

# Configuration, Command, and File Reference

*iPlanet Directory Server*

**Version 5.1**

816-2671  
December 2001

Copyright © 2001 Sun Microsystems, Inc. Some preexisting portions Copyright © 2001 Netscape Communications Corporation. All rights reserved.

Sun, Sun Microsystems, the Sun logo, Solaris, SunTone, iPlanet and the iPlanet logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Netscape and the Netscape N logo are registered trademarks of Netscape Communications Corporation in the U.S. and other countries. Other Netscape logos, product names, and service names are also trademarks of Netscape Communications Corporation, which may be registered in other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

Portions of the Software copyright © 1995 PEER Networks, Inc. All rights reserved. Contains the Taligent® Unicode Collation Classes™ from Taligent, Inc. and IBM Corp. Portions of the Software copyright © 1992-1998 Regents of the University of Michigan. All rights reserved.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of the product or this document may be reproduced in any form by any means without prior written authorization of the Sun-Netscape Alliance and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright © 2001 Sun Microsystems, Inc. Pour certaines parties préexistantes, Copyright © 2001 Netscape Communications Corp. Tous droits réservés.

Sun, Sun Microsystems, le logo Sun, Solaris, SunTone, iPlanet et le logo iPlanet sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et d'autre pays. Netscape et the Netscape N logo sont des marques déposées de Netscape Communications Corporation aux Etats-Unis et d'autre pays. Les autres logos, les noms de produit, et les noms de service de Netscape sont des marques déposées de Netscape Communications Corporation dans certains autres pays.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company Ltd.

Certains composants du Logiciel sont copyright © 1995 PEER Networks, Inc. Tous droits réservés. Ce Logiciel contient les modules Taligent® Unicode Collation Classes™ provenant de Taligent, Inc. et IBM Corp. Des portions du Logiciel sont copyright © 1992-1998 Regents of the University of Michigan. Tous droits réservés.

Le produit décrit dans ce document est distribué selon des conditions de licence qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ni de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de l'Alliance Sun-Netscape et, le cas échéant, de ses bailleurs de licence.

CETTE DOCUMENTATION EST FOURNIE “EN L'ÉTAT”, ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.



# Contents

Prerequisite Reading .....	15
What Is In This Reference Guide? .....	16
Conventions Used In This Reference Guide .....	16
Related Information .....	17
<b>Chapter 1 Introduction .....</b>	<b>19</b>
Overview of Directory Server Management .....	19
Directory Server Configuration .....	20
Directory Server Instance File Reference .....	20
Migrating Directory Server .....	20
Using Directory Server Command-Line Utilities .....	20
Using Directory Server Command-Line Scripts .....	21
<b>Chapter 2 Core Server Configuration Reference .....</b>	<b>23</b>
Server Configuration - Overview .....	23
LDIF Configuration Files - Location .....	25
Schema Configuration Files - Location .....	25
How the Server Configuration is Organized .....	25
Configuration Attributes .....	25
Configuration of Plug-in Functionality .....	26
Configuration of Databases .....	27
Configuration of Indexes .....	27
Migration of Pre-Directory Server 5.1 Configuration Files to LDIF Format .....	28
Accessing and Modifying Server Configuration .....	28
Access Control For Configuration Entries .....	28
Changing Configuration Attributes .....	29
Modifying Configuration Entries Using LDAP .....	30
Restrictions to Modifying Configuration Entries .....	31
Restrictions to Modifying Configuration Attributes .....	31
Configuration Changes Requiring Server Restart .....	31

Core Server Configuration Attributes Reference .....	32
cn=config .....	33
nsIdleTimeout (Idle Timeout) .....	33
nsslapd-accesscontrol (Enable Access Control) .....	34
nsslapd-accesslog (Access Log) .....	34
nsslapd-accesslog-level .....	35
nsslapd-accesslog-list .....	36
nsslapd-accesslog-logbuffering (Log Buffering) .....	36
nsslapd-accesslog-logexpirationtime (Access Log Expiration Time) .....	36
nsslapd-accesslog-logexpirationtimeunit (Access Log Expiration Time Unit) .....	37
nsslapd-accesslog-logging-enabled (Access Log Enable Logging) .....	37
nsslapd-accesslog-logmaxdiskspace (Access Log Maximum Disk Space) .....	37
nsslapd-accesslog-logminfreediskspace (Access Log Minimum Free Disk Space) .....	38
nsslapd-accesslog-logrotationtime (Access Log Rotation Time) .....	38
nsslapd-accesslog-logrotationtimeunit (Access Log Rotation Time Unit) .....	39
nsslapd-accesslog-maxlogsize (Access Log Maximum Log Size) .....	39
nsslapd-accesslog-maxlogsperdir (Access Log Maximum Number of Log Files) .....	40
nsslapd-attribute-name-exceptions .....	40
nsslapd-auditlog (Audit Log) .....	41
nsslapd-auditlog-list .....	42
nsslapd-auditlog-logexpirationtime (Audit Log Expiration Time) .....	42
nsslapd-auditlog-logexpirationtimeunit (Audit Log Expiration Time Unit) .....	42
nsslapd-auditlog-logging-enabled (Audit Log Enable Logging) .....	43
nsslapd-auditlog-logmaxdiskspace (Audit Log Maximum Disk Space) .....	43
nsslapd-auditlog-logminfreediskspace (Audit Log Minimum Free Disk Space) .....	44
nsslapd-auditlog-logrotationtime (Audit Log Rotation Time) .....	44
nsslapd-auditlog-logrotationtimeunit (Audit Log Rotation Time Unit) .....	45
nsslapd-auditlog-maxlogsize (Audit Log Maximum Log Size) .....	45
nsslapd-auditlog-maxlogsperdir (Audit Log Maximum Number of Log Files) .....	46
nsslapd-certmap-basedn (Certificate Map Search Base) .....	46
nsslapd-config .....	47
nsslapd-ds4-compatible-schema .....	47
nsslapd-enquote-sup-oc (Enable Superior Object Class Enquoting) .....	47
nsslapd-errorlog (Error Log) .....	48
nsslapd-errorlog-level (Error Log Level) .....	49
nsslapd-errorlog-list .....	50
nsslapd-errorlog-logexpirationtime (Error Log Expiration Time) .....	51
nsslapd-errorlog-logexpirationtimeunit (Error Log Expiration Time Unit) .....	51
nsslapd-errorlog-logging-enabled (Enable Error Logging) .....	51
nsslapd-errorlog-logmaxdiskspace (Error Log Maximum Disk Space) .....	52
nsslapd-errorlog-logminfreediskspace (Error Log Minimum Free Disk Space) .....	52
nsslapd-errorlog-logrotationtime (Error Log Rotation Time) .....	53
nsslapd-errorlog-logrotationtimeunit (Error Log Rotation Time Unit) .....	53

nsslapd-errorlog-maxlogsize (Maximum Error Log Size)	54
nsslapd-errorlog-maxlogspedir (Maximum Number of Error Log Files)	54
nsslapd-groupevalnestlevel	55
nsslapd-instancedir (Instance Directory)	55
nsslapd-ioblocktimeout (IO Block Time Out)	55
nsslapd-lastmod (Track Modification Time)	56
nsslapd-listenhost (Listen to IP Address)	56
nsslapd-localhost (Local Host)	57
nsslapd-localuser (Local User)	57
nsslapd-maxbersize (Maximum Message Size)	58
nsslapd-maxdescriptors (Maximum File Descriptors)	58
nsslapd-maxthreadsperconn (Maximum Threads Per Connection)	59
nsslapd-nagle	60
nsslapd-plug-in	60
nsslapd-port (Port Number)	60
nsslapd-privatenamespaces	61
nsslapd-readonly (Read Only)	61
nsslapd-referral (Referral)	61
nsslapd-referralmode (Referral Mode)	62
nsslapd-reservedescriptors (Reserved File Descriptors)	62
nsslapd-return-exact-case (Return Exact Case)	64
nsslapd-rootdn (Manager DN)	65
nsslapd-rootpw (Root Password)	65
nsslapd-rootpwstoragescheme (Root Password Storage Scheme)	66
nsslapd-schemacheck (Schema Checking)	66
nsslapd-securelistenhost	67
nsslapd-securePort (Encrypted Port Number)	68
nsslapd-security (Security)	68
nsslapd-sizelimit (Size Limit)	68
nsslapd-threadnumber (Thread Number)	69
nsslapd-timelimit (Time Limit)	69
nsslapd-versionstring	71
passwordChange (Password Change)	71
passwordCheckSyntax (Check Password Syntax)	72
passwordExp (Password Expiration)	72
passwordHistory (Password History)	73
passwordInHistory (Number of Passwords to Remember)	73
passwordLockout (Account Lockout)	74
passwordLockoutDuration (Lockout Duration)	74
passwordMaxAge (Password Maximum Age)	75
passwordMaxFailure (Maximum Password Failures)	75
passwordMinAge (Password Minimum Age)	75
passwordMinLength (Password Minimum Length)	76

passwordMustChange (Password Must Change)	76
passwordResetFailureCount (Reset Password Failure Count After)	77
passwordStorageScheme (Password Storage Scheme)	77
passwordUnlock (Unlock Account)	78
passwordWarning (Send Warning)	78
cn=changelog5	79
nsslapd-changelogdir	79
nsslapd-changelogmaxage (Max Changelog Age)	80
nsslapd-changelogmaxentries (Max Changelog Records)	80
cn=encryption	81
nsslsessiontimeout	81
nssslclientauth	81
nsssl2	82
nsssl3	82
nsssl3ciphers	82
cn=features	84
cn=mapping tree	84
Suffix Configuration Attributes Under cn="suffixName"	85
nsslapd-state	85
nsslapd-backend	85
Replication Attributes Under cn=replica, cn="suffixName",cn=mapping tree,cn=config	86
cn	86
nsDS5Flags	87
nsDS5ReplicaBindDN	87
nsDS5ReplicaChangeCount	88
nsDS5ReplicaId	88
nsDS5ReplicaLegacyConsumer	89
nsDS5ReplicaName	89
nsDS5ReplicaPurgeDelay	89
nsDS5ReplicaReferral	90
nsDS5ReplicaRoot	90
nsDS5ReplicaTombstonePurgeInterval	90
nsDS5ReplicaType	91
nsState	91
Replication Attributes Under cn=ReplicationAgreementName,cn=replica, cn="suffixName", cn=mapping tree,cn=config	91
description	92
nsDS5ReplicaBindDN	92
nsDS5ReplicaBindMethod	92
nsDS5ReplicaChangesSentSinceStartup	93
nsDS5ReplicaCredentials	93
nsDS5ReplicaHost	94
nsDS5ReplicaLastInitEnd	94

nsDS5ReplicaLastInitStart .....	94
nsDS5ReplicaLastInitStatus .....	95
nsDS5ReplicaLastUpdateEnd .....	95
nsDS5ReplicaLastUpdateStart .....	96
nsDS5ReplicaLastUpdateStatus .....	96
nsDS5ReplicaPort .....	96
nsDS5ReplicaRefresh .....	97
nsDS5ReplicaRoot .....	97
nsDS5ReplicaTimeout .....	97
nsDS5ReplicaTransportInfo .....	98
nsDS5ReplicaUpdateInProgress .....	98
nsDS5ReplicaUpdateSchedule .....	99
nsDS50ruv .....	99
cn=monitor .....	99
connection .....	99
currentConnections .....	100
totalConnections .....	100
dTableSize .....	100
readWaiters .....	100
opsInitiated .....	100
opsCompleted .....	100
entriesSent .....	100
bytesSent .....	100
currentTime .....	100
startTime .....	100
nbackEnds .....	100
backendMonitorDN .....	101
cn=replication .....	101
cn=SNMP .....	101
nssnmpenabled .....	101
nssnmporganization .....	101
nssnmplocation .....	102
nssnmpcontact .....	102
nssnmpdescription .....	102
nssnmpmasterhost .....	103
nssnmpmasterport .....	103
cn=tasks .....	103
cn=uniqueid generator .....	104
nsstate .....	104
Configuration Quick Reference Tables .....	104
LDIF Configuration Files .....	104
Configuration Changes Requiring Server Restart .....	107

<b>Chapter 3 Plug-in Implemented Server Functionality Reference</b> .....	<b>109</b>
Overview .....	109
Object Classes for Plug-in Configuration .....	110
Server Plug-in Functionality Reference .....	111
7-bit check Plug-in .....	111
ACL Plug-in .....	112
ACL preoperation Plug-in .....	112
Binary Syntax Plug-in .....	113
Boolean Syntax Plug-in .....	113
Case Exact String Syntax Plug-in .....	114
Case Ignore String Syntax Plug-in .....	114
Chaining database Plug-in .....	115
Class of Service Plug-in .....	115
Country String Syntax Plug-in .....	116
Distinguished Name Syntax Plug-in .....	116
Generalized Time Syntax Plug-in .....	117
Integer Syntax Plug-in .....	118
Internationalization Plug-in .....	118
ldbm database Plug-in .....	119
Legacy Replication Plug-in .....	119
Multimaster Replication Plug-in .....	120
Octet String Syntax Plug-in .....	120
CLEAR Password Storage Plug-in .....	121
CRYPT Password Storage Plug-in .....	121
NS-MTA-MD5 Password Storage Scheme Plug-in .....	122
SHA Password Storage Scheme Plug-in .....	123
SSHA Password Storage Scheme Plug-in .....	123
Postal Address String Syntax Plug-in .....	124
PTA Plug-in .....	124
Referential Integrity Postoperation Plug-in .....	125
Retro Changelog Plug-in .....	126
Roles Plug-in .....	126
Telephone Syntax Plug-in .....	127
UID Uniqueness Plug-in .....	128
URI Plug-in .....	129
List of Attributes Common to all Plug-ins .....	129
nsslapd-pluginPath .....	129
nsslapd-pluginInitfunc .....	130
nsslapd-pluginType .....	130
nsslapd-pluginEnabled .....	130
nsslapd-pluginId .....	131
nsslapd-pluginVersion .....	131
nsslapd-pluginVendor .....	131



nsslapd-pluginDescription .....	132
Attributes Allowed by Certain Plug-ins .....	132
nsslapd-plugin-depends-on-type .....	132
nsslapd-plugin-depends-on-named .....	133
Database Plug-in Attributes .....	133
Database Attributes Under cn=config,cn=ldbm database,cn=plugins,cn=config .....	134
nsLookthroughLimit .....	134
nsslapd-allidsthreshold .....	134
nsslapd-cache-autosize .....	135
nsslapd-cache-autosize-split .....	135
nsslapd-dbcachesize .....	136
nsslapd-db-checkpoint-interval .....	136
nsslapd-db-circular-logging .....	137
nsslapd-db-durable-transactions .....	138
nsslapd-db-home-directory .....	138
nsslapd-db-idl-divisor .....	140
nsslapd-db-logbuf-size .....	140
nsslapd-db-logdirectory .....	141
nsslapd-db-logfile-size .....	141
nsslapd-db-page-size .....	142
nsslapd-db-transaction-batch-val .....	142
nsslapd-db-transaction-logging .....	143
nsslapd-dbncache .....	144
nsslapd-import-cachesize .....	144
nsslapd-mode .....	145
Database Attributes Under cn=monitor,cn=ldbm database, cn=plugins,cn=config .....	145
dbcachehits .....	145
dbcachetries .....	145
dbcachehitratio .....	145
dbcachepagein .....	145
dbcachepageout .....	145
dbcacheroevict .....	146
dbcacherwevict .....	146
Database Attributes Under cn=NetscapeRoot,cn=ldbm database, cn=plugins,cn=config and cn=UserRoot,cn=ldbm database, cn=plugins,cn=config .....	146
nsslapd-cachesize .....	147
nsslapd-cachememsize .....	147
nsslapd-directory .....	148
nsslapd-readonly .....	148
nsslapd-require-index .....	149
nsslapd-suffix .....	149
Database Attributes Under cn=database,cn=monitor,cn=ldbm database, cn=plugins, cn=config .....	150

nsslapd-db-abort-rate	150
nsslapd-db-active-txns	150
nsslapd-db-cache-hit	150
nsslapd-db-cache-try	150
nsslapd-db-cache-region-wait-rate	150
nsslapd-db-cache-size-bytes	150
nsslapd-db-clean-pages	150
nsslapd-db-commit-rate	150
nsslapd-db-deadlock-rate	150
nsslapd-db-dirty-pages	151
nsslapd-db-hash-buckets	151
nsslapd-db-hash-elements-examine-rate	151
nsslapd-db-hash-search-rate	151
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-longest-chain-length	152
nsslapd-db-page-create-rate	152
nsslapd-db-page-read-rate	152
nsslapd-db-page-ro-evict-rate	152
nsslapd-db-page-rw-evict-rate	152
nsslapd-db-page-trickle-rate	152
nsslapd-db-page-write-rate	152
nsslapd-db-pages-in-use	152
nsslapd-db-txn-region-wait-rate	152
Database Attributes Under cn=default indexes,cn=config,cn=ldbm database,cn=plugins, cn=config	153
nsSystemIndex	153
nsIndexType	154
nsMatchingRule	154
cn	155
description	155
Database Attributes Under cn=monitor,cn=Netscaperoot,cn=ldbm database,cn=plugins, cn=config	156
dbfilenamenumber	156
dbfilecachehit	156
dbfilecachemiss	156
dbfilepagein	156
dbfilepageout	156

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	157
VLV Index Object Classes Under cn= <i>MCCsuffixName</i> , cn=userRoot, cn=ldbm database, cn=plugins, cn=config	158
vlvIndex	158
vlvSearch	159
VLV Index Attributes Under cn= <i>MCCsuffixName</i> , cn=userRoot, cn=ldbm database, cn=plugins,cn=config	159
vlvBase	159
vlvEnabled	160
vlvFilter	160
vlvScope	160
vlvSort	161
vlvUses	161
Database Link Plug-in Attributes (chaining attributes)	162
Database Link Attributes Under cn=config,cn=chaining database, cn=plugins,cn=config	162
nsActiveChainingComponents	162
nsMaxResponseDelay	163
nsMaxTestResponseDelay	163
nsTransmittedControls	164
Database Link Attributes Under cn=default instance config,cn=chaining database, cn=plugins,cn=config	164
nsAbandonedSearchCheckInterval	164
nsBindConnectionsLimit	165
nsBindRetryLimit	165
nsBindTimeout	166
nsCheckLocalACI	166
nsConcurrentBindLimit	166
nsConcurrentOperationsLimit	167
nsConnectionLife	167
nsOperationConnectionsLimit	167
nsProxiedAuthorization	168
nsReferralOnScopedSearch	168
nsSizeLimit	169
nsTimeLimit	169
Database Link Attributes Under cn=database link instance name,cn=chaining database, cn=plugins,cn=config	169
nsFarmServerURL	170
nsMultiplexorBindDN	170
nsMultiplexorCredentials	170
nshoplimit	171
Database Link Attributes Under cn=monitor,cn=database instance name, cn=chaining database,cn=plugins,cn=config	171

nsAddCount .....	171
nsDeleteCount .....	172
nsModifyCount .....	172
nsRenameCount .....	172
nsSearchBaseCount .....	172
nsSearchOneLevelCount .....	172
nsSearchSubtreeCount .....	172
nsAbandonCount .....	172
nsBindCount .....	172
nsUnbindCount .....	172
nsCompareCount .....	172
nsOperationConnectionCount .....	172
nsBindConnectionCount .....	172
Retro Changelog Plug-in Attributes .....	173
nsslapd-changelogdir .....	173
nsslapd-changelogmaxage (Max Changelog Age) .....	174
<b>Chapter 4 Server Instance File Reference .....</b>	<b>175</b>
Overview of Directory Server Files .....	175
Backup Files .....	176
Configuration Files .....	177
Database Files .....	177
ldif Files .....	178
Lock Files .....	179
Log Files .....	179
<b>Chapter 5 Access Log and Connection Code Reference .....</b>	<b>181</b>
Access Log Content .....	181
Access Logging Levels .....	182
Default Access Logging Content .....	183
Connection Number .....	184
File Descriptor .....	184
Slot Number .....	184
Operation Number .....	185
Method Type .....	185
Version Number .....	185
Error Number .....	185
Tag Number .....	185
Number of Entries .....	186
Elapsed Time .....	186
LDAP Request Type .....	186
LDAP Response Type .....	187

Unindexed Search Indicator .....	187
Extended Operation OID .....	187
Change Sequence Number .....	188
Abandon Message .....	189
Message ID .....	189
SASL Multi-Stage Bind Logging .....	189
Access Log Content for Additional Access Logging Levels .....	190
Connection Description .....	192
Options Description .....	192
Common Connection Codes .....	192
LDAP Result Codes .....	193
<b>Chapter 6 Migration from Earlier Versions .....</b>	<b>197</b>
Migration from 4.x Directory Server to 5.0 or 5.1 .....	197
Server Attributes .....	197
Database Attributes .....	200
Upgrade from Directory Server 5.0 to 5.1 .....	201
General Server Configuration Attributes .....	202
Database Attributes .....	205
Database Link Attributes .....	207
SNMP Attributes .....	208
<b>Chapter 7 Command-Line Utilities .....</b>	<b>209</b>
Finding and Executing Command-Line Utilities .....	209
Command-Line Utilities Quick Reference .....	210
Using Special Characters .....	211
ldapsearch .....	211
ldapmodify .....	217
ldapdelete .....	221
ldif .....	223
<b>Chapter 8 Command-Line Scripts .....</b>	<b>225</b>
Command-Line Scripts Quick Reference .....	225
Shell and Batch Scripts .....	228
bak2db (Restore database from backup) .....	228
db2bak (Create backup of database) .....	229
db2ldif (Export database contents to LDIF) .....	229
getpwenc (Print encrypted password) .....	231
ldif2db (Import) .....	231
ldif2ldap (Perform import operation over LDAP) .....	233
monitor (Retrieve monitoring information) .....	233
restart-slapd (Restart the Directory Server) .....	234

restoreconfig (Restore Admin Server Configuration) .....	234
saveconfig (Save Admin Server Configuration) .....	235
start-slapd (Start the Directory Server) .....	235
stop-slapd (Stop the Directory Server) .....	236
suffix2instance (Map Suffix to Backend Name) .....	236
vindex (Create virtual list view (VLV) indexes) .....	237
Perl Scripts .....	238
bak2db.pl (Restore database from backup) .....	238
db2bak.pl (Create backup of database) .....	239
db2index.pl (Create and generate indexes) .....	240
db2ldif.pl (Export database contents to LDIF) .....	241
ldif2db.pl (Import) .....	242
migrateInstance5 (Migrate to Directory Server 5.0 or 5.1) .....	244
ns-accountstatus.pl (Establish account status) .....	245
ns-activate.pl (Activate an entry or group of entries) .....	246
ns-inactivate.pl (Inactivate an entry or group of entries) .....	247
<b>Appendix A Using the ns-slapd and slapd.exe Command-Line Utilities .....</b>	<b>249</b>
Overview of ns-slapd and slapd.exe Commands .....	249
ns-slapd (UNIX) .....	250
slapd.exe (Windows NT) .....	250
Finding and Executing the ns-slapd and slapd.exe Command-Line Utilities .....	250
ns-slapd and slapd.exe Command-Line Utilities for Exporting Databases .....	251
db2ldif .....	251
ns-slapd and slapd.exe Command-Line Utilities for Restoring and Backing up Databases .....	253
ldif2db .....	253
archive2db .....	255
db2archive .....	255
ns-slapd and slapd.exe Command-Line Utilities for Creating and Regenerating Indexes .....	256
db2index .....	256
<b>Index .....</b>	<b>275</b>

# About this Reference Guide

iPlanet Directory Server 5.1 is a powerful and scalable distributed directory server based on the industry-standard Lightweight Directory Access Protocol (LDAP). iPlanet Directory Server is the cornerstone for building a centralized and distributed data repository that can be used in your intranet, over your extranet with your trading partners, or over the public Internet to reach your customers.

For the latest information about new features and enhancements in this release of iPlanet Directory Server, please see the online release notes at:

<http://docs.iplanet.com/docs/manuals/directory.html>

This *Configuration, Command, and File Reference* documents the server configuration and command-line utilities provided with iPlanet Directory Server.

## Prerequisite Reading

This reference guide does not describe many of the basic directory and architectural concepts that you need to successfully design, implement, and administer your directory service. You should be familiar with those concepts, which are described in the *iPlanet Directory Server Deployment Guide* and the *iPlanet Directory Server Administrator's Guide*.

When you are familiar with directory server concepts and have done some preliminary planning for your directory service, you can install the iPlanet Directory Server. The instructions for installing the various Directory Server components are contained in the *iPlanet Directory Server Installation Guide*.

*Managing Servers with iPlanet Console* contains general background information on how to use iPlanet servers. You should read and understand the concepts in that book before you attempt to administer the Directory Server.

# What Is In This Reference 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 your server, use this reference guide to help you maintain it.

You can also manage the Directory Server using the Directory Server Console, a graphical user interface. The *iPlanet Directory Server Administrator's Guide* describes how to do this and explains individual administration tasks more fully.

## Conventions Used In This Reference Guide

This section explains the typographic conventions used in this book.

**Monospaced font** - This typeface is used for literal text, such as the names of attributes and object classes when they appear in text. It is also used for URLs, filenames and examples.

**Italic font** - This typeface is used for emphasis, for new terms, and for text that you must substitute for actual values, such as placeholders in path names.

---

**NOTE** Notes, Cautions and Tips highlight important conditions or limitations. Be sure to read this information before continuing.

---

This book uses the following format for paths and file names:

*installDir*/*slapd-serverID*/...

The actual path and server identifier will depend on your platform, your installation, and your configuration. The default path is platform-dependent:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/...</code>
<b>Other UNIX platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/...</code>
<b>Windows platform</b>	<code>C:\iPlanet\Servers\slapd-<i>serverID</i>\...</code>

If you have installed the Directory Server in a different location, you should adapt the path accordingly. *serverID* represents the server identifier you gave the server when you installed it. For example, if you gave the name `phonebook` to your directory server, then the actual path would be:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-phonebook/...</code>
<b>Other UNIX platforms</b>	<code>/usr/iplanet/servers/slapd-phonebook/...</code>
<b>Windows platform</b>	<code>C:\iPlanet\Servers\slapd-phonebook\...</code>



Most paths and commands specified in this manual are in UNIX format. If you are using a Windows-based version of Directory Server, use equivalent paths and commands. All commands on Windows platforms have the same name with the .exe or .bat extension.

## Related Information

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

**iPlanet Directory Server Installation Guide.** Procedures for installing Directory Server as well as procedures for migrating your Netscape Directory Server to iPlanet Directory Server.

**iPlanet Directory Server Deployment Guide.** Provides an overview for planning your deployment of the Directory Server. Includes deployment examples.

**iPlanet Directory Server Administrator's Guide.** Procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.

**iPlanet Directory Server Schema Reference.** Information about the LDAP schema shipped with Directory Server and useful for client applications.

Other useful iPlanet information can be found at the following Internet locations:

- **iPlanet product documentation online:**  
<http://docs.iplanet.com/docs/manuals/>
- **iPlanet product status:**  
[http://www.iplanet.com/support/technical\\_resources/](http://www.iplanet.com/support/technical_resources/)
- **iPlanet Professional Services information:**  
[http://www.iplanet.com/services/professional\\_services\\_3\\_3.html](http://www.iplanet.com/services/professional_services_3_3.html)
- **Sun Enterprise Services for Solaris patches and support:**  
<http://www.sun.com/service/>
- **iPlanet developer information:**  
<http://developer.iplanet.com/>
- **iPlanet learning solutions:**  
<http://www.iplanet.com/learning/index.html>
- **iPlanet product data sheets:**  
<http://www.iplanet.com/products/index.html>

## Related Information

# Introduction

This chapter provides a brief overview of the configuration and administration utilities provided to manage the iPlanet Directory Server.

This chapter is divided into the following sections:

- Overview of Directory Server Management
- Directory Server Configuration
- Directory Server Instance File Reference
- Migrating Directory Server
- Using Directory Server Command-Line Utilities
- Using Directory Server Command-Line Scripts

## Overview of Directory Server Management

iPlanet 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 enterprise-wide directories of users and resources, extranets, and e-commerce applications over the Internet. The Directory Server runs as the `ns-slapd` process or service (`slapd` on Windows NT) on your machine. The server manages the directory databases and responds to client requests.

You can perform most Directory Server administrative tasks through iPlanet Console, the graphical user interface provided with the iPlanet Directory Server. For information on the general use of the iPlanet Console, see *Managing Servers with iPlanet Console*, and for details of how to use the console to manage the Directory Server in particular, see *iPlanet Directory Server Administrator's Guide*.

This reference manual deals with the other methods of managing the Directory Server, namely altering the server configuration attributes via the command line and using the command-line utilities.

## Directory Server Configuration

The format and method for storing configuration information for iPlanet Directory Server 5.1 mark a significant change from previous versions of the Directory Server. A full explanation of these changes and a listing for all server attributes can be found in Chapter 2, “Core Server Configuration Reference” and Chapter 3, “Plug-in Implemented Server Functionality Reference”.

## Directory Server Instance File Reference

Having an overview of the files and configuration information stored in each instance of Directory Server is useful, as this helps administrators understand the changes or absence of changes in the course of directory activity. From a security standpoint, such an overview can help customers detect errors and intrusion as they know what kind of changes to expect and what will be considered abnormal behavior. See Chapter 4, “Server Instance File Reference” for further information.

## Migrating Directory Server

In earlier versions of the Directory Server, all configuration parameters were stored in text files. However, in iPlanet Directory Server 5.1, configuration attributes are now stored as LDAP configuration entries in the `dse.ldif` file. The mapping of configuration parameters in Directory Server 4.1, 4.11, and 4.12 to the corresponding configuration entries and attributes in iPlanet Directory Server 5.1 is described in Chapter 6, “Migration from Earlier Versions”.

## Using Directory Server Command-Line Utilities

Directory Server comes with a set of configurable command-line utilities that you can use to search and modify entries in the directory and administer the server. Chapter 7, “Command-Line Utilities” describes these command-line utilities and contains information on where the utilities are stored and how to access them. In

In addition to these command-line utilities, Directory Server also provides `ns-slapd` and `slapd.exe` command-line utilities for performing directory operations as described in Appendix A, “Using the `ns-slapd` and `slapd.exe` Command-Line Utilities”.

## 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 8, “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 iPlanet Directory Server 5.1 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 via LDAP while it is still running, and avoids having to shut it down.

This chapter gives details of how the configuration is organized, how to alter it, and provides an alphabetical reference for all attributes. The material is divided into the following sections:

- Server Configuration - Overview
- Accessing and Modifying Server Configuration
- Core Server Configuration Attributes Reference
- Configuration Quick Reference Tables

## Server Configuration - Overview

When you install the iPlanet Directory Server 5.1, 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 in LDIF format: `dse.ldif`. This `dse.ldif` file contains all of the server configuration information. It is worth noting that 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 iPlanet Directory Server 5.1 are

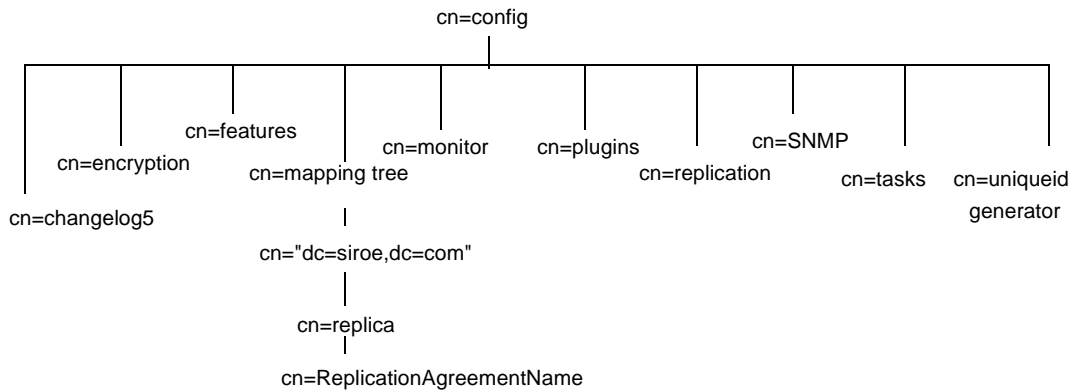
designed as discrete modules that plug into the core server. The details of the internal configuration for each plug-in are contained in separate entries under `cn=plugins`, `cn=config`. For example, the configuration of the Telephone Syntax plug-in is contained in the entry:

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

Similarly, database-specific configuration is stored under:

```
cn=ldbm database,cn=plugins,cn=config and cn=chaining
database,cn=plugins,cn=config
```

The following diagram shows how the configuration data fits within the `cn=config` Directory Information Tree.



This overview is divided into the following sections:

- LDIF Configuration Files - Location
- Schema Configuration Files - Location
- December 2001
- Migration of Pre-Directory Server 5.1 Configuration Files to LDIF Format



## LDIF Configuration Files - Location

The Directory Server configuration data is automatically output to files in LDIF format that are located in the following directory by default:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/config</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/config</code>

where *serverID* is the server identifier that you defined when you installed your Directory Server. In this chapter, all examples use `phonebook` for the server identifier where appropriate.

## Schema Configuration Files - Location

Schema configuration is also stored in LDIF format and these files are located in the following directory:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/config/schema</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/config/schema</code>

For a full list of the LDIF configuration files that are supplied with Directory Server, see Table 2-7 under Configuration Quick Reference Tables at the end of this chapter.

## 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, and directory specific entries related to the database, also created by the directory at server startup. The file includes the Root DSE (named by `"`) and the entire contents of `cn=config`. When the server generates the `dse.ldif` file, it lists the entries in hierarchical order. It does so in the order that the entries appear in the directory under `cn=config`.

This section provides an overview of configuration attributes, plug-in functionality configuration, database configuration, and index configuration.

### 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 cod example gives an example of part of the `dse.ldif` file for a Directory Server and shows, amongst other things, that schema checking has been turned *on*. This is represented by the attribute `nsslapd-schemacheck`, which takes the value `on`.

**Code Example 2-1** Extract of `dse.ldif` File

```
dn: cn=config
objectclass: top
objectclass: extensibleObject
objectclass: nsslapdConfig
nsslapd-accesslog-logging-enabled: on
nsslapd-enquote-sup-oc: on
nsslapd-localhost: phonebook.siroe.com
nsslapd-errorlog: installDir/slapd-phonebook/logs/errors
nsslapd-schemacheck: on
nsslapd-store-state-info: on
nsslapd-port: 389
nsslapd-localuser: nobody
...
```

## 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 example shows an example of the configuration entry for a plug-in, in this case the Telephone Syntax plug-in.

**Code Example 2-2** Configuration Entry for Telephone Syntax Plug-in

```
dn: cn=Telephone Syntax,cn=plugins,cn=config
objectclass: top
objectclass: nsSlapdPlugin
objectclass: extensibleObject
cn: Telephone Syntax
nsslapd-pluginPath: installDir/lib/syntax-plugin-in.so
nsslapd-pluginInitfunc: tel_init
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. You can 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 iPlanet Directory Server 5.1, general plug-in configuration information, the plug-in configuration attribute reference, and a list of plug-ins requiring restart see Chapter 3, “Plug-in Implemented Server Functionality Reference”.

## Configuration of Databases

The `cn=NetscapeRoot` and `cn=UserRoot` subtrees contain configuration data for the databases containing the `o=NetscapeRoot` and `o=UserRoot` suffixes respectively. The `cn=NetscapeRoot` subtree contains the configuration data used by the iPlanet Administration Server for authentication and all actions that cannot be performed through LDAP (such as start/stop). The `cn=UserRoot` subtree contains all the configuration data for the first user-defined database created during server installation. The `cn=UserRoot` subtree is called `UserRoot` by default. However, this is not hard-coded, and, given the fact that there will be multiple database instances, this name will be changed and defined by the user when new databases are added.

## Configuration of Indexes

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

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

For more information regarding indexes in general, see the *iPlanet Directory Server Administrator's Guide* and for information regarding the index configuration attributes, see “Database Attributes Under `cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config`” on page 153. The attributes are presented here because this node is the first to appear in the representation of the configuration attributes based on the `cn=config` information tree.

## Migration of Pre-Directory Server 5.1 Configuration Files to LDIF Format

The iPlanet Directory Server 5.1 only recognizes configuration files that are in LDIF format, which means that the `slapd.conf` and `slapd.ldbm.conf` configuration files from 4.x versions of Netscape Directory Server must be converted to LDIF format. Netscape Directory Server 4.x configurations can be migrated to the new LDIF format using the tool `migrateInstance5` tool. For more information, see Chapter 5, “Migrating From Previous Versions” in the *iPlanet Directory Server Installation Guide* and the *Innosoft Distributed Directory Server Transition Guide*.

## 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 on the types of modification that can be made and discusses attributes that require the server to be restarted for changes to take effect. This section has been divided into the following parts:

- Access Control For Configuration Entries
- Changing Configuration Attributes

### 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`. Code Example 2-3 on page 29 shows an example of these default ACIs.

**Code Example 2-3** Default ACIs in `dse.ldif`

```

aci: (targetattr = "*")(version 3.0; acl "Configuration Administrators Group";
  allow (all)
  groupdn = "ldap:///cn=Configuration Administrators,ou=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=Siroe,dc=com");
aci: (targetattr = "*")(version 3.0; acl "SIE Group";
  allow(all)
  groupdn = "ldap:///cn=slapd-phonebook, cn=Netscape Directory Server,
  cn=Server Group, cn=phonebook.siroe.com, dc=Siroe,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, who has the uid admin that can be configured at installation time
- Members of local Directory Administrators Group
- The local Directory Administrator (root DN)
- The SIE (Server Instance Entry) Group that is usually assigned using the Set Access Permissions from the main topology view in the main console.

For more information on Access Control, see Chapter 5 of the *iPlanet Directory Server Administrator's Guide*.

## Changing Configuration Attributes

You can view and change server attribute values in one of three ways: by using LDAP through iPlanet Console, by performing `ldapsearch` and `ldapmodify` commands, or by manually editing the `dse.ldif` file.

---

**NOTE** If you edit the `dse.ldif` file, you must stop the server beforehand, otherwise your changes will be lost. Editing the `dse.ldif` file is recommended only for changes to attributes which cannot be altered dynamically. For further information, see “Configuration Changes Requiring Server Restart,” on page 107.

