldapmodify` makes changes to directory entries via LDAP.

- [Syntax](#)
- [Commonly-Used `ldapmodify` Options](#)
- [SSL Options](#)
- [SASL Options](#)
- [Additional `ldapmodify` Options](#)

### Syntax.

```
ldapmodify [ optional_options ]
```

```
ldapmodify [ -D binddn ] [ -w passwd ] [ -acmnrvFR ] [ -d debug_level ] [ -h host ] [ -p port ] [ -M auth_mechanism ] [ -Z/ZZ/ZZZ ] [ -V version ] [ -f file ] [ -l number_of_ldap_connections ] [ entryfile ]
```

## Commonly-Used Idapmodify Options.

Option	Description
-a	<p>Adds LDIF entries to the directory without requiring the <code>changetype:add</code> LDIF update statement. This provides a simplified method of adding entries to the directory. This option also allows directly adding a file created by <code>ldapmodify</code>.</p>
-B	<p>Specifies the suffix under which the new entries will be added.</p>
-D	<p>Specifies the distinguished name with which to authenticate to the server. The value must be a DN recognized by the Directory Server, and it must also have the authority to modify the entries. For example:</p> <pre data-bbox="810 943 1359 1003">-D "uid=bjensen, dc=example,dc=com"</pre> <p>This option cannot be used with the <code>-N</code> option.</p>
-f	<p>Option that specifies the file containing the LDIF update statements used to define the directory modifications. For example:</p> <pre data-bbox="810 1240 1359 1301">-f modify_statements</pre> <p>If this option is not supplied, the update statements are read from <code>stdin</code>.</p> <p>For information on supplying LDIF update statements from the command-line, see the "Creating Directory Entries" chapter in the <i>Directory Server Administration Guide</i>.</p>
-g	<p>Specifies that the password policy request control not be sent with the bind request. By default, the new LDAP password policy request control is sent with bind requests. The <code>ldapmodify</code> tool can parse and display information from the response control if it is returned by a server; that is, the tool will print an appropriate error or warning message when a server sends the password policy response control with an appropriate value. The criticality of the request control is set to</p>

Option	Description
	<p><code>false</code> to ensure that all LDAPv3 servers that do not understand the control can ignore it. To suppress sending of the request control with the bind request, include <code>-g</code> on the command-line.</p>
<p><code>-h</code></p>	<p>Specifies the name of the host on which the server is running. For example:</p> <pre data-bbox="807 607 1390 674">-h cyclops</pre>
<p><code>-p</code></p>	<p>Specifies the port number that the server uses. For example:</p> <pre data-bbox="807 801 1390 869">-p 1049</pre> <p>The default is 389. If <code>-z</code> is used, the default is 636.</p>
<p><code>-q</code></p>	<p>Causes each add to be performed silently as opposed to being echoed to the screen individually.</p>
<p><code>-w</code></p>	<p>Specifies the password associated with the distinguished name specified in the <code>-D</code> option. For example:</p> <pre data-bbox="807 1238 1390 1305">-w mypassword</pre> <p>If a dash (-) is used as the password value, the utility prompts for the password after the command is entered. This avoids having the password on the command line.</p>

**Table 6.10. Commonly-Used ldapmodify Options**

### SSL Options.

Use the following command-line options to specify that `ldapmodify` is to use LDAP over SSL (LDAPS) when communicating with the Directory Server. LDAPS encrypts data during transit. Also, use these options for certificate-based authentication. These options are valid only when SSL has been turned on and configured for the Directory Server. For more information on certificate-based authentication and on creating a certificate database for use with LDAP clients, see the "Managing SSL" chapter in the *Directory Server Administration Guide*.

Ensure that the Directory Server's encrypted port is specified when using these options.

Option	Description
-3	Specifies that hostnames should be checked in SSL certificates.
-I	Specifies the SSL key password <i>file</i> that contains the token:password pair.
-K	Specifies the path, including the filename, of the private key database of the client. Either the absolute or relative (to the server root) path can be specified. The <code>-K</code> option must be used when the key database has a different name than <code>key3.db</code> or when the key database is not under the same directory as the certificate database, the <code>cert8.db</code> file (the path for which is specified with the <code>-P</code> option).
-N	<p>Specifies the certificate name to use for certificate-based client authentication. For example:</p> <pre data-bbox="810 969 1390 1032">-N Server-Cert</pre> <p>If this option is specified, then the <code>-z</code> and <code>-w</code> options are required. Also, if this option is specified, then the <code>-D</code> and <code>-w</code> options must not be specified, or certificate-based authentication will not occur, and the bind operation will use the authentication credentials specified on <code>-D</code> and <code>-w</code>.</p>
-P	<p>Specifies the absolute path, including the filename, of the certificate database of the client. This option is used only with the <code>-z</code> option. When used on a machine where an SSL-enabled web browser is configured, the path specified on this option can be pointed to the certificate database for the web browser. For example:</p> <pre data-bbox="810 1659 1390 1722">-P /security/cert.db</pre> <p>The client security files can be stored on the Directory Server in the <code>/etc/dirsrv/slapd-<i>instance_name</i></code> directory. In this case, the <code>-P</code> option calls out a path and filename similar to the following:</p> <pre data-bbox="810 1962 1390 2024">-P</pre>

Option	Description
	<code>/client-cert.db</code>
<code>-Q</code>	Specifies the token and certificate name, which is separated by a semicolon (;) for PKCS11.
<code>-W</code>	Specifies the password for the certificate database identified on the <code>-P</code> option. For example:  <code>-W serverpassword</code>
<code>-Z</code>	Specifies that SSL is to be used for the directory request.
<code>-ZZ</code>	Specifies the Start TLS request. Use this option to make a cleartext connection into a secure one. If the server does not support Start TLS, the command does not need aborted; it will continue in cleartext.
<code>-ZZZ</code>	Enforces the Start TLS request. The server must respond that the request was successful. If the server does not support Start TLS, such as Start TLS is not enabled or the certificate information is incorrect, the command is aborted immediately.

**Table 6.11. Idapmodify SSL Options**

**SASL Options.**

SASL mechanisms can be used to authenticate a user, using the `-o` the required SASL information.

To learn which SASL mechanisms are supported, search the root DSE. See the `-b` option in [Table 6.3, “Commonly-Used Idapsearch Options”](#).

Option	Description
<code>-o</code>	Specifies SASL options. The format is <code>-o saslOption=value</code> . <i>saslOption</i> can have one of six values:  <ul style="list-style-type: none"> <li>• mech</li> </ul>


Option	Description
	<ul style="list-style-type: none"> <li>• authid</li> <li>• authzid</li> <li>• secProp</li> <li>• realm</li> <li>• flags</li> </ul> <p>The expected values depend on the supported mechanism. The <code>-o</code> can be used multiple times to pass all of the required SASL information for the mechanism. For example:</p> <pre style="background-color: #f0f0f0; padding: 5px;">-o "mech=DIGEST-MD5" -o "authzid=test_user" -o "authid=test_user"</pre>

**Table 6.12. SASL Options**

See [SASL Options](#) for information on how to use SASL options with `ldapmodify`.

**Additional ldapmodify Options.**

Option	Description
<p><code>-b</code></p>	<p>Causes the utility to check every attribute value to determine whether the value is a valid file reference. If the value is a valid file reference, then the content of the referenced file is used as the attribute value. This is often used for specifying a path to a file containing binary data, such as JPEG.</p> <p>For example, to add a <code>jpegPhoto</code> attribute, specify the <code>-b</code> option on the <code>ldapmodify</code> call. In the LDIF provided to <code>ldapmodify</code>, include a line like the following:</p> <pre style="background-color: #f0f0f0; padding: 5px;">jpegPhoto: /tmp/photo.jpeg</pre> <p><code>ldapmodify</code> reads the contents of the <code>photo.jpeg</code> file into the <code>jpegPhoto</code> attribute</p>

Option	Description
	<p>being added to the entry.</p> <p>As an alternative to the <code>-b</code> option, use the <code>:&lt;</code> URL specifier notation, which is simpler. For example:</p> <pre data-bbox="810 510 1359 573">jpegphoto:&lt; file:///tmp/myphoto.jpg</pre> <p>Although the official notation requires three <code>///</code>, the use of one <code>/</code> is accepted.</p> <div data-bbox="810 725 1359 1169" style="background-color: #333; color: #fff; padding: 10px;"> <p> <b>NOTE</b></p> <p>The <code>:&lt;</code> URL specifier notation only works if LDIF statement is version 1 or later, meaning <code>version: 1</code> is inserted in the LDIF file. Otherwise, the file URL is appended as the attribute value rather than the contents of the file.</p> </div> <p>For further information on the LDIF format, see the "Managing Directory Entries" chapter in the <i>Directory Server Administration Guide</i>.</p>
-c	Specifies that the utility run in continuous operation mode. Errors are reported, but the utility continues with modifications. The default is to quit after reporting an error.
-H	Lists all available <code>ldapmodify</code> options.
-M	Manages smart referrals. This causes the server not to return the smart referral contained on the entry but, instead, to apply the modification request directly to the entry. Use this option to add, change, or delete a directory entry that contains a smart referral. For more information about smart referrals, see the "Configuring Directory Databases" chapter in the <i>Directory Server Administration Guide</i> .
-n	Specifies that the entries are not actually to

Option	Description
	be modified but that <code>ldapmodify</code> is to show what it would do with the specified input.
<code>-O</code>	Specifies the maximum number of referral hops to follow. For example:  <code>-O 2</code>
<code>-R</code>	Specifies that referrals are not to be followed automatically.
<code>-v</code>	Specifies that the utility is to run in verbose mode.
<code>-V</code>	Specifies the LDAP version number to be used on the operation. For example:  <code>-V 2</code>  LDAPv3 is the default. An LDAPv3 operation cannot be performed against a Directory Server that only supports LDAPv2.
<code>-Y</code>	Specifies the proxy DN to use for the modify operation. This argument is provided for testing purposes. For more information about proxied authorization, see the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i> .

**Table 6.13. Additional ldapmodify Options**

## 6. Idapdelete

`ldapdelete` performs delete operations on directory entries via LDAP.

- [Syntax](#)
- [Commonly-Used ldapdelete Options](#)
- [SSL Options](#)
- [SASL Options](#)
- [Additional ldapdelete Options](#)

**Syntax.**

```
ldapdelete [ optional_options ]
```

**Commonly-Used ldapdelete Options.**

Option	Description
-D	<p>Specifies the distinguished name with which to authenticate to the server. The value must be a DN recognized by the Directory Server, and it must also have the authority to delete the entries. For example:</p> <pre data-bbox="810 779 1359 846">-D "uid=bjensen, dc=example,dc=com"</pre> <p>For more information on access control, see the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i>. The -D option cannot be used with the -N option.</p>
<i>dn</i>	Specifies the <i>dn</i> of the entry to delete.
-g	<p>Specifies that the password policy request control not be sent with the bind request. By default, the new LDAP password policy request control is sent with bind requests. The <code>ldapdelete</code> tool can parse and display information from the response control if it is returned by a server; that is, the tool will print an appropriate error or warning message when a server sends the password policy response control with the appropriate value. The criticality of the request control is set to <code>false</code> to ensure that all LDAPv3 servers that do not understand the control can ignore it. To suppress sending of the request control with the bind request, include -g on the command-line.</p>
-h	<p>Specifies the name of the host on which the server is running. For example:</p> <pre data-bbox="810 1796 1359 1863">-h cyclops</pre> <p>The default is <code>localhost</code>.</p>
-p	Specifies the port number that the server uses. The default is <code>389</code> . If -z is used, the

Option	Description
	default is 636.
-w	<p>Specifies the password associated with the distinguished name specified in the -D option. For example:</p> <pre>-w mypassword</pre> <p>The default is "", or anonymous. If a password is not sent on the command line and the server requires one, the command prompts for one. It is more secure not to provide a password on the command line so that it does not show up in clear text in a listing of commands.</p>

**Table 6.14. Commonly-Used Idapdelete Options**

### SSL Options.

Use the following options to specify that `ldapdelete` use LDAPS when communicating with the Directory Server or to use certificate-based authentication. These options are valid only when LDAPS has been turned on and configured for the Directory Server. For more information on certificate-based authentication and how to create a certificate database for use with LDAP clients, see the "Managing SSL" and "Managing SASL" chapters in the *Directory Server Administration Guide*.

Ensure that the Directory Server's encrypted port is set when using these options.

Option	Description
-3	Specifies that hostnames should be checked in SSL certificates.
-I	Specifies the SSL key password <i>file</i> that contains the token:password pair.
-K	Specifies the path, including the filename, of the private key database of the client. Either the absolute or relative (to the server root) path can be used. The -K option must be used when the key database has a different name than <code>key3.db</code> or when the key database is not under the same directory as the certificate database, the <code>cert8.db</code> file (the path for which is specified with the -P option).
-N	Specifies the certificate name to use for

Option	Description
	<p>certificate-based client authentication. For example:</p> <pre data-bbox="810 409 1390 472">-N Server-Cert</pre> <p>If this option is specified, then the <code>-z</code> and <code>-w</code> options are required. Also, if this option is specified, then the <code>-D</code> and <code>-w</code> options must not be specified, or certificate-based authentication will not occur, and the bind operation will use the authentication credentials specified on <code>-D</code> and <code>-w</code>.</p>
-P	<p>Specifies the absolute path, including the filename, of the certificate database of the client. This option is used only with the <code>-z</code> option.</p> <p>When used on a machine where an SSL-enabled web browser is configured, the path specified on this option can be pointed to the certificate database for the web browser. For example:</p> <pre data-bbox="810 1189 1390 1252">-P /security/cert.db</pre> <p>The client security files can be stored on the Directory Server in the <code>/etc/dirsrv/slapd-<i>instance_name</i></code> directory. In this case, the <code>-P</code> option calls out a path and filename similar to the following:</p> <pre data-bbox="810 1514 1390 1615">-P /etc/dirsrv/slapd-<i>instance_name</i>/client-cert.db</pre>
-Q	<p>Specifies the token and certificate name, which is separated by a semicolon (;) for PKCS11.</p>
-W	<p>Specifies the password for the certificate database identified on the <code>-P</code> option. For example:</p> <pre data-bbox="810 1906 1390 1968">-W serverpassword</pre>

Option	Description
-z	Specifies that SSL is to be used for the delete request.
-zz	Specifies the Start TLS request. Use this option to make a cleartext connection into a secure one. If the server does not support Start TLS, the command does not need to be aborted; it will continue in plain text.
-zzz	Enforces the Start TLS request. The server must respond that the request was successful. If the server does not support Start TLS, such as Start TLS is not enabled or the certificate information is incorrect, the command is aborted immediately.

**Table 6.15. Idapdelete SSL Options**

### SASL Options.

SASL mechanisms can be used to authenticate a user, using the `-o` the required SASL information.

To learn which SASL mechanisms are supported, search the root DSE. See the `-b` option in [Table 6.3, “Commonly-Used Idapsearch Options”](#).

Option	Description
-o	<p>Specifies SASL options. The format is <code>-o saslOption=value</code>. <i>saslOption</i> can have one of six values:</p> <ul style="list-style-type: none"> <li>• mech</li> <li>• authid</li> <li>• authzid</li> <li>• secProp</li> <li>• realm</li> <li>• flags</li> </ul> <p>The expected values depend on the supported mechanism. The <code>-o</code> can be used multiple times to pass all of the required SASL</p>

Option	Description
	<p>information for the mechanism. For example:</p> <pre>-o "mech=DIGEST-MD5" -o "authzid=test_user" -o "authid=test_user"</pre>

Table 6.16. SASL Options

See [SASL Options](#) for information on how to use SASL options with `ldapdelete`.

### Additional `ldapdelete` Options.

Option	Description
-c	Specifies that the utility must run in continuous operation mode. Errors are reported, but the utility continues with deletions. The default is to quit after reporting an error.
-f	<p>Specifies the file containing the distinguished names of entries to be deleted. For example:</p> <pre>-f modify_statements</pre> <p>Omit this option to supply the distinguished name of the entry to be deleted directly to the command-line.</p>
-H	Lists all available <code>ldapdelete</code> options.
-M	Manages smart referrals. This causes the server not to return the smart referral contained on the entry but, instead, to delete the actual entry containing the smart referral. For more information about smart referrals, see the "Configuring Directory Databases" chapter in the <i>Directory Server Administration Guide</i> .
-n	Specifies that the entries are not actually to be deleted, but that <code>ldapdelete</code> is to show what it would do with the specified input.
-o	Specifies the maximum number of referral hops to follow. For example:

Option	Description
	<p>-O 2</p> <p>There is no maximum number of referral hops.</p>
-R	Specifies that referrals are not to be followed automatically. By default, the server follows referrals.
-v	Specifies that the utility is to run in verbose mode.
-V	<p>Specifies the LDAP version number to be used on the operation. For example:</p> <p>-V 2</p> <p>LDAPv3 is the default. An LDAPv3 operation cannot be performed against a Directory Server that only supports LDAPv2.</p>
-Y	Specifies the proxy DN to use for the delete operation. This argument is provided for testing purposes. For more information about proxied authorization, see the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i> .

**Table 6.17. Additional Idapdelete Options**

## 7. Idappasswd

Use `ldappasswd` to set or change user passwords in Directory Server.

- [Syntax](#)
- [Idappasswd-specific Options](#)
- [General Idappasswd Options](#)
- [Examples](#)

### Syntax.

`ldappasswd [ options ] [ user ]`

`user` is the authentication identity, typically a DN. If not specified, the distinguished name specified by the `-D` option (bind name) is used.

### Idappasswd-specific Options.

Option	Description
<code>-A</code>	Specifies that the command should prompt for the user's existing password.
<code>-a</code>	Specifies the user's existing password. For example:  <code>-a old_password</code>
<code>-S</code>	Specifies that the command should prompt for a new password for the user.
<code>-s</code>	Specifies a new password for the user. For example:  <code>-S new_password</code>
<code>-T</code>	Specifies a file from which to read the new password. For example:  <code>-T new_password.txt</code>
<code>-t</code>	Specifies a file from which to read the user's existing password. For example:  <code>-t old_password.txt</code>
<code>-w</code>	Specifies the password associated with the distinguished name specified in the <code>-D</code> option. For example:  <code>-w mypassword</code>

**Table 6.18. Idappasswd-specific Options**

### General Idappasswd Options.

**NOTE**

The `ldappasswd` utility requires confidentiality. If the messages are not encrypted with SSL, TLS, or an appropriate SASL mechanism, the server will not perform the request.

