



OpenDJ Administration Guide

Version 3

Mark Craig
Nemanja Lukić
Ludovic Poitou
Chris Ridd

ForgeRock AS
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Copyright © 2011-2016 ForgeRock AS.

Abstract

Hands-on guide to configuring and using OpenDJ features. The OpenDJ project offers open source LDAP directory services in Java.



This work is licensed under the [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License](http://creativecommons.org/licenses/by-nc-nd/3.0/).

To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

ForgeRock™ is the trademark of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. Trademarks are the property of their respective owners.

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong @ free . fr .

Admonition graphics by Yannick Lung. Free for commercial use. Available at [Freeecs Cumulus](http://Freeecs.Cumulus).

Table of Contents

Preface	vii
1. Using This Guide	viii
2. Formatting Conventions	ix
3. Accessing Documentation Online	ix
4. Joining the ForgeRock Community	x
1. Understanding Directory Services	1
1.1. How Directories and LDAP Evolved	2
1.2. About Data In LDAP Directories	3
1.3. About LDAP Client and Server Communication	6
1.4. About LDAP Controls and Extensions	7
1.5. About Indexes	8
1.6. About LDAP Schema	8
1.7. About Access Control	9
1.8. About Replication	9
1.9. About DSMLv2	10
1.10. About RESTful Access to Directory Services	10
1.11. About Building Directory Services	11
2. Administration Interfaces and Tools	13
2.1. Control Panel	13
2.2. Command-Line Tools	16
3. Managing Server Processes	23
3.1. Starting a Server	23
3.2. Stopping a Server	25
3.3. Restarting a Server	25
3.4. Server Recovery	26
4. Importing and Exporting LDIF Data	29
4.1. Generating Test Data	29
4.2. Importing and Exporting Data	30
4.3. Other Tools For Working With LDIF Data	33
4.4. Creating a New Database Backend	34
4.5. Setting Disk Space Thresholds For Database Backends	36
4.6. Updating an Existing Backend to Add a New Base DN	37
4.7. Deleting a Database Backend	38
5. Configuring Connection Handlers	39
5.1. LDAP Client Access	40
5.2. Preparing For Secure Communications	41
5.3. LDAP Client Access With Transport Layer Security	52
5.4. LDAP Client Access Over SSL	53
5.5. Restricting Client Access	55
5.6. TLS Protocols and Cipher Suites	57
5.7. Client Certificate Validation and the Directory	58
5.8. RESTful Client Access	60
5.9. DSML Client Access	64

5.10. JMX Client Access	66
5.11. LDIF File Access	67
5.12. SNMP Access	68
6. Configuring Privileges and Access Control	69
6.1. About Access Control Instructions	70
6.2. About Privileges	79
6.3. Configuring Privileges	81
6.4. Configuring Access Control	85
6.5. Viewing Effective Rights	93
7. Indexing Attribute Values	97
7.1. Index Types and Their Functions	98
7.2. What To Index	100
7.3. Configuring and Rebuilding Indexes	104
7.4. Verifying Indexes	113
7.5. Default Indexes	114
8. Managing Data Replication	117
8.1. Replication Quick Setup	117
8.2. About Replication	118
8.3. Configuring Replication	123
8.4. Change Notification For Your Applications	150
8.5. Recovering From User Error	159
9. Backing Up and Restoring Data	163
9.1. Backing Up Directory Data	163
9.2. Restoring Directory Data From Backup	166
10. Configuring Password Policy	169
10.1. About OpenDJ Password Policies	169
10.2. Configuring Password Policies	175
10.3. Assigning Password Policies	180
10.4. Configuring Password Generation	184
10.5. Configuring Password Storage	185
10.6. Configuring Password Validation	188
10.7. Sample Password Policies	191
11. Implementing Account Lockout and Notification	197
11.1. Configuring Account Lockout	198
11.2. Managing Accounts Manually	199
11.3. Managing Account Status Notification	200
12. Setting Resource Limits	205
12.1. Limiting Search Resources	205
12.2. Limiting Idle Time	207
12.3. Limiting Maximum Request Size	208
12.4. Resource Limits and Proxied Authorization	209
13. Implementing Attribute Value Uniqueness	211
14. Managing Schema	221
14.1. About Directory Schema	222
14.2. Updating Directory Schema	224
14.3. Relaxing Schema Checking to Import Legacy Data	230

14.4. Standard Schema Included With OpenDJ Server	231
15. Configuring Pass-Through Authentication	235
15.1. About Pass-through Authentication	235
15.2. Setting Up Pass-Through Authentication	236
15.3. Assigning Pass-Through Authentication Policies	242
16. Samba Password Synchronization	247
17. Monitoring, Logging, and Alerts	251
17.1. LDAP-Based Monitoring	251
17.2. SNMP-Based Monitoring	252
17.3. JMX-Based Monitoring	254
17.4. Server Operation and Tasks	255
17.5. Server Logs	256
17.6. Alert Notifications	281
18. Tuning Servers For Performance	287
18.1. Defining Performance Requirements and Constraints	288
18.2. Testing Performance	290
18.3. Tweaking OpenDJ Performance	291
19. Securing and Hardening OpenDJ Directory Server	297
19.1. Set Up a System Account for OpenDJ Directory Server	298
19.2. Install and Use Java Security Updates	298
19.3. Only Enable Necessary Services	299
19.4. Configure Logging Appropriately	299
19.5. Limit Use of the cn=Directory Manager Account	300
19.6. Reconsider Default Global ACIs	300
19.7. Protect Directory Server Network Connections	301
19.8. Use Appropriate Password Storage and Password Policies	302
19.9. Protect OpenDJ Directory Server Files	304
20. Changing Server Certificates	307
21. Moving Servers	317
21.1. Overview	317
21.2. Before You Move	318
21.3. Moving a Server	319
22. Troubleshooting Server Problems	323
22.1. Identifying the Problem	323
22.2. Troubleshooting Installation and Upgrade	324
22.3. Resetting Administrator Passwords	324
22.4. Enabling Debug Logging	326
22.5. Preventing Access While You Fix Issues	328
22.6. Troubleshooting LDIF Import	330
22.7. Troubleshooting TLS/SSL Connections	330
22.8. Troubleshooting Client Operations	336
22.9. Troubleshooting Replication	340
22.10. Asking For Help	340
Index	343

Preface

This guide shows you how to configure, maintain, and troubleshoot OpenDJ directory services. OpenDJ directory services allow applications to access directory data:

- Over Lightweight Directory Access Protocol (LDAP)
- Using Directory Services Markup Language (DSML)
- Over Hypertext Transfer Protocol (HTTP) by using HTTP methods in the Representational State Transfer (REST) style

In reading and following the instructions in this guide, you will learn how to:

- Use OpenDJ administration tools
- Manage OpenDJ server processes
- Import, export, backup, and restore directory data
- Configure OpenDJ server connection handlers for all supported protocols
- Configure administrative privileges and fine-grained access control
- Index directory data, manage schemas for directory data, and enforce uniqueness of directory data attribute values
- Configure data replication between OpenDJ directory servers
- Implement password policies, pass-through authentication to another directory, password synchronization with Samba, account lockout, and account status notification

- Set resource limits to prevent unfair use of directory server resources
- Monitor directory servers through logs and alerts and over JMX
- Tune directory servers for best performance
- Secure directory server deployments
- Change directory server key pairs and public key certificates
- Move a directory server to a different system
- Troubleshoot directory server issues

1 Using This Guide

This guide is intended for system administrators who build, deploy, and maintain OpenDJ directory services for their organizations.

This guide starts with an introduction to directory services. The rest of this guide is written with the assumption that you have basic familiarity with the following topics:

- The client-server model of distributed computing
- Lightweight Directory Access Protocol (LDAP), including how clients and servers exchange messages
- Managing Java-based services on operating systems and application servers
- Using command-line tools and reading command-line examples written for UNIX/Linux systems
- Configuring network connections on operating systems
- Managing Public Key Infrastructure (PKI) used to establish secure connections

Depending on the features you use, you should also have basic familiarity with the following topics:

- Directory Services Markup Language (DSML), including how clients and servers exchange messages
- Hypertext Transfer Protocol (HTTP), including how clients and servers exchange messages
- Java Management Extensions (JMX) for monitoring services

- Simple Network Management Protocol (SNMP) for monitoring services

2 Formatting Conventions

Most examples in the documentation are created in GNU/Linux or Mac OS X operating environments. If distinctions are necessary between operating environments, examples are labeled with the operating environment name in parentheses. To avoid repetition file system directory names are often given only in UNIX format as in `/path/to/server`, even if the text applies to `C:\path\to\server` as well.

Absolute path names usually begin with the placeholder `/path/to/`. This path might translate to `/opt/`, `C:\Program Files\`, or somewhere else on your system.

Command line, terminal sessions are formatted as follows:

```
$ echo $JAVA_HOME
/path/to/jdk
```

Command output is sometimes formatted for narrower, more readable output even though formatting parameters are not shown in the command. In the following example, the query string parameter `_prettyPrint=true` is omitted and some of the output is replaced with an ellipsis (...):

```
$ curl https://bjensen:hifalutin@opendj.example.com:8443/users/newuser
{
  "_rev" : "000000005b337348",
  "_id" : "newuser",
  ...
}
```

Program listings are formatted as follows:

```
class Test {
    public static void main(String [] args) {
        System.out.println("This is a program listing.");
    }
}
```

3 Accessing Documentation Online

ForgeRock core documentation, such as this document, aims to be technically accurate and complete with respect to the software documented.

Core documentation therefore follows a three-phase review process designed to eliminate errors:

- Product managers and software architects review project documentation design with respect to the readers' software lifecycle needs.
- Subject matter experts review proposed documentation changes for technical accuracy and completeness with respect to the corresponding software.
- Quality experts validate implemented documentation changes for technical accuracy, completeness in scope, and usability for the readership.

The review process helps to ensure that documentation published for a ForgeRock release is technically accurate and complete.

Fully reviewed, published core documentation is available at <http://backstage.forgerock.com/>. Use this documentation when working with a ForgeRock Enterprise release.

You can find pre-release draft documentation at the online [community resource center](#). Use this documentation when trying a nightly build.

4 Joining the ForgeRock Community

Visit the [community resource center](#) where you can find information about each project, download nightly builds, browse the resource catalog, ask and answer questions on the forums, find community events near you, and of course get the source code as well.

Chapter 1

Understanding Directory Services

This chapter introduces directory concepts and directory server features. In this chapter you will learn:

- Why directory services exist and what they do well
- How data is arranged in directories that support Lightweight Directory Access Protocol (LDAP)
- How clients and servers communicate in LDAP
- What operations are standard according to LDAP and how standard extensions to the protocol work
- Why directory servers index directory data
- What LDAP schemas are for
- What LDAP directories provide to control access to directory data
- Why LDAP directory data is replicated and what replication does
- What Directory Services Markup Language (DSML) is for
- How HTTP applications can access directory data in the Representation State Transfer (REST) style

A directory resembles a dictionary or a phone book. If you know a word, you can look it up its entry in the dictionary to learn its definition or its pronunciation. If you know a name, you can look it up its entry in the phone book to find the

telephone number and street address associated with the name. If you are bored, curious, or have lots of time, you can also read through the dictionary, phone book, or directory, entry after entry.

Where a directory differs from a paper dictionary or phone book is in how entries are indexed. Dictionaries typically have one index—words in alphabetical order. Phone books, too—names in alphabetical order. Directories' entries on the other hand are often indexed for multiple attributes, names, user identifiers, email addresses, and telephone numbers. This means you can look up a directory entry by the name of the user the entry belongs to, but also by their user identifier, their email address, or their telephone number, for example.

OpenDJ directory services are based on the Lightweight Directory Access Protocol (LDAP). Much of this chapter serves therefore as an introduction to LDAP. OpenDJ directory services also provide RESTful access to directory data, yet, as directory administrator, you will find it useful to understand the underlying model even if most users are accessing the directory over HTTP rather than LDAP.

1.1 How Directories and LDAP Evolved

Phone companies have been managing directories for many decades. The Internet itself has relied on distributed directory services like DNS since the mid 1980s.

It was not until the late 1980s, however, that experts from what is now the International Telecommunications Union published the X.500 set of international standards, including Directory Access Protocol. The X.500 standards specify Open Systems Interconnect (OSI) protocols and data definitions for general purpose directory services. The X.500 standards were designed to meet the needs of systems built according to the X.400 standards, covering electronic mail services.

Lightweight Directory Access Protocol has been around since the early 1990s. LDAP was originally developed as an alternative protocol that would allow directory access over Internet protocols rather than OSI protocols, and be lightweight enough for desktop implementations. By the mid-1990s, LDAP directory servers became generally available and widely used.

Until the late 1990s, LDAP directory servers were designed primarily with quick lookups and high availability for lookups in mind. LDAP directory servers replicate data, so when an update is made, that update is applied to other peer directory servers. Thus, if one directory server goes down, lookups can continue on other servers. Furthermore, if a directory service needs to support more lookups, the administrator can simply add another directory server to replicate with its peers.

As organizations rolled out larger and larger directories serving more and more applications, they discovered that they needed high availability not only for lookups, but also for updates. Around the year 2000, directories began to support multi-master replication; that is, replication with multiple read-write servers. Soon thereafter, the organizations with the very largest directories started to need higher update performance as well as availability.

The OpenDJ code base began in the mid-2000s, when engineers solving the update performance issue decided the cost of adapting the existing C-based directory technology for high-performance updates would be higher than the cost of building a next generation, high performance directory using Java technology.

1.2 About Data In LDAP Directories

LDAP directory data is organized into entries, similar to the entries for words in the dictionary, or for subscriber names in the phone book. A sample entry follows:

```
dn: uid=bjensen,ou=People,dc=example,dc=com
uid: bjensen
cn: Babs Jensen
cn: Barbara Jensen
facsimileTelephoneNumber: +1 408 555 1992
gidNumber: 1000
givenName: Barbara
homeDirectory: /home/bjensen
l: San Francisco
mail: bjensen@example.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
ou: People
ou: Product Development
roomNumber: 0209
sn: Jensen
telephoneNumber: +1 408 555 1862
uidNumber: 1076
```

Barbara Jensen's entry has a number of attributes, such as `uid: bjensen`, `telephoneNumber: +1 408 555 1862`, and `objectClass: posixAccount`¹. When you look up her entry in the directory, you specify one or more attributes and values to match. The directory server then returns entries with attribute values that match what you specified.

¹The `objectClass` attribute type indicates which types of attributes are allowed and optional for the entry. As the entries object classes can be updated online, and even the definitions of object classes and attributes are expressed as entries that can be updated online, directory data is extensible on the fly.

The attributes you search for are indexed in the directory, so the directory server can retrieve them more quickly.²

The entry also has a unique identifier, shown at the top of the entry, dn: uid=bjensen,ou=People,dc=example,dc=com. DN is an acronym for distinguished name. No two entries in the directory have the same distinguished name. Yet, DNs are typically composed of case-insensitive attributes.

Sometimes distinguished names include characters that you must escape. The following example shows an entry that includes escaped characters in the DN:

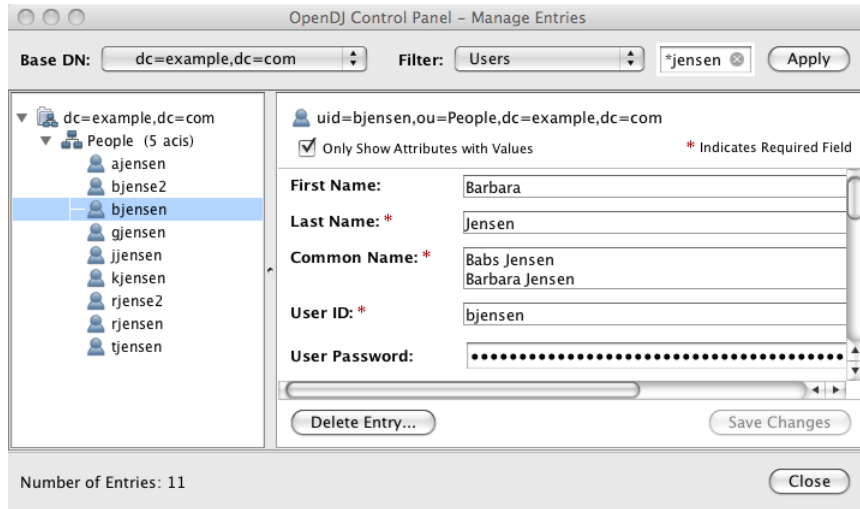
```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(uid=escape)"
dn: cn=\" # \+ \, \; \< = \> \\ DN Escape Characters,dc=example,dc=com
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
givenName: \" # + , ; < = > \
uid: escape
cn: \" # + , ; < = > \ DN Escape Characters
sn: DN Escape Characters
mail: escape@example.com
```

LDAP entries are arranged hierarchically in the directory. The hierarchical organization resembles a file system on a PC or a web server, often imagined as an upside-down tree structure, looking similar to a pyramid.³ The distinguished name consists of components separated by commas, uid=bjensen,ou=People,dc=example,dc=com. The names are little-endian. The components reflect the hierarchy of directory entries.

²Attribute values do not have to be strings. Some attribute values are pure binary like certificates and photos.

³Hence pyramid icons are associated with directory servers.

Figure 1.1. Directory Data



Barbara Jensen's entry is located under an entry with DN `ou=People,dc=example,dc=com`, an organization unit and parent entry for the people at Example.com. The `ou=People` entry is located under the entry with DN `dc=example,dc=com`, the base entry for Example.com. DC is an acronym for domain component. The directory has other base entries, such as `cn=config`, under which the configuration is accessible through LDAP. A directory can serve multiple organizations, too. You might find `dc=example,dc=com`, `dc=mycompany,dc=com`, and `o=myOrganization` in the same LDAP directory. Therefore, when you look up entries, you specify the base DN to look under in the same way you need to know whether to look in the New York, Paris, or Tokyo phone book to find a telephone number.⁴

A directory server stores two kinds of attributes in a directory entry: *user attributes* and *operational attributes*. User attributes hold the information for users of the directory. All of the attributes shown in the entry at the outset of this section are user attributes. Operational attributes hold information used by the directory itself. Examples of operational attributes include `entryUUID`, `modifyTimestamp`, and `subschemaSubentry`. When an LDAP search operation finds an entry in the directory, the directory server returns all the visible user attributes unless the search request restricts the list of attributes by specifying those attributes explicitly. The directory server does not, however, return any operational attributes unless the search request specifically asks for them. Generally speaking, applications should change only user attributes, and leave updates of operational attributes to the server, relying on public directory server

⁴The root entry for the directory, technically the entry with DN `"` (the empty string), is called the root DSE, and contains information about what the server supports, including the other base DNs it serves.

interfaces to change server behavior. An exception is access control instruction (aci) attributes, which are operational attributes used to control access to directory data.

1.3 About LDAP Client and Server Communication

In some client server communication, like web browsing, a connection is set up and then torn down for each client request to the server. LDAP has a different model. In LDAP the client application connects to the server and authenticates, then requests any number of operations, perhaps processing results in between requests, and finally disconnects when done.

The standard operations are as follows:

- Bind (authenticate). The first operation in an LDAP session usually involves the client binding to the LDAP server, with the server authenticating the client.⁵ Authentication identifies the client's identity in LDAP terms, the identity which is later used by the server to authorize (or not) access to directory data that the client wants to lookup or change.
- Search (lookup). After binding, the client can request that the server return entries based on an LDAP filter, which is an expression that the server uses to find entries that match the request, and a base DN under which to search. For example, to look up all entries for people with the email address bjensen@example.com in data for Example.com, you would specify a base DN such as ou=People,dc=example,dc=com and the filter (mail=bjensen@example.com).
- Compare. After binding, the client can request that the server compare an attribute value the client specifies with the value stored on an entry in the directory.
- Modify. After binding, the client can request that the server change one or more attribute values on an entry. Often administrators do not allow clients to change directory data, so allow appropriate access for client application if they have the right to update data.
- Add. After binding, the client can request to add one or more new LDAP entries to the server.
- Delete. After binding, the client can request that the server delete one or more entries. To delete an entry with other entries underneath, first delete the children, then the parent.

⁵ If the client does not bind explicitly, the server treats the client as an anonymous client. An anonymous client is allowed to do anything that can be done anonymously. What can be done anonymously depends on access control and configuration settings. The client can also bind again on the same connection.

- **Modify DN.** After binding, the client can request that the server change the distinguished name of the entry. In other words, this renames the entry or moves it to another location. For example, if Barbara changes her unique identifier from bjensen to something else, her DN would have to change. For another example, if you decide to consolidate ou=Customers and ou=Employees under ou=People instead, all the entries underneath must change distinguished names.⁶
- **Unbind.** When done making requests, the client can request an unbind operation to end the LDAP session.
- **Abandon.** When a request seems to be taking too long to complete, or when a search request returns many more matches than desired, the client can send an abandon request to the server to drop the operation in progress.

For practical examples showing how to perform the key operations using the command-line tools delivered with OpenDJ directory server, read Chapter 2, in the *OpenDJ Directory Server Developer's Guide*.

1.4 About LDAP Controls and Extensions

LDAP has standardized two mechanisms for extending the operations directory servers can perform beyond the basic operations listed above. One mechanism involves using LDAP controls. The other mechanism involves using LDAP extended operations.

LDAP controls are information added to an LDAP message to further specify how an LDAP operation should be processed. For example, the Server-Side Sort request control modifies a search to request that the directory server return entries to the client in sorted order. The Subtree Delete request control modifies a delete to request that the server also remove child entries of the entry targeted for deletion.

One special search operation that OpenDJ supports is Persistent Search. The client application sets up a Persistent Search to continue receiving new results whenever changes are made to data that is in the scope of the search, thus using the search as a form of change notification. Persistent Searches are intended to remain connected permanently, though they can be idle for long periods of time.