---

The following sections describe how to modify entries using LDAP (both via iPlanet Console and over the command line), the restrictions to modifying entries, the restrictions to modifying attributes and the configuration changes requiring restart.

## Modifying Configuration Entries Using LDAP

The configuration entries in the directory can be searched and modified using LDAP, either via the iPlanet 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 that you can make the changes while the server is running. You must remember to specify the port number when modifying configuration entries as the server is not necessarily running on port 389. For further information see Chapter 4, “Managing Directory Entries” in the *iPlanet Directory Server Administrator’s Guide*. However, certain changes do require the server to be restarted before they are taken into account. For further information, see “Configuration Changes Requiring Server Restart,” on page 107.

---

**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 iPlanet 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
```

where *bindDN* is the DN chosen for the Directory Manager when the server was installed and *password* is the password chosen for Directory Manager. For more information on using `ldapsearch` see Chapter 7, “Command-Line Utilities.”

Previously we saw an example of the configuration entry for the Telephone Syntax plug-in where the plug-in was enabled. If you want to disable this feature you can use the following series of commands to implement this change.

#### Code Example 2-4 Disabling the Telephone Syntax Plug-in

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

## Restrictions to Modifying Configuration Entries

Certain restrictions apply when modifying server entries:

- The `dse.ldif cn=monitor` entry and its child entries are read-only and cannot be modified.

## Restrictions to Modifying Configuration Attributes

Certain restrictions apply when modifying server attributes:

- If an attribute is added to `cn=config`, the server will ignore it.
- If an invalid value is entered for an attribute, the server will ignore it.
- Since `ldapdelete` is used for deleting entire entries, you should use `ldapmodify` if you want to remove an attribute from an entry.

## Configuration Changes Requiring Server Restart

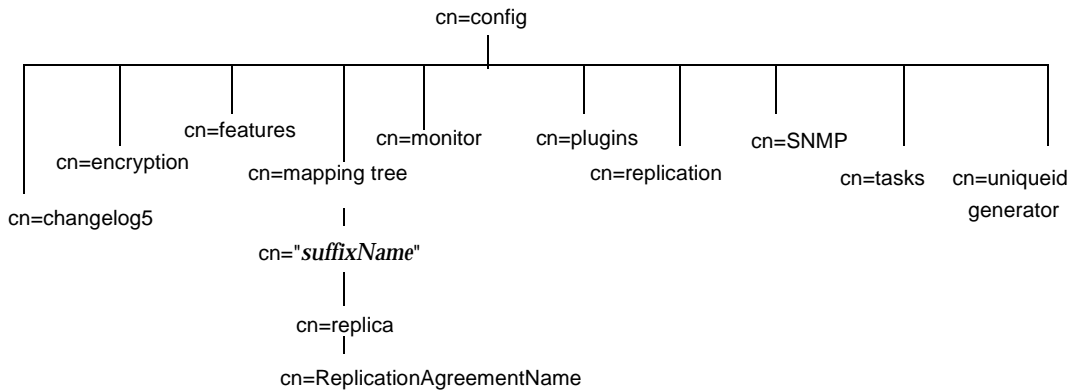
Some configuration attributes cannot be altered dynamically while the server is running. In these cases the server needs to be shut down and restarted for the changes to take effect. The modifications should be made either through the Directory Server Console or by manually editing the `dse.ldif` file. Table 2-8 under Configuration Quick Reference Tables at the end of this chapter contains a list of these attributes.

# Core Server Configuration Attributes Reference

This section guides you through all the core server functionality configuration attributes. For server functionality implemented via plug-ins, see the section “Configuration Quick Reference Tables,” on page 104. For implementing your own server functionality, contact iPlanet Professional Services.

For information on where to find the server configuration and how to change it, see “Server Configuration - Overview,” on page 23 and “Accessing and Modifying Server Configuration,” on page 28. For a list of the server features that are plug-ins and the attributes that apply to them, see Table 2-1, under Configuration Quick Reference Tables at the end of this chapter.

The configuration information which is stored in the `dse.ldif` file is organized as an information tree under the general configuration entry `cn=config` as shown below:



The list of configuration tree nodes covered in this section is as follows:

- `cn=config`
- `cn=changelog5`
- `cn=encryption`
- `cn=features`
- `cn=mapping tree`
- `cn=monitor`
- `cn=replica`



- `cn=replication`
- `cn=SNMP`
- `cn=tasks`
- `cn=uniqueid generator`

The `cn=plugins` node is covered in the “Configuration Quick Reference Tables” section. We arrange the attributes alphabetically and provide a full description for each, giving the DN of its directory entry, its default value, the valid range of values, and an example of its use.

---

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

---

## cn=config

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

### nsIdleTimeout (Idle Timeout)

Specifies the amount of time in seconds after which an idle LDAP client connection is closed by the server. A value of 0 indicates that the server will never close idle connections.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	0 to the maximum 32 bit integer value (2147483647)
<b>Default Value</b>	0
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsIdleTimeout: 0</code>

## nsslapd-accesscontrol (Enable Access Control)

Turns access control on and off. If this attribute has a value `off`, any valid bind attempt (including an anonymous bind) results in full access to all information stored in the Directory Server.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-accesscontrol: off</code>

## nsslapd-accesslog (Access Log)

Specifies the path and filename of the log used to record each database access. The following information is recorded in the log file by default:

- IP address of the client machine that accessed the database
- operations performed (for example, search, add, modify)
- result of the access (for example, the number of entries returned)

For more information on turning access logging off, see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

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

**Table 2-1** Possible Value Combinations of Access Log Attributes

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

**Table 2-1** Possible Value Combinations of Access Log Attributes

Attribute Pair	Value Pair	Logging Status
nsslapd-accesslog-logging-enabled	off	Disabled
nsslapd-accesslog	<i>filename</i>	

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	Any valid filename.
<b>Default Value</b>	<i>installDir</i> /slapd- <i>serverID</i> /logs/access
<b>Syntax</b>	DirectoryString
<b>Solaris 9 Example</b>	nsslapd-accesslog: /var/ds5/slapd- <i>serverID</i> /logs/access
<b>Other Platform Example</b>	nsslapd-accesslog: /usr/iplanet/servers/slapd- <i>serverID</i> /logs/access

## nsslapd-accesslog-level

Controls what is logged to the access log.

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	0—No access logging 4—Logging for internal access operations 256—Logging for access to an entry 512—Logging for access to an entry and referrals.  These values can be added together to provide you with the exact type of logging you require, for example 516 (4 + 512) to obtain internal access operation, entry access and referral logging.
<b>Default Value</b>	256
<b>Syntax</b>	Integer
<b>Example</b>	nsslapd-accesslog-level: 256

## nsslapd-accesslog-list

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

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>N/A</code>
<b>Default Value</b>	<code>None</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-accesslog-list:accesslog2,accesslog3</code>

## nsslapd-accesslog-logbuffering (Log Buffering)

When set to `off`, the server writes all access log entries directly to disk.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-accesslog-logbuffering: off</code>

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

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.

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

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

Specifies the unit for the `nsslapd-accesslog-logexpirationtime` attribute. If the unit is unknown by the server, the log will never expire.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>month   week   day</code>
<b>Default Value</b>	<code>month</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-accesslog-logexpirationtimeunit: week</code>

## 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 filename 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 filename. Table 2-1 on page 34 lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of access logging.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-accesslog-logging-enabled: off</code>

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

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 3 different log files (access log, audit log, and error log) maintained by the Directory Server, each of which will consume disk space. Compare these considerations to the total amount of disk space that you want to be used by the access log.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>-1</code>   1 to the maximum 32 bit integer value (2147483647)
<b>Default Value</b>	500 (A value of -1 means that the disk space allowed to the access log is unlimited in size).
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-accesslog-logmaxdiskspace: 200</code>

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

Specifies 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 log is deleted until enough disk space is freed to satisfy this attribute

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

### `nsslapd-accesslog-logrotationtime` (Access Log Rotation Time)

Specifies the time between access log file rotations. The access log will be 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.

For performance reasons, it is not recommended to specify no log rotation as the log will grow indefinitely. However, you have two ways of specifying this. Either you set the `nsslapd-accesslog-maxlogsperdir` attribute value to 1 or 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 “`nsslapd-accesslog-maxlogsperdir` (Access Log Maximum Number of Log Files)” on page 40 for more information.

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

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

Specifies the units for the `nsslapd-accesslog-logrotationtime` attribute.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>month   week   day   hour   minute</code>
<b>Default Value</b>	<code>day</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-accesslog-logrotationtimeunit: week</code>

### `nsslapd-accesslog-maxlogsize` (Access Log Maximum Log Size)

Specifies the maximum access log size in megabytes. When this value is reached, the access log is rotated. That is, the server starts writing log information to a new log file. If you set the `nsslapd-accesslog-maxlogsperdir` attribute 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 3 different log files (access log, audit log, and error log) maintained by the Directory Server, each of which will consume disk space. Compare these considerations to the total amount of disk space that you want to be used by the access log.

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

### `nsslapd-accesslog-maxlogspdir` (Access Log Maximum Number of Log Files)

Specifies the total number of access logs that can be contained in the directory where the access log is stored. If you are using log file rotation, 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 on this attribute, then the oldest version of the log file is deleted. For performance reasons, it is not recommended that you set this value to 1, as the server will not rotate the log and it will grow indefinitely.

If the value for this attribute is higher than 1, then you need to check the `nsslapd-accesslog-logrotationtime` attribute to establish whether or not log rotation is specified. If the `nsslapd-accesslog-logrotationtime` attribute has a value of `-1`, there is no log rotation. For more information, see “`nsslapd-accesslog-logrotationtime` (Access Log Rotation Time)” on page 38.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	1 to the maximum 32 bit integer value (2147483647)
<b>Default Value</b>	<code>10</code>
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-accesslog-maxlogspdir: 10</code>

### `nsslapd-attribute-name-exceptions`

Allows non-standard characters in attribute names to be used for backwards compatibility with older servers.



<b>Entry DN</b>	cn=config
<b>Valid Range</b>	on   off
<b>Default Value</b>	off
<b>Syntax</b>	DirectoryString
<b>Example</b>	nsslapd-attribute-name-exceptions: on

## nsslapd-auditlog (Audit Log)

Specifies the pathname and filename of the log used to record changes made to each database.

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	Any valid filename
<b>Default Value</b>	<i>installDir</i> /slapd- <i>serverID</i> /logs/audit
<b>Syntax</b>	DirectoryString
<b>Solaris 9 Example</b>	nsslapd-auditlog: /var/ds5/slapd- <i>serverID</i> /logs/audit
<b>Other Platform Example</b>	nsslapd-auditlog: /usr/iplanet/servers/slapd- <i>serverID</i> /logs/audit

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

**Table 2-2** Possible Value Combinations of Audit Log Attributes

Attribute Pair	Value Pair	Logging Status
nsslapd-auditlog-logging-enabled nsslapd-auditlog	on empty string	Disabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	on <i>filename</i>	Enabled

**Table 2-2** Possible Value Combinations of Audit Log Attributes

Attribute Pair	Value Pair	Logging Status
nsslapd-auditlog-logging-enabled nsslapd-auditlog	off empty string	Disabled
nsslapd-accesslog-logging-enabled nsslapd-auditlog	off <i>filename</i>	Disabled

### nsslapd-auditlog-list

Provides a list of audit log files.

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	N/A
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	nsslapd-auditlog-list: auditlog2,auditlog3

### nsslapd-auditlog-logexpirationtime (Audit Log Expiration Time)

Specifies the maximum age that a log file can 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.

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

### nsslapd-auditlog-logexpirationtimeunit (Audit Log Expiration Time Unit)

Specifies the units for the `nsslapd-auditlog-logexpirationtime` attribute. If the unit is unknown by the server, the log will never expire.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>month   week   day</code>
<b>Default Value</b>	<code>week</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-auditlog-logexpirationtimeunit: day</code>

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

Turns audit logging on and off.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-auditlog-logging-enabled: off</code>

For audit logging to be enabled this attribute must have a valid path and file name and the `nsslapd-auditlog-logging-enabled` configuration attribute must be switched to `on`. Table 2-2 on page 41 lists the four possible combinations of values for these two configuration attributes and their outcome in terms of disabling or enabling of audit logging.

### `nsslapd-auditlog-logmaxdiskspace` (Audit Log Maximum Disk Space)

Specifies 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 will consume disk space. Compare these considerations with the total amount of disk space that you want to be used by the audit log.

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

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

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

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

### nsslapd-auditlog-logrotationtime (Audit Log Rotation Time)

Specifies the time between audit log file rotations. The audit log will be 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 you set the `nsslapd-auditlog-maxlogsperdir` attribute to 1, the server ignores this attribute.

For performance reasons, it is not recommended to specify no log rotation, as the log will grow indefinitely. However, you have two ways of specifying this. Either you set the `nsslapd-auditlog-maxlogsperdir` attribute value to 1 or 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 “`nsslapd-auditlog-maxlogsperdir` (Audit Log Maximum Number of Log Files)” on page 46 for more information.

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

### `nsslapd-auditlog-logrotationtimeunit` (Audit Log Rotation Time Unit)

Specifies the units for the `nsslapd-auditlog-logrotationtime` attribute.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>month</code>   <code>week</code>   <code>day</code>   <code>hour</code>   <code>minute</code>
<b>Default Value</b>	<code>week</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-auditlog-logrotationtimeunit: day</code>

### `nsslapd-auditlog-maxlogsize` (Audit Log Maximum Log Size)

Specifies the maximum audit log size in megabytes. When this value is reached, the audit log is rotated. That is, the server starts writing log information to a new log file. If you set `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 3 different log files (access log, audit log, and error log) maintained by the Directory Server, each of which will consume disk space. Compare these considerations to the total amount of disk space that you want to be used by the audit log.

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

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

Specifies the total number of audit logs that can be contained in the directory where the audit log is stored. If you are using log file rotation, then 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 you accept this default, the server will not rotate the log and it will grow indefinitely.

If the value for this attribute is higher than 1, then you need to check the `nsslapd-auditlog-logrotationtime` attribute to establish whether or not log rotation is specified. If the `nsslapd-auditlog-logrotationtime` attribute has a value of `-1`, then there is no log rotation. See “`nsslapd-auditlog-logrotationtime` (Audit Log Rotation Time)” on page 44 for more information.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid range</b>	1 to the maximum 32 bit integer value (2147483647)
<b>Default value</b>	1
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-auditlog-maxlogsperdir: 10</code>

### `nsslapd-certmap-basedn` (Certificate Map Search Base)

This attribute can be used when client authentication is performed using SSL certificates in order to avoid limitation of the security subsystem certificate mapping, configured in `certmap.conf`. Depending on the `certmap.conf` configuration, the certificate mapping may be done using a directory subtree

search based at the root DN. Note that 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. For further information, see Chapter 11, “Managing SSL” in the *iPlanet Directory Server Administrator’s Guide*.

## nsslapd-config

This read-only attribute is the config DN.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any valid config DN.
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-config:cn=config</code>

## nsslapd-ds4-compatible-schema

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

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

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

Controls whether the quoting in the `objectclasses` attributes contained in the `cn=schema` entry conforms to the quoting specified by internet draft RFC 2252. By default, the Directory Server places single quotes around the superior object class identified on the `objectclasses` attributes contained in `cn=schema`. RFC 2252 indicates that this value should not be quoted.

That is, the Directory Server publishes `objectclasses` attributes in the `cn=schema` entry as follows:

```
objectclasses: ( 2.5.6.6 NAME 'person' DESC 'Standard ObjectClass'
SUP 'top' MUST ( objectclass $ sn $ cn ) MAY ( aci $ description $
seealso $ telephonenumber $ userpassword ) )
```

However, RFC 2252 indicates that this attribute should be published as follows:

```
objectclasses: ( 2.5.6.6 NAME 'person' DESC 'Standard ObjectClass'
SUP top MUST ( objectclass $ sn $ cn ) MAY ( aci $ description $
seealso $ telephonenumber $ userpassword ) )
```

Notice the absence of single quotes around the word `top`.

Turning this attribute on means that the Directory Server Resource Kit LDAP clients will no longer function, as they require the schema as defined in RFC 2252.

Turning this attribute off causes the Directory Server to conform to RFC 2252, but doing so may interfere with some earlier LDAP clients. Specifically, any client written using the iPlanet LDAP SDK for Java 4.x will no longer be able to correctly read and modify schema. This includes the 4.x version of the iPlanet Console. Please note that turning this attribute on or off does not affect the 5.0 iPlanet Console.

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

## nsslapd-errorlog (Error Log)

Specifies the pathname 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 will contain informative conditions such as:

- server startup and shutdown times
- port number the server uses

This log will contain differing amounts of information depending on the current setting of the Log Level attribute. See “nsslapd-errorlog-level (Error Log Level),” on page 49 for more information.



<b>Entry DN</b>	cn=config
<b>Valid Range</b>	Any valid filename
<b>Default Value</b>	<i>installDir</i> /slapd- <i>serverID</i> /logs/error
<b>Syntax</b>	DirectoryString
<b>Solaris 9 Example</b>	nsslapd-errorlog: /var/ds5/slapd- <i>serverID</i> /logs/error
<b>Other Platform Example</b>	nsslapd-errorlog: /usr/iplanet/servers/slapd- <i>serverID</i> /logs/error

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

**Table 2-3** Possible Value Combinations of Error Log Attributes

Attribute Pair	Value Pair	Logging Status
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

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

Specifies the level of logging to be used by the Directory Server. The log level is additive; that is, specifying a value of 3 causes both levels 1 and 2 to be performed.

To turn logging off, remove the `nsslapd-errorlog-level` attribute from `dse.ldif` and restart the Directory Server.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<p>1 = Trace function calls. Logs a message when the server enters and exits a function.</p> <p>2 = Debug Packet handling</p> <p>4 = Heavy trace output debugging</p> <p>8 = Connection management</p> <p>16 = Print out packets sent/received</p> <p>32 = Search filter processing</p> <p>64 = Config file processing</p> <p>128 = Access control list processing</p> <p>2048 = Log entry parsing debugging</p>
<b>Valid Range</b>	<p>4096 = Housekeeping thread debugging</p> <p>8192 = Replication debugging</p> <p>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.</p> <p>32768 = Database cache debugging.</p> <p>65536 = Server plug-in debugging. It writes an entry to the log file when a server plug-in calls <code>slapi-log-error</code>.</p>
<b>Default Value</b>	Logging is turned off (the <code>nsslapd-errorlog-level</code> attribute is not included in the <code>dse.ldif</code> file).
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-errorlog-level: 8192</code>

### `nsslapd-errorlog-list`

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

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	N/A
<b>Default Value</b>	None

<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-errorlog-list:errorlog2,errorlog3</code>

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

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 (day, week, month, and so forth) are given by the `nsslapd-errorlog-logexpirationtimeunit` attribute.

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

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

Specifies the units for the `nsslapd-errorlog-logexpirationtime` attribute. If the unit is unknown by the server, the log will never expire.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>month   week   day</code>
<b>Default Value</b>	<code>month</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-errorlog-logexpirationtimeunit: week</code>

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

Turns error logging on and off.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>

<b>Default Value</b>	on
<b>Syntax</b>	DirectoryString
<b>Example</b>	nsslapd-errorlog-logging-enabled: on

### nsslapd-errorlog-logmaxdiskspace (Error Log Maximum Disk Space)

Specifies 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 3 different log files (access log, audit log, and error log) maintained by the Directory Server, each of which will consume disk space. Compare these considerations to the total amount of disk space that you want to be used by the error log.

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	-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.
<b>Default Value</b>	500
<b>Syntax</b>	Integer
<b>Example</b>	nsslapd-errorlog-logmaxdiskspace: 500

### nsslapd-errorlog-logminfreediskspace (Error Log Minimum Free Disk Space)

Specifies 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.

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

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

Specifies the time between error log file rotations. The error log will be 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.

For performance reasons, it is not recommended to specify no log rotation as the log will grow indefinitely. However, you have two ways of specifying this. Either you set the `nsslapd-errorlog-maxlogsperdir` attribute value to 1 or 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 “`nsslapd-errorlog-maxlogsperdir` (Maximum Number of Error Log Files)” on page 54 for more information.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	-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).
<b>Default Value</b>	1
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-errorlog-logrotationtime: 100</code>

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

Specifies the units for `nsslapd-errorlog-logrotationtime` (Error Log Rotation Time). If the unit is unknown by the server, the log will never expire.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>month   week   day   hour   minute</code>
<b>Default Value</b>	<code>week</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-errorlog-logrotationtimeunit: day</code>

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

Specifies the maximum error log size in megabytes. When this value is reached, the error log is rotated. That is, the server starts writing log information to a new log file. If you set `nsslapd-errorlog-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 3 different log files (access log, audit log, and error log) maintained by the Directory Server, each of which will consume disk space. Compare these considerations to the total amount of disk space that you want to be used by the error log.

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

## nsslapd-errorlog-maxlogsperdir (Maximum Number of Error Log Files)

Specifies the total number of error logs that can be contained in the directory where the error log is stored. If you are using log file rotation, then 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 you accept this default, the server will not rotate the log and it will grow indefinitely.

If the value for this attribute is higher than 1, then you need to check the `nsslapd-errorlog-logrotationtime` attribute to establish whether or not log rotation is specified. If the `nsslapd-errorlog-logrotationtime` attribute has a value of -1 then there is no log rotation. See “`nsslapd-errorlog-logrotationtime` (Error Log Rotation Time)” on page 53 for more information.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	1 to the maximum 32 bit integer value (2147483647)
<b>Default Value</b>	1

<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-errorlog-maxlogspendir: 10</code>

### nsslapd-groupevalnestlevel

Specifies the number of levels of nesting that the access control system will perform for group evaluation.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	0 to 5
<b>Default Value</b>	5
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-groupevalnestlevel:5</code>

### nsslapd-instancedir (Instance Directory)

Specifies the full path to the directory where this server instance is installed. The hostname is the default *serverID* given at installation time.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any valid file path.
<b>Default Value</b>	<code>installDir/slapd-serverID</code>
<b>Syntax</b>	DirectoryString
<b>Solaris 9 Example</b>	<code>nsslapd-instancedir: /var/ds5/slapd-phonebook</code>
<b>Other Platform Example</b>	<code>nsslapd-instancedir: /usr/iplanet/servers/slapd-phonebook</code>

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

Specifies 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.

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

### nsslapd-lastmod (Track Modification Time)

Specifies whether the Directory Server maintains the modification attributes for Directory Server entries. 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.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-lastmod: off</code>

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

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). Provide the hostname which corresponds to the IP interface you want to specify as a value for this attribute. Directory Server will only respond to requests sent to the interface that corresponds to the hostname provided on this attribute.



<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any hostname
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-listenhost: <i>host_name</i></code>

### nsslapd-localhost (Local Host)

This read-only attribute specifies the host machine on which the Directory Server runs.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any fully qualified hostname.
<b>Default Value</b>	Hostname of installed machine.
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-localhost:phonebook.siroe.com</code>

### nsslapd-localuser (Local User)

UNIX installations only. Specifies the user under which the Directory Server runs. The group under which the user runs is derived from this attribute, by examining the groups that the user is a member of. Should the user change, then all the files in the installation directory need to be owned by this user.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any valid user on the local UNIX machine.
<b>Default Value</b>	To run as the same user who started the Directory Server.
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-localuser: nobody</code>

## 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 the entry in the request is larger than two megabytes, then the add request is denied. Care should be taken when changing this attribute and we recommend contacting iPlanet Professional Services before doing so.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	0 - 2GB (2,147,483,647 bytes) where a value of 0 indicates that the default value should be used.
<b>Default Value</b>	2097152
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-maxbersize: 2097152</code>

## nsslapd-maxdescriptors (Maximum File Descriptors)

Not applicable to directory installations on NT and AIX.

This attribute sets the maximum, platform-dependent number of file descriptors that the Directory Server will try to use. A file descriptor is used whenever a client connects to the server. It is also used for some server activities such as index maintenance. The number of available file descriptors for TCP/IP connections is the total for the `nsslapd-maxdescriptors` attribute minus the number of file descriptors used by the server for non-client connections, such as index management and managing replication, as specified in the `nsslapd-reservedescriptors` attribute. (see “`nsslapd-reservedescriptors` (Reserved File Descriptors)” on page 62).

The number that you specify here should not be greater than the total number of file descriptors that your operating system allows the `ns-slapd` process to use. This number will differ depending on your operating system. Some operating systems allow you to configure the number of file descriptors available to a process. See your operating system documentation for details on file descriptor limits and configuration. It is worth noting that the included `idsktune` program can be used to suggest changes to the system kernel or TCP/IP tuning attributes, including

increasing the number of file descriptors if necessary. You should consider increasing 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
```

---

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

---

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	1 to 65535
<b>Default Value</b>	1024
<b>Syntax</b>	Integer
<b>Example</b>	nsslapd-maxdescriptors: 1024

### nsslapd-maxthreadspconn (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, you should use the default value. For situations where a client binds and simultaneously issues many requests, you should increase this value to allow each connection enough resources to perform all the operations. This attribute is not available from the server console.

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	1 to maximum threadnumber
<b>Default Value</b>	5
<b>Syntax</b>	Integer
<b>Example</b>	nsslapd-maxthreadspconn: 5

## 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. That is, the sending of data is delayed, in the hope that this will enable additional data to be grouped into one packet of the underlying network MTU size (typically 1500 bytes for Ethernet).

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid range</b>	<code>on   off</code>
<b>Default value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-nagle: off</code>

## nsslapd-plug-in

This read-only attribute lists the syntaxes and matching rules loaded by the server.

## nsslapd-port (Port Number)

TCP/IP port number used for LDAP communications. If you want to run SSL/TLS over this port, you can do so through 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. On UNIX systems, specifying a port number of less than 1024 requires the Directory Server to run as root.

If you are changing the port number for a configuration directory, you must also update the corresponding Server Instance Entry in the configuration directory. Please note that you need to restart the server for the port number change to be taken into account.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>1 to 65535</code>
<b>Default Value</b>	<code>389</code>
<b>Syntax</b>	<code>Integer</code>
<b>Example</b>	<code>nsslapd-port: 389</code>

## nsslapd-privatenamespaces

Contains the list of the private naming contexts `cn=config`, `cn=schema` and `cn=monitor`.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>cn=config</code> , <code>cn=schema</code> and <code>cn=monitor</code>
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-privatenamespaces: cn=config</code>

## nsslapd-readonly (Read Only)

Specifies whether the whole server is in read-only mode, meaning that neither data in the database(s) 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.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on</code>   <code>off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-readonly: off</code>

## nsslapd-referral (Referral)

This multi valued attribute specifies the LDAP URL(s) 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, suppose the database contains only the entries:

```
ou=People, dc=siroe,dc=com
```

but the request is for:

```
ou=Groups, dc=siroe,dc=com
```

In this case, the referral is returned so the client may the corresponding directory for the requested entry. Although only one referral is allowed per Directory Server instance, this referral can have multiple values.

---

**NOTE** If you want to use SSL and TLS communications, the Referral attribute should be in the following form:

`ldaps://serverHost`

Start TLS does not support referrals.

---

For more information on managing referrals, see Chapter 2, “Configuring Directory Databases” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Valid LDAP URL in the following format: <code>ldap://serverHost</code>
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-referral: ldap://alternate.siroe.com</code>

### nsslapd-referralmode (Referral Mode)

When set, this attribute will send back the referral for *any* request on *any* suffix.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Valid LDAP URL in the following format: <code>ldap://serverHost</code>
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-referralmode: ldap://backup.siroe.com</code>

### nsslapd-reservedescriptors (Reserved File Descriptors)

Not applicable to directory installations on NT and AIX.

This read-only 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 “*nsslapd-maxdescriptors (Maximum File Descriptors)*” on page 58).

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.
- You get error messages reporting that the server is unable to open file descriptors (the actual error message will differ 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 your directory. Therefore, when you increase the value on this attribute, increase the value on the `nsslapd-maxdescriptors` attribute also. Note that you may not be able to increase the `nsslapd-maxdescriptors` value if your server is already using the maximum number of file descriptors that your operating system allows a process to use (see your operating system documentation for details). If this is the case, then reduce the load on your server by causing LDAP clients to search alternative directory replicas.

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

$$\text{nsslapd-reservedescriptor} = 20 + (\text{NumBackends} * 4) + \text{NumGlobalIndexes} + \text{ReplicationDescriptors} + \text{ChainingBackendDescriptors} + \text{PTADescriptors} + \text{SSLDescriptors}$$

where the terms are given in the following table:

**Table 2-4** Terms for computing the value of `nsslapd-reservedescriptor`

Term	Definition
<i>NumldbmBackends</i>	Number of ldbm databases.
<i>NumGlobalIndexes</i>	Total number of configured indexes for all databases including system indexes. By default, there are 8 system indexes and 17 additional indexes per database.

**Table 2-4** Terms for computing the value of `nsslapd-reservedescriptor`

Term	Definition
<i>ReplicationDescriptors</i>	<i>NumSupplierReplicas</i> + 8  Where <i>NumSupplierReplicas</i> is number of replicas in the server that can act as a supplier (hub or master).
<i>ChainingBackendDescriptors</i>	<i>NumChainingBackends</i> * <i>nsOperationConnectionsLimit</i>  Where <i>nsOperationConnectionsLimit</i> is defined in the database link configuration and 10 by default.
<i>PTADescriptors</i>	3 if PTA is configured, 0 if PTA is not configured.
<i>SSLDescriptors</i>	5 (4 files + 1 listen socket) if SSL is configured, 0 if SSL is not configured.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	1 to 65535
<b>Default Value</b>	64
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-reservedescriptors: 64</code>

### `nsslapd-return-exact-case` (Return Exact Case)

Returns the exact case of attribute type names as requested by the client. Some client applications require attribute names to exactly match 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. This attribute is therefore disabled by default. Do not modify it unless you have legacy clients that can check the case of attribute names in results returned from the server.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>



<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-return-exact-case: off</code>

### nsslapd-rootdn (Manager DN)

Specifies the distinguished name of an entry that is not subject to access control restrictions, administrative limit restrictions for operations on the directory or resource limits in general. The attributes `nsslapd-sizelimit`, `nsslapd-timelimit`, and `nsslapd-schemacheck` do not apply to this DN either.

For information on changing the Root DN, see Chapter 4, “Managing Directory Entries” in the *iPlanet Directory Server Administrator’s Guide*

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any valid distinguished name
<b>Default Value</b>	N/A
<b>Syntax</b>	DN
<b>Example</b>	<code>nsslapd-rootdn: cn=Directory Manager</code>

### nsslapd-rootpw (Root Password)

Allows you to specify the password associated with the "Manager DN". When you provide the root password, it will be encrypted according to the encryption method you selected for “`nsslapd-rootpwstoragescheme` (Root Password Storage Scheme)” on page 66. 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. Please note that the example below is what you *view*, *not* what you type.

---

**CAUTION** If you configure a root DN at server installation time, you must also provide a root password. However, it is possible for the root password to be deleted from `dse.ldif` by direct editing of the file. In this situation, the root DN can only obtain the same access to your directory as you allow for anonymous access. Always make sure that a root password is defined in `dse.ldif` when a root DN is configured for your database.

---

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any valid password encrypted by any one of the encryption methods which are described in “passwordStorageScheme (Password Storage Scheme),” on page 77.
<b>Default Value</b>	N/A
<b>Syntax</b>	<code>DirectoryString {encryption_method} encrypted_password</code>
<b>Example</b>	<code>nsslapd-rootpw: {SSHA}9Eko69APCJff</code>

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

Available only from the server console. This attribute indicates the encryption method used for the root password.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any encryption method as described in “passwordStorageScheme (Password Storage Scheme)” on page 77.
<b>Default Value</b>	CLEAR
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-rootpwstoragescheme: SSHA</code>

### nsslapd-schemacheck (Schema Checking)

Specifies whether the database schema will be enforced during entry insertion or modification. 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. You can extend the default schema using the `objectclasses` and attribute types. For information on how to extend your schema using the Directory Server Console, see Chapter 9, “Extending the Directory Schema” in the *iPlanet Directory Server Administrator’s Guide*.

---

**NOTE** Schema checking works by default when database modifications are made using an LDAP client, such as `ldapmodify`, the Directory Server Console, or when importing a database from LDIF using `ldif2db` (`directoryserver ldif2db` on Solaris 9 platforms).

If you turn schema checking off, you will have to verify manually that your entries conform to the schema. If schema checking is turned on, the server sends an error message to inform you of the entries which do not match the schema. Make sure that the attributes and object classes you create in your LDIF statements are both spelled correctly and identified in `dse.ldif`. You will need to create a file in LDIF format in the schema directory or add the elements to `99user.ldif`.

---

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

### `nsslapd-securelistenhost`

Allows multiple Directory Server instances to run on a multihomed machine, using secure SSL / TLS connections (or makes it possible to limit listening to one interface of a multihomed machine). Provide the hostname which corresponds to the IP interface you want to specify as a value for this attribute. Directory Server will only respond to requests sent to the interface that corresponds to the hostname provided on this attribute.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	Any secure hostname.
<b>Default Value</b>	N/A
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-securelistenhost: <i>secure_host_name</i></code>

## nsslapd-securePort (Encrypted Port Number)

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. For UNIX systems, specifying a port number of less than 1024 requires that Directory Server runs as root.

The default value 636 is only used if the server has been configured with a private key and a certificate; otherwise it does not listen on this port.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	1 to 65535
<b>Default Value</b>	636
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-securePort: 636</code>

## nsslapd-security (Security)

Specifies whether the Directory Server is to accept SSL/TLS communications on its encrypted port. If you want secure connections, this attribute should be set to `on`.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on</code>   <code>off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-security: off</code>

## nsslapd-sizelimit (Size Limit)

Specifies 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` will return every matching entry to the client regardless of the number found. To set a no limit value whereby the Directory Server will wait 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 the `dse.ldif` is the same as leaving the attribute blank in the server console, in that it causes no limit to be used. Please note, however, that you cannot specify a negative integer for this field in the server console. You cannot specify a null value in `dse.ldif` either, as it is not a valid integer.

---

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

### nsslapd-threadnumber (Thread Number)

Defines the number of operation threads that the Directory Server will create during startup. The `nsslapd-threadnumber` value should be increased if you have many directory clients performing time-consuming operations such as add or modify. This ensures that there are other threads available for servicing short-lived operations such as simple searches. This attribute is not available from the server console.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	1 to the number of threads supported by your system
<b>Default Value</b>	30
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-threadnumber: 60</code>

### nsslapd-timelimit (Time Limit)

Specifies 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` will return every matching entry to the client regardless of the time it takes. To set a no limit value whereby Directory Server will wait 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. Please note, however, that you cannot specify a negative integer for this field in the server console. You cannot specify a null value in `dse.ldif` either, as it is not a valid integer.

---

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid range</b>	-1 to the maximum 32 bit integer value (2147483647) in seconds
<b>Default value</b>	3600
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-timelimit: 3600</code>

### nsslapd-versionstring

Specifies the server version number.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid range</b>	Any valid server version number.
<b>Default value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-versionstring:iPlanet-Directory/5.1</code>

### passwordChange (Password Change)

Indicates whether users may change their passwords.

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>passwordChange: on</code>

## passwordCheckSyntax (Check Password Syntax)

Indicates whether the password syntax will be 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.

For more information on password policies see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on</code>   <code>off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>passwordCheckSyntax: off</code>

## passwordExp (Password Expiration)

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

For more information on password policies see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on</code>   <code>off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>passwordExp: on</code>



## passwordHistory (Password History)

Enables password history. Password history refers to whether users are allowed to reuse passwords or not. By default, password history is disabled and users can reuse passwords. If you set this attribute to `on`, the directory stores a given number of old passwords and prevents users from reusing any of the stored passwords. You set the number of old passwords the Directory Server stores using the `passwordInHistory` attribute.

For more information on password policies see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>passwordHistory: on</code>

## 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. That is, the Directory Server does not store any old passwords and so users can reuse passwords. You can enable password history by using the `passwordHistory` attribute.

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

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>2 to 24 passwords</code>
<b>Default Value</b>	<code>6</code>
<b>Syntax</b>	<code>Integer</code>
<b>Example</b>	<code>passwordInHistory: 7</code>

## passwordLockout (Account Lockout)

Indicates whether users will be locked out of the directory after a given number of failed bind attempts. By default, users will not be locked out of the directory after a series of failed bind attempts. If you enable account lockout, you can set the number of failed bind attempts after which the user will be locked out using the `passwordMaxFailure` attribute.

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>passwordLockout: off</code>

## passwordLockoutDuration (Lockout Duration)

Indicates the amount of time in seconds during which users will be 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. You enable and disable the account lockout feature using the `passwordLockout` attribute.

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

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

## passwordMaxAge (Password Maximum Age)

Indicates the number of seconds after which user passwords will expire. To use this attribute, you must enable password expiration using the `passwordExp` attribute.

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

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

## passwordMaxFailure (Maximum Password Failures)

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

For more information on password policies see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	1 to maximum integer bind failures
<b>Default Value</b>	3
<b>Syntax</b>	Integer
<b>Example</b>	<code>passwordMaxFailure: 3</code>

## 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) indicates that the user can change the password immediately.

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

### passwordMinLength (Password Minimum Length)

Specifies the minimum number of characters that must be used in Directory Server user password attributes. In general, shorter passwords are easier to crack, so you are recommended to set a password length of at least 6 or 7 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 Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	2 to 512 characters
<b>Default Value</b>	6
<b>Syntax</b>	Integer
<b>Example</b>	<code>passwordMinLength: 6</code>

### 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 Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>passwordMustChange: off</code>

### passwordResetFailureCount (Reset Password Failure Count After)

Indicates the amount of time in seconds after which the password failure counter will be reset. 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 will be 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 Chapter 7, "User Account Management" in the *iPlanet Directory Server Administrator's Guide*.

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

### passwordStorageScheme (Password Storage Scheme)

Specifies the type of encryption used to store Directory Server passwords. Entering the password in `CLEAR` for this attribute indicates that the password will appear in plain text.

The following encryption types are supported by the Directory Server 5.1:

- SSHA (Salted Secure Hash Algorithm) is the recommended method as it is the most secure.
- SHA (Secure Hash Algorithm). This is the method supported by 4.x Directory Servers.
- CRYPT is the UNIX crypt algorithm. It is provided for compatibility with UNIX passwords.

---

**NOTE** You can no longer choose to encrypt passwords 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 Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

### passwordUnlock (Unlock Account)

Indicates whether users will be 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 will be locked indefinitely.