Option	Description
-3	Specifies that hostnames should be checked in SSL certificates.
-D	<p>Specifies the distinguished name with which to authenticate to the server. This value must be a DN recognized by the Directory Server, and it must also have the authority to delete the entries. For example:</p> <pre data-bbox="810 943 1353 1003">-D "uid=bjensen, dc=example,dc=com"</pre> <p>The <code>-D</code> option cannot be used with the <code>-N</code> option.</p> <p>For more information on access control, see the "Managing Access Control" chapter in the <i>Directory Server Administration Guide</i>.</p>
-g	<p>Specifies that the password policy request control not be sent with the bind request. By default, the new LDAP password policy request control is sent with bind requests.</p> <p>The <code>ldappasswd</code> tool can parse and display information from the response control if it is returned by a server; that is, the tool will print an appropriate error or warning message when a server sends the password policy response control with the appropriate value.</p> <p>The criticality of the request control is set to <code>false</code> to ensure that all LDAPv3 servers that do not understand the control can ignore it. To suppress sending of the request control with the bind request, include <code>-g</code> on the command-line.</p>
-h	Specifies the name of the host on which the

Option	Description
	<p>server is running. For example:</p> <pre data-bbox="810 369 1390 434">-h cyclops</pre> <p>The default is <code>localhost</code>.</p>
-I	<p>Specifies the SSL key password <i>file</i> that contains the token:password pair.</p>
-K	<p>Specifies the path, including the filename, of the private key database of the client. This can be the absolute or relative (to the server root) path.</p> <p>The <code>-K</code> option must be used when the key database is not called <code>key3.db</code> or when the key database is not in the same directory as the certificate database (that is, the <code>cert8.db</code> file, the path for which is specified with the <code>-P</code> option).</p>
-N	<p>Specifies the certificate name to use for certificate-based client authentication. For example:</p> <pre data-bbox="810 1198 1390 1263">-N Server-Cert</pre> <p>If this option is specified, then the <code>-Z</code> and <code>-w</code> options are required.</p> <p>If this option is specified, then the <code>-D</code> and <code>-w</code> options must not be specified, or certificate-based authentication will not occur, and the bind operation will use the authentication credentials specified by <code>-D</code> and <code>-w</code>.</p>
-P	<p>Specifies the absolute path, including the filename, of the certificate database of the client. This option is used only with the <code>-Z</code> option.</p> <p>When used on a machine where an SSL-enabled web browser is configured, the path specified on this option can be that of the certificate database for the browser. For</p>

Option	Description
	<p>example:</p> <pre data-bbox="810 398 1390 461">-P /security/cert.db</pre> <p>The client security files can also be stored on the Directory Server in the <code>/etc/dirsrv/slapd-<i>instance_name</i></code> directory. In this case, the <code>-P</code> option would call out a path and filename similar to the following:</p> <pre data-bbox="810 763 1390 853">-P /etc/dirsrv/slapd-<i>instance_name</i>/client-cert.db</pre>
-p	Specifies the port number that the server uses. The default is 389. If <code>-z</code> is used, the default is 636.
-Q	Specifies the token and certificate name, which is separated by a semicolon (;) for PKCS11.
-W	Specifies the password for the certificate database identified on the <code>-P</code> option. For example: <pre data-bbox="810 1279 1390 1341">-W serverpassword</pre>
-w	Specifies the password associated with the distinguished name that is specified in the <code>-D</code> option. For example: <pre data-bbox="810 1541 1390 1603">-w diner892</pre> <p>The default is "", or anonymous.</p> <p>If a password is not sent on the command line and the server requires one, the command prompts for one. It is more secure not to provide a password on the command-line so that it does not show up in clear text in a listing of commands.</p>
-z	Specifies that SSL is to be used for the

Option	Description
	search request.
-ZZ	Specifies the Start TLS request. Use this option to make a cleartext connection into a secure one. If the server does not support Start TLS, the command does not need to be aborted; it will continue in cleartext.
-ZZZ	Enforces the Start TLS request. The server must respond that the request was successful. If the server does not support Start TLS, such as Start TLS is not enabled or the certificate information is incorrect, the command is aborted immediately.

**Table 6.19. General ldappasswd Options**

### Examples.

The following examples provide show how to perform various tasks using the `ldappasswd` command.

The Directory Manager changes the password of the user

`uid=tuser1,ou=People,dc=example,dc=com` to `new_password` over SSL.

```
ldappasswd -Z -h myhost -P /etc/dirsrv/slapd-instance_name/cert8.db -D
"cn=Directory Manager"
-w dmpassword -s new_password "uid=tuser1,ou=People,dc=example,dc=com"
```

### Example 6.1. Directory Manager Changing a User's Password Over SSL

The Directory Manager generates the password of the user

`uid=tuser2,ou=People,dc=example,dc=com` over SSL.

```
ldappasswd -Z -h myhost -P /etc/dirsrv/slapd-instance_name/cert8.db -D
"cn=Directory Manager"
-w dmpassword "uid=tuser2,ou=People,dc=example,dc=com"
```

### Example 6.2. Directory Manager Generating a User's Password

**NOTE**

For more information on newly-generated passwords, see the "Managing the Password Policy" section of the *Directory Server Administration Guide*.

A user, `tuser3`, changes the password from `old_newpassword` to `new_password` over SSL.

```
ldappasswd -Z -h myhost -P /etc/dirsrv/slaped-instance_name/cert8.db -D
"uid=tuser3,pu=People,dc=example,dc=com"
-w old_password -a old_password -s new_password
```

**Example 6.3. User Changing His Own Password**

A user, `tuser4`, authenticates with the user certificate and changes the password to `new_password` over SSL.

```
ldappasswd -Z -h myhost -P /etc/dirsrv/slaped-instance_name/cert8.db -W
dbpassword -N "uid=tuser4"
-K /etc/dirsrv/slaped-instance_name/key3.db -s new_password
```

**Example 6.4. User Authenticating With a User Certificate and Changing His Password**

A user, `tuser5`, authenticates with DIGEST-MD5 and changes the password to `new_password`.

```
ldappasswd -h myhost -o "mech=DIGEST-MD5" -o
"authid=dn:uid=tuser5,ou=People,dc=example,dc=com"
-w old_password -s new_password
```

**Example 6.5. User Authenticating with DIGEST\_MD5 and Changing His Password**

A user, who has already authenticated by Kerberos, prompts for the new password. This is not performed over SSL.

```
ldappasswd -h myhost -o "mech=GSSAPI" -S
```

## Example 6.6. User Already Authenticating by Kerberos Prompts for a New Password

### 8. Idif

`ldif` automatically formats LDIF files and creates base-64 encoded attribute values. Base-64 encoding makes it possible to represent binary data, such as a JPEG image, in LDIF. Base-64 encoded data is represented using a double colon (`::`) symbol. For example:

```
jpegPhoto::encoded data
```

In addition to binary data, other values that must be base-64 encoded can be identified with other symbols, including the following:

- Any value that begins with a space.
- Any value that begins with a single colon (`:`).
- Any value that contains non-ASCII data, including newlines.

The `ldif` command-line utility will take any input and format it with the correct line continuation and appropriate attribute information. The `ldif` utility also senses whether the input requires base-64 encoding.

- [Syntax](#)
- [Options](#)


#### Syntax.

The `ldif` command has the following format:

```
ldif [ -b ] [ attrtypes ] [ optional_options ]
```

#### Options.

Option	Description
<code>-b</code>	Specifies that the <code>ldif</code> utility should interpret the entire input as a single binary value. If <code>-b</code>

Option	Description
	<p>is not present, each line is considered to be a separate input value.</p> <p>As an alternative to the <code>-b</code> option, use the <code>:&lt;</code> URL specifier notation. For example:</p> <pre data-bbox="810 510 1390 573">jpegphoto:&lt; file:///tmp/myphoto.jpg</pre> <p>Although the official notation requires three <code>///</code>, the use of one <code>/</code> is accepted.</p> <div data-bbox="810 698 1390 1144" style="background-color: #333; color: white; padding: 10px;"> <p> <b>NOTE</b></p> <p>The <code>:&lt;</code> URL specifier notation only works if LDIF statement is version 1 or later, meaning <code>version: 1</code> is inserted in the IDIF file. Otherwise, the file URL is appended as the attribute value rather than the contents of the file.</p> </div>

**Table 6.20. Idif Options**

## 9. dbscan

The `dbscan` tool analyzes and extracts information from a Directory Server database file. See [Section 4, “Database Files”](#) for more information on database files.

Database files use the `.db2`, `.db3`, and `.db4` extensions in their filename, depending on the version of Directory Server.

- [Syntax](#)
- [Options](#)

### Syntax.

```
dbscan -f filename [ options ]
```

**Options.**

Option	Parameter	Description
-f	<i>filename</i>	Specifies the name of the database file, the contents of which are to be analyzed and extracted. This option is required.
-R		Dump the database as raw data.
-t	<i>size</i>	Specifies the entry truncate size (in bytes).

**Table 6.21. Common Options****NOTE**

The options listed in *Table 6.22, “Entry File Options”* are meaningful only when the database file is `id2entry.db4`.

Option	Parameter	Description
-K	<i>entry_id</i>	Specifies the entry to ID to look up.

**Table 6.22. Entry File Options****NOTE**

The index file options, listed in *Table 6.23, “Index File Options”*, are meaningful only when the database file is the secondary index file.

Option	Parameter	Description
-k	<i>key</i>	Specifies the key to look up in the secondary index file.
-l	<i>size</i>	Sets the maximum length of the dumped ID list. The valid range is from 40 to 1048576

Option	Parameter	Description
		bytes. The default value is 4096.
-G	<i>n</i>	Sets only to display those index entries with ID lists exceeding the specified length.
-n		Sets only to display the length of the ID list.
-r		Sets to display the contents of the ID list.
-s		Gives the summary of index counts.

**Table 6.23. Index File Options**

### Examples.

The following are command-line examples of different situations using `dbscan` to examine the Directory Server databases.

```
dbscan -f /var/lib/dirsrv/slaped-instance_name/db/userRoot/id2entry.db4
```

### Example 6.7. Dumping the Entry File

```
dbscan -f /var/lib/dirsrv/slaped-instance_name/db/userRoot/cn.db4
```

### Example 6.8. Displaying the Index Keys in cn.db4

```
dbscan -r -f /var/lib/dirsrv/slaped-instance_name/db/userRoot/mail.db4
```

### Example 6.9. Displaying the Index Keys and the Count of Entries with the Key in mail.db4

```
dbscan -r -G 20 -f /var/lib/DIRSRV/slapd-instance_name/db/userRoot/sn.db4
```

### Example 6.10. Displaying the Index Keys and the All IDs with More Than 20 IDs in sn.db4

```
dbscan -s -f /var/lib/DIRSRV/slapd-instance_name/db/userRoot/objectclass.db4
```

### Example 6.11. Displaying the Summary of objectclass.db4

```
dbscan -r -f  
/var/lib/DIRSRV/slapd-instance_name/db/userRoot/vlv#bymccoupeoledcpeoledccom.db4
```

### Example 6.12. Displaying VLV Index File Contents

```
dbscan -f  
/var/lib/DIRSRV/slapd-instance_name/changelogdb/c1a2fc02-1d11b2-8018afa7-fdce000_424c8a00f0
```

### Example 6.13. Displaying the Changelog File Contents

```
dbscan -R -f /var/lib/DIRSRV/slapd-instance_name/db/userRoot/uid.db4
```

### Example 6.14. Dumping the Index File uid.db4 with Raw Mode

In this example, the common name key is `=hr managers`, and the equals sign (=) means the key is an equality index.

```
dbscan -k "=hr managers" -r -f  
/var/lib/DIRSRV/slapd-instance_name/db/userRoot/cn.db4 =hr%20managers 7
```

### Example 6.15. Displaying the entryID with the Common Name Key "=hr managers"

```
dbscan -K 7 -f id2entry.db4 id 7 dn: cn=HR
Managers,ou=groups,dc=example,dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: HR Manager
ou: groups
description: People who can manage HR entries
creatorsName: cn=directory manager
modifiersName: cn=directory manager
createTimestamp: 20050408230424Z
modifyTimestamp: 20050408230424Z
nsUniqueId: 8b465f73-1dd211b2-807fd340-d7f40000 parentid: 3
entryid: 7
entrydn: cn=hr managers,ou=groups,dc=example,dc=com
```

### Example 6.16. Displaying an Entry with the entry ID of 7



# Command-Line Scripts

This chapter provides information on the scripts for managing Red Hat Directory Server, such as backing-up and restoring the database. Scripts are a shortcut way of executing the `ns-slapd` interface commands that are documented in [Appendix A, Using the ns-slapd Command-Line Utilities](#).

## 1. Finding and Executing Command-Line Scripts

Most scripts are located in the `/usr/lib/DIRSRV/slapd-instance_name` directory, though a few are located in the `/usr/bin` directory. The exact locations are listed in [Section 2, “Command-Line Scripts Quick Reference”](#).

When scripts request either a directory name or a filename, always provide the absolute path. The scripts assume the `dse.ldif` file is located in the `/etc/DIRSRV/slapd-instance_name` directory.

## 2. Command-Line Scripts Quick Reference

The following shell and Perl scripts are located in the `/usr/lib/DIRSRV/slapd-instance_name` directory.

Shell Script	Description
<code>bak2db</code>	Restores the database from the most recent archived backup.
<code>db2bak</code>	Creates a backup of the current database contents.
<code>db2ldif</code>	Exports the contents of the database to LDIF.
<code>db2index</code>	Reindexes the database index files.
<code>dbverify</code>	Checks backend database files.
<code>ldif2db</code>	Imports LDIF files to the database. Runs the <code>ns-slapd</code> command-line utility with the <code>ldif2db</code> keyword.
<code>ldif2ldap</code>	Performs an import operation over LDAP to the Directory Server.
<code>monitor</code>	Retrieves performance monitoring information using the <code>ldapsearch</code> command-line utility.
<code>restart-slapd</code>	Restarts Directory Server.
<code>restoreconfig</code>	Restores by default the most recently saved Administration Server configuration to <code>NetscapeRoot</code> partition.
<code>saveconfig</code>	Saves Administration Server configuration stored in the <code>NetscapeRoot</code> database to the

Shell Script	Description
	<code>/var/lib/dirsrv/slapd-<i>instance_name</i>/bak</code> directory.
<code>start-slapd</code>	Starts Directory Server.
<code>stop-slapd</code>	Stops Directory Server.
<code>suffix2instance</code>	Maps a suffix to a backend name.
<code>verify-db.pl</code>	Checks backend database files.
<code>vlvindex</code>	Creates and generates virtual list view (VLV) indexes.

**Table 7.1. Shell Scripts in `/usr/lib/dirsrv/slapd-instance_name`**

Perl Script	Description
<code>bak2db.pl</code>	Restores the database from the most recent archived backup.
<code>db2bak.pl</code>	Creates a backup of the current database contents.
<code>db2index.pl</code>	Creates and regenerates indexes.
<code>db2ldif.pl</code>	Exports the contents of the database to LDIF.
<code>ldif2db.pl</code>	Imports LDIF files to a database and runs the <code>ns-slapd</code> command-line utility with the <code>ldif2db</code> keyword.
<code>ns-accountstatus.pl</code>	Provides account status information to establish whether an entry or group of entries is locked.
<code>ns-activate.pl</code>	Activates an entry or a group of entries by unlocking them.
<code>ns-inactivate.pl</code>	Deactivates an entry or a group of entries.
<code>ns-newpwpolicy.pl</code>	Adds relevant entries required for the fine-grained (user- and subtree-level) password policy.
<code>verify-db.pl</code>	Checks backend database files.

**Table 7.2. Perl Scripts in `/usr/lib/dirsrv/slapd-instance_name`**

Script Name	Description	Perl or Shell Script
<code>cl-dump</code>	Dumps and decodes the changelog.	Shell

Script Name	Description	Perl or Shell Script
cl-dump.pl	Dumps and decodes the changelog.	Perl
logconv.pl	Analyzes the access logs of a Directory Server to extract usage statistics and count the occurrences of significant events.	Perl
pwdhash	Prints the encrypted form of a password using one of the server's encryption algorithms. If a user cannot log in, use this script to compare the user's password to the password stored in the directory.	Shell
repl-monitor	Provides in-progress status of replication.	Shell
repl-monitor.pl	Provides in-progress status of replication.	Perl

**Table 7.3. Scripts in /usr/bin**

### 3. Shell Scripts

This section covers the following scripts:

- [Section 3.1, “bak2db \(Restores a Database from Backup\)”](#)
- [Section 3.2, “cl-dump \(Dumps and Decodes the Changelog\)”](#)
- [Section 3.3, “dbverify \(Checks for Corrupt Databases\)”](#)
- [Section 3.4, “db2bak \(Creates a Backup of a Database\)”](#)
- [Section 3.5, “db2ldif \(Exports Database Contents to LDIF\)”](#)
- [Section 3.6, “db2index \(Reindexes Database Index Files\)”](#)
- [Section 3.7, “ldif2db \(Import\)”](#)
- [Section 3.8, “ldif2ldap \(Performs Import Operation over LDAP\)”](#)
- [Section 3.10, “monitor \(Retrieves Monitoring Information\)”](#)

- [Section 3.9, “pwdhash \(Prints Encrypted Passwords\)”](#)
- [Section 3.11, “repl-monitor \(Monitors Replication Status\)”](#)
- [Section 3.12, “restart-slapd \(Restarts the Directory Server\)”](#)
- [Section 3.13, “restoreconfig \(Restores Administration Server Configuration\)”](#)
- [Section 3.14, “saveconfig \(Saves Administration Server Configuration\)”](#)
- [Section 3.15, “start-slapd \(Starts the Directory Server\)”](#)
- [Section 3.16, “stop-slapd \(Stops the Directory Server\)”](#)
- [Section 3.17, “suffix2instance \(Maps a Suffix to a Backend Name\)”](#)
- [Section 3.18, “vlvindex \(Creates Virtual List View Indexes\)”](#)

Some of the shell scripts can be executed while the server is running. For others, the server must be stopped. The description of each script below indicates whether the server must be stopped or if it can continue to run while executing the script.

When a shell script has a Perl equivalent, there is a cross-reference to the section describing the equivalent Perl script.

### 3.1. bak2db (Restores a Database from Backup)

Restores the database from the most recent archived backup. To run this script, the server must be stopped.

#### Syntax.

```
bak2db backupDirectory [ -n backend ]
```

#### Options.

Option	Description
<i>backupDirectory</i>	Gives the backup directory path.
<i>-n backendInstance</i>	<i>Optional.</i> Specifies the backend name, such as <code>userRoot</code> , which is being restored. This option is only used for filesystem replica initialization or to restore a single database; it is not necessary to use the <code>n</code> option to restore the entire directory.

**Table 7.4. bak2db Options**

For information on the equivalent Perl script, see [Section 4.1, “bak2db.pl \(Restores a Database from Backup\)”](#). For more information on restoring databases, see the "Populating Directory Databases" chapter in the *Red Hat Directory Server Administration Guide*. For more information on using filesystem replica initialization, see the "Managing Replication" chapter in the *Red Hat Directory Server Administration Guide*.

### 3.2. cl-dump (Dumps and Decodes the Changelog)

Troubleshoots replication-related problems. `cl-dump` is a shell script wrapper of `cl-dump.pl` to set the appropriate library path.

#### Syntax.

```
cl-dump [ -h host ] [ -p port ] [ -D bindDn ] -w bindPassword | -P bindCert [ -r replicaRoots ]
[ -o outputFile ] [ -c ] [ -v ]
```

```
cl-dump -i changelogFile [ -o outputFile ] [ -c ]
```

#### Options.

Without the `-i` option, the script must be run when the Directory Server is running from a location from which the server's changelog directory is accessible.

Option	Description
<code>-c</code>	Dumps and interprets CSN only. This option can be used with or without the <code>-i</code> option.
<code>-D bindDn</code>	Specifies the Directory Server's bind DN. Defaults to <code>cn=Directory Manager</code> if the option is omitted.
<code>-h host</code>	Specifies the Directory Server's host. This defaults to the server where the script is running.
<code>-i changelogFile</code>	Specifies the path to the changelog file. If there is a changelog file and if certain changes in that file are base-64 encoded, use this option to decode that changelog.
<code>-o outputFile</code>	Specifies the path, including the filename, for the final result. Defaults to STDOUT if omitted.
<code>-p port</code>	Specifies the Directory Server's port. The default value is 389.
<code>-P bindCert</code>	Specifies the path, including the filename, to the certificate database that contains the certificate used for binding.
<code>-r replicaRoots</code>	Specifies the replica-roots whose changelog

Option	Description
	to dump. When specifying multiple roots, use commas to separate roots. If the option is omitted, all the replica roots will be dumped.
-v	Prints the version of the script.
-w <i>bindPassword</i>	Specifies the password for the bind DN.

**Table 7.5. cl-dump Options**

For information on the equivalent Perl script, see [Section 4.2, “cl-dump.pl \(Dumps and Decodes the Changelog\)”](#).

### 3.3. dbverify (Checks for Corrupt Databases)

Verifies the backend database files. `dbverify` is a shell script wrapper of `verify-db.pl` to set the appropriate library path.

#### Syntax.

```
dbverify [ -a /path/to/database_directory ]
```

#### Options.

Option	Description
-a <i>path</i>	Gives the path to the database directory. If this option is not passed with the <code>verify-db.pl</code> command, then it uses the default database directory, <code>/var/lib/dirsrv/slapd-<i>instance_name</i>/db</code> .

**Table 7.6. dbverify Options**

For information on the equivalent Perl script, see [Section 4.13, “verify-db.pl \(Check for Corrupt Databases\)”](#).