The directory server can also send response controls in some cases to indicate that the response contains special information. Examples include responses for entry change notification, password policy, and paged results.

For the list of supported LDAP controls, see Appendix F, in the *OpenDJ Reference*.

⁶Renaming entire branches of entries can be a major operation for the directory, so avoid moving entire branches if you can.

LDAP extended operations are additional LDAP operations not included in the original standard list. For example, the Cancel Extended Operation works like an abandon operation, but finishes with a response from the server after the cancel is complete. The StartTLS Extended Operation allows a client to connect to a server on an unsecure port, but then starts Transport Layer Security negotiations to protect communications.

For the list of supported LDAP extended operations, see Appendix G, in the *OpenDJ Reference*.

1.5 About Indexes

As mentioned early in this chapter, directories have indexes for multiple attributes. In fact, by default OpenDJ does not let normal users perform searches that are not indexed, because such searches mean OpenDJ has to scan the entire directory looking for matches.

As directory administrator, part of your responsibility is making sure directory data is properly indexed. OpenDJ provides tools for building and rebuilding indexes, for verifying indexes, and also for evaluating how well they are working.

For help better understanding and managing indexes, read [Chapter 7, "Indexing Attribute Values"](#).

1.6 About LDAP Schema

Some databases are designed to hold huge amounts of data for a particular application. Although such databases might support multiple applications, how their data is organized depends a lot on the particular applications served.

In contrast, directories are designed for shared, centralized services. Although the first guides to deploying directory services suggested taking inventory of all the applications that would access the directory, many current directory administrators do not even know how many applications use their services. The shared, centralized nature of directory services fosters interoperability in practice, and has helped directory services be successful in the long term.

Part of what makes this possible is the shared model of directory user information, and in particular the LDAP schema. LDAP schema defines what the directory can contain. This means that directory entries are not arbitrary data, but instead tightly codified objects whose attributes are completely predictable from publicly readable definitions. Many schema definitions are in fact standard. They are the same not just across a directory service but across different directory services.

At the same time, unlike some databases, LDAP schema and the data it defines can be extended on the fly while the service is running. LDAP schema is also accessible over LDAP. One attribute of every entry is its set of objectClass values. This gives you as administrator great flexibility in adapting your directory service to store new data without losing or changing the structure of existing data, and also without ever stopping your directory service.

For a closer look, see [Chapter 14, "Managing Schema"](#).

1.7 About Access Control

In addition to directory schema, another feature of directory services that enables sharing is fine-grained access control.

As directory administrator, you can control who has access to what data when, how, where and under what conditions by using access control instructions (ACI). You can allow some directory operations and not others. You can scope access control from the whole directory service down to individual attributes on directory entries. You can specify when, from what host or IP address, and what strength of encryption is needed in order to perform a particular operation.

As ACIs are stored on entries in the directory, you can furthermore update access controls while the service is running, and even delegate that control to client applications. OpenDJ combines the strengths of ACIs with separate administrative privileges to help you secure access to directory data.

For more information, read [Chapter 6, "Configuring Privileges and Access Control"](#).

1.8 About Replication

Replication in OpenDJ consists of copying each update to the directory service to multiple directory servers. This brings both redundancy, in the case of network partitions or of crashes, and also scalability for read operations. Most directory deployments involve multiple servers replicating together.

When you have replicated servers, all of which are writable, you can have replication conflicts. What if, for example, there is a network outage between two replicas, and meanwhile two different values are written to the same attribute on the same entry on the two replicas? In nearly all cases, OpenDJ replication can resolve these situations automatically without involving you, the directory administrator. This makes your directory service resilient and safe even in the unpredictable real world.

One perhaps counterintuitive aspect of replication is that although you do add directory *read* capacity by adding replicas to your deployment, you do not add directory *write* capacity by adding replicas. As each write operation must be replayed everywhere, the result is that if you have N servers, you have N write operations to replay.

Another aspect of replication to keep in mind is that it is "loosely consistent." Loosely consistent means that directory data will eventually converge to be the same everywhere, but it will not necessarily be the same everywhere right away. Client applications sometimes get this wrong when they write to a pool of load-balanced directory servers, immediately read back what they wrote, and are surprised that it is not the same. If your users are complaining about this, either make sure their application always gets sent to the same server, or else ask that they adapt their application to work in a more realistic manner.

To get started with replication, see [Chapter 8, "Managing Data Replication"](#).

1.9 About DSMLv2

Directory Services Markup Language (DSMLv2) v2.0 became a standard in 2001. DSMLv2 describes directory data and basic directory operations in XML format, so they can be carried in Simple Object Access Protocol (SOAP) messages. DSMLv2 further allows clients to batch multiple operations together in a single request, to be processed either in sequential order or in parallel.

OpenDJ provides support for DSMLv2 as a DSML gateway, which is a Servlet that connects to any standard LDAPv3 directory. DSMLv2 opens basic directory services to SOAP-based web services and service oriented architectures.

To set up DSMLv2 access, see [Section 5.9, "DSML Client Access"](#).

1.10 About RESTful Access to Directory Services

OpenDJ can expose directory data as JSON resources over HTTP to REST clients, providing easy access to directory data for developers who are not familiar with LDAP. RESTful access depends on a configuration that describes how the JSON representation maps to LDAP entries.

Although client applications have no need to understand LDAP, OpenDJ's underlying implementation still uses the LDAP model for its operations. The mapping adds some overhead. Furthermore, depending on the configuration, individual JSON resources can require multiple LDAP operations. For example, an LDAP user entry represents manager as a DN (of the manager's entry). The same manager might be represented in JSON as an object holding the manager's

user ID and full name, in which case OpenDJ must look up the manager's entry to resolve the mapping for the manager portion of the JSON resource, in addition to looking up the user's entry. As another example, suppose a large group is represented in LDAP as a set of 100,000 DNs. If the JSON resource is configured so that a member is represented by its name, then listing that resource would involve 100,000 LDAP searches to translate DNs to names.

A primary distinction between LDAP entries and JSON resources is that LDAP entries hold sets of attributes and their values, whereas JSON resources are documents containing arbitrarily nested objects. As LDAP data is governed by schema, almost no LDAP objects are arbitrary collections of data.⁷ Furthermore, JSON resources can hold arrays, ordered collections that can contain duplicates, whereas LDAP attributes are sets, unordered collections without duplicates. For most directory and identity data, these distinctions do not matter. You are likely to run into them, however, if you try to turn your directory into a document store for arbitrary JSON resources.

Despite some extra cost in terms of system resources, exposing directory data over HTTP can unlock your directory services for a new generation of applications. The configuration provides flexible mapping, so that you can configure views that correspond to how client applications need to see directory data. OpenDJ also gives you a deployment choice for HTTP access. You can deploy the REST to LDAP gateway, which is a Servlet that connects to any standard LDAPv3 directory, or you can activate the HTTP connection handler on OpenDJ itself to allow direct and more efficient HTTP and HTTPS access.

For examples showing how to use RESTful access, see Chapter 1, in the *OpenDJ Directory Server Developer's Guide*.

1.11 About Building Directory Services

This chapter is meant to serve as an introduction, and so does not even cover everything in this guide, let alone everything you might want to know about directory services.

When you have understood enough of the concepts to build the directory services that you want to deploy, you must still build a prototype and test it before you roll out shared, centralized services for your organization. Read [Chapter 18, "Tuning Servers For Performance"](#) for a look at how to meet the service levels that directory clients expect.

⁷LDAP has the object class `extensibleObject`, but its use should be the exception rather than the rule.

Chapter 2

Administration Interfaces and Tools

This chapter covers OpenDJ administration tools. In this chapter you will learn to:

- Find and run OpenDJ control panel
- Find and run OpenDJ command-line tools

OpenDJ server software installs with a cross-platform, Java Swing-based control panel for many day-to-day tasks. OpenDJ server software also installs command-line tools for configuration and management tasks.

This chapter is one of the few to include screen shots of the control panel. Most examples make use of the command-line tools. Once you understand the concepts and how to use the command-line tools, you only need to know where to start in the control panel to accomplish what you set out to do.

At a protocol level, administration tools and interfaces connect to servers through a different network port than that used to listen for traffic from other client applications.

This chapter takes a quick look at the tools for managing directory services.

2.1 Control Panel

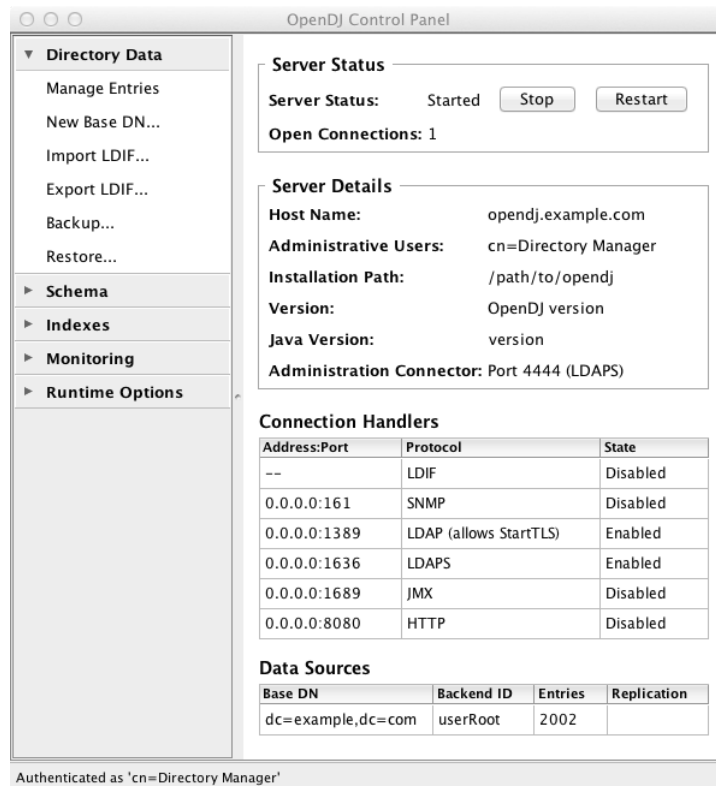
OpenDJ control panel offers a GUI for managing both local and remote servers. You choose the server to manage when you start the control panel. The control panel connects to the administration server port, making a secure LDAPS connection.

The version of OpenDJ control panel must be the same as the target version of OpenDJ directory server.

Start OpenDJ control panel by running the **control-panel** command, described in control-panel(1) in the *OpenDJ Reference*:

- (Linux, Solaris) Run **/path/to/openssl/bin/control-panel**.
- (Windows) Double-click C:\path\to\openssl\bat\control-panel.bat.
- (Mac OS X) Double-click /path/to/openssl/bin/ControlPanel.app.

When you log in to OpenDJ control panel, you authenticate over LDAP. This means that if users can run the control panel, they can use it to manage a running server. Yet, to start and stop the server process through OpenDJ control panel, you must start the control panel on the system where OpenDJ runs, as the user who owns the OpenDJ server files (such as the user who installed OpenDJ). In other words, the OpenDJ control panel does not do remote process management.

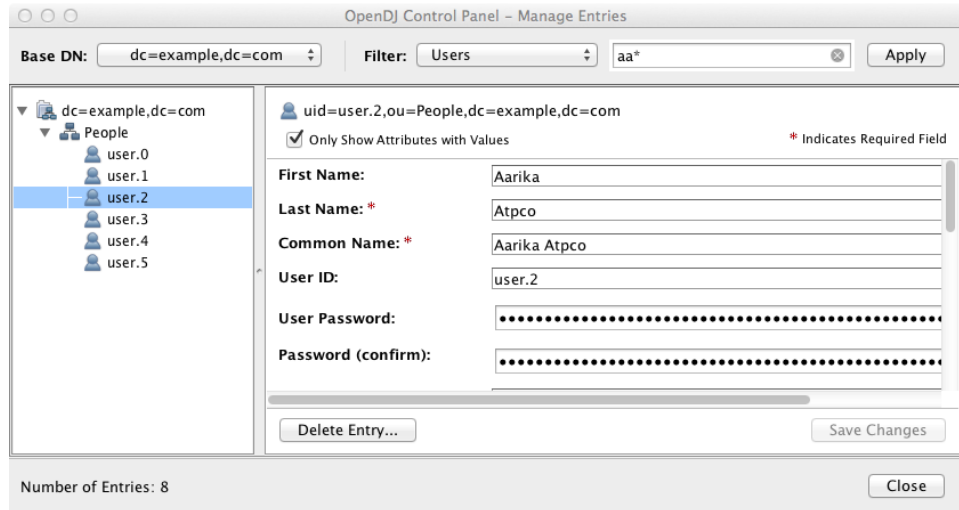


OpenDJ control panel displays key information about the server.

Down the left side of OpenDJ control panel, notice what you can configure:

Directory Data

Directory data provisioning is typically not something you do by hand in most deployments. Usually entries are created, modified, and deleted through specific directory client applications. The Manage Entries window can be useful in the lab as you design and test directory data and if you modify individual ACIs or debug issues with particular entries.



The Manage Entries window can check that your changes are valid before sending the request to the directory.

Additionally, the Directory Data list makes it easy to create a new base DN, and then import user data for the new base DN from LDAP Data Interchange Format (LDIF) files. You can also use the tools in the list to export user data to LDIF, and to backup and restore user data.

Schema

The Manage Schema window lets you browse and modify the rules that define how data is stored in the directory. You can add new schema definitions such as new attribute types and new object classes while the server is running, and the changes you make take effect immediately.

Indexes

The Manage Indexes window gives you a quick overview of all the indexes currently maintained for directory attributes. To protect your directory resources from being absorbed by costly searches on unindexed attributes, you may choose to keep the default behavior, preventing unindexed searches, instead adding indexes required by specific applications. (Notice that if the

number of user data entries is smaller than the default resource limits, you can still perform what appear to be unindexed searches. That is because the `dn2id` index returns all user data entries without hitting a resource limit that would make the search unindexed.)

OpenDJ control panel also allows you to verify and rebuild existing indexes, which you may have to do after an upgrade operation, or if you have reason to suspect index corruption.

Monitoring

The Monitoring list gives you windows to observe information about the system, the Java Virtual Machine (JVM) used, and indications about how the cache is used, whether the work queue has been filling up, as well as details about the database. You can also view the numbers and types of requests arriving over the connection handlers, and the current tasks in progress as well.

Runtime Options

If you did not set appropriate JVM runtime options during the installation process, this is the list that allows you to do so through the control panel.

2.2 Command-Line Tools

Before you try the examples in this guide, set your `PATH` to include the OpenDJ directory server tools. The location of the tools depends on the operating environment and on the packages used to install OpenDJ. [Table 2.1, "Paths To Administration Tools"](#) indicates where to find the tools.

Table 2.1. Paths To Administration Tools

OpenDJ running on...	OpenDJ installed from...	Default path to tools...
Apple Mac OS X, Linux distributions, Oracle Solaris	.zip	/path/to/opendj/bin
Linux distributions	.deb, .rpm	/opt/opendj/bin
Microsoft Windows	.zip	C:\path\to\opendj\bat
Oracle Solaris	SVR4	/usr/opendj/bin

You find the installation and upgrade tools, **setup**, **upgrade**, and **uninstall**, in the parent directory of the other tools, as these tools are not used for everyday

administration. For example, if the path to most tools is `/path/to/openssl/bin` you can find these tools in `/path/to/openssl`. For instructions on how to use the installation and upgrade tools, see the OpenDJ Installation Guide.

All OpenDJ command-line tools take the `--help` option.

All commands call Java programs and therefore involve starting a JVM.

Table 2.2, "Tools and Server Constraints" indicates the constraints, if any, that apply when using a command-line tool with a directory server.

Table 2.2. Tools and Server Constraints

Commands	Constraints
backendstat create-rc-script dsjavaproperties encode-password list-backends setup start-ds upgrade windows-service	<p>These commands must be used with the local OpenDJ directory server in the same installation as the tools.</p> <p>These commands are not useful with non-OpenDJ directory servers.</p>
control-panel dsconfig export-ldif import-ldif manage-account manage-tasks rebuild-index restore status stop-ds uninstall verify-index	<p>These commands must be used with OpenDJ directory server having the same version as the command.</p> <p>These commands are not useful with non-OpenDJ directory servers.</p>
dsreplication	<p>With one exception, this command can be used with current and previous OpenDJ directory server versions. The one exception is the dsreplication reset-change-number subcommand, which requires OpenDJ directory server version 3.0.0 or later.</p>

Commands	Constraints
	This commands is not useful with other types of directory servers.
make-ldif	<p>This command depends on template files. The template files can make use of configuration files installed with OpenDJ directory server under config/MakeLDIF/.</p> <p>The LDIF output can be used with OpenDJ and other directory servers.</p>
base64 ldapcompare ldapdelete ldapmodify ldappasswordmodify ldapsearch ldif-diff ldifmodify ldifsearch	These commands can be used independently of OpenDJ directory server, and so are not tied to a specific version.

The following list uses the UNIX names for the commands. On Windows all command-line tools have the extension .bat:

backendstat

Debug databases for pluggable backends.

For details see backendstat(1) in the *OpenDJ Reference*.

backup

Back up or schedule backup of directory data.

For details see backup(1) in the *OpenDJ Reference*.

base64

Encode and decode data in base64 format.

Base64-encoding represents binary data in ASCII, and can be used to encode character strings in LDIF, for example.

For details see base64(1) in the *OpenDJ Reference*.

create-rc-script (UNIX)

Generate a script you can use to start, stop, and restart the server either directly or at system boot and shutdown. Use **create-rc-script -f script-file**.

For details see `create-rc-script(1)` in the *OpenDJ Reference*.

dsconfig

The **dsconfig** command is the primary command-line tool for viewing and editing an OpenDJ configuration. When started without arguments, **dsconfig** prompts you for administration connection information. Once connected it presents you with a menu-driven interface to the server configuration.

When you pass connection information, subcommands, and additional options to **dsconfig**, the command runs in script mode and so is not interactive.

You can prepare **dsconfig** batch scripts by running the command with the `--commandFilePath` option in interactive mode, then reading from the batch file with the `--batchFilePath` option in script mode. Batch files can be useful when you have many **dsconfig** commands to run and want to avoid starting the JVM for each command.

Alternatively, you can read commands from standard input by using the `--batch` option.

For details see `dsconfig(1)` in the *OpenDJ Reference*.

dsjavaproperties

Apply changes you make to `opendj/config/java.properties`, which sets Java runtime options.

For details see `dsjavaproperties(1)` in the *OpenDJ Reference*.

dsreplication

Configure data replication between directory servers to keep their contents in sync.

For details see `dsreplication(1)` in the *OpenDJ Reference*.

encode-password

Encode a cleartext password according to one of the available storage schemes.

For details see `encode-password(1)` in the *OpenDJ Reference*.

export-ldif

Export directory data to LDIF, the standard, portable, text-based representation of directory content.

For details see `export-ldif(1)` in the *OpenDJ Reference*.

import-ldif

Load LDIF content into the directory, overwriting existing data.

For details see `import-ldif(1)` in the *OpenDJ Reference*.

ldapcompare

Compare the attribute values you specify with those stored on entries in the directory.

For details see `ldapcompare(1)` in the *OpenDJ Reference*.

ldapdelete

Delete one entry or an entire branch of subordinate entries in the directory.

For details see `ldapdelete(1)` in the *OpenDJ Reference*.

ldapmodify

Modify the specified attribute values for the specified entries.

Use the **ldapmodify** command with the `-a` option to add new entries.

For details see `ldapmodify(1)` in the *OpenDJ Reference*.

ldappasswordmodify

Modify user passwords.

For details see `ldappasswordmodify(1)` in the *OpenDJ Reference*.

ldapsearch

Search a branch of directory data for entries that match the LDAP filter you specify.

For details see `ldapsearch(1)` in the *OpenDJ Reference*.

ldif-diff

Display differences between two LDIF files, with the resulting output having LDIF format.

For details see `ldif-diff(1)` in the *OpenDJ Reference*.

ldifmodify

Similar to the **ldapmodify** command, modify specified attribute values for specified entries in an LDIF file.

For details see `ldifmodify(1)` in the *OpenDJ Reference*.

ldifsearch

Similar to the **ldapsearch** command, search a branch of data in LDIF for entries matching the LDAP filter you specify.

For details see `ldifsearch(1)` in the *OpenDJ Reference*.

list-backends

List backends and base DNs served by OpenDJ directory server.

For details see `list-backends(1)` in the *OpenDJ Reference*.

make-ldif

Generate directory data in LDIF based on templates that define how the data should appear.

The **make-ldif** command is designed to help generate test data that mimics data expected in production, but without compromising real, potentially private information.

For details see `make-ldif(1)` in the *OpenDJ Reference*.

manage-account

Lock and unlock user accounts, and view and manipulate password policy state information.

For details see `manage-account(1)` in the *OpenDJ Reference*.

manage-tasks

View information about tasks scheduled to run in the server, and cancel specified tasks.

For details see `manage-tasks(1)` in the *OpenDJ Reference*.

rebuild-index

Rebuild an index stored in an indexed backend.

For details see `rebuild-index(1)` in the *OpenDJ Reference*.

restore

Restore data from backup.

For details see `restore(1)` in the *OpenDJ Reference*.

start-ds

Start OpenDJ directory server.

For details see `start-ds(1)` in the *OpenDJ Reference*.

status

Display information about the server.

For details see `status(1)` in the *OpenDJ Reference*.

stop-ds

Stop OpenDJ directory server.

For details see `stop-ds(1)` in the *OpenDJ Reference*.

verify-index

Verify that an index stored in an indexed backend is not corrupt.

For details see `verify-index(1)` in the *OpenDJ Reference*.

windows-service (Windows)

Register OpenDJ as a Windows Service.

For details see `windows-service(1)` in the *OpenDJ Reference*.