For more information on password policies, see Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config</code>
<b>Valid Range</b>	<code>on</code>   <code>off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>passwordUnlock: off</code>

### passwordWarning (Send Warning)

Indicates the number of seconds before a user’s password expires that the user will receive 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 Chapter 7, “User Account Management” in the *iPlanet Directory Server Administrator’s Guide*.

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

## cn=changelog5

Multi-master replication change log 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:

- “`nsslapd-dbcachesize`,” on page 136
- “`nsslapd-db-checkpoint-interval`,” on page 136
- “`nsslapd-db-circular-logging`,” on page 137
- “`nsslapd-db-durable-transactions`,” on page 138
- “`nsslapd-db-logfile-size`,” on page 141
- “`nsslapd-db-page-size`,” on page 142
- “`nsslapd-cachesize`,” on page 147
- “`nsslapd-cachememsize`,” on page 147

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

It is worth noting that two different types of change logs are maintained by iPlanet Directory Server 5.1. The first type, which is stored here and referred to as *changelog*, is used by multi-master replication; the second change log, which is actually a plug-in and referred to as *retro changelog*, is intended for use by iPlanet Meta Directory. See “Retro Changelog Plug-in” on page 126 of Chapter 3, “Plug-in Implemented Server Functionality Reference” for further information regarding the Retro Changelog Plug-in. Multi-master replication changelog attributes are presented in this section.

### nsslapd-changelogdir

This required attribute specifies the name of the directory in which the change log database will be created. Whenever a change log configuration entry is created it must contain a valid directory or the operation will be rejected. The GUI proposes by default that this database be stored under:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/changelogdb</code>
<b>Other platforms</b>	<code>/usr/ipplanet/servers/slapd-<i>serverID</i>/changelogdb</code>

---

**NOTE** For performance reasons, it is recommended that you store this database on a different physical disk.

---

**Entry DN** `cn=changelog5,cn=config`

**Valid Range** Any valid path to the directory storing the changelog

**Default Value** None

**Syntax** DirectoryString

**Example** `nsslapd-changelogdir:  
/usr/myhome/slapd-local/changelogdb`

### nsslapd-changelogmaxage (Max Changelog Age)

Specifies the maximum age of any entry in the change log. The change log 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 will be removed. If this attribute is absent, there is no age limit on change log records. For information on the change log, see “nsslapd-changelogdir.”

**Entry DN** `cn=changelog5,cn=config`

**Valid Range** 0 (meaning that entries are not removed according to their age) to maximum integer (2147483647)

**Default Value** 0

**Syntax** DirectoryString *IntegerAgeID*  
where AgeID is “s” for seconds, “m” for minutes, “h” for hours, “d” for days, or “w” for weeks.

**Example** `nsslapd-changelogmaxage: 30d`

### nsslapd-changelogmaxentries (Max Changelog Records)

Specifies the maximum number of records the change log may contain. If this attribute is absent, there is no maximum number of records the change log can contain. For information on the change log, see “nsslapd-changelogdir,” on page 79.



<b>Entry DN</b>	<code>cn=changelog5,cn=config</code>
<b>Valid Range</b>	0 (meaning that the only maximum limit is the disk size) to maximum integer (2147483647)
<b>Default Value</b>	0
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-changelogmaxentries: 5000</code>

## 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. For encryption related 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. Encryption configuration attributes are presented in this section.

### nssslsessiontimeout

Specifies the lifetime duration of an SSL session for both SSLv2 and SSLv3. The minimum timeout value is 5 seconds and if you enter a value below this, then it is automatically replaced by 5 seconds. Values outside the valid ranges are replaced by the default value of 100 seconds (SSLv2).

<b>Entry DN</b>	<code>cn=encryption,cn=config</code>
<b>Valid Range</b>	SSLv2 5 seconds to 100 seconds SSLv3 5 seconds to 24 hours
<b>Default Value</b>	0 which stands for 100 seconds in you are running SSLv2 and 24 hours if you are running SSLv3
<b>Syntax</b>	Integer
<b>Example</b>	<code>nssslsessiontimeout: 5</code>

### nssslclientauth

Specifies whether client authentication uses SSL or not.

<b>Entry DN</b>	<code>cn=encryption,cn=config</code>
<b>Valid Range</b>	<code>off   allowed   required</code>
<b>Default Value</b>	<code>allowed</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nssslclientauth: allowed</code>

## nsssl2

Supports SSL version 2.

<b>Entry DN</b>	<code>cn=encryption,cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsssl2: on</code>

## nsssl3

Supports SSL version 3.

<b>Entry DN</b>	<code>cn=encryption,cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsssl3: on</code>

## nsssl3ciphers

This multi-valued attribute specifies the set of encryption ciphers the Directory Server will use during SSL communications. For more information on the ciphers supported by the Directory Server, see Chapter 11, “Managing SSL”, in the *iPlanet Directory Server Administrator’s Guide*

<b>Entry DN</b>	cn=config
<b>Valid Range</b>	For domestic versions, any combination of the following: <p style="text-align: center;"><b>For SSLv3</b></p> <pre>rsa_null_md5 rsa_rc4_128_md5 rsa_rc4_40_md5 rsa_rc2_40_md5 rsa_des_sha rsa_fips_des_sha rsa_3des_sha rsa_fips_3des_sha</pre> <p style="text-align: center;"><b>For TLS</b></p> <pre>tls_rsa_export1024_with_rc4_56_sha tls_rsa_export1024_with_des_cbc_sha</pre>
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString <p>+ symbol to enable or - symbol to disable followed by the cipher(s). It is important to note that 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) you can specify <code>+all</code>.</p>
<b>Example</b>	<pre>nsslapd-SSL3ciphers: +RSA_NULL_MD5,+RC4_56_SHA,-RC4_56_SHA</pre>

If you are using the Directory Server Console to set the cipher preferences, the values on the SSL 3.0 tab of the Cipher Preference dialog box correspond to the following:

**Table 2-5** SSLv3 Ciphers

Cipher in Console	Corresponding SSLv3 Cipher
None	<code>rsa_null_md5</code>
RC4	<code>rsa_rc4_128_md5</code>
RC4 (Export)	<code>rsa_rc4_40_md5</code>
RC2(Export)	<code>rsa_rc2_40_md5</code>
DES	<code>rsa_des_sha</code>

**Table 2-5** SSLv3 Ciphers

Cipher in Console	Corresponding SSLv3 Cipher
DES (FIPS)	rsa_fips_des_sha
Triple-DES	rsa_3des_sha
Triple-DES (FIPS)	rsa_fips_3des_sha

If you are using the Directory Server Console to set the cipher preferences, the values on the TLS tab of the Cipher Preference dialog box correspond to the following:

**Table 2-6** TLS Ciphers

Cipher in Console	Corresponding TLS Cipher
RC4 (Export)	tls_rsa_export1024_with_rc4_56_sha
DES (Export)	tls_rsa_export1024_with_des_cbc_sha

## cn=features

No attributes to document

## cn=mapping tree

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

`cn="suffixName",cn=mapping tree,cn=config`.

Replication configuration attributes are stored under

`cn=replica,cn="suffixName",cn=mapping tree,cn=config`

with the replication agreement attributes under

`cn=replicationAgreementName,cn=replica,cn="suffixName",cn=mapping tree,cn=config`.

## Suffix Configuration Attributes Under `cn="suffixName"`

Suffix configuration attributes are stored under the `cn="suffixName"` entry, for example `cn="dc=siroe,dc=com"`. This 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. Suffix configuration attributes are presented in this section.

### nsslapd-state

Determines how the suffix handles operations.

<b>Entry DN</b>	<code>cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	<p><code>backend</code> = the backend (database) is used to process all operations</p> <p><code>disabled</code> = 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><code>referral</code> = a referral is returned for requests made to this suffix.</p> <p><code>referral on update</code> = the database is used for all operations except update requests, which receive a referral.</p>
<b>Default Value</b>	<code>disabled</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-state: backend</code>

### 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`.

<b>Entry DN</b>	<code>cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	Any valid partition name
<b>Default Value</b>	None

<b>Syntax</b>	DirectoryString
<b>Example</b>	nsslapd-backend: NetscapeRoot

## Replication Attributes Under cn=replica, cn="suffixName",cn=mapping tree,cn=config

Replication configuration attributes are stored under cn=replica,cn="suffixName",cn=mapping tree,cn=config. The cn=replica entry is an instance of the nsDS5Replia 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. Replication configuration attributes are presented in this section. For further information regarding replication, see Chapter 8, "Managing Replication" in the *iPlanet Directory Server Administrator's Guide*.

### cn

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

<b>Entry DN</b>	cn=replica,cn="suffixName",cn=mapping tree,cn=config
<b>Valid Range</b>	Any valid suffix name
<b>Default Value</b>	cn=replica
<b>Syntax</b>	DirectoryString
<b>Example</b>	cn: "cn=replica"

## nsDS5Flags

This attribute allows you to specify replica properties you have previously defined in flags. At present only one flag exists, which allows you to specify whether your log changes or not.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	Changelog activation 0 = no changes are logged 1 = changes are logged
<b>Default Value</b>	0 (no changes are logged)
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsDS5Flags: 0</code>

## nsDS5ReplicaBindDN

This multivalued attribute specifies the DN to use when binding. Although you can have more than one value in this `cn=replica` entry, you can only have one supplier bind DN per replication agreement. The value can either be the DN of the local entry on the consumer server or, in the case of an SSL connection, the certificate identity associated with same DN.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	Any valid DN
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsDS5ReplicaBindDN: cn=replication manager, cn=config</code>

## nsDS5ReplicaChangeCount

This read-only attribute informs you of the total number of entries in the change log (whether they still remain to be replicated or not). When the change log is purged, only the entries that are still to be replicated are left. See “nsDS5ReplicaPurgeDelay,” on page 89 and “nsDS5ReplicaTombstonePurgeInterval,” on page 90 for more information regarding purge operation properties.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	-1 to maximum integer (2147483647)
<b>Default Value</b>	N/A
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsDS5ReplicaChangeCount: 675</code>

## nsDS5ReplicaId

Specifies the unique ID for masters in a given replication environment.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	0 to 254
<b>Default Value</b>	N/A
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsDS5ReplicaId: 1</code>



## nsDS5ReplicaLegacyConsumer

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

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	<code>true   false</code>
<b>Default Value</b>	<code>false</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsDS5ReplicaLegacyConsumer: false</code>

## nsDS5ReplicaName

This read-only attribute specifies the name of the replica with a unique identifier for internal operations. This unique identifier is allocated by the server when the replica is created. This attribute is destined for internal use only.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	<code>N/A</code>
<b>Default Value</b>	<code>N/A</code>
<b>Syntax</b>	<code>DirectoryString (a UID identifies the replica)</code>
<b>Example</b>	<code>nsDS5ReplicaName: 66a2b699-1dd211b2-807fa9c3-a58714648</code>

## nsDS5ReplicaPurgeDelay

This multi-valued attribute specifies the period of time in seconds after which internal purge operations will be performed on the change log. When setting this attribute, ensure that the purge delay is longer than the longest replication cycle in your replication policy, to avoid incurring conflict resolution problems and server divergence.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	<code>0 (keep forever) to maximum integer (2147483647)</code>
<b>Default Value</b>	<code>604800 (1 week (60x60x24x7))</code>

<b>Syntax</b>	Integer
<b>Example</b>	<code>nsDS5ReplicaPurgeDelay: 604800</code>

## 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.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	Any valid LDAP URL
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsDS5ReplicaReferral: ldap://ldap.aceindustry.com</code>

## nsDS5ReplicaRoot

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

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	Suffix of the database being replicated
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsDS5ReplicaRoot: "dc=siroe,dc=com"</code>

## nsDS5ReplicaTombstonePurgeInterval

Specifies the time interval in seconds between purge operation cycles. When setting this attribute, bear in mind that the purge operation is time consuming.

<b>Entry DN</b>	<code>cn=replica,cn="suffixName",cn=mapping tree,cn=config</code>
<b>Valid Range</b>	0 to maximum integer (2147483647) in seconds

<b>Default Value</b>	3600 (1 hour)
<b>Syntax</b>	Integer
<b>Example</b>	nsDS5ReplicaTombstonePurgeInterval: 3600

## nsDS5ReplicaType

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

<b>Entry DN</b>	cn=ReplicationAgreementName, cn=" <i>suffixName</i> ", cn=mapping tree, cn=config
<b>Valid Range</b>	0 = unknown 1 = primary (not yet used) 2 = consumer (read-only) 3 = consumer/supplier (updateable)
<b>Default Value</b>	N/A
<b>Syntax</b>	Integer
<b>Example</b>	nsDS5ReplicaType: 2

## nsState

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

## 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="suffixName", cn=mapping tree, cn=config`. Like the `cn=replica` entry, the `cn=ReplicationAgreementName` entry is an instance of the `nsDS5Replica` object class. For replication 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. Replication Agreements are configured only on supplier replicas. The replication agreement configuration attributes are presented in this section.

### description

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	Any string.
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>description: Replication Agreement between Server A and Server B.</code>

### nsDS5ReplicaBindDN

Specifies the DN to use when binding. 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. This can also be modified.

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	Any valid DN
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsDS5ReplicaBindDN: cn=replication manager, cn=config</code>

### nsDS5ReplicaBindMethod

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	SIMPLE (This bind method requires a DN and password) SSLCLIENTAUTH
<b>Default Value</b>	SIMPLE
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsDS5ReplicaBindMethod: SIMPLE</code>

## nsDS5ReplicaChangesSentSinceStartup

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	0 to maximum integer (2147483647)
<b>Default Value</b>	N/A
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsDS5ReplicaChangesSentSinceStartup: 647</code>

## nsDS5ReplicaCredentials

Specifies 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. Please note that when certificate based authentication is used, this attribute may not have a value. Please note that the example below is what you view, not what you type.

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	Any valid password which will then be encrypted using the DES reversible password encryption schema.
<b>Default Value</b>	N/A

<b>Syntax</b>	DirectoryString {DES} <i>encrypted_password</i>
<b>Example</b>	nsDS5ReplicaCredentials: {DES} 9Eko69APCJfFReplica

## nsDS5ReplicaHost

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

<b>Entry DN</b>	cn= <i>ReplicationAgreementName</i> , cn=" <i>suffixName</i> ", cn=mapping tree, cn=config
<b>Valid Range</b>	Any valid host server name
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	nsDS5ReplicaHost: <i>MyServer</i>

## nsDS5ReplicaLastInitEnd

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

<b>Entry DN</b>	cn= <i>ReplicationAgreementName</i> , cn=" <i>suffixName</i> ", cn=mapping tree, cn=config
<b>Valid Range</b>	N/A
<b>Default Value</b>	N/A
<b>Syntax</b>	GeneralizedTime
<b>Example</b>	nsDS5ReplicaLastInitEnd: <i>YYYYMMDDhhmmssZ</i> (19711223113229)

## nsDS5ReplicaLastInitStart

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="suffixName", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	N/A
<b>Default Value</b>	N/A
<b>Syntax</b>	GeneralizedTime
<b>Example</b>	<code>nsDS5ReplicaLastInitStart: YYYYMMDDhhmmssZ (20000902160000)</code>

### nsDS5ReplicaLastInitStatus

This optional, read-only attribute provides status for the initialization of the consumer.

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="suffixName", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	0 (Consumer Initialization Succeeded) followed by any other status message.
<b>Default Value</b>	N/A
<b>Syntax</b>	String
<b>Example</b>	<code>nsDS5ReplicaLastUpdateStatus: 0 Consumer Initialization Succeeded</code>

### nsDS5ReplicaLastUpdateEnd

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="suffixName", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	0 = meaning that the Consumer Initialization has succeeded
<b>Default Value</b>	N/A
<b>Syntax</b>	GeneralizedTime
<b>Example</b>	<code>nsDS5ReplicaLastUpdateEnd: YYYYMMDDhhmmssZ (20000902160000)</code>

## nsDS5ReplicaLastUpdateStart

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

<b>Entry DN</b>	<i>cn=ReplicationAgreementName</i> , <i>cn="suffixName"</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
<b>Valid Range</b>	N/A
<b>Default Value</b>	N/A
<b>Syntax</b>	GeneralizedTime
<b>Example</b>	<i>nsDS5ReplicaLastUpdateStart: YYYYMMDDhhmmssZ</i> <i>(20000902160000)</i>

## nsDS5ReplicaLastUpdateStatus

This read-only attribute provides the status for the most recent replication schedule updates.

<b>Entry DN</b>	<i>cn=ReplicationAgreementName</i> , <i>cn="suffixName"</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
<b>Valid Range</b>	0 (no replication sessions started) followed by any other error or status message
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<i>nsDS5ReplicaLastUpdateStatus: 0 replica acquired successfully</i>

## nsDS5ReplicaPort

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

<b>Entry DN</b>	<i>cn=ReplicationAgreementName</i> , <i>cn="suffixName"</i> , <i>cn=mapping tree</i> , <i>cn=config</i>
<b>Valid Range</b>	Port number for the remote server containing the replica.
<b>Default Value</b>	N/A



<b>Syntax</b>	Integer
<b>Example</b>	nsDS5ReplicaPort: 389

## nsDS5ReplicaRefresh

Allows you to initialize your replica. This attribute is absent by default. However, if you add this attribute with a value of `start`, the server reinitializes the replica and removes the attribute value.

<b>Entry DN</b>	<code>cn=ReplicationAgreementName, cn="suffixName", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	<code>stop   start</code>
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	nsDS5ReplicaRefresh: <i>start</i>

## nsDS5ReplicaRoot

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

<b>Entry DN</b>	<code>cn=ReplicationAgreementName, cn="suffixName", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	Suffix of the database being replicated
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	nsDS5ReplicaRoot: "dc=siroe,dc=com"

## nsDS5ReplicaTimeout

This allowed attribute specifies the number of seconds outbound LDAP operations will wait for a response from the remote replica before timing out and failing. If you see "Warning: timed out waiting" messages in the error log file, then you should increase the value of this attribute.

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	0 to maximum integer value (2147483647) in seconds
<b>Default Value</b>	600
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsDS5ReplicaTimeout: 600 seconds</code>

### nsDS5ReplicaTransportInfo

Specifies the type of transport used for transporting data to and from the replica. The attribute values can either be 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, regular LDAP connections are used. This attribute cannot be modified once set.

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	SSL   LDAP
<b>Default Value</b>	absent
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsDS5ReplicaTransportInfo: LDAP</code>

### nsDS5ReplicaUpdateInProgress

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

<b>Entry DN</b>	<code>cn=<i>ReplicationAgreementName</i>, cn="<i>suffixName</i>", cn=mapping tree, cn=config</code>
<b>Valid Range</b>	true   false
<b>Default Value</b>	N/A

<b>Syntax</b>	DirectoryString
<b>Example</b>	nsDS5ReplicaUpdateInProgress:true

## nsDS5ReplicaUpdateSchedule

This multi valued attribute specifies the replication schedule. It can be modified.

<b>Entry DN</b>	cn= <i>ReplicationAgreementName</i> , cn=" <i>suffixName</i> ", cn=mapping tree, cn=config
<b>Valid Range</b>	Time schedule presented as XXXX-YYYY 012345 where XXXX is the starting hour, YYYY is the finishing hour and the numbers 0123456 are the days of the week starting with Sunday.
<b>Default Value</b>	0000-2359 0123456 (all the time)
<b>Syntax</b>	Integer
<b>Example</b>	nsDS5ReplicaUpdateSchedule: 0000-2359 0123456

## nsDS50ruv

This attribute is responsible for managing the internal state of the replica via the replication update vector. It is always present and must not be changed.

## cn=monitor

Monitoring read-only information is stored under `cn=monitor, cn=config`. The `cn=monitor` entry is an instance of the `extensibleObject` object class. For `cn=monitor` 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. The `cn=monitor` read-only attributes are presented in this section.

## connection

List of open connections given in the following format:

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

31 is the connection number, 20010201164808Z is the date the connection was opened, 45 is the number of operations received, 45 is the number of completed operations, and `cn=directory manager` is the bind DN.

### **currentConnections**

Number of current Directory Server connections.

### **totalConnections**

Total number of Directory Server connections.

### **dTableSize**

Size of the Directory Server descriptor table.

### **readWaiters**

Number of connections where some requests are pending and not currently being serviced by a thread in Directory Server.

### **opsInitiated**

Number of Directory Server operations initiated.

### **opsCompleted**

Number of Directory Server operations completed.

### **entriesSent**

Number of entries sent by Directory Server.

### **bytesSent**

Number of bytes sent by Directory Server.

### **currentTime**

Current time usually given in Greenwich Mean Time (indicated by GeneralizedTime syntax z notation, for example 20010202131102Z).

### **startTime**

Directory Server start time.

### **nbackEnds**

Number of Directory Server backends.

## backendMonitorDN

DN for each Directory Server backend.

For further database monitoring information, see “Database Attributes Under `cn=monitor,cn=ldbm database, cn=plugins,cn=config`” on page 145, “Database Attributes Under `cn=database,cn=monitor,cn=ldbm database, cn=plugins,cn=config`” on page 150, “Database Attributes Under `cn=monitor,cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config`” on page 156, and “Database Link Attributes Under `cn=monitor,cn=database instance name,cn=chaining database, cn=plugins,cn=config`” on page 171.

## cn=replication

No attributes to document. When configuring legacy replication, it will be stored under this `cn=replication` node, which serves as a placeholder.

## cn=SNMP

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

### nssnmpenabled

Specifies whether SNMP is enabled or not.

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

### nssnmporganization

Specifies the organization to which the Directory Server belongs.

<b>Entry DN</b>	<code>cn=SNMP,cn=config</code>
<b>Valid Range</b>	Organization name
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nssnmporganization: iplanet</code>

### nssnmplocation

Specifies the location within the company or organization where the Directory Server resides.

<b>Entry DN</b>	<code>cn=SNMP,cn=config</code>
<b>Valid Range</b>	Location
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nssnmplocation: B14</code>

### nssnmpcontact

Specifies the E-mail address of the person responsible for maintaining the Directory Server.

<b>Entry DN</b>	<code>cn=SNMP,cn=config</code>
<b>Valid Range</b>	Contact E-mail address
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nssnmpcontact: ITdept@siroe.com</code>

### nssnmpdescription

Provides a unique description of the Directory Server instance

<b>Entry DN</b>	<code>cn=SNMP,cn=config</code>
<b>Valid Range</b>	Description
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nssnmpdescription: Employee directory instance</code>

## nssnmpmasterhost

This *required* attribute specifies the hostname of the machine on which the master agent is installed. For UNIX only.

<b>Entry DN</b>	<code>cn=SNMP,cn=config</code>
<b>Valid Range</b>	machine hostname or local host
<b>Default Value</b>	<code>localhost</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nssnmpmasterhost: localhost</code>

## nssnmpmasterport

Specifies the port number used to communicate with the master agent. For UNIX only.

<b>Entry DN</b>	<code>cn=SNMP,cn=config</code>
<b>Valid Range</b>	Operating System dependent port number. Refer to your Operating System documentation for further information.
<b>Default Value</b>	199
<b>Syntax</b>	Integer
<b>Example</b>	<code>nssnmpmasterport: 199</code>

## cn=tasks

No attributes to document.

## cn=uniqueid generator

The uniqueid generator configuration attributes are stored under `cn=uniqueid generator,cn=config`. The `cn=uniqueid generator` entry is an instance of the `extensible` object class. For uniqueid generator 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. Uniqueid generator configuration attributes are presented in this section.

### nsstate

Saves the state of the uniqueid generator across server restarts. This attribute is maintained by the server. Do not edit it.

<b>Entry DN</b>	<code>cn=uniqueid generator,cn=config</code>
<b>Valid Range</b>	N/A
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsstate:AbId0c3oMIDUntiLCyYNGgAAAAAAAAAA</code>

## Configuration Quick Reference Tables

This section provides quick reference tables for LDIF configuration files supplied with the Directory Server, object classes and schema used in server configuration, and attributes requiring server restart.

### LDIF Configuration Files

Table 2-7 on page 105 lists all the configuration files which are supplied with the Directory Server, including those for the schema of other iPlanet and Netscape 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). See “LDIF Configuration Files - Location” on page 25 for information on where these files are stored.



**Table 2-7** Directory Server Configuration LDIF Files

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 cn=config and cn=monitor.
00core.ldif	Contains LDAPv3 standard operational schema, such as "subschemaSubentry," the LDAPv3 standard user and organization schema defined in RFC 2256 (based on X.520/X.521), inetOrgPerson and other widely-used attributes, and the operational attributes used by iPlanet Directory Server 5.1 configuration. Modifying this file will cause interoperability problems. User defined attributes should be added using iPlanet Console.
05rfc2247.ldif	Schema from RFC 2247 and related pilot schema: "Using Domains in LDAP/X500 Distinguished Names."
05rfc2927.ldif	Schema from RFC 2927: "MIME Directory Profile for LDAP Schema." Contains the ldapSchemas operational attribute required for the attribute to show up in the subschema subentry.
10rfc2307	Schema from RFC 2307: "An Approach for Using LDAP as a Network Information Service."
20subscriber.ldif	Contains new schema elements and the Nortel subscriber interoperability specification. Also contains the adminRole and memberOf attributes and inetAdmin object class previously stored in 50ns-delegated-admin.ldif file.
25java-object.ldif	Schema from RFC 2713: "Schema for Representing Java(tm) Objects in an LDAP Directory."
28pilot.ldif	Contains pilot directory schema from FRC 1274 which is no longer recommended for new deployments. Please note that future RFCs which succeed RFC 1274 may deprecate some or all of 28pilot.ldif attribute types and classes.
30ns-common.ldif	Schema that contains objects classes and attributes common to the iPlanet Console framework.
50ns-admin.ldif	Schema used by iPlanet Administration Services.
50ns-calendar.ldif	Schema used by iPlanet Calendar Server.

**Table 2-7** Directory Server Configuration LDIF Files

<b>Configuration Filename</b>	<b>Purpose</b>
50ns-certificate.ldif	Schema for iPlanet Certificate Management System.
50ns-compass.ldif	Schema used by Netscape Compass Server to define personal interest profiles.
50ns-delegated-admin.ldif	Schema used by iPlanet Delegated Administrator 4.5.
50ns-directory.ldif	Contains additional configuration schema used by iPlanet Directory Server 4.12 and earlier versions of the directory, which is no longer applicable to iPlanet Directory Server 5.1. This schema is required for replicating between iPlanet Directory Server 4.12 and iPlanet Directory Server 5.1.
50ns-legacy.ldif	Legacy Netscape Schema used by iPlanet Administration Server for legacy servers.
50ns-mail.ldif	Schema used by iPlanet Messaging Server to define mail users and mail groups.
50ns-mcd-browser.ldif	Schema used by Netscape Mission Control Desktop to hold browser client preferences.
50ns-mcd-config.ldif	Schema used by Netscape Mission Control Desktop to set MCD "config()" preferences.
50ns-mcd-li.ldif	Schema used by Mission Control Desktop to define location independence.
50ns-mcd-mail.ldif	Schema used by Mission Control Desktop to hold mail client and messenger security preferences.
50ns-media.ldif	Schema used for Netscape Media Server.
50ns-mlm.ldif	Schema used by iPlanet Messaging Server 4.0 for mailing list management.
50ns-msg.ldif	Schema used for iPlanet Web Mail.
50ns-netshare.ldif	Schema used for iPlanet Netshare.
50ns-news.ldif	Schema used for iPlanet Collabra Server to hold news group preferences.
50ns-proxy.ldif	Schema used for iPlanet Proxy Server.
50ns-value.ldif	Schema for iPlanet servers' "value item" schema.
50ns-wcal.ldif	Schema for iPlanet Web Calendaring.
50ns-web.ldif	Schema for iPlanet Web Server.

**Table 2-7** Directory Server Configuration LDIF Files

Configuration Filename	Purpose
99user.ldif	User-defined schema maintained by Directory Server replication consumers which contains the attributes and object classes from the suppliers.

## Configuration Changes Requiring Server Restart

Table 2-8 lists the configuration attributes that cannot take effect dynamically, while the server is still running. After modifying these parameters through the console or the `ldapmodify` command, the server must be stopped and restarted for them to take effect. The table lists the configuration attributes concerned, with their full DN's, and provides a brief description of their functions.

**Table 2-8** Configuration Changes Requiring Server Restart

Configuration attribute	Action requiring restart
cn=config,cn=ldbm:nsslapd-cachesize	Modifying the cachesize attribute.
cn=config,cn=ldbm:nsslapd-dbcachesize	Modifying the dbcachesize attribute.
cn=config,cn=ldbm:nsslapd-dbcache	Modifying the database cache
cn=config,cn=ldbm:nsslapd-plug-in	Enabling or disabling a database plug-in.
cn=config:nsslapd-changelogdir	Modifying the change log directory.
cn=config:nsslapd-changelogmaxage	Modifying the maximum age limit of the change log.
cn=config:nsslapd-changelogmaxentries	Modifying the maximum number of entries supported by the change log.
cn=config:nsslapd-changelogsuffix	Modifying the change log suffix.
cn=config:nsslapd-port	Changing the port number.
cn=config:nsslapd-secureport	Changing the secure port number.
cn=changelog5,cn=config:nsslapd-db*	Modifying any of the changelog database parameters.
cn=encryption,cn=config:nsssl2	Enabling or disabling SSL Version 2 for Directory Server.
cn=encryption,cn=config:nsssl3	Enabling or disabling SSL Version 3 for Directory Server.

**Table 2-8** Configuration Changes Requiring Server Restart

<b>Configuration attribute</b>	<b>Action requiring restart</b>
cn=encryption,cn=config:nssslclientauth	Enabling or disabling client authentication.
cn=encryption,cn=config:nssslsessiontimeout	Changing the lifetime of an SSL session.

# Plug-in Implemented Server Functionality Reference

This chapter serves as a plug-in implemented server functionality reference and is divided into the following sections:

- Overview
- Server Plug-in Functionality Reference
- List of Attributes Common to all Plug-ins
- Attributes Allowed by Certain Plug-ins
- Database Plug-in Attributes
- Database Link Plug-in Attributes (chaining attributes)
- Retro Changelog Plug-in Attributes

## Overview

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`. A second look at Code Example 2-2 (configuration entry for the Telephone Syntax Plug-in) which we saw in Chapter 2, “Core Server Configuration Reference”:

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

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

## Object Classes for Plug-in Configuration

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
```

# Server Plug-in Functionality Reference

The following tables provide you with a quick overview of the plug-ins provided with iPlanet Directory Server 5.1, along with their configurable options, configurable arguments, default setting, dependencies, general performance related information and further reading. These tables will allow you to weigh up plug-in performance gains and costs and choose the optimal settings for your deployment. The Further Information heading cross references further reading where this is available.

## 7-bit check Plug-in

<b>Plug-in Name</b>	7-bit check (NS7bitAtt)
<b>DN of Configuration Entry</b>	cn=7-bit check,cn=plugins,cn=config
<b>Description</b>	Checks certain attributes are 7-bit clean
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	List of attributes (uid mail userpassword) followed by "," and then suffix(es) on which the check is to occur.
<b>Dependencies</b>	None
<b>Performance Related Information</b>	None
<b>Further Information</b>	If your Directory Server uses non-ASCII characters, for example, Japanese, turn this plug-in off.

## ACL Plug-in

<b>Plug-in Name</b>	ACL Plugin
<b>DN of Configuration Entry</b>	cn=ACL Plugin,cn=plugins,cn=config
<b>Description</b>	ACL access check plug-in
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	N/A
<b>Further Information</b>	Chapter 6, “Managing Access Control” in the <i>iPlanet Directory Server Administrator’s Guide</i> .

## ACL preoperation Plug-in

<b>Plug-in Name</b>	ACL preoperation
<b>DN of Configuration Entry</b>	cn=ACL preoperation,cn=plugins,cn=config
<b>Description</b>	ACL access check plug-in
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	database
<b>Performance Related Information</b>	None
<b>Further Information</b>	Chapter 6, “Managing Access Control” in the <i>iPlanet Directory Server Administrator’s Guide</i> .



## Binary Syntax Plug-in

<b>Plug-in Name</b>	Binary Syntax
<b>DN of Configuration Entry</b>	<code>cn=Binary Syntax,cn=plugins,cn=config</code>
<b>Description</b>	Syntax for handling binary data
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## Boolean Syntax Plug-in

<b>Plug-in Name</b>	Boolean Syntax
<b>DN of Configuration Entry</b>	<code>cn=Boolean Syntax,cn=plugins,cn=config</code>
<b>Description</b>	Syntax for handling booleans.
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## Case Exact String Syntax Plug-in

<b>Plug-in Name</b>	Case Exact String Syntax
<b>DN of Configuration Entry</b>	cn=Case Exact String Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling case-sensitive strings
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## Case Ignore String Syntax Plug-in

<b>Plug-in Name</b>	Case Ignore String Syntax
<b>DN of Configuration Entry</b>	cn=Case Ignore String Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling case-insensitive strings
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## Chaining database Plug-in

<b>Plug-in Name</b>	Chaining Database
<b>DN of Configuration Entry</b>	cn=Chaining database,cn=plugins,cn=config
<b>Description</b>	Syntax for handling DNs
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	Chapter 2, "Configuring Directory Databases" in the <i>iPlanet Directory Server Administrator's Guide</i>

## Class of Service Plug-in

<b>Plug-in Name</b>	Class of Service
<b>DN of Configuration Entry</b>	cn=Class of Service,cn=plugins,cn=config
<b>Description</b>	Allows for sharing of attributes between entries
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	Chapter 5, "Advanced Entry Management" in the <i>iPlanet Directory Server Administrator's Guide</i>

## Country String Syntax Plug-in

<b>Plug-in Name</b>	Country String Syntax Plug-in
<b>DN of Configuration Entry</b>	cn=Country String Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling countries
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## Distinguished Name Syntax Plug-in

<b>Plug-in Name</b>	Distinguished Name Syntax
<b>DN of Configuration Entry</b>	cn=Distinguished Name Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling DNs
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## Generalized Time Syntax Plug-in

<b>Plug-in Name</b>	Generalized Time Syntax
<b>DN of Configuration Entry</b>	cn=Generalized Time Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for dealing with dates, times, and time zones
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	<p>The Generalized Time String consists of the following:</p> <p>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. We strongly recommend that you use the Z time zone indication which stands for Greenwich Mean Time.</p>

## Integer Syntax Plug-in

<b>Plug-in Name</b>	Integer Syntax
<b>DN of Configuration Entry</b>	cn=Integer Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling integers
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.

## Internationalization Plug-in

<b>Plug-in Name</b>	Internationalization Plugin
<b>DN of Configuration Entry</b>	cn=Internationalization Plugin,cn=plugins,cn=config
<b>Description</b>	Syntax for handling DN's
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	The Internationalization has one argument which must not be modified: <i>installDir/slapd-serverID/config/slapd-collations.conf</i> This directory stores the collation orders and locales used by the internationalization plug-in.
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	See Appendix D, "Internationalization" in the <i>iPlanet Directory Server Administrator's Guide</i> .

## Idbm database Plug-in

<b>Plug-in Name</b>	ldbm database Plug-in
<b>DN of Configuration Entry</b>	cn=ldbm database plug-in,cn=plugins,cn=config
<b>Description</b>	Implements local databases
<b>Configurable Options</b>	N/A
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	See “Database Plug-in Attributes” on page 133 for further information on database configuration.
<b>Further Information</b>	Chapter 2, “Configuring Directory Databases” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## Legacy Replication Plug-in

<b>Plug-in Name</b>	Legacy Replication plug-in
<b>DN of Configuration Entry</b>	cn=Legacy Replication plug-in,cn=plugins,cn=config
<b>Description</b>	Enables iPlanet Directory Server 5.1 to be a consumer of a 4.1 supplier
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None. This plug-in can be disabled if the server is not (and never will be) a consumer of a 4.x server.
<b>Dependencies</b>	database
<b>Performance Related Information</b>	None
<b>Further Information</b>	Chapter 8, “Managing Replication” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## Multimaster Replication Plug-in

<b>Plug-in Name</b>	Multimaster Replication Plugin
<b>DN of Configuration Entry</b>	cn=Multimaster Replication plugin,cn=plugins,cn=config
<b>Description</b>	Enables replication between two 5.x Directory Servers
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	database
<b>Performance Related Information</b>	N/A
<b>Further Information</b>	You can turn this plug-in off if you only have one server which will never replicate. See also Chapter 8, “Managing Replication” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## Octet String Syntax Plug-in

<b>Plug-in Name</b>	Octet String Syntax
<b>DN of Configuration Entry</b>	cn=Octet String Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling octet strings
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	



## CLEAR Password Storage Plug-in

<b>Plug-in Name</b>	CLEAR
<b>DN of Configuration Entry</b>	cn=CLEAR,cn>Password Storage Schemes,cn=plugins,cn=config
<b>Description</b>	CLEAR password storage scheme used for password encryption
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	Chapter 7, “User Account Management” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## CRYPT Password Storage Plug-in

<b>Plug-in Name</b>	CRYPT
<b>DN of Configuration Entry</b>	cn=CRYPT,cn>Password Storage Schemes,cn=plugins,cn=config
<b>Description</b>	CRYPT password storage scheme used for password encryption
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	Chapter 7, “User Account Management” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## NS-MTA-MD5 Password Storage Scheme Plug-in

<b>Plug-in Name</b>	NS-MTA-MD5
<b>DN of Configuration Entry</b>	cn=NS-MTA-MD5,cn>Password Storage Schemes,cn=plugins,cn=config
<b>Description</b>	NS-MTA-MD5 password storage scheme for password encryption
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	You can no longer choose to encrypt passwords using the NS-MTA-MD5 password storage scheme. The storage scheme is still present but only for reasons of backward compatibility, i.e. if the data in your directory still contains passwords encrypted with the NS-MTA-MD5 password storage scheme. See Chapter 7, “User Account Management” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## SHA Password Storage Scheme Plug-in

<b>Plug-in Name</b>	SHA
<b>DN of Configuration Entry</b>	cn=SHA,cn=Password Storage Schemes,cn=plugins,cn=config
<b>Description</b>	SHA password storage scheme for password encryption
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	If there are no passwords encrypted using the SHA password storage scheme, you may turn this plug-in off. If you want to encrypt your password with the SHA password storage scheme, we recommend that you choose SSHA instead, as SSHA is a far more secure option.
<b>Further Information</b>	Chapter 7, “User Account Management” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## SSHA Password Storage Scheme Plug-in

<b>Plug-in Name</b>	SSHA
<b>DN of Configuration Entry</b>	cn=SSHA,cn=Password Storage Schemes,cn=plugins,cn=config
<b>Description</b>	SSHA password storage scheme for password encryption
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	Chapter 7, “User Account Management” in the <i>iPlanet Directory Server Administrator’s Guide</i>

## Postal Address String Syntax Plug-in

<b>Plug-in Name</b>	Postal Address Syntax
<b>DN of Configuration Entry</b>	<code>cn=Postal Address Syntax,cn=plugins,cn=config</code>
<b>Description</b>	Syntax used for handling postal addresses
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## PTA Plug-in

<b>Plug-in Name</b>	Pass-Through Authentication Plugin
<b>DN of Configuration Entry</b>	<code>cn=Pass Through Authentication,cn=plugins,cn=config</code>
<b>Description</b>	Enables pass-through authentication, the mechanism which allows one directory to consult another to authenticate bind requests.
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	off
<b>Configurable Arguments</b>	<code>ldap://iplanet.com:389/o=iplanet</code>
<b>Dependencies</b>	None
<b>Performance Related Information</b>	
<b>Further Information</b>	Chapter 16, "Using the Pass-Through Authentication Plug-in" in the <i>iPlanet Directory Server Administrator's Guide</i> .

## Referential Integrity Postoperation Plug-in

<b>Plug-in Name</b>	Referential Integrity Postoperation
<b>DN of Configuration Entry</b>	cn=Referential Integrity Postoperation, cn=plugins, cn=config
<b>Description</b>	Enables the server to ensure referential integrity
<b>Configurable Options</b>	All configuration and on   off
<b>Default Setting</b>	off
<b>Configurable Arguments</b>	<p>When enabled, the post operation Referential Integrity plug-in performs integrity updates on the <code>member</code>, <code>uniquemember</code>, <code>owner</code> and <code>seeAlso</code> attributes immediately after a delete or rename operation. You can reconfigure the plug-in to perform integrity checks on all other attributes.</p> <p>The following arguments are configurable:</p> <ol style="list-style-type: none"> <li>1. Check for referential integrity <ul style="list-style-type: none"> <li>-1 = no check for referential integrity</li> <li>0 = check for referential integrity is performed immediately</li> <li>positive integer = request for referential 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 specified.</li> </ul> </li> <li>2. Log file for storing the change, for example <code>/usr/iplanet/logs/referint</code></li> <li>3. All the additional attribute names you want to be checked for referential integrity.</li> </ol>
<b>Dependencies</b>	database
<b>Performance Related Information</b>	You should enable the Referential Integrity plug-in on only one master in a multi-master replication environment to avoid conflict resolution loops. When enabling the plug-in on chained servers you must be sure to analyze your performance resource and time needs as well as your integrity needs.
<b>Further Information</b>	See Chapter 2, “Configuring Directory Databases” in the <i>iPlanet Directory Server Administrator’s Guide</i> .

## Retro Changelog Plug-in

<b>Plug-in Name</b>	Retro Changelog Plugin
<b>DN of Configuration Entry</b>	cn=Retro Changelog Plugin,cn=plugins,cn=config
<b>Description</b>	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.
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	off
<b>Configurable Arguments</b>	See “Retro Changelog Plug-in Attributes,” on page 173 for further information on the two configuration attributes for this plug-in.
<b>Dependencies</b>	None
<b>Performance Related Information</b>	May slow down Directory Server performance.
<b>Further Information</b>	Chapter 8, “Managing Replication” in the <i>iPlanet Directory Server Administrator’s Guide</i> .

## Roles Plug-in

<b>Plug-in Name</b>	Roles Plugin
<b>DN of Configuration Entry</b>	cn=Roles Plugin,cn=plugins,cn=config
<b>Description</b>	Enables the use of roles in the Directory Server
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.

<b>Plug-in Name</b>	Roles Plugin
<b>Further Information</b>	Chapter 5, “Advanced Entry Management” in the <i>iPlanet Directory Server Administrator’s Guide</i> .

## Telephone Syntax Plug-in

<b>Plug-in Name</b>	Telephone Syntax
<b>DN of Configuration Entry</b>	cn=Telephone Syntax,cn=plugins,cn=config
<b>Description</b>	Syntax for handling telephone numbers
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## UID Uniqueness Plug-in

<b>Plug-in Name</b>	UID Uniqueness plug-in
<b>DN of Configuration Entry</b>	cn=UID Uniqueness,cn=plugins,cn=config
<b>Description</b>	Checks that the values of specified attributes are unique each time a modification occurs on an entry.
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	off
<b>Configurable Arguments</b>	<p>Enter the following arguments:</p> <pre>uid "DN" "DN"...</pre> <p>if you want to check for UID attribute uniqueness in all listed subtrees. However, enter the following arguments:</p> <pre>attribute="uid" MarkerObjectclass = "ObjectClassName"</pre> <p>and optionally</p> <pre>requiredObjectclass = "ObjectClassName"</pre> <p>if you want to check for UID attribute uniqueness when adding or updating entries with the <code>requiredObjectclass</code>, starting from the parent entry containing the <code>ObjectClass</code> as defined by the <code>MarkerObjectClass</code> attribute.</p>
<b>Dependencies</b>	N/A
<b>Performance Related Information</b>	<p>iPlanet Directory Server 5.1 provides the UID Uniqueness plug-in default. If you want to ensure unique values for other attributes, you can create instances of the UID Uniqueness plug-in for those attributes. For more information, see Chapter 17, “Using the Attribute Uniqueness Plug-in” in the <i>iPlanet Directory Server Administrator’s Guide</i>.</p> <p>The UID Uniqueness plug-in may slow down Directory Server performance.</p>
<b>Further Information</b>	Chapter 17, “Using the Attribute Uniqueness Plug-in” in the <i>iPlanet Directory Server Administrator’s Guide</i> .



## URI Plug-in

<b>Plug-in Name</b>	URI Syntax
<b>DN of Configuration Entry</b>	cn=URI Syntax, cn=plugins, cn=config
<b>Description</b>	Syntax for handling URIs (Unique Resource Identifiers) including URLs (Unique Resource Locators)
<b>Configurable Options</b>	on   off
<b>Default Setting</b>	on
<b>Configurable Arguments</b>	None
<b>Dependencies</b>	None
<b>Performance Related Information</b>	Do not modify the configuration of this plug-in. iPlanet recommends that you leave this plug-in running at all times.
<b>Further Information</b>	

## 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.

### nsslapd-pluginPath

Specifies the full path to the plug-in.

<b>Entry DN</b>	cn= <i>plug-inName</i> , cn=plugins, cn=config
<b>Valid Range</b>	Any valid path
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Solaris 9 Example</b>	nsslapd-pluginPath: /usr/iplanet/ds5/lib/uid-plugin.so
<b>Other Platforms Example</b>	nsslapd-pluginPath: /usr/iplanet/servers/lib/uid-plugin.so

## nsslapd-pluginInitfunc

Specifies the plug-in function to be initiated.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any valid plug-in function
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginInitfunc: NS7bitAttr_Init</code>

## nsslapd-pluginType

Specifies the plug-in type. See “nsslapd-plugin-depends-on-type” on page 132 for further information.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any valid plug-in type
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginType: preoperation</code>

## nsslapd-pluginEnabled

Specifies whether or not the plug-in is enabled. This attribute can be changed over protocol, but will only take effect when the server is next restarted.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginEnabled: on</code>

## nsslapd-pluginId

Specifies the plug-in ID.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any valid plug-in ID
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginId: chaining database</code>

## nsslapd-pluginVersion

Specifies the plug-in version.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any valid plug-in version
<b>Default Value</b>	Product version
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginVersion: 5.0b1</code>

## nsslapd-pluginVendor

Specifies the vendor of the plug-in.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any approved plug-in vendor.
<b>Default Value</b>	Sun   Netscape Alliance
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginVendor: iPlanet</code>

**nsslapd-pluginDescription**

Provides a description of the plug-in.

<b>Entry DN</b>	<code>cn=<i>plug-in name</i>, cn=plugins, cn=config</code>
<b>Valid Range</b>	N/A
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-pluginDescription: acl access check plug-in</code>

## Attributes Allowed by Certain Plug-ins

**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`. For further information, see “`nsslapd-pluginType`” on page 130. All plug-ins whose type value matches one of the values in the following valid range will be started by the server prior to this plug-in. The following post operation Referential Integrity Plug-in example shows that the database plug-in will be started prior to the postoperation Referential Integrity Plug-in.

<b>Entry DN</b>	<code>cn=referential integrity postoperation, cn=plugins, cn=config</code>
<b>Valid Range</b>	database
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-plugin-depends-on-type:database</code>

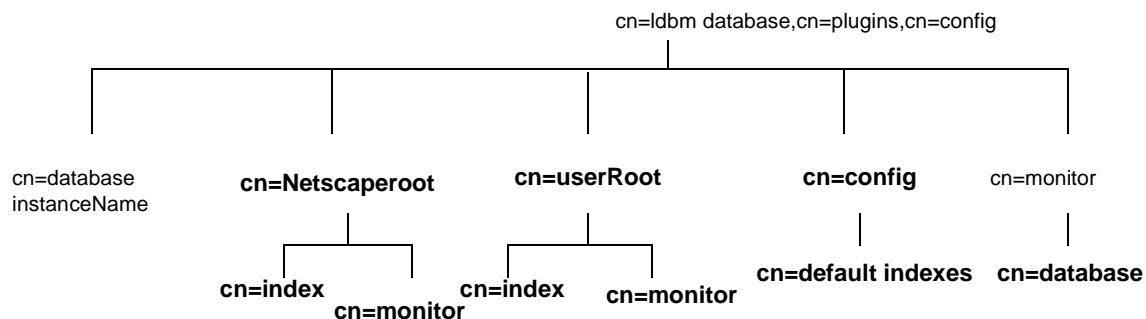
## nsslapd-plugin-depends-on-named

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 whose `cn` value matches one of the values below will be started by the server prior to this plug-in. If the plug-in does not exist, the server will fail to start. The following post operation Referential Integrity Plug-in example shows that the Class of Service plug-in will be started prior to the postoperation Referential Integrity Plug-in. If the Class of Service plug-in does not exist then the server will fail to start.

<b>Entry DN</b>	<code>cn=referential integrity</code> <code>postoperation,cn=plugins,cn=config</code>
<b>Valid Range</b>	Class of Service
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-plugin-depends-on-named: Class of Service</code>

## Database Plug-in Attributes

The database plug-in is also organized in an information tree as shown below:



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.

## Database Attributes Under `cn=config,cn=ldbm` database, `cn=plugins,cn=config`

Global configuration attributes common to all instances are stored in the `cn=config,cn=ldbm` database, `cn=plugins,cn=config` tree node.

### `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. If you bind as the directory manager DN, however, unlimited is set by default and overrides any other settings you may specify 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 you bind as, the default limit will be overridden. If you attempt to set a value that is not a number or is too big for a 32-bit signed integer, you will receive an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

<b>Entry DN</b>	<code>cn=config,cn=ldbm</code> database, <code>cn=plugins,cn=config</code>
<b>Valid Range</b>	-1 to maximum integer in entries (where -1 is unlimited)
<b>Default Value</b>	5000
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsLookthroughLimit: 5000</code>

### `nsslapd-allidsthreshold`

This performance related attribute is present by default. It specifies the number of entry IDs that can be maintained for an index key, before the server sets the All IDs token and stops maintaining a list of IDs for that specific key. If you attempt to set a value that is not a number or is too big for a 32-bit signed integer, you will receive an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

However, as tuning this attribute is a complex task and can severely degrade performance, it is advisable to keep the default value. For a more detailed explanation of the All IDs Threshold see Chapter 10, “Managing Indexes” in the *iPlanet Directory Server Administrator’s Guide*.

### nsslapd-cache-autosize

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	100 to the maximum 32-bit integer value (2147483647) entry IDs
<b>Default Value</b>	4000
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-allidsthreshold: 4000</code>

This performance tuning related attribute is turned off by default. It 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 is claimed for the cache. If you plan to run other servers on the machine, then the value will be lower. Setting the value to 0 turns off the cache autosizing and uses the normal `nsslapd-cachememsize` and `nsslapd-dbcachesize` attributes.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	0 (turns cache autosizing off) to 100
<b>Default Value</b>	0
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-cache-autosize: 80</code>

### 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 2 databases, each of them would receive 20 percent. This attribute only applies when the `nsslapd-cache-autosize` attribute has a value of 0.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	

<b>Default Value</b>	66 (This will not necessarily optimize your operations)
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-cache-autosize-split: 66</code>

## nsslapd-dbcachesize

This performance tuning related attribute specifies database cache size. Note that this is neither the index cache nor the entry cache. If you activate automatic cache resizing, you override this attribute, by replacing these values with its own guessed values at a later stage of the server startup.

If you attempt to set a value that is not a number or is too big for a 32-bit signed integer, you will receive an LDAP\_UNWILLING\_TO\_PERFORM error message with additional error information explaining the problem.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	500KB to 4GB for 32-bit platforms and 500KB to 2 <sup>64</sup> -1 for 64-bit platforms
<b>Default Value</b>	10,000,000 bytes
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-dbcachesize: 10,000,000</code>

---

**NOTE** On HP-UX only the maximum value for the `nsslapd-dbcachesize` attribute is 1GB, due to a PA-RISC hardware limitation that prevents memory-mapped files from crossing quadrant boundaries.

---

## nsslapd-db-checkpoint-interval

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, you add the attribute to `dse.ldif`. This attribute can be dynamically modified using `ldapmodify`. For further information on modifying this attribute, see Chapter 14, “Tuning Directory Server Performance” in the *iPlanet Directory Server Administrator’s Guide*.

This attribute is provided only for system modification/diagnostics and should be changed only with the guidance of iPlanet engineering staff and iPlanet 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, see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	10 to 300 seconds
<b>Default Value</b>	60
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-db-checkpoint-interval: 120 seconds</code>

### nsslapd-db-circular-logging

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. It should therefore only be modified with the guidance of iPlanet engineering staff and iPlanet Professional Services.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	on or off
<b>Default Value</b>	on
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-db-circular-logging: on</code>

## nsslapd-db-durable-transactions

Indicates 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 be able to be recovered in the event of a system failure. However, the durable transactions feature may also slow down 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 is a system failure before a directory change is physically written to disk, that change is not recoverable. The `nsslapd-db-durable-transactions` attribute is absent from `dse.ldif`. To disable durable transactions, you add the attribute to `dse.ldif`.

This attribute is provided only for system modification/diagnostics and should be changed only with the guidance of iPlanet engineering staff and iPlanet 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, see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config,cn=ldbm_database,cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-db-durable_transactions: on</code>

## nsslapd-db-home-directory

UNIX only. Used to fix a situation on UNIX platforms where the operating system endlessly flushes pages. This flushing can be so excessive that performance of the entire system is severely degraded.

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 100mb.

For example, if your Solaris host seems excessively slow and your database cache size is around 100mb or more, then you can use the `iostat` utility to diagnose the problem. Use `iostat` to monitor the activity of the disk where the Directory Server's database files are stored. If all of the following conditions are true:

- The disk is heavily used (more than 1mb per second of data transfer)
- There is a long service time (more than 100ms)
- There is mostly write activity

then you should use the `nsslapd-db-home-directory` attribute to specify a subdirectory of a `tempfs` type file system.

---

**NOTE** The directory referenced by the `nsslapd-db-home-directory` attribute must be a subdirectory of a file system of type `tempfs` (such as `/tmp`). However, Directory Server does not create the subdirectory referenced by this attribute. You must create the directory either manually or by using a script. Failure to create the directory referenced on the `nsslapd-db-home-directory` attribute will result in Directory Server being unable to start.

Also, if you have 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.

Finally, 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 committed. This is a symptom of an overly large database cache size being configured for your server. If this happens, reduce the size of your database cache size to a value where the server will start again.

---

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid directory name in a <code>tempfs</code> file system, such as <code>/tmp</code> .
<b>Default Value</b>	<i>N/A</i>
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nsslapd-db-home-directory: /tmp/slapd-phonebook</code>

## nsslapd-db-idl-divisor

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.

---

**NOTE** 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.

---

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	0 to 8
<b>Default Value</b>	0
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-db-idl-divisor: 2</code>

## nsslapd-db-logbuf-size

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.

---

**NOTE** The `nsslapd-db-logbuf-size` attribute is only valid if the `nsslapd-db-durable-transaction` attribute is set to on.

---

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	32K to maximum integer (limited to the amount of memory available on the machine)
<b>Default Value</b>	32K
<b>Syntax</b>	Integer

**Example**            `nsslapd-db-logbuf-size: 32K`

### nsslapd-db-logdirectory

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:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/db</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/db</code>

For fault-tolerance and performance reasons, you may want to 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, you add the attribute to `dse.ldif`.

For more information on database transaction logging, see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid path and directory name
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-db-logdirectory: /logs/txnlog</code>

### nsslapd-db-logfile-size

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 MB is used. The maximum size is an unsigned 4-byte value. The value of this attribute can have significant impact on performance, as it can be tuned to avoid extensive log switching in the event of heavy entries.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	0 to unsigned 4-byte integer

<b>Default Value</b>	10MB
<b>Syntax</b>	Integer
<b>Example</b>	nsslapd-db-logfile-size: 10 MB

### nsslapd-db-page-size

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 64K bytes. If the page size is not explicitly set, Directory Server defaults to a page size of 8K bytes. Changing this default value can have 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.

---

**NOTE** 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.

---

<b>Entry DN</b>	cn=config,cn=ldbm database,cn=plugins,cn=config
<b>Valid Range</b>	512 bytes to 64 K bytes
<b>Default Value</b>	8K bytes
<b>Syntax</b>	Integer
<b>Example</b>	nsslapd-db-page-size: 8K bytes

### nsslapd-db-transaction-batch-val

Specifies how many transactions will be batched before being committed. You can use this attribute to 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, see Chapter 14, “Tuning Directory Server Performance” in the *iPlanet Directory Server Administrator’s Guide*.

If you do not define this attribute or set it 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 you

to modify this attribute remotely via LDAP. A value of 1 for this attribute allows you to modify 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. Bear in mind that the value you choose for this attribute may require you to modify the `nsslapd-db-logbuf-size` attribute to ensure sufficient log buffer size for accommodating your 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, see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	0 to 30
<b>Default Value</b>	0 (or turned off)
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-db-transaction-batch-val: 5</code>

### nsslapd-db-transaction-logging

Specifies whether transaction logging is on or off. Turning transaction logging off can considerably improve Directory Server performance but at the risk of data loss and/or database corruption in the event of a system crash. If turned off, you must set up other database recovery procedures.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	on   off
<b>Default Value</b>	on
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-db-transaction-logging: on</code>

## nsslapd-dbncache

This attribute allows you to split the `ldb` 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.

This attribute is provided only for system modification/diagnostics and should be changed only with the guidance of iPlanet engineering staff and iPlanet Professional Services. Inconsistent settings of this attribute and other configuration attributes may cause the Directory Server to be unstable.

## nsslapd-import-cachesize

This performance tuning related attribute determines the size of the database cache used in the bulk import process. By setting this attribute value so that the maximum available system physical memory is used for the database cache during bulk importing, you can optimize bulk import speed. If you attempt to set a value that is not a number or is too big for a 32-bit signed integer, you will receive 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 1GB, then 1GB is used when loading one database, 2GB is used when loading 2 databases, etc.

Ensure that you have sufficient physical memory to prevent swapping from occurring, as this results in performance degradation.

---

<b>Entry DN</b>	<code>cn=config,cn=ldb database,cn=plugins,cn=config</code>
<b>Valid Range</b>	500KB to 4GB for 32-bit platforms and 500KB to $2^{64}-1$ for 64-bit platforms
<b>Default Value</b>	20 000 000
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-import-cachesize: 20 000 000</code>



## nsslapd-mode

Specifies the permissions used for newly created index files.

<b>Entry DN</b>	<code>cn=config,cn=ldb database,cn=plugins,cn=config</code>
<b>Valid Range</b>	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 that <code>ns-slapd</code> runs as), and no access for other users.
<b>Default Value</b>	<code>0600</code>
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-mode: 0600</code>

## Database Attributes Under `cn=monitor,cn=ldb database,cn=plugins,cn=config`

Global read-only attributes containing database statistics for monitoring activity on your databases are stored in the `cn=monitor,cn=ldb database,cn=plugins,cn=config` tree node. For more information on these monitoring read-only entries see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

### dbcachehits

Requested pages found in the database.

### dbcachetries

Total requested pages found in the database cache.

### dbcachehitratio

Percentage of requested pages found in the database cache (hits/tries)

### dbcachepagein

Pages read into the database cache.

### dbcachepageout

Pages written from the database cache to the backing file.

### dbcacheroevict

Clean pages forced from the cache.

### dbcacherwevict

Dirty pages forced from the cache.

## 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 the databases containing the `o=NetscapeRoot` and `o=France.Sun` suffixes respectively. The `cn=NetscapeRoot` subtree contains the configuration data used by the iPlanet Administration Server for authentication and all actions that cannot be performed through LDAP (such as start/stop). 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 will be multiple database instances, this name will be changed and defined by the user 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.

## nsslapd-cachesize

This performance tuning related attribute specifies the cache size in terms of the entries it can hold. However, it is worth noting that it is simpler to limit by memory size only (see `nsslapd-cachememsize` attribute). If you attempt to set a value that is not a number or is too big for a 32-bit signed integer, you will receive an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

<b>Entry DN</b>	<code>cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config</code> or <code>cn=UserRoot,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	1 to 2,147,483,647 (or -1 which means limitless) entries
<b>Default Value</b>	-1
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-cachesize: -1</code>

## nsslapd-cachememsize

This performance tuning related attribute specifies the cache size in terms of available memory space. Limiting `cachesize` in terms of memory occupied is the simplest method. By activating automatic cache resizing, you override this attribute, replacing these values with its own guessed values at a later stage of the server startup. If you attempt to set a value that is not a number or is too big for a 32-bit signed integer, you will receive an `LDAP_UNWILLING_TO_PERFORM` error message with additional error information explaining the problem.

<b>Entry DN</b>	<code>cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config</code> or <code>cn=UserRoot,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	200KB to 4GB
<b>Default Value</b>	10 485 760 (10Mb)
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsslapd-cachememsize:10Mb</code>

## nsslapd-directory

Specifies absolute path to the database instance. If your database instance is manually created then this attribute must be included. This is set by default in the iPlanet Console and it is modifiable. Once your database instance is created, do not modify this path as any changes risk preventing the server from accessing data. This attribute is related to `server5`.

<b>Entry DN</b>	<code>cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid absolute path to the database instance
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Solaris 9 Example</b>	<code>nsslapd-directory: /var/ds5/slapd-<i>serverID</i>/db</code>
<b>Other Platforms Example</b>	<code>nsslapd-directory: /usr/iplanet/servers/slapd-<i>serverID</i>/db</code>

## nsslapd-readonly

Specifies Read Only permission rights. If this attribute has a value of `off`, then the user has all read, write, and execute permissions.

<b>Entry DN</b>	<code>cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config or cn=UserRoot,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-readonly: off</code>

## nsslapd-require-index

When switched to `on`, this attribute allows you to refuse non-indexed or allids searches. This performance related attribute avoids saturating the server with erroneous searches.

<b>Entry DN</b>	<code>cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config</code> or <code>cn=UserRoot,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>on</code>   <code>off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-require: off</code>

## nsslapd-suffix

Specifies the suffix of the database link. This is a mono-valued attribute as 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 mono-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 you restart the server containing the database link.

<b>Entry DN</b>	<code>cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config</code> or <code>cn=UserRoot,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	<i>Any valid DN</i>
<b>Default Value</b>	<i>N/A</i>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-suffix: o=Netscaperoot</code>

## 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

Number of transactions that have been aborted.

### nsslapd-db-active-txns

Number of transactions that are currently active.

### nsslapd-db-cache-hit

Requested pages found in the cache.

### nsslapd-db-cache-try

Total cache lookups.

### nsslapd-db-cache-region-wait-rate

Number of times that a thread of control was forced to wait before obtaining the region lock.

### nsslapd-db-cache-size-bytes

Total cache size in bytes.

### nsslapd-db-clean-pages

Clean pages currently in the cache.

### nsslapd-db-commit-rate

Number of transactions that have been committed.

### nsslapd-db-deadlock-rate

Number of deadlocks detected.

**nsslapd-db-dirty-pages**

Dirty pages currently in the cache.

**nsslapd-db-hash-buckets**

Number of hash buckets in buffer hash table.

**nsslapd-db-hash-elements-examine-rate**

Total number of hash elements traversed during hash table lookups.

**nsslapd-db-hash-search-rate**

Total number of buffer hash table lookups.

**nsslapd-db-lock-conflicts**

Total number of locks not immediately available due to conflicts.

**nsslapd-db-lock-region-wait-rate**

Number of times that a thread of control was forced to wait before obtaining the region lock.

**nsslapd-db-lock-request-rate**

Total number of locks requested.

**nsslapd-db-lockers**

Number of current lockers.

**nsslapd-db-log-bytes-since-checkpoint**

Number of bytes written to this log since the last checkpoint.

**nsslapd-db-log-region-wait-rate**

Number of times that a thread of control was forced to wait before obtaining the region lock.

**nsslapd-db-log-write-rate**

Number of megabytes and bytes written to this log.

### nsslapd-db-longest-chain-length

Longest chain ever encountered in buffer hash table lookups.

### nsslapd-db-page-create-rate

Pages created in the cache.

### nsslapd-db-page-read-rate

Pages read into the cache.

### nsslapd-db-page-ro-evict-rate

Clean pages forced from the cache.

### nsslapd-db-page-rw-evict-rate

Dirty pages forced from the cache.

### nsslapd-db-page-trickle-rate

Dirty pages written using the `memp_trickle` interface.

### nsslapd-db-page-write-rate

Pages read into the cache.

### nsslapd-db-pages-in-use

All pages, clean or dirty, currently in use.

### nsslapd-db-txn-region-wait-rate

Number of times that a thread of control was force to wait before obtaining the region lock.



## 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 set up scenarios. All indexes, except system essential ones, can be removed, but care should be taken not to cause unnecessary disruptions. This section presents four required indexing attributes and one optional indexing attribute. For further information on indexes see Chapter 10, “Managing Indexes” in the *iPlanet Directory Server Administrator’s Guide*.

### `nsSystemIndex`

This mandatory attribute specifies whether or not the index is a system index, that is, an index which is vital for iPlanet Directory Server 5.1 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.

<b>Entry DN</b>	<code>cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>true   false</code>
<b>Default Value</b>	N/A
<b>Syntax</b>	<code>DirectoryString</code>
<b>Example</b>	<code>nssystemindex: true</code>

## nsIndexType

This optional, multi-valued attribute specifies the types of index used in iPlanet Directory Server 5.1 operations and the values of the attributes to be indexed. Each desired index type has to be entered on a separate line.

<b>Entry DN</b>	<code>cn=default_indexes,cn=config,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>pres = presence index eq = equality index approx = approximate index sub = substring index matching rule = international index index browse = browsing index</code>
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsindextype: eq</code>

## nsMatchingRule

This optional, multi-valued attribute specifies the collation order object identifier (OID) required for the Directory Server to operate international indexing.

<b>Entry DN</b>	<code>cn=default_indexes,cn=monitor,cn=ldbm database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid collation order object identifier (OID)
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>cn: 2.16.840.1.113730.3.3.2.3.1 (For Bulgarian)</code>

**cn**

Provides the name of the attribute you want to index

<b>Entry DN</b>	cn=default_indexes,cn=monitor,cn=ldbm database,cn=plugins,cn=config
<b>Valid Range</b>	Any valid index cn
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	cn: aci

**description**

This allowed attribute provides a free-hand text description of what the index actually performs.

<b>Entry DN</b>	cn=default_indexes,cn=monitor,cn=ldbm database,cn=plugins,cn=config
<b>Valid Range</b>	N/A
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	description:substring index

## Database Attributes Under cn=monitor,cn=Netscaperoot,cn=ldbm database,cn=plugins,cn=config

Global, read-only entries for monitoring activity on the NetscapeRoot database. These attributes contain database statistics. They are given for each file that makes up your database. For further information see Chapter 13, “Monitoring Logging and Statistics” in the *iPlanet Directory Server Administrator’s Guide*.

### dbfilenamenum

This attribute indicates 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 the same numerical identifier.

### dbfilecachehit

Number of times that a search requiring data from this file was performed and that the data was successfully obtained from the cache.

### dbfilecachemiss

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

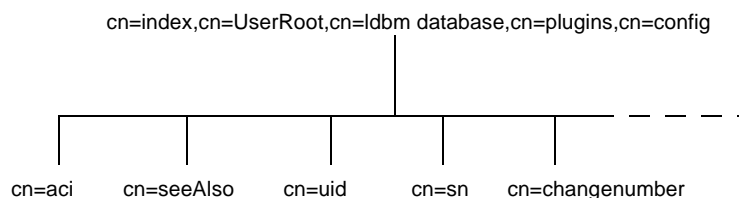
Number of pages brought to the cache from this file.

### dbfilepageout

Number of pages for this file written from cache to disk.

## 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` and `o=UserRoot` and are stored under the `cn=index,cn=NetscapeRoot,cn=ldbm database,cn=plugins,cn=config`, and `cn=index,cn=UserRoot,cn=ldbm database,cn=plugins,cn=config`, respectively. Each indexed attribute represents a subentry entry under the above `cn=config` information tree nodes, as shown below:**



For example, the index file for the `aci` attribute under `o=UserRoot` will appear in the Directory Server as follows:

```

dn:cn=aci,cn=index,cn=UserRoot,cn=ldbm
database,cn=plugins,cn=confi
objectclass:top
objectclass:nsIndex
cn=aci
nssystemindex:true
nsindextype:pres

```

For details on the five possible indexing attributes, see the section “Database Attributes Under `cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config`,” on page 153. For further information about indexes see Chapter 10, “Managing Indexes” in the *iPlanet Directory Server Administrator’s Guide*.

## VLV Index Object Classes Under `cn=MCCsuffixName`, `cn=userRoot`, `cn=ldbm database`, `cn=plugins`, `cn=config`

A VLV (virtual list view) index provides fast searches against a known result set and sort ordering. To do this, the object class `vlvSearch` is needed to define the VLV search, and the object class `vlvIndex` is needed to order the search.

### `vlvIndex`

Used to define the sort criteria of a Virtual List View index. Each VLV index specification defines the sort order to be imposed on the result set defined in the VLV search entry. A set of VLV index entries may appear below the VLV search entry. The `cn` (`commonName`) attribute is used as the naming component for the entry.

<b>Entry DN</b>	<code>cn=MCCsuffixName, cn=userRoot, cn=ldbm database, cn=plugins, cn=config</code>
<b>Superior Class</b>	<code>top</code>
<b>OID</b>	<code>2.16.840.1.113730.3.2.42</code>
<b>Required Attributes</b>	<code>cn</code> <code>objectClass</code> <code>vlvSort</code>
<b>Allowed Attributes</b>	<code>vlvEnabled</code> <code>vlvUses</code>

## vlvSearch

Used to define a VLV search. Specifies the entry result set to be VLV indexed.

<b>Entry DN</b>	<code>cn=MCCsuffixName, cn=userRoot, cn=ldbm database, cn=plugins, cn=config</code>
<b>Superior Class</b>	<code>top</code>
<b>OID</b>	<code>2.16.840.1.113730.3.2.38</code>
<b>Required Attributes</b>	<code>cn</code> <code>objectClass</code> <code>vlvBase</code> <code>vlvFilter</code> <code>vlvScope</code>
<b>Allowed Attributes</b>	<code>multiLineDescription</code>

## VLV Index Attributes Under `cn=MCCsuffixName, cn=userRoot, cn=ldbm database, cn=plugins, cn=config`

These attributes are stored in the `cn=userRoot, cn=ldbm database, cn=plugins, cn=config` tree node.

### vlvBase

Defines the base DN of a VLV search.

<b>Entry DN</b>	<code>cn=userRoot, cn=ldbm database, cn=plugins, cn=config</code>
<b>Valid Range</b>	<code>N/A</code>
<b>Default Value</b>	<code>N/A</code>
<b>Syntax</b>	<code>DN</code>
<b>Example</b>	<code>vlvBase:o=Airius.com</code>

## vlvEnabled

Used by the server to signal whether the index is available or unavailable. When VLV indexes are created offline, new `vlvSearch` entries are enabled when the indexes are rebuilt. VLV indexes can also be created while the server is running in read-only mode. This attribute is read-only and single-valued.

<b>Entry DN</b>	<code>cn=userRoot, cn=ldbm database, cn=plugins, cn=config</code>
<b>Valid Range</b>	<code>0</code>
<b>Default Value</b>	<code>N/A</code>
<b>Syntax</b>	<code>INTEGER</code>
<b>Example</b>	<code>vlvEnabled:0</code>

## vlvFilter

Defines the filter for a VLV search.

<b>Entry DN</b>	<code>cn=userRoot, cn=ldbm database, cn=plugins, cn=config</code>
<b>Valid Range</b>	
<b>Default Value</b>	<code>N/A</code>
<b>Syntax</b>	<code>IA5String</code>
<b>Example</b>	<code>vlvFilter:(uid&gt;=r)</code>

## vlvScope

Defines the scope of a VLV search. Possible values include:

`0`=base search

`1`=one level search

`2`=subtree search

<b>Entry DN</b>	<code>cn=userRoot, cn=ldbm database, cn=plugins, cn=config</code>
<b>Valid Range</b>	<code>0-2</code>
<b>Default Value</b>	<code>N/A</code>



<b>Syntax</b>	INTEGER
<b>Example</b>	vlvScope:1

## vlvSort

Defines the sort specification for a VLV search. Consists of a list of comma-delimited attribute names. A minus sign is used to denote a reverse sort. The example below will result in a sort by uid, then by reverse common name.

<b>Entry DN</b>	cn=userRoot, cn=ldbm database, cn=plugins, cn=config
<b>Valid Range</b>	N/A
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	vlvSort:uid, -cn

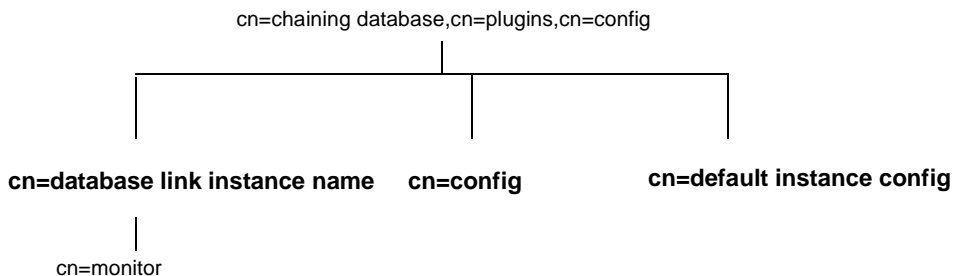
## vlvUses

Displays the number of times the VLV index was used. This number resets after a restart of the server.

<b>Entry DN</b>	cn=userRoot, cn=ldbm database, cn=plugins, cn=config
<b>Valid Range</b>	1-x
<b>Default Value</b>	N/A
<b>Syntax</b>	INTEGER
<b>Example</b>	vlvUses:7

## Database Link Plug-in Attributes (chaining attributes)

The database link plug-in is also organized in an information tree as shown below:



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.

### Database Link Attributes Under `cn=config,cn=chaining database,cn=plugins,cn=config`

Global configuration attributes common to all instances are stored in the `cn=config,cn=chaining database,cn=plugins,cn=config` tree node.

#### `nsActiveChainingComponents`

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 you to alter the components used to chain. 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.

<b>Entry DN</b>	<code>cn=config,cn=chaining database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid component entry
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsActiveChainingComponents: cn=uid uniqueness,cn=plugins,cn=config</code>

### 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.

### nsMaxTestResponseDelay

<b>Entry DN</b>	<code>cn=config,cn=chaining database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid delay period in seconds
<b>Default Value</b>	60 seconds
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsMaxResponseDelay: 60</code>

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.

<b>Entry DN</b>	<code>cn=config,cn=chaining database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid delay period in seconds

<b>Default Value</b>	15 seconds
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsMaxTestResponseDelay: 15</code>

## nsTransmittedControls

This attribute, which can be both a global (and thus dynamic) configuration or an instance (i.e. `cn=database link instance,cn=chaining database,cn=plugins,cn=config`) configuration attribute, allows you to alter the controls that the database link forwards. The following controls are forwarded by default by the database link:

- Managed DSA, object identifier: 2.16.840.1.113730.3.4.2.
- Virtual list view (VLV), object identifier:2.16.840.1.113730.3.4.9
- Server side sorting, object identifier: 1.2.840.113556.1.4.473

<b>Entry DN</b>	<code>cn=config,cn=chaining database,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid OID or the above listed controls forwarded by the database link.
<b>Default Value</b>	None
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsTransmittedControls: 1.2.840.113556.1.4.473</code>

## 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.

### nsAbandonedSearchCheckInterval

Number of seconds that pass before the server checks for abandoned operations.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	0 to 2147483647 seconds
<b>Default Value</b>	2
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsabandonedsearchcheckinterval: 10</code>

### nsBindConnectionsLimit

Maximum number of TCP connections the database link establishes with the remote server.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	1 to 50 connections
<b>Default Value</b>	3
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsbindconnectionslimit: 3</code>

### 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 0 here indicates that the database link will only attempt to bind once.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	1 to 5
<b>Default Value</b>	3
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsbindretrylimit: 3</code>

## nsBindTimeout

Amount of time, before the bind attempt times out. There is no real Valid Range for this attribute, except reasonable patience limits.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	0 to 60 seconds
<b>Default Value</b>	15
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsbindtimeout:15</code>

## nsCheckLocalACI

Reserved for advanced use only. 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.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	on   off
<b>Default Value</b>	off
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nschecklocalaci: on</code>

## nsConcurrentBindLimit

Maximum number of concurrent bind operations per TCP connection.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	1 to 25 binds
<b>Default Value</b>	10
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsconcurrentbindlimit:10</code>

## nsConcurrentOperationsLimit

Specifies the maximum number of concurrent operations allowed.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	1 to 50 operations
<b>Default Value</b>	50
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsconcurrentoperationslimit: 50</code>

## nsConnectionLife

Specifies connection lifetime. You can keep connections between the database link and the remote server open for an unspecified time, or you can close them 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 you provide a list of failover servers in the `nsFarmServerURL` attribute, the “main” server is never contacted after failover to the alternate server.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	0 to limitless seconds (where 0 means forever)
<b>Default Value</b>	0
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsconnectionlife: 0</code>

## nsOperationConnectionsLimit

Maximum number of LDAP connections the database link establishes with the remote server.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	1 to 20 connections
<b>Default Value</b>	10

<b>Syntax</b>	Integer
<b>Example</b>	<code>nsoperationconnectionslimit:10</code>

## nsProxiedAuthorization

Reserved for advanced use only. Allows you to disable proxied authorization, where a value of `off` means proxied authorization is disabled.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>on</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsproxiedauthorization: on</code>

## nsReferralOnScopedSearch

Controls whether or not referrals are returned by scoped searches. This attribute allows you to optimize your directory, because returning referrals in response to scoped searches is more efficient.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins,cn=config</code>
<b>Valid Range</b>	<code>on   off</code>
<b>Default Value</b>	<code>off</code>
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsreferralonscopedsearch: off</code>



## nsSizeLimit

Specifies the default size limit for the database link in bytes.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	-1 (no limit) to 2147483647 entries
<b>Default Value</b>	2000
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsSizeLimit: 2000</code>

## nsTimeLimit

Specifies the default search time limit for the database link.

<b>Entry DN</b>	<code>cn=default instance config,cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	-1 to 2147483647 seconds
<b>Default Value</b>	3600
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsTimeLimit: 3600</code>

## 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 containing data in one or more databases. This attribute can contain optional servers for failover, separated by spaces. For cascading chaining, this URL can point to another database link.

## nsFarmServerURL

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. For cascading chaining, this URL can point to another database link.

<b>Entry DN</b>	<code>cn=<i>database link instance name</i>, cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any valid remote server LDAP URL
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsFarmServerURL: ldap://epdiote.siroe.com:alternate_server:3333</code>

## nsMultiplexorBindDN

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.

<b>Entry DN</b>	<code>cn=<i>database link instance name</i>, cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	N/A
<b>Default Value</b>	DN of the multiplexor
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsMultiplexerBindDN: cn=proxy manager</code>

## 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. Please note that the example below is what you *view*, *not* what you type.

<b>Entry DN</b>	<code>cn=<i>database link instance name</i>, cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	Any valid password which will then be encrypted using the DES reversible password encryption schema.
<b>Default Value</b>	N/A
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsMultiplexerCredentials: {DES} 9Eko69APCJff</code>

### nshoplmit

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.

<b>Entry DN</b>	<code>cn=<i>database link instance name</i>, cn=chaining database, cn=plugins, cn=config</code>
<b>Valid Range</b>	1 to an appropriate upper limit for your deployment
<b>Default Value</b>	10
<b>Syntax</b>	Integer
<b>Example</b>	<code>nsHopLimit: 3</code>

## Database Link Attributes Under cn=monitor,cn=database instance name,cn=chaining database, cn=plugins,cn=config

Attributes used for monitoring activity on your instances are stored in the `cn=monitor, cn=database instance name, cn=chaining database, cn=plugins, cn=config` information tree.

### nsAddCount

Number of add operations received.

### **nsDeleteCount**

Number of delete operations received.

### **nsModifyCount**

Number of modify operations received.

### **nsRenameCount**

Number of rename operations received.

### **nsSearchBaseCount**

Number of base level searches received.

### **nsSearchOneLevelCount**

Number of one-level searches received.

### **nsSearchSubtreeCount**

Number of subtree searches received.

### **nsAbandonCount**

Number of abandon operations received.

### **nsBindCount**

Number of bind requests received.

### **nsUnbindCount**

Number of unbinds received.

### **nsCompareCount**

Number of compare operations received.

### **nsOperationConnectionCount**

Number of open connections for normal operations.

### **nsBindConnectionCount**

Number of open connections for bind operations.

# Retro Changelog Plug-in Attributes

Two different types of changelogs are maintained by iPlanet Directory Server 5.1. The first type, referred to as *changelog*, is used by multi-master replication and the second changelog, which is in fact a plug-in referred to as *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:

- A number that uniquely identifies the modification. This number is sequential with respect to other entries in the change log.
- The modification action; that is, exactly how the directory was modified.

It is through the Retro Changelog plug-in that you access the changes performed to the DS using searches to “cn=changelog,cn=config” file.

## 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:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/db/changelog</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/db/changelog</code>

---

**NOTE** For performance reasons you will probably want to store this database on a different physical disk.

---

<b>Entry DN</b>	<code>cn=Retro Changelog Plugin,cn=plugins,cn=config</code>
<b>Valid Range</b>	Any valid path to the directory
<b>Default Value</b>	None
<b>Syntax</b>	DirectoryString
<b>Example</b>	<code>nsslapd-changelogdir: /var/slapd-<i>serverID</i>/changelog</code>

## nsslapd-changelogmaxage (Max Changelog Age)

Specifies the maximum age of any entry in the change log. The change log 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 will be removed. If this attribute is absent, there is no age limit on change log records, which is the default behavior as this attribute is not present by default.

<b>Entry DN</b>	<code>cn=Retro Changelog Plugin,cn=plugins,cn=config</code>
<b>Valid Range</b>	0 (meaning that entries are not removed according to their age) to the maximum 32 bit integer value (2147483647)
<b>Default Value</b>	0
<b>Syntax</b>	DirectoryString <i>IntegerAgeID</i> where AgeID is “s” for seconds, “m” for minutes, “h” for hours, “d” for days, or “w” for weeks.
<b>Example</b>	<code>nsslapd-changelogmaxage: 30d</code>

# Server Instance File Reference

This chapter provides an overview of the files stored under `/usr/iplanet/servers/slaped-serverID`. Having an overview of the files and configuration information stored in each instance of Directory Server will help you understand the file changes or absence of file changes which occur in the course of directory activity. It will also help you to detect errors and intrusion, by indicating what kind of changes to expect, and as a result, what changes are considered abnormal.

## Overview of Directory Server Files

Directory Server files and command-line scripts are stored under `installDir/slaped-serverID`, where *serverID* is the server identifier. The only exception is the `migrateInstance5` script, which is stored under `installDir/bin/slaped/admin/bin`.

The following listing shows the contents of `installDir/slaped-serverID` on a UNIX platform, where directories are marked with a slash (/) and scripts are marked with an asterisk (\*). See Chapter 8, “Command-Line Scripts” for further information on command-line Scripts.

---

**NOTES** On the Solaris 9 platform, all scripts are also available through the `/usr/sbin/directoryserver name` command.

On Windows platforms, all scripts have the `.bat` extension.

---

**Code Example 4-1** Contents of the *installDir/slapd-serverID* Directory

./	db2ldif*	ns-inactivate.pl*
../	db2ldif.pl*	restart-slapd*
bak/	getpwenc*	restoreconfig*
bak2db*	ldif/	saveconfig*
bak2db.pl*	ldif2db*	start-slapd*
conf_bk/	ldif2db.pl*	stop-slapd*
confbak/	ldif2ldap*	suffix2instance*
config/	locks/	tmp/
db/	logs/	vlvindex*
db2bak*	monitor*	
db2bak.pl*	ns-accountstatus.pl*	
db2index.pl*	ns-activate.pl*	

To reflect the directory structure under *installDir/slapd-serverID*, this chapter is divided into the following sections:

- Backup Files
- Configuration Files
- Database Files
- ldif Files
- Lock Files
- Log Files

Each section describes the file type and contents.

## Backup Files

Each Directory Server instance contains the following three directories for storing backup related files:

- **bak** - contains a directory dated with the time and date of your database backup, for example `2001_02_13_174524/`, which in turn holds your database backup copy.



- `confbak` - is the default directory used by the `restoreconfig` script and the `saveconfig` scripts. See Chapter 8, “Command-Line Scripts” for further information on Command-line Scripts.
- `conf_bk` - contains a backup copy of the `dse.ldif` configuration file from the time of installation.

## Configuration Files

Each Directory Server instance contains the following directory for storing configuration files:

- `config` - contains the configuration files as explained in “Server Configuration - Overview” on page 23.

## Database Files

Each Directory Server instance contains the `db` directory for storing all the database files. The following listing shows the sample contents of the `db` directory.

**Code Example 4-2** Sample Contents of the `db` Directory

<code>./</code>	<code>__db.002</code>	<code>__db.005</code>	<code>NetscapeRoot/</code>
<code>../</code>	<code>__db.003</code>	<code>DBVERSION</code>	<code>userRoot/</code>
<code>__db.001</code>	<code>__db.004</code>	<code>log.0000000017</code>	

- `db.00x` files - used internally by the database. Should not be moved, deleted, or modified in any way
- `log.xxxxxxxxxxxx` files - used to store the transaction logs per database
- `DBVERSION` - used for storing the version of the database.
- `NetscapeRoot` - this directory stores the `o=NetscapeRoot` database created by default at Typical installation.
- `userRoot` - this directory stores the user-defined suffix (user-defined databases) created at Typical installation time, for example `dc=siroe,dc=com`.

The following listing shows the sample contents of the `NetscapeRoot` directory.

**Code Example 4-3** Sample Contents of the `NetscapeRoot` Subdirectory

<code>./</code>	<code>entrydn.db3</code>	<code>parentid.db3</code>
<code>../</code>	<code>givenName.db3</code>	<code>sn.db3</code>
<code>aci.db3</code>	<code>id2entry.db3</code>	<code>uid.db3</code>
<code>cn.db3</code>	<code>nsUniqueId.db3</code>	<code>uniquemember.db3</code>
<code>DBVERSION</code>	<code>numsubordinates.db3</code>	
<code>dncomp.db3</code>	<code>objectclass.db3</code>	

The `NetscapeRoot` subdirectories contain an `index_name.db3` file for every index currently defined in the database, where `index_name` is the name of the index. In addition to these `index_name.db3` files, the `Netscape` and `userRoot` subdirectories contain the following files:

- `dncomp.db3` - contains a list of partial DNs enabling you to find IDs.
- `entrydn.db3` - contains a list of full DNs enabling you to find IDs.
- `id2entry.db3` - contains the actual directory database entries. All other database files can be recreated from this one, if necessary.
- `nsuniqueid.db3` - contains a list of Netscape unique IDs enabling you to find IDs.
- `objectclass.db3` - contains a list of IDs which have a particular objectclass.
- `parentid.db3` - contains a list of IDs allowing you to find ID of parent.

## Ldif Files

Each Directory Server instance contains the `ldif` directory for storing `ldif` related files. The following listing shows the sample contents of the `ldif` directory.

**Code Example 4-4** Sample Contents of the `ldif` Directory

<code>./</code>	<code>European.ldif</code>	<code>Siroe-roles.ldif</code>
<code>../</code>	<code>Siroe.ldif</code>	

The following list describes the content of each of the `ldif` files:

- `European.ldif` - contains European character samples.
- `Siroe.ldif` - is a sample ldif file.
- `Siroe-roles.ldif` - is a sample ldif file similar to `Siroe.ldif` except that it uses roles and class of service instead of groups for setting access control and resource limits for Directory Administrators.

## Lock Files

Each Directory Server instance contains a `locks` directory for storing lock related files. The following listing shows the sample contents of the `locks` directory.

**Code Example 4-5** Sample Contents of the `locks` Directory

```
./                exports/          server/
../              imports/
```

The lock mechanisms stored under the `locks` subdirectories `exports`, `imports`, and `server` prevent 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 (or one `directoryserver ldif2db` operation on Solaris 9 platforms) at a time to the exclusion of all export and `slapd` server operations.

This restriction does not apply to the `ldif2db.pl` script (`directoryserver ldif2db-task` on Solaris 9 platforms), since you can run multiple `ldif2db.pl` operations at any time.

## Log Files

Each Directory Server instance contains a `logs` directory for storing log related files. Code Example 4-6 on page 179 shows a sample listing of the `logs` directory contents.

**Code Example 4-6** Contents of a sample `logs` directory

```
./                access.20010126-120123  audit
errors.rotationinfo
../              access.20010130-140221
audit.rotationinfo  pid
access          access.20010201-100122  errors
slapd.stats
access.20010124-180611  access.rotationinfo
errors.20010124-180607
```

The following list describes the content of the log related files:

- 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.
- The `pid` is the `slapd` process identifier.

# Access Log and Connection Code Reference

iPlanet Directory Server 5.1 provides you with logs to help you monitor directory activity. Monitoring allows you to quickly detect and remedy failures and where done proactively, anticipate and resolve potential problems before they result in failure or poor performance. To monitor your directory effectively, you need to understand the structure and content of your logs.

This chapter does not, and indeed cannot, set out to provide an exhaustive list of error messages. However, the information presented in this chapter will serve as a good starting point for common problems. This chapter includes the following sections:

- Access Log Content
- Common Connection Codes
- LDAP Result Codes

If you require further assistance in the investigation of your access log reports, please contact iPlanet Technical Support:

[http://www.iplanet.com//support\\_services\\_10\\_0.html](http://www.iplanet.com//support_services_10_0.html)

## Access Log Content

The iPlanet Directory Server 5.1 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/2001:11:39:51 -0700]- the format of which may vary depending on which platform you are using, where -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 iPlanet Directory Server 5.1, then describes the default access logging content and ends with a description of the additional access logging level content. This section is divided into the following parts:

- “Access Logging Levels,” on page 182
- “Default Access Logging Content,” on page 183
- “Access Log Content for Additional Access Logging Levels,” on page 190

## Access Logging Levels

Different levels of access logging exist and by changing the value of the `nsslapd-accesslog-level` configuration attribute, you can select the exact type of logging you require. The default level of logging is level 256 which logs access to an entry but you can choose from the following logging levels, combining more than one level to suit your needs:

0=No access logging

4=Logging for internal access operations

256=Logging for access to an entry

512=Logging for access to an entry and referrals

131072=Precise timing of operation duration. This gives microsecond resolution for the Elapsed Time item in the access log.

For example, if you want to log internal access operations, entry access, and referrals, you would set a value of 516 (512+4) in the `nsslapd-accesslog-level` configuration attribute. For further information on other access log configuration attributes, see Chapter 2, “Core Server Configuration Reference”.

## Default Access Logging Content

This section describes the access log content in detail, based on the default access logging level extract in Code Example 5-1.

### Code Example 5-1 Access Log Extract with Default Access Logging Level (level 256)

```
[21/Apr/2001:11:39:51 -0700] conn=11 fd=608 slot=608 connection
from 207.1.153.51 to 192.18.122.139
[21/Apr/2001:11:39:51 -0700] conn=11 op=0 BIND dn="cn=Directory
Manager" method=128 version=3
[21/Apr/2001:11:39:51 -0700] conn=11 op=0 RESULT err=0 tag=97
nentries=0 etime=0
[21/Apr/2001:11:39:51 -0700] conn=11 op=1 SRCH
base="dc=sioe,dc=com" scope=2 filter="(uid=scarter)"
[21/Apr/2001:11:39:51 -0700] conn=11 op=1 RESULT err=0 tag=101
nentries=1 etime=1000 notes=U
[21/Apr/2001:11:39:51 -0700] conn=11 op=2 UNBIND
[21/Apr/2001:11:39:51 -0700] conn=11 op=2 fd=608 closed - U1
[21/Apr/2001:11:39:52 -0700] conn=12 fd=634 slot=634 connection
from 207.1.153.51 to 192.18.122.139
[21/Apr/2001:11:39:52 -0700] conn=12 op=0 BIND dn="cn=Directory
Manager" method=128 version=3
[21/Apr/2001:11:39:52 -0700] conn=12 op=0 RESULT err=0 tag=97
nentries=0 etime=0
[21/Apr/2001:11:39:52 -0700] conn=12 op=1 SRCH
base="dc=sioe,dc=com" scope=2 filter="(uid=scarter)"
[21/Apr/2001:11:39:52 -0700] conn=12 op=2 ABANDON targetop=1
msgid=2 nentries=0 etime=0
[21/Apr/2001:11:39:52 -0700] conn=12 op=3 UNBIND
[21/Apr/2001:11:39:52 -0700] conn=12 op=3 fd=634 closed - U1
[21/Apr/2001:11:39:53 -0700] conn=13 fd=659 slot=659 connection
from 207.1.153.51 to 192.18.122.139
[21/Apr/2001:11:39:53 -0700] conn=13 op=0 BIND dn="cn=Directory
Manager" method=128 version=3
[21/Apr/2001:11:39:53 -0700] conn=13 op=0 RESULT err=0 tag=97
nentries=0 etime=0
[21/Apr/2001:11:39:53 -0700] conn=13 op=1 EXT
oid="2.16.840.1.113730.3.5.3"
[21/Apr/2001:11:39:53 -0700] conn=13 op=1 RESULT err=0 tag=120
nentries=0 etime=0
21/Apr/2001:11:39:53 -0700] conn=13 op=2 ADD dn="cn=Sat Apr 21
11:39:51 MET DST 2001, dc=sioe,dc=com"
```

**Code Example 5-1** Access Log Extract with Default Access Logging Level (level 256)

```
[21/Apr/2001:11:39:53 -0700] conn=13 op=2 RESULT err=0 tag=105
nentries=0 etime=0 csn=3b4c8cfb000000030000
[21/Apr/2001:11:39:53 -0700] conn=13 op=3 EXT
oid="2.16.840.1.113730.3.5.5"
[21/Apr/2001:11:39:53 -0700] conn=13 op=3 RESULT err=0 tag=120
nentries=0 etime=0
[21/Apr/2001:11:39:53 -0700] conn=13 op=4 UNBIND
[21/Apr/2001:11:39:53 -0700] conn=13 op=4 fd=659 closed - U1
[21/Apr/2001:11:39:55 -0700] conn=14 fd=700 slot=700 connection
from 207.1.153.51 to 192.18.122.139
[21/Apr/2001:11:39:55 -0700] conn=14 op=0 BIND dn="" method=sasl
version=3 mech=DIGEST-MD5
[21/Apr/2001:11:39:55 -0700] conn=14 op=0 RESULT err=14 tag=97
nentries=0 etime=0, SASL bind in progress
[21/Apr/2001:11:39:55 -0700] conn=14 op=1 BIND
dn="uid=coulbeck,dc=siroe,dc=com" method=sasl version=3
mech=DIGEST-MD5
[21/Apr/2001:11:39:55 -0700] conn=14 op=1 RESULT err=0 tag=97
nentries=0 etime=0 dn="uid=coulbeck,dc=siroe,dc=com"
[21/Apr/2001:11:39:55 -0700] conn=14 op=2 UNBIND
[21/Apr/2001:11:39:53 -0700] conn=14 op=2 fd=700 closed - U1
```

## Connection Number

Every external LDAP request is listed with an incremental connection number, in this case `conn=11` or `conn=28`, starting at `conn=0` immediately after server startup. 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.

## 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 file descriptor number 608 was used out of the total pool of available file descriptors.

## Slot Number

The slot number, in this case `slot=608`, is a legacy part of the access log. It has the same meaning as file descriptor. Ignore this part of the access log.



## 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. In Code Example 5-1 on page 183, `op=0` is given for the bind operation request and result pair, then `op=1` for the LDAP search request and result pair, and so on. Should you see `op=-1` in the access log, it generally means that the LDAP request for this connection was not issued by an external LDAP client, but instead initiated internally.

## Method Type

The method number, in this case `method=128`, indicates which LDAPv3 bind method was used by the client. There are three possible bind method values:

`0` = no authentication

`128` = simple bind with user password

`sasl` = SASL bind using external authentication mechanism

## 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.

## 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 “LDAP Result Codes,” on page 193.

## 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. Commonly used tags include:

`tag=97` for a result from a client bind operation

`tag=100` indicates the actual entry for which you were searching

`tag=101` for a result from a search operation

`tag=103` for a result from a modify operation

tag=105 for a result from an add operation

tag=107 for a result from a delete operation

tag=109 for a result from a moddn operation

tag=111 for a result from a compare operation

tag=115 indicates a search reference when the entry you perform your search on holds a referral to the entry you require. Search references are expressed in terms of a referral.

tag=120 for a result from an extended operation

---

**NOTE** tag=100 and tag=115 are not result tags as such. It is unlikely that you will see them in your access log.

---

## Number of Entries

The number of entries, in this case `nentries=0`, indicates the number of entries that were found matching the LDAP client's request.

## Elapsed Time

Elapsed time, in this case `etime=1000`, indicates the amount of time (in seconds) that it took the directory server to perform the LDAP operation. An `etime` value of 0 means that the operation actually took milliseconds to perform. If you want 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.

## LDAP Request Type

The LDAP request type indicates the type of LDAP request being issued by the LDAP client. Possible values are:

SRCH=search

MOD=modify

DEL=delete

ADD=add

MODDN=moddn

EXT=extended operation

ABANDON=abandon operation

## LDAP Response Type

The LDAP response type indicates the LDAP response being issued by the LDAP client. Possible values are:

RESULT=result

ENTRY=entry

REFERRAL=referral or search reference

## 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 either when the All IDs Threshold was reached within the index file used for the search, when no index file existed or 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.

---

## 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. Table 5-1 on page 187 provides the list of the LDAPv3 extended operations which are supported iPlanet Directory Server 5.1, and their OIDs.

**Table 5-1** LDAPv3 Extended Operations supported by iPlanet Directory Server 5.1

Extended Operation Name	Description	OID
iPlanet Directory Server 5.x Start Replication Request	Sent by a replication initiator to indicate that a replication session is requested	2.16.840.1.113730.3.5.3

**Table 5-1** LDAPv3 Extended Operations supported by iPlanet Directory Server 5.1

iPlanet Directory Server 5.x 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
iPlanet Directory Server 5.x End Replication Request	Sent to indicate that a replication session is to be terminated	2.16.840.1.113730.3.5.5
iPlanet Directory Server 5.x Replication Entry Request	Carries an entry, along with its state information (csn and UniqueIdentifier), and is used to perform a replica initialization.	2.16.840.1.113730.3.5.6
iPlanet Directory Server 5.x Bulk Import Start	Sent by the client to request a bulk import together with the suffix being imported to <i>and</i> sent by the server to indicate that the bulk import may begin.	2.16.840.1.113730.3.5.7
iPlanet Directory Server 5.x Bulk Import Finished	Sent by the client to signal the end of a bulk import <i>and</i> sent by the server to acknowledge it.	2.16.840.1.113730.3.5.8

## Change Sequence Number

The change sequence number, in this case `csn=3b4c8cfb000000030000`, is the replication change sequence number, thus indicating that replication is enabled on this particular naming context.

## Abandon Message

The abandon message, in this case, `[21/Apr/2001:11:39:52 -0700] conn=12 op=2 ABANDON targetop=1 msgid=2 nentries=0 etime=0`, indicates that an operation has been aborted, where `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 or not. 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/2001:11:39:52 -0700] conn=12 op=2 ABANDON targetop=NOTFOUND
msgid=2
```

where `targetop=NOTFOUND` indicates that the operation to be aborted was either an unknown operation or already complete.

## 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 to the iPlanet Directory Server Operation Number, but identifies the same operation. The message ID is used in the context of an `ABANDON` operation and tells the user which client operation is being abandoned.

---

**NOTE** The iPlanet Directory Server operation number starts counting at 0. In the majority of LDAP SDK/client implementations the message ID number starts counting at 1. This explains why the message ID is frequently equal to the iPlanet Directory Server operation number plus 1.

---

## SASL Multi-Stage Bind Logging

iPlanet Directory Server 5.1 logging for multi-stage binds is now more explicit. Each stage in the bind process is now logged and, where appropriate, the progress statement `SASL bind in progress` is included.

---

**NOTE** Note also that the authenticated DN (the DN used for access control decisions) is now logged in the BIND result line and not in the bind request line, as was previously the case:

```
[21/Apr/2001:11:39:55 -0700] conn=14 op=1 RESULT err=0  
tag=97 nentries=0 etime=0  
dn="uid=coulbeck,dc=siroe,dc=com"
```

For SASL binds, the DN value displayed in the BIND request line is not used by the server and is, therefore, 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.

---

## Access Log Content for Additional Access Logging Levels

This section presents the additional access logging levels available in the iPlanet Directory Server 5.1 access log.

In Code Example 5-2 on page 191, access logging level 512, which logs access to entries and referrals, is enabled. In this extract, 6 entries and 1 referral are returned in response to the search request in bold.

**Code Example 5-2** Access Log Extract with Entry Access and Referral Logging Level (Level 512)

```

12/Jul/2001:16:43:02 +0200] conn=306 fd=60 slot=60 connection from 127.0.0.1 to
127.0.0.1
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 SRCH base="dc=siroe,dc=com"
scope=2 filter="(description=*)" attrs=ALL
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 ENTRY dn="ou=Special
Users,dc=siroe,dc=com"
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 ENTRY
dn="cn=Accounting Managers,ou=groups,dc=siroe,dc=com"
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=HR
Managers,ou=groups,dc=siroe,dc=com"
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=QA
Managers,ou=groups,dc=siroe,dc=com"
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 ENTRY dn="cn=PD
Managers,ou=groups,dc=siroe,dc=com"
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 ENTRY dn="ou=iPlanet
Servers,dc=siroe,dc=com"
[12/Jul/2001:16:43:02 +0200] conn=306 op=0 REFERRAL

```

In Code Example 5-3 on page 191 access logging level 4, which logs internal operations, is enabled.

**Code Example 5-3** Access Log Extract with Internal Access Operations Level (Level 4)

```

[12/Jul/2001:16:45:46 +0200] conn=Internal op=-1 SRCH
base="cn=\22dc=siroe,dc=com\22,cn=mapping tree,cn=config"scope=0
filter="objectclass=nsMappingTree"attrs="nsslapped-referral"
options=persistent
12/Jul/2001:16:45:46 +0200] conn=Internal op=-1 RESULT err=0
tag=48 nentries=1etime=0
[12/Jul/2001:16:45:46 +0200] conn=Internal op=-1 SRCH
base="cn=\22dc=siroe,dc=com\22,cn=mapping tree,cn=config"
scope=0 filter="objectclass=nsMappingTree" attrs="nsslapped-state"
[12/Jul/2001:16:45:46 +0200] conn=Internal op=-1 RESULT err=0
tag=48 nentries=1etime=0

```

Access log level 4 enables logging for internal operations which log the details of the search being performed, and the search base, scope, filter, and requested search attributes.

## Connection Description

The connection description, in this case `conn=Internal`, indicates that the connection is an internal connection. The operation number `op=-1` indicates that the operation was initiated internally.

## 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. They can be configured to return changes to given configurations when changes occur.

---

**NOTE** iPlanet Directory Server 5.1 access log now distinguishes between persistent and regular searches. Previous iPlanet Directory Server releases did not make this distinction.

---

In Code Example 5-4 on page 192, both access logging level 512 and 4 are enabled, which results in both internal access operations, as well as entry access and referrals being logged.

**Code Example 5-4** Access Log Extract with Internal Access Operation, Entry Access and Referral Logging Levels (Levels 4+512)

```
[12/Jul/2001:16:45:46 +0200] conn=Internal op=-1 ENTRY
dn="cn=\22dc=siroe,dc=com\22, cn=mapping tree, cn=config"
[12/Jul/2001:16:45:46 +0200] conn=Internal op=-1 ENTRY
dn="cn=\22dc=siroe,dc=com\22, cn=mapping tree, cn=config"
```

# Common Connection Codes

A connection code is a code which is added to the `closed` log message to provide additional information related to the connection closure. Common connection codes include:

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 `nsslapd-maxbersize` attribute value. For further information about this configuration attribute, see “`nsslapd-maxbersize` (Maximum Message Size),” on page 58.

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 `idletimeout` period

T2=Server closed connection after `ioblocktimeout` period was exceeded

U1= Connection closed by server after client sends an UNBIND request. The server will always close the connection when it sees an UNBIND request.

## LDAP Result Codes

LDAP has a set of result codes that it is useful to be familiar with.

Result Code	Defined Value
0	SUCCESS
1	OPERATION_ERROR
2	PROTOCOL_ERROR
3	TIME_LIMIT_EXCEEDED
4	SIZE_LIMIT_EXCEEDED
5	COMPARE_FALSE
6	COMPARE_TRUE
7	AUTH_METHOD_NOT_SUPPORTED
8	STRONG_AUTH_REQUIRED
9	LDAP_PARTIAL_RESULTS
10	REFERRAL (LDAP v3)

11	ADMIN_LIMIT_EXCEEDED (LDAP v3)
12	UNAVAILABLE_CRITICAL_EXTENSION (LDAP v3)
13	CONFIDENTIALITY_REQUIRED (LDAP v3)
14	SASL_BIND_IN_PROGRESS
16	NO_SUCH_ATTRIBUTE
17	UNDEFINED_ATTRIBUTE_TYPE
18	INAPPROPRIATE_MATCHING
19	CONSTRAINT_VIOLATION
20	ATTRIBUTE_OR_VALUE_EXISTS
21	INVALID_ATTRIBUTE_SYNTAX
32	NO_SUCH_OBJECT
33	ALIAS_PROBLEM
34	INVALID_DN_SYNTAX
35	IS_LEAF
36	ALIAS_DEREFERENCING_PROBLEM
48	INAPPROPRIATE_AUTHENTICATION
49	INVALID_CREDENTIALS
50	INSUFFICIENT_ACCESS_RIGHTS
51	BUSY
52	UNAVAILABLE
53	UNWILLING_TO_PERFORM
54	LOOP_DEFECT
64	NAMING_VIOLATION
65	OBJECT_CLASS_VIOLATION
66	NOT_ALLOWED_ON_NONLEAF
67	NOT_ALLOWED_ON_RDN
68	ENTRY_ALREADY_EXISTS
69	OBJECT_CLASS_MODS_PROHIBITED
71	AFFECTS_MULTIPLE_DSAS (LDAP v3)

80	OTHER
81	SERVER_DOWN
85	LDAP_TIMEOUT
89	PARAM_ERROR
91	CONNECT_ERROR
92	LDAP_NOT_SUPPORTED
93	CONTROL_NOT_FOUND
94	NO_RESULTS_RETURNED
95	MORE_RESULTS_TO_RETURN
96	CLIENT_LOOP
97	REFERRAL_LIMIT_EXCEEDED



# Migration from Earlier Versions

This chapter is intended to provide a reference of the information migrated by the `migrateInstance5` script. In the case of migration from a 4.x Directory Server to a 5.0 or 5.1 Directory Server, it describes the mapping of configuration parameters to configuration attributes and configuration entries in the new Directory Server.

In the case of an upgrade from Directory Server 5.0 to Directory Server 5.1, it describes which attributes are migrated automatically by the migration script, and which ones must be set manually.

For information on how to run the `migrateInstance5` script, refer to the *iPlanet Directory Server Installation Guide*.

## Migration from 4.x Directory Server to 5.0 or 5.1

In the Directory Server 4.x architecture, all configuration parameters were stored in text files. In iPlanet Directory Server 5.0 and 5.1, all configuration attributes are stored in LDAP configuration entries in the `dse.ldif` file.

This section describes the mapping of configuration parameters in Directory Server 4.1, 4.11, 4.12, and 4.13 to the corresponding LDAP configuration entries and attributes in iPlanet Directory Server 5.1.

### Server Attributes

In Directory Server 4.1, 4.11, 4.12, and 4.13, configuration parameters are stored in the `slapd.conf` file under the `/usr/netscape/server4/slapd-serverID` directory.

The corresponding configuration attributes in iPlanet Directory Server 5.1 are stored in the `cn=config` entry. Table 6-1 shows the mapping of Directory Server 4.x configuration parameters to Directory Server 5.1 configuration attributes.

**Table 6-1** Mapping of Legacy Server Parameters to Configuration Attributes

<b>Legacy Configuration Parameter</b>	<b>iPlanet Directory Server Configuration Attribute</b>
accesscontrol	nsslapd-accesscontrol
error-logging-enabled	nsslapd-error-logging-enabled
audit-logging-enabled	nsslapd-audit-logging-enabled
logbuffering	nsslapd-accesslog-buffering
accesslog-logexpirationtime	nsslapd-accesslog-logexpirationtime
accesslog-logexpirationtimeunit	nsslapd-accesslog-logexpirationtimeunit
accesslog-maxlogdiskspace	nsslapd-accesslog-logmaxdiskspace
accesslog-minfreediskspace	nsslapd-accesslog-minfreediskspace
accesslog-logrotationtime	nsslapd-accesslog-logrotationtime
accesslog-logrotationtimeunit	nsslapd-accesslog-logrotationtimeunit
accesslog-maxlogsize	nsslapd-accesslog-maxlogsize
accesslog-MaxNumOfLogsPerDir	nsslapd-accesslog-maxlogsperdir
auditlog-logexpirationtime	nsslapd-auditlog-logexpirationtime
auditlog-logexpirationtimeunit	nsslapd-auditlog-logexpirationtimeunit
auditlog-maxlogdiskspace	nsslapd-auditlog-logmaxdiskspace
auditlog-minfreediskspace	nsslapd-auditlog-minfreediskspace
auditlog-logrotationtime	nsslapd-auditlog-logrotationtime
auditlog-logrotationtimeunit	nsslapd-auditlog-logrotationtimeunit
auditlog-maxlogsize	nsslapd-auditlog-maxlogsize
auditlog-MaxNumOfLogsPerDir	nsslapd-auditlog-maxlogsperdir
certmap-basedn	nsslapd-certmap-basedn
enquote_sup_oc	nsslapd-enquote_sup_oc
loglevel	nsslapd-error-loglevel
errorlog-logexpirationtime	nsslapd-errorlog-logexpirationtime
errorlog-logexpirationtimeunit	nsslapd-errorlog-logexpirationtimeunit
errorlog-maxlogdiskspace	nsslapd-errorlog-logmaxdiskspace
errorlog-minfreediskspace	nsslapd-errorlog-logminfreediskspace
errorlog-logrotationtime	nsslapd-errorlog-logrotationtime

**Table 6-1** Mapping of Legacy Server Parameters to Configuration Attributes

<b>Legacy Configuration Parameter</b>	<b>iPlanet Directory Server Configuration Attribute</b>
errorlog-logrotationtimeunit	nsslapd-errorlog-logrotationtimeunit
errorlog-maxlogsize	nsslapd-errorlog-maxlogsize
errorlog-maxlogsperdir	nsslapd-errorlog-maxlogsperdir
idletimeout	nsslapd-idletimeout
ioblocktimeout	nsslapd-ioblocktimeout
lastmod	nsslapd-ioblocktimeout
listenhost	nsslapd-listenhost
maxdescriptors	nsslapd-maxdescriptors
NOTHING	nsslapd-depends-on-named
NOTHING	nsslapd-depends-on-type
referral	nsslapd-referral
reservedescriptors	nsslapd-reservedescriptors
rootpwstoragescheme	nsslapd-rootpwstoragescheme
schemacheck	nsslapd-schemacheck
secure-port	nsslapd-securePort
security	nsslapd-security
sizelimit	nsslapd-sizelimit
SSL3ciphers	nsslapd-SSL3ciphers
timelimit	nsslapd-timelimit
pw_change	passwordChange
pw_syntax	passwordCheckSyntax
pw_exp	passwordExp
pw_history	passwordHistory
pw_inhistory	passwordinHistory
pw_lockout	passwordLockout
pw_lockduration	passwordLockoutDuration
pw_maxage	passwordMaxAge
pw_maxfailure	passwordMaxFailure
pw_minage	passwordMinAge

**Table 6-1** Mapping of Legacy Server Parameters to Configuration Attributes

<b>Legacy Configuration Parameter</b>	<b>iPlanet Directory Server Configuration Attribute</b>
pw_minlength	passwordMinLength
pw_must_change	passwordMustChange
pw_reset_failurecount	passwordResetFailureCount
pw_storagescheme	passwordStorageScheme
pw_unlock	passwordUnlock
pw_warning	passwordWarning
localhost	nsslapd-localhost
localuser	nsslapd-localuser
port	nsslapd-port
rootdn	nsslapd-rootdn
rootpw	nsslapd-rootpw
accesslog	nsslapd-accesslog
accesslog-level	nsslapd-accesslog-level
auditfile	nsslapd-auditlog
errorlog	nsslapd-errorlog
instancedir	nsslapd-instancedir
maxbersize	nsslapd-maxbersize
nagle	nsslapd-nagle
result_tweak	nsslapd-result_tweak
return_exact_case	nsslapd-return_exact_case
threadnumber	nsslapd-threadnumber
maxthreadsperconn	maxthreadsperconn

## Database Attributes

In Directory Server 4.1, 4.11, 4.12, and 4.13, database parameters are stored in the `slapd.ldbm.conf` file under the `/usr/netscape/server4/slapd-serverID` directory.



Because one instance of iPlanet Directory Server 5.0 or 5.1 can manage several databases, the corresponding attributes in iPlanet Directory Server 5.0 or 5.1 are stored in a general entry for all databases (`cn=config,cn=ldbm database,cn=plugins,cn=config`), or in an entry specific to a particular database, of the form `cn=database instance name,cn=ldbm database,cn=config`.

Table 6-2 shows the mapping of general database configuration parameters between Directory Server 4.x and Directory Server 5.0 or 5.1. Table 6-3 shows the mapping of database-specific parameters between Directory Server 4.x and Directory Server 5.0 or 5.1.

**Table 6-2** Mapping of Legacy Database Parameters to Configuration Attributes (general)

Legacy Configuration Parameter	iPlanet Directory Server Configuration Attribute
<code>allidthreshold</code>	<code>nsslapd-allidthreshold</code>
<code>lookthroughlimit</code>	<code>nsslapd-lookthroughlimit</code>
<code>mode</code>	<code>nsslapd-mode</code>
<code>dbcachesize</code>	<code>nsslapd-dbcachesize</code>
<code>database</code>	OBSOLETE (used to specify database type)

**Table 6-3** Mapping of Legacy Database Parameters to Configuration Attributes (database-specific)

Legacy Configuration Parameter	iPlanet Directory Server Configuration Attribute
<code>cachesize</code>	<code>nsslapd-cachesize</code>
<code>readonly</code>	<code>nsslapd-readonly</code>
<code>directory</code>	<code>nsslapd-directory</code>

## Upgrade from Directory Server 5.0 to 5.1

In Directory Server 5.0 and 5.1, configuration information is stored in the same way. This section explains which configuration attributes are automatically migrated by the `migrateInstance5` script, and which ones are not. Attributes which are not automatically migrated are either configured during the installation process for the new Directory Server, or need to be configured manually for security reasons after the initial set up.