### 3.4. db2bak (Creates a Backup of a Database)

Creates a backup of the current database contents. This script can be executed while the server is still running.

#### Syntax.

db2bak [ *backupDirectory* ]

For information on the equivalent Perl script, see [Section 4.3, “db2bak.pl \(Creates a Backup of a Database\)”](#).

### 3.5. db2ldif (Exports Database Contents to LDIF)

Exports the contents of the database to LDIF. This script can be executed while the server is still running, except with the `-r` option. To export the replication state information, shutdown the server first, then run `db2ldif` with `-r`.

For information on the equivalent Perl script, see [Section 4.5, “db2ldif.pl \(Exports Database Contents to LDIF\)”](#).

For the shell scripts, the script runs the `ns-slapd` command-line utility with the `db2ldif` keyword. Ellipses (...) indicate that multiple occurrences are allowed.

#### Syntax.

```
db2ldif [ -n backendInstance | -s includeSuffix ] [ -X excludeSuffix ] [ -r ] [ -C ] [ -u ] [ -U ]
[ -m ] [ M ] [ -a outputFile ] [ -1 ] [ -N ] [ -E ]
```

#### Options.

Either the `-n` or the `-s` option must be specified. By default, the output LDIF will be stored in one file. To specify the use of several files, use the option `-m`.

Option	Description
-1	Deletes, for reasons of backward compatibility, the first line of the LDIF file which gives the version of the LDIF standard.
-a <i>outputFile</i>	Gives the name of the output LDIF file.
-C	Uses only the main database file.
-E	Decrypts encrypted data during export. This option is used only if database encryption is enabled.
-m	Sets minimal base-64 encoding.
-M	Use of several files for storing the output LDIF, with each instance stored in <i>instance filename</i> (where <i>filename</i> is the filename specified for <code>-a</code> option).
-n <i>backendInstance</i>	Gives the instance to be exported.
-N	Specifies that the entry IDs are not to be included in the LDIF output. The entry IDs are necessary only if the <code>db2ldif</code> output is to be

Option	Description
	used as input to <code>db2index</code> .
<code>-r</code>	Exports a replica.
<code>-s suffix_name</code>	Names the suffixes to be included or the subtrees to be included if <code>-n</code> has been used.
<code>-u</code>	Requests that the unique ID is not exported.
<code>-U</code>	Requests that the output LDIF is not folded.
<code>-x suffix_name</code>	Names the suffixes to be excluded.

**Table 7.7. db2ldif Options**

### 3.6. db2index (Reindexes Database Index Files)

Reindexes the database index files. Ellipses indicate that multiple occurrences are allowed.

For information on the equivalent Perl script, see [Section 4.4, “db2index.pl \(Creates and Generates Indexes\)”](#).

#### Syntax.

```
db2index [[ -n backendInstance ] | [ -s includeSuffix ] ] [ -t  
[attributeName{:indextypes(:mathingrules)}] ] [ -T vlvAttribute ]
```

#### Usage.

Here are a few sample commands:

- Reindex all the database index files:

```
db2index
```

- Reindex `cn` and `givenname` in the database instance `userRoot`:

```
db2index -n userRoot -t cn -t givenname
```

- Reindex `cn` in the database where the root suffix is `dc=example,dc=com`:

```
db2index -s "dc=example,dc=com" -t cn
```

**Options.**

Option	Description
<code>-n backendInstance</code>	Gives the name of the instance to be reindexed.
<code>-s includeSuffix</code>	Gives suffixes to be included or the subtrees to be included if <code>-n</code> has been used.
<code>-t attributeName{:indextypes(:matchingrules)}</code>	Names of the attributes to be reindexed. Optionally, this can include the index type (e.g, <code>pres</code> , <code>sub</code> , <code>approx</code> ) and a matching rule OID.
<code>-T vlvAttributeName</code>	Gives the names of the VLV attributes to be reindexed. The name is the VLV index object's common name in <code>cn=config</code> .

**Table 7.8. db2index Options****3.7. Idif2db (Import)**

Runs the `ns-slapd` command-line utility with the `ldif2db` keyword. To run this script, the server must be stopped. Ellipses indicate that multiple occurrences are allowed.

For information on the equivalent Perl script, see [Section 4.6, “ldif2db.pl \(Import\)”](#).

**NOTE**

`ldif2db` supports LDIF version 1 specifications. An attribute can also be loaded using the `:<` URL specifier notation; for example:

```
jpegphoto:< file:///tmp/myphoto.jpg
```

Although the official notation requires three `///`, the use of one `/` is accepted. For further information on the LDIF format, see the “Managing Directory Entries” chapter in the *Red Hat Directory Server Administration Guide*.

**Syntax.**

```
ldif2db [ -n backendInstance | { -S includeSuffix } ... ] [ -X excludeSuffix ] [ { -i ldifFile } ] [ -O ] [ -g string ] [ -G namespaceId ] [ -E ]
```

**Options.**

Option	Description
-c	Merges chunk size.
-E	Encrypts data during import. This option is used only if database encryption is enabled.
-g <i>string</i>	<p>Generates a unique ID. Type <code>none</code> for no unique ID to be generated and <code>deterministic</code> for the generated unique ID to be name-based.</p> <p>By default, a time-based unique ID is generated. When using the <code>deterministic</code> generation to have a name-based unique ID, it is also possible to specify the namespace for the server to use, as follows:</p> <pre data-bbox="810 864 1359 927">-g deterministic namespace_id</pre> <p><i>namespace_id</i> is a string of characters in the format  00-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx.</p> <p>Use this option to import the same LDIF file into two different Directory Servers and the contents of both directories should have the same set of unique IDs. If unique IDs already exist in the LDIF file being imported, then the existing IDs are imported to the server, regardless of the options specified.</p>
-G <i>namespaceId</i>	Generates a namespace ID as a name-based unique ID. This is the same as specifying the <code>-g deterministic</code> option.
-i <i>ldifFile</i>	Gives the names of the input LDIF files. When multiple files are imported, they are imported in the order they are specified on the command line.
-n <i>backendInstance</i>	Gives the instance to be imported. Ensure that the specified instance corresponds to the suffix contained by the LDIF file; otherwise, the data contained by the database is deleted, and the import fails.
-O	Requests that only the core database is created, without attribute indexes.
-s <i>includeSuffix</i>	Gives the suffixes to be included or to specify the subtrees to be included if <code>-n</code> has been

Option	Description
	used.
<code>-x excludeSuffix</code>	Gives the suffixes to be excluded.

**Table 7.9. Idif2db Options**

### 3.8. Idif2ldap (Performs Import Operation over LDAP)

Performs an import operation over LDAP to the Directory Server. To run this script, the server must be running.

#### Syntax.

```
ldif2ldap -D rootdn -W password -f filename
```

#### Options.

Option	Description
<code>-D rootdn</code>	Gives a user DN with <code>root</code> permissions, such as Directory Manager.
<code>-f filename</code>	Gives the name of the file to be imported. When importing multiple files, the files are imported in the order they are specified on the command line.
<code>-w password</code>	Gives the password associated with the user DN.

**Table 7.10. Idif2ldap Options**

### 3.9. pwdhash (Prints Encrypted Passwords)

Prints the encrypted form of a password using one of the server's encryption algorithms. If a user cannot log in, use this script to compare the user's password to the password stored in the directory.

#### Syntax.

```
pwdhash -D config_directory [ -H ] [ [ -s scheme ] ] [ [ -c comparepwd ] ] [ password ]
```

#### Options.

Option	Description
-D <i>config_directory</i>	Gives the full path to the configuration directory.
-c <i>password</i>	Gives the hashed password string to which to compare the user's password.
-s <i>scheme</i>	Gives the scheme to hash the given password.
-H	Shows the help.

**Table 7.11. pwddhash Options**

For more information on the different storage schemes, such as SSHA, SHA, CRYPT, and CLEAR, see the *Directory Server Administration Guide*.

### 3.10. monitor (Retrieves Monitoring Information)

Retrieves performance monitoring information using the `ldapsearch` command-line utility.

#### Syntax.

```
monitor
```

#### monitor Options.

There are no options for this script.

For more information on the `ldapsearch` command-line utility, see [Section 8, “Idif”](#).

### 3.11. repl-monitor (Monitors Replication Status)

Shows in-progress status of replication. `repl-monitor` is a shell script wrapper of `repl-monitor.pl` to set the appropriate library path.

For more information on the Perl script, see [Section 4.12, “repl-monitor.pl \(Monitors Replication Status\)”](#).

#### Syntax.

```
repl-monitor -h host -p port -f configFile [-u refreshUrl] [-t refreshInterval] [-r] [-v]
```

#### Options.

Option	Description
-h <i>host</i>	Specifies the initial replication supplier's host.

Option	Description
	The default value is the current hostname.
<code>-f configFile</code>	Specifies the absolute path to the configuration file, which defines the connection parameters used to connect to LDAP servers to get replication information. For more information about the configuration file, see <a href="#">Configuration File Format</a> .
<code>-p port</code>	Specifies the initial replication supplier's port. The default value is 389.
<code>-r</code>	If specified, causes the routine to be entered without printing the HTML header information. This is suitable when making multiple calls to this routine — such as specifying multiple, different, unrelated supplier servers — and expecting a single HTML output.
<code>-t refreshInterval</code>	Specifies the refresh interval in seconds. The default value is 300 seconds. This option must be used with the <code>-u</code> option.
<code>-u refreshUrl</code>	Specifies the refresh URL. The output HTML file may invoke a CGI program periodically. If this CGI program in turn calls this script, the effect is that the output HTML file would automatically refresh itself. This is useful for continuous monitoring. See also the <code>-t</code> option. The script has been integrated into Red Hat Administration Express, so that the replication status can be monitored through the gateway.
<code>-v</code>	Prints the version of this script.

**Table 7.12. repl-monitor Options**

### Configuration File Format.

The configuration file defines the following:

- The connection parameters for connecting to the LDAP servers to get replication information; specifying this information is mandatory.
- The server alias for more readable server names; specifying this information is optional.

- The color thresholds for time lags; specifying this information is optional.

The format for the configuration file is shown below.

```
[connection]
host:port:binddn:bindpwd:bindcert
host:port:binddn:bindpwd:bindcert
...

[alias]
alias = host:port
alias = host:port
...

[color]
lowmark = color
lowmark = color
```

The connection section defines how this tool may connect to each LDAP server in the replication topology to get the replication-agreement information. The default *binddn* is *cn=Directory Manager*. Simple bind will be used unless *bindcert* is specified with the path of a certificate database.

A server may have a dedicated or shared entry in the connection section. The script will find out the most matched entry for a given server. For example, if all the LDAP servers except *host1* share the same *binddn* and *bindpassword*, the connection section will need to contain just two entries:

```
[connection]
*:*:binddn:bindpassword:
host1*:binddn1:bindpassword1:
```

In the optional alias section, use aliases such as *Supplier1*, *Supplier2*, and *Hub1*, to identify the servers in the replication topology. If used, the output shows these aliases, instead of *http(s)://hostname:port*.

The CSN time lags between suppliers and consumers can be displayed in different colors based on their range. The default color set is green for 0-5 minutes lag, yellow for 5-60 minutes lag, and pink for a lag of 60 minutes or more.

The connection parameters for all the servers in a replication topology must be specified within one configuration file. One configuration file, however, may contain information for multiple replication topologies.

Because of the connection parameters, the replication monitoring tool does not need to perform DES decryption of the credentials stored in the Directory Server. Each line in this file could either be a comment started with the # character or a connection entry of the format:

```
host:port:binddn:bindpwd:bindcert
```

- *host*, *port*, and *binddn* can be replaced with relevant values or \*, or omitted altogether. If *host* is null or \*, the entry may apply to any host that does not have a dedicated entry in the file. If *port* is null or \*, the port will default to the port stored in the current replication agreement. If *binddn* is null or \*, it defaults to `cn=Directory Manager`.
- *bindcert* can be replaced with the full path to the certificate database, null, or \*. If *bindcert* is omitted or replaced with \*, the connection will be a simple bind.

For example, the configuration file may appear as follows:

```
#Configuration File for Monitoring Replication Via Admin Express
[connection]
*:*:*:mypassword

[alias]
M1 = host1.example.com:10011
C1 = host4.example.com:10021
C2 = host2.example.com:10022

[color]
0 = #ccffcc
5 = #FFFFCC
60 = #FFCCCC
```

A *shadow port* can be set in the replication monitor configuration file. For example:

```
host:port=shadowport:binddn:bindpwd:bindcert
```

When the replication monitor finds a replication agreement that uses the specified port, it will use the shadow port to connect to retrieve statistics.

### 3.12. restart-slapd (Restarts the Directory Server)

Restarts the Directory Server.

#### Syntax.

```
restart-slapd
```

#### Options.

There are no options for this script.

### Exit Status.

Exit Code	Description
0	Server restarted successfully.
1	Server could not be started.
2	Server restarted successfully but was already stopped.
3	Server could not be stopped.

**Table 7.13. restart-slapd Exit Status Codes**

### 3.13. restoreconfig (Restores Administration Server Configuration)

Restores, by default, the most recently saved Administration Server configuration information to the `NetscapeRoot` partition under the `/etc/dirsrv/slapd-instance_name/` directory.

To restore the Administration Server configuration, do the following:

1. Stop the Directory Server.
2. Run the `restoreconfig` script.
3. Restart the Directory Server.
4. Restart the Administration Server for the changes to be taken into account.

#### Syntax.

```
restoreconfig
```

#### Options.

There are no options for this script.

### 3.14. saveconfig (Saves Administration Server Configuration)

Saves Administration Server configuration information to `/var/lib/dirsrv/slapd-instance_name/bak` directory.

This script will only run if the server is running.

#### Syntax.

saveconfig

**Options.**

There are no options for this script.

### 3.15. start-slapd (Starts the Directory Server)

Starts the Directory Server. It might be a good idea to check whether the server has been effectively started using the `ps` command because it could sometimes be that the script returned while the startup process was still on-going, resulting in a confusing message.

**Syntax.**

start-slapd

**Options.**

There are no options for this script.

**Exit Status Codes.**

Exit Code	Description
0	Server started successfully.
1	Server could not be started.
2	Server was already started.

**Table 7.14. start-slapd Exit Status Codes**

### 3.16. stop-slapd (Stops the Directory Server)

Stops the Directory Server. It might be a good idea to check whether the server has been effectively stopped using the `ps` command because it could sometimes be that the script returned while the shutdown process was still on-going, resulting in a confusing message.

**Syntax.**

stop-slapd

**Options.**

There are no options for this script.

**Exit Status.**

Exit Code	Description
0	Server stopped successfully.
1	Server could not be stopped.
2	Server was already stopped.

**Table 7.15. stop-slapd Exit Status Codes**

### 3.17. suffix2instance (Maps a Suffix to a Backend Name)

Maps a suffix to a backend name.

#### Syntax.

```
suffix2instance { -s suffix }
```

#### Options.

Option	Description
-s	Suffix to be mapped to the backend.

**Table 7.16. suffix2instance Options**

### 3.18. vlvindex (Creates Virtual List View Indexes)

To run the `vlvindex` script, the server must be stopped. The `vlvindex` script creates virtual list view (VLV) indexes, known in the Directory Server Console as browsing indexes. VLV indexes introduce flexibility in the way search results are viewed. VLV indexes can organize search results alphabetically or in reverse alphabetical order, making it easy to scroll through the list of results. VLV index configuration must already exist prior to running this script.

#### Syntax.

```
vlvindex [ -d debugLevel ] [ [ -n backendInstance ] | [ -s suffix ] ] [ -T vlvTag ]
```

#### Options.

Either the `-n` or the `-s` option must be specified.

Option	Description
-d <i>debugLevel</i>	Specifies the debug level to use during index creation. Debug levels are defined in <a href="#">Section 3.1.42, “nsslapd-errorlog-level (Error</a>

Option	Description
	<a href="#">Log Level)</a> ”
-n <i>backendInstance</i>	Gives the name of the database containing the entries to index.
-s <i>suffix</i>	Gives the name of the suffix containing the entries to index.
-T <i>vlvTag</i>	VLV index identifier to use to create VLV indexes. The Console can specify VLV index identifier for each database supporting the directory tree, as described in the <i>Directory Server Administration Guide</i> . Define additional VLV tags by creating them in LDIF and adding them to Directory Server's configuration, as described in the <i>Red Hat Directory Server Administration Guide</i> . Red Hat recommends using the DN of the entry for which to accelerate the search sorting.

**Table 7.17. vlvindex Options**

## 4. Perl Scripts

This section describes the following Perl scripts:

- [Section 4.1, “bak2db.pl \(Restores a Database from Backup\)”](#)
- [Section 4.2, “cl-dump.pl \(Dumps and Decodes the Changelog\)”](#)
- [Section 4.3, “db2bak.pl \(Creates a Backup of a Database\)”](#)
- [Section 4.4, “db2index.pl \(Creates and Generates Indexes\)”](#)
- [Section 4.5, “db2ldif.pl \(Exports Database Contents to LDIF\)”](#)
- [Section 4.6, “ldif2db.pl \(Import\)”](#)
- [Section 4.7, “logconv.pl \(Log Converter\)”](#)
- [Section 4.8, “ns-accountstatus.pl \(Establishes Account Status\)”](#)
- [Section 4.9, “ns-activate.pl \(Activates an Entry or Group of Entries\)”](#)
- [Section 4.10, “ns-inactivate.pl \(Inactivates an Entry or Group of Entries\)”](#)
- [Section 4.11, “ns-newpwpolicy.pl \(Adds Attributes for Fine-Grained Password Policy\)”](#)

- [Section 4.12, “repl-monitor.pl \(Monitors Replication Status\)”](#)
- [Section 4.13, “verify-db.pl \(Check for Corrupt Databases\)”](#)

## 4.1. bak2db.pl (Restores a Database from Backup)

Restores a database from a backup.

### Syntax.

```
bak2db.pl [ -v ] -D rootdn -w password [ -a backupDirectory ] [ -t databaseType ] [ -n backend ]
```

### Options.

The script `bak2db.pl` creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values provided for each option.

Option	Description
<code>-a backupDirectory</code>	The directory of the backup files.
<code>-D rootdn</code>	Gives the user DN with <code>root</code> permissions, such as Directory Manager. The default is the DN of the Directory Manager, which is read from the <code>nsslapd-root</code> attribute under <code>cn=config</code> .
<code>-n backendInstance</code>	Specifies the backend name, such as <code>userRoot</code> , which is being restored. This option is only used for filesystem replica initialization or to restore a single database; it is not necessary to use the <code>-n</code> option to restore the entire directory.
<code>-t databaseType</code>	The database type. Currently, the only possible database type is <code>ldbm</code> .
<code>-v</code>	Verbose mode.
<code>-w password</code>	The password associated with the user DN.

**Table 7.18. bak2db.pl Options**

## 4.2. cl-dump.pl (Dumps and Decodes the Changelog)

Troubleshoots replication-related problems.

### Syntax.

```
cl-dump.pl [ -h host ] [ -p port ] [ -D bindDn ] -w bindPassword | -P bindCert [ -r
replicaRoots ] [ -o outputFile ] [ -c ] [ -v ]
```

```
cl-dump.pl -i changelogFile [ -o outputFile ] [ -c ]
```

### Options.

Without the `-i` option, the script must be run when the Directory Server is running from a location from which the server's changelog directory is accessible.

Option	Description
<code>-c</code>	Dumps and interprets CSN only. This option can be used with or without the <code>-i</code> option.
<code>-D bindDn</code>	Specifies the Directory Server's bind DN. Defaults to <code>cn=Directory Manager</code> if the option is omitted.
<code>-h host</code>	Specifies the Directory Server's host. Defaults to the server where the script is running.
<code>-i changelogFile</code>	Specifies the path to the changelog file. If there is a changelog file and if certain changes in that file are base-64 encoded, use this option to decode that changelog.
<code>-o outputFile</code>	Specifies the path, including the filename, for the final result. Defaults to <code>STDOUT</code> if omitted.
<code>-p port</code>	Specifies the Directory Server's port. The default value is <code>389</code> .
<code>-P bindCert</code>	Specifies the path, including the filename, to the certificate database that contains the certificate used for binding.
<code>-r replicaRoots</code>	Specifies the replica-roots whose changelog to dump. When specifying multiple roots, use commas to separate roots. If the option is omitted, all the replica roots will be dumped.
<code>-v</code>	Prints the version of the script.
<code>-w bindPassword</code>	Specifies the password for the bind DN.