Chapter 3

Managing Server Processes

This chapter covers starting and stopping OpenDJ directory server. In this chapter you will learn to:

- Start, restart, and stop OpenDJ directory server using OpenDJ command-line tools, OpenDJ control panel, or system service integration on Linux and Windows systems
- Understand how to recognize that OpenDJ directory server is recovering from a crash or abrupt shutdown
- Configure whether OpenDJ directory server loads data into cache at server startup before accepting client connections

3.1 Starting a Server

Use one of the following techniques:

- Use the **start-ds** command, described in start-ds(1) in the *OpenDJ Reference*:

```
$ start-ds
```

Alternatively, you can specify the `--no-detach` option to start the server in the foreground.

- (Linux) If OpenDJ directory server was installed from a .deb or .rpm package, then service management scripts were created at setup time.

Use the **service opendj start** command:

```
centos# service opendj start
Starting opendj (via systemctl): [ OK ]
```

```
ubuntu$ sudo service opendj start
$Starting opendj: > SUCCESS.
```

- (UNIX) Create an RC script by using the **create-rc-script** command, described in create-rc-script(1) in the *OpenDJ Reference*, and then use the script to start the server.

Unless you run OpenDJ on Linux as root, use the `--userName userName` option to specify the user who installed OpenDJ:

```
$ sudo create-rc-script \
--outputFile /etc/init.d/opendj \
--userName mark

$ sudo /etc/init.d/opendj start
```

For example, if you run OpenDJ on Linux as root, you can use the RC script to start the server at system boot, and stop the server at system shutdown:

```
$ sudo update-rc.d opendj defaults
update-rc.d: warning: /etc/init.d/opendj missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
Adding system startup for /etc/init.d/opendj ...
/etc/rc0.d/K20opendj -> ../init.d/opendj
/etc/rc1.d/K20opendj -> ../init.d/opendj
/etc/rc6.d/K20opendj -> ../init.d/opendj
/etc/rc2.d/S20opendj -> ../init.d/opendj
/etc/rc3.d/S20opendj -> ../init.d/opendj
/etc/rc4.d/S20opendj -> ../init.d/opendj
/etc/rc5.d/S20opendj -> ../init.d/opendj
```

- (Windows) Register OpenDJ as a Windows Service by using the **windows-service** command, described in windows-service(1) in the *OpenDJ Reference*, and then manage the service through Windows administration tools:

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

By default OpenDJ saves a compressed version of the server configuration used on successful startup. This ensures that the server provides a last known good configuration, which can be used as a reference or copied into the active configuration if the server fails to start with the current active configuration. It is possible, though not usually recommended, to turn this behavior off by changing the global server setting `save-config-on-successful-startup` to `false`.

3.2 Stopping a Server

Use one of the following techniques:

- Use the **stop-ds** command, described in `stop-ds(1)` in the *OpenDJ Reference*:

```
$ stop-ds
```

- (Linux) If OpenDJ directory server was installed from a `.deb` or `.rpm` package, then service management scripts were created at setup time.

Use the **service opendj stop** command:

```
centos# service opendj stop
Stopping opendj (via systemctl): [ OK ]
```

```
ubuntu$ sudo service opendj stop
$Stopping opendj: ... > SUCCESS.
```

- (UNIX) Create an RC script, and then use the script to stop the server:

```
$ sudo create-rc-script \
--outputFile /etc/init.d/opendj \
--userName mark

$ sudo /etc/init.d/opendj stop
```

- (Windows) Register OpenDJ as a Windows Service, and then manage the service through Windows administration tools:

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

3.3 Restarting a Server

Use one of the following techniques:

- Use the **stop-ds** command:

```
$ stop-ds --restart
```

- (Linux) If OpenDJ directory server was installed from a .deb or .rpm package, then service management scripts were created at setup time.

Use the **service opendj restart** command:

```
centos# service opendj restart
Restarting opendj (via systemctl): [ OK ]
```

```
ubuntu$ sudo service opendj restart
$Stopping opendj: ... > SUCCESS.

$Starting opendj: > SUCCESS.
```

- (UNIX) Create an RC script, and then use the script to stop the server:

```
$ sudo create-rc-script \
  --outputFile /etc/init.d/opendj \
  --userName mark

$ /etc/init.d/opendj restart
```

- (Windows) Register OpenDJ as a Windows Service, and then manage the service through Windows administration tools:

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

3.4 Server Recovery

OpenDJ tends to show resilience when restarting after a crash or after the server process is killed abruptly. OpenDJ might have to replay the last few entries in a transaction log. Generally, OpenDJ returns to service quickly.

Database recovery messages are found in the database log file, such as `/path/to/opendj/db/userRoot/dj.log`.

The following example shows two example messages from the recovery log. The first message is written at the beginning of the recovery process. The second message is written at the end of the process:

```
111104 10:23:48:967 CONFIG [/path/to/openssl/db/userRoot]Recovery
underway, found end of log
...
111104 10:23:49:015 CONFIG [/path/to/openssl/db/userRoot]Recovery finished:
Recovery Info ...
```

What can take some time during server startup is preloading database content into memory when the server starts. Objects cached in memory do not survive a crash. By default, OpenDJ does not cache objects in memory before starting to accept client requests. You can, however, set the `preload-time-limit` property for the database cache of your backend if you do want to load objects into the database cache before OpenDJ begins accepting client connections.

Chapter 4

Importing and Exporting LDIF Data

This chapter covers management of LDAP Data Interchange Format (LDIF) data. In this chapter you will learn to:

- Generate test LDIF data
- Import and export LDIF data
- Perform searches and modifications on LDIF files with command-line tools
- Create and manage database backends to house directory data imported from LDIF
- Delete database backends

LDIF provides a mechanism for representing directory data in text format. LDIF data is typically used to initialize directory databases, but also may be used to move data between different directories that cannot replicate directly, or even as an alternative backup format.

4.1 Generating Test Data

When you install OpenDJ, you have the option of importing sample data that is generated during the installation. This procedure demonstrates how to generate LDIF by using the **make-ldif** command, described in `make-ldif(1)` in the *OpenDJ Reference*.

Procedure 4.1. To Generate Test LDIF Data

The **make-ldif** command uses templates to provide sample data. Default templates are located in the `/path/to/openssl/config/MakeLDIF/` directory. The `example.template` file can be used to create a suffix with entries of the type `inetOrgPerson`. You can do the equivalent in OpenDJ control panel (Directory Data > New Base DN... > Import Automatically Generated Example Data).

1. Write a file to act as the template for your generated LDIF.

The resulting test data template depends on what data you expect to encounter in production. Base your work on your knowledge of the production data, and on the sample template, `/path/to/openssl/config/MakeLDIF/example.template`, and associated data.

See `make-ldif.template(5)` in the *OpenDJ Reference* for reference information about template files.

2. Create additional data files for the content in your template to be selected randomly from a file, rather than generated by an expression.

Additional data files are located in the same directory as your template file.

3. Decide whether you want to generate the same test data each time you run the **make-ldif** command with your template.

If so, provide the same `randomSeed` integer each time you run the command.

4. Before generating a very large LDIF file, make sure you have enough space on disk.

5. Run the **make-ldif** command to generate your LDIF file:

```
$ make-ldif \
--randomSeed 0 \
--templateFile /path/to/my.template \
--ldifFile /path/to/generated.ldif
Processed 1000 entries
Processed 2000 entries
...
Processed 10000 entries
LDIF processing complete. 10003 entries written
```

4.2 Importing and Exporting Data

You can use OpenDJ control panel to import data (Directory Data > Import LDIF) and to export data (Directory Data > Export LDIF). The following procedures

demonstrate how to use the **import-ldif** and **export-ldif** commands, described in `import-ldif(1)` in the *OpenDJ Reference* and `export-ldif(1)` in the *OpenDJ Reference*.

Procedure 4.2. To Import LDIF Data

The most efficient method of importing LDIF data is to take the OpenDJ server offline. Alternatively, you can schedule a task to import the data while the server is online.



Note

Importing from LDIF overwrites all data in the target backend with entries from the LDIF data.

1. If you do not want to use the default `userRoot` backend, create a new backend for your data.

See [Section 4.4, "Creating a New Database Backend"](#) for details.

2. The following example imports `dc=example,dc=org` data into the `userRoot` backend, overwriting existing data:
 - If you want to speed up the process—for example because you have millions of directory entries to import—first shut down the server, and then run the **import-ldif** command:

```
$ stop-ds
$ import-ldif \
  --includeBranch dc=example,dc=org \
  --backendID userRoot \
  --ldifFile /path/to/generated.ldif
```

- If not, schedule a task to import the data while online:

```
$ import-ldif \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --includeBranch dc=example,dc=org \
  --backendID userRoot \
  --ldifFile /path/to/generated.ldif \
  --trustAll
```

Notice that the task is scheduled through communication over SSL on the administration port, by default 4444. You can schedule the import task to start at a particular time using the `--start` option.

The `--trustAll` option trusts all SSL certificates, such as a default self-signed certificate used for testing.

3. If the server is replicated with other servers, initialize replication again after the successful import.

For details see [Section 8.3.2, "Initializing Replicas"](#).

Initializing replication overwrites data in the remote servers in the same way that import overwrites existing data with LDIF data.

Procedure 4.3. To Export LDIF Data

The following examples export `dc=example,dc=org` data from the `userRoot` backend:

1. To expedite export, shut down the server and then use the **export-ldif** command:

```
$ stop-ds
$ export-ldif \
  --includeBranch dc=example,dc=org \
  --backendID userRoot \
  --ldifFile /path/to/backup.ldif
```

2. To export the data while online, leave the server running and schedule a task:

```
$ export-ldif \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --includeBranch dc=example,dc=org \
  --backendID userRoot \
  --ldifFile /path/to/backup.ldif \
  --start 20111221230000 \
  --trustAll
```

The `--start 20111221230000` option tells OpenDJ to start the export at 11 PM on December 21, 2012.

If OpenDJ is stopped at this time, then when you start OpenDJ again, the server attempts to perform the task after starting up.

4.3 Other Tools For Working With LDIF Data

This section demonstrates the **ldifsearch**, **ldifmodify** and **ldif-diff** commands, described in `ldifsearch(1)` in the *OpenDJ Reference*, `ldifmodify(1)` in the *OpenDJ Reference*, and `ldif-diff(1)` in the *OpenDJ Reference*.

4.3.1 Searching in LDIF With **ldifsearch**

The **ldifsearch** command is to LDIF files what the **ldapsearch** command is to directory servers:

```
$ ldifsearch \  
--baseDN dc=example,dc=org \  
--ldifFile generated.ldif \  
"(sn=Grenier)" \  
mobile  
dn: uid=user.4630,ou=People,dc=example,dc=org  
mobile: +1 728 983 6669
```

The `--ldifFile ldif-file` option replaces the `--hostname` and `--port` options used to connect to an LDAP directory. Otherwise, the command syntax and LDIF output is familiar to **ldapsearch** users.

4.3.2 Updating LDIF With **ldifmodify**

The **ldifmodify** command lets you apply changes to LDIF files, generating a new, changed version of the original file:

```
$ cat changes.ldif  
dn: uid=user.0,ou=People,dc=example,dc=org  
changetype: modify  
replace: description  
description: This is the new description for Aaccf Amar.  
-  
replace: initials  
initials: AAA  
  
$ ldifmodify \  
--sourceLDIF generated.ldif \  
--changesLDIF changes.ldif \  
--targetLDIF new.ldif
```

Notice that the resulting new LDIF file is likely to be about the same size as the source LDIF file.

4.3.3 Comparing LDIF With **ldif-diff**

The **ldif-diff** command reports differences between two LDIF files in LDIF format:

```
$ ldif-diff --sourceLDIF old.ldif --targetLDIF new.ldif
dn: uid=user.0,ou=People,dc=example,dc=org
changetype: modify
add: initials
initials: AAA
-
delete: initials
initials: ASA
-
add: description
description: This is the new description for Aaccf Amar.
-
delete: description
description: This is the description for Aaccf Amar.
```

The **ldif-diff** command reads both files into memory, and constructs tree maps to perform the comparison. The command is designed to work with small files and fragments, and can quickly run out of memory when calculating differences between large files.

4.4 Creating a New Database Backend

OpenDJ stores your directory data in a *backend*. A backend is a repository that a directory server can access to store data. OpenDJ directory server offers different implementations, such as memory backends, LDIF file backends, and database backends. Database backends can be backed up and restored. By default, OpenDJ stores your data in a database backend named `userRoot`.

You can create new backends using the **dsconfig create-backend** command, described in `dsconfig create-backend(1)` in the *OpenDJ Reference*. OpenDJ directory server supports a variety of backend types, including in-memory backends, backends that store data in LDIF files, and backends that store data in key-value databases with indexes to improve performance with large data sets. When you create a backend, choose the type of backend that fits your purpose.

The following example creates a backend named `myData`. The backend is of type `pdb`, which relies on a PDB database for data storage and indexing. Alternatively, you can choose a different backend type with a different argument to the `--type` option, as in `--type je`:

```
$ dsconfig \
create-backend \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--type pdb \
--backend-name myData \
--set base-dn:dc=example,dc=com \
--set enabled:true \
--set db-cache-percent:25 \
--trustAll \
--no-prompt
```

Notice the setting `db-cache-percent:25`. This says to allocate 25% of memory available to the JVM to the new backend's database cache. The default setting for `db-cache-percent` allocates 50%. When creating a new database backend, take care to keep the total memory allocated to all database caches lower than the total memory available to the JVM. As an alternative to `db-cache-percent`, you can use `db-cache-size`. The `db-cache-size` value is a specific amount of memory, such as 2 GB.

After creating the backend, you can view the settings as in the following example:

```
$ dsconfig \
get-backend-prop \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--backend-name myData \
--trustAll \
--no-prompt
Property          : Value(s)
-----
backend-id        : myData
base-dn           : "dc=example,dc=com"
compact-encoding  : true
db-cache-percent  : 25
db-cache-size     : 0 b
db-directory      : db
enabled           : true
index-entry-limit : 4000
writability-mode  : enabled
```

Alternatively, you can create a new backend in OpenDJ control panel (Directory Data > New Base DN > Backend > New Backend: *backend-name*).

When you create a new backend using the **dsconfig** command, OpenDJ directory server creates the following indexes automatically:

aci presence

ds-sync-conflict equality
ds-sync-hist ordering
entryUUID equality
objectClass equality

You can create additional indexes as described in [Section 7.3, “Configuring and Rebuilding Indexes”](#).

4.5 Setting Disk Space Thresholds For Database Backends

Directory data growth depends on applications that use the directory. As a result, when directory applications add more data than they delete, the database backend grows until it fills the available disk space. The system can end up in an unrecoverable state if no disk space is available.

Database backends therefore have advanced properties, `disk-low-threshold` and `disk-full-threshold`. When available disk space falls below `disk-low-threshold`, OpenDJ server only allows updates from users and applications that have the `bypass-lockdown` privilege, as described in [Section 6.2, “About Privileges”](#). When available space falls below `disk-full-threshold`, OpenDJ server stops allowing updates, instead returning an `UNWILLING_TO_PERFORM` error to each update request.

OpenDJ server continues to apply replication updates without regard to the thresholds. OpenDJ server can therefore fill available disk space despite the thresholds, by accepting replication updates made on other servers. You can give yourself more time to react to the situation both by monitoring directory data growth and also by increasing the thresholds.

If growth across the directory service tends to happen quickly, set the thresholds higher than the defaults to allow more time to react when growth threatens to fill the disk. The following example sets `disk-low-threshold` to 2 GB `disk-full-threshold` to 1 GB for the `userRoot` backend:

```
$ dsconfig \
  set-backend-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --set "disk-low-threshold:2 GB" \
  --set "disk-full-threshold:1 GB" \
  --trustAll \
  --no-prompt
```

The properties `disk-low-threshold` and `disk-full-threshold` are listed as *advanced* properties. To examine their values with the **dsconfig** command, use the `--advanced` option as shown in the following example:

```
$ dsconfig \
  get-backend-prop \
  --advanced \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --property disk-low-threshold \
  --property disk-full-threshold \
  --trustAll \
  --no-prompt
Property          : Value(s)
-----
disk-full-threshold : 1 gb
disk-low-threshold  : 2 gb
```

4.6 Updating an Existing Backend to Add a New Base DN

In addition to letting you create new backends as described in [Section 4.4, "Creating a New Database Backend"](#), OpenDJ lets you add a new base DN to an existing backend.

The following example adds the suffix `o=example` to the existing backend `userRoot`:

```
$ dsconfig \
  set-backend-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --add base-dn:o=example \
  --trustAll \
  --no-prompt

$ dsconfig \
  get-backend-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --property base-dn \
  --trustAll \
  --no-prompt
Property : Value(s)
-----:-----
base-dn  : "dc=example,dc=com", o=example
```

Alternatively, you can update an existing backend in OpenDJ control panel (Directory Data > New Base DN, then select the existing backend from the dropdown Backend list, and enter the new Base DN name).

4.7 Deleting a Database Backend

You delete a database backend by using the **dsconfig delete-backend** command, described in `dsconfig delete-backend(1)` in the *OpenDJ Reference*.

When you delete a database backend by using the **dsconfig delete-backend** command, OpenDJ does not actually remove the database files for two reasons. First, a mistake could potentially cause lots of data to be lost. Second, deleting a large database backend could cause severe service degradation due to a sudden increase in I/O load.

Instead, after you run the **dsconfig delete-backend** command you must also manually remove the database backend files.

If you do run the **dsconfig delete-backend** command by mistake and have not yet deleted the actual files, then you can recover from the mistake by creating the backend again, reconfiguring the indexes that were removed, and rebuilding the indexes as described in [Section 7.3, "Configuring and Rebuilding Indexes"](#).

Chapter 5

Configuring Connection Handlers

This chapter shows you how to configure OpenDJ directory server to listen for directory client requests using connection handlers. You can view information about connection handlers in the OpenDJ control panel, and update the configuration using the **dsconfig** command, described in `dsconfig(1)` in the *OpenDJ Reference*.

In this chapter you will learn to:

- Enable client applications to access the directory over LDAP and secure LDAP (LDAPS)
- Enable client applications to access the directory over HTTP whether using DSML, or the REST style
- Enable monitoring using Java Management Extensions (JMX), or over Simple Network Management Protocol (SNMP)
- Enable automated processing of LDIF files
- Configure restrictions for client access such as requiring authentication or limiting the maximum number of concurrent connections
- Configure transport layer security for all relevant protocols

5.1 LDAP Client Access

You configure LDAP client access by using the command-line tool **dsconfig**. By default you configure OpenDJ to listen for LDAP when you install.

The standard port number for LDAP client access is 389. If you install OpenDJ directory server as a user who can use port 389 and the port is not yet in use, then 389 is the default port number presented at installation time. If you install as a user who cannot use a port < 1024, then the default port number presented at installation time is 1389.

Procedure 5.1. To Change the LDAP Port Number

1. Change the port number using the **dsconfig** command:

```
$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAP Connection Handler" \
  --set listen-port:11389 \
  --trustAll \
  --no-prompt
```

This example changes the port number to 11389 in the configuration.

2. Restart the connection handler so the change takes effect.

To restart the connection handler, you disable it, then enable it again:

```
$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAP Connection Handler" \
  --set enabled:false \
  --trustAll \
  --no-prompt

$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAP Connection Handler" \
  --set enabled:true \
  --trustAll \
  --no-prompt
```

5.2 Preparing For Secure Communications

One common way to protect connections between OpenDJ and client applications involves using StartTLS for LDAP or LDAPS to secure connections. OpenDJ and client applications use X.509 digital certificates to set up secure connections.

Both OpenDJ and client applications check that certificates are signed by a trusted party before accepting them. Merely setting up a secure connection therefore involves a sort of authentication using certificates. If either OpenDJ or the client application cannot trust the peer certificate, then the attempt to set up a secure connection will fail.

By default OpenDJ client tools prompt you if they do not recognize the server certificate. Other clients might not prompt you. OpenDJ server has no one to prompt when a client presents a certificate that cannot be trusted, so refuses to set up the connection.¹ In other words, it is important for both OpenDJ and client applications to be able to verify that peer certificates exchanged have been signed by a trusted party.

In practice, this means that both OpenDJ and client applications must put the certificates that were used to sign each others' certificates in their respective truststores. Conventionally, certificates are therefore signed by a Certificate Authority (CA). A CA is trusted to sign other certificates. The Java runtime environment, for example, comes with a truststore holding certificates from many

¹Unless you use the Blind Trust Manager Provider, which is recommended only for test purposes.

well-known CAs.² If your client uses a valid certificate signed by one of these CAs, then OpenDJ can verify the certificate without additional configuration, because OpenDJ can find the CA certificate in the Java CA certificate truststore. Likewise, if you set up StartTLS or LDAPS in OpenDJ using a valid certificate signed by one of these CAs, then many client applications can verify the OpenDJ server certificate without further configuration.

In summary, if you need a certificate to be recognized automatically, get the certificate signed by a well-known CA.

You can, however, choose to have your certificates signed some other way. You can set up your own CA. You can use a CA whose signing certificate is not widely distributed. You can also use self-signed certificates. In each case, you must add the signing certificates into the truststore of each peer making secure connections.

For OpenDJ directory server, you can choose to import your own CA-signed certificate as part of the installation process, or later using command-line tools. Alternatively, you can let the OpenDJ installation program create a self-signed certificate as part of the OpenDJ installation process. In addition, you can add a signing certificate to the OpenDJ truststore using the Java **keytool** command.