## General Server Configuration Attributes

Table 6-4 lists the configuration attributes stored in the `cn=config` entry that are automatically migrated when you run the `migrateInstance5` script.

Table 6-5 lists the configuration attributes stored in the `cn=config` entry that are *not* automatically migrated when you run the `migrateInstance5` script. Attributes that are not automatically migrated are either configured during the installation process for the new Directory Server, or need to be configured manually. The reason for not migrating an attribute is stated in the table.

**Table 6-4** Attributes in `cn=config` Automatically Migrated

---

<code>nsslapd-accesscontrol</code>
<code>nsslapd-errorlog-logging-enabled</code>
<code>nsslapd-accesslog-logging-enabled</code>
<code>nsslapd-auditlog-logging-enabled</code>
<code>nsslapd-accesslog-level</code>
<code>nsslapd-accesslog-logbuffering</code>
<code>nsslapd-accesslog-logexpirationtime</code>
<code>nsslapd-accesslog-logexpirationtimeunit</code>
<code>nsslapd-accesslog-logmaxdiskspace</code>
<code>nsslapd-accesslog-logminfreediskspace</code>
<code>nsslapd-accesslog-logrotationtime</code>
<code>nsslapd-accesslog-logrotationtimeunit</code>
<code>nsslapd-accesslog-maxlogsize</code>
<code>nsslapd-accesslog-maxlogsperdir</code>
<code>nsslapd-attribute_name_exceptions</code>
<code>nsslapd-auditlog-logexpirationtime</code>
<code>nsslapd-auditlog-logexpirationtimeunit</code>
<code>nsslapd-auditlog-logmaxdiskspace</code>
<code>nsslapd-auditlog-logminfreediskspace</code>
<code>nsslapd-auditlog-logrotationtime</code>
<code>nsslapd-auditlog-logrotationtimeunit</code>
<code>nsslapd-auditlog-maxlogsize</code>

---

**Table 6-4** Attributes in cn=config Automatically Migrated

---

nsslapd-auditlog-maxlogsperdir
nsslapd-certmap-basedn
nsslapd-ds4-compatible-schema
nsslapd-enquote_sup_oc
nsslapd-errorlog-level
nsslapd-errorlog-logexpirationtime
nsslapd-errorlog-logexpirationtimeunit
nsslapd-errorlog-logmaxdiskspace
nsslapd-errorlog-logminfreediskspace
nsslapd-errorlog-logrotationtime
nsslapd-errorlog-logrotationtimeunit
nsslapd-errorlog-maxlogsize
nsslapd-errorlog-maxlogsperdir
nsslapd-groupevalnestlevel
nsslapd-idletimeout
nsslapd-ioblocktimeout
nsslapd-lastmod
nsslapd-listenhost
nsslapd-maxdescriptors (Not applicable on NT and AIX platforms)
nsslapd-nagle
nsslapd-readonly
nsslapd-referralmode
nsslapd-plugin-depends-on-name
nsslapd-plugin-depends-on-type
nsslapd-referral
nsslapd-reservedescriptors (Not applicable on NT and AIX platforms)
nsslapd-rootpwstoragescheme
nsslapd-schemacheck
nsslapd-securePort
nsslapd-security

---

**Table 6-4** Attributes in cn=config Automatically Migrated

---

nsslapd-sizelimit
nsslapd-SSL3ciphers
nsslapd-timelimit
passwordChange
passwordCheckSyntax
passwordExp
passwordExpirationTime
passwordHistory
passwordInHistory
passwordLockout
passwordLockoutDuration
passwordMaxAge
passwordMaxFailure
passwordMinAge
passwordMinLength
passwordMustChange
passwordResetFailureCount
passwordStorageScheme
passwordUnlock
passwordWarning

---

**Table 6-5** Attributes in cn=config not Migrated

Attribute Name	Reason for not Migrating Automatically
nsslapd-localhost	Already set up.
nsslapd-localuser	Configured during the installation process.
nsslapd-port	Configured during the installation process.
nsslapd-rootdn	Configured during the installation process.
nsslapd-rootpw	Configured during the installation process.

---

**Table 6-5** Attributes in `cn=config` not Migrated

Attribute Name	Reason for not Migrating Automatically
<code>nsslapd-accesslog</code>	Path name to the log that records database access. It is set up during installation.
<code>nsslapd-accesslog-list</code>	Read-only attribute.
<code>nsslapd-auditlog</code>	Path name to the log that records changes made to the directory database. It is set up during installation.
<code>nsslapd-accesslog-level</code>	Read-only attribute.
<code>nsslapd-errorlog</code>	Path name to the log that records error messages generated by Directory Server. It is set up during installation.
<code>nsslapd-errorlog-list</code>	Read-only attribute.
<code>nsslapd-instancedir</code>	Configured during the installation process.
<code>nsslapd-maxbersize</code>	Do not change the value of this attribute unless told to do so by iPlanet technical staff.
<code>nsslapd-plug-in</code>	
<code>nsslapd-result-tweak</code>	Reserved for future use. Do not change or remove. Doing so can have unpredictable results
<code>nsslapd-return-exact-case</code>	Do not modify unless you have legacy client applications that can check the case of attribute names in results returned from the server.
<code>nsslapd-threadnumber</code>	This attribute is not available from the Directory Server Console.
<code>nsslapd-maxthreadsperconn</code>	This attribute corresponds to a system parameter.

## Database Attributes

All general database configuration attributes are automatically migrated. These attributes are stored in the entry `cn=config,cn=ldbm database,cn=plugins,cn=config`, and are listed in Table 6-6.

Database-specific attributes are stored in entries of the form `cn=database instance name,cn=ldbm database,cn=config`. The attributes that are migrated are listed in Table 6-7, the ones that are not migrated are listed in Table 6-8.

**Table 6-6** General Database Attributes Automatically Migrated

---

nsslapd-allidthreshold
nsslapd-lookthroughlimit
nsslapd-mode
nsslapd-dbcachesize
nsslapd-cache-autosize
nsslapd-cache-autosize-split
nsslapd-db-transaction-logging

---

**Table 6-7** Database-Specific Attributes Automatically Migrated

---

nsslapd-cachesize
nsslapd-cachememsize
nsslapd-readonly
nsslapd-require-index

---

**Table 6-8** Database-Specific Attributes not Migrated

---

<b>Attribute Name</b>	<b>Reason for not Migrating Automatically</b>
nsslapd-directory	Set up automatically during installation.
nsslapd-db-logdirectory	Set up automatically during installation.
nsslapd-db-checkpoint-interval	This attribute is provided only for system modification/diagnostics and should be changed only under guidance from iPlanet technical staff. Inconsistent settings of this attribute might cause Directory Server crashes.
nsslapd-db-durable-transactions	This attribute is provided only for system modification/diagnostics and should be changed only under guidance from iPlanet technical staff. Inconsistent settings of this attribute might cause Directory Server crashes.

---

**Table 6-8** Database-Specific Attributes not Migrated

Attribute Name	Reason for not Migrating Automatically
nsslapd-db-home-directory	If you have several directory servers running on the same machine, the value of this attribute must be different for each instance of the directory server. Therefore, it needs to be configured manually.

## Database Link Attributes

All database link configuration attributes are automatically migrated. Table 6-9 lists the configuration attributes that are common to all database links. These attributes are stored in the entry `cn=config`, `cn=chaining database`, `cn=plugins`, `cn=config`.

Table 6-10 lists the configuration attributes for a default instance of a database link. These attributes are stored in the entry `cn=default instance config`, `cn=chaining database`, `cn=plugins`, `cn=config`.

**Table 6-9** General Database Link Attributes Automatically Migrated

<code>nsActivechainingComponents</code>
<code>nsTransmittedControls</code>

**Table 6-10** Default Instance Database Link Attributes Automatically Migrated

<code>nsAbandonedSearchCheckInterval</code>
<code>nsBindConnectionsLimit</code>
<code>nsBindTimeout</code>
<code>nsBindRetryLimit</code>
<code>nsHopLimit</code>
<code>nsmaxresponsedelay</code>
<code>nsmaxtestresponsedelay</code>
<code>nsCheckLocalACI</code>
<code>nsConcurrentBindLimit</code>
<code>nsConcurrentOperationsLimit</code>

**Table 6-10** Default Instance Database Link Attributes Automatically Migrated

---

nsConnectionLife  
nsOperationConnectionslimit  
nsProxiedAuthorization  
nsReferralOnScopedSearch  
nsslapped-sizelimit  
nsslapped-timelimit

---

## SNMP Attributes

All SNMP configuration attributes are automatically migrated. These attributes are stored in the entry `cn=SNMP,cn=config`, and are listed in Table 6-11.

**Table 6-11** SNMP Attributes Automatically Migrated

---

nssnmpenabled  
nssnmporganization  
nssnmplocation  
nssnmpcontact  
nssnmpdescription  
nssnmpmasterhost  
nssnmpmasterport

---



# Command-Line Utilities

This chapter contains reference information on command-line utilities provided by iPlanet Directory Server 5.1 that allow you to access and modify entries. These command-line utilities make it easy to perform administration tasks on the Directory Server. This chapter is divided into the following sections:

- Finding and Executing Command-Line Utilities
- Command-Line Utilities Quick Reference
- Using Special Characters
- `ldapsearch`
- `ldapmodify`
- `ldapdelete`
- `ldif`

## Finding and Executing Command-Line Utilities

The `ldapsearch`, `ldapmodify`, and `ldapdelete` command line utilities are stored in the following directory:

<b>Solaris 9 platform</b>	<code>/usr/iplanet/ds5/shared/bin</code>
<b>Other platforms</b>	<code>installDir/shared/bin</code>

and the `ldif` command line utility is stored in the following directory:

<b>Solaris 9 platform</b>	<code>/usr/iplanet/ds5/bin/slapd/server</code>
<b>Other platforms</b>	<code>installDir/bin/slapd/server</code>

---

**CAUTION** In order to execute the command-line utilities, you must change to the directory where the command-line utilities are stored. Although it is possible to set `command-path` and `library-path` variables to execute the utilities, this is *not* recommended procedure. You run the risk of disrupting the correct execution of other utilities and of compromising the security of the system, particularly when you have more than one server version installed.

The same procedure also applies to the Perl scripts provided with Directory Server. For further information on these and other scripts, see Chapter 8, “Command-Line Scripts.”

---

## Command-Line Utilities Quick Reference

**Table 7-1** Commonly Used Command-Line Utilities

Command-line utility	Description
<code>ldapsearch</code>	Allows you to search the directory. Returns search results in LDIF format. For details on this tool, see Appendix B, “Finding Directory Entries” in the <i>iPlanet Directory Server Administrator’s Guide</i> .
<code>ldapmodify</code>	Allows you to add, delete, modify, or rename entries. All operations are specified using LDIF update statements. For details on this tool, see “Adding and Modifying Entries Using <code>ldapmodify</code> ”.
<code>ldapdelete</code>	Allows you to delete entries in the directory. For information on using this utility, see “Deleting Entries Using <code>ldapdelete</code> ”.
<code>ldif</code>	Automatically formats LDIF files for you, and creates base 64 encoded attribute values. For details on this tool, see “Base 64 Encoding”.

---

**CAUTION** *iPlanet Directory Server* `ldap` utilities are not to be confused with the Solaris `ldap` utilities. If you have Directory Server installed on a Solaris machine, the `ldap` man pages you can access are for the Solaris `ldap` utilities and NOT for *iPlanet Directory Server* `ldap` utilities.

---

## Using Special Characters

When using the `ldapsearch` command-line utility, you may need to specify values containing 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=siroe,dc=com"
```

Depending on which command-line interpreter you use, use either single or double quotation marks for this purpose. Refer to your operating system documentation for more information.

Also, if you are using DNs that contain commas (,) in values, you must escape the commas with a backslash. For example:

```
-D "cn=Patricia Fuentes, ou=people, dc=Siroe,dc=Bolivia\, S.A."
```

## ldapsearch

A configurable utility that allows you to locate and retrieve 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.

The `ldapsearch` command has the following format:

```
ldapsearch -b baseDN [options] filter [list_of_attributes]
```

where

- *options* is a series of optional command line options. These must be specified before the search filter, if any.
- *filter* is an LDAP search filter as described in *iPlanet Directory Server Administrator's Guide*. Do not specify a search filter if you are supplying search filters in a file using the `-f` option.

- *list\_of\_attributes* is an optional 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 *iPlanet Directory Server Administrator's Guide*. If you do not specify a list of attributes, the search returns values for all attributes permitted by the access control set in the directory, with the exception of operational attributes.

If you want operational attributes returned as a result of a search operation, you must explicitly specify them in the search command. To retrieve regular attributes in addition to explicitly specified operational attributes, specify "\*" in addition to the operational attributes.

### ldapsearch options

The following three sections list the options which can be specified with `ldapsearch`. The first section lists those options most commonly used, the second section lists SSL options, and the third section lists less common options.

#### Commonly Used ldapsearch options

The following lists the most commonly used `ldapsearch` command-line options. If you specify a value that contains a space, the value should be surrounded by double quotation marks, for example, `-b "ou=groups, dc=siroe,dc=com"`.

---

-b	<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> <p><code>-b "cn=Barbara Jensen, ou=Product Development, dc=siroe,dc=com"</code>.</p> <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, you must supply a search base of "", a search scope of <code>base</code>, and a filter of <code>"objectclass=*"</code>. For example:</p> <p><code>-b "" -s base "objectclass=*"</code></p>
-D	<p>Specifies the distinguished name with which to authenticate to the server. This option is optional if anonymous access is supported by your 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> <p><code>-D "uid=bjensen, dc=siroe,dc=com"</code>.</p>

---

- 
- h** Specifies the hostname or IP address of the machine on which the Directory Server is installed. If you do not specify a host, `ldapsearch` uses the `localhost`. For example, `-h mozilla`.
- j** Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the `-w` option must not be specified.
- l** Specifies the maximum number of seconds to wait for a search request to complete. Regardless of the value specified here, `ldapsearch` will never wait longer than is allowed by the server's `nsslapd-timelimit` attribute. For example, `-l 300`. The default value for the `nsslapd-timelimit` attribute is 3,600 seconds. See “`nsslapd-timelimit (Time Limit)`,” on page 69 for more information.
- p** Specifies the TCP port number that the Directory Server uses. For example, `-p 1049`. The default is 389. If `-z` is used, the default is 636.
- s** Specifies the scope of the search. The scope can be one of the following:
- `base` - Search only the entry specified in the `-b` option or defined by the `LDAP_BASEDN` environment variable.
  - `one` - Search only the immediate children of the entry specified in the `-b` option. Only the children are searched, the actual entry specified in the `-b` option is not searched.
  - `sub` - Search the entry specified in the `-b` option and all of its descendants. That is, perform a subtree search starting at the point identified in the `-b` option. This is the default.
- w** Specifies the password associated with the distinguished name that is specified in the `-D` option. If you do not specify this option, anonymous access is used. If you specify `-w -`, the utility prompts for the password. If either `w` option is specified, the `-j` option must not be specified. For example, `-w diner892`.
- x** Specifies that the search results are sorted on the server rather than on the client. This is useful if you want to sort according to a matching rule, as with an international search. In general, it is faster to sort on the server than on the client.
- z** Specifies the maximum number of entries to return in response to a search request. For example, `-z 1000`. Normally, regardless of the value specified here, `ldapsearch` never returns more entries than the number allowed by the server's `nsslapd-sizelimit` attribute. However, you can override this limitation by binding as the root DN when using this command-line argument. This is because, when you bind as the root DN, this option defaults to zero (0). The default value for the `nsslapd-sizelimit` attribute is 2,000 entries. See “`nsslapd-sizelimit (Size Limit)`,” on page 68 for more information.
-

### SSL options

You use the following command-line options to specify that `ldapsearch` use LDAPS when communicating with your SSL-enabled Directory Server. You also use these options if you want to use certificate-based authentication. These options are valid only when LDAPS has been turned on and configured for your Directory Server. For information on certificate-based authentication and creating a certificate database for use with LDAP clients, see Chapter 11, “Managing SSL” in the *iPlanet Directory Server Administrator’s Guide*.

In addition to the standard `ldapsearch` options, to run an `ldapsearch` command using SSL, you must specify the following:

- `-p` to specify Directory Server’s encrypted port
- `-z` to specify SSL
- `-P` to specify your certificate database’s file and pathname
- `-N` to specify your certificate name
- `-K` to specify your private key file and pathname
- `-w` to specify your private key database password

---

<code>-K</code>	Specifies the file and path name of the private key database of the client. This information is required for certificate-based client authentication.
<code>-m</code>	Specifies the path to the security module database. For example, <i>installDir</i> /secmodule.db. You only need to specify this option if the security module database is in a different directory from the certificate database itself.
<code>-N</code>	Specifies the certificate name to use for certificate-based client authentication. For example, <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 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> .
<code>-P</code>	Specifies the path and 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 version of Netscape Communicator is configured, the path specified on this option can be that of the certificate database for Communicator. For example, <code>-P c:\security\cert.db</code> . The client security files can also be stored on the Directory Server in the <i>installDir</i> /alias directory. In this case, the <code>-P</code> option calls out a path and filename similar to the following:  <code>-P c:\iplanet\servers\alias\client-cert.db</code>

---

---

-W	Specifies the password for the private key database identified in the -P option. For example, -W serverpassword
-Z	Specifies that SSL is to be used for the search request.

---

### Additional ldapsearch Options

To further customize a search, use the following optional options:

---

-A	Specifies that the search retrieve the attributes only, not the attribute values. This option is useful if you just want to determine if an attribute is present for an entry and you are not interested in the value.
-a	Specifies how alias dereferencing is completed. Value can be “never,” “always,” “search,” or “find.” Default value is “never.”
-B	Print binary values. Specifies that binary values stored in the directory should be printed in the search output. If you use -B and -o together, then the binary data will not use base 64 encoding.
-F	Specify a different separator. This option can only be used with -o. This option allows you to specify a separator other than a colon “:” to separate an attribute name from the corresponding value. For example, -F +
-f	Specifies the file containing the search filter(s) to be used in the search. For example, -f search_filters. Omit this option if you want to supply a search filter directly to the command line. For more information about search filters, see Appendix B, “Finding Directory Entries” in the <i>iPlanet Directory Server Administrator’s Guide</i> .
-G	Virtual list search. Allows you to specify the number of entries before or after the search target, and the index or value of the first entry returned. For example, if you are sorting by surname, -G 20:30:johnson returns the first entry with a surname equal to or less than johnson, 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.

---

- 
- i** Character set. Specifies the character set to use for command line input. The default is the character set specified in the `LANG` environment variable. You might want to use this option to perform the conversion from the specified character set to UTF8, thus overriding the environment variable setting.

Using this argument, you can input the bind DN, base DN, and the search filter pattern in the specified character set. `ldapsearch` converts the input from these arguments before it processes the search request. For example, `-i no` 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 you specify a file containing a search filter (with the `-f` option), `ldapsearch` will not convert the data in the file.
  - k** Conversion routines directory. If you want to specify a sort language that is not supported by default in this release of the Directory Server, for example, one obtained from a later release of the LDAP SDK, you need to supply the directory in which you store the conversion routines. You can view the list of supported languages in Table B.1 in the *iPlanet Directory Server Administrator's Guide*.

When performing the search, the server looks in the current working directory. However, if the conversion routines are not in the current working directory, you need to specify this option when using `ldapsearch`. The conversion routines directory is located by default in `installDir/lib/nls`.
  - M** Manage smart referrals. The server does not return the smart referral contained on the entry, but returns the actual entry containing the referral instead. Use this option if you are attempting to search for entries that contain smart referrals. For more information about smart referrals, see Chapter 2, "Configuring Directory Databases" in the *iPlanet Directory Server Administrator's Guide*.
  - n** Specifies that the search is not actually performed, but that `ldapsearch` shows what it would do with the specified input.
  - O** Specifies the maximum number of referral hops `ldapsearch` should automatically follow. For example, `-O 2`.
  - o** Specifies that the output for individual values be formatted without line breaks and that equal signs "=" be used to separate attribute names from values. This argument produces output in a non-LDIF format.
  - R** Specifies that referrals are not to be followed automatically. By default, referrals are followed automatically.
-



---

-S	Specifies the attribute to use as the sort criteria. For example, <code>-S sn</code> . You can use multiple <code>-S</code> arguments if you want to further define the sort order. In the following example, the search results will be sorted first by surname and then by given name:  <code>-S sn -S givenname</code>  The default is not to sort the returned entries.
-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. When you use this option, each attribute value is placed in a separate file within the system temporary directory. No base64 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, <code>-V 2</code> . LDAP v3 is the default. You cannot perform an LDAP v3 search against a Directory Server that only supports LDAP v2. Only use LDAP v2 when connecting to LDAP v2 servers, such as Netscape Directory Server 1.x.
-y	Specifies the proxy DN to use for the search. This argument is provided for testing purposes. For more information about proxied authorization, see Chapter 6, “Managing Access Control” in the <i>iPlanet Directory Server Administrator’s Guide</i> .

---

## ldapmodify

Allows you to make changes to directory entries via LDAP.

### Syntax

```
ldapmodify -D bindDN [-w password] [-acmnrVFR] [-d debugLevel]
[-h host] [-p port] [-M auth_mechanism] [-Z] [-V version]
[-l number_of_ldap_connections] [-f file | < entryfile ]
```

### ldapmodify options

The following three sections list the options that can be specified with `ldapmodify`. The first section lists those options most commonly used, the second section lists SSL options, and the third section lists less common options.

### Commonly Used ldapmodify options

To modify an entry or entries in an existing directory, use the `ldapmodify` command-line utility with the following options:

---

-a	Allows you to add 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 you to directly add a file created by <code>ldapsearch</code> .
-B	Specifies the suffix under which the new entries will be added.
-D	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, <code>-D "uid=bjensen, dc=siroe, dc=com"</code> . You cannot use this option with the <code>-N</code> option.
-f	Optional option that specifies the file containing the LDIF update statements used to define the directory modifications. For example, <code>-f modify_statements</code> . If you do not supply this option, the update statements are read from <code>stdin</code> . For information on supplying LDIF update statements from the command line, see Chapter 4, "Managing Directory Entries" in the <i>iPlanet Directory Server Administrator's Guide</i> .
-h	Specifies the name of the host on which the server is running. For example, <code>-h cyclops</code> .
-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-p	Specifies the port number that the server uses. For example, <code>-p 1049</code> . The default is 389. If <code>-Z</code> is used, the default is 636.
-q	Causes each add to be performed silently rather than being echoed to the screen individually.
-w	Specifies the password associated with the distinguished name that is specified in the <code>-D</code> option. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .
-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	Specifies the LDAP version number to be used on the operation. For example, <code>-V 2</code> . LDAP v3 is the default. You cannot perform an LDAP v3 operation against a Directory Server that only supports LDAP v2.

---

---

-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 Chapter 4, “Managing Directory Entries” in the <i>iPlanet Directory Server Administrator’s Guide</i> .
----	--

---

### SSL options

You can use the following command-line options to specify that `ldapmodify` is to use LDAP over SSL (LDAPS) when communicating with your Directory Server. LDAPS encrypts data during transit. You also use these options if you want to use certificate-based authentication. These options are valid only when SSL has been turned on and configured for your Directory Server. For more information on certificate-based authentication and on creating a certificate database for use with LDAP clients, see Chapter 11, “Managing SSL” in the *iPlanet Directory Server Administrator’s Guide*.

Make sure that you specify your Directory Server’s encrypted port when you use these options:

---

-K	Specifies the name of the certificate key used for certificate-based client authentication. For example, <code>-K Server-Key</code> .
-N	Specifies the certificate name to use for certificate-based client authentication. For example, <code>-N Server-Cert</code> . 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	Specifies the path and filename of the security files for the client. This option is used only with the <code>-z</code> option. When used on a machine where a SSL-enabled web browser is configured, the path specified on this option can be pointed to the security database for the web browser. For example, <code>-P c:\security\cert.db</code> . You can also store the client security files on the Directory Server in the <code>installDir/alias</code> directory.
-W	Specifies the password for the certificate database identified on the <code>-P</code> option. For example, <code>-W serverpassword</code> .
-Z	Specifies that SSL is to be used for the directory request.

---

### Additional ldapmodify options

The following options offer additional functionality:

- 
- b** 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 images. For example, if you wanted to add a `jpegPhoto` attribute, then specify the `-b` option on the `ldapmodify` call. In the LDIF you provide to `ldapmodify`, include a statement using the following notation:
- ```
jpegPhoto: /tmp/photo.jpeg
```
- `ldapmodify` reads the contents of the `photo.jpeg` file into the `jpegPhoto` attribute that you are placing on the entry.
- On Windows NT, the format of this option is exactly the same (including the forward slashes, except that you can specify a drive letter). For example:
- ```
jpegPhoto: c:\tmp\photo.jpeg.
```
- Note that this behavior is not supported by Directory Console. In the Console, values that begin with a slash are added literally to the directory.
- For further information on importing binary data into the directory, see Chapter 4, “Managing Directory Entries” in the *iPlanet Directory Server Administrator’s Guide*.
- 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 `ldapmodify` options.
- M** Manage smart referrals. The server does not return the smart referral contained on the entry, but applies the modification request directly to the entry instead. Use this option if you are attempting to add, change, or delete a directory entry that contains a smart referral. For more information about smart referrals, see Chapter 2, “Configuring Directory Databases” in the *iPlanet Directory Server Administrator’s Guide*.
- n** Specifies that the entries are not actually modified, but that `ldapmodify` shows what it would do with the specified input.
- O** Specifies the maximum number of referral hops to follow. For example, `-O 2`.
- R** Specifies that referrals are not to be followed automatically.
- v** Specifies that the utility is to run in verbose mode.
- V** Specifies the LDAP version number to be used on the operation. For example, `-V 2`. LDAP v3 is the default. You can not perform an LDAP v3 operation against a Directory Server that only supports LDAP v2.
-

---

-y	Specifies the proxy DN to use for the modify operation. This argument is provided for testing purposes. For more information about proxied authorization, see Chapter 6, “Managing Access Control” in the <i>iPlanet Directory Server Administrator’s Guide</i> .
----	---

---

## ldapdelete

Allows you to perform delete operations on directory entries via LDAP.

### Syntax

```
ldapdelete [options]
```

### ldapdelete options

The following three sections list the options that can be specified with `ldapsdelete`. The first section lists those options most commonly used, the second section lists SSL options, and the third section lists less common options.

#### Commonly Used ldapdelete options

To delete an entry or entries from an existing database, use the `ldapdelete` command-line utility with the following options:

---

-D	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, <code>-D "uid=bjensen, dc=siroe, dc=com"</code> . For more information on access control, see Chapter 6, “Managing Access Control” in the <i>iPlanet Directory Server Administrator’s Guide</i> . If you use the <code>-D</code> option, you cannot use the <code>-N</code> option.
-h	Specifies the name of the host on which the server is running. For example, <code>-h cyclops</code> . The default is <code>localhost</code> .
-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-p	Specifies the port number that the server uses. Default is 389. If <code>-z</code> is used, the default is 636.
-w	Specifies the password associated with the distinguished name that is specified in the <code>-D</code> option. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .

---

---

dn	Specifies the dn of the entry to delete.
----	--

---

### SSL options

You use the following options to specify that `ldapdelete` use LDAPS when communicating with your Directory Server. You also use these options if you want to use certificate-based authentication. These options are valid only when LDAPS has been turned on and configured for your Directory Server. For more information on certificate-based authentication and how to create a certificate database for use with LDAP clients, see Chapter 11, “Managing SSL” in the *iPlanet Directory Server Administrator’s Guide*.

Make sure that you specify your Directory Server’s encrypted port when you use these options:

---

-K	Specifies the name of the certificate key used for certificate-based client authentication. For example, <code>-K Server-Key</code> .
-N	Specifies the certificate name to use for certificate-based client authentication. For example, <code>-N Server-Cert</code> . 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	Specifies the path and filename of the security files for 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 point to the security database for the web browser. For example, <code>-P c:\security\cert.db</code> . The client security files can also be stored on the Directory Server in the <code>installDir/alias</code> directory.
-W	Specifies the password for the certificate database identified on the <code>-P</code> option. For example, <code>-W serverpassword</code> .
-Z	Specifies that SSL is to be used for the delete request.

---

### Additional ldapdelete options

The following options offer additional functionality:

- 
- 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 Specifies the file containing the distinguished names of entries to be deleted. For example, `-f modify_statements`. Omit this option if you want to supply the distinguished name of the entry to be deleted directly to the command line.
  - H Lists all available `ldapdelete` options.
  - M Manage smart referrals. The server does not return the smart referral contained on the entry, but deletes the actual entry containing the smart referral instead. For more information about smart referrals, see Chapter 2, “Configuring Directory Databases” in the *iPlanet Directory Server Administrator’s Guide*.
  - n Specifies that the entries are not actually deleted, but that `ldapdelete` shows what it would do with the specified input.
  - O Specifies the maximum number of referral hops to follow. For example, `-O 2`. There is no maximum number of referral hops.
  - 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 Specifies the LDAP version number to be used on the operation. For example, `-V 2`. LDAP v3 is the default. You cannot perform an LDAP v3 operation against a Directory Server that only supports LDAP v2.
  - 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 Chapter 6, “Managing Access Control” in the *iPlanet Directory Server Administrator’s Guide*.
- 

## ldif

Automatically formats LDIF files for you, and creates base 64 encoded attribute values. With Base 64 Encoding you can represent Binary data, such as a JPEG image, in LDIF by using base 64 encoding. You identify base 64 encoded data by using the `::` symbol. For example:

```
jpegPhoto::<encoded data>
```

In addition to binary data, other values that must be base 64 encoded include:

- any value that begins with a semicolon (;) or a space
- 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

The `ldif` command has the following format:

<b>Solaris 9 platform</b>	<code>/usr/sbin/directoryserver ldif [-b] [attrtypes]</code>
<b>Other platforms</b>	<code>installDir/bin/slapd/server ldif [-b] [attrtypes]</code>

### Options

---

**-b** Specifies that the `ldif` utility should interpret the entire input as a single binary value. If `-b` is not present, each line is considered to be a separate input value.

As an alternative to the `-b` option, you can use the `:<` URL specifier notation, which is in fact simpler to use. For example:

```
jpegphoto:< file:///tmp/myphoto.jpg
```

Although the official notation requires three `///`, the use of one `/` is tolerated.

---



# Command-Line Scripts

This chapter provides information on the scripts you can use to back up and restore your database. Scripts are a shortcut way of executing the ns-slapd interface commands which are documented in Appendix A, “Using the ns-slapd and slapd.exe Command-Line Utilities.”

This chapter is divided into the following sections:

- Command-Line Scripts Quick Reference
- Shell and Batch Scripts
- Perl Scripts

## Command-Line Scripts Quick Reference

All scripts and commands are available in the following ways:

<b>Solaris 9 platform</b>	Using the <code>/usr/sbin/directoryserver <i>name</i></code> command
<b>Other platforms</b>	As the <code>/usr/iplanet/servers/slapd-<i>serverID</i>/<i>name</i></code> script or <code>.bat</code> file

Refer to the tables below for the name and purpose of each script.

When scripts request either a directory name or a file name, always provide the absolute path. The scripts assume that you want to use the `dse.ldif` file located in:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/config</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/config</code>

---

**CAUTION** In order to execute the Perl Scripts, you must change to the directory where the command-line utilities are stored. Although it is possible to set command path and library-path variables to execute these scripts, this is *not* the recommended procedure. You run the risk of disrupting the correct execution of other scripts and utilities and of compromising the security of the system, particularly when you have more than one server version installed.

The same procedure also applies to the `ldapsearch`, `ldapmodify`, `ldapdelete` and `ldif` command-line utilities. For more information on these command-line utilities, see Chapter 7, “Command-Line Utilities.”

Please also note that when you are running the Perl scripts on Windows machines, you must make sure that the path environment variable contains the Perl executable (`perl.exe`) file. You therefore need to run the scripts from the following directory on Windows:

```
\usr\iplanet\servers\bin\slapd\admin\bin
```

---

The following table lists command-line script *names*, which are also option *names* for the `/usr/sbin/directoryserver` command on the Solaris 9 platform.

**Table 8-1** Commonly Used Command-Line Shell and Batch Scripts

Command <i>name</i>	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>getpwenc</code>	Prints the encrypted form of a password using one of the server’s encryption algorithms. If a user cannot log in, you can use this script to compare the user’s password to the password stored in the directory. This command name is not an option for the <code>directoryserver</code> command on the Solaris 9 platform.
<code>ldif2db</code>	Imports LDIF files to the database.  Runs the <code>slapd</code> (Windows NT) or <code>ns-slapd</code> (Unix) command-line utility with the <code>ldif2db</code> keyword. By default, the script first saves and then merges any existing configuration tree ( <code>o=NetscapeRoot</code> ) with any files to be imported.

---

**Table 8-1** Commonly Used Command-Line Shell and Batch Scripts (Continued)

<b>Command name</b>	<b>Description</b>
<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. Use the following command on the Solaris 9 platform: <code>/usr/sbin/directoryserver restart</code> .
<code>restoreconfig</code>	Restores by default the most recently saved Admin Server configuration to NetscapeRoot partition.
<code>saveconfig</code>	Saves Admin Server configuration, stored in the NetscapeRoot suffix to <code>installDir/slapd-serverID/confbak</code> directory.
<code>start-slapd</code>	Starts Directory Server. Use the following command on the Solaris 9 platform: <code>/usr/sbin/directoryserver start</code> .
<code>stop-slapd</code>	Stops Directory Server. Use the following command on the Solaris 9 platform: <code>/usr/sbin/directoryserver stop</code> .
<code>suffix2instance</code>	Maps a suffix to a backend name.
<code>vlvindex</code>	Creates and generates virtual list view (VLV) indexes, also called browsing indexes.

The following table gives the names of perl scripts and their equivalent command on the Solaris 9 platform.

**Table 8-2** Commonly Used Command-Line Perl Scripts

<b>Command Line Perl script</b>	<b>Description</b>
<code>bak2db.pl</code> <code>directoryserver bak2db-task</code>	Restores the database from the most recent archived backup.
<code>db2bak.pl</code> <code>directoryserver db2bak-task</code>	Creates a backup of the current database contents
<code>db2index.pl</code> <code>directoryserver db2index-task</code>	Creates and regenerates indexes.
<code>db2ldif.pl</code> <code>directoryserver db2ldif-task</code>	Exports the contents of the database to LDIF

**Table 8-2** Commonly Used Command-Line Perl Scripts

Command Line Perl script	Description
<code>ldif2db.pl</code>	Imports LDIF files to database.
<code>directoryserver ldif2db-task</code>	Runs the <code>slapd</code> (Windows NT) or <code>ns-slapd</code> (Unix) command-line utility with the <code>ldif2db</code> keyword. By default, the script first saves and then merges any existing configuration tree ( <code>o=NetscapeRoot</code> ), with any files to be imported.
<code>migrateInstance5</code> (not available on the Solaris 9 platform)	Migrates a 4.x or 5.0 version of the Directory Server to the 5.1 version, converting the configuration files to LDIF format.  Located in: <code>/usr/iplanet/servers/bin/slapd/admin/bin</code>
<code>ns-accountstatus.pl</code> <code>directoryserver account-status</code>	Provides account status information to establish whether an entry or group of entries is locked or not.
<code>ns-activate.pl</code> <code>directoryserver account-activate</code>	Activates an entry or a group of entries by unlocking it (them).
<code>ns-inactivate.pl</code> <code>directoryserver account-inactivate</code>	Inactivates an entry or a group of entries.

## Shell and Batch Scripts

Some of the Shell and Batch 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 you execute the script.

When a Shell or Batch script has a Perl equivalent, there is a cross-reference to the section describing the equivalent Perl script.

### bak2db (Restore database from backup)

Restores the database from the most recent archived backup. To run this script the server must be stopped.

#### Syntax

Command (Solaris 9)    `directoryserver bak2db [backup_directory]`

Script (Other UNIX)    `bak2db [backup_directory]`

Batch file (Windows)    `bak2db [ backup_directory ]`

For information on the equivalent Perl script, see “bak2db.pl (Restore database from backup),” on page 238.

For more information on restoring databases, see Chapter 3, “Populating Directory Databases” in the *iPlanet Directory Server Administrator’s Guide*.

## db2bak (Create backup of database)

Creates a backup of the current database contents. This script can be executed while the server is still running.

### Syntax

Command (Solaris 9)    `directoryserver db2bak [ backup_directory ]`

Script (Other UNIX)    `db2bak [ backup_directory ]`

Batch file (NT)        `db2bak [ backup_directory ]`

For information on the equivalent Perl script, refer to “db2bak.pl (Create backup of database),” on page 239.

## db2ldif (Export database contents to LDIF)

Exports the contents of the database to LDIF. This script can be executed while the server is still running.

For information on the equivalent Perl script, refer to “db2ldif.pl (Export database contents to LDIF),” on page 241.

For the shell and batch scripts, the script runs the `slapd` (Windows NT) or `ns-slapd` (UNIX) command-line utility with the `ldif2db` keyword.

### Syntax

Command (Solaris 9)    `directoryserver db2ldif options`

Script (Other UNIX)    `db2ldif options`