**Table 7.19. cl-dump.pl command options**

## 4.3. db2bak.pl (Creates a Backup of a Database)

Creates a backup of the database.

**Syntax.**

```
db2bak.pl [ -v ] -D rootdn -w password [ -a dirName ]
```

**Options.**

The script `db2bak.pl` creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values provided for each option. Currently, the only possible database type is `ldbm`.

Option	Description
<code>-a dirName</code>	The directory where the backup files will be stored. The <code>/var/lib/dirsrv/slapd-instance_name/backup</code> directory is used by default. The backup file is named according to the year-month-day-hour format (YYYY_MM_DD_hhmmss).
<code>-D rootdn</code>	The user DN with <code>root</code> permissions, such as Directory Manager. The default is the DN of the Directory Manager, which is read from the <code>nsslapd-root</code> attribute under <code>cn=config</code> .
<code>-t</code>	The database type. Currently, the only possible database type is <code>ldbm</code> .
<code>-v</code>	Verbose mode.
<code>-w password</code>	The password associated with the user DN.

**Table 7.20. db2bak.pl Options**

**4.4. db2index.pl (Creates and Generates Indexes)**

Creates and generates the new set of indexes to be maintained following the modification of indexing entries in the `cn=config` configuration file.

**Syntax.**

```
db2index.pl [ -v ] -D rootdn { -w password -j filename } [ -n backendInstance ] [ -t attributeName { :indextypes( :matchingrules ) } ] [ -T vlvAttributeName ]
```

**Options.**

The script `db2index.pl` creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values provided for each option.

Option	Description
-D <i>rootdn</i>	Gives the user DN with <code>root</code> permissions, such as Directory Manager.
-j <i>filename</i>	The name of the file containing the password.
-n <i>backendInstance</i>	Gives the instance to be indexed. If the instance is not specified, the script reindexes all instances.
-t <i>attributeName{:indextypes(:matchingrules)}</i>	Gives the name of the attribute to be indexed. If omitted, all the indexes defined for the specified instance are generated. Optionally, this can include the index type ( <code>eq</code> , <code>pres</code> , <code>sub</code> , <code>approx</code> ) and a matching rule OID.
-T <i>vlvAttributeName</i>	Gives the names of the VLV attributes to be reindexed. The name is the VLV index object's common name in <code>cn=config</code> .
-v	Verbose mode.
-w <i>password</i>	Gives the password associated with the user DN.

Table 7.21. db2index.pl Options

## 4.5. db2ldif.pl (Exports Database Contents to LDIF)

Exports the contents of the database to LDIF. This script creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values provided for each option. Ellipses indicate that multiple occurrences are allowed.

### Syntax.

```
db2ldif.pl [ -v ] -D rootdn -w password [ -n backendInstance | -s includeSuffix ] -x
excludeSuffix [ -a outputFile ] [ -N ] [ -r ] [ -C ] [ -u ] [ -U ] [ -m ] [ -o ] [ -1 ] [ M ]
```

### Options.

To run this script, the server must be running, and either the `-n` or `-s` option is required.

Option	Description
-1	Deletes, for reasons of backward compatibility, the first line of the LDIF file that gives the version of the LDIF standard.
-a <i>outputFile</i>	Gives the filename of the output LDIF file.
-C	Uses only the main database file.

Option	Description
-D <i>rootdn</i>	Gives the user DN with <code>root</code> permissions, such as Directory Manager.
-m	Sets minimal base-64 encoding.
-M	Sets the output LDIF is stored in multiple files.
-n <i>backendInstance</i>	Gives the instance to be exported.
-N	Suppresses printing sequential numbers.
-o	Sets the output LDIF to be stored in one file by default with each instance stored in <i>instance_filename</i> .
-r	Exports a replica.
-s	<i>includeSuffix</i>
-u	Requests that the unique ID is not exported.
-U	Requests that the output LDIF is not folded.
-v	Verbose mode.
-w <i>password</i>	Gives the password associated with the user DN.
-x <i>excludeSuffix</i>	Gives suffixes to be excluded.

Table 7.22. db2ldif.pl Options

## 4.6. Idif2db.pl (Import)

To run this script, the server must be running. The script creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values provided for each option. Ellipses indicate that multiple occurrences are allowed.

### Syntax.

```
ldif2db.pl [ -v ] -D rootdn -w password [ -n backendInstance | -s includeSuffix ] -x
excludeSuffix [ -O ] [ -c ] [ -g string ] [ -G namespaceId ] -i filename
```

### Options.

Option	Description
-c	Merges chunk size.
-D <i>rootdn</i>	Specifies the user DN with <code>root</code> permissions, such as Directory Manager.
-g <i>string</i>	Generates a unique ID. Type <code>none</code> for no

Option	Description
	<p>unique ID to be generated and <code>deterministic</code> for the generated unique ID to be name-based. By default, a time-based unique ID is generated.</p> <p>When using the <code>deterministic</code> generation to have a name-based unique ID, it is also possible to specify the namespace for the server to use, as follows:</p> <pre data-bbox="810 663 1390 725">-g deterministic namespaceId</pre> <p><code>namespaceId</code> is a string of characters in the format  00-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx.</p> <p>Use this option to import the same LDIF file into two different Directory Servers and the contents of both directories should have the same set of unique IDs. If unique IDs already exist in the LDIF file being imported, then the existing IDs are imported to the server, regardless of the options specified.</p>
<code>-G namespaceId</code>	Generates a namespace ID as a name-based unique ID. This is the same as specifying the <code>-g deterministic</code> option.
<code>-i filename</code>	Specifies the filename of the input LDIF files. When multiple files are imported, they are imported in the order they are specified on the command line.
<code>-n backendInstance</code>	Specifies the instance to be imported.
<code>-O</code>	Requests that only the core db is created without attribute indexes.
<code>-s includeSuffix</code>	Specifies the suffixes to be included or specifies the subtrees to be included if <code>-n</code> has been used.
<code>-v</code>	Specifies verbose mode.
<code>-w password</code>	Specifies the password associated with the user DN.
<code>-x excludeSuffix</code>	Specifies the suffixes to be excluded.

Table 7.23. `ldif2db.pl` Options

### 4.7. logconv.pl (Log Converter)

Analyzes the access logs of a Directory Server to extract usage statistics and count the occurrences of significant events. It is compatible with log formats from previous releases of Directory Server. For information on access logs, see [Chapter 5, Access Log and Connection Code Reference](#).

The tool will extract the following information from access logs:

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• Number of restarts</li><li>• Total number of connections</li><li>• Total operations requested</li><li>• Total results returned</li><li>• Results to requests ratio</li><li>• Number of searches</li><li>• Number of modifications</li><li>• Number of adds</li><li>• Number of deletes</li><li>• Number of modified RDNs</li><li>• Persistent searches</li><li>• Internal operations (with verbose logs)</li><li>• Entry operations (with verbose logs)</li><li>• Extended operations</li><li>• Abandoned requests</li><li>• Smart referrals received (verbose logs)</li><li>• VLV (virtual list view) operations</li><li>• VLV unindexed searches</li><li>• Server-side sorting operations</li><li>• SSL connections</li><li>• Performance lowering operations:</li><li>• Entire database searches</li><li>• Unindexed searches (details optional)</li></ul> | <ul style="list-style-type: none"><li>• FDs (file descriptors) taken</li><li>• FDs returned</li><li>• Highest FD taken</li><li>• Disruptions:</li><li>• Broken pipes</li><li>• Connections reset by peer</li><li>• Unavailable resources (and detail)</li><li>• Total binds and types of binds</li><li>• Most frequent occurrence lists (optional)</li><li>• Error and return codes</li><li>• Failed logins</li><li>• Connection codes</li><li>• Client IP addresses and connection codes</li><li>• Bind DNs</li><li>• Base DNs for searching</li><li>• Search filters</li><li>• Etimes (elapsed operation time)</li><li>• Longest etimes</li><li>• Nentries (number of entries in result)</li><li>• Largest Nentries</li><li>• Extended operations</li><li>• Most requested attributes</li><li>• Recommendations (optional)</li></ul> |
|---|--|

#### Table 7.24. Information Extracted from Access Logs

The `logconv.pl` tool displays two types of statistics useful for monitoring and optimizing directory usage:

- Simple counts of events such as the total number of binds and the total number of searches provide overall usage information. This is the basic information that the tool will always print.
- Lists of the most frequently occurring parameters in LDAP requests provide insight into how the directory information is being accessed. For example, lists of the top ten bind DNs, base DNs, filter strings, and attributes returned can help administrators optimize the directory for its

users. These lists are optional because they are computation intensive: specify only the command-line options required (see [Options](#)).

Some information that is extracted by the `logconv.pl` script is available only in logs from current releases of Directory Server; the corresponding values will be zero when analyzing logs from older versions. In addition, some information will only be present in the logs if verbose logging is enabled in the Directory Server. For more information, see [Section 3.1.2, “nsslapd-accesslog-level”](#).

The following issues will affect the output and performance of this tool:

- Some data extracted from logs depend on connection and operation numbers that are reset and no longer unique after a server restarts. Therefore, to obtain the most accurate counts, the logs to be analyzed should not span the restart of the Directory Server.
- Due to changes in access log format in current releases of Directory Server that affected operation numbers, the tool will be more accurate logs from current versions when processing large amounts of access logs.
- For performance reasons, it is not recommended to run more than one gigabyte of access logs through the script at any one time.

## Syntax.

```
logconv.pl [-S] [-E] [-d] [-X] [-v] [-h] [-s] [-V] [-y] [-p] [-efcibaltnxgjuh] accessLog
```

## Options.

[Table 7.25, “logconv.pl Options”](#) describes the `logconv.pl` command-line options.

Option	Description
<code>-d mgrDN</code>	Specifies the distinguished name (DN) of the Directory Manger in the logs being analyzed. This allows the tool to collect statistics for this special user. The <code>mgrDN</code> parameter should be given in double quotes ( " ") for the shell. When this parameter is omitted, <code>logconv.pl</code> will use the default manager DN of the Directory Server, "cn=Directory Manager".
<code>-E endTimestamp</code>	Specifies the end timestamp; the timestamp must follow the exact format as specified in the access log.
<code>-h</code>	Displays the usage help text that briefly describes all options.
<code>-p</code>	Lists open connection ID statistics, which

Option	Description
	indicates the FDs that are not yet closed.
<code>-s number</code>	Specifies the number of items in each of the list options below. The default is 20 when this parameter is omitted. For example, <code>-s 10 -i</code> will list the ten client machines that access the Directory Server most often. This parameter will apply to all lists that are enabled, and it will have no effect if none are displayed.
<code>-S startTimestamp</code>	Specifies the start timestamp; the timestamp must follow the exact format as specified in the access log.
<code>-v</code>	Displays the version number of the <code>logconv.pl</code> script.
<code>-V</code>	Enables verbose output. With this option, <code>logconv.pl</code> will compute and display all of the optional lists described in <a href="#">Table 7.26</a> , “ <i>logconv.pl Options to Display Occurrences</i> ”
<code>-X ipAddress</code>	Specifies the IP address of a client to exclude from the statistics. This client will not appear in lists of IP addresses (the <code>i</code> flag), and the connection codes it generates will not be tallied in the total connections (default statistic) nor in the connection code details (the <code>c</code> flag). For example, an administrator may want the server to ignore the effect of a load balancer that connects to the Directory Server at regular intervals. This option may be repeated to exclude multiple IP addresses.
<code>-y</code>	Lists connection latency details, which indicates the overall connection latency.
<code>accessLog</code>	The name of a file that contains the access log of the Directory Server. Wildcards can be used in the filename. It is also possible to specify multiple filenames. However, the statistics are computed over the set of all logs, so all logs should pertain to the same Directory Server. The tool ignores any file with the name <code>access.rotationinfo</code> .

Table 7.25. `logconv.pl` Options

Table 7.26, “logconv.pl Options to Display Occurrences” describes the options that enable the optional lists of occurrences. Specify only those required; specifying a large number of options can produce excessive output and affect execution speed. These parameters can be specified in any number and in any order, but they must all be given together as a single option on the command line, such as `-abcefg`.

The lists are always output in the order in which they appear in the following table, regardless of the order in which they are given on the command line.

Option	Description
e	Lists the most frequent error and return codes.
f	Lists the bind DNs with the most failed logins (invalid password).
c	Lists the number of occurrences for each type of connection code.
i	Lists the IP addresses and connection codes of the clients with the most connections, which detects clients that may be trying to compromise security.
b	Lists the most frequently used bind DNs.
a	Lists the most frequent base DNs when performing operations.
l	Lists the most frequently used filter strings for searches.
t	Lists the longest and most frequent <code>etimes</code> (elapsed operation time).
n	Lists the largest and most frequent <code>nentries</code> (entries per result).
x	Lists the number and OID of all extended operations.
r	Lists the names of the most requested attributes.
g	Lists the details of all abandoned operations.
j	Gives recommendations based on data collected from the log file.
u	Gives operation details about unindexed searches.

**Table 7.26. logconv.pl Options to Display Occurrences**

## 4.8. ns-accountstatus.pl (Establishes Account Status)

Provides account status information to establish whether an entry or group of entries is inactivated.

### Syntax.

```
ns-accountstatus.pl [ -D rootdn ] -w password [ -p port ] [ -h host ] -l DN
```

### Options.

Option	Description
-D <i>rootdn</i>	Specifies the Directory Server user DN with <i>root</i> permissions, such as Directory Manager.
-h <i>host</i>	Specifies the hostname of the Directory Server. The default value is the full hostname of the machine where Directory Server is installed.
-l <i>DN</i>	Specifies the entry DN or role DN whose status is required.
-p <i>port</i>	Specifies the Directory Server's port. The default value is the LDAP port of Directory Server specified at installation time.
-w <i>password</i>	Specifies the password associated with the user DN.

**Table 7.27. ns-accountstatus.pl Options**

## 4.9. ns-activate.pl (Activates an Entry or Group of Entries)

Activates an entry or group of entries.

### Syntax.

```
ns-activate.pl [ -D rootdn ] -w password [ -p port ] [ -h host ] -l DN
```

### Options.

Option	Description
-D <i>rootdn</i>	Specifies the Directory Server user DN with <i>root</i> permissions, such as Directory

Option	Description
	Manager.
-h <i>host</i>	Specifies the hostname of the Directory Server. The default value is the full hostname of the machine where Directory Server is installed.
-l <i>DN</i>	Specifies the entry DN or role DN to activate.
-p <i>port</i>	Specifies the Directory Server's port. The default value is the LDAP port of Directory Server specified at installation time.
-w <i>password</i>	Specifies the password associated with the user DN.

**Table 7.28. ns-activate.pl Options**

## 4.10. ns-inactivate.pl (Inactivates an Entry or Group of Entries)

Inactivates, and consequently locks, an entry or group of entries.

### Syntax.

```
ns-inactivate.pl [ -D rootdn ] -w password [ -p port ] [ -h host ] -l DN
```

### Options.

Option	Description
-D <i>rootdn</i>	Specifies the Directory Server user DN with <i>root</i> permissions, such as Directory Manager.
-h <i>host</i>	Specifies the hostname of the Directory Server. The default value is the full hostname of the machine where Directory Server is installed.
-l <i>DN</i>	Specifies the entry DN or role DN to deactivate.
-p <i>port</i>	Specifies the Directory Server's port. The default value is the LDAP port of Directory Server specified at installation time.
-w <i>password</i>	Specifies the password associated with the user DN.

Table 7.29. ns-inactivate.pl Options

## 4.11. ns-newpwdpolicy.pl (Adds Attributes for Fine-Grained Password Policy)

Adds entries required for implementing the user- and subtree-level password policy. For instructions on how to enable this feature, see the *Red Hat Directory Server Administration Guide*.

### Syntax.

```
ns-newpwdpolicy.pl [ -D rootdn ] { -w password | -w - | -j filename } [ -p port ] [ -h host ] -U userDN -S suffixDN
```

### Options.

Option	Description
-D <i>rootdn</i>	Specifies the Directory Server user DN with root permissions, such as Directory Manager. The default value is <code>cn=directory manager</code> .
-h <i>host</i>	Specifies the hostname of the Directory Server. The default value is <code>localhost</code> or the full hostname of the machine where Directory Server is installed.
-j <i>filename</i>	Specifies the path, including the filename, to the file that contains the password associated with the user DN.
-p <i>port</i>	Specifies the Directory Server's port. The default value is <code>389</code> or the LDAP port of Directory Server specified at installation time.
-S <i>suffixDN</i>	Specifies the DN of the suffix entry that needs to be updated with subtree-level password policy attributes.
-U <i>userDN</i>	Specifies the DN of the user entry that needs to be updated with user-level password policy attributes.
-w <i>password</i>	Specifies the password associated with the user DN.
-w -	Prompts for the password associated with the user DN.

Table 7.30. ns-newpwdpolicy.pl Options

## 4.12. repl-monitor.pl (Monitors Replication Status)

Shows in-progress status of replication.

### Syntax.

```
repl-monitor.pl -h host -p port -f configFile [ -u refreshUrl ] [ -t refreshInterval ] [ -r ]
[ -v ]
```

### Options.

Option	Description
-h <i>host</i>	Specifies the initial replication supplier's host. The default value is the current hostname.
-f <i>configFile</i>	Specifies the absolute path to the configuration file, which defines the connection parameters used to connect to LDAP servers to get replication information. For more information about the configuration file, see <a href="#">Configuration File Format</a> .
-p <i>port</i>	Specifies the initial replication supplier's port. The default value is 389.
-r	If specified, causes the routine to be entered without printing the HTML header information. This is suitable when making multiple calls to this routine — such as specifying multiple, different, unrelated supplier servers — and expecting a single HTML output.
-t <i>refreshInterval</i>	Specifies the refresh interval in seconds. The default value is 300 seconds. This option must be used with the -u option.
-u <i>refreshUrl</i>	Specifies the refresh URL. The output HTML file may invoke a CGI program periodically. If this CGI program in turn calls this script, the effect is that the output HTML file would automatically refresh itself. This is useful for continuous monitoring. See also the -t option. The script has been integrated into Red Hat Administration Express, so that the replication status can be monitored through

Option	Description
	the gateway.
-v	Prints the version of this script.

**Table 7.31. repl-monitor.pl Options**

### Configuration File Format.

The configuration file defines the following:

- The connection parameters for connecting to the LDAP servers to get replication information; specifying this information is mandatory.
- The server alias for more readable server names; specifying this information is optional.
- The color thresholds for time lags; specifying this information is optional.

The format for the configuration file is shown below.

```
[connection]
host:port:binddn:bindpwd:bindcert
host:port:binddn:bindpwd:bindcert
...

[alias]
alias = host:port
alias = host:port
...

[color]
lowmark = color
lowmark = color
```

The connection section defines how this tool may connect to each LDAP server in the replication topology to get the replication-agreement information. The default *binddn* is *cn=Directory Manager*. Simple bind will be used unless *bindcert* is specified with the path of a certificate database.

A server may have a dedicated or shared entry in the connection section. The script will find out the most matched entry for a given server. For example, if all the LDAP servers except *host1* share the same *binddn* and *bindpassword*, the connection section will need to contain just two entries:

```
[connection]
*:*:binddn:bindpassword:
```

```
host1:*:binddn1:bindpassword1:
```

In the optional alias section, use aliases such as `Supplier1`, `Supplier2`, and `Hub1`, to identify the servers in the replication topology. If used, the output shows these aliases, instead of `http(s)://hostname:port`.

The CSN time lags between suppliers and consumers can be displayed in different colors based on their range. The default color set is green for 0-5 minutes lag, yellow for 5-60 minutes lag, and pink for a lag of 60 minutes or more.