The following example shows the **keytool** command to add a client application's binary format, self-signed certificate to the OpenDJ truststore (assuming OpenDJ is already configured to use secure connections). This enables OpenDJ to recognize the self-signed client application certificate. By definition a self-signed certificate is itself the signing certificate. Notice that the Owner and the Issuer are the same:

²`$JAVA_HOME/jre/lib/security/cacerts` holds the CA certificates. To read the full list, use the following command:

```
$ keytool \  
-list \  
-v \  
-keystore $JAVA_HOME/jre/lib/security/cacerts \  
-storepass changeit
```

```
$ keytool \  
-import \  
-alias myapp-cert \  
-file myapp-cert.crt \  
-keystore /path/to/openssl/config/truststore \  
-storepass `cat /path/to/openssl/config/keystore.pin`  
Owner: CN=My App, OU=Apps, DC=example, DC=com  
Issuer: CN=My App, OU=Apps, DC=example, DC=com  
Serial number: 5ae2277  
Valid from: Fri Jan 18 18:27:09 CET 2013 until: Thu Jan 13 18:27:09 CET 2033  
Certificate fingerprints:  
MD5: 48:AC:F9:13:11:E0:AB:C4:65:A2:83:9E:DB:FE:0C:37  
SHA1: F9:61:54:37:AA:C1:BC:92:45:07:64:4B:23:6C:BC:C9:CD:1D:44:0F  
SHA256: 2D:B1:58:CD:33:40:E9:ED:...:EA:C9:FF:6A:19:93:FE:E4:84:E3  
Signature algorithm name: SHA256withRSA  
Version: 3  
  
Extensions:  
  
#1: ObjectId: 2.5.29.14 Criticality=false  
SubjectKeyIdentifier [  
KeyIdentifier [  
0000: 54 C0 C5 9C 73 37 85 4B F2 3B D3 37 FD 45 0A AB T...s7.K.;.7.E..  
0010: C9 6B 32 95 .k2.  
]  
]  
  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

When working with a certificate in printable encoding format (.pem) rather than binary format, use the `-rfc` option, too.

Restart OpenDJ after adding certificates to the truststore to make sure that OpenDJ reads the updated truststore file.

On the client side, if your applications are Java applications, then you can also import the OpenDJ signing certificate into the trust store for the applications using the **keytool** command.

The following example shows the **keytool** command to export the OpenDJ self-signed certificate in binary format:

```
$ keytool \  
-export \  
-alias server-cert \  
-file server-cert.crt \  
-keystore /path/to/openssl/config/keystore \  
-storepass `cat /path/to/openssl/config/keystore.pin`  
Certificate stored in file <server-cert.crt>
```

Importing the server certificate is similar to importing the client certificate, as shown above.

The following sections describe how to get and install certificates for OpenDJ directory server on the command-line, for use when setting up StartTLS or LDAPS.

Procedure 5.2. To Request and Install a CA-Signed Certificate

First, create a server private key and public key certificate in a Java Keystore. Next, issue a signing request to the CA, and get the CA-signed certificate as a reply. Then, set up the key manager provider and trust manager provider to rely on your new server certificate stored in the OpenDJ keystore.

1. Generate the server private key and public key certificate by using the Java **keytool** command.

The FQDN for OpenDJ directory server, which you can see under Server Details in the OpenDJ control panel, is set both as a `DNSName` in the certificate's `SubjectAlternativeName` list, and also in the `CN` of the certificate's subject name DN for backwards compatibility:

```
$ keytool \  
-genkey \  
-alias server-cert \  
-keyalg rsa \  
-ext "san=dns:opendj.example.com" \  
-dname "CN=opendj.example.com,O=Example Corp,C=FR" \  
-keystore /path/to/opendj/config/keystore \  
-storepass changeit \  
-keypass changeit
```



Note

Notice that the `-storepass` and `-keypass` options take identical password arguments. OpenDJ requires that you use the same password to protect both the keystore and the private key.

If the server can respond on multiple FQDNs, then specify multiple subject alternative names when using the **keytool** command's `-ext` option. In the following example the primary FQDN is `opendj.example.com` and the alternative is `ldap.example.com`:

```
$ keytool \  
-genkey \  
-alias server-cert \  
-keyalg rsa \  
-ext "san=dns:opendj.example.com,dns:ldap.example.com" \  
-dname "CN=opendj.example.com,O=Example Corp,C=FR" \  
-keystore /path/to/opendj/config/keystore \  
-storepass changeit \  
-keypass changeit
```

2. Create a certificate signing request file for the certificate you generated:

```
$ keytool \  
-certreq \  
-alias server-cert \  
-keystore /path/to/opendj/config/keystore \  
-storepass changeit \  
-file server-cert.csr
```

3. Have the CA sign the request (server-cert.csr).

See the instructions from your CA on how to provide the request.

The CA returns the signed certificate.

4. If you have set up your own CA and signed the certificate, or are using a CA whose signing certificate is not included in the Java runtime environment, import the CA certificate into the keystore so that it can be trusted.

Otherwise, when you import the signed certificate in the reply from the (unknown) CA, **keytool** fails to import the signed certificate with the message `keytool error: java.lang.Exception: Failed to establish chain from reply`.

The following example illustrates the import of a CA certificate created with the **openssl** command. See the **openssl** documentation for instructions on creating CAs and on signing other certificates with the CA you created:

```
$ keytool \  
-import \  
-trustcacerts \  
-keystore /path/to/openssl/config/keystore \  
-file ca.crt \  
-alias ca-cert \  
-storepass changeit  
Owner: EMAILADDRESS=admin@example.com, CN=Example CA, O=Example Corp, C=FR  
Issuer: EMAILADDRESS=admin@example.com, CN=Example CA, O=Example Corp, C=FR  
Serial number: d4586ea05c878b0c  
Valid from: Tue Jan 29 09:30:31 CET 2013 until: Mon Jan 24 09:30:31 CET 2033  
Certificate fingerprints:  
MD5: 8A:83:61:9B:E7:18:A2:21:CE:92:94:96:59:68:60:FA  
SHA1: 01:99:18:38:3A:57:D7:92:7B:D6:03:8C:7B:E4:1D:37:45:0E:29:DA  
SHA256: 5D:20:F1:86:CC:CD:64:50:...:DF:15:43:07:69:44:00:FB:36:CF  
Signature algorithm name: SHA1withRSA  
Version: 3  
  
Extensions:  
  
#1: ObjectId: 2.5.29.35 Criticality=false  
AuthorityKeyIdentifier [  
KeyIdentifier [  
0000: 30 07 67 7D 1F 09 B6 E6 90 85 95 58 94 37 FD 31 0.g.....X.7.1  
0010: 03 D4 56 7B ..V.  
]  
[EMAILADDRESS=admin@example.com, CN=Example CA, O=Example Corp, C=FR]  
SerialNumber: [ d4586ea0 5c878b0c]  
]  
  
#2: ObjectId: 2.5.29.19 Criticality=false  
BasicConstraints:[  
CA:true  
PathLen:2147483647  
]  
  
#3: ObjectId: 2.5.29.14 Criticality=false  
SubjectKeyIdentifier [  
KeyIdentifier [  
0000: 30 07 67 7D 1F 09 B6 E6 90 85 95 58 94 37 FD 31 0.g.....X.7.1  
0010: 03 D4 56 7B ..V.  
]  
]  
  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

5. Import the signed certificate from the CA reply into the keystore where you generated the server certificate.

In this example the certificate from the reply is `~/Downloads/server-cert.crt`:


```
$ keytool \  
-import \  
-trustcacerts \  
-alias server-cert \  
-file ~/Downloads/server-cert.crt \  
-keystore /path/to/openssl/config/keystore \  
-storepass changeit \  
-keypass changeit  
Certificate reply was installed in keystore
```

6. Configure the file-based key manager provider for the Java Keystore (JKS) to use the file name and keystore PIN that you set up with the **keytool** command:

```
$ dsconfig \  
set-key-manager-provider-prop \  
--hostname openssl.example.com \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--provider-name JKS \  
--set enabled:true \  
--set key-store-pin:changeit \  
--remove key-store-pin-file:config/keystore.pin \  
--trustAll \  
--no-prompt
```

7. Configure the file-based trust manager provider.

By convention and by default, the OpenSSL file-based trust manager provider uses a JKS file, openssl/config/truststore, to hold trusted public key certificates. Follow these steps to set up the truststore file, and to configure the trust manager provider.

- a. If you imported your own CA certificate into the keystore, also import the file into the truststore:

```
$ keytool \  
-import \  
-trustcacerts \  
-keystore /path/to/openssl/config/truststore \  
-file ca.crt \  
-alias ca-cert \  
-storepass changeit  
Owner: EMAILADDRESS=admin@example.com, CN=Example CA, O=Example Corp, C=FR  
Issuer: EMAILADDRESS=admin@example.com, CN=Example CA, O=Example Corp, C=FR  
Serial number: d4586ea05c878b0c  
Valid from: Tue Jan 29 09:30:31 CET 2013 until: Mon Jan 24 09:30:31 CET 2033  
Certificate fingerprints:  
MD5: 8A:83:61:9B:E7:18:A2:21:CE:92:94:96:59:68:60:FA  
SHA1: 01:99:18:38:3A:57:D7:92:7B:D6:03:8C:7B:E4:1D:37:45:0E:29:DA  
SHA256: 5D:20:F1:86:CC:CD:64:50:...:DF:15:43:07:69:44:00:FB:36:CF  
Signature algorithm name: SHA1withRSA  
Version: 3  
  
Extensions:  
  
#1: ObjectId: 2.5.29.35 Criticality=false  
AuthorityKeyIdentifier [  
KeyIdentifier [  
0000: 30 07 67 7D 1F 09 B6 E6 90 85 95 58 94 37 FD 31 0.g.....X.7.1  
0010: 03 D4 56 7B ..V.  
]  
[EMAILADDRESS=admin@example.com, CN=Example CA, O=Example Corp, C=FR]  
SerialNumber: [ d4586ea0 5c878b0c]  
]  
  
#2: ObjectId: 2.5.29.19 Criticality=false  
BasicConstraints:[  
CA:true  
PathLen:2147483647  
]  
  
#3: ObjectId: 2.5.29.14 Criticality=false  
SubjectKeyIdentifier [  
KeyIdentifier [  
0000: 30 07 67 7D 1F 09 B6 E6 90 85 95 58 94 37 FD 31 0.g.....X.7.1  
0010: 03 D4 56 7B ..V.  
]  
]  
  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

- b. Import the signed server certificate into the truststore:

```
$ keytool \  
-import \  
-trustcacerts \  
-alias server-cert \  
-file ~/Downloads/server-cert.crt \  
-keystore /path/to/openssl/config/truststore \  
-storepass changeit \  
-keypass changeit  
Certificate was added to keystore
```

- c. Configure the file-based trust manager provider to use the truststore:

```
$ dsconfig \  
set-trust-manager-provider-prop \  
--hostname openssl.example.com \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--provider-name JKS \  
--set enabled:true \  
--set trust-store-file:config/truststore \  
--set trust-store-pin:changeit \  
--trustAll \  
--no-prompt
```

At this point, OpenDJ directory server can use your new CA-signed certificate, for example, for StartTLS and LDAPS connection handlers.

8. If you use a CA certificate that is not known to clients, such as a CA that you set up yourself rather than a well-known CA whose certificate is included with the client system, import the CA certificate into the client application truststore. Otherwise the client application cannot trust the signature on the OpenDJ CA-signed server certificate.

Procedure 5.3. To Create and Install a Self-Signed Certificate

If you choose to configure LDAP secure access when setting up OpenDJ directory server, the setup program generates a key pair in the JKS `/path/to/openssl/config/keystore`, and self-signs the public key certificate, which has the alias `server-cert`. The password for the keystore and the private key is stored in cleartext in the file `/path/to/openssl/config/keystore.pin`.

If you want to secure communications, but did not chose to configure LDAP secure access at setup time, this procedure can help. The following steps explain how to create and install a key pair with a self-signed certificate in preparation for configuring LDAPS or HTTPS. First, create a key pair in a new JKS, and then self-sign the certificate. Next, set up the key manager provider and trust manager provider to access the new server certificate in the new keystore.

To replace the existing server key pair with a self-signed certificate and new private key, first, use **keytool -delete -alias server-cert** to delete the existing keys, then generate a new key pair with the same alias. Either reuse the existing password in `keystore.pin`, or use a new password as shown in the steps below.

1. Generate the server certificate using the Java **keytool** command:

```
$ keytool \  
-genkey \  
-alias server-cert \  
-keyalg rsa \  
-ext "san=dns:opendj.example.com" \  
-dname "CN=opendj.example.com,O=Example Corp,C=FR" \  
-keystore /path/to/opendj/config/keystore \  
-storepass changeit \  
-keypass changeit
```

In this example, OpenDJ is running on a system with fully qualified host name `opendj.example.com`. The JKS is created in the `config` directory where OpenDJ is installed, which is the default value for a JKS.



Note

Notice that the `-storepass` and `-keypass` options take identical password arguments. OpenDJ requires that you use the same password to protect both the keystore and the private key.

If the server can respond on multiple FQDNs, then specify multiple subject alternative names when using the **keytool** command's `-ext` option. In the following example the primary FQDN is `opendj.example.com` and the alternative is `ldap.example.com`:

```
$ keytool \  
-genkey \  
-alias server-cert \  
-keyalg rsa \  
-ext "san=dns:opendj.example.com,dns:ldap.example.com" \  
-dname "CN=opendj.example.com,O=Example Corp,C=FR" \  
-keystore /path/to/opendj/config/keystore \  
-storepass changeit \  
-keypass changeit
```

Keep track of the password provided to the `-storepass` and `-keypass` options.

2. Self-sign the server certificate:

```
$ keytool \  
-selfcert \  
-alias server-cert \  
-keystore /path/to/openssl/config/keystore \  
-storepass changeit
```

3. Configure the file-based key manager provider for JKS to access the Java Keystore with keystore/private key password.

In this example, the alias is server-cert and the password is changeit.

If you are replacing a key pair with a self-signed certificate, reusing the server-cert alias and password stored in keystore.pin, then you can skip this step:

```
$ echo changeit > /path/to/openssl/config/keystore.pin  
$ chmod 600 /path/to/openssl/config/keystore.pin  
$ dsconfig \  
  set-key-manager-provider-prop \  
    --hostname openssl.example.com \  
    --port 4444 \  
    --bindDN "cn=Directory Manager" \  
    --bindPassword password \  
    --provider-name JKS \  
    --set enabled:true \  
    --set key-store-file:config/keystore \  
    --set key-store-pin-file:config/keystore.pin \  
    --trustAll \  
    --no-prompt
```

4. Configure the file-based trust manager provider for JKS to use the new server certificate.

By convention and by default, the OpenDJ file-based trust manager provider uses a Java Keystore file, openssl/config/truststore, to hold trusted public key certificates. Follow these steps to set up the truststore file, and to configure the trust manager provider.

a. Set up a truststore containing the server's public key certificate:

```
$ keytool \  
-export \  
-alias server-cert \  
-keystore /path/to/openssl/config/keystore \  
-storepass changeit \  
-file server-cert.crt  
Certificate stored in file <server-cert.crt>  
$ keytool \  
-import \  
-trustcacerts \  
-alias server-cert \  
-file server-cert.crt \  
-keystore /path/to/openssl/config/truststore \  
-storepass changeit  
...  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

- b. Configure the trust manager provider to use the truststore:

```
$ echo changeit > /path/to/openssl/config/truststore.pin  
$ chmod 600 /path/to/openssl/config/truststore.pin  
$ dsconfig \  
set-trust-manager-provider-prop \  
--hostname openssl.example.com \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--provider-name JKS \  
--set enabled:true \  
--set trust-store-file:config/truststore \  
--set trust-store-pin-file:config/truststore.pin \  
--trustAll \  
--no-prompt
```

At this point, OpenDJ directory server can use your new self-signed certificate, for example, for StartTLS and LDAPS or HTTPS connection handlers.

5.3 LDAP Client Access With Transport Layer Security

StartTLS negotiations start on the unsecure LDAP port, and then protect communication with the client. You can configure StartTLS during installation, or later using the **dsconfig** command.

Procedure 5.4. To Enable StartTLS on the LDAP Port

1. Make sure you have a server certificate installed:

```
$ keytool \  
-list \  
-alias server-cert \  
-keystore /path/to/openssl/config/keystore \  
-storepass `cat /path/to/openssl/config/keystore.pin`  
server-cert, Jun 17, 2013, PrivateKeyEntry,  
Certificate fingerprint (SHA1): 92:B7:4C:4F:2E:24:...:EB:7C:22:3F
```

2. Activate StartTLS on the current LDAP port:

```
$ dsconfig \  
set-connection-handler-prop \  
--hostname openssl.example.com \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--handler-name "LDAP Connection Handler" \  
--set allow-start-tls:true \  
--set key-manager-provider:JKS \  
--set trust-manager-provider:JKS \  
--trustAll \  
--no-prompt
```

The change takes effect. No need to restart the server.

5.4 LDAP Client Access Over SSL

You configure LDAPS (LDAP/SSL) client access by using the command-line tool **dsconfig**. You can opt to configure LDAPS access when you install.

The standard port number for LDAPS client access is 636. If you install OpenDJ directory server as a user who can use port 636 and the port is not yet in use, then 636 is the default port number presented at installation time. If you install as a user who cannot use a port < 1024, then the default port number presented at installation time is 1636.

Procedure 5.5. To Set Up LDAPS Access

1. Make sure you have a server certificate installed:

```
$ keytool \  
-list \  
-alias server-cert \  
-keystore /path/to/openssl/config/keystore \  
-storepass `cat /path/to/openssl/config/keystore.pin`  
server-cert, Jun 17, 2013, PrivateKeyEntry,  
Certificate fingerprint (SHA1): 92:B7:4C:4F:2E:24:...:EB:7C:22:3F
```

2. Configure the server to activate LDAPS access:

```
$ dsconfig \  
set-connection-handler-prop \  
--hostname openssl.example.com \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--handler-name "LDAPS Connection Handler" \  
--set listen-port:1636 \  
--set enabled:true \  
--set use-ssl:true \  
--trustAll \  
--no-prompt
```

This example changes the port number to 1636 in the configuration.

Procedure 5.6. To Change the LDAPS Port Number

1. Change the port number using the **dsconfig** command:

```
$ dsconfig \  
set-connection-handler-prop \  
--hostname openssl.example.com \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--handler-name "LDAPS Connection Handler" \  
--set listen-port:11636 \  
--trustAll \  
--no-prompt
```

This example changes the port number to 11636 in the configuration.

2. Restart the connection handler so the change takes effect.

To restart the connection handler, you disable it, then enable it again:


```
$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAPS Connection Handler" \
  --set enabled:false \
  --trustAll \
  --no-prompt

$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAPS Connection Handler" \
  --set enabled:true \
  --trustAll \
  --no-prompt
```

5.5 Restricting Client Access

Using the OpenDJ directory server global configuration properties, you can add global restrictions on how clients access the server. These settings are per server, and so must be set independently on each server in replication topology.

These global settings are fairly coarse-grained. For a full discussion of the rich set of administrative privileges and fine-grained access control instructions that OpenDJ directory server supports, see [Chapter 6, "Configuring Privileges and Access Control"](#).

Consider the following global configuration settings:

`bind-with-dn-requires-password`

Whether the directory server should reject any simple bind request that contains a DN but no password. Default: `true`

To change this setting use the following command:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set bind-with-dn-requires-password:false \
  --no-prompt
```

max-allowed-client-connections

Restricts the number of concurrent client connections to the directory server. Default: 0, meaning no limit is set.

To set a limit of 32768 use the following command:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set max-allowed-client-connections:32768 \
  --no-prompt
```

reject-unauthenticated-requests

Rejects any request (other than bind or StartTLS requests) received from a client that has not yet been authenticated, whose last authentication attempt was unsuccessful, or whose last authentication attempt used anonymous authentication. Default: false.

To shut down anonymous binds use the following command:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set reject-unauthenticated-requests:true \
  --no-prompt
```

return-bind-error-messages

Does not restrict access, but by default prevents OpenDJ directory server from returning extra information about why a bind failed, as that information could be used by an attacker. Instead, the information is written to the server errors log. Default: false.

To have OpenDJ return additional information about why a bind failed use the following command:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set return-bind-error-messages:true \
  --no-prompt
```

5.6 TLS Protocols and Cipher Suites

By default OpenDJ supports the SSL and TLS protocols and the cipher suites supported by the underlying Java virtual machine. For details see the documentation for the Java virtual machine (JVM) in which you run OpenDJ. For Oracle Java, see the *Java Cryptography Architecture Oracle Providers Documentation* for the [The SunJSSE Provider](#).

To list the available protocols and cipher suites, read the `supportedTLSProtocols` and `supportedTLSCiphers` attributes of the root DSE. Install unlimited strength Java cryptography extensions for stronger ciphers:

```
$ ldapsearch --port 1389 --baseDN "" --searchScope base "(objectclass=*)" \
supportedTLSCiphers supportedTLSProtocols
dn:
supportedTLSCiphers: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_RSA_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
supportedTLSCiphers: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_RSA_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_DHE_DSS_WITH_AES_128_CBC_SHA
supportedTLSCiphers: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
supportedTLSCiphers: TLS_ECDHE_RSA_WITH_RC4_128_SHA
supportedTLSCiphers: SSL_RSA_WITH_RC4_128_SHA
supportedTLSCiphers: TLS_ECDH_ECDSA_WITH_RC4_128_SHA
supportedTLSCiphers: TLS_ECDH_RSA_WITH_RC4_128_SHA
supportedTLSCiphers: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: SSL_RSA_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
supportedTLSCiphers: SSL_RSA_WITH_RC4_128_MD5
supportedTLSCiphers: TLS_EMPTY_RENEGOTIATION_INFO_SCSV
supportedTLSProtocols: SSLv2Hello
supportedTLSProtocols: SSLv3
supportedTLSProtocols: TLSv1
supportedTLSProtocols: TLSv1.1
supportedTLSProtocols: TLSv1.2
```

You can restrict the list of protocols and cipher suites used by setting the `ssl-protocol` and `ssl-cipher-suite` connection handler properties to include only the protocols or cipher suites you want.