```

Batch file (NT)      db2ldif options
options            {-n backend_instance}* |
                   {-s includesuffix}* [{-x excludesuffix}*]
                   [-r] [-C] [-u] [-U] [-m] [-M] [-a outfile] [-1] [-N]

```

---

**NOTE**      You must specify either the `-n` or the `-s` option.

---

### Options

---

`-a`      File name of the output LDIF file.

`-n`      Instance to be exported.

`-s`      Suffix(es) to be included or to specify the subtree(s) to be included if `-n` has been used.

`-x`      Suffix(es) to be excluded.

`-m`      Minimal base64 encoding.

`-M`      Use of several files for storing the output LDIF, with each *instance* stored in *instance\_outfile* (where *outfile* is the file name specified for `-a` option).

`-r`      Export replica.

`-u`      Request that the unique id is not exported.

`-C`      Only the main db file is used.

`-N`      Specifies that entry IDs are not to be included in the LDIF output. The entry IDs are necessary only if the `db2ldif` output is to be used as input to `db2index`.

`-U`      Request that the output LDIF is not folded.

`-1`      For reasons of backward compatibility, delete the first line of the LDIF file which gives the version of the LDIF standard.

---



---

**NOTE**      Please note that the output LDIF will be stored in one file by default. Should you want to specify the use of several files, then use the option `-M`.

---

## getpwenc (Print encrypted password)

Prints the encrypted form of a password using one of the server's encryption algorithms. If a user cannot log in, you can use this script to compare the user's password to the password stored in the directory.

### Syntax

Command (Solaris 9)	<code>/var/ds5/slapd-<i>serverID</i>/getpwenc <i>storagescheme</i> <i>clearpassword</i></code>
Script (Other UNIX)	<code>getpwenc <i>storagescheme</i> <i>clearpassword</i></code>
Batch file (NT)	<code>getpwenc <i>storagescheme</i> <i>clearpassword</i></code>

### Options

There are no options for this script.

For more information on the different storage schemes such as SSHA, SHA, CRYPT and CLEAR, see the *iPlanet Directory Server Administrator's Guide*.

## ldif2db (Import)

Runs the `slapd` (Windows NT) or `ns-slapd` (Unix) command-line utility with the `ldif2db` keyword. To run this script the server must be stopped.

For information on the equivalent Perl script, see "ldif2db.pl (Import)," on page 242.

---

**NOTE** Note that `ldif2db` supports LDIF version 1 specifications. You can load an attribute using the `:< URL` specifier notation. For example:

```
jpegphoto:< file:///tmp/myphoto.jpg
```

Although the official notation requires three `///`, the use of one `/` is tolerated. For further information on the LDIF format, see the *iPlanet Directory Server Administrator's Guide*.

---

### Syntax

Command (Solaris 9)	<code>directoryserver ldif2db <i>options</i></code>
---------------------	---

```

Script (Other UNIX)    ldif2db options
Batch file (NT)       ldif2db options
options               -n backend_instance |
                       {-s includesuffix}* [{-x excludesuffix}*]
                       {-i ldiffile}* [-O] [-g string] [-G namespace_id]

```

## Options

---

-n	Instance to be imported. Ensure that you specify an instance that corresponds to the suffix contained by the LDIF file. Otherwise the data contained by the database is deleted and the import fails.
-i	File name of the input ldif file(s). When you import multiple files, they are imported in the order in which you specify them on the command line.
-s	Suffix(es) to be included or to specify the subtree(s) to be included if -n has been used.
-x	Suffix(es) to be included.
-O	Request that only the core db is created without attribute indexes.
-c	Merge chunk size.
-g <i>string</i>	<p>Generation of 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>If you use the <code>deterministic</code> generation to have a name-based unique ID, you can also specify the namespace you want the server to use as follows:</p> <pre>-g deterministic namespace_id</pre> <p>where <code>namespace_id</code> is a string of characters in the following format</p> <pre>00-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx</pre> <p>Use this option if you want to import the same LDIF file into two different directory servers, and if you want the contents of both directories to have the same set of unique IDs. If unique IDs already exist in the LDIF file you are importing, then the existing IDs are imported to the server regardless of the options you have specified.</p>
-G <i>namespace_id</i>	Generates a namespace ID as a name-based unique ID. This is the same as specifying the <code>-g deterministic</code> option.

---



## ldif2ldap (Perform import operation over LDAP)

Performs an import operation over LDAP to the Directory Server. To run this script the server must be running.

### Syntax

Command (Solaris 9)	<code>directoryserver ldif2ldap -D <i>rootDN</i> -w <i>password</i> -f <i>filename</i></code>
Script (Other UNIX)	<code>ldif2ldap -D <i>rootDN</i> -w <i>password</i> -f <i>filename</i></code>
Batch file (NT)	<code>ldif2ldap -D <i>rootDN</i> -w <i>password</i> -f <i>filename</i></code>

### Options

---

-D	User DN with root permissions, such as Directory Manager.
-w	Password associated with the user DN.
-f	File name of the file to be imported. When you import multiple files, they are imported in the order in which you specify them on the command line.

---

## monitor (Retrieve monitoring information)

Retrieves performance monitoring information using the `ldapsearch` command-line utility.

### Syntax

Command (Solaris 9)	<code>directoryserver monitor</code>
Script (Other UNIX)	<code>monitor</code>
Batch file (NT)	<code>monitor</code>

### Options

There are no options for this script.

For more information on the `ldapsearch` command-line utility, see Chapter 7, “Command-Line Utilities”.

## restart-slapd (Restart the Directory Server)

Restarts the Directory Server.

### Syntax

Command (Solaris 9)	<code>directoryserver restart</code>
Script (Other UNIX)	<code>restart-slapd</code>
Batch file (NT)	<code>restart-slapd</code>

### Options

There are no options for this script.

### Exit Status

- 0: Server restarted successfully.
- 1: Server could not be started.
- 2: Server restarted successfully but was already stopped.
- 3: Server could not be stopped.

## restoreconfig (Restore Admin Server Configuration)

By default, restores the most recently saved Admin Server configuration information to the `NetscapeRoot` suffix under the following directory:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/config</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/config</code>

To restore the Admin Server configuration:

1. Stop the Directory Server
2. Run the `restoreconfig` script
3. Restart the Directory Server
4. Restart the Admin Server for the changes to be taken into account

**Syntax**

Command (Solaris 9)	<code>directoryserver restoreconfig</code>
Script (Other UNIX)	<code>restoreconfig</code>
Batch file (NT)	<code>restoreconfig</code>

**Options**

There are no options for this script.

## saveconfig (Save Admin Server Configuration)

Saves Admin Server configuration information to the following directory:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i>/confbak</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i>/confbak</code>

---

**NOTE** This script will only run if the server is running.

---

**Syntax**

Command (Solaris 9)	<code>directoryserver saveconfig</code>
Script (Other UNIX)	<code>saveconfig</code>
Batch file (NT)	<code>saveconfig</code>

**Options**

There are no options for this script.

## start-slapd (Start the Directory Server)

Starts the Directory Server.

**Syntax**

Command (Solaris 9)	<code>directoryserver start</code>
---------------------	------------------------------------

Script (Other UNIX)	<code>start-slapd</code>
Batch file (NT)	<code>start-slapd</code>

### Options

There are no options for this script.

### Exit Status

- 0: Server started successfully.
- 1: Server could not be started.
- 2: Server was already started.

## stop-slapd (Stop the Directory Server)

Stops the Directory Server.

### Syntax

Command (Solaris 9)	<code>directoryserver stop</code>
Script (Other UNIX)	<code>stop-slapd</code>
Batch file (NT)	<code>stop-slapd</code>

### Options

There are no options for this script.

### Exit Status

- 0: Server stopped successfully.
- 1: Server could not be stopped.
- 2: Server was already stopped.

## suffix2instance (Map Suffix to Backend Name)

Maps a suffix to a backend name.

**Syntax**

Command (Solaris 9)    `directoryserver suffix2instance {-s suffix}`  
 Script (Other UNIX)    `suffix2instance {-s suffix}`  
 Batch file (NT)        `suffix2instance {-s suffix}`

**Options**


---

`-s`            The suffix to be mapped to the backend

---

## vlvindex (Create virtual list view (VLV) 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 you view search results. Using VLV indexes, you can organize search results alphabetically or in reverse alphabetical order, and you can scroll through the list of results. VLV index configuration must already exist prior to running this script.

**Syntax**

Command (Solaris 9)    `directoryserver vlvindex options`  
 Script (Other UNIX)    `vlvindex options`  
 Batch file (NT)        `vlvindex options`  
*options*                `[-d debug_level] [-n backend_instance] [-s suffix]  
                          [-T VLVTag]`

**Options**


---

`-d`    Specifies the debug level to use during index creation. Debug levels are defined in “`nsslapd-errorlog-level (Error Log Level)`,” on page 49.

`-D`    Specifies the server configuration directory that contains the configuration information for the index creation process. You must specify the full path to the `slapd-serverID` directory.

`-n`    Name of the database containing the entries to index.

---

- 
- s Name of the suffix containing the entries to index.
  - T VLV index identifier to use to create VLV indexes. You can use the console to specify VLV index identifier for each database supporting your directory tree, as described in the *iPlanet Directory Server Administrator's Guide*. You can define additional VLV tags by creating them in LDIF, and adding them to Directory Server's configuration, as described in the *iPlanet Directory Server Administrator's Guide*. In any case, we recommend you use the dn of the entry for which you want to accelerate the search sorting.
- 

---

**NOTE** You must specify either the `-n` or the `-s` option.

---

## Perl Scripts

### bak2db.pl (Restore database from backup)

This perl script `bak2db.pl` creates an entry in the directory that launches this dynamic task. An entry is generated based upon the values you provide for each option.

#### Syntax

Command (Solaris 9) `directoryserver bak2db-task options`

Perl script (All others) `bak2db.pl options`

*options* `[-v] -D rootDN {-w password | -w - | -j filename }  
[-a backup_directory] [-t databasetype]`

#### Options

- 
- D User DN with root permissions, such as Directory Manager. The default is the DN of the directory manager which is read from the `nsslapd-root` attribute under `cn=config`.
-

- 
- w Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify `-w -`, the utility prompts for the password. If either `-w` option is specified, the `-j` option must not be specified. For example, `-w diner892`.
  - j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the `-w` option must not be specified.
  - a Directory of the backup files.
  - v Verbose mode.
  - t Database type. Currently, `ldbm` is the only possible type and the default value.
- 

## db2bak.pl (Create backup of database)

This perl script `db2bak.pl` creates an entry in the directory that launches this dynamic task. An entry is generated based upon the values you provide for each option.

### Syntax

Command (Solaris 9) `directoryserver db2bak-task options`

Perl script (All others) `db2bak.pl options`

*options* `[-v] -D rootDN {-w password | -w - | -j filename } [-a backup_directory] [-t databasetype]`

### Options

- 
- D User DN with root permissions, such as Directory Manager. The default is the DN of the directory manager which is read from the `nsslapd-root` attribute under `cn=config`.
  - w Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify `-w -`, the utility prompts for the password. If either `-w` option is specified, the `-j` option must not be specified. For example, `-w diner892`.
  - j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the `-w` option must not be specified.
-

- 
- a Directory where the backup files will be stored. By default it is under *installDir/slapd-serverID/bak*.  
The backup file is named according to the year-month-day-hour format (YYYY\_MM\_DD\_hh\_mm\_ss).
  - v Verbose mode.
  - t Database type. Currently, *ldbm* is the only possible type and the default value.
- 

## db2index.pl (Create and generate 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

Command (Solaris 9) `directoryserver db2index-task options`

Perl script (All others) `db2bindex.pl options`

*options* `[-v] -D rootDN { -w password | -w - | -j filename }  
-n backend_instance [-t attributeName]`

### Options

- 
- D User DN with root permissions, such as Directory Manager.
  - w Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify `-w -`, the utility prompts for the password. If either `-w` option is specified, the `-j` option must not be specified. For example, `-w diner892`.
  - j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the `-w` option must not be specified.
  - n Instance to be indexed.
  - t Name of the attribute to be indexed. If omitted, all indexes defined for that instance are generated.
  - v Verbose mode.
-



---

**NOTE** This perl script `db2index.pl` creates an entry in the directory that launches this dynamic task. An entry is generated based upon the values you provide for each option.

---

## db2ldif.pl (Export database contents to LDIF)

Exports the contents of the database to LDIF. This Perl script creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values you provide for each option. The \* indicates that multiple occurrences are allowed.

### Syntax

Command (Solaris 9) `directoryserver db2ldif-task options`

Perl script (All others) `db2ldif.pl options`

*options* `[-v] -D rootDN {-w password | -w - | -j filename }  
 {-n backend_instance}* |  
 {-s includesuffix}* [ {-x excludesuffix}* ]  
 [-a outfile] [-N] [-r] [-C] [-u] [-U] [-m] [-o]  
 [-l] [M]`

---

**CAUTION** To run this script the server must be running and either `-n backend_instance` or `-s includesuffix` is required.

This perl script `bak2db.pl` creates an entry in the directory that launches this dynamic task. An entry is generated based upon the values you provide for each option.

---

### Options

- 
- `-D` User DN with root permissions, such as Directory Manager.
  - `-w` Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify `-w -`, the utility prompts for the password. If either `-w` option is specified, the `-j` option must not be specified. For example, `-w diner892`.
-

- 
- j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the -w option must not be specified.
  - n Instance to be exported.
  - a File name of the output LDIF file.
  - s Suffix(es) to be included or to specify the subtree(s) to be included if -n has been used.
  - x Suffix(es) to be excluded.
  - m Minimal base64 encoding.
  - o Output LDIF to be stored in one file by default with each *instance* stored in *instance\_outfile*.
  - r Export replica.
  - u Request that the unique id is not exported.
  - C Only the main db file is used.
  - N Suppress printing sequential number.
  - U Request that the output LDIF is not folded.
  - v Verbose mode.
  - 1 Delete, for reasons of backward compatibility the first line of the LDIF file that gives the version of the LDIF standard.
  - M Output LDIF is stored in multiple files.
- 

## ldif2db.pl (Import)

To run this Perl script, the server must be running. This script creates an entry in the directory that launches this dynamic task. The entry is generated based upon the values you provide for each option.

### Syntax

Command (Solaris 9) `directoryserver ldif2db options`

Perl script (All others) `ldif2db.pl options`

*options* `[-v] -D rootDN {-w password | -w - | -j filename }  
 -n backend_instance |  
 {-s includesuffix}* [ {-x excludesuffix}* ]  
 [-O] [-c] [-g string] [-G namespace_id] {-i filename}*`

## Options

---

-D	User DN with root permissions, such as Directory Manager.
-w	Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .
-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-n	Instance to be imported.
-i	File name of the input LDIF file(s). When you import multiple files, they are imported in the order in which you specify them on the command line.
-s	Suffix(es) to be included or to specify the subtree(s) to be included if <code>-n</code> has been used.
-x	Suffix(es) to be excluded.
-O	Request that only the core db is created without attribute indexes.
-c	Merge chunk size.
-g <i>string</i>	<p>Generation of 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>If you use the <code>deterministic</code> generation to have a name-based unique ID, you can also specify the namespace you want the server to use as follows:</p> <pre>-g deterministic namespace_id</pre> <p>where <code>namespace_id</code> is a string of characters in the following format</p> <pre>00-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx</pre> <p>Use this option if you want to import the same LDIF file into two different directory servers, and if you want the contents of both directories to have the same set of unique IDs. If unique IDs already exist in the LDIF file you are importing, then the existing IDs are imported to the server regardless of the options you have specified.</p>
-G <i>namespace_id</i>	Generates a namespace ID as a name-based unique ID. This is the same as specifying the <code>-g deterministic</code> option.
-v	Verbose mode.

---

---

**NOTE** This perl script `ldif2db.pl` creates an entry in the directory that launches this dynamic task. An entry is generated based upon the values you provide for each option.

---

## migrateInstance5 (Migrate to Directory Server 5.0 or 5.1)

The `migrateInstance5` Perl script (note that this is a Perl script despite the fact that it does not have the `.pl` extension) migrates a 4.x Directory Server to Directory Server 5.0 or 5.1. It can also be used to upgrade from Directory Server 5.0 to Directory Server 5.1.

When you run this script, it migrates the configuration files or configuration entries, database instances and schema with minimum manual intervention. The `migrateInstance5` script calls on the `migrateTo5` script which then executes the migration.

For complete information on the configuration parameters and attributes that are migrated, see Chapter 6, “Migration from Earlier Versions.”

Before performing the migration, check that the user-defined variables contain the following associated values, where `installDir` is the path to where iPlanet Directory Server 5.1 is installed:

```
SPERL5LIB          installDir/bin/slapd/admin/bin
PATH               installDir/bin/slapd/admin/bin
```

### Syntax

```
Perl script (All others) migrateInstance5
                        -D rootDN { -w password | -w - | -j filename }
                        -n backend_instance -p port
                        -o 4.xInstancePath -n 5.0InstancePath [-t] [-L]
```

## Options

---

-D	Directory Server 5.1 userDN with root permissions, such as Directory Manager.
-w	Password associated with the Directory Server 5.1 user DN. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .
-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-p	Directory Server 5.1 port.
-o <i>4.xInstancePath</i>	Netscape Directory Server 4.x.
-n <i>5.0InstancePath</i>	Path for the new Directory Server 5.0 instance.
-t	Trace level. The trace level is set to 0 by default with a valid range of 0 to 3.
-L	File in which to log the migration report. By default the migration report is stored under <code>installDir/slapd-serverID/logs/Migration_ddmmyyy_hhmmss.log</code> . A sample log might contain:  <code>/usr/iplanet/servers/slapd-serverID/logs/Migration_20022001_153604.log</code> for a log created on 20 February 2001 at 15:36:04.

---

## ns-accountstatus.pl (Establish account status)

Provides account status information to establish whether an entry or group of entries is inactivated or not.

### Syntax

Command (Solaris 9) `directoryserver account-status options`

Perl script (All others) `ns-accountstatus.pl options`

*options* `[-D rootDN] {-w password | -w - | -j filename } [-h host] [-p port] -I DN`

## Options

---

-D	Directory Server 5.1 userDN with root permissions, such as Directory Manager.
-w	Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .
-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-p	Directory Server 5.1 port. The default value is the LDAP port of Directory Server 5.1 specified at installation time.
-h	Host name of Directory Server 5.1. The default value is the full host name of the machine where Directory Server 5.1. is installed.
-I <i>DN</i>	Entry DN or role DN whose status is required.

---

## ns-activate.pl (Activate an entry or group of entries)

Activates an entry or group of entries.

### Syntax

Command (Solaris 9) `directoryserver account-activate options`

Perl script (All others) `ns-activate.pl options`

*options* `[-D rootDN] {-w password | -w - | -j filename }  
[-h host] [-p port] -I DN`

### Options

---

-D	Directory Server 5.1 userDN with root permissions, such as Directory Manager.
-w	Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .

---

---

-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-p	Directory Server 5.1 port. The default value is the LDAP port of Directory Server 5.1 specified at installation time.
-h	Host name of Directory Server 5.1. The default value is the full hostname of the machine where Directory Server 5.1. is installed.
-I <i>DN</i>	Entry DN or role DN to activate.

---

## ns-inactivate.pl (Inactivate an entry or group of entries)

Inactivates, and thus locks, an entry or group of entries.

### Syntax

Command (Solaris 9) `directoryserver account-inactivate options`

Perl script (All others) `ns-inactivate.pl options`

*options* `[-D rootDN] {-w password | -w - | -j filename }  
[-h host] [-p port] -I DN`

### Options

---

-D	Directory Server 5.1 userDN with root permissions, such as Directory Manager.
-w	Password associated with the user DN. If you do not specify this option, anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .
-j	Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the <code>-w</code> option must not be specified.
-p	Directory Server 5.1 port. The default value is the LDAP port of Directory Server 5.1 specified at installation time.
-h	Host name of Directory Server 5.1. The default value is the full hostname of the machine where Directory Server 5.1. is installed.
-I <i>DN</i>	Entry DN or role DN to inactivate.

---





# Using the ns-slapd and slapd.exe Command-Line Utilities

In Chapter 8, “Command-Line Scripts,” we looked at the scripts for performing routine administration tasks on the Directory Server. In this Appendix we will look at the `ns-slapd` (UNIX) and `slapd.exe` (Windows) command-line utilities that can also be used to perform the same tasks. This chapter contains the following sections:

- Overview of ns-slapd and slapd.exe Commands
- Finding and Executing the ns-slapd and slapd.exe Command-Line Utilities
- ns-slapd and slapd.exe Command-Line Utilities for Exporting Databases
- ns-slapd and slapd.exe Command-Line Utilities for Restoring and Backing up Databases
- ns-slapd and slapd.exe Command-Line Utilities for Creating and Regenerating Indexes

## Overview of ns-slapd and slapd.exe Commands

The `ns-slapd` and `slapd.exe` command-line utilities all perform server administration tasks, and while it can be argued that they allow a greater degree of flexibility for users, we still recommend that you use the command-line scripts presented in Chapter 8, “Command-Line Scripts”.

## ns-slapd (UNIX)

`ns-slapd` is used on a UNIX operating system 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, see Chapter 3, “Populating Directory Databases” in the *iPlanet Directory Server Administrator’s Guide*.

## slapd.exe (Windows NT)

`slapd.exe` is the `ns-slapd` Windows NT equivalent

---

**NOTE** You must stop the server before running the `ns-slapd` and `slapd.exe` command-line utilities.

---

# Finding and Executing the ns-slapd and slapd.exe Command-Line Utilities

After a default installation, the `ns-slapd` command line utilities are stored under the following paths and names:

<b>Solaris 9 platform</b>	<code>/usr/iplanet/ds5/bin/slapd/server/ns-slapd</code>
<b>Windows platforms</b>	<code>\iPlanet\Servers\bin\slapd\server\slapd.exe</code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/bin/slapd/server/ns-slapd</code>

Do not mistake `ns-slapd.exe`, the `slapd` process watchdog, for `slapd.exe` on Windows NT.

---

**CAUTION** In order to execute the command line utilities, you must change to the directory where the command line utilities are stored. Although it is possible to set command path and library path variables to execute the utilities, this is *not* recommended procedure. You run the risk of disrupting the correct execution of other utilities and of compromising the security of the system, particularly when you have more than one server version installed.

---

# ns-slapd and slapd.exe Command-Line Utilities for Exporting Databases

## db2ldif

Exports the contents of the database to LDIF.

### Shell syntax (UNIX)

```
ns-slapd db2ldif -D slapd-serverID -a output_file [-d debug_level] [-n
backend_instance] [-r] [-s include_suffix] [-x exclude_suffix] [-N] [-u] [-U]
```

where `slapd-serverID` is the location of your server configuration directory. Enter the full path to the `slapd-serverID` directory.

### Batch file syntax (NT)

```
slapd.exe db2ldif -D slapd-serverID -a output_file [-d debug_level] [-n
backend_instance] [-r] [-s include_suffix] [-x exclude_suffix] [-N] [-u] [-U]
```

---

**NOTE** You must specify either the `-n` or the `-s` option.

---

### Options

- a 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 Specifies the debug level to use during the `db2ldif` runtime. For further information, see “`nsslapd-errorlog-level (Error Log Level)`” on page 49.
- D Specifies the server configuration directory that contains the configuration information for the export process. You *must* specify the full path to the `slapd-serverID` directory.

- N** Specifies that entry IDs are not to be included in the LDIF output. The entry IDs are necessary only if the `db2ldif` output is to be used as input to `db2index`.
- r** Causes the server to include the `copiedFrom` attribute and its contents in the LDIF output when importing the LDIF file to a consumer server. This information is required by the server by the replication process.

Note that if you use the `-r` option, you also need to specify the suffix you want to export by using the `-s` option. You *must* shut down the server before exporting using this option.
- s** Specifies the suffix or suffixes to include in the export. You may use multiple `-s` arguments. If you do not specify `-s` or `-x`, the server exports all suffixes within the database. If you use both `-x` and `-s` arguments with the same suffix, the `-x` operation takes precedence. *Exclusion always takes precedence over inclusion.*

Note if you exclude one or more suffixes from the exported LDIF file, and you intend to import the LDIF file into your configuration directory, *do not* exclude `o=NetscapeRoot`. If you use `-s` to specify a suffix to include, and you intend to import the LDIF file into your configuration directory, make sure that you also use `-s` to include `o=NetscapeRoot`.
- 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.

Use this option if you intend to use the exported LDIF to initialize a 4.x consumer server. However, do not use this option when you are importing into a 5.0 consumer, as it 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** Specifies a suffix or suffixes to exclude in the export. You may use multiple `-x` arguments. If you do not specify `-s` or `-x`, the server exports all suffixes within the database. If you use both `-x` and `-s` options with the same suffix, the `-x` operation takes precedence. *Exclusion always takes precedence over inclusion.* If you intend to import the LDIF file into your configuration directory, *do not* exclude `o=NetscapeRoot`.
- n** Specifies the name of the backend instance to be exported.

# ns-slapd and slapd.exe Command-Line Utilities for Restoring and Backing up Databases

## ldif2db

Imports LDIF files to the database.

### Shell script syntax (UNIX)

```
ns-slapd ldif2db -D slapd-serverID -i ldif_file [-d debug_level]
[-g string] [-n backend_instance] -O [-s include_suffix] -x exclude_suffix
```

where *ldif\_file* is the name of the file containing the LDIF to be imported and *slapd-serverID* is the location of your server configuration directory. You can find a sample LDIF file under *installDir*/*slapd-serverID*/ldif. Enter the full path to the *slapd-serverID* directory, by default:

<b>Solaris 9 platform</b>	<code>/var/ds5/slapd-<i>serverID</i></code>
<b>Windows platforms</b>	<code>\iPlanet\Servers\slapd-<i>serverID</i></code>
<b>Other platforms</b>	<code>/usr/iplanet/servers/slapd-<i>serverID</i></code>

### Batch file syntax (NT)

```
slapd ldif2db -D slapd-serverID -i ldif_file [-d debug_level] [-g string]
[-n backend_instance] [-O] [-s include_suffix] [-x exclude_suffix]
```

---

**NOTE** You must specify either the `-n` or the `-s` option.

---

### Options

`-d` Specifies the debug level to use during runtime. For further information, see “nsslapd-errorlog-level (Error Log Level)” on page 49.

- D            Specifies the server configuration directory that contains the configuration information for the import process. You *must* specify the full path to the `slapd-serverID` directory.
- g *string*    Generation of a unique ID. Type `none` for no unique ID to be generated and `deterministic` for the generated unique ID to be name-based. By default, a time-based unique ID is generated.  
  
If you use the `deterministic` generation to have a name-based unique ID, you can also specify the namespace you want the server to use as follows:  
  
`-g deterministic namespace_id`  
  
where `namespace_id` is a string of characters in the following format  
  
`00-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx`  
  
Use this option if you want to import the same LDIF file into two different directory servers, and if you want the contents of both directories to have the same set of unique IDs. If unique IDs already exist in the LDIF file you are importing, then the existing IDs are imported to the server regardless of the options you have specified.
- i            Specifies the LDIF file to be imported. This option is required. You can use multiple `-i` arguments to import more than one LDIF file at a time. When you import multiple files, the server imports the LDIF files in the order in which you specify them from the command line.
- n            Specifies the name of the backend to be imported.
- O            Specifies that no attribute indexes are created for the imported database. If you specify this option and you want to restore the indexes later, you will need to recreate the indexes by hand. See the *iPlanet Directory Server Administrator's Guide* for further information.
- s            Specifies the suffix or suffixes within the LDIF file you want to import. If you use `-s` to specify a suffix to include, and you are importing the LDIF file into your configuration directory, make sure that you also use `-s` to include `o=NetscapeRoot`. You can use multiple `-s` arguments. If you use both `-x` and `-s` with the same suffix, `-x` takes precedence. *Exclusion always takes precedence over inclusion*. If you do not specify `-x` or `-s`, then all available suffixes will be imported from the LDIF file.
- x            Allows you to specify suffixes within the LDIF file to exclude during the import. You can use multiple `-x` arguments. This option lets you selectively import portions of the LDIF file. If you use both `-x` and `-s` with the same suffix, `-x` takes precedence. *Exclusion always takes precedence over inclusion*. If you do not specify `-x` or `-s`, then all available suffixes will be imported from the LDIF file. If you are importing the LDIF file into your configuration directory, *do not* exclude `o=NetscapeRoot`.

---

**CAUTION** If you are importing the LDIF file into your configuration directory, make sure the `o=NetscapeRoot` suffix and its contents are included in your LDIF file *before* you import. Do not exclude the suffix `o=NetscapeRoot` using `-s`, `-x`, or combination of the two. The iPlanet Administration Server uses this suffix to store information about installed Netscape Servers. Failure to import `o=NetscapeRoot` into your configuration directory could force you to reinstall (or restore from backup) all of your Netscape 4.x servers including the Directory Server.

---

## archive2db

Restores database from the archives.

### Shell script syntax (UNIX)

```
slapd archive2db -D configdir -a archivedir
```

### Batch file syntax (NT)

```
slapd archive2db -D configdir -a archivedir
```

### Options

- D Specifies the server configuration directory that contains the configuration information for the index creation process. You *must* specify the full path to the `slapd-serverID` directory.
- a Specifies the archive directory.

## db2archive

Backs up all databases to the archives.

### Shell script syntax (UNIX)

```
slapd db2archive -D configdir -a archivedir
```

### Batch file syntax (NT)

```
slapd db2archive -D configdir -a archivedir
```

### Options

- D Specifies the server configuration directory that contains the configuration information for the index creation process. You *must* specify the full path to the `slapd-serverID` directory.
- a Specifies the archive directory.

# ns-slapd and slapd.exe Command-Line Utilities for Creating and Regenerating Indexes

## db2index

Creates and regenerates indexes.

### Shell script syntax (UNIX)

```
slapd db2index -D slapd-serverID [-d debug_level] -n backend_name  
-t attributeName[ : indexTypes[ : matchingRules] ] | [-T VLVTag]
```

### Batch file syntax (NT)