The connection parameters for all the servers in a replication topology must be specified within one configuration file. One configuration file, however, may contain information for multiple replication topologies.

Because of the connection parameters, the replication monitoring tool does not need to perform DES decryption of the credentials stored in the Directory Server. Each line in this file could either be a comment started with the `#` character or a connection entry of the following format:

```
host:port:binddn:bindpwd:bindcert
```

- *host*, *port*, and *binddn* can be replaced with relevant values or `*`, or omitted altogether. If *host* is null or `*`, the entry may apply to any host that does not have a dedicated entry in the file. If *port* is null or `*`, the port will default to the port stored in the current replication agreement. If *binddn* is null or `*`, it defaults to `cn=Directory Manager`.
- *bindcert* can be replaced with the full path to the certificate database, null, or `*`. If *bindcert* is omitted or replaced with `*`, the connection will be a simple bind.

For example, the configuration file may appear as follows:

```
#Configuration File for Monitoring Replication Via Admin Express
[connection]
*:*:*:mypassword

[alias]
M1 = host1.example.com:10011
C1 = host4.example.com:10021
C2 = host2.example.com:10022

[color]
0 = #ccffcc
5 = #ffffcc
60 = #ffcccc
```

A *shadow port* can be set in the replication monitor configuration file. For example:

```
host:port=shadowport:binddn:bindpwd:bindcert
```

When the replication monitor finds a replication agreement that uses the specified port, it will use the shadow port to connect to retrieve statistics.

### 4.13. verify-db.pl (Check for Corrupt Databases)

Verifies the backend database files.

#### Syntax.

```
verify-db.pl [ -a /path/to/database_directory ]
```

#### Options.

Option	Description
<i>-a path</i>	Gives the path to the database directory. If this option is not passed with the <code>verify-db.pl</code> command, then it uses the default database directory, <code>/var/lib/dirsrv/slapd-<i>instance_name</i>/db</code> .

**Table 7.32. verify-db.pl Options**

---

# Appendix A. Using the ns-slapd Command-Line Utilities

[Chapter 7, Command-Line Scripts](#) discussed the scripts for performing routine administration tasks on the Red Hat Directory Server (Directory Server). This appendix discusses the `ns-slapd` command-line utilities that can be used to perform the same tasks.

The `ns-slapd` command-line utilities all perform server administration tasks, and, while it can be argued that they allow a greater degree of flexibility for users, Red Hat recommends using the command-line scripts described in [Chapter 7, Command-Line Scripts](#)

## 1. Overview of ns-slapd

`ns-slapd` is used to start the Directory Server process, to build a directory database from an LDIF file, or to convert an existing database to an LDIF file. For more information on starting and stopping the Directory Server, importing from LDIF using the command-line, and exporting to LDIF using the command-line, refer to the "Populating Directory Databases" chapter in the *Red Hat Directory Server Administration Guide*.

## 2. Finding and Executing the ns-slapd Command-Line Utilities

The `ns-slapd` command-line utilities are stored in `/usr/lib/DIRSRV/slaped-instance_name`



### NOTE

In order to execute the command-line utilities, set the library paths set in the command-line scripts.

## 3. Utilities for Exporting Databases: db2ldif

Exports the contents of the database to LDIF.

### Syntax.

```
ns-slapd db2ldif -D configDir -a outputFile [ -d debugLevel ] [ -n backendInstance ] [ -r ] [ -s includeSuffix ] [ -x excludeSuffix ] [ -N ] [ -u ] [ -U ] [ -m ] [ -M ] [ -E ]
```

With this command, enter the full path to the configuration directory, `/etc/DIRSRV/slaped-instance_name`. Either the `-n` or the `-s` option must be specified.

**Options.**

Option	Description
-a <i>outputFile</i>	Defines the output file in which the server saves the exported LDIF. This file is stored by default in the directory where the command-line utility resides.
-d <i>debugLevel</i>	Specifies the debug level to use during the <code>db2ldif</code> runtime. For further information, refer to <a href="#">Section 3.1.42, “nsslapd-errorlog-level (Error Log Level)”</a> .
-D <i>configDir</i>	Specifies the location of the server configuration directory that contains the configuration information for the export process. This must be the full path to the configuration directory, <code>/etc/dirsrv/slapd-<i>instance_name</i></code> .
-E	Decrypts an encrypted database during export. This option is used only if database encryption is enabled.
-m	Sets minimal base-64 encoding.
-M	Uses several files to store the output LDIF, with each instance stored in <i>instance filename</i> , where <i>filename</i> is the filename specified in option <code>-a</code> .
-n <i>backendInstance</i>	Specifies the name of the backend instance to be exported.
-N	Specifies that entry IDs are not to be included in the LDIF output. The entry IDs are necessary only if the <code>db2ldif</code> output is to be used as input to <code>db2index</code> .
-r	Exports replication state information. The server <i>must</i> be shut down before exporting using this option.
-s <i>includeSuffix</i>	Specifies the suffix or suffixes to include in the export. There can be multiple <code>-s</code> arguments.
-u	Specifies that the uniqueID will not be included in the LDIF output. By default, the server includes the uniqueID for all entries with a uniqueID in the exported LDIF file. Only use this option to use the exported LDIF to initialize a 4.x consumer server; otherwise,

Option	Description
	this option does not cause the server to create a uniqueID for entries but simply takes what already exists in the database.
-U	Outputs the contents of the database without wrapping lines.
-x <i>excludeSuffix</i>	Specifies a suffix or suffixes to exclude in the export. There can be multiple -x arguments. If neither -s or -x is not specified, the server exports all suffixes within the database. When using both -x and -s options with the same suffix, the -x operation takes precedence. Exclusion always takes precedence over inclusion. If the LDIF file will be imported into the configuration directory, do not exclude o=NetscapeRoot.

**Table A.1. db2ldif Options**

## 4. Utilities for Restoring and Backing up Databases: Idif2db

Imports LDIF files to the database.

### Syntax.

```
ns-slapd ldif2db -D configDir -i ldifFile [ -d debugLevel ] [ -g string ] [ -n backendInstance ] [ -O ] [ -s includeSuffix ] [ -x excludeSuffix ] [ -E ]
```

Enter the full path to the server configuration directory (*configdir*). *ldifFile* is the name of the file containing the LDIF to be imported. There is an example LDIF file under the `/var/lib/dirsrv/slapd-instance_name/ldif` directory. Either the -n or the -s option must be specified.

### Options.

Option	Description
-d <i>debugLevel</i>	Specifies the debug level to use during runtime. For further information, refer to <a href="#">Section 3.1.42, “nsslapd-errorlog-level (Error Log Level)”</a> .
-D <i>configDir</i>	Specifies the location of the server

Option	Description
	<p>configuration directory that contains the configuration information for the import process. This must be the full path to the configuration directory,  <code>/etc/dirsrv/slapd-<i>instance_name</i></code>.</p>
-E	<p>Decrypts an encrypted database during export. This option is used only if database encryption is enabled.</p>
-g <i>string</i>	<p>Generates a unique ID. Type <code>none</code> for no unique ID to be generated and <code>deterministic</code> for the generated unique ID to be name-based. By default, a time-based unique ID is generated.</p> <p>When using the <code>deterministic</code> generation to have a name-based unique ID, it is also possible to specify the namespace for the server to use, as follows:</p> <pre data-bbox="807 1048 1390 1115">-g deterministic namespaceId</pre> <p><i>namespaceId</i> is a string of characters in the format  <code>00-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx</code>.</p> <p>Use this option to import the same LDIF file into two different Directory Servers and the contents of both directories should have the same set of unique IDs. If unique IDs already exist in the LDIF file being imported, then the existing IDs are imported to the server, regardless of the options specified.</p>
-i <i>ldifFile</i>	<p>Specifies the LDIF file to be imported. This option is required. There can be multiple <code>-i</code> arguments to import more than one LDIF file at a time. When importing multiple files, the server imports the LDIF files in the order they are specified on the command line.</p>
-n <i>backendInstance</i>	<p>Specifies the name of the backend to be imported.</p>
-O	<p>Specifies that no attribute indexes are created for the imported database. If this option is specified and the indexes need to be restored</p>

Option	Description
	later, the indexes have to be recreated by hand. See the <i>Directory Server Administration Guide</i> for further information.
<code>-s includeSuffix</code>	Specifies the suffix or suffixes within the LDIF file to import.
<code>-x excludeSuffix</code>	Specifies suffixes within the LDIF file to exclude during the import. There can be multiple <code>-x</code> arguments. This option can selectively import portions of the LDIF file. If both <code>-x</code> and <code>-s</code> are used with the same suffix, <code>-x</code> takes precedence. Exclusion always takes precedence over inclusion. If <code>-x</code> or <code>-s</code> are not specified, then all available suffixes will be imported from the LDIF file. To import the LDIF file into the configuration directory, do not exclude <code>o=NetscapeRoot</code> .

Table A.2. Idif2db Options

## 5. Utilities for Restoring and Backing up Databases: archive2db

Restores database from the archives.

### Syntax.

```
ns-slapd archive2db -D configDir -a archiveDir
```

### Options.

Option	Description
<code>-D configDir</code>	Specifies the location of the server configuration directory that contains the configuration information for the index creation process. This must be the full path to the configuration directory, <code>/etc/dirsrv/slapd-instance_name</code> .
<code>-a archiveDir</code>	Specifies the archive directory.

Table A.3. archive2db Options

## 6. Utilities for Restoring and Backing up Databases: db2archive

Backs up all databases to the archives.

### Syntax.

```
ns-slapd db2archive -D configDir -a archiveDir
```

### Options.

Option	Description
-D <i>configDir</i>	Specifies the location of the server configuration directory that contains the configuration information for the index creation process. This must be the full path to the configuration directory, <i>/etc/dirsrv/slapd-instance_name</i> .
-a <i>archiveDir</i>	Specifies the archive directory.

Table A.4. db2archive Options

## 7. Utilities for Creating and Regenerating Indexes: db2index

Creates and regenerates indexes.

### Syntax.

```
ns-slapd db2index -D configDir [ -d debugLevel ] -n backendName -t  
attributeName [ :indexTypes{ :matchingRules } ] [ -T vlvTag ]
```

### Options.

Option	Description
-d <i>debugLevel</i>	Specifies the debug level to use during index creation. For further information, refer to <a href="#">Section 3.1.42, “nsslapd-errorlog-level (Error Log Level)”</a> .
-D <i>configDir</i>	Specifies the location of the server configuration directory that contains the

Option	Description
	configuration information for the index creation process. This must be the full path to the configuration directory, <i>/etc/dirsrv/slapd-instance_name</i> .
<b>-n</b> <i>backendName</i>	Specifies the name of the backend containing the entries to index.
<b>-t</b> <i>attributeName[:indextypes(:matchingrules)]</i>	Specifies the attribute to be indexed as well as the types of indexes to create and matching rules to apply, if any. If the matching rule is specified, an index type must be specified. This option cannot be used with <b>-T</b> . <i>indexTypes</i> specifies a comma-separated list of indexes to be created for the attributes. <i>matchingRules</i> is an optional, comma-separated list of the OIDs for the languages in which the attribute will be indexed. This option is used to create international indexes. For information on supported locales and collation order OIDs, see the Appendix "Internationalization" in the <i>Directory Server Administration Guide</i> .
<b>-T</b> <i>vlvTag</i>	Specifies the VLV tag to use to create VLV indexes. The Console can be used to specify VLV tags for each database supporting the directory tree, as described in the <i>Directory Server Administration Guide</i> . Additional VLV tags can be defined by creating them in LDIF and adding them in the Directory Server configuration. This options cannot be used with <b>-t</b> .

Table A.5. db2index Options



---

## Appendix B. Revision History

Revision History

Revision 8.0.0-2                      Thursday, January 10, 2008      Ella DeonLackey<>

Technical edits to chapters 3, 4, 6, 7, and appendix, and final review.

Revision 8.0.0-1                      December 2007                      JoshuaOakes<>

Some XML clean-up and review and technical edits.

Revision 8.0.0-0                      Wednesday, August 8, 2007      DavidO'Brien<>

Initial setup.



---

# Glossary

## A

access control instruction	See <a href="#">ACI</a> .
ACI	An instruction that grants or denies permissions to entries in the directory. See Also <a href="#">access control instruction</a> .
access control list	See <a href="#">ACL</a> .
ACL	The mechanism for controlling access to your directory. See Also <a href="#">access control list</a> .
access rights	In the context of access control, specify the level of access granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, selfwrite, proxy and all.
account inactivation	Disables a user account, group of accounts, or an entire domain so that all authentication attempts are automatically rejected.
All IDs Threshold	<i>Replaced with the ID list scan limit in Directory Server version 7.1.</i> A size limit which is globally applied to every index key managed by the server. When the size of an individual ID list reaches this limit, the server replaces that ID list with an All IDs token. See Also <a href="#">ID list scan limit</a> .
All IDs token	A mechanism which causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the server to behave as if no index was available for the search request.
anonymous access	When granted, allows anyone to access directory information without providing credentials, and regardless of the conditions of the bind.
approximate index	Allows for efficient approximate or "sounds-like" searches.
attribute	Holds descriptive information about an entry. Attributes have a label and a value. Each attribute also follows a standard syntax for the type of information that can be stored as the attribute

	value.
attribute list	A list of required and optional attributes for a given entry type or object class.
authenticating directory server	In pass-through authentication (PTA), the authenticating Directory Server is the Directory Server that contains the authentication credentials of the requesting client. The PTA-enabled host sends PTA requests it receives from clients to the host.
authentication	<p>(1) Process of proving the identity of the client user to the Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator.</p> <p>(2) Allows a <i>client</i> to make sure they are connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when it is not.</p>
authentication certificate	Digital file that is not transferable and not forgeable and is issued by a third party. Authentication certificates are sent from server to client or client to server in order to verify and authenticate the other party.

## B

base DN	Base distinguished name. A search operation is performed on the base DN, the DN of the entry and all entries below it in the directory tree.
base distinguished name	See <i>base DN</i> .
bind DN	Distinguished name used to authenticate to Directory Server when performing an operation.
bind distinguished name	See <i>bind DN</i> .
bind rule	In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.
branch entry	An entry that represents the top of a subtree in the directory.
browser	Software, such as Mozilla Firefox, used to request and view World Wide Web material stored as HTML files. The browser

---

uses the HTTP protocol to communicate with the host server.

browsing index                      Speeds up the display of entries in the Directory Server Console. Browsing indexes can be created on any branch point in the directory tree to improve display performance. See Also [virtual list view index](#) .

## C

CA                                      See [Certificate Authority](#).

cascading replication              In a cascading replication scenario, one server, often called the hub supplier, acts both as a consumer and a supplier for a particular replica. It holds a read-only replica and maintains a changelog. It receives updates from the supplier server that holds the master copy of the data and in turn supplies those updates to the consumer.

certificate                            A collection of data that associates the public keys of a network user with their DN in the directory. The certificate is stored in the directory as user object attributes.

Certificate Authority              Company or organization that sells and issues authentication certificates. You may purchase an authentication certificate from a Certification Authority that you trust. Also known as a [CA](#).

CGI                                    Common Gateway Interface. An interface for external programs to communicate with the HTTP server. Programs written to use CGI are called CGI programs or CGI scripts and can be written in many of the common programming languages. CGI programs handle forms or perform output parsing that is not done by the server itself.

chaining                            A method for relaying requests to another server. Results for the request are collected, compiled, and then returned to the client.

changelog                            A changelog is a record that describes the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on replica servers or on other masters, in the case of multi-master replication.

character type                      Distinguishes alphabetic characters from numeric or other characters and the mapping of upper-case to lower-case letters.

ciphertext	Encrypted information that cannot be read by anyone without the proper key to decrypt the information.
class definition	Specifies the information needed to create an instance of a particular object and determines how the object works in relation to other objects in the directory.
class of service	See <a href="#">CoS</a> .
classic CoS	A classic CoS identifies the template entry by both its DN and the value of one of the target entry's attributes.
client	See <a href="#">LDAP client</a> .
code page	An internal table used by a locale in the context of the internationalization plug-in that the operating system uses to relate keyboard keys to character font screen displays.
collation order	Provides language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.
consumer	Server containing replicated directory trees or subtrees from a supplier server.
consumer server	In the context of replication, a server that holds a replica that is copied from a different server is called a consumer for that replica.
CoS	A method for sharing attributes between entries in a way that is invisible to applications.
CoS definition entry	Identifies the type of CoS you are using. It is stored as an LDAP subentry below the branch it affects.
CoS template entry	Contains a list of the shared attribute values. See Also <a href="#">template entry</a> .

## D

daemon	A background process on a Unix machine that is responsible for a particular system task. Daemon processes do not need human intervention to continue functioning.
DAP	Directory Access Protocol. The ISO X.500 standard protocol that provides client access to the directory.

---

data master	The server that is the master source of a particular piece of data.
database link	An implementation of chaining. The database link behaves like a database but has no persistent storage. Instead, it points to data stored remotely.
default index	One of a set of default indexes created per database instance. Default indexes can be modified, although care should be taken before removing them, as certain plug-ins may depend on them.
definition entry	See <a href="#">CoS definition entry</a> .
Directory Access Protocol	See <a href="#">DAP</a> .
directory tree	The logical representation of the information stored in the directory. It mirrors the tree model used by most filesystems, with the tree's root point appearing at the top of the hierarchy. Also known as <a href="#">DIT</a> .
Directory Manager	The privileged database administrator, comparable to the root user in UNIX. Access control does not apply to the Directory Manager.
Directory Server Gateway	A collection of CGI forms that allows a browser to perform LDAP client functions, such as querying and accessing a Directory Server, from a web browser. Also called <a href="#">DSGW</a> .
directory service	A database application designed to manage descriptive, attribute-based information about people and resources within an organization.
distinguished name	String representation of an entry's name and location in an LDAP directory.
DIT	See <a href="#">directory tree</a> .
DN	See <a href="#">distinguished name</a> .
DM	See <a href="#">Directory Manager</a> .
DNS	Domain Name System. The system used by machines on a network to associate standard IP addresses (such as 198.93.93.10) with hostnames (such as <code>www.example.com</code> ). Machines normally get the IP address for a hostname from a DNS server, or they look it up in tables maintained on their systems.
DNS alias	A DNS alias is a hostname that the DNS server knows points

to a different host#specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.yourdomain.domain` might point to a real machine called `realthing.yourdomain.domain` where the server currently exists.

DSGW

See [Directory Server Gateway](#).

## E

**entry** A group of lines in the LDIF file that contains information about an object.

**entry distribution** Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

**entry ID list** Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that may match the client application's search request.

**equality index** Allows you to search efficiently for entries containing a specific attribute value.

## F

**file extension** The section of a filename after the period or dot (.) that typically defines the type of file (for example, .GIF and .HTML). In the filename `index.html` the file extension is `html`.

**file type** The format of a given file. For example, graphics files are often saved in GIF format, while a text file is usually saved as ASCII text format. File types are usually identified by the file extension (for example, .GIF or .HTML).

**filter** A constraint applied to a directory query that restricts the information returned.

**filtered role** Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

## G

---

gateway	See <a href="#">Directory Server Gateway</a> .
general access	When granted, indicates that all authenticated users can access directory information.
GSS-API	Generic Security Services. The generic access protocol that is the native way for UNIX-based systems to access and authenticate Kerberos services; also supports session encryption.

## H

hostname	A name for a machine in the form machine.domain.dom, which is translated into an IP address. For example, <code>www.example.com</code> is the machine <code>www</code> in the subdomain <code>example</code> and <code>com</code> domain.
HTML	Hypertext Markup Language. The formatting language used for documents on the World Wide Web. HTML files are plain text files with formatting codes that tell browsers such as the Mozilla Firefox how to display text, position graphics, and form items and to display links to other pages.
HTTP	Hypertext Transfer Protocol. The method for exchanging information between HTTP servers and clients.
HTTPD	An abbreviation for the HTTP daemon or service, a program that serves information using the HTTP protocol. The daemon or service is often called an <code>httpd</code> .
HTTPS	A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.
hub	In the context of replication, a server that holds a replica that is copied from a different server, and, in turn, replicates it to a third server. See Also <a href="#">cascading replication</a> .