For example, to restrict the cipher suites to TLS_EMPTY_RENEGOTIATION_INFO_SCSV and TLS_RSA_WITH_AES_256_CBC_SHA use the **dsconfig set-connection-handler-prop** command as shown in the following example:

```
$ dsconfig \
  set-connection-handler-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAPS Connection Handler" \
  --add ssl-cipher-suite:TLS_EMPTY_RENEGOTIATION_INFO_SCSV \
  --add ssl-cipher-suite:TLS_RSA_WITH_AES_256_CBC_SHA \
  --no-prompt \
  --trustAll
```

5.7 Client Certificate Validation and the Directory

This section clarifies the roles that client applications' X.509 digital certificates play in establishing secure connections and in authenticating the client as a directory user. Keep in mind that establishing a secure connection happens before the server handles the LDAP or HTTP requests that the client sends over the secure connection. Establishing a secure connection is handled separately from authenticating a client as a directory user, even though both processes can involve the client's certificate.

When a client and a server negotiate a secure connection over LDAPS or HTTPS, they can use public key cryptography to authenticate each other. The server, client, or both present certificates to each other. By default, OpenDJ directory server LDAPS and HTTPS connection handlers are configured to present the server certificate, and to consider the client certificate optional. The connection handlers' `ssl-client-auth-policy` property makes the latter behavior configurable. For the DSML and REST to LDAP gateways, HTTPS negotiation is handled by the web application container where the gateway runs. See the web application container documentation for details on configuring how the container handles the client certificate.

One step toward establishing a secure connection involves validating the certificate that was presented by the other party. Part of this is trusting the certificate. The certificate identifies the client or server and the CA certificate used to sign the client or server certificate. The validating party checks that the other party corresponds to the one identified by the certificate, and checks that the signature can be trusted. If the signature is valid, and the CA certificate used to sign the certificate can be trusted, then the certificate can be trusted. This part of the validation process is also described briefly in [Section 5.2, "Preparing For Secure Communications"](#).

Certificates can be revoked after they are signed. Therefore, the validation process can involve checking whether the certificate is still valid. Two different methods for performing this validation use the Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRLs). OCSP is a newer solution that provides an online service to handle the revocation check for a specific certificate. CRLs are potentially large lists of user certificates that are no longer valid or that are on hold. A CRL is signed by the CA. The validating party obtains the CRL and checks that the certificate being validated is not listed. For a brief comparison, see [OCSP: Comparison to CRLs](#). A certificate can include links to contact the OCSP responder or to the CRL distribution point. The validating party can use these links to check whether the certificate is still valid.

In both cases, the CA who signed the certificate acts as the OCSP responder or publishes the CRLs. When establishing a secure connection with a client application, OpenDJ relies on the CA for OCSP and CRLs. This is the case even when OpenDJ is the repository for the CRLs.

OpenDJ is a logical repository for certificates and CRLs. For example, OpenDJ directory server can store CRLs in a `certificateRevocationList` attribute as in the following example entry:

```
dn: cn=My CA,dc=example,dc=com
objectClass: top
objectClass: applicationProcess
objectClass: certificationAuthority
cn: My CA
authorityRevocationList;binary: Base64-encoded ARL
cACertificate;binary:: Base64-encoded CA certificate
certificateRevocationList;binary:: Base64-encoded CRL
```

The CRL could then be replicated to other OpenDJ directory servers for high availability. (Notice the ARL in this entry. An ARL is like a CRL, but for CA certificates.)

Again, despite being a repository for CRLs, OpenDJ does not use the CRLs directly when checking a client certificate. Instead, when negotiating a secure connection, OpenDJ depends on the JVM security configuration. The JVM configuration governs whether validation uses OCSP, CRLs, or both. As described in the *Java PKI Programmer's Guide* under [Support for the CRL Distribution Points Extension](#), and [Appendix C: On-Line Certificate Status Protocol \(OCSP\) Support](#), the JVM relies on system properties that define whether to use the CRL distribution points defined in certificates, and how to handle OCSP requests. These system properties can be set system-wide in `$JAVA_HOME/lib/security/java.security` (`$JAVA_HOME/jre/lib/security/java.security` for the JDK). The JVM handles revocation checking without OpenDJ's involvement.

After a connection is negotiated, OpenDJ directory server can authenticate a client application at the LDAP level based on the certificate. For details, see

Section 2.9, “Authenticating Using a Certificate” in the *OpenDJ Directory Server Developer's Guide*.

OCSP and obtaining CRLs depend on network access to the CA. If OpenDJ directory servers or the DSML or REST to LDAP gateways run on a network where the CA is not accessible, and the deployment nevertheless requires OSCP or checking CRLs for client application certificates, then you must provide some alternative means to handle OCSP or CRL requests. The JVM can be configured to use a locally available OCSP responder, for example, and that OCSP responder might depend on OpenDJ directory server. If the solution depends on CRLs, you could regularly update the CRLs in the directory with copies of the CA CRLs obtained by other means.

5.8 RESTful Client Access

OpenDJ offers two ways to give RESTful client applications HTTP access to directory data as JSON resources:

1. Enable the listener on OpenDJ directory server to respond to REST requests.

With this approach, you do not need to install additional software.

2. Configure the external REST to LDAP gateway Servlet to access your directory service.

With this approach, you must install the gateway separately.

Procedure 5.7. To Set Up REST Access to OpenDJ Directory Server

OpenDJ directory server has a handler for HTTP connections where it exposes the RESTful API demonstrated in Chapter 1, in the *OpenDJ Directory Server Developer's Guide*. The HTTP connection handler is not enabled by default.

You configure the mapping between JSON resources and LDAP entries by editing the configuration file for the HTTP connection handler, by default `/path/to/openssl/config/http-config.json`. The configuration is described in Appendix A, in the *OpenDJ Reference*. The default mapping works out of the box with Example.com data generated as part of the setup process and with [Example.ldif](#):

1. Enable the connection handler:

```
$ dsconfig \
  set-connection-handler-prop \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "HTTP Connection Handler" \
    --set enabled:true \
    --no-prompt \
    --trustAll
```

2. Enable the HTTP access log:

```
$ dsconfig \
  set-log-publisher-prop \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based HTTP Access Logger" \
    --set enabled:true \
    --no-prompt \
    --trustAll
```

This enables the HTTP access log, `opendj/logs/http-access`. For details on the format of the HTTP access log, see [Section 17.5, "Server Logs"](#).

3. Try reading a resource.

The HTTP connection handler paths start by default at the root context, as shown in the following example:

```
$ curl http://bjensen:hifalutin@opendj.example.com:8080/users/bjensen
{
  "_rev" : "00000000315fb731",
  "schemas" : [ "urn:scim:schemas:core:1.0" ],
  "manager" : [ {
    "_id" : "trigden",
    "displayName" : "Torrey Rigden"
  } ],
  "contactInformation" : {
    "telephoneNumber" : "+1 408 555 1862",
    "emailAddress" : "bjensen@example.com"
  },
  "_id" : "bjensen",
  "name" : {
    "familyName" : "Jensen",
    "givenName" : "Barbara"
  },
  "userName" : "bjensen@example.com",
  "displayName" : "Barbara Jensen"
}
```

4. If necessary, change the connection handler configuration using the **dsconfig** command.

The following example shows how to set the port to 8443, and to configure the connection handler to use transport layer security (using the default server certificate). If you did not generate a default, self-signed certificate when installing OpenDJ directory server, see [Procedure 5.3, "To Create and Install a Self-Signed Certificate"](#), and more generally see [Section 5.2, "Preparing For Secure Communications"](#) for additional instructions including how to import a CA-signed certificate:


```

$ dsconfig \
  set-trust-manager-provider-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Blind Trust" \
  --set enabled:true \
  --no-prompt \
  --trustAll

$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "HTTP Connection Handler" \
  --set listen-port:8443 \
  --set use-ssl:true \
  --set key-manager-provider:JKS \
  --set trust-manager-provider:"Blind Trust" \
  --no-prompt \
  --trustAll

$ stop-ds --restart
Stopping Server...
.... The Directory Server has started successfully

$ keytool \
  -export \
  -rfc \
  -alias server-cert \
  -keystore /path/to/opendj/config/keystore \
  -storepass `cat /path/to/opendj/config/keystore.pin` \
  -file server-cert.pem
Certificate stored in file <server-cert.pem>

$ curl \
  --cacert server-cert.pem \
  --user bjensen:hifalutin \
  https://opendj.example.com:8443/users/bjensen
{
  "_rev" : "0000000018c8b685",
  "schemas" : [ "urn:scim:schemas:core:1.0" ],
  "contactInformation" : {
    "telephoneNumber" : "+1 408 555 1862",
    "emailAddress" : "bjensen@example.com"
  },
  "_id" : "bjensen",
  "name" : {
    "familyName" : "Jensen",
    "givenName" : "Barbara"
  },
  "userName" : "bjensen@example.com",
  "displayName" : "Barbara Jensen",
  "manager" : [ {
    "_id" : "trigden",
    "displayName" : "Torrey Rigden"
  } ]
}

```

Notice the `--cacert server-cert.pem` option used with the **curl** command. This is the way to specify a self-signed server certificate when using HTTPS.

Procedure 5.8. To Set Up OpenDJ REST to LDAP Gateway

Follow these steps to set up OpenDJ REST to LDAP gateway Servlet to access your directory service.

1. Download and install the gateway as described in Procedure 1.9, “To Install OpenDJ REST to LDAP Gateway” in the *OpenDJ Installation Guide*.
2. Adjust the configuration for your directory service as described in Appendix A, in the *OpenDJ Reference*.

5.9 DSML Client Access

Directory Services Markup Language (DSML) client access is implemented as a servlet that runs in a web application container.

You configure DSML client access by editing the `WEB-INF/web.xml` after you deploy the web application. In particular, you must at least set the `ldap.host` and `ldap.port` parameters if they differ from the default values, which are `localhost` and `389`.

The list of DSML configuration parameters, including those that are optional, consists of the following:

`ldap.host`

Required parameter indicating the host name of the underlying directory server. Default: `localhost`.

`ldap.port`

Required parameter indicating the LDAP port of the underlying directory server. Default: `389`.

`ldap.userdn`

Optional parameter specifying the DN used by the DSML gateway to bind to the underlying directory server. Not used by default.

`ldap.userpassword`

Optional parameter specifying the password used by the DSML gateway to bind to the underlying directory server. Not used by default.

`ldap.authzidtypeisid`

This parameter can help you set up the DSML gateway to do HTTP Basic Access Authentication, given the appropriate mapping between the user ID, and the user's entry in the directory.

Required boolean parameter specifying whether the HTTP Authorization header field's Basic credentials in the request hold a plain ID, rather than a DN. If set to true, then the gateway performs an LDAP SASL bind using SASL plain, enabled by default in OpenDJ to look for an exact match between a uid value and the plain ID value from the header. In other words, if the plain ID is bjensen, and that corresponds in the directory server to Babs Jensen's entry with DN uid=bjensen,ou=people,dc=example,dc=com, then the bind happens as Babs Jensen. Note also that you can configure OpenDJ identity mappers for scenarios that use a different attribute than uid, such as the mail attribute.

Default: false

`ldap.usessl`

Required parameter indicating whether `ldap.port` points to a port listening for LDAPS (LDAP/SSL) traffic. Default: false.

`ldap.usestarttls`

Required parameter indicating whether to use StartTLS to connect to the specified `ldap.port`. Default: false.

`ldap.trustall`

Required parameter indicating whether to blindly trust all certificates presented to the DSML gateway when using secure connections (LDAPS or StartTLS). Default: false.

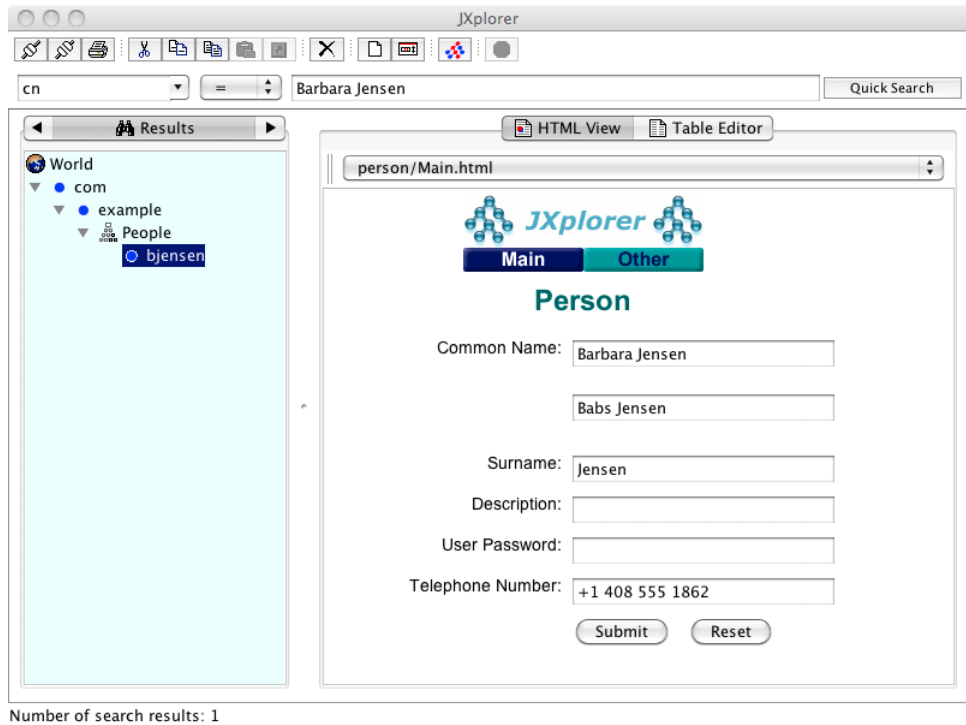
`ldap.truststore.path`

Optional parameter indicating the truststore used to verify certificates when using secure connections. If you want to connect using LDAPS or StartTLS, and do not want the gateway blindly to trust all certificates, then you must set up a truststore. Not used by default.

`ldap.truststore.password`

Optional parameter indicating the truststore password. If you set up and configure a truststore, then you need to set this as well. Not used by default.

The DSML servlet translates between DSML and LDAP, and passes requests to the directory server. For initial testing purposes, you might try [JXplorer](#), where DSML Service: `/webapp-dir/DSMLServlet`. Here, *webapp-dir* refers to the name of the directory in which you unpacked the DSML .war. [Figure 5.1, "JXplorer Accessing OpenDJ Directory Server"](#) shows the result.

Figure 5.1. JXplorer Accessing OpenDJ Directory Server

5.10 JMX Client Access

You configure Java Management Extensions (JMX) client access by using the command-line tool, **dsconfig**.

Procedure 5.9. To Set Up JMX Access

1. Configure the server to activate JMX access:

```
$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "JMX Connection Handler" \
  --set enabled:true \
  --trustAll \
  --no-prompt
```

This example uses the default port number, 1689.

2. Restart the server so the change takes effect:

```
$ stop-ds --restart
```

Procedure 5.10. To Configure Access To JMX

After you set up OpenDJ directory server to listen for JMX connections, you must assign privileges in order to allow a user to connect over protocol:

1. Assign the privileges, `jmx-notify`, `jmx-read`, and `jmx-write` as necessary to the user who connects over JMX. For details see [Section 6.3, "Configuring Privileges"](#).
2. Connect using the service URI, user name, and password:

Service URI

Full URI to the service including the hostname or IP address and port number for JMX where OpenDJ directory server listens for connections. For example, if the server IP is `192.168.0.10` and you configured OpenDJ to listen for JMX connections on port 1689, then the service URI is `service:jmx:rmi:///jndi/rmi://192.168.0.10:1689/org.opends.server.protocols.jmx.client-unknown`.

User name

The full DN of the user with privileges to connect over JMX such as `uid=kvaughan,ou=People,dc=example,dc=com`.

Password

The bind password for the user.

5.11 LDIF File Access

The LDIF connection handler lets you make changes to directory data by placing LDIF in a file system directory that OpenDJ server regularly polls for changes. The LDIF, once consumed, is deleted.

You configure LDIF file access by using the command-line tool **dsconfig**.

Procedure 5.11. To Set Up LDIF File Access

1. Activate LDIF file access:

```
$ dsconfig \
  set-connection-handler-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDIF Connection Handler" \
  --set enabled:true \
  --trustAll \
  --no-prompt
```

The change takes effect immediately.

2. Add the directory where you put LDIF to be processed:

```
$ mkdir /path/to/opendj/config/auto-process-ldif
```

This example uses the default value of the `ldif-directory` property for the LDIF connection handler.

5.12 SNMP Access

For instructions on setting up the SNMP connection handler, see [Section 17.2, "SNMP-Based Monitoring"](#).

Chapter 6

Configuring Privileges and Access Control

OpenDJ supports two mechanisms to protect access to the directory, *access control instructions* and administrative *privileges*. Access control instructions apply to directory data, providing fine-grained control over what a user or group member is authorized to do in terms of LDAP operations. Most access control instructions specify scopes (targets) to which they apply such that an administrative user who has all access to `dc=example,dc=com` need not have any access to `dc=example,dc=org`. Privileges control the administrative tasks that users can perform, such as bypassing the access control mechanism, performing backup and restore operations, making changes to the configuration, and other tasks.

Privileges are implemented independently from access control. By default, privileges restrict administrative access to directory root users, though any user can be assigned a privilege. Privileges apply to a directory server, and do not have a scope. This chapter covers both access control and privileges. In this chapter you will learn to:

- Configure privileges for directory administration
- Read and write access control instructions
- Configure access rights by setting access control instructions
- Evaluate effective access rights for a particular user

Some operations require both privileges and also access control instructions. For example, in order to reset user's passwords, an administrator needs both the password-reset privilege and also access control to write userPassword values on the user entries. By combining an access control instruction with a privilege, you can effectively restrict the scope of that privilege to a particular branch of the Directory Information Tree.

6.1 About Access Control Instructions

OpenDJ directory server access control instructions (ACIs) exist as operational aci attribute values on directory entries, and as global ACIs stored in the configuration. ACIs apply to a scope defined in the instruction, and set permissions that depend on what operation is requested, who requested the operation, and how the client connected to the server.

For example, the ACIs on the following entry allow anonymous read access to all attributes except passwords, and allow read-write access for directory administrators under dc=example,dc=com:

```
dn: dc=example,dc=com
objectClass: domain
objectClass: top
dc: example
aci: (target = "ldap:///dc=example,dc=com")(targetattr !=
"userPassword")(version 3.0;acl "Anonymous read-search access";
allow (read, search, compare)(userdn = "ldap:///anyone");)
aci: (target="ldap:///dc=example,dc=com") (targetattr =
"")(version 3.0; acl "allow all Admin group"; allow(all) groupdn =
"ldap:///cn=Directory Administrators,ou=Groups,dc=example,dc=com";)
```

OpenDJ directory server's default behavior is that no access is allowed unless it is specifically granted by an access control instruction. In addition privileges assigned to certain users such as cn=Directory Manager allow them to bypass access control checks.

OpenDJ directory server provides several global ACIs out of the box to facilitate evaluation while maintaining a reasonable security policy. By default users are allow to read the root DSE, to read the schema, to use certain controls and extended operations, to modify their own entries, to bind, and other operations. Global ACIs are defined on the access control handler, and apply to the entire directory server. You must adjust the default global ACIs to match the security policies for your organization, for example, to restrict anonymous access.

ACI attribute values use a specific language described in this section. Although ACI attribute values can become difficult to read in LDIF, the basic syntax is simple:


```
targets(version 3.0;acl "name";permissions subjects;)
```

The following list briefly explains the variables in the syntax above:

targets

The *targets* specifies entries, attributes, controls, and extended operations to which the ACI applies.

To include multiple *targets*, enclose each individual target in parentheses, (). When you specify multiple targets, all targets must match for the ACI to apply (AND).

name

Supplies a human-readable description of what the ACI does.

permissions

Defines which actions to allow, and which to deny. Paired with *subjects*.

subjects

Identify clients to which the ACI applies depending on who connected, and when, where, and how they connected. Paired with *permissions*.

Separate multiple pairs of *permissions subjects* definitions with semicolons, ;. When you specify multiple permissions-subjects pairs, at least one must match (OR).

6.1.1 ACI Targets

The seven types of ACI targets identify the objects to which the ACI applies. Most expressions allow you to use either = to specify that the target should match the value or != to specify that the target should not match the value:

```
(target [!]= "ldap:///DN")
```

Sets the scope to the entry with distinguished name *DN*, and to child entries.

You can use asterisks, *, to replace attribute types, attribute values, and entire DN components. In other words, the following specification targets both uid=bjensen,ou=People,dc=example,dc=com and also cn=Frank Zappa,ou=Musicians,dc=example,dc=com:

```
(target = "ldap:///*=*,*,dc=example,dc=com")
```

The *DN* must be in the subtree of the entry on which the ACI is defined.

If you do not specify target, then the entry holding this ACI will be affected. If targetscope is also omitted, then this entry and all subordinates will be affected.

(targetattr [!]= "*attr-list*")

Replace *attr-list* with a list of attribute type names, such as `userPassword`, separating multiple attribute type names with `||`.

This specification affects the entry where the ACI is located, or the entries specified by other targets in the ACI.

You can use an asterisk, `*`, to specify all user attributes, although you will see better performance when explicitly including or excluding attribute types needed. You can use a plus sign, `+`, to specify all operational attributes.

Note that a negated *attr-list* of operational attributes will only match other operational attributes and never any user attributes, and vice-versa.

If you do not include this target specification, then by default no attributes are affected by the ACI.

(targetfilter [!]= "*ldap-filter*")

Sets the scope to match the *ldap-filter* dynamically, as in an LDAP search. The *ldap-filter* can be any valid LDAP filter.

(targetattrfilters [!]= "*expression*")

Use this target specification when managing changes made to particular attributes.