```
slapd db2index -D slapd-serverID [-d debug_level] -n backend_name  
-t attributeName[ : indexTypes[ : matchingRules] ] | [-T VLVTag]
```



## Options

- d Specifies the debug level to use during index creation. For further information see “nsslapd-errorlog-level (Error Log Level)” on page 49.
- D Specifies the server configuration directory that contains the configuration information for the index creation process. You must specify the full path to the `slapd-serverID` directory.
- n Specifies the name of the backend containing the entries to index.
- t Specifies the attribute to be indexed as well as the types of indexes to create and matching rules to apply (if any). If you want to specify a matching rule, you must specify an index type. You cannot use this option with option `-T`.
- T Specifies the VLV tag to use to create VLV indexes. You can use the console to specify VLV tags for each database supporting your directory tree, as described in xref. You can define additional VLV tags by creating them in LDIF, and adding them in the directory server configuration, as described in xref. You cannot use this option with option `-t`.
- :indexTypes* A comma separated list of indexes to be created for the attributes.
- :matchingRules* An optional, comma-separated list of the OIDs for the languages in which you want the attribute to be indexed. This option is used to created international indexes. For information on supported locales and collation order OIDs, see Appendix D, “Internationalization” in the *iPlanet Directory Server Administrator’s Guide*.



# Glossary

**access control instruction** *See ACI.*

**ACI** Access Control Instruction. An instruction that grants or denies permissions to entries in the directory.

**access control list** *See ACL.*

**ACL** Access control list. The mechanism for controlling access to your directory.

**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, self-write, 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** 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.

**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 bind host.

**authentication** (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 to access files and directories based on the permissions granted to that user by the directory administrator.

(2) Allows a client 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.

**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.

**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 base DN.*

**bind DN** Distinguished name used to authenticate to Directory Server when performing an operation.

**bind distinguished name** *See bind DN.*

**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 Netscape Navigator, 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** Otherwise known as the virtual view index, speeds up the display of entries in the Directory Server Console. Browsing indexes can be created on any branchpoint in the directory tree to improve display performance.

**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 change log. 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 within 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.

**chaining** A method for relaying requests to another server. Results for the request are collected, compiled and then returned to the client.

**change log** A change log 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 consumer 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.

**CIR** *See consumer-initiated replication.*

**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 CoS.*

**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 LDAP client.*

**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-initiated replication** Replication configuration where consumer servers pull directory data from supplier servers.

**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.

**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 CoS definition entry.*

**Directory Access Protocol** *See DAP.*

**directory tree** The logical representation of the information stored in the directory. It mirrors the tree model used by most file systems, with the tree's root point appearing at the top of the hierarchy. Also known as DIT.

**Directory Manager** The privileged database administrator, comparable to the root user in UNIX. Access control does not apply to the directory manager.

**Directory Server Console** An LDAP client application that provides a graphic user interface to browse, configure, and manage the contents of your directory. It is a component of the iPlanet Directory Server product.

**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 directory tree.*

**DM** *See Directory Manager.*

**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 `www.iPlanet.com`). 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.

**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.

**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.

**general access** When granted, indicates that all authenticated users can access directory information.

**hostname** A name for a machine in the form `machine.domain.dom`, which is translated into an IP address. For example, `www.iPlanet.com` is the machine `www` in the subdomain `iPlanet` and `com` 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 Netscape Navigator how to display text, position graphics and form items, and 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 `httpd`.

**HTTP-NG** The next generation of Hypertext Transfer Protocol.

**HTTPS** A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.

**hub supplier** 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 cascading replication.

**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** *See ISO.*

**IP address** Internet Protocol address. 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

**knowledge reference** Pointers to directory information stored in different databases.

**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 *browser*.

**LDAP Data Interchange Format** *See LDIF.*

**LDAP URL** Provides the means of locating directory servers using DNS and then completing the query via LDAP. A sample LDAP URL is

`ldap://ldap.ipplanet.com`

**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.

**Lightweight Directory Access Protocol** *See LDAP.*

**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.

**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** Allow you to create an explicit enumerated list of members.

**management information base** *See MIB.*

**mapping tree** A data structure that associates the names of suffixes (subtrees) with databases.

**master agent** *See SNMP master agent.*

**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 Namespace. The means for directory data to be named and referenced. Also called the directory tree.

**monetary format** Specifies the monetary symbol used by a 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 change log 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 + 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** Allow you to create roles that contain other roles.

**network management application** Network Management Station component that graphically displays information about SNMP managed devices (which device is up or down, which and how many error messages were received, etc.).

**network management station** *See NMS.*

**NIS** Network Information Service. A system of programs and data files that Unix machines use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computers.

**NMS** Network Management Station. Powerful workstation with one or more network management applications installed.

**ns-slapd** IPlanet's LDAP Directory Server daemon or service that is responsible for all actions of the Directory Server. See also `slapd`.

**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.

**OID** See *object identifier*.

**operational attribute** Operational attributes contain information used internally by the directory to keep track of modifications and subtree properties. They are not returned in response to a search unless explicitly requested.

**parent access** When granted, indicates that users have access to entries below their own in the directory tree, that is, if the bind DN is the parent of the targeted entry.

**pass-through authentication** See *PTA*.

**pass-through subtree** In pass-through authentication, the PTA directory server will pass through bind requests to the authenticating directory server 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 `/etc/passwd`, because of where it is kept.

**password policy** A set of rules that govern how passwords are used in a given directory.

**permission** In the context of access control, the permission states whether access to the directory information is granted or denied, and the level of access that is granted or denied. See *access rights*.

**PDU** Protocol Data Unit. Encoded messages which form the basis of data exchanges between SNMP devices.

**pointer CoS** A pointer CoS identifies the template entry using the template DN only.

**presence index** Allows you to search for entries that contain a specific indexed attribute.

**protocol** A set of rules that describes how devices on a network exchange information.

**protocol data unit** *See PDU.*

**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** Pass-through authentication. Mechanism by which one directory server consults another to check bind credentials.

**PTA directory server** In pass-through authentication (PTA), the PTA directory server is the server that sends (passes through) bind requests it receives to the authenticating directory server.

**PTA LDAP URL** In pass-through authentication, the URL that defines the authenticating directory server, pass-through subtree(s) and optional parameters.

**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 `/etc/rc.local` because of its location.

**RDN** Relative distinguished name. The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name.

**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 a pointer back to the client to the LDAP server 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.

**replica** A database that participates in replication

**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 RDN.*

**replication** Act of copying directory trees or subtrees from supplier servers to consumer servers.

**replication agreement** Set of configuration parameters that are stored on the supplier server and identify the databases to replicate, the consumer 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 *members*, 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.

**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 SSL.*

**self access** When granted, indicates that users have access to their own entries, that is, if the bind DN matches the targeted entry.

**server daemon** The server daemon is a process that, once running, listens for and accepts requests from clients.

**server service** The server service is a process on Windows NT that, once running, listens for and accepts requests from clients. It is the SMB server on Windows NT.

**server root** A directory on the server machine dedicated to holding the server program and configuration, maintenance, and information files.

**Server Selector** Interface that allows you to select and configure servers using a browser.

**service** A background process on a Windows NT machine that is responsible for a particular system task. Service processes do not need human intervention to continue functioning.

**SIE** Server Instance Entry.

**Simple Network Management Protocol** *See SNMP.*

**single-master replication** The most basic replication scenario in which two servers each hold a copy of the same read-write replicas to consumer servers. In a single-master replication scenario, the supplier server maintains a change log.

**SIR** *See supplier-initiated replication.*

**slapd** LDAP Directory Server daemon or service that is responsible for most functions of a directory except replication. *See also ns-slapd.*

**SNMP** Simple Network Management Protocol. Used to monitor and manage application processes running on the servers, by exchanging data about network activity.

**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.

**SSL** Secure Sockets Layer. A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP.

**standard index** Indexes that are maintained by default.

**sub suffix** A branch underneath a root suffix.

**subagent** *See SNMP subagent.*

**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 (also called root). The superuser has complete access privileges to all files on the machine.

**supplier** Server containing the master copy of directory trees or subtrees that are replicated to consumer 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 supplier servers replicate directory data to consumer 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.

**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 CoS template entry.*

**time / date format** Indicates the customary formatting for times and dates in a specific region.

**TLS** Transport Layer Security. The new standard for secure socket layers, a public key based protocol.

**topology** The way a directory tree is divided among physical servers and how these servers link with one another.

**Transport Layer Security** *See TLS.*

**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 `[protocol]://[machine:port]/[document]`. 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.

**virtual list view index** Otherwise known as a browsing index, speeds up the display of entries in the Directory Server Console. Virtual list view indexes can be created on any branchpoint in the directory tree to improve display performance.

**X.500 standard** The set of ISO/ITU-T documents outlining the recommended information model, object classes and attributes used by directory server implementations.



## SYMBOLS

::, in LDIF statements 223

## NUMERICS

00core.ldif

ldif files 105

05rfc2247.ldif

ldif files 105

05rfc2927.ldif

ldif files 105

10rfc2307.ldif

ldif files 105

20subscriber.ldif

ldif files 105

25java-object.ldif

ldif files 105

28pilot.ldif

ldif files 105

30ns-common.ldif

ldif files 105

50ns-admin.ldif

ldif files 105

50ns-calendar.ldif

ldif files 105

50ns-certificate.ldif

ldif files 106

50ns-compass.ldif

ldif files 106

50ns-delegated-admin.ldif

ldif files 106

50ns-directory.ldif

ldif files 106

50ns-legacy.ldif

ldif files 106

50ns-mail.ldif

ldif files 106

50ns-mcd-browser.ldif

ldif files 106

50ns-mcd-config.ldif

ldif files 106

50ns-mcd-li.ldif

ldif files 106

50ns-mcd-mail.ldif

ldif files 106

50ns-media.ldif

ldif files 106

50ns-mlm.ldif

ldif files 106

50ns-msg.ldif

ldif files 106

50ns-netshare.ldif

ldif files 106

50ns-news.ldif

ldif files 106

50ns-proxy.ldif

ldif files 106

50ns-value.ldif

ldif files 106

50ns-wcal.ldif

ldif files 106

- 50ns-web.ldif
  - ldif files 106
- 99user.ldif
  - ldif files 107

## A

- alias dereferencing 215

## B

- backendMonitorDN attribute 101
- backup files 176
- bak2db
  - command-line shell and batch script 228
  - quick reference 226
- bak2db.pl
  - command-line perl script 238
  - quick reference 227
- Base 223
- base 64 encoding 223
- binary data, LDIF and 223
- bytessentattribute 100

## C

- changelog
  - multi-master replication changelog 79
- changelog configuration attributes
  - changelogmaxentries 80
  - nsslapd-changelogdir 79
  - nsslapd-changelogmaxage 80
- changelog configuration entries
  - cn=changelog5 79
- ciphers
  - list of 83
- cn attribute 86, 155
- cn=changelog5

- changelog configuration entries 79
- object classes 79
- cn=config
  - general 23
  - general configuration entries 33
  - object classes 33
- cn=config Directory Information Tree
  - configuration data 24
- cn=encryption
  - encryption configuration entries 81
  - object classes 81
- cn=mapping tree
  - object classes 84
  - suffix and replication configuration entries 84
- cn=monitor
  - object classes 99
  - read-only monitoring configuration entries 99
- cn=NetscapeRoot
  - configuration 27
- cn=SNMP
  - object classes 101
  - SNMP configuration entries 101
- cn=uniqueid generator
  - object classes 104
  - uniqueid generator configuration entries 104
- cn=UserRoot
  - configuration 27
- command-line scripts
  - bak2db 228
  - bak2db.pl 238
  - db2bak 229
  - db2bak.pl 239
  - db2index.pl 240
  - db2ldif 229
  - db2ldif.pl 241
  - getpwenc 231
  - ldif2db 231
  - ldif2db.pl 242
  - ldif2ldap 233
  - monitor 233
  - ns-accountstatus.pl 245
  - ns-activate.pl 246
  - ns-inactivate.pl 247
  - perl scripts 238–247, ??–247
  - quick reference 225–228
  - restart-slapd 234

- restoreconf 234
- saveconfig 235
- shell and batch scripts 228–238
- start-slapd 235
- stop-slapd 236
- suffix2instance 236
- vlvindex 237
- command-line utilities
  - finding and executing 209
  - ldapdelete 221–??
  - ldapmodify 217–??
  - ldapsearch 211–??
  - ldif 223–??
- Configuration
  - plug-in functionality 26
- configuration
  - access control 28
  - accessing and modifying 28
  - changing attributes 29
  - cn=NetscapeRoot 27
  - cn=UserRoot 27
  - database-specific 24
  - overview 23
- configuration attributes
  - changelog5 configuration attributes 79–81
  - changing 29
  - core server configuration attributes 32–104
  - database link plug-in configuration
    - attributes 162–172
  - database plug-in configuration
    - attributes 133–158
  - encryption configuration attributes 81–83
  - mapping tree configuration attributes 84–99
  - monitoring configuration attributes 99–101
  - overview 25
  - plug-in functionality configuration
    - attributes 129–172
  - plug-in functionality configuration attributes
    - allowed by certain plug-ins 132–133
  - plug-in functionality configuration attributes
    - common to all plug-ins 129–132
  - replication agreement configuration
    - attributes 91–99
  - replication configuration attributes 86–91
  - restrictions to modifying 31
  - retro changelog plug-in configuration
    - attributes 173–174
  - SNMP configuration attributes 101–103
  - suffix configuration attributes 85–86
  - uniqueid generator configuration attributes 104
- configuration changes
  - requiring server restart 31, 107
- configuration entries
  - modifying using LDAP 30
  - restrictions to modifying 31
- configuration files 177
  - location of 28
- configuration files, pre-5.0
  - migration to LDIF format 28
- configuration information tree
  - dse.ldif file 32
- connection attribute 99
- core server configuration attributes
  - backendMonitorDN 101
  - bytessent 100
  - cn 86
  - connection 99
  - currentconnection 100
  - currenttime 100
  - description 92
  - dtablesize 100
  - entriessent 100
  - nbackends 100
  - nsDS50ruv 99
  - nsDS5Flags 87
  - nsDS5ReplicaBindDN 87, 92
  - nsDS5ReplicaBindMethod 92
  - nsDS5ReplicaChangeCount 88
  - nsDS5ReplicaChangesSentSinceStartup 93
  - nsDS5ReplicaCredentials 93
  - nsDS5ReplicaHost 94
  - nsDS5ReplicaID 88
  - nsDS5ReplicaLastInitEnd 94
  - nsDS5ReplicaLastInitStart 94
  - nsDS5ReplicaLastInitStatus 95
  - nsDS5ReplicaLastUpdateEnd 95
  - nsDS5ReplicaLastUpdateStart 96
  - nsDS5ReplicaLastUpdateStatus 96
  - nsDS5ReplicaLegacyConsumer 89
  - nsDS5ReplicaName 89
  - nsDS5ReplicaPort 96
  - nsDS5ReplicaPurgeDelay 89
  - nsDS5ReplicaReferral 90

nsDS5ReplicaRefresh 97  
 nsDS5ReplicaRoot 90, 97  
 nsDS5ReplicaTimeout 97  
 nsDS5ReplicaTombstonePurgeInterval 90  
 nsDS5ReplicaTransportInfo 98  
 nsDS5ReplicaType 91  
 nsDS5ReplicaUpdateInProgress 38  
 nsDS5ReplicaUpdateSchedule 99  
 nsIdleTimeout 33  
 nsslapd-accesscontrol 34  
 nsslapd-accesslog 34  
 nsslapd-accesslog-level 35  
 nsslapd-accesslog-list 36  
 nsslapd-accesslog-logbuffering 36  
 nsslapd-accesslog-logexpirationtime 36, 71  
 nsslapd-accesslog-logexpirationtimeunit 37, 39  
 nsslapd-accesslog-logging-enabled 37  
 nsslapd-accesslog-logmaxdiskspace 37  
 nsslapd-accesslog-logminfreediskspace 38  
 nsslapd-accesslog-logrotationtime 38  
 nsslapd-accesslog-maxlogsize 39  
 nsslapd-accesslog-maxlogsperdir 40  
 nsslapd-attribute-name-exceptions 40  
 nsslapd-auditlog-list 42  
 nsslapd-auditlog-logexpirationtime 42  
 nsslapd-auditlog-logexpirationtimeunit 42  
 nsslapd-auditlog-logging-enabled 43  
 nsslapd-auditlog-logmaxdiskspace 43  
 nsslapd-auditlog-logminfreediskspace 44  
 nsslapd-auditlog-logrotationtime 44  
 nsslapd-auditlog-logrotationtimeunit 45  
 nsslapd-auditlog-maxlogsize 45  
 nsslapd-auditlog-maxlogsperdir 46  
 nsslapd-backend 85  
 nsslapd-certmap-basedn 46  
 nsslapd-changelogdir 79  
 nsslapd-changelogmaxage 80  
 nsslapd-changelogmaxentries 80  
 nsslapd-config 47  
 nsslapd-ds4-compatible-schema 47  
 nsslapd-errorlog 48  
 nsslapd-errorlog-level 49  
 nsslapd-errorlog-llist 50  
 nsslapd-errorlog-logexpirationtime 51  
 nsslapd-errorlog-logexpirationtimeunit 51  
 nsslapd-errorlog-logging-enabled 51  
 nsslapd-errorlog-logmaxdiskspace 52  
 nsslapd-errorlog-logminfreediskspace 52  
 nsslapd-errorlog-logrotationtime 53  
 nsslapd-errorlog-logrotationtimeunit 53  
 nsslapd-errorlog-maxlogsize 54  
 nsslapd-errorlog-maxlogsperdir 54  
 nsslapd-groupvalnestlevel 55  
 nsslapd-instancedir 55  
 nsslapd-ioblocktimeout 55  
 nsslapd-lastmod 56  
 nsslapd-listenhost 56  
 nsslapd-localhost 57  
 nsslapd-localuser 57  
 nsslapd-maxbersize 58  
 nsslapd-maxdescriptors 58  
 nsslapd-maxthreadsperconn 59  
 nsslapd-nagle 60  
 nsslapd-plug-in 60  
 nsslapd-port 60  
 nsslapd-privatenamespaces 61  
 nsslapd-readonly 61  
 nsslapd-referral 61  
 nsslapd-referralmode 62  
 nsslapd-reservedescriptors 62  
 nsslapd-return-exact-case 64  
 nsslapd-rootdn 65  
 nsslapd-rootpw 65  
 nsslapd-rootpwstoragescheme 66  
 nsslapd-schemacheck 66  
 nsslapd-securelistenhost 67  
 nsslapd-securePort 68  
 nsslapd-security 68  
 nsslapd-sizelimit 68  
 nsslapd-SSL3ciphers 69  
 nsslapd-state 85  
 nsslapd-threadnumber 69  
 nsslapd-timelimit 69  
 nsslapd-versionstring 71  
 nssnmpcontact 102  
 nssnmpdescription 102  
 nssnmpenabled 101  
 nssnmplocation 102  
 nssnmpmasterhost 103  
 nssnmpmasterport 103  
 nssnmporganization 101  
 nsssl2 attribute 82  
 nsssl3 attribute 82

- nssl3ciphers attribute 82
- nsslclientauth attribute 81
- nsslsessiontimeout attribute 81
- nsState 91
- nsstate 104
- opscompleted 100
- opsinitiated 100
- passwordCheckSyntax 72
- passwordExp 72
- passwordHistory 73
- passwordInHistory 73
- passwordLockout 74
- passwordLockoutDuration 74
- passwordMaxAge 75
- passwordMaxFailure 75
- passwordMinAge 75
- passwordMinLength 76
- passwordMustChange 76
- passwordResetFailureCount 77
- passwordStorageScheme 77
- passwordUnlock 78
- passwordWarning 78
- readwaiters 100
- starttime 100
- totalconnections 100
- currentconnections attribute 100
- currenttime attribute 100

**D**

- database
  - exporting 229
- database files 177
- database link plug-in configuration attributes
  - nsAbandonCount 172
  - nsAbandonedSearchCheckInterval 164
  - nsActiveChainingComponents 162
  - nsAddCount 171
  - nsBindConnectionCount 172
  - nsBindConnectionsLimit 165
  - nsBindCount 172
  - nsBindRetryLimit 165
  - nsBindTimeout 166
  - nsCheckLocalACI 166
  - nsCompareCount 172
  - nsConcurrentBindLimit 166
  - nsConcurrentOperationsLimit 167
  - nsConnectionLife 167
  - nsDeleteCount 172
  - nsFarmServerURL 170
  - nshoplmit 171
  - nsMaxResponseDelay 163
  - nsMaxTestResponseDelay 163
  - nsModifyCount 172
  - nsMultiplexorBindDN 170
  - nsMultiplexorCredentials 170
  - nsOperationConnectionCount 172
  - nsOperationConnectionsLimit 167
  - nsProxiedAuthorization 168
  - nsReferralOnScopedSearch 168
  - nsRenameCount 172
  - nsSearchBaseCount 172
  - nsSearchOneLevelCount 172
  - nsSearchSubtreeCount 172
  - nsSizeLimit 169
  - nsslapd-changelogmaxage 174
  - nsTimeLimit 169
  - nsTransmittedControls 164
  - nsUnbindCount 172
- database plug-in configuration attributes
  - cn 155
  - dbcachehitratio 145
  - dbcachehits 145
  - dbcachepagein 145
  - dbcachepageout 145
  - dbcacheroevict 146
  - dbcacherwevict 146
  - dbcachetries 145
  - dbfilecachehit 156
  - dbfilecachemiss 156
  - dbfilenamenumber 156, 165
  - dbfilepagein 156
  - dbfilepageout 156
  - description 155
  - nsIndexType 154
  - nsLookThroughLimit 134
  - nsMatchingRule 154
  - nsslapd-allidsthreshold 134
  - nsslapd-cache-autosize 135
  - nsslapd-cache-autosize-split 135
  - nsslapd-cachememsize 147

- 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-dbcachesize 136
- nsslapd-db-cache-size-bytes 150
- nsslapd-db-cache-try 150
- nsslapd-db-checkpoint-interval 136
- nsslapd-db-circular-logging 137
- nsslapd-db-clean-pages 150
- nsslapd-db-commit-rate 150
- nsslapd-db-deadlock-rate 150
- nsslapd-db-dirty-pages 151
- nsslapd-db-durable-transactions 138
- nsslapd-db-hash-buckets 151
- nsslapd-db-hash-elements-examine-rate 151
- nsslapd-db-hash-search-rate 151
- nsslapd-db-home-directory 138
- nsslapd-db-idl-divisor 140
- nsslapd-db-lock-conflicts 151
- nsslapd-db-lockers 151
- nsslapd-db-lock-region-wait-rate 151
- nsslapd-db-lock-request-rate 151
- nsslapd-db-logbuf-size 140
- nsslapd-db-log-bytes-since-checkpoint 151
- nsslapd-db-logdirectory 141
- nsslapd-db-logfile-size 141
- nsslapd-db-log-region-wait-rate 151
- nsslapd-db-log-write-rate 151
- nsslapd-db-longest-chain-length 152
- nsslapd-dbncache 144
- nsslapd-db-page-create-rate 152
- nsslapd-db-page-ro-evict-rate 152
- nsslapd-db-page-rw-evict-rate 152
- nsslapd-db-pages-in-use 152
- nsslapd-db-page-size 142
- nsslapd-db-page-trickle-rate 152
- nsslapd-db-page-write-rate 152
- nsslapd-db-transaction-batch-val 142
- nsslapd-db-transaction-logging 143
- nsslapd-db-txn-region-wait-rate 152
- nsslapd-directory 148
- nsslapd-import-cachesize 144
- nsslapd-mode 145
- nsslapd-readonly 148
- nsslapd-require-index 149
- nsslapd-suffix 149
- nsSystemIndex 153
- database schema
  - defined 66
- database-specific configuration
  - location of 24
- db2bak
  - command-line shell and batch script 229
  - quick reference 226
- db2bak.pl
  - command-line perl script 239
  - quick reference 227
- db2index.pl
  - command-line perl script 240
  - quick reference 227
- db2indexns-slapd and slapd.exe command-line utilities
  - db2index 256
- db2ldif
  - command-line shell and batch script 229
  - quick reference 226
- db2ldif.pl
  - command-line perl script 241
  - quick reference 227
- dbcachehitratio attribute 145
- dbcachehits attribute 145
- dbcachepagein attribute 145
- dbcachepageout attribute 145
- dbcacheroevict attribute 146
- dbcacherwevict attribute 146
- dbcachetries attribute 145
- dbfilecachehit attribute 156
- dbfilecachemiss attribute 156
- dbfilenamenum attribute 156, 165
- dbfilepagein attribute 156
- dbfilepageout attribute 156
- description attribute 92, 155
- distinguished names
  - root 65
- dse.ldif
  - ldif files 105
- dse.ldif file
  - configuration information tree 32
  - contents of 23, 25



- editing 31
- dtablesize attribute 100

## E

- editing
  - dse.ldif file 31
- encryption
  - root password 65, 66
  - specifying password storage scheme 77
- encryption configuration attributes
  - nsssl2 82
  - nsssl3 82
  - nsssl3ciphers 82
  - nssslclientauth 81
  - nssslsessiontimeout 81
- encryption configuration entries
  - cn=encryption 81
- encryption method, for root password 65, 66
- entriessent attribute 100
- entrydn.db3 178

## F

- files
  - containing search filters 215
  - id2entry.db2 178
  - locating configuration 28
  - slapd.conf 65

## G

- getpwenc
  - command-line shell and batch script 231
  - quick reference 226

## I

- id2entry.db2 file 178
- Indexes
  - configuration of 27

## J

- jpeg images 223

## L

- LDAP
  - modifying configuration entries 30
- LDAP Data Interchange Format (LDIF)
  - binary data 223
- ldapdelete command-line utility
  - additional options 222
  - commonly used options 221
  - ssl options 222
- ldapmodify command-line utility
  - additional options 219
  - commonly used options 218
  - ssl options 219
- ldapsearch command-line utility
  - additional options 215
  - commonly used options 212
  - ssl options 214
- ldif 50ns-delegated-admin.ldif 106
- ldif command-line utility
  - options 224
- LDIF configuration files
  - contents of 25
  - detailed contents of 104
  - location of 25
  - migration of pre-5.0 configuration files to 28
- LDIF entries
  - binary data in 223
- ldif files 178
  - 00core.ldif 105
  - 05rfc2247.ldif 105

- 05rfc2927.ldif 105
- 10rfc2307.ldif 105
- 20subscriber.ldif 105
- 25java-object.ldif 105
- 28pilot.ldif 105
- 30ns-common.ldif 105
- 50ns-admin.ldif 105
- 50ns-calendar.ldif 105
- 50ns-certificate.ldif 106
- 50ns-compass.ldif 106
- 50ns-directory.ldif 106
- 50ns-legacy.ldif 106
- 50ns-mail.ldif 106
- 50ns-mcd-browser.ldif 106
- 50ns-mcd-config.ldif 106
- 50ns-mcd-li.ldif 106
- 50ns-mcd-mail.ldif 106
- 50ns-media.ldif 106
- 50ns-mlm.ldif 106
- 50ns-msg.ldif 106
- 50ns-netshare.ldif 106
- 50ns-news.ldif 106
- 50ns-proxy.ldif 106
- 50ns-value.ldif 106
- 50ns-wcal.ldif 106
- 50ns-web.ldif 106
- 99user.ldif 107
- dse.ldif 105

- ldif2db
  - command-line shell and batch script 231
  - quick reference 226

- ldif2db.pl
  - command-line perl script 242
  - quick reference 228

- ldif2ldap
  - command-line shell and batch script 233
  - quick reference 227

- lock files 179

- log files 179
  - access 34
  - error 48

## M

- Meta Directory changelog
  - retro changelog 79
- migrateInstance5
  - quick reference 228
- monitor
  - command-line shell and batch script 233
  - quick reference 227
- multi-master replication changelog
  - changelog 79

## N

- nbackends attribute 100
- nsAbandonCount attribute 172
- nsAbandonedSearchCheckInterval attribute 164
- ns-accountstatus.pl
  - command-line perl script 245
  - quick reference 228
- ns-activate.pl
  - command-line perl script 246
  - quick reference 228
- nsActiveChainingComponents attribute 162
- nsAddCount attribute 171
- nsBindConnectionCount attribute 172
- nsBindConnectionsLimit attribute 165
- nsBindCount attribute 172
- nsBindRetryLimit attribute 165
- nsBindTimeout attribute 166
- nsCheckLocalACI attribute 166
- nsCompareCount attribute 172
- nsConcurrentBindLimit attribute 166
- nsConcurrentOperationsLimit attribute 167
- nsConnectionLife attribute 167
- nsDeleteCount attribute 172
- nsDS50ruv attribute 99
- nsDS5Flags attribute 87
- nsDS5ReplicaBindDN attribute 87, 92
- nsDS5ReplicaBindMethod attribute 92
- nsDS5ReplicaChangeCount attribute 88
- nsDS5ReplicaChangesSentSinceStartup attribute 93

nsDS5ReplicaCredentials attribute 93  
 nsDS5ReplicaHost attribute 94  
 nsDS5ReplicaID attribute 88  
 nsDS5ReplicaLastInitEnd attribute 94  
 nsDS5ReplicaLastInitStart attribute 94  
 nsDS5ReplicaLastInitStatus attribute 95  
 nsDS5ReplicaLastUpdateEnd attribute 95  
 nsDS5ReplicaLastUpdateStart attribute 96  
 nsDS5ReplicaLastUpdateStatus attribute 96  
 nsDS5ReplicaLegacyConsumer attribute 89  
 nsDS5ReplicaName attribute 89  
 nsDS5ReplicaPort attribute 96  
 nsDS5ReplicaPurgeDelay attribute 89  
 nsDS5ReplicaReferral attribute 90  
 nsDS5ReplicaRefresh attribute 97  
 nsDS5ReplicaRoot attribute 90, 97  
 nsDS5ReplicaTimeout attribute 97  
 nsDS5ReplicaTombstonePurgeInterval attribute 90  
 nsDS5ReplicaTransportInfo attribute 98  
 nsDS5ReplicaType attribute 91  
 nsDS5ReplicaUpdateInProgress attribute 98  
 nsDS5ReplicaUpdateSchedule attribute 99  
 nsFarmServerURL attribute 170  
 nshoplmit attribute 171  
 nsIdleTimeout attribute 33  
 ns-inactivate.pl  
     command-line perl script 247  
     quick reference 228  
 nsIndexType attribute 154  
 nsLookThroughLimit attribute 134  
 nsMatchingRule attribute 154  
 nsMaxResponseDelay attribute 163  
 nsMaxTestResponseDelay attribute 163  
 nsModifyCount attribute 172  
 nsMultiplexorBindDN attribute 170  
 nsMultiplexorCredentials attribute 170  
 nsOperationConnectionCount attribute 172  
 nsOperationConnectionsLimit attribute 167  
 nsProxiedAuthorization attribute 168  
 nsReferralOnScopedSearch attribute 168  
 nsRenameCount attribute 172  
 nsSearchBaseCount attribute 172  
 nsSearchOneLevelCount attribute 172  
 nsSearchSubtreeCount attribute 172  
 nsSizeLimit attribute 169  
 ns-slapd and slapd.exe command-line utilities  
     archive2db 255  
     db2archive 255  
     db2ldif 251  
     finding and executing 250  
     ldif2db 253  
 ns-slapd and slapd.exe commands  
     overview 249  
 nsslapd-accesscontrol attribute 34  
 nsslapd-accesslog attribute 34  
 nsslapd-accesslog-auditlog-list attribute 42  
 nsslapd-accesslog-level attribute 35  
 nsslapd-accesslog-list attribute 36  
 nsslapd-accesslog-logbuffering attribute 36  
 nsslapd-accesslog-logexpirationtime attribute 36  
 nsslapd-accesslog-logexpirationtimeunit  
     attribute 37, 39  
 nsslapd-accesslog-logging-enabled attribute 37  
 nsslapd-accesslog-logmaxdiskspace attribute 37  
 nsslapd-accesslog-logminfreediskspace attribute 38  
 nsslapd-accesslog-logrotationtime attribute 38  
 nsslapd-accesslog-maxlogsize attribute 39  
 nsslapd-accesslog-maxlogspendir attribute 40  
 nsslapd-allidsthreshold attribute 134  
 nsslapd-attribute-name-exceptions attribute 40  
 nsslapd-auditlog-logexpirationtime attribute 42  
 nsslapd-auditlog-logexpirationtimeunit attribute 42  
 nsslapd-auditlog-logging-enabled attribute 43  
 nsslapd-auditlog-logmaxdiskspace attribute 43  
 nsslapd-auditlog-logminfreediskspace attribute 44  
 nsslapd-auditlog-logrotationtime attribute 44  
 nsslapd-auditlog-logrotationtimeunit attribute 45  
 nsslapd-auditlog-maxlogsize attribute 45  
 nsslapd-auditlog-maxlogspendir attribute 46  
 nsslapd-backend attribute 85  
 nsslapd-cache-autosize attribute 135  
 nsslapd-cache-autosize-split attribute 135  
 nsslapd-cachememsize attribute 147  
 nsslapd-cachesize attribute 147

nsslapd-certmap-basedn attribute 46  
nsslapd-changelogdir attribute 79, 173  
nsslapd-changelogmaxage attribute 80, 174  
nsslapd-changelogmaxentries attribute 80  
nsslapd-config attribute 47  
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-dbcachesize attribute 136  
nsslapd-db-cache-size-bytes attribute 150  
nsslapd-db-cache-try attribute 150  
nsslapd-db-checkpoint-interval attribute 136  
nsslapd-db-circular-logging attribute 137  
nsslapd-db-clean-pages attribute 150  
nsslapd-db-commit-rate attribute 150  
nsslapd-db-deadlock-rate attribute 150  
nsslapd-db-dirty-pages attribute 151  
nsslapd-db-durable-transactions attribute 138  
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 138  
nsslapd-db-idl-divisor attribute 140  
nsslapd-db-lock-conflicts attribute 151  
nsslapd-db-lockers attribute 151  
nsslapd-db-lock-region-wait-rate attribute 151  
nsslapd-db-lock-request-rate attribute 151  
nsslapd-db-logbuf-size attribute 140  
nsslapd-db-log-bytes-since-checkpoint attribute 151  
nsslapd-db-logdirectory attribute 141  
nsslapd-db-logfile-size attribute 141  
nsslapd-db-log-region-wait-rate attribute 151  
nsslapd-db-log-write-rate attribute 151  
nsslapd-db-longest-chain-length attribute 152  
nsslapd-dbnocache attribute 144  
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-pages-in-use attribute 152  
nsslapd-db-page-size attribute 142  
nsslapd-db-page-trickle-rate attribute 152  
nsslapd-db-page-write-rate attribute 152  
nsslapd-db-transaction-batch-val attribute 142  
nsslapd-db-transaction-logging attribute 143  
nsslapd-db-txn-region-wait-rate attribute 152  
nsslapd-directory attribute 148  
nsslapd-ds4-compatible-schema attribute 47  
nsslapd-errorlog attribute 48  
nsslapd-errorlog-level attribute 49  
nsslapd-errorlog-list attribute 50  
nsslapd-errorlog-logexpirationtime attribute 51  
nsslapd-errorlog-logexpirationtimeunit attribute 51  
nsslapd-errorlog-logging-enabled attribute 51  
nsslapd-errorlog-logmaxdiskpace attribute 52  
nsslapd-errorlog-logminfreediskpace attribute 52  
nsslapd-errorlog-logrotationtime attribute 53  
nsslapd-errorlog-logrotationtimeunit attribute 53  
nsslapd-errorlog-maxlogsize attribute 54  
nsslapd-errorlog-maxlogsperdir attribute 54  
nsslapd-groupvalnestlevel attribute 55  
nsslapd-import-cachesize attribute 144  
nsslapd-instancedir attribute 55  
nsslapd-ioblocktimeout attribute 55  
nsslapd-lastmod attribute 56  
nsslapd-listenhost attribute 56  
nsslapd-localhost attribute 57  
nsslapd-localuser attribute 57  
nsslapd-maxbersize attribute 58  
nsslapd-maxdescriptors attribute 58  
nsslapd-maxthreadsperconn attribute 59  
nsslapd-mode attribute 145  
nsslapd-nagle attribute 60  
nsslapd-plugin attribute 60  
nsslapd-plugin-depends-on-named attribute 133  
nsslapd-plugin-depends-on-type attribute 132  
nsslapd-pluginDescription attribute 132  
nsslapd-pluginEnabled attribute 130  
nsslapd-pluginId attribute 131  
nsslapd-pluginInitFunc attribute 130  
nsslapd-pluginPath attribute 129  
nsslapd-pluginType attribute 130  
nsslapd-pluginVendor attribute 131

- nsslapd-pluginVersion attribute 131
- nsslapd-port attribute 60
- nsslapd-privatenamespaces attribute 61
- nsslapd-readonly attribute 61, 148
- nsslapd-referral attribute 61
- nsslapd-referralmode attribute 62
- nsslapd-require-index attribute 149
- nsslapd-reservedescriptors attribute 62
- nsslapd-return-exact-case attribute 64
- nsslapd-rootdn attribute 65
- nsslapd-rootpw attribute 65
- nsslapd-rootpwstoragescheme attribute 66
- nsslapd-schemacheck attribute 66
- nsslapd-securelistenhost attribute 67
- nsslapd-securePort attribute 68
- nsslapd-security attribute 68
- nsslapd-sizelimit attribute 68
- nsslapd-SSL3ciphers attribute 69
- nsslapd-state attribute 85
- nsslapd-suffix attribute 149
- nsslapd-threadnumber attribute 69
- nsslapd-timelimit attribute 69
- nsslapd-versionstring attribute 71
- nssnmpcontact attribute 102
- nssnmpdescription attribute 102
- nssnmpenabled attribute 101
- nssnmplocation attribute 102
- nssnmpmasterhost attribute 103
- nssnmpmasterport attribute 103
- nssnmporganization attribute 101
- nsssl2 attribute 82
- nsssl3 attribute 82
- nsssl3ciphers attribute 82
- nssslclientauth attribute 81
- nssslsessiontimeout attribute 81
- nsState attribute 91
- nsstate attribute 104
- nsSystemIndex attribute 153
- nsTimeLimit attribute 169
- nsTransmittedControls attribute 164
- nsUnbindCount attribute 172
- nsuniqueid.db3 178

## O

- objectclass.db3 178
- opscompleted attribute 100
- opsinitiated attribute 100

## P

- parentid.db3 178
- passwordLockoutDuration attribute 74
- passwordChange attribute 71
- passwordCheckSyntax attribute 72
- passwordExp attribute 72
- passwordHistory attribute 73
- passwordInHistory attribute 73
- passwordLockout attribute 74
- passwordMaxAge attribute 75
- passwordMaxFailure attribute 75
- passwordMinAge attribute 75
- passwordMinLength attribute 76
- passwordMustChange attribute 76
- passwordResetFailureCount attribute 77
- passwords
  - root 65
- passwordStorageScheme attribute 77
- passwordUnlock attribute 78
- passwordWarning attribute 78
- permissions
  - specifying for index files 145
- plug-in functionality configuration attributes
  - cn 155
  - dbcachehitratio 145
  - dbcachehits 145
  - dbcachepagein 145
  - dbcachepageout 145
  - dbcacheroevict 146
  - dbcacherwevict 146
  - dbcachetries 145
  - dbfilecachehit 156
  - dbfilecachemiss 156
  - dbfilenamenum 156, 165
  - dbfilepagein 156

dbfilepageout 156  
 description 155  
 nsAbandonedCount 172  
 nsAbandonedSearchCheckInterval 164  
 nsActiveChainingComponents 162  
 nsAddCount 171  
 nsBindConnectionCount 172  
 nsBindConnectionsLimit 165  
 nsBindCount 172  
 nsBindRetryLimit 165  
 nsBindTimeout 166  
 nsCheckLocalACI 166  
 nsCompareCount 172  
 nsConcurrentBindLimit 166  
 nsConcurrentOperationsLimit 167  
 nsConnectionLife 167  
 nsDeleteCount 172  
 nsFarmServerURL 170  
 nshoplmit 171  
 nsIndexType 154  
 nsLookThroughLimit 134  
 nsMatchingRule 154  
 nsMaxResponseDelay 163  
 nsMaxTestResponseDelay 163  
 nsModifyCount 172  
 nsMultiplexorBindDN 170  
 nsMultiplexorCredentials 170  
 nsOperationConnectionCount 172  
 nsOperationConnectionsLimit 167  
 nsProxiedAuthorization 168  
 nsReferralOnScopedSearch 168  
 nsRenameCount 172  
 nsSearchBaseCount 172  
 nsSearchOneLevelCount 172  
 nsSearchSubtreeCount 172  
 nsSizeLimit 169  
 nsslapd-allidsthreshold 134  
 nsslapd-cache-autosize 135  
 nsslapd-cache-autosize-split 135  
 nsslapd-cachememsize 147  
 nsslapd-cachesize 147  
 nsslapd-changelogdir 173  
 nsslapd-changelogmaxage 174  
 nsslapd-db-abort-rate 150  
 nsslapd-db-active-txns 150  
 nsslapd-db-cache-hit 150  
 nsslapd-db-cache-region-wait-rate 150  
 nsslapd-dbcachesize 136  
 nsslapd-db-cache-size-bytes 150  
 nsslapd-db-cache-try 150  
 nsslapd-db-checkpoint-interval 136  
 nsslapd-db-circular-logging 137  
 nsslapd-db-clean-pages 150  
 nsslapd-db-commit-rate 150  
 nsslapd-db-deadlock-rate 150  
 nsslapd-db-dirty-pages 151  
 nsslapd-db-durable-transactions 138  
 nsslapd-db-hash-buckets 151  
 nsslapd-db-hash-elements-examine-rate 151  
 nsslapd-db-hash-search-rate 151  
 nsslapd-db-home-directory 138  
 nsslapd-db-idl-divisor 140  
 nsslapd-db-lock-conflicts 151  
 nsslapd-db-lockers 151  
 nsslapd-db-lock-region-wait-rate 151  
 nsslapd-db-lock-request-rate 151  
 nsslapd-db-logbuf-size 140  
 nsslapd-db-log-bytes-since-checkpoint 151  
 nsslapd-db-logdirectory 141  
 nsslapd-db-logfile-size 141  
 nsslapd-db-log-region-wait-rate 151  
 nsslapd-db-log-write-rate 151  
 nsslapd-db-longest-chain-length 152  
 nsslapd-dbncache 144  
 nsslapd-db-page-create-rate 152  
 nsslapd-db-page-ro-evict-rate 152  
 nsslapd-db-page-rw-evict-rate 152  
 nsslapd-db-pages-in-use 152  
 nsslapd-db-page-size 142  
 nsslapd-db-page-trickle-rate 152  
 nsslapd-db-page-write-rate 152  
 nsslapd-db-transaction-batch-val 142  
 nsslapd-db-transaction-logging 143  
 nsslapd-db-txn-region-wait-rate 152  
 nsslapd-directory 148  
 nsslapd-import-cachesize 144  
 nsslapd-mode 145  
 nsslapd-plugin-depends-on-named 133  
 nsslapd-plugin-depends-on-type 132  
 nsslapd-pluginDescription 132  
 nsslapd-pluginEnabled 130  
 nsslapd-pluginId 131  
 nsslapd-pluginInitFunc 130  
 nsslapd-pluginPath 129

- nsslapd-pluginType 130
- nsslapd-pluginVendor 131
- nsslapd-pluginVersion 131
- nsslapd-readonly 148
- nsslapd-require-index 149
- nsslapd-suffix 149
- nsSystemIndex 153
- nsTimeLimit 169
- nsTransmittedControls 164
- nsUnbindCount 172
- plug-ins
  - configuration of 24
- port numbers
  - less than 1024 60

## R

- read-only monitoring configuration attributes
  - backendMonitorDN 101
  - bytessent 100
  - connection 99
  - currentconnections 100
  - currenttime 100
  - dtablesize 100
  - entriessent 100
  - nbackends 100
  - opscompleted 100
  - opsinitiated 100
  - readwaiters 100
  - starttime 100
  - totalconnections 100
- read-only monitoring configuration entries
  - cn=monitor 99
- readwaiters attribute 100
- replication agreement configuration attributes
  - description 92
  - nsDS50ruv 99
  - nsDS5ReplicaBindDN 92
  - nsDS5ReplicaBindMethod 92
  - nsDS5ReplicaChangesSentSinceStartup 93
  - nsDS5ReplicaCredentials 93
  - nsDS5ReplicaHost 94
  - nsDS5ReplicaLastInitEnd 94
  - nsDS5ReplicaLastInitStart 94
  - nsDS5ReplicaLastInitStatus 95
  - nsDS5ReplicaLastUpdateEnd 95
  - nsDS5ReplicaLastUpdateStart 96
  - nsDS5ReplicaLastUpdateStatus 96
  - nsDS5ReplicaPort 96
  - nsDS5ReplicaRefresh 97
  - nsDS5ReplicaRoot 97
  - nsDS5ReplicaTimeout 97
  - nsDS5ReplicaTransportInfo 98
  - nsDS5ReplicaUpdateInProgress 98
  - nsDS5ReplicaUpdateSchedule 99
  - object classes 91
- replication configuration attributes
  - cn 86
  - nsDS5Flags 87
  - nsDS5ReplicaBindDN 87
  - nsDS5ReplicaChangeCount 88
  - nsDS5ReplicaID 88
  - nsDS5ReplicaLegacyConsumer 89
  - nsDS5ReplicaName 89
  - nsDS5ReplicaPurgeDelay 89
  - nsDS5ReplicaReferral 90
  - nsDS5ReplicaRoot 90
  - nsDS5ReplicaTombstonePurgeInterval 90
  - nsDS5ReplicaType 91
  - nsState 91
  - object classes 86
- restart 234
- restarting server
  - requirement for certain configuration changes 31, 107
- restart-slapd
  - command-line shell and batch script 234
  - quick reference 227
- restoreconfig
  - command-line shell and batch script 234
  - quick reference 227
- retro changelog
  - Meta Directory changelog 79
- retro changelog plug-in configuration attributes
  - nsslapd-changelogdir 173
- root password, Root DN and 65

## S

- saveconfig
  - command-line shell and batch script 235
  - quick reference 227
- search filters
  - specifying file 215, 223
- search operations
  - limiting entries returned 68
  - setting time limits 69
- searches
  - sort criteria 217
  - specifying scope 213
- server restart
  - after configuration changes 31, 107
- slapd.conf file
  - converting to LDIF format 28
  - location of 28
  - root password and 65
- slapd.ldbm.conf file
  - converting to LDIF format 28
- smart referrals
  - ldapsearch option 216
- SNMP configuration attributes
  - nssnmpcontact 102
  - nssnmpdescription 102
  - nssnmpenabled 101
  - nssnmplocation 102
  - nssnmpmasterhost 103
  - nssnmpmasterport 103
  - nssnmporganization 101
- SNMP configuration entries
  - cn=SNMP 101
- sort criteria 217
- start-slapd
  - command-line shell and batch script 235
  - quick reference 227
- starttime attribute 100
- stop-slapd
  - command-line shell and batch script 236
  - quick reference 227
- suffix and replication configuration entries
  - cn=mapping tree 84
- suffix configuration attributes
  - nsslapd-backend 85

- nsslapd-state 85
- object classes 85
- suffix2instance
  - quick reference 227
- suffixd2instance
  - command-line shell and batch script 236

## T

- totalconnections attribute 100

## U

- Uniform Resource Locators, <Italic>See URLs
- uniqueid generator configuration attributes
  - nsstate 104
- uniqueid generator configuration entries
  - cn=uniqueid generator 104
- URL
  - LDAP 61

## V

- vlvindex
  - command-line shell and batch script 237
  - quick reference 227