## I

ID list scan limit	A size limit which is globally applied to any indexed search operation. When the size of an individual ID list reaches this limit, the server replaces that ID list with an all IDs token.
index key	Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS	An indirect CoS identifies the template entry using the value of one of the target entry's attributes.
international index	Speeds up searches for information in international directories.
International Standards Organization IP address	See <a href="#">ISO</a> .  <i>Also Internet Protocol address.</i> A set of numbers, separated by dots, that specifies the actual location of a machine on the Internet (for example, 198.93.93.10).
ISO	International Standards Organization.

## K

knowledge reference	Pointers to directory information stored in different databases.
---------------------	--

## L

LDAP	Lightweight Directory Access Protocol. Directory service protocol designed to run over TCP/IP and across multiple platforms.
LDAPv3	Version 3 of the LDAP protocol, upon which Directory Server bases its schema format.
LDAP client	Software used to request and view LDAP entries from an LDAP Directory Server. See Also <a href="#">browser</a> .
LDAP Data Interchange Format LDAP URL	See <a href="#">LDAP Data Interchange Format</a> .  Provides the means of locating Directory Servers using DNS and then completing the query via LDAP. A sample LDAP URL is <code>ldap://ldap.example.com</code> .
LDBM database	A high-performance, disk-based database consisting of a set of large files that contain all of the data assigned to it. The primary data store in Directory Server.
LDIF	LDAP Data Interchange Format. Format used to represent Directory Server entries in text form.
leaf entry	An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

---

Access Protocol	See <a href="#">LDAP</a> .
locale	Identifies the collation order, character type, monetary format and time / date format used to present data for users of a specific region, culture, and/or custom. This includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.
<b>M</b>	
managed object	A standard value which the SNMP agent can access and send to the NMS. Each managed object is identified with an official name and a numeric identifier expressed in dot-notation.
managed role	Allows creation of an explicit enumerated list of members.
management information base mapping tree	See <a href="#">MIB</a> .
master	See <a href="#">supplier</a> .
master agent	See <a href="#">SNMP master agent</a> .
matching rule	Provides guidelines for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.
MD5	A message digest algorithm by RSA Data Security, Inc., which can be used to produce a short digest of data that is unique with high probability and is mathematically extremely hard to produce; a piece of data that will produce the same message digest.
MD5 signature	A message digest produced by the MD5 algorithm.
MIB	Management Information Base. All data, or any portion thereof, associated with the SNMP network. We can think of the MIB as a database which contains the definitions of all SNMP managed objects. The MIB has a tree-like hierarchy, where the top level contains the most general information about the network and lower levels deal with specific, separate network areas.
MIB namespace	Management Information Base namespace. The means for directory data to be named and referenced. Also called the

*directory tree.*

monetary format	Specifies the monetary symbol used by specific region, whether the symbol goes before or after its value, and how monetary units are represented.
multi-master replication	An advanced replication scenario in which two servers each hold a copy of the same read-write replica. Each server maintains a changelog for the replica. Modifications made on one server are automatically replicated to the other server. In case of conflict, a time stamp is used to determine which server holds the most recent version.
multiplexor	The server containing the database link that communicates with the remote server.

## N

n + 1 directory problem	The problem of managing multiple instances of the same information in different directories, resulting in increased hardware and personnel costs.
name collisions	Multiple entries with the same distinguished name.
nested role	Allows the creation of roles that contain other roles.
network management application	Network Management Station component that graphically displays information about SNMP managed devices, such as which device is up or down and which and how many error messages were received.
network management station NIS	See <i>NMS</i> .  Network Information Service. A system of programs and data files that Unix machines use to collect, collate, and share specific information about machines, users, filesystems, and network parameters throughout a network of computers.
NMS	Powerful workstation with one or more network management applications installed. Also <i>network management station</i> .
ns-slapd	Red Hat's LDAP Directory Server daemon or service that is responsible for all actions of the Directory Server. See Also <i>slapd</i> .

## O

---

object class	Defines an entry type in the directory by defining which attributes are contained in the entry.
object identifier	A string, usually of decimal numbers, that uniquely identifies a schema element, such as an object class or an attribute, in an object-oriented system. Object identifiers are assigned by ANSI, IETF or similar organizations. See Also <a href="#">OID</a> .
OID	See <a href="#">object identifier</a> .
operational attribute	Contains information used internally by the directory to keep track of modifications and subtree properties. Operational attributes are not returned in response to a search unless explicitly requested.

## P

parent access	When granted, indicates that users have access to entries below their own in the directory tree if the bind DN is the parent of the targeted entry.
pass-through authentication	See <a href="#">PTA</a> .
pass-through subtree	In pass-through authentication, the <a href="#">PTA directory server</a> will pass through bind requests to the <a href="#">authenticating directory server</a> from all clients whose DN is contained in this subtree.
password file	A file on Unix machines that stores Unix user login names, passwords, and user ID numbers. It is also known as <code>/etc/passwd</code> because of where it is kept.
password policy	A set of rules that governs how passwords are used in a given directory.
permission	In the context of access control, permission states whether access to the directory information is granted or denied and the level of access that is granted or denied. See Also <a href="#">access rights</a> .
PDU	Encoded messages which form the basis of data exchanges between SNMP devices. Also <a href="#">protocol data unit</a> .
pointer CoS	A pointer CoS identifies the template entry using the template DN only.
presence index	Allows searches for entries that contain a specific indexed attribute.

## Glossary

---

protocol	A set of rules that describes how devices on a network exchange information.
protocol data unit	See <a href="#">PDU</a> .
proxy authentication	A special form of authentication where the user requesting access to the directory does not bind with its own DN but with a proxy DN.
proxy DN	Used with proxied authorization. The proxy DN is the DN of an entry that has access permissions to the target on which the client-application is attempting to perform an operation.
PTA	Mechanism by which one Directory Server consults another to check bind credentials. Also <a href="#">pass-through authentication</a> .
PTA directory server	In pass-through authentication ( <a href="#">PTA</a> ), the PTA Directory Server is the server that sends (passes through) bind requests it receives to the <a href="#">authenticating directory server</a> .
PTA LDAP URL	In pass-through authentication, the URL that defines the <a href="#">authenticating directory server</a> , pass-through subtree(s), and optional parameters.

## R

RAM	Random access memory. The physical semiconductor-based memory in a computer. Information stored in RAM is lost when the computer is shut down.
rc.local	A file on Unix machines that describes programs that are run when the machine starts. It is also called <code>/etc/rc.local</code> because of its location.
RDN	The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name. Also <a href="#">relative distinguished name</a> .
referential integrity	Mechanism that ensures that relationships between related entries are maintained within the directory.
referral	(1) When a server receives a search or update request from an LDAP client that it cannot process, it usually sends back to the client a pointer to the LDAP sever that can process the request.  (2) In the context of replication, when a read-only replica receives an update request, it forwards it to the server that holds the corresponding read-write replica. This forwarding

---

	process is called a referral.
read-only replica	A replica that refers all update operations to read-write replicas. A server can hold any number of read-only replicas.
read-write replica	A replica that contains a master copy of directory information and can be updated. A server can hold any number of read-write replicas.
relative distinguished name	See <a href="#">RDN</a> .
replica	A database that participates in replication.
replica-initiated replication	Replication configuration where replica servers, either hub or consumer servers, pull directory data from supplier servers. This method is available only for legacy replication.
replication	Act of copying directory trees or subtrees from supplier servers to replica servers.
replication agreement	Set of configuration parameters that are stored on the supplier server and identify the databases to replicate, the replica servers to which the data is pushed, the times during which replication can occur, the DN and credentials used by the supplier to bind to the consumer, and how the connection is secured.
RFC	Request for Comments. Procedures or standards documents submitted to the Internet community. People can send comments on the technologies before they become accepted standards.
role	An entry grouping mechanism. Each role has <i>members</i> , which are the entries that possess the role.
role-based attributes	Attributes that appear on an entry because it possesses a particular role within an associated CoS template.
root	The most privileged user available on Unix machines. The root user has complete access privileges to all files on the machine.
root suffix	The parent of one or more sub suffixes. A directory tree can contain more than one root suffix.

## S

SASL	An authentication framework for clients as they attempt to bind to a directory. Also <a href="#">Simple Authentication and Security Layer</a> .
------	---

schema	Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results.
schema checking	Ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default, and users will receive an error if they try to save an entry that does not conform to the schema.
Secure Sockets Layer	See <a href="#">SSL</a> .
self access	When granted, indicates that users have access to their own entries if the bind DN matches the targeted entry.
Server Console	Java-based application that allows you to perform administrative management of your Directory Server from a GUI.
server daemon	The server daemon is a process that, once running, listens for and accepts requests from clients.
server service	A process on Windows that, once running, listens for and accepts requests from clients. It is the SMB server on Windows NT.
Server Selector	Interface that allows you select and configure servers using a browser.
service	A background process on a Windows machine that is responsible for a particular system task. Service processes do not need human intervention to continue functioning.
SIE	Server Instance Entry. The ID assigned to an instance of Directory Server during installation.
Simple Authentication and Security Layer	See <a href="#">SASL</a> .
Simple Network Management Protocol	See <a href="#">SNMP</a> .
single-master replication	The most basic replication scenario in which multiple servers, up to four, each hold a copy of the same read-write replicas to replica servers. In a single-master replication scenario, the supplier server maintains a changelog.
SIR	See <a href="#">supplier-initiated replication</a> .
slapd	LDAP Directory Server daemon or service that is responsible for most functions of a directory except replication.

---

	See Also <a href="#">ns-slapd</a> .
SNMP	Used to monitor and manage application processes running on the servers by exchanging data about network activity. Also <a href="#">Simple Network Management Protocol</a> .
SNMP master agent	Software that exchanges information between the various subagents and the NMS.
SNMP subagent	Software that gathers information about the managed device and passes the information to the master agent. Also called a <a href="#">subagent</a> .
SSL	A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP. Also called <a href="#">Secure Sockets Layer</a> .
standard index	index maintained by default.
sub suffix	A branch underneath a root suffix.
subagent	See <a href="#">SNMP subagent</a> .
substring index	Allows for efficient searching against substrings within entries. Substring indexes are limited to a minimum of two characters for each entry.
suffix	The name of the entry at the top of the directory tree, below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.
superuser	The most privileged user available on Unix machines. The superuser has complete access privileges to all files on the machine. Also called <a href="#">root</a> .
supplier	Server containing the master copy of directory trees or subtrees that are replicated to replica servers.
supplier server	In the context of replication, a server that holds a replica that is copied to a different server is called a supplier for that replica.
supplier-initiated replication	Replication configuration where <a href="#">supplier</a> servers replicate directory data to any replica servers.
symmetric encryption	Encryption that uses the same key for both encrypting and decrypting. DES is an example of a symmetric encryption algorithm.
system index	Cannot be deleted or modified as it is essential to Directory Server operations.

---

### T

target	In the context of access control, the target identifies the directory information to which a particular ACI applies.
target entry	The entries within the scope of a CoS.
TCP/IP	Transmission Control Protocol/Internet Protocol. The main network protocol for the Internet and for enterprise (company) networks.
template entry	See <a href="#">CoS template entry</a> .
time/date format	Indicates the customary formatting for times and dates in a specific region.
TLS	The new standard for secure socket layers; a public key based protocol. Also <a href="#">Transport Layer Security</a> .
topology	The way a directory tree is divided among physical servers and how these servers link with one another.
Transport Layer Security	See <a href="#">TLS</a> .

### U

uid	A unique number associated with each user on a Unix system.
URL	Uniform Resource Locator. The addressing system used by the server and the client to request documents. It is often called a location. The format of a URL is <i>protocol://machine:port/document</i> . The port number is necessary only on selected servers, and it is often assigned by the server, freeing the user of having to place it in the URL.

### V

virtual list view index	Speeds up the display of entries in the Directory Server Console. Virtual list view indexes can be created on any branch point in the directory tree to improve display performance. See Also <a href="#">browsing index</a> .
-------------------------	--

### X

---

X.500 standard

The set of ISO/ITU-T documents outlining the recommended information model, object classes and attributes used by directory server implementation.



---

# Index

## Symbols

00core.ldif  
    ldif files, 4  
01common.ldif  
    ldif files, 5  
05rfc2247.ldif  
    ldif files, 5  
05rfc2927.ldif  
    ldif files, 5  
10presence.ldif  
    ldif files, 5  
10rfc2307.ldif  
    ldif files, 5  
20subscriber.ldif  
    ldif files, 5  
25java-object.ldif  
    ldif files, 5  
28pilot.ldif  
    ldif files, 5  
30ns-common.ldif  
    ldif files, 6  
50ns-admin.ldif  
    ldif files, 6  
50ns-certificate.ldif  
    ldif files, 6  
50ns-directory.ldif  
    ldif files, 6  
50ns-mail.ldif  
    ldif files, 6  
50ns-value.ldif  
    ldif files, 6  
50ns-web.ldif  
    ldif files, 6  
60pam-plugin.ldif, 6  
99user.ldif  
    ldif files, 6  
::, in LDIF statements, 234

## A

access log  
    connection code, 191  
    A1, 191

B1, 191  
B2, 191  
B3, 191  
B4, 191  
P2, 191  
T1, 191  
T2, 191  
U1, 191

contents, 179

abandon message (ABANDON), 188  
change sequence number (csn), 188  
connection description (conn), 190  
connection number (conn), 181  
elapsed time (etime), 184  
error number (err), 183  
extended operation OID (oid), 187  
file descriptor (fd), 181  
format, 179  
LDAP request type, 184  
LDAP response type, 185  
message ID (msgid), 188  
method type (method), 182  
number of entries (nentries), 184  
operation number (op), 182  
options description (options), 190  
SASL multi-stage binds, 189  
scope of the search (scope), 186  
slot number (slot), 182  
sort (SORT), 184  
tag number (tag), 183  
unindexed search indicator (notes=U), 185  
version number (version), 182  
VLV-related entries, 185

LDAP result codes, 192

levels, 180

    sample 1 (level 256), 180  
    sample 2 (level 4), 189  
    sample 3 (level 768), 190

statistics for monitoring and optimizing  
    directory usage, 266

alias dereferencing, 210

ancestorid.db4 file, 174

## B

backendMonitorDN attribute, 101

- backup files, 173
- bak2db
  - command-line shell script, 244
  - quick reference, 241
- bak2db.pl
  - command-line perl script, 260
  - quick reference, 242
- base, 234
- base 64 encoding, 234
- binary data, LDIF and, 234
- Browsing Indexes, 258
- bytessentattribute, 100
- C**
- changelog
  - multi-master replication changelog, 72
- changelog configuration attributes
  - changelogmaxentries, 74
  - nsslapd-changelogdir, 73
  - nsslapd-changelogmaxage, 74
- changelog configuration entries
  - cn=changelog5, 72
- cl-dump
  - command-line shell script, 245
  - quick reference, 242
- cl-dump.pl
  - command-line perl script, 260
  - quick reference, 242
- cn attribute, 85
- cn=changelog5
  - changelog configuration entries, 72
  - object classes, 72
- cn=config
  - general, 3
  - general configuration entries, 12
  - object classes, 12
- cn=config Directory Information Tree
  - configuration data, 3
- cn=encrypted attributes, 156
  - attribute, 156
  - object class, 156
- cn=encryption
  - encryption configuration entries, 75
  - object classes, 75
- cn=mapping tree
  - object classes, 78
  - suffix and replication configuration entries, 78
- cn=monitor
  - object classes, 99
  - read-only monitoring configuration entries, 99
- cn=NetscapeRoot
  - configuration, 8
- cn=SNMP
  - object classes, 101
  - SNMP configuration entries, 101
- cn=uniqueid generator
  - object classes, 105
  - uniqueid generator configuration entries, 105
- cn=UserRoot
  - configuration, 8
- command-line scripts, 241
  - finding and executing, 241
  - location of perl scripts, 242
  - location of shell scripts, 241
  - perl scripts, 259
    - bak2db.pl , 260
    - cl-dump.pl , 260
    - db2bak.pl, 261
    - db2index.pl , 262
    - db2ldif.pl , 263
    - ldif2db.pl , 264
    - ns-accountstatus.pl , 270
    - ns-activate.pl , 270
    - ns-inactivate.pl , 271
    - ns-newpwpolicy.pl , 272
    - repl-monitor.pl , 273
    - verify-db.pl , 276
  - quick reference, 241
  - shell scripts, 243
    - bak2db , 244
    - cl-dump , 245
    - db2bak , 246
    - db2index , 248
    - db2ldif , 247
    - dbverify, 246
    - ldif2db , 249
    - ldif2ldap , 251
    - monitor, 252
    - pwdhash , 251
    - repl-monitor, 252

- 
- restart-slapd , 255
  - restoreconf , 256
  - saveconf , 256
  - start-slapd , 257
  - stop-slapd , 257
  - suffix2instance , 258
  - vlvindex , 258
  - command-line utilities
    - dbscan, 235
    - finding and executing, 195
    - ldapdelete, 221
    - ldapmodify, 214
    - ldappasswd, 227
    - ldapsearch, 197
    - ldif, 234
  - configuration
    - access control, 8
    - accessing and modifying, 8
    - changing attributes, 9
    - cn=NetscapeRoot, 8
    - cn=UserRoot, 8
    - database-specific, 3
    - overview, 3
    - plug-in functionality, 7
  - configuration attributes
    - changelog5 configuration attributes, 72
    - changing, 9
    - core server configuration attributes, 11
    - database link plug-in configuration attributes, 158
    - database plug-in configuration attributes, 131
    - encryption configuration attributes, 75
    - mapping tree configuration attributes, 78
    - monitoring configuration attributes, 99
    - overview, 7
    - plug-in functionality configuration attributes, 127
    - plug-in functionality configuration attributes allowed by certain plug-ins, 129
    - plug-in functionality configuration attributes common to all plug-ins, 127
    - replication agreement configuration attributes, 85
    - replication configuration attributes, 79
    - restrictions to modifying, 10
    - retro changelog plug-in configuration attributes, 167
    - SNMP configuration attributes, 101
    - suffix configuration attributes, 78
    - synchronization agreement attributes, 96
    - uniqueid generator configuration attributes, 105
  - configuration changes
    - requiring server restart, 11
  - configuration entries
    - modifying using LDAP, 10
    - restrictions to modifying, 10
  - configuration files, 173
    - location of, 8
  - configuration information tree
    - dse.ldif file, 12
  - connection attribute, 99
  - connection code, 191
  - core server configuration attributes
    - backendMonitorDN, 101
    - bytessent, 100
    - cn, 85
    - connection, 99
    - currentconnection, 99
    - currenttime, 100
    - description, 86
    - dtablesize, 100
    - entriessent, 100
    - nbackends, 101
    - nsDS50ruv, 96
    - nsDS5BeginReplicaRefresh, 92
    - nsDS5Flags, 80
    - nsDS5ReplConflict, 85
    - nsDS5ReplicaBindDN, 80
    - nsDS5ReplicaBindMethod, 87
    - nsDS5ReplicaBusyWaitTime, 87
    - nsDS5ReplicaChangeCount, 80
    - nsDS5ReplicaChangesSentSinceStartup, 87
    - nsDS5ReplicaCredentials, 88
    - nsDS5ReplicaHost, 88
    - nsDS5ReplicaID, 81
    - nsDS5ReplicaLastInitEnd, 89
    - nsDS5ReplicaLastInitStart, 89
    - nsDS5ReplicaLastInitStatus, 89
    - nsDS5ReplicaLastUpdateEnd, 90
    - nsDS5ReplicaLastUpdateStart, 90
    - nsDS5ReplicaLastUpdateStatus, 90
-