Here *expression* takes one of the following forms. Separate expressions with semicolons (`;`):

```
op=attr1:filter1[&& attr2:filter2 ...][;op=attr3:filter3[&& attr4:filter4 ...] ...]
```

Here *op* can be either `add` for operations creating attributes, or `del` for operations removing them. Replace *attr* with an attribute type. Replace *filter* with an LDAP filter that corresponds to the *attr* attribute type.

(targetscope = "*base|onelevel|subtree|subordinate*")

Here *base* refers to the entry where the ACI is defined, *onelevel* to immediate children, *subtree* to the base entry and all children, and *subordinate* to all children only.

If you do not specify *targetscope*, then the default is *subtree*.

(targetcontrol [!]= "*OID*")

Replace *OID* with the object identifier for the LDAP control to target. Separate multiple OIDs with `||`.

To use an LDAP control, the bind DN user must have `allow(read)` permissions.

This target cannot be restricted to a specific subtree by combining it with another target.

(extop [!]= "*OID*")

Replace *OID* with the object identifier for the extended operation to target.
Separate multiple OIDs with ||.

To use an LDAP extended operation, the bind DN user must have allow(read) permissions.

This target cannot be restricted to a specific subtree by combining it with another target.

6.1.2 ACI Permissions

ACI permission definitions take one of the following forms:

allow(*action*[, *action* ...])

deny(*action*[, *action* ...])



Tip

Although deny is supported, avoid restricting permissions by using deny. Instead, explicitly allow access only where needed. What looks harmless and simple in your lab examples can grow difficult to maintain in a real-world deployment with nested ACIs.

Replace *action* with one of the following:

add

Entry creation, as for an LDAP add operation.

all

All permissions, except export, import, proxy.

compare

Attribute value comparison, as for an LDAP compare operation.

delete

Entry deletion, as for an LDAP delete operation.

export

Entry export during a modify DN operation.

Despite the name, this action is unrelated to LDIF export operations.

import

Entry import during a modify DN operation.

Despite the name, this action is unrelated to LDIF import operations.

proxy

Access the ACI target using the rights of another user.

read

Read entries and attributes, or use an LDAP control or extended operation.

search

Search the ACI targets. Needs to be combine with read in order to read the search results.

selfwrite

Add or delete own DN from a group.

write

Modify attributes on ACI target entries.

6.1.3 ACI Subjects

ACI subjects match characteristics of the client connection to the server. Use subjects to restrict whether the ACI applies depending on who connected, and when, where, and how they connected. Most expressions allow you to use either = to specify that the subject condition should match the value or != to specify that the subject condition should not match the value:

authmethod [!]= "*none|simple|ssl|sasl mech*"

Here you use *none* to mean do not check, *simple* for simple authentication, *ssl* for certificate-based authentication over LDAPS, *sasl mech* for SASL where *mech* is DIGEST-MD5, EXTERNAL, or GSSAPI.

dayofweek [!]= "*day[, day ...]*"

Replace *day* with one of sun, mon, tue, wed, thu, fri, sat.

dns [!]= "*hostname*"

You can use asterisks, *, to replace name components, such as *dns* = "*.myCompany.com".

groupdn [!]= "*ldap:///DN[| ldap:///DN ...]*"

Replace *DN* with the distinguished name of a group to permit or restrict access for members.

ip [!]= "*addresses*"

Here *addresses* can be specified for IPv4 or IPv6. IPv6 addresses are specified in brackets as *ldap://[address]/subnet-prefix* where */subnet-prefix* is optional. You can specify individual IPv4 addresses, addresses with

asterisks (*) to replace subnets and host numbers, CIDR notation, and forms such as 192.168.0.*+255.255.255.0 to specify subnet masks.

```
ssf = "strength"  
ssf != "strength"  
ssf > "strength"  
ssf >= "strength"  
ssf < "strength"  
ssf <= "strength"
```

Here the security strength factor pertains to the cipher key strength for connections using DIGEST-MD5, GSSAPI, SSL, or TLS. For example, to require that the connection must have at least 128 bits of encryption, specify `ssf >= "128"`.

```
timeofday = "hhmm"  
timeofday != "hhmm"  
timeofday > "hhmm"  
timeofday >= "hhmm"  
timeofday < "hhmm"  
timeofday <= "hhmm"
```

Here *hhmm* is expressed as on a 24-hour clock. For example, 1:15 PM is written 1315.

```
userattr [!]= "attr#value"  
userattr [!]= ldap-url#LDAPURL"  
userattr [!]= "[parent[child-level]. ]attr#GROUPDN|USERDN"
```

The `userattr` subject specifies an attribute that must match on both the bind entry and the target of the ACI.

To match when the user attribute on the bind DN entry corresponds directly to the attribute on the target entry, replace *attr* with the user attribute type, and *value* with the attribute value. To get the attributes of the bind entry, OpenDJ performs an internal search for the user attributes. This ACI subject therefore does not work with operational attributes.

To match when the target entry is identified by an LDAP URL, and the bind DN is in the subtree of the DN of the LDAP URL, use `ldap-url#LDAPURL`.

To match when the bind DN corresponds to a member of the group identified by the *attr* value on the target entry, use `attr#GROUPDN`.

To match when the bind DN corresponds to the *attr* value on the target entry, use `attr#USERDN`.

The optional inheritance specification, `parent[child-level].`, lets you specify how many levels below the target entry inherit the ACI. Here *child-level* is a number from 0 to 9, with 0 indicating the target entry only. Separate multiple *child-level* digits with commas (.).

```
userdn [!]= "ldap-url++[|] ldap-url++ ...]"
```

To match the bind DN, replace *ldap-url++* with either a valid LDAP URL such as `ldap:///uid=bjensen,ou=People,dc=example,dc=com`, `ldap:///dc=example,dc=com??sub?(uid=bjensen)`, or a special LDAP URL-like keyword from the following list:

`ldap:///all`

Match authenticated users.

`ldap:///anyone`

Match anonymous and authenticated users.

`ldap:///parent`

Match when the bind DN is a parent of the ACI target.

`ldap:///self`

Match when the bind DN entry corresponds to ACI target.

6.1.4 How ACI is Evaluated

Understanding how OpenDJ evaluates the *aci* values is critical when implementing an access control policy. The rules the server follows are simple:

1. To determine if an operation is allowed or denied, the OpenDJ server looks in the directory for the target of the operation. It collects any *aci* values from that entry, and then walks up the directory tree to the suffix, collecting all *aci* values en route. Global *aci* values are then collected.
2. It then separates the *aci* values into two lists; one list contains all the *aci* values that matches the target and denies the required access, and the other list contains all the *aci* values that matches the target and allows the required access.
3. If the deny list contains any *aci* values after this procedure, access will be immediately denied.
4. If the deny list is empty, then the allow list is processed. If the allow list contains any *aci* values, access will be allowed.
5. If both lists are empty, access will be denied.



Note

Some operations require multiple permissions and involve multiple targets. Evaluation will therefore take place multiple

times. For example, a search operation requires the search permission for each attribute in the search filter. If all those are allowed, the read permission is used to decide what attributes and values can be returned.

6.1.5 ACI Required For LDAP Operations

The minimal access control information required for specific LDAP operations is described here:

Add

The ACI must allow the add permission to entries in the target. This implicitly allows the attributes and values to be set. Use `targattrfilters` to explicitly deny access to any values if required.

For example, the ACI required to allow `uid=bjensen,ou=People,dc=example,dc=com` to add an entry is:

```
aci: (version 3.0;acl "Add entry"; allow (add)(userdn =  
"ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

Bind

Because this is used to establish the user's identity and derived authorizations, ACI is irrelevant for this operation and is not checked. To prevent authentication, disable the account instead. For details see [Section 11.2, "Managing Accounts Manually"](#).

Compare

The ACI must allow the compare permission to the attribute in the target entry.

For example, the ACI required to allow `uid=bjensen,ou=People,dc=example,dc=com` to compare values against the `sn` attribute is:

```
aci: (targetattr = "sn")(version 3.0;acl "Compare surname";  
allow (compare)(userdn =  
"ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

Delete

The ACI must allow the delete permission to the target entry. This implicitly allows the attributes and values in the target to be deleted. Use `targattrfilters` to explicitly deny access to the values if required.

For example, the ACI required to allow uid=bjensen,ou=People,dc=example,dc=com to delete an entry is:

```
aci: (version 3.0;acl "Delete entry"; allow (delete)
      (userdn = "ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

Modify

The ACI must allow the write permission to attributes in the target entries. This implicitly allows all values in the target attribute to be modified. Use targattrfilters to explicitly deny access to specific values if required.

For example, the ACI required to allow uid=bjensen,ou=People,dc=example,dc=com to modify the description attribute in an entry is:

```
aci: (targetattr = "description")(version 3.0;
      acl "Modify description"; allow (write)(userdn =
      "ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

ModifyDN

If the entry is being moved to a newSuperior, the export permission must be allowed on the target, and the import permission must be allowed on the newSuperior entry.

The ACI must allow write permission to the attributes in the old RDN and the new RDN. All values of the old RDN and new RDN can be written implicitly; use targattrfilters to explicitly deny access to values used if required.

For example, the ACI required to allow uid=bjensen,ou=People,dc=example,dc=com to rename entries named with the uid attribute to new locations:

```
aci: (targetattr = "uid")(version 3.0;acl "Rename uid= entries";
      allow (write, import, export)(userdn =
      "ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

Search

ACI is required to process the search filter, and to determine what attributes and values may be returned in the results. The search permission is used to allow particular attributes in the search filter. The read permission is used to allow particular attributes to be returned. If read permission is allowed to any attribute, the server will automatically allow the objectClass attribute to also be read.

For example, the ACI required to allow uid=bjensen,ou=People,dc=example,dc=com to search for uid attributes, and also to read that attribute in matching entries is:


```
aci: (targetattr = "uid")(version 3.0;acl "Search and read uid";  
  allow (search, read)(userdn =  
    "ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

Use Control or Extended Operation

The ACI must allow the read permission to the targetcontrol or extop OIDs.

For example, the ACI required to allow uid=bjensen,ou=People,dc=example,dc=com to use the Persistent Search request control with OID 2.16.840.1.113730.3.4.3 is:

```
aci: (targetcontrol = "2.16.840.1.113730.3.4.3")(version 3.0;acl  
  "Request Persistent Search"; allow (read)(userdn =  
    "ldap:///uid=bjensen,ou=People,dc=example,dc=com");)
```

6.2 About Privileges

Privileges provide access control for server administration independently from access control instructions.

Directory root users, such as cn=Directory Manager, are granted privileges in the following list and marked with an asterisk (*) by default. Other administrator users can be assigned privileges, too:

backend-backup*

Request a task to back up data

backend-restore*

Request a task to restore data from backup

bypass-acl*

Perform operations without regard to ACIs

bypass-lockdown*

Perform operations without regard to lockdown mode

cancel-request*

Cancel any client request

changelog-read*

Read the changelog (under cn=changelog)

config-read*

Read the server configuration

`config-write*`
Change the server configuration

`data-sync`
Perform data synchronization

`disconnect-client*`
Close any client connection

`jmx-notify`
Subscribe to JMX notifications

`jmx-read`
Read JMX attribute values

`jmx-write`
Write JMX attribute values

`ldif-export*`
Export data to LDIF

`ldif-import*`
Import data from LDIF

`modify-acl*`
Change ACIs

`password-reset*`
Reset other users' passwords

`privilege-change*`
Change the privileges assigned to users

`proxied-auth`
Use the Proxied Authorization control

`server-lockdown*`
Put OpenDJ into and take OpenDJ out of lockdown mode

`server-restart*`
Request a task to restart the server

`server-shutdown*`
Request a task to stop the server

`subentry-write*`
Perform LDAP subentry write operations

`unindexed-search*`
Search using a filter with no corresponding index

update-schema*
Change OpenDJ schema definitions

* = default directory root user privileges

6.3 Configuring Privileges

For root directory administrators, by default `cn=Directory Manager`, you configure privileges using the **dsconfig** command.

For non-root directory administrators, you add privileges with the **ldapmodify** command.

Procedure 6.1. To Change Root DN Privileges

1. Start **dsconfig** in interactive mode:

```
$ dsconfig \  
--port 4444 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password
```

2. Select the Root DN menu.
3. Select View and edit the Root DN.
4. Edit the `default-root-privilege-name`.
5. Make sure you apply the changes when finished.

Procedure 6.2. To Add Privileges on an Individual Entry

Privileges are specified using the `ds-privilege-name` operational attribute, which you can change on the command-line using **ldapmodify**.

1. Determine the privileges to add:

```
$ cat privilege.ldif  
dn: uid=kvaughan,ou=People,dc=example,dc=com  
changetype: modify  
add: ds-privilege-name  
ds-privilege-name: config-read  
ds-privilege-name: password-reset
```

This example lets the user read the server configuration, and reset user passwords. In order for the user to be able to change a user password, you must also allow the modification using ACIs. For this example, Kirsten Vaughan is a member of the Directory Administrators group for Example.com, and already has access to modify user entries.

Prior to having the privileges, Kirsten gets messages about insufficient access when trying to read the server configuration, or reset a user password:

```
$ ldapsearch \
--port 1389 \
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
--bindPassword bribery \
--baseDN cn=config \
"(objectclass=*)"
SEARCH operation failed
Result Code: 50 (Insufficient Access Rights)
Additional Information: You do not have sufficient privileges to perform
search operations in the Directory Server configuration

$ ldappasswordmodify \
--port 1389 \
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
--bindPassword bribery \
--authzID "dn:uid=scarter,ou=People,dc=example,dc=com" \
--newPassword changeit
The LDAP password modify operation failed with result code 50
Error Message: You do not have sufficient privileges to perform password
reset operations
```

2. Apply the change as a user with the privilege-change privilege:

```
$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename privilege.ldif
Processing MODIFY request for uid=kvaughan,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=kvaughan,ou=People,dc=example,dc=com
```

At this point, Kirsten can perform the operations requiring privileges:

```
$ ldapsearch
--port 1389
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com"
--bindPassword bribery
--baseDN cn=config
"(objectclass=*)"
dn: cn=config
ds-cfg-return-bind-error-messages: false
ds-cfg-default-password-policy: cn=Default Password Policy,cn=Password Policies,
cn=config
...

$ ldapmodify -x \
--port 1389 \
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
--bindPassword bribery \
--authID "dn:uid=scarter,ou=People,dc=example,dc=com" \
--newPassword changeit
The LDAP password modify operation was successful
```

Procedure 6.3. To Add Privileges For a Group of Administrators

For deployments with more than one administrator, you no doubt use a group to define administrative rights. You can use a collective attribute subentry to specify privileges for the administrator group.

Collective attributes provide a standard mechanism for defining attributes that appear on all the entries in a particular subtree. OpenDJ extends collective attributes to give you fine-grained control over which entries in the subtree are targeted. Also, OpenDJ lets you use virtual attributes, such as `isMemberOf` to construct the filter for targeting entries to which the collective attributes apply. This allows you, for example, to define administrative privileges that apply to all users who belong to an administrator group:

1. Create an LDAP subentry that specifies the collective attributes:

```
$ cat collective.ldif
dn: cn=Administrator Privileges,dc=example,dc=com
objectClass: collectiveAttributeSubentry
objectClass: extensibleObject
objectClass: subentry
objectClass: top
cn: Administrator Privileges
ds-privilege-name;collective: config-read
ds-privilege-name;collective: config-write
ds-privilege-name;collective: ldif-export
ds-privilege-name;collective: modify-acl
ds-privilege-name;collective: password-reset
ds-privilege-name;collective: proxied-auth
subtreeSpecification: {base "ou=people", specificationFilter
  "(isMemberOf=cn=Directory Administrators,ou=Groups,dc=example,dc=com)" }

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename collective.ldif
Processing ADD request for cn=Administrator Privileges,dc=example,dc=com
ADD operation successful for DN cn=Administrator Privileges,dc=example,dc=com
```

The Directory Administrators group for Example.com includes members like Kirsten Vaughan.

2. Observe that the change takes effect immediately:

```
$ ldappasswordmodify \
--port 1389 \
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
--bindPassword bribery \
--authzID "dn:uid=scarter,ou=People,dc=example,dc=com" \
--newPassword changeit
The LDAP password modify operation was successful
```

Procedure 6.4. To Limit Inherited Privileges

When privileges are set as described in [Procedure 6.3, "To Add Privileges For a Group of Administrators"](#), the same list of privileges is applied to every target account. OpenDJ also assigns default directory root user privileges. In some cases the list of inherited privileges can be too broad. OpenDJ has a mechanism to limit the privileges assigned by preceding the privilege attribute value with a `-`.

The following steps show how to prevent Kirsten Vaughan from resetting passwords when the privilege is assigned as in [Procedure 6.3, "To Add Privileges For a Group of Administrators"](#):

1. Check the privilege settings for the account:

```
$ ldapsearch \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--baseDN dc=example,dc=com \
"(uid=kvaughan)" \
ds-privilege-name
dn: uid=kvaughan,ou=People,dc=example,dc=com
ds-privilege-name: config-read
ds-privilege-name: config-write
ds-privilege-name: ldif-export
ds-privilege-name: modify-acl
ds-privilege-name: password-reset
ds-privilege-name: proxied-auth
```

2. Set the privilege attribute for the account to deny the privilege:

```
$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password
dn: uid=kvaughan,ou=people,dc=example,dc=com
changetype: modify
add: ds-privilege-name
ds-privilege-name: -password-reset

Processing MODIFY request for uid=kvaughan,ou=people,dc=example,dc=com
MODIFY operation successful for DN uid=kvaughan,ou=people,dc=example,dc=com
```

3. Observe that the privilege is no longer in effect:

```
$ ldappasswordmodify \
--port 1389 \
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
--bindPassword bribery \
--authzID "dn:uid=scarter,ou=People,dc=example,dc=com" \
--newPassword changeit
The LDAP password modify operation failed with result code 50
Error Message: You do not have sufficient privileges to perform password
reset operations
```

6.4 Configuring Access Control

Access control instructions are defined in the data as values for `aci` attributes. They can be imported in LDIF and modified over LDAP. Yet in order to make changes to ACIs users first need the `modify-acl` privilege described previously. By default, only the root DN user has the `modify-acl` privilege.

Global ACIs on `cn=Access Control Handler,cn=config` can be set using the **dsconfig** command. Global ACIs have attribute type `ds-cfg-global-aci`. For a list, see [Table 6.1, "Default Global ACIs"](#).

You can modify global ACIs from the Access Control Handler menu in **dsconfig**. Modifying and removing global ACIs can have deleterious effects. Generally the impact depends on your deployment requirements.

Modifications to global ACIs fall into the following categories:

- Modification or removal is permitted.

You must test client applications when deleting the specified ACI.

- Modification or removal may affect applications.

You must test client applications when modifying or deleting the specified ACI.

- Modification or removal may affect applications, but is not recommended.

You must test client applications when modifying or deleting the specified ACI.

- Do not modify or delete.

Table 6.1. Default Global ACIs

Name	Description	ACI Definition
Anonymous control access	Anonymous and authenticated users can use the LDAP controls that are specified by OID. Modification or removal may affect applications.	<pre>(targetcontrol="2.16.840.1.113730.3.4.2 2.16.840.1.113730.3.4.17 2.16.840.1.113730.3.4.19 1.3.6.1.4.1.4203.1.10.2 1.3.6.1.4.1.42.2.27.8.5.1 2.16.840.1.113730.3.4.16 1.2.840.113556.1.4.1413 1.3.6.1.4.1.36733.2.1.5.1") (version 3.0; acl "Anonymous control access"; allow(read) userdn="ldap:///anyone");)</pre>
Anonymous extended operation access	Anonymous and authenticated users can request the LDAP extended operations that are specified by OID. Modification or removal may affect applications.	<pre>(extop="1.3.6.1.4.1.26027.1.6.1 1.3.6.1.4.1.26027.1.6.3 1.3.6.1.4.1.4203.1.11.1 1.3.6.1.4.1.1466.20037 1.3.6.1.4.1.4203.1.11.3") (version 3.0; acl "Anonymous extended operation access"; allow(read) userdn="ldap:///anyone");)</pre>

Name	Description	ACI Definition
Anonymous read access	Anonymous and authenticated users can read the user data attributes that are specified by their names. Modification or removal is permitted.	<pre>(targetattr!="userPassword authPassword debugsearchindex changes changeNumber changeType changeTime targetDN newRDN newSuperior deleteOldRDN")(version 3.0; acl "Anonymous read access"; allow (read,search,compare) userdn="ldap:///anyone";)</pre>
Authenticated users control access	Authenticated users can use the LDAP controls that are specified by OID. Modification or removal may affect applications.	<pre>(targetcontrol="1.3.6.1.1.12 1.3.6.1.1.13.1 1.3.6.1. 1.13.2 1.2.840.113556.1.4. 319 1.2.826.0.1.3344810.2.3 2.16.840.1.113730.3.4.18 2.16.840.1.113730.3.4.9 1. 2.840.113556.1.4.473 1.3.6. 1.4.1.42.2.27.9.5.9") (version 3.0; acl "Authenticated users control access"; allow(read) userdn="ldap:///all";)</pre>
Self entry modification	Authenticated users can modify the specified attributes on their own entries. Modification or removal is permitted.	<pre>(targetattr="audio authPassword description displayName givenName homePhone homePostalAddress initials jpegPhoto labeledURI mobile pager postalAddress postalCode preferredLanguage telephoneNumber userPassword") (version 3.0; acl "Self entry modification"; allow (write) userdn="ldap:///self";)</pre>
Self entry read	Authenticated users can read the password values on their own entries. By default, the server applies a one-way hash algorithm to the password value before writing it to the entry, so it is computationally difficult to recover the cleartext version of	<pre>(targetattr="userPassword authPassword")(version 3. 0; acl "Self entry read"; allow (read,search,compare) userdn="ldap:///self";)</pre>

Name	Description	ACI Definition
	the password from the stored value. Modification or removal is permitted.	
User-Visible Operational Attributes	Anonymous and authenticated users can read attributes that identify entries and that contain information about modifications to entries. Modification or removal may affect applications.	(targetattr="createTimestamp creatorsName modifiersName modifyTimestamp entryDN entryUUID subschemaSubentry etag governingStructureRule structuralObjectClass hasSubordinates numSubordinates isMemberOf") (version 3.0; acl "User-Visible Operational Attributes"; allow (read,search,compare) userdn="ldap:///anyone";)
User-Visible Root DSE Operational Attributes	Anonymous and authenticated users can read attributes that describe what the server supports. Modification or removal may affect applications.	(target="ldap:///") (targetscope="base") (targetattr="objectClass namingContexts supportedAuthPasswordSchemes supportedControl supportedExtension supportedFeatures supportedLDAPVersion supportedSASLMechanisms supportedTLSCiphers supportedTLSProtocols vendorName vendorVersion") (version 3.0; acl "User-Visible Root DSE Operational Attributes"; allow (read,search,compare) userdn="ldap:///anyone";)
User-Visible Schema Operational Attributes	Anonymous and authenticated users can read LDAP schema definitions. Modification or removal may affect applications.	(target="ldap:///cn=schema") (targetscope="base") (targetattr="objectClass attributeTypes dITContentRules dITStructureRules ldapSyntaxes matchingRules matchingRuleUse nameForms objectClasses")(version 3.