- nsDS5ReplicaLegacyConsumer, 81
- nsDS5ReplicaName, 81
- nsDS5ReplicaPort, 91
- nsDS5ReplicaPurgeDelay, 82
- nsDS5ReplicaReapActive, 92
- nsDS5ReplicaReferral, 83
- nsDS5ReplicaRoot, 83
- nsDS5ReplicaSessionPauseTime, 93
- nsDS5ReplicatedAttributeList, 94
- nsDS5ReplicaTimeout, 94
- nsDS5ReplicaTombstonePurgeInterval, 83
- nsDS5ReplicaTransportInfo, 95
- nsDS5ReplicaType, 84
- nsDS5ReplicaUpdateInProgress, 95
- nsDS5ReplicaUpdateSchedule, 95
- nsslapd-accesslog, 12
- nsslapd-accesslog-level, 13
- nsslapd-accesslog-list, 14
- nsslapd-accesslog-logbuffering, 14
- nsslapd-accesslog-logexpirationtime, 15
- nsslapd-accesslog-logexpirationtimeunit, 15
- nsslapd-accesslog-logging-enabled, 16
- nsslapd-accesslog-logmaxdiskspace, 16
- nsslapd-accesslog-logminfreediskspace, 17
- nsslapd-accesslog-logrotationsync-enabled, 17
- nsslapd-accesslog-logrotationsynhour, 18
- nsslapd-accesslog-logrotationsyncmin, 18
- nsslapd-accesslog-logrotationtime, 19
- nsslapd-accesslog-maxlogsize, 19
- nsslapd-accesslog-maxlogsperdir, 20
- nsslapd-accesslog-mode, 21
- nsslapd-attribute-name-exceptions, 21
- nsslapd-auditlog-list, 23
- nsslapd-auditlog-logexpirationtime, 23
- nsslapd-auditlog-logexpirationtimeunit, 23
- nsslapd-auditlog-logging-enabled, 24
- nsslapd-auditlog-logmaxsdiskspace, 25
- nsslapd-auditlog-logminfreediskspace, 25
- nsslapd-auditlog-logrotationsync-enabled, 25
- nsslapd-auditlog-logrotationsynhour, 26
- nsslapd-auditlog-logrotationsyncmin, 26
- nsslapd-auditlog-logrotationtime, 27
- nsslapd-auditlog-logrotationtimeunit, 27
- nsslapd-auditlog-maxlogsize, 28
- nsslapd-auditlog-maxlogsperdir, 28
- nsslapd-auditlog-mode, 29
- nsslapd-backend, 79
- nsslapd-certmap-basedn, 30
- nsslapd-changelogdir, 73
- nsslapd-changelogmaxage, 74
- nsslapd-changelogmaxentries, 74
- nsslapd-config, 30
- nsslapd-conntablesizes, 31
- nsslapd-csnlogging, 31
- nsslapd-ds4-compatible-schema, 32
- nsslapd-errorlog, 32
- nsslapd-errorlog-level, 33
- nsslapd-errorlog-list, 35
- nsslapd-errorlog-logexpirationtime, 35
- nsslapd-errorlog-logexpirationtimeunit, 35
- nsslapd-errorlog-logging-enabled, 36
- nsslapd-errorlog-logmaxdiskspace, 36
- nsslapd-errorlog-logminfreediskspace, 36
- nsslapd-errorlog-logrotationsync-enabled, 37
- nsslapd-errorlog-logrotationsynhour, 37
- nsslapd-errorlog-logrotationsyncmin, 38
- nsslapd-errorlog-logrotationtime, 38
- nsslapd-errorlog-logrotationtimeunit, 39
- nsslapd-errorlog-maxlogsize, 39
- nsslapd-errorlog-maxlogsperdir, 39
- nsslapd-errorlog-mode, 40
- nsslapd-groupvalnestlevel, 41
- nsslapd-idletimeout, 41
- nsslapd-instancedir, 42
- nsslapd-ioblocktimeout, 42
- nsslapd-lastmod, 42
- nsslapd-listenhost, 43
- nsslapd-localhost, 44
- nsslapd-localuser, 44
- nsslapd-maxbersize, 45
- nsslapd-maxdescriptors, 45
- nsslapd-maxthreadsperconn, 47
- nsslapd-nagle, 47
- nsslapd-outbound-ldap-io-timeout, 47
- nsslapd-plug-in, 48
- nsslapd-port, 48
- nsslapd-privatenamespaces, 48
- nsslapd-pwpolicy-local, 49
- nsslapd-readonly, 49
- nsslapd-referral, 50
- nsslapd-referralmode, 50

---

- nsslapd-reservedescriptors, 51
- nsslapd-return-exact-case, 52
- nsslapd-rootdn, 53
- nsslapd-rootpw, 53
- nsslapd-rootpwstoragescheme, 54
- nsslapd-saslpath, 54
- nsslapd-schema-ignore-trailing-spaces, 55
- nsslapd-schemacheck, 55
- nsslapd-schemareplace, 57
- nsslapd-securelistenhost, 57
- nsslapd-securePort, 57
- nsslapd-security, 58
- nsslapd-sizelimit, 58
- nsslapd-ssl-check-hostname, 59
- nsslapd-state, 78
- nsslapd-threadnumber, 59
- nsslapd-timelimit, 60
- nsslapd-versionstring, 61
- nssnmpcontact, 102
- nssnmpdescription, 102
- nssnmpenabled, 101
- nssnmplocation, 102
- nssnmpmasterhost, 103
- nssnmpmasterport, 103
- nssnmporganization, 101
- nsssl2 attribute, 76
- nsssl3 attribute, 76
- nsssl3ciphers attribute, 76
- nssslclientauth attribute, 75
- nssslsessiontimeout attribute, 75
- nsState, 85
- nsstate, 106
- opscompleted, 100
- opsinitiated, 100
- passwordCheckSyntax, 62
- passwordExp, 63
- passwordHistory, 64
- passwordInHistory, 64
- passwordLockout, 65
- passwordLockoutDuration, 65
- passwordMaxAge, 66
- passwordMaxFailure, 66
- passwordMinAge, 67
- passwordMinLength, 68
- passwordMustChange, 70
- passwordResetFailureCount, 70
- passwordStorageScheme, 71

- passwordUnlock, 72
- passwordWarning, 72
- readwaiters, 100
- starttime, 100
- totalconnections, 99
- currentconnections attribute, 99
- currenttime attribute, 100

## D

- database
  - exporting, 247
  - reindexing index files, 248
- database encryption
  - nsAttributeEncryption, 156
  - nsEncryptionAlgorithm, 156
- database files, 173
- database link plug-in configuration attributes
  - nsAbandonCount, 167
  - nsAbandonedSearchCheckInterval, 160
  - nsActiveChainingComponents, 158
  - nsAddCount, 166
  - nsBindConnectionCount, 167
  - nsBindConnectionsLimit, 160
  - nsBindCount, 167
  - nsBindRetryLimit, 161
  - nsBindTimeout, 161
  - nsCheckLocalACI, 162
  - nsCompareCount, 167
  - nsConcurrentBindLimit, 162
  - nsConcurrentOperationsLimit, 162
  - nsConnectionLife, 162
  - nsDeleteCount, 166
  - nsFarmServerURL, 165
  - nshoplimit, 166
  - nsMaxResponseDelay, 159
  - nsMaxTestResponseDelay, 159
  - nsModifyCount, 166
  - nsMultiplexorBindDN, 165
  - nsMultiplexorCredentials, 165
  - nsOperationConnectionCount, 167
  - nsOperationConnectionsLimit, 163
  - nsProxiedAuthorization, 163
  - nsReferralOnScopedSearch, 164
  - nsRenameCount, 167
  - nsSearchBaseCount, 167
  - nsSearchOneLevelCount, 167

- nsSearchSubtreeCount, 167
- nsSizeLimit, 164
- nsslapd-changelogmaxage, 168
- nsTimeLimit, 164
- nsTransmittedControls, 159
- nsUnbindCount, 167
- database plug-in configuration attributes
  - cn, 154
  - dbcachehitratio, 146
  - dbcachehits, 146
  - dbcachepagein, 147
  - dbcachepageout, 147
  - dbcacheroevict, 147
  - dbcacherwevict, 147
  - dbcachetries, 146
  - dbfilecachehit, 155
  - dbfilecachemiss, 155
  - dbfilenamenum, 155
  - dbfilepagein, 155
  - dbfilepageout, 155
  - description, 154
  - nsIndexType, 153
  - nsLookThroughLimit, 132
  - nsMatchingRule, 153
  - nsslapd-cache-autosize, 133
  - nsslapd-cache-autosize-split, 133
  - nsslapd-cachememsize, 148
  - nsslapd-cachesize, 147
  - nsslapd-db-abort-rate, 150
  - nsslapd-db-active-txns, 150
  - nsslapd-db-cache-hit, 150
  - nsslapd-db-cache-region-wait-rate, 150
  - nsslapd-db-cache-size-bytes, 150
  - nsslapd-db-cache-try, 150
  - nsslapd-db-checkpoint-interval, 135
  - nsslapd-db-circular-logging, 135
  - nsslapd-db-clean-pages, 150
  - nsslapd-db-commit-rate, 150
  - nsslapd-db-deadlock-rate, 151
  - nsslapd-db-debug, 136
  - nsslapd-db-dirty-pages, 151
  - nsslapd-db-durable-transactions, 136
  - nsslapd-db-hash-buckets, 151
  - nsslapd-db-hash-elements-examine-rate, 151
  - nsslapd-db-hash-search-rate, 151
  - nsslapd-db-home-directory, 137
  - nsslapd-db-idl-divisor, 138
  - nsslapd-db-lock-conflicts, 151
  - nsslapd-db-lock-region-wait-rate, 151
  - nsslapd-db-lock-request-rate, 151
  - nsslapd-db-lockers, 151
  - nsslapd-db-log-bytes-since-checkpoint, 151
  - nsslapd-db-log-region-wait-rate, 151
  - nsslapd-db-log-write-rate, 151
  - nsslapd-db-logbuf-size, 139
  - nsslapd-db-logdirectory, 139
  - nsslapd-db-logfile-size, 140
  - nsslapd-db-longest-chain-length, 152
  - nsslapd-db-page-create-rate, 152
  - nsslapd-db-page-ro-evict-rate, 152
  - nsslapd-db-page-rw-evict-rate, 152
  - nsslapd-db-page-size, 140
  - nsslapd-db-page-trickle-rate, 152
  - nsslapd-db-page-write-rate, 152
  - nsslapd-db-pages-in-use, 152
  - nsslapd-db-spin-count, 140
  - nsslapd-db-transaction-batch-val, 141
  - nsslapd-db-trickle-percentage, 142
  - nsslapd-db-txn-region-wait-rate, 152
  - nsslapd-db-verbose, 142
  - nsslapd-dbcachesize, 134
  - nsslapd-dbncache, 143
  - nsslapd-directory, 143, 148
  - nsslapd-idlistscanlimit, 132
  - nsslapd-import-cache-autosize, 144
  - nsslapd-import-cachesize, 144
  - nsslapd-mode, 146
  - nsslapd-readonly, 149
  - nsslapd-require-index, 149
  - nsslapd-suffix, 149
  - nsSystemIndex, 152
- database schema
  - defined, 55
- database-specific configuration
  - location of, 3
- db.00x files, 174
- db2bak
  - command-line shell script, 246
  - quick reference, 241
- db2bak.pl
  - command-line perl script, 261
  - quick reference, 242
- db2dsml

---

- quick reference, 241
- db2index, 282
  - command-line shell script, 248
  - quick reference, 241
- db2index.pl
  - command-line perl script, 262
  - quick reference, 242
- db2ldif
  - command-line shell script, 247
  - quick reference, 241
- db2ldif.pl
  - command-line perl script, 263
  - quick reference, 242
- dbcachehitratio attribute, 146
- dbcachehits attribute, 146
- dbcachepagein attribute, 147
- dbcachepageout attribute, 147
- dbcacheroevict attribute, 147
- dbcacherwevict attribute, 147
- dbcachetries attribute, 146
- dbfilecachehit attribute, 155
- dbfilecachemiss attribute, 155
- dbfilenamenum attribute, 155
- dbfilepagein attribute, 155
- dbfilepageout attribute, 155
- dbscan command-line utility
  - examples, 237
  - options, 236
  - syntax, 235
- dbverify
  - command-line shell script, 246
  - quick reference, 241
- description attribute, 86
- distinguished names
  - root, 53
- dse.ldif
  - configuration information tree, 12
  - contents of, 3
  - editing, 11
  - ldif files, 4
- dse.ldif.bak file, 3
- dse.ldif.startOK file, 3
- dsml2db
  - quick reference, 241
- dtablesize attribute, 100

## E

- editing
  - dse.ldif file, 11
- encryption
  - root password, 53
  - specifying password storage scheme, 71
- encryption configuration attributes
  - nsssl2, 76
  - nsssl3, 76
  - nsssl3ciphers, 76
  - nssslclientauth, 75
  - nssslsessiontimeout, 75
- encryption configuration entries
  - cn=encryption, 75
- encryption method, for root password, 53
- entriessent attribute, 100
- entrydn.db4 file, 175

## F

- feedback
  - contact information for this manual, x
- files
  - ancestorid.db4, 174
  - containing search filters, 210
  - entrydn.db4, 175
  - id2entry.db4, 175
  - locating configuration, 8
  - nsuniqueid.db4, 175
  - numsubordinates.db4, 175
  - objectclass.db4, 175
  - parentid.db4, 175

## I

- id2entry.db4 file, 175
- Indexes
  - configuration of, 8

## J

- jpeg images, 234

## L

- LDAP
  - modifying configuration entries, 10
- LDAP Data Interchange Format (LDIF)
  - binary data, 234

- LDAP result codes, 192
  - ldapdelete command-line utility
    - additional options, 226
    - commonly used options, 222
    - SASL options, 225
    - ssl options, 223
    - syntax, 222
  - ldapmodify command-line utility
    - additional options, 219
    - commonly used options, 215
    - options, 214
    - SASL options, 218
    - ssl options, 216
    - syntax, 214
  - ldappasswd command-line utility
    - changing user password, 232, 233, 233, 233
    - examples, 232
    - generating user password, 232
    - options, 228
    - prompting for new password, 233
    - syntax, 227
  - ldapsearch command-line utility
    - additional options, 210
    - commonly used options, 198
    - SASL options, 204
    - ssl options, 201
  - ldif command-line utility
    - options, 234
    - syntax, 234
  - LDIF configuration files
    - contents of, 6
    - detailed contents of, 4
    - location of, 4
  - LDIF entries
    - binary data in, 234
  - ldif files
    - 00core.ldif, 4
    - 01common.ldif, 5
    - 05rfc2247.ldif, 5
    - 05rfc2927.ldif, 5
    - 10presence.ldif, 5
    - 10rfc2307.ldif, 5
    - 20subscriber.ldif, 5
    - 25java-object.ldif, 5
    - 28pilot.ldif, 5
    - 30ns-common.ldif, 6
    - 50ns-admin.ldif, 6
    - 50ns-certificate.ldif, 6
    - 50ns-directory.ldif, 6
    - 50ns-mail.ldif, 6
    - 50ns-value.ldif, 6
    - 50ns-web.ldif, 6
    - 99user.ldif, 6
    - dse.ldif, 4
  - LDIF files, 175
  - ldif2db
    - command-line shell script, 249
    - quick reference, 241
  - ldif2db.pl
    - command-line perl script, 264
    - quick reference, 242
  - ldif2ldap
    - command-line shell script, 251
    - quick reference, 241
  - lock files, 176
  - log files, 176
    - access, 12
    - error, 32
  - log.xxxxxxxxx files, 174
  - logconv.pl
    - quick reference, 242
  - logconv.pl script, 266
    - options, 267
- ## M
- Meta Directory changelog
    - retro changelog, 72
  - monitor
    - command-line shell script, 252
    - quick reference, 241
  - multi-master replication changelog
    - changelog, 72
- ## N
- nbackends attribute, 101
  - ns-accountstatus.pl
    - command-line perl script, 270
    - quick reference, 242
  - ns-activate.pl
    - command-line perl script, 270
    - quick reference, 242
  - ns-inactivate.pl

---

command-line perl script, 271  
quick reference, 242

ns-newpolicy.pl  
quick reference, 242

ns-newpwpolicy.pl  
command-line perl script, 272

ns-slapd command-line utilities  
archive2db, 281  
db2archive, 282  
db2index, 282  
db2ldif, 277  
finding and executing, 277  
ldif2db, 279

nsAbandonCount attribute, 167

nsAbandonedSearchCheckInterval attribute, 160

nsActiveChainingComponents attribute, 158

nsAddCount attribute, 166

nsAttributeEncryption, 156

nsBindConnectionCount attribute, 167

nsBindConnectionsLimit attribute, 160

nsBindCount attribute, 167

nsBindRetryLimit attribute, 161

nsBindTimeout attribute, 161

nsCheckLocalACI attribute, 162

nsCompareCount attribute, 167

nsConcurrentBindLimit attribute, 162

nsConcurrentOperationsLimit attribute, 162

nsConnectionLife attribute, 162

nsDeleteCount attribute, 166

nsDS50ruv attribute, 96

nsDS5BeginReplicaRefresh attribute, 92

nsDS5Flags attribute, 80

nsDS5ReplConflict attribute, 85

nsDS5ReplicaBindDN attribute, 80

nsDS5ReplicaBindMethod attribute, 87

nsDS5ReplicaBusyWaitTime attribute, 87

nsDS5ReplicaChangeCount attribute, 80

nsDS5ReplicaChangesSentSinceStartup attribute, 87

nsDS5ReplicaCredentials attribute, 88

nsDS5ReplicaHost attribute, 88

nsDS5ReplicaID attribute, 81

nsDS5ReplicaLastInitEnd attribute, 89

nsDS5ReplicaLastInitStart attribute, 89

nsDS5ReplicaLastInitStatus attribute, 89

nsDS5ReplicaLastUpdateEnd attribute, 90

nsDS5ReplicaLastUpdateStart attribute, 90

nsDS5ReplicaLastUpdateStatus attribute, 91

nsDS5ReplicaLegacyConsumer attribute, 81

nsDS5ReplicaName attribute, 81

nsDS5ReplicaPort attribute, 91

nsDS5ReplicaPurgeDelay attribute, 82

nsDS5ReplicaReapActive attribute, 92

nsDS5ReplicaReferral attribute, 83

nsDS5ReplicaRoot attribute, 83

nsDS5ReplicaSessionPauseTime attribute, 93

nsDS5ReplicatedAttributeList attribute, 94

nsDS5ReplicaTimeout attribute, 94

nsDS5ReplicaTombstonePurgeInterval attribute, 83

nsDS5ReplicaTransportInfo attribute, 95

nsDS5ReplicaType attribute, 84

nsDS5ReplicaUpdateInProgress attribute, 95

nsDS5ReplicaUpdateSchedule attribute, 95

nsds7DirectoryReplicaSubtree, 97

nsds7DirsyncCookie, 97

nsds7NewWinGroupSyncEnabled, 97

nsds7NewWinUserSyncEnabled, 98

nsds7WindowsDomain, 98

nsds7WindowsReplicaSubtree, 98

nsEncryptionAlgorithm, 156

nsFarmServerURL attribute, 165

nshoplimit attribute, 166

nsIndexType attribute, 153

nsLookThroughLimit attribute, 132

nsMatchingRule attribute, 153

nsMaxResponseDelay attribute, 159

nsMaxTestResponseDelay attribute, 159

nsModifyCount attribute, 166

nsMultiplexorBindDN attribute, 165

nsMultiplexorCredentials attribute, 165

nsOperationConnectionCount attribute, 167

nsOperationConnectionsLimit attribute, 163

nsProxiedAuthorization attribute, 163

nsReferralOnScopedSearch attribute, 164

nsRenameCount attribute, 167

nsSearchBaseCount attribute, 167

nsSearchOneLevelCount attribute, 167

nsSearchSubtreeCount attribute, 167

nsSizeLimit attribute, 164

nsslapd-accesslog attribute, 12

nsslapd-accesslog-level attribute, 13

nsslapd-accesslog-list attribute, 14

- nsslapd-accesslog-logbuffering attribute, 14
- nsslapd-accesslog-logexpirationtime attribute, 15
- nsslapd-accesslog-logexpirationtimeunit attribute, 15
- nsslapd-accesslog-logging-enabled attribute, 16
- nsslapd-accesslog-logmaxdiskspace attribute, 16
- nsslapd-accesslog-logminfreediskspace attribute, 17
- nsslapd-accesslog-logrotationsync-enabled attribute, 17
- nsslapd-accesslog-logrotationsynchour attribute, 18
- nsslapd-accesslog-logrotationsyncmin attribute, 18
- nsslapd-accesslog-logrotationtime attribute, 19
- nsslapd-accesslog-maxlogsize attribute, 19
- nsslapd-accesslog-maxlogspendir attribute, 20
- nsslapd-accesslog-mode attribute, 21
- nsslapd-attribute-name-exceptions attribute, 21
- nsslapd-auditlog-list attribute, 23
- nsslapd-auditlog-logexpirationtime attribute, 23
- nsslapd-auditlog-logexpirationtimeunit attribute, 23
- nsslapd-auditlog-logging-enabled attribute, 24
- nsslapd-auditlog-logmaxdiskspace attribute, 25
- nsslapd-auditlog-logminfreediskspace attribute, 25
- nsslapd-auditlog-logrotationsync-enabled attribute, 25
- nsslapd-auditlog-logrotationsynchour attribute, 26
- nsslapd-auditlog-logrotationsyncmin attribute, 26
- nsslapd-auditlog-logrotationtime attribute, 27
- nsslapd-auditlog-logrotationtimeunit attribute, 27
- nsslapd-auditlog-maxlogsize attribute, 28
- nsslapd-auditlog-maxlogspendir attribute, 28
- nsslapd-auditlog-mode attribute, 29
- nsslapd-backend attribute, 79
- nsslapd-cache-autosize attribute, 133
- nsslapd-cache-autosize-split attribute, 133
- nsslapd-cachememsize attribute, 148
- nsslapd-cachesize attribute, 147
- nsslapd-certmap-basedn attribute, 30
- nsslapd-changelogdir attribute, 73
- nsslapd-changelogmaxage attribute, 74
- nsslapd-changelogmaxentries attribute, 74
- nsslapd-config attribute, 30
- nsslapd-conntablesizes attribute, 31
- nsslapd-csnlogging attribute, 31
- nsslapd-db-abort-rate attribute, 150
- nsslapd-db-active-txns attribute, 150
- nsslapd-db-cache-hit attribute, 150
- nsslapd-db-cache-region-wait-rate attribute, 150
- nsslapd-db-cache-size-bytes attribute, 150
- nsslapd-db-cache-try attribute, 150
- nsslapd-db-checkpoint-interval attribute, 135
- nsslapd-db-circular-logging attribute, 135
- nsslapd-db-clean-pages attribute, 150
- nsslapd-db-commit-rate attribute, 150
- nsslapd-db-deadlock-rate attribute, 151
- nsslapd-db-debug attribute, 136
- nsslapd-db-dirty-pages attribute, 151
- nsslapd-db-durable-transactions attribute, 136
- nsslapd-db-hash-buckets attribute, 151
- nsslapd-db-hash-elements-examine-rate attribute, 151
- nsslapd-db-hash-search-rate attribute, 151
- nsslapd-db-home-directory attribute, 137
- nsslapd-db-idl-divisor attribute, 138
- nsslapd-db-lock-conflicts attribute, 151
- nsslapd-db-lock-region-wait-rate attribute, 151
- nsslapd-db-lock-request-rate attribute, 151
- nsslapd-db-lockers attribute, 151
- nsslapd-db-log-bytes-since-checkpoint attribute, 151
- nsslapd-db-log-region-wait-rate attribute, 151
- nsslapd-db-log-write-rate attribute, 151
- nsslapd-db-logbuf-size attribute, 139
- nsslapd-db-logdirectory attribute, 139
- nsslapd-db-logfile-size attribute, 140
- nsslapd-db-longest-chain-length attribute, 152
- nsslapd-db-page-create-rate attribute, 152
- nsslapd-db-page-ro-evict-rate attribute, 152
- nsslapd-db-page-rw-evict-rate attribute, 152

---

nsslapd-db-page-size attribute, 140  
nsslapd-db-page-trickle-rate attribute, 152  
nsslapd-db-page-write-rate attribute, 152  
nsslapd-db-pages-in-use attribute, 152  
nsslapd-db-spin-count attribute, 140  
nsslapd-db-transaction-batch-val attribute, 141  
nsslapd-db-trickle-percentage attribute, 142  
nsslapd-db-txn-region-wait-rate attribute, 152  
nsslapd-db-verbose attribute, 142  
nsslapd-dbcachesize attribute, 134  
nsslapd-dbncache attribute, 143  
nsslapd-directory attribute, 143, 148  
nsslapd-ds4-compatible-schema attribute, 32  
nsslapd-errorlog attribute, 32  
nsslapd-errorlog-level attribute, 33  
nsslapd-errorlog-list attribute, 35  
nsslapd-errorlog-logexpirationtime attribute, 35  
nsslapd-errorlog-logexpirationtimeunit attribute, 35  
nsslapd-errorlog-logging-enabled attribute, 36  
nsslapd-errorlog-logmaxdiskpace attribute, 36  
nsslapd-errorlog-logminfreediskpace attribute, 36  
nsslapd-errorlog-logrotationsync-enabled attribute, 37  
nsslapd-errorlog-logrotationsynchour attribute, 37  
nsslapd-errorlog-logrotationsyncmin attribute, 38  
nsslapd-errorlog-logrotationtime attribute, 38  
nsslapd-errorlog-logrotationtimeunit attribute, 39  
nsslapd-errorlog-maxlogsize attribute, 39  
nsslapd-errorlog-maxlogspendir attribute, 39  
nsslapd-errorlog-mode attribute, 40  
nsslapd-groupvalnestlevel attribute, 41  
nsslapd-idletimeout attribute, 41  
nsslapd-idlistscanlimit attribute, 132  
nsslapd-import-cache-autosize attribute, 144  
nsslapd-import-cachesize attribute, 144  
nsslapd-instancedir attribute, 42  
nsslapd-ioblocktimeout attribute, 42  
nsslapd-lastmod attribute, 42  
nsslapd-listenhost attribute, 43  
nsslapd-localhost attribute, 44  
nsslapd-localuser attribute, 44  
nsslapd-maxbersize attribute, 45  
nsslapd-maxdescriptors attribute, 45  
nsslapd-maxthreadsperconn attribute, 47  
nsslapd-mode attribute, 146  
nsslapd-nagle attribute, 47  
nsslapd-outbound-ldap-io-timeout attribute, 47  
nsslapd-plugin attribute, 48  
nsslapd-plugin-depends-on-named attribute, 130  
nsslapd-plugin-depends-on-type attribute, 130  
nsslapd-pluginDescription attribute, 129  
nsslapd-pluginEnabled attribute, 128  
nsslapd-pluginId attribute, 128  
nsslapd-pluginInitFunc attribute, 127  
nsslapd-pluginLoadGlobal attribute, 130  
nsslapd-pluginLoadNow attribute, 129  
nsslapd-pluginPath attribute, 127  
nsslapd-pluginType attribute, 127  
nsslapd-pluginVendor attribute, 129  
nsslapd-pluginVersion attribute, 128  
nsslapd-port attribute, 48  
nsslapd-privatenamespaces attribute, 48  
nsslapd-pwpolicy-local attribute, 49  
nsslapd-readonly attribute, 49  
nsslapd-referral attribute, 50  
nsslapd-referralmode attribute, 50  
nsslapd-require-index attribute, 149  
nsslapd-reservedescriptors attribute, 51  
nsslapd-return-exact-case attribute, 52  
nsslapd-rootdn attribute, 53  
nsslapd-rootpw attribute, 53  
nsslapd-rootpwstoragescheme attribute, 54  
nsslapd-saspath attribute, 54  
nsslapd-schema-ignore-trailing-spaces attribute, 55  
nsslapd-schemacheck attribute, 55  
nsslapd-schemareplace attribute, 57  
nsslapd-securelistenhost attribute, 57  
nsslapd-securePort attribute, 57  
nsslapd-security attribute, 58  
nsslapd-sizelimit attribute, 58  
nsslapd-ssl-check-hostname attribute, 59  
nsslapd-state attribute, 78  
nsslapd-suffix attribute, 149  
nsslapd-threadnumber attribute, 59  
nsslapd-timelimit attribute, 60

- nsslapd-versionstring attribute, 61
- nssnmpcontact attribute, 102
- nssnmpdescription attribute, 102
- nssnmpenabled attribute, 101
- nssnmplocation attribute, 102
- nssnmpmasterhost attribute, 103
- nssnmpmasterport attribute, 103
- nssnmporganization attribute, 101
- nsssl2 attribute, 76
- nsssl3 attribute, 76
- nsssl3ciphers attribute, 76
- nssslclientauth attribute, 75
- nssslsessiontimeout attribute, 75
- nsState attribute, 85
- nsstate attribute, 106
- nsSystemIndex attribute, 152
- nsTimeLimit attribute, 164
- nsTransmittedControls attribute, 159
- nsUnbindCount attribute, 167
- nsuniqueid.db4 file, 175
- numsubordinates.db4 file, 175

## O

- objectclass.db4 file, 175
- opscompleted attribute, 100
- opsinitiated attribute, 100

## P

- parentid.db4 file, 175
- passwordLockoutDuration attribute, 65
- passwordChange attribute, 62
- passwordCheckSyntax attribute, 62
- passwordExp attribute, 63
- passwordHistory attribute, 64
- passwordInHistory attribute, 64
- passwordLockout attribute, 65
- passwordMaxAge attribute, 66
- passwordMaxFailure attribute, 66
- passwordMinAge attribute, 67
- passwordMinLength attribute, 68
- passwordMustChange attribute, 70
- passwordResetFailureCount attribute, 70
- passwords
  - root, 53
- passwordStorageScheme attribute, 71
- passwordUnlock attribute, 72

- passwordWarning attribute, 72
- perl scripts, 259
  - locating, 242
- permissions
  - specifying for index files, 146
- plug-in functionality configuration attributes
  - cn, 154
  - dbcachehitratio, 146
  - dbcachehits, 146
  - dbcachepagein, 147
  - dbcachepageout, 147
  - dbcacheroevict, 147
  - dbcacherwevict, 147
  - dbcachetries, 146
  - dbfilecachehit, 155
  - dbfilecachemiss, 155
  - dbfilenamenum, 155
  - dbfilepagein, 155
  - dbfilepageout, 155
  - description, 154
  - nsAbandonCount, 167
  - nsAbandonedSearchCheckInterval, 160
  - nsActiveChainingComponents, 158
  - nsAddCount, 166
  - nsBindConnectionCount, 167
  - nsBindConnectionsLimit, 160
  - nsBindCount, 167
  - nsBindRetryLimit, 161
  - nsBindTimeout, 161
  - nsCheckLocalACI, 162
  - nsCompareCount, 167
  - nsConcurrentBindLimit, 162
  - nsConcurrentOperationsLimit, 162
  - nsConnectionLife, 162
  - nsDeleteCount, 166
  - nsFarmServerURL, 165
  - nshoplmit, 166
  - nsIndexType, 153
  - nsLookThroughLimit, 132
  - nsMatchingRule, 153
  - nsMaxResponseDelay, 159
  - nsMaxTestResponseDelay, 159
  - nsModifyCount, 166
  - nsMultiplexorBindDN, 165
  - nsMultiplexorCredentials, 165
  - nsOperationConnectionCount, 167
  - nsOperationConnectionsLimit, 163

---

nsProxiedAuthorization, 163  
nsReferralOnScopedSearch, 164  
nsRenameCount, 167  
nsSearchBaseCount, 167  
nsSearchOneLevelCount, 167  
nsSearchSubtreeCount, 167  
nsSizeLimit, 164  
nsslapd-cache-autosize, 133  
nsslapd-cache-autosize-split, 133  
nsslapd-cachememsize, 148  
nsslapd-cachesize, 147  
nsslapd-changelogdir, 168  
nsslapd-changelogmaxage, 168  
nsslapd-db-abort-rate, 150  
nsslapd-db-active-txns, 150  
nsslapd-db-cache-hit, 150  
nsslapd-db-cache-region-wait-rate, 150  
nsslapd-db-cache-size-bytes, 150  
nsslapd-db-cache-try, 150  
nsslapd-db-checkpoint-interval, 135  
nsslapd-db-circular-logging, 135  
nsslapd-db-clean-pages, 150  
nsslapd-db-commit-rate, 150  
nsslapd-db-deadlock-rate, 151  
nsslapd-db-debug, 136  
nsslapd-db-dirty-pages, 151  
nsslapd-db-durable-transactions, 136  
nsslapd-db-hash-buckets, 151  
nsslapd-db-hash-elements-examine-rate, 151  
nsslapd-db-hash-search-rate, 151  
nsslapd-db-home-directory, 137  
nsslapd-db-idl-divisor, 138  
nsslapd-db-lock-conflicts, 151  
nsslapd-db-lock-region-wait-rate, 151  
nsslapd-db-lock-request-rate, 151  
nsslapd-db-lockers, 151  
nsslapd-db-log-bytes-since-checkpoint, 151  
nsslapd-db-log-region-wait-rate, 151  
nsslapd-db-log-write-rate, 151  
nsslapd-db-logbuf-size, 139  
nsslapd-db-logdirectory, 139  
nsslapd-db-logfile-size, 140  
nsslapd-db-longest-chain-length, 152  
nsslapd-db-page-create-rate, 152  
nsslapd-db-page-ro-evict-rate, 152  
nsslapd-db-page-rw-evict-rate, 152  
nsslapd-db-page-size, 140  
nsslapd-db-page-trickle-rate, 152  
nsslapd-db-page-write-rate, 152  
nsslapd-db-pages-in-use, 152  
nsslapd-db-spin-count, 140  
nsslapd-db-transaction-batch-val, 141  
nsslapd-db-trickle-percentage, 142  
nsslapd-db-txn-region-wait-rate, 152  
nsslapd-db-verbose, 142  
nsslapd-dbcachesize, 134  
nsslapd-dbncache, 143  
nsslapd-directory, 143, 148  
nsslapd-idlistscanlimit, 132  
nsslapd-import-cache-autosize, 144  
nsslapd-import-cachesize, 144  
nsslapd-mode, 146  
nsslapd-plugin-depends-on-named, 130  
nsslapd-plugin-depends-on-type, 130  
nsslapd-pluginDescription, 129  
nsslapd-pluginEnabled, 128  
nsslapd-pluginId, 128  
nsslapd-pluginInitFunc, 127  
nsslapd-pluginLoadGlobal, 130  
nsslapd-pluginLoadNow, 129  
nsslapd-pluginPath, 127  
nsslapd-pluginType, 127  
nsslapd-pluginVendor, 129  
nsslapd-pluginVersion, 128  
nsslapd-readonly, 149  
nsslapd-require-index, 149  
nsslapd-suffix, 149  
nsSystemIndex, 152  
nsTimeLimit, 164  
nsTransmittedControls, 159  
nsUnbindCount, 167  
plug-ins  
    configuration of, 3  
port numbers  
    less than 1024, 48  
pwdhash  
    command-line shell script, 251  
    quick reference, 242

## R

read-only monitoring configuration attributes  
    backendMonitorDN, 101

- bytessent, 100
  - connection, 99
  - currentconnections, 99
  - currenttime, 100
  - dtablesize, 100
  - entriessent, 100
  - nbackends, 101
  - opscompleted, 100
  - opsinitiated, 100
  - readwaiters, 100
  - starttime, 100
  - totalconnections, 99
  - read-only monitoring configuration entries
    - cn=monitor, 99
  - readwaiters attribute, 100
  - repl-monitor
    - command-line shell script, 252
    - quick reference, 242
  - repl-monitor.pl
    - command-line perl script, 273
    - quick reference, 242
  - replication agreement configuration attributes
    - cn, 85
    - description, 86
    - nsDS50ruv, 96
    - nsDS5BeginReplicaRefresh, 92
    - nsDS5ReplicaBindDN, 86
    - nsDS5ReplicaBindMethod, 87
    - nsDS5ReplicaBusyWaitTime, 87
    - nsDS5ReplicaChangesSentSinceStartup, 87
    - nsDS5ReplicaCredentials, 88
    - nsDS5ReplicaHost, 88
    - nsDS5ReplicaLastInitEnd, 89
    - nsDS5ReplicaLastInitStart, 89
    - nsDS5ReplicaLastInitStatus, 89
    - nsDS5ReplicaLastUpdateEnd, 90
    - nsDS5ReplicaLastUpdateStart, 90
    - nsDS5ReplicaLastUpdateStatus, 91
    - nsDS5ReplicaPort, 91
    - nsDS5ReplicaReapActive, 92
    - nsDS5ReplicaRoot, 92
    - nsDS5ReplicaSessionPauseTime, 93
    - nsDS5ReplicatedAttributeList, 94
    - nsDS5ReplicaTimeout, 94
    - nsDS5ReplicaTransportInfo, 95
    - nsDS5ReplicaUpdateInProgress, 95
    - nsDS5ReplicaUpdateSchedule, 95
  - object classes, 85
  - replication configuration attributes
    - nsDS5Flags, 80
    - nsDS5ReplConflict, 85
    - nsDS5ReplicaBindDN, 80
    - nsDS5ReplicaChangeCount, 80
    - nsDS5ReplicaID, 81
    - nsDS5ReplicaLegacyConsumer, 81
    - nsDS5ReplicaName, 81
    - nsDS5ReplicaPurgeDelay, 82
    - nsDS5ReplicaReferral, 83
    - nsDS5ReplicaRoot, 83
    - nsDS5ReplicaTombstonePurgeInterval, 83
    - nsDS5ReplicaType, 84
    - nsState, 85
  - object classes, 79
  - restart, 255
  - restart-slapd
    - command-line shell script, 255
    - quick reference, 241
  - restarting server
    - requirement for certain configuration changes, 11
  - restoreconfig
    - command-line shell script, 256
    - quick reference, 241
  - retro changelog
    - Meta Directory changelog, 72
  - retro changelog plug-in configuration attributes
    - nsslapd-changelogdir, 168
- ## S
- saveconfig
    - command-line shell script, 256
    - quick reference, 241
  - scripts, 241
    - location of perl scripts, 242
    - location of shell scripts, 241
    - perl scripts, 259
  - search filters
    - specifying file, 210
  - search operations
    - limiting entries returned, 58
    - setting time limits, 60
  - server restart

---

- after configuration changes, 11
- setting the location of SASL plugins, 54
- slapd.conf file
  - location of, 8
- smart referrals
  - ldapsearch option, 210
- SNMP configuration attributes
  - nssnmpcontact, 102
  - nssnmpdescription, 102
  - nssnmpenabled, 101
  - nssnmplocation, 102
  - nssnmpmasterhost, 103
  - nssnmpmasterport, 103
  - nssnmporganization, 101
- SNMP configuration entries
  - cn=SNMP, 101
- start-slapd
  - command-line shell script, 257
  - quick reference, 241
- starttime attribute, 100
- statistics
  - from access logs, 266
- stop-slapd
  - command-line shell script, 257
  - quick reference, 241
- suffix and replication configuration entries
  - cn=mapping tree, 78
- suffix configuration attributes
  - nsslapd-backend, 79
  - nsslapd-state, 78
  - object classes, 78
- suffix2instance
  - command-line shell script, 258
  - quick reference, 241
- synchronization agreement attributes
  - nsds7DirectoryReplicaSubtree, 97
  - nsds7DirsyncCookie, 97
  - nsds7NewWinGroupSyncEnabled, 97
  - nsds7NewWinUserSyncEnabled, 98
  - nsds7WindowsDomain, 98
  - nsds7WindowsReplicaSubtre, 98

## T

- totalconnections attribute, 99
- trailing spaces in object class names, 55

## U

- uniqueid generator configuration attributes
  - nsstate, 106
- uniqueid generator configuration entries
  - cn=uniqueid generator, 105

## V

- verify-db.pl
  - command-line perl script, 276
  - quick reference, 241, 242
- vlindex
  - command-line shell script, 258
  - quick reference, 241