Name	Description	ACI Definition
		0; acl "User-Visible Schema Operational Attributes"; allow (read,search,compare) userdn="ldap:///anyone";)

Users with write access to add ACIs and with the `modify-acl` privilege can use the **ldapmodify** command to change ACIs located in user data.

This section therefore focuses on ACI examples, rather than demonstrating how to update the directory for each example. To update ACIs, either change them using the **ldapmodify** command, or using OpenDJ control panel.

If you use OpenDJ control panel, find the entry to modify in the Manage Entries window. Then try View > LDIF View to edit the entry. The control panel checks your syntax and lets you know if you made an error before it saves any changes.

For hints on updating directory entries with the **ldapmodify** command, see Section 2.4.2, “Modifying Entry Attributes” in the *OpenDJ Directory Server Developer's Guide*, keeping in mind that the name of the ACI attribute is `aci` as shown in the examples that follow.

Example 6.1. ACI: Anonymous Reads and Searches

This works when the only attributes you do not want world-readable are password attributes:

```
aci: (target = "ldap:///dc=example,dc=com")(targetattr !=
  "authPassword || userPassword")(version 3.0;acl "Anonymous read-search access";
  allow (read, search, compare)(userdn = "ldap:///anyone");)
```

Example 6.2. ACI: Disable Anonymous Access

By default OpenDJ denies access unless an access control explicitly allows access.¹ However, OpenDJ also allows anonymous access by default to use some controls, to perform certain extended operations, to view root DSE operational attributes, to view directory schema definitions, to view some other operational attributes, and to perform compare and search operations.

These default capabilities are defined on the `global-aci` property of the access control handler, which you can read by using the **dsconfig get-access-control-handler-prop** command:

¹This does not apply to the directory root user, such as `cn=Directory Manager`, who bypasses ACIs.

```
$ dsconfig \
  get-access-control-handler-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --property global-aci
```

You can disable anonymous access either by editing relevant `global-aci` properties, or by using the global server configuration property, `reject-unauthenticated-requests`. Editing relevant `global-aci` properties lets you take a fine-grained approach to limit anonymous access. Setting `reject-unauthenticated-requests:true` causes OpenDJ directory server to reject all requests from clients who are not authenticated except bind requests and StartTLS requests.

To take a fine-grained approach, use the **dsconfig** command to edit `global-aci` properties. One of the most expedient ways to do this is to use the command interactively on one OpenDJ directory server, capturing the output to a script with the `--commandFilePath script` option, and then editing the script for use on other servers. With this approach, you can allow anonymous read access to the root DSE and to directory schemas so that clients do not have to authenticate to discover server capabilities, and also allow anonymous users access to some controls and extended operations:

```
$ dsconfig \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --commandFilePath /tmp/captured-global-aci-edits.sh

# The dsconfig command runs interactively.

# Edit Access Control Handler, global-aci attributes replacing
# userdn="ldap:///anyone" (anonymous) with userdn="ldap:///all" (authenticated)
# in "Anonymous read access" and "User-Visible Operational Attributes" ACIs.

# To make this change, you first remove the existing values,
# then add the edited values, and finally apply the changes.
```

Make sure that you also set appropriate ACIs on any data that you import.

At this point, clients must authenticate to view search results, for example:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(uid=bjensen)"
$ ldapsearch \
--bindDN uid=bjensen,ou=people,dc=example,dc=com \
--bindPassword hifalutin \
--port 1389 \
--baseDN dc=example,dc=com \
"(uid=bjensen)" cn uid
dn: uid=bjensen,ou=People,dc=example,dc=com
cn: Barbara Jensen
cn: Babs Jensen
uid: bjensen
```

An example of the captured command is the shell script, [captured-global-aci-edits.sh](#).

To reject anonymous access except bind and StartTLS requests, set `reject-unauthenticated-requests:true`:

```
$ dsconfig \
set-global-configuration-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--trustAll \
--no-prompt \
--set reject-unauthenticated-requests:true
```

Once you set the property, anonymous clients trying to search, for example, get an `Unwilling to Perform` response from OpenDJ directory server:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(uid=bjensen)"
SEARCH operation failed
Result Code: 53 (Unwilling to Perform)
Additional Information: Rejecting the requested operation
because the connection has not been authenticated
```

In both cases, notice that the changes apply to a single OpenDJ directory server configuration, and so are not replicated to other servers. You must instead apply the changes separately to each server.

Example 6.3. ACI: Full Access for Administrators

Directory Administrators need privileges as well for full access to administrative operations:

```
aci: (target="ldap:///dc=example,dc=com") (targetattr =
  "*" || +)(version 3.0;acl "Admins can run amok"; allow(
  all, proxy, import, export) groupdn =
  "ldap:///cn=Directory Administrators,ou=Groups,dc=example,dc=com");)
```

targetattr = "*" || +" permits access to all user attributes and all operational attributes. allow(all, proxy, import, export) permits all user operations, proxy authorization, and data import and export operations.

Example 6.4. ACI: Change Your Password

By default this capability is set in a global ACI:

```
aci: (target = "ldap:///ou=People,dc=example,dc=com")(targetattr =
  "authPassword || userPassword")(version 3.0;acl "Allow users to change pass
  words"; allow (write)(userdn = "ldap:///self");)
```

Example 6.5. ACI: Manage Your Group Membership

For some static groups such as carpoolers and social club members, you might choose to let users manage their own memberships:

```
aci: (target = "ldap:///ou=Self Service,ou=Groups,dc=example,dc=com")(
  targetattr = "member")(version 3.0;acl "Self registration"; allow(selfwrite)(
  userdn = "ldap:///uid=*,ou=People,dc=example,dc=com");)
```

Example 6.6. ACI: Manage Self-Service Groups

Let users create and delete self-managed groups:

```
aci: (target = "ldap:///ou=Self Service,ou=Groups,dc=example,dc=com")(
  targattrfilters="add=objectClass:(objectClass=groupOfNames)")(version 3.0;
  acl "All can create self service groups"; allow (add)(userdn= "
  ldap:///uid=*,ou=People,dc=example,dc=com");)
aci: (target = "ldap:///ou=Self Service,ou=Groups,dc=example,dc=com")(version 3
  .0; acl "Owner can delete self service groups"; allow (delete)(userattr= "
  owner#USERDN");)
```

Example 6.7. ACI: Permit Cleartext Access Over Loopback Only

This ACI uses IP address and Security Strength Factor subjects:

```
aci: (target = "ldap:///dc=example,dc=com")(targetattr =
  "**")(version 3.0;acl "Use loopback only for LDAP in the clear"; deny (all)(
  ip != "127.0.0.1" and ssf <= "1");)
```

When you use TLS but have not configured a cipher, ssf is one. Packets are checksummed for integrity checking, but all content is sent in cleartext.

6.5 Viewing Effective Rights

Once you set up a number of ACIs, you might find it difficult to understand by inspection what rights a user actually has to a given entry. The Get Effective Rights control can help.



Note

The control OID, 1.3.6.1.4.1.42.2.27.9.5.2, is not allowed by the default global ACIs.

In this example, Babs Jensen is the owner of a small group of people who are willing to carpool:

```
$ ldapsearch \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword hifalutin \
--baseDN "ou=Self Service,ou=Groups,dc=example,dc=com" \
"cn=*"
dn: cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com
objectClass: groupOfNames
objectClass: top
member: uid=bjensen,ou=People,dc=example,dc=com
description: People who are willing to carpool
owner: uid=bjensen,ou=People,dc=example,dc=com
cn: Carpoolers
```

Performing the same search with the get effective rights control, and asking for the `aclRights` attribute, shows what rights Babs has on the entry:

```
$ ldapsearch \
--control effectiveRights \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword hifalutin \
--baseDN "ou=Self Service,ou=Groups,dc=example,dc=com" \
"cn=*" \
aclRights
dn: cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com
aclRights;entryLevel: add:0,delete:1,read:1,write:0,proxy:0
```

When you request the `aclRightsInfo` attribute, the server responds with information about the ACIs applied:

```
$ ldapsearch \
--control effectiveRights \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword hifalutin \
--baseDN "ou=Self Service,ou=Groups,dc=example,dc=com" \
"cn=*" \
aclRights \
aclRightsInfo
dn: cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com
aclRightsInfo;logs;entryLevel;read: acl_summary(main): access allowed(read) on e
ntry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, objectClas
s) to (uid=bjensen,ou=People,dc=example,dc=com) (not proxied) ( reason: evaluat
ed allow , deciding_aci: Anonymous read-search access)
aclRightsInfo;logs;entryLevel;write: acl_summary(main): access not allowed(write
) on entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL
) to (uid=bjensen,ou=People,dc=example,dc=com) (not proxied) ( reason: no acis
matched the subject )
aclRightsInfo;logs;entryLevel;add: acl_summary(main): access not allowed(add) on
entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL) to
(uid=bjensen,ou=People,dc=example,dc=com) (not proxied) ( reason: no acis matc
hed the subject )
aclRightsInfo;logs;entryLevel;delete: acl_summary(main): access allowed(delete)
on entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL)
to (uid=bjensen,ou=People,dc=example,dc=com) (not proxied) ( reason: evaluated
allow , deciding_aci: Owner can delete self service groups)
aclRights;entryLevel: add:0,delete:1,read:1,write:0,proxy:0
aclRightsInfo;logs;entryLevel;proxy: acl_summary(main): access not allowed(proxy
) on entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL
) to (uid=bjensen,ou=People,dc=example,dc=com) (not proxied) ( reason: no acis
matched the subject )
```

You can also request the effective rights for another user by using the `--getEffectiveRightsAuthzid` (short form: `-g`) option, which takes the authorization identity of the other user as an argument. The following example shows Directory Manager checking anonymous user rights to the same entry. Notice that the authorization identity for an anonymous user is expressed as `dn::`:


```
$ ldapsearch \
--getEffectiveRightsAuthzid "dn:" \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--baseDN "ou=Self Service,ou=groups,dc=example,dc=com" \
"cn=" aclRightsInfo
dn: cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com
aclRightsInfo;logs;entryLevel;read: acl_summary(main): access allowed(read) on e
ntry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, objectClas
s) to (anonymous) (not proxied) ( reason: evaluated allow , deciding_aci: Anony
mous read-search access)
aclRightsInfo;logs;entryLevel;write: acl_summary(main): access not allowed(write
) on entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL
) to (anonymous) (not proxied) ( reason: no acis matched the subject )
aclRightsInfo;logs;entryLevel;add: acl_summary(main): access not allowed(add) on
entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL) to
(anonymous) (not proxied) ( reason: no acis matched the subject )
aclRightsInfo;logs;entryLevel;delete: acl_summary(main): access not allowed(dele
te) on entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NU
LL) to (anonymous) (not proxied) ( reason: no acis matched the subject )
aclRightsInfo;logs;entryLevel;proxy: acl_summary(main): access not allowed(proxy
) on entry/attr(cn=Carpoolers,ou=Self Service,ou=Groups,dc=example,dc=com, NULL
) to (anonymous) (not proxied) ( reason: no acis matched the subject )
```

When you need to check access to an attribute that might not yet exist on the entry, use the `--getEffectiveRightsAttribute` (short form: `-e`) option, which takes an attribute list as an argument. The following example shows Directory Manager checking anonymous user access to the description attribute for the Self Service groups organizational unit entry. The description attribute is not yet in the entry:

```
$ ldapsearch \
--port 1389 \
--baseDN "ou=Self Service,ou=groups,dc=example,dc=com" \
"ou=Self Service" description
dn: ou=Self Service,ou=Groups,dc=example,dc=com

$ ldapsearch \
--getEffectiveRightsAuthzid "dn:" \
--getEffectiveRightsAttribute description \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--baseDN "ou=Self Service,ou=groups,dc=example,dc=com" \
"ou=Self Service" aclRights
dn: ou=Self Service,ou=Groups,dc=example,dc=com
aclRights;attributeLevel;description: search:1,read:1,compare:1,write:0,selfwrit
e_add:0,selfwrite_delete:0,proxy:0
aclRights;entryLevel: add:0,delete:0,read:1,write:0,proxy:0
```

Chapter 7

Indexing Attribute Values

This chapter covers OpenDJ indexing features used to speed up searches, and to limit the impact of searches on directory server resources. In this chapter you will learn to:

- Determine which attributes to index and what types of indexes to configure
- Configure, build, and rebuild indexes
- Check that indexes are valid

When a client requests a directory search operation, the client sends the server a filter expression such as `(&(uid=*jensen*)(l=Stavanger))`. The server then uses applicable indexes to find entries with attribute values likely to match the search. If no indexes are applicable, then the server potentially has to go through all entries to look for candidate matches.

Looking through all entries is resource-intensive for large directories. For this reason, the `unindexed-search` privilege, which lets users request searches that have no applicable index, is reserved for the directory root user by default.

Rather than granting the `unindexed-search` privilege to more users and client applications, you configure indexes to correspond to the searches that clients need to perform. See [Section 7.2, "What To Index"](#) for details.

7.1 Index Types and Their Functions

OpenDJ provides several different index types, each corresponding to a different type of search.

7.1.1 Approximate Index

An approximate index is used to match values that "sound like" those provided in the filter. An approximate index on `cn` lets clients find people even when they misspell names, as in the following example:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(cn~=Babs Jansen)" cn
dn: uid=bjensen,ou=People,dc=example,dc=com
cn: Barbara Jensen
cn: Babs Jensen
```

7.1.2 Equality Index

An equality index is used to match values that correspond exactly (though generally without case sensitivity) to the value provided in the search filter. An equality index requires clients to match values without wildcards or misspellings:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(uid=bjensen)" mail
dn: uid=bjensen,ou=People,dc=example,dc=com
mail: bjensen@example.com
```

7.1.3 Ordering Index

An ordering index is used to match values for a filter that specifies a range. The `ds-sync-hist` has an ordering index by default because searches on that attribute often seek entries with changes more recent than the last time a search was performed.

The following example shows a search that specifies ranges:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com \  
"(&(uidNumber>=1120)(roomNumber>=4500))" uid  
dn: uid=charvey,ou=People,dc=example,dc=com  
uid: charvey  
  
dn: uid=eward,ou=People,dc=example,dc=com  
uid: eward  
  
dn: uid=mvaughan,ou=People,dc=example,dc=com  
uid: mvaughan  
  
dn: uid=pchassin,ou=People,dc=example,dc=com  
uid: pchassin
```

7.1.4 Presence Index

A presence index is used to match an attribute that is present on the entry, regardless of the value. The aci attribute is indexed for presence by default to allow quick retrieval of entries with ACIs:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(aci=*)" -  
dn: dc=example,dc=com  
  
dn: ou=People,dc=example,dc=com
```

7.1.5 Substring Index

A substring index is used to match values specified with wildcards in the filter. Substring indexes can be expensive to maintain, especially for large attribute values:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(cn=Barb*)" cn  
dn: uid=bfrancis,ou=People,dc=example,dc=com  
cn: Barbara Francis  
  
dn: uid=bhal2,ou=People,dc=example,dc=com  
cn: Barbara Hall  
  
dn: uid=bjablons,ou=People,dc=example,dc=com  
cn: Barbara Jablonski  
  
dn: uid=bjensen,ou=People,dc=example,dc=com  
cn: Barbara Jensen  
cn: Babs Jensen  
  
dn: uid=bmaddox,ou=People,dc=example,dc=com  
cn: Barbara Maddox
```

7.1.6 Virtual List View (Browsing) Index

A virtual list view (VLV) or browsing index is designed to help the server respond to client applications that need virtual list view results, for example, to browse through a long list in a GUI. They also help the server respond to clients that request server-side sorting of the search results.

VLV indexes correspond to particular searches. Configure your VLV indexes using the control panel, and copy the command-line equivalent from the Details pane for the operation, if necessary.

7.1.7 Extensible Matching Rule Index

In some cases you need an index for a matching rule other than those described above. For example, OpenDJ supports generalized time-based matching so applications can search for all times later than, or earlier than a specified time.

7.2 What To Index

OpenDJ search performance depends on indexes. As mentioned above, unindexed searches are so resource-intensive that by default OpenDJ refuses to perform unindexed searches. The reason for this is that OpenDJ has to scan the entire directory in order to find candidate matches for an unindexed search. Most searches should therefore use indexes.

A simple way of checking the indexes that match a search is to request the `debugsearchindex` attribute in your results:

```
$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
"(uid=user.1000)" \
debugsearchindex
dn: cn=debugsearch
debugsearchindex: filter=(uid=user.1000)[INDEX:uid.equality][COUNT:1] final=[COU
NT:1]
```

When you request the `debugsearchindex` attribute, instead of performing the search, OpenDJ returns debug information indicating how it would process the search operation. In the example above you notice OpenDJ hits the equality index for `uid` right away.

A less exact search requires more work from OpenDJ. In the following example OpenDJ would have to return over 10,000 entries:

```
$ ldapsearch \  
--port 1389 \  
--baseDN dc=example,dc=com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
"(uid=*)" \  
debugsearchindex  
dn: cn=debugsearch  
debugsearchindex: filter=(uid=*)[NOT-INDEXED] scope=sub[LIMIT-EXCEEDED:10002]  
final=[NOT-INDEXED]
```

About debugsearchindex Values

The values of the debugsearchindex attribute show you how OpenDJ directory server uses search filters and scope to determine the results of the search. In general, the debugsearchindex attribute has the form: (filter|vlv)=*filter-with-info*(scope=*scope-idscope-info*) final=*final-info*.

If a normal filter applies, the value starts with filter=. If the search operation parameters have an associated VLV index, the value starts with vlv=. A scope component provides information about how the scope affected the results. The final component provides information about the overall result.

filter-with-info

This field looks like a string representation of the LDAP filter with extra information after the closing parenthesis of each simple filter component.

For a VLV index, only the extra information is shown:

The extra information takes the form: ([INDEX:*index-id*])([COUNT:*entry-count*]|[LIMIT-EXCEEDED]|[NOT-INDEXED]), where:

- [INDEX:*index-id*] identifies the index that could be used to find matches for this filter.
- [COUNT:*entry-count*] specifies the number of entries found to match the filter.
- [LIMIT-EXCEEDED] indicates the server maintains a matching index, but the index entry limit was exceeded for the value specified.
- [NOT-INDEXED] indicates no matching index value or index key was found.

For example, the debugsearchindex attribute value excerpt filter=(amp(objectClass=person)[INDEX:objectClass.equality] [LIMIT-EXCEEDED](cn=*a*) [INDEX:cn.substring][NOT-INDEXED])[NOT-INDEXED] provides information about how OpenDJ evaluates the complex filter (&(objectClass=person)(cn=*a*)). The filter component (objectClass=person) does correspond to the equality index for objectClass, but there are so many entries matching

objectClass=person that the server has stopped maintaining index entries for that value. The filter component cn=*a* did not match an index, as might be expected for such a short substring. No matching index was found for the whole complex filter.

scope-id

The scope can be one of base, one, sub, or subordinate.

scope-info

This field is similar to the extra information for filter components:

- [COUNT:entry-count] specifies the number of entries found in the scope.
- [LIMIT-EXCEEDED:entry-count] indicates the scope did not prevent the search from exceeding the resource limit that caps the number of entries a search can return.

For example, the debugsearchindex attribute value excerpt scope=sub[LIMIT-EXCEEDED:10002] indicates that the number of matches in the subtree scope that exceeded the resource limit capping how many entries a search can return.

final-info

This field shows at a glance whether the search was indexed:

- [COUNT:entry-count] specifies the number of entries found, and indicates that the search was indexed.
- [NOT-INDEXED] indicates that the search was unindexed.

By default OpenDJ rejects unindexed searches when the number of candidate entries goes beyond the search or look-through limit:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com "(uid=*)"
SEARCH operation failed
Result Code: 50 (Insufficient Access Rights)
Additional Information: You do not have sufficient privileges to perform
an unindexed search
```

When an unindexed search is performed, it shows up in the access log with the unindexed label:

```
...SEARCH RES ... result=50 message="You do not have sufficient privileges
to perform an unindexed search" nentries=0 unindexed etime=1
```


If directory users tell you their client applications are getting this error, then you can work with them either to help them make their search filter specific enough to use existing indexes, or to index attributes they need indexed in order to perform their searches. For example, if a directory client application is having trouble performing a search with a filters such as `(objectClass=person)`, you can help them make sure their search filter is specific enough, such as `(&(mail=username@maildomain.net)(objectClass=person))`, so that the server can use an index. In the example, the search relies on the equality index for mail, to limit the number of candidate entries to check for matches.

You can view and edit what is indexed through OpenDJ control panel, Indexes > Manage Indexes. Alternatively you can manage indexes using the command-line tools demonstrated in [Section 7.3, "Configuring and Rebuilding Indexes"](#). If an index already exists, but you suspect it is not working properly, see [Section 7.4, "Verifying Indexes"](#), too.

If you must allow some applications to perform unindexed searches, because they need to retrieve very large numbers of entries, for example, then you can assign them the unindexed-search privilege. See [Section 6.3, "Configuring Privileges"](#) for details. A successful unindexed search also shows up in the access log with the label unindexed, usually with a large etime as well:

```
...SEARCH RES conn=11 op=1 msgID=2 result=0 nentries=10000 unindexed etime=1129
```

There is a trade off between the cost of maintaining an index and the value the index has in speeding up searches. Although monitoring index use is not something to leave active in production due to the additional cost and memory needed to maintain the statistics, in a test environment you can activate index analysis using the **dsconfig set-backend-prop** command:

```
$ dsconfig \
  set-backend-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --set index-filter-analyzer-enabled:true \
  --no-prompt \
  --trustAll
```

The command causes OpenDJ to analyze filters used and keep the results in memory, so that you can read them through the `cn=monitor` interface:

```
$ ldapsearch \  
--port 1389 \  
--baseDN "cn=userRoot Database Environment,cn=monitor" \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
"(objectclass=*)" \  
filter-use  
dn: cn=userRoot Database Environment,cn=monitor  
filter-use: (mail=aa@maildomain.net) hits:1 maxmatches:0 message:  
filter-use: (objectClass=*) hits:1 maxmatches:-1 message:presence index type is  
disabled for the objectClass attribute  
filter-use: (uid=user.1000) hits:2 maxmatches:1 message:  
filter-use: (uid=user.1001) hits:1 maxmatches:1 message:  
filter-use: (cn=aa*) hits:1 maxmatches:10 message:  
filter-use: (cn=b*) hits:1 maxmatches:834 message:
```

The filter-use values are the filter, the hits (number of times the filter was used), the maxmatches (number of matches found), and an optional message.

You can turn off index analysis with the **dsconfig set-backend-prop** command as well:

```
$ dsconfig \  
set-backend-prop \  
--port 4444 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--backend-name userRoot \  
--set index-filter-analyzer-enabled:false \  
--no-prompt \  
--trustAll
```

7.3 Configuring and Rebuilding Indexes

You modify index configurations by using the **dsconfig** command. The subcommands to use depend on the backend type, as shown in the examples that follow. The configuration changes then take effect after you rebuild the index according to the new configuration, using the **rebuild-index** command. The **dsconfig --help-database** command lists subcommands for creating, reading, updating, and deleting index configuration.



Tip

Indexes are per directory backend rather than per suffix. To maintain separate indexes for different suffixes on the same directory server, put the suffixes in different backends.

7.3.1 Configuring a Standard Index

You can configure standard indexes from the control panel, and also on the command-line using the **dsconfig** command. After you finish configuring the index, you must rebuild the index for the changes to take effect.

Example 7.1. Create a New Index

The following example creates a new equality index for the `cn` (common name) attribute in a backend of type `pdb` named `myData`:

```
$ dsconfig \
  create-backend-index \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name myData \
  --index-name cn \
  --set index-type:equality \
  --trustAll \
  --no-prompt
```

Example 7.2. Configure an Approximate Index

The following example configures an approximate index for the `cn` (common name) attribute in a backend of type `pdb` named `myData`:

```
$ dsconfig \
  set-backend-index-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name myData \
  --index-name cn \
  --set index-type:approximate \
  --trustAll \
  --no-prompt
```

Example 7.3. Configure an Extensible Match Index

The OpenDJ control panel New Index window does not help you set up extensible matching rule indexes. Use the **dsconfig** command instead.

The following example configures an extensible matching rule index for "later than" and "earlier than" generalized time matching on a `lastLoginTime` attribute in a backend of type `pdb` named `myData`:

```
$ dsconfig \
  create-backend-index \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name myData \
  --set index-type:extensible \
  --set index-extensible-matching-rule:1.3.6.1.4.1.26027.1.4.5 \
  --set index-extensible-matching-rule:1.3.6.1.4.1.26027.1.4.6 \
  --index-name lastLoginTime \
  --trustAll \
  --no-prompt
```

7.3.2 Configuring a Virtual List View Index

In the OpenDJ control panel, select `Manage Indexes > New VLV Index`, and then set up your VLV index using the New VLV Index window as shown in [Figure 7.1](#), "New VLV Index Window".

Figure 7.1. New VLV Index Window

The screenshot shows the 'OpenDJ Control Panel - New VLV Index' window. It contains the following fields and controls:

- Name:** A text field containing 'people-by-last-name'.
- Backend:** A text field containing 'userRoot'.
- Base DN:** A text field containing 'Other:' with a dropdown arrow, and a text field containing 'ou=People,dc=example,dc=com'. Below this is a hint: 'For example: dc=subtree,dc=example,dc=com'.
- Search Scope:** Four radio buttons: 'Base Object', 'Single Level' (selected), 'Subordinate Subtree', and 'Whole Subtree'.
- Filter:** A text field containing '(&(givenName=*)(sn=*))'. Below this is a hint: 'For example: (&(cn=*)(sn=*))'.
- Sort Order:** A text field containing 'gidNumber' with a dropdown arrow, and a text field containing '(ascending)' with a dropdown arrow.
- Buttons:** 'Add', 'Move Up', 'Move Down', 'Remove', 'OK', and 'Cancel'.
- List:** A list box containing two entries: 'sn (ascending)' (highlighted) and 'givenName (ascending)'.

After you finish configuring your index and click OK, the Control Panel prompts you to make the additional changes necessary to complete the VLV index configuration, and then to build the index.

You can also create the equivalent index configuration by using the **dsconfig** command.

The following example shows how to create the VLV index for a backend of type `pdb` named `myData`:

```
$ dsconfig \
  create-backend-vlv-index \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDn "cn=Directory Manager" \
  --bindPassword password \
  --backend-name myData \
  --index-name people-by-last-name \
  --set base-dn:ou=People,dc=example,dc=com \
  --set filter:"(|(givenName=*)(sn=*))" \
  --set scope:single-level \
  --set sort-order:"+sn +givenName" \
  --trustAll \
  --no-prompt
```



Note

When referring to a VLV index after creation, you must add `vlv.` as a prefix. In other words, if you named the VLV index `people-by-last-name`, you refer to it as `vlv.people-by-last-name` when rebuilding indexes, changing index properties such as the index entry limit, or verifying indexes.

7.3.3 Rebuilding Indexes

After you change an index configuration, or when you find that an index is corrupt, you can rebuild the index. When you rebuild indexes, you specify the base DN of the data to index, and either the list of indexes to rebuild or `--rebuildAll`. You can rebuild indexes while the server is offline, or while the server is online. If you rebuild the index while the server is online, then you must schedule the rebuild process as a task.

Example 7.4. Rebuild Index

The following example rebuilds the `cn` index immediately with the server online:

```
$ rebuild-index \  
--port 4444 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--baseDN dc=example,dc=com \  
--index cn \  
--start 0 \  
--trustAll  
Rebuild Index task 20150219181540575 scheduled to start Feb 19, 2015 6:15:40
```

Example 7.5. Rebuild Degraded Indexes

The following example rebuilds degraded indexes immediately with the server online:

```
$ rebuild-index \  
--port 4444 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--baseDN dc=example,dc=com \  
--rebuildDegraded  
...  
..message="Due to changes in the configuration,  
index dc=com,dc=example_description is currently operating in a degraded state  
and must be rebuilt before it can be used"  
..message="Rebuild of all degraded indexes started  
with 177 total entries to process"  
..."Rebuild complete. Processed 177 entries in 0 seconds  
(average rate 3160.7/sec)"  
...  
Rebuild Index task 20151031164835613 has been successfully completed
```

Example 7.6. Clear New, Unused, Degraded Indexes

When you add a new attribute as described in [Section 14.2, "Updating Directory Schema"](#), and then create indexes for the new attribute, the new indexes appear as degraded, even though the attribute has not yet been used, and so indexes are sure to be empty, rather than degraded.

In this special case, you can safely use the **rebuild-index --clearDegradedState** command to avoid having to scan the entire directory backend before rebuilding the new, unused index. In this example, an index has just been created for newUnusedAttribute.

Before using the **rebuild-index** command, test the index status to make sure that the index has not yet been used: by using the **backendstat** command, described in backendstat(1) in the *OpenDJ Reference*.

OpenDJ directory server must be stopped before you use the **backendstat** command:

```
$ stop-ds
```

The third column of the output is the Index Valid column, which is false before the rebuild, true after:

```
$ backendstat show-index-status --backendID userRoot --baseDN dc=example,dc=com \  
| grep newunusedattribute  
newunusedattribute.presence           ...           false ...  
newunusedattribute.caseIgnoreMatch    ...           false ...  
newunusedattribute.caseIgnoreSubstringsMatch:6 ...       false ...
```

Update the index information to fix the value of the unused index:

```
$ rebuild-index --baseDN dc=example,dc=com --clearDegradedState \  
--index newUnusedAttribute
```

Check that the Index Valid column for the index status is now set to true:

```
$ backendstat show-index-status --backendID userRoot --baseDN dc=example,dc=com \  
| grep newunusedattribute  
newunusedattribute.presence           ...           true ...  
newunusedattribute.caseIgnoreMatch    ...           true ...  
newunusedattribute.caseIgnoreSubstringsMatch:6 ...       true ...
```

Start OpenDJ directory server:

```
$ start-ds
```

If the newly indexed attribute has already been used, rebuild the index instead of clearing the degraded state.

7.3.4 Changing Index Entry Limits

As the number of entries in your directory grows, it can make sense not to maintain indexes for particular values. For example, every entry in the directory has the value `top` for the `objectClass` attribute, so maintaining a list of entries that match the filter `(objectClass=top)` is not a reasonable use of resources.

In a very, very large directory, the same can be true for (givenName=John) and (sn=Smith).

In an index, each index key points to a list of entries that are candidates to match. For the objectClass index key that corresponds to =top, the list of entries can include every entry in the directory.

OpenDJ directory server therefore defines an index entry limit. When the number of entries that an index key points to exceeds the index entry limit, OpenDJ stops maintaining the list of entries for that index key.

The default index entry limit value is 4000. 4000 is intended to be large enough for most index keys, though it prevents OpenDJ from maintaining indexes at any cost.

Evaluate how well attributes are indexed, and consider whether to change the index entry limit.

The following examples describe how to interpret information about indexes. In this case, the directory server holds 10,000 user entries. The settings for this directory server are reasonable.

Use the **backendstat show-index-status** command, described in backendstat(1) in the *OpenDJ Reference*.

OpenDJ directory server must be stopped before you use the **backendstat** command:

```
$ stop-ds
```

Non-zero values in the Over Entry Limit column of the output table indicate the number of index keys that have reached the limit and are no longer maintained. The keys that are over the limit are then listed below the table:

```
$ backendstat show-index-status --backendID userRoot --baseDN dc=example,dc=com
```

Index Name	Raw DB Name	Index Valid	Record Count	Over Entry Limit	95%	90%
uniqueMember.uniqueMemberMatch	...uniqueMember.uniqueMemberMatch	true	0	0	0	0
mail.caseIgnoreIA5Match	...mail.caseIgnoreIA5Match	true	10000	0	0	0
mail.caseIgnoreIA5SubstringsMatch:6	...mail.caseIgnoreIA5SubstringsMatch:6	true	31235	15	0	0
telephoneNumber...	...telephoneNumber...	true	73235	0	0	0
telephoneNumber.telephoneNumberMatch	...telephoneNumber.telephoneNumberMatch	true	10000	0	0	0
aci.presence	...aci.presence	true	0	0	0	0
ds-sync-hist...	...ds-sync-hist...	true	0	0	0	0
cn.caseIgnoreMatch	...cn.caseIgnoreMatch	true	10000	0	0	0
cn.caseIgnoreSubstringsMatch:6	...cn.caseIgnoreSubstringsMatch:6	true	86040	0	0	0
objectClass.objectIdentifierMatch	...objectClass.objectIdentifierMatch	true	6	4	0	0
entryUUID.uuidMatch	...entryUUID.uuidMatch	true	10002	0	0	0
uid.caseIgnoreMatch	...uid.caseIgnoreMatch	true	10000	0	0	0
givenName.caseIgnoreMatch	...givenName.caseIgnoreMatch	true	8605	0	0	0
givenName.caseIgnoreSubstringsMatch:6	...givenName.caseIgnoreSubstringsMatch:6	true	19629	0	0	0
member.distinguishedNameMatch	...member.distinguishedNameMatch	true	0	0	0	0
sn.caseIgnoreMatch	...sn.caseIgnoreMatch	true	10000	0	0	0
sn.caseIgnoreSubstringsMatch:6	...sn.caseIgnoreSubstringsMatch:6	true	32217	0	0	0
ds-sync-conflict...	...ds-sync-conflict...	true	0	0	0	0

Total: 18

Index: /dc=com,dc=example/objectClass.objectIdentifierMatch
Over index-entry-limit keys: [2.5.6.0] [2.5.6.6] [2.5.6.7] [inetorgperson]

Index: /dc=com,dc=example/mail.caseIgnoreIA5SubstringsMatch:6
Over index-entry-limit keys: [.net] [@maild] [aildom] [ain.ne] [domain] [et] [ildoma] [in.net] [ldomai] [maildo] [main.n] [n.net] [ne] [omain.] [t]

Every user entry has the object classes listed, and every user entry has an email address ending in @maildomain.net, so those values are not specific enough to be used in search filters. The ds-sync-hist and ds-sync-conflict indexes are for OpenDJ's internal use.

Start OpenDJ directory server:

```
$ start-ds
```

If you do find the limit is too low for a certain key, you can change the index entry limit on a per-index basis.

Example 7.7. Change Index Entry Limit

The following example changes the index entry limit for the objectClass index, and then rebuilds the index for the configuration change to take effect. The example is contrived, but the steps are the same for any other index.



Important

Changing the index entry limit significantly can result in serious performance degradation. Be prepared to test performance thoroughly before you roll out an index entry limit change in production.

The following example shows how to use the **dsconfig set-backend-index-prop** command to change the index entry limit for a backend of type pdb:

```
$ dsconfig \
  set-backend-index-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --index-name objectClass \
  --set index-entry-limit:5000 \
  --trustAll \
  --no-prompt

$ rebuild-index \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --baseDN dc=example,dc=com \
  --index objectClass \
  --start 0
Rebuild Index task 20150520135018932 scheduled to start May 20, 2015 1:50:18 PM
```

Alternatively, you can configure the index entry limit for all indexes stored in a backend by using the **dsconfig set-backend-prop** command with the `--backend-name backendName --set index-entry-limit:limitValue` options.

7.4 Verifying Indexes

You can verify that indexes correspond to current directory data, and that indexes do not contain errors by using the **verify-index** command, described in `verify-index(1)` in the *OpenDJ Reference*.

Example 7.8. Verify Index

The following example verifies the `cn` (common name) index for completeness and for errors:

```
$ verify-index \
--baseDN dc=example,dc=com \
--index cn \
--clean \
--countErrors
...msg=Checked 1316 records and found 0 error(s) in 0 seconds
(average rate 2506.7/sec)
...msg=Number of records referencing more than one entry: 315
...msg=Number of records that exceed the entry limit: 0
...msg=Average number of entries referenced is 1.58/record
...msg=Maximum number of entries referenced by any record is 32
```

Ignore the messages regarding lock tables and cleaner threads. The important information is whether any errors are found in the indexes.

7.5 Default Indexes

When you first install OpenDJ directory server and import your data from LDIF, the following indexes are configured.

Table 7.1. Default Indexes

Index	Approx.	Equality	Ordering	Presence	Substring	Entry Limit
aci	-	-	-	Yes	-	4000
cn	-	Yes	-	-	Yes	4000
dn2id	Non-configurable internal index					
ds-sync-conflict	-	Yes	-	-	-	4000
ds-sync-hist	-	-	Yes	-	-	4000
entryUUID	-	Yes	-	-	-	4000
givenName	-	Yes	-	-	Yes	4000
id2children	Non-configurable internal index					
id2subtree	Non-configurable internal index					
mail	-	Yes	-	-	Yes	4000

Index	Approx.	Equality	Ordering	Presence	Substring	Entry Limit
member	-	Yes	-	-	-	4000
objectClass	-	Yes	-	-	-	4000
sn	-	Yes	-	-	Yes	4000
telephone-Number	-	Yes	-	-	Yes	4000
uid	-	Yes	-	-	-	4000
unique-Member	-	Yes	-	-	-	4000

When you create a new backend using the **dsconfig** command, OpenDJ directory server creates the following indexes automatically:

aci presence
ds-sync-conflict equality
ds-sync-hist ordering
entryUUID equality
objectClass equality

You can create additional indexes as described in [Section 7.3, “Configuring and Rebuilding Indexes”](#).

Chapter 8

Managing Data Replication

OpenDJ uses advanced data replication with automated conflict resolution to help ensure your directory services remain available during administrative operations that take an individual server offline, or in the event a server crashes or a network goes down. This chapter explains how to manage OpenDJ directory data replication. In this chapter you will learn to:

- Set up replication as part of initial installation using OpenDJ control panel, or at any time using command-line tools
- Understand how replication operates in order to configure it appropriately
- Enable, initialize, and stop data replication
- Configure standalone directory servers and replication servers, or break a server that plays both roles into two standalone servers
- Configure replication groups, read-only replicas, assured replication, subtree replication, and fractional replication for complex deployments
- Configure and use change notification to synchronize external applications with changes to directory data
- Recover from situations where a user error has been applied to all replicas

8.1 Replication Quick Setup

You can set up replication during installation by using the setup wizard, starting with the Topology Options screen:

- In the Topology Options screen for the first server you set up, select This server will be part of a replication topology.

If you also choose Configure as Secure, then replication traffic is protected by Transport Layer Security.

- In the Topology Options screen for subsequent servers, select There is already a server in the topology.

Provide the Host Name, Administration Connector Port number, global Admin User identifier, and Admin Password for the first server.

- When presented with the Create Global Administrator screen, provide a Global Administrator ID and Global Administrator Password.

The Global Administrator account exists on all servers in the replication topology. The account is stored under `cn=admin` data. It provides an account to administer replication with the same credentials on every server in the topology.

- In the Data Replication screen, select the user and application data base DN(s) to replicate.

OpenDJ directory server automatically replicates configuration data and directory schema.

Once replication is set up, it works for all the replicas. You can monitor replication status through OpenDJ control panel.

8.2 About Replication

Before you take replication further than setting up replication in the setup wizard, read this section to learn more about how OpenDJ replication works.

8.2.1 Replication Defined

Replication is the process of copying updates between OpenDJ directory servers such that all servers converge on identical copies of directory data. Replication is designed to let convergence happen over time by default.¹ Letting convergence

¹Assured replication can require, however, that the convergence happen before the client application is notified that the operation was successful.

happen over time means that different replicas can be momentarily out of sync, but it also means that if you lose an individual server or even an entire data center, your directory service can keep on running, and then get back in sync when the servers are restarted or the network is repaired.

Replication is specific to the OpenDJ directory service. Replication uses a specific protocol that replays update operations quickly, storing enough historical information about the updates to resolve most conflicts automatically. For example, if two client applications separately update a user entry to change the phone number, replication can identify the latest change, and apply it across servers. The historical information needed to resolve these issues is periodically purged to avoid becoming too large. As a directory administrator, you must ensure that you do not purge the historical information more often than you back up your directory data.

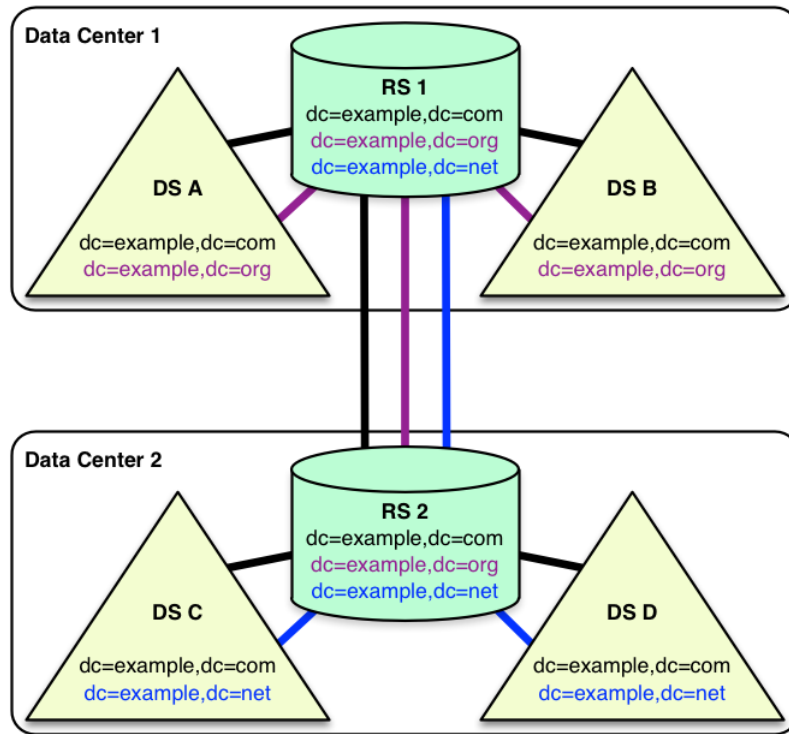
Keep server clocks synchronized for your topology. You can use NTP for example. Keeping server clocks synchronized helps prevent issues with SSL connections and with replication itself. Keeping server clocks synchronized also makes it easier to compare timestamps from multiple servers.

8.2.2 Replication Per Suffix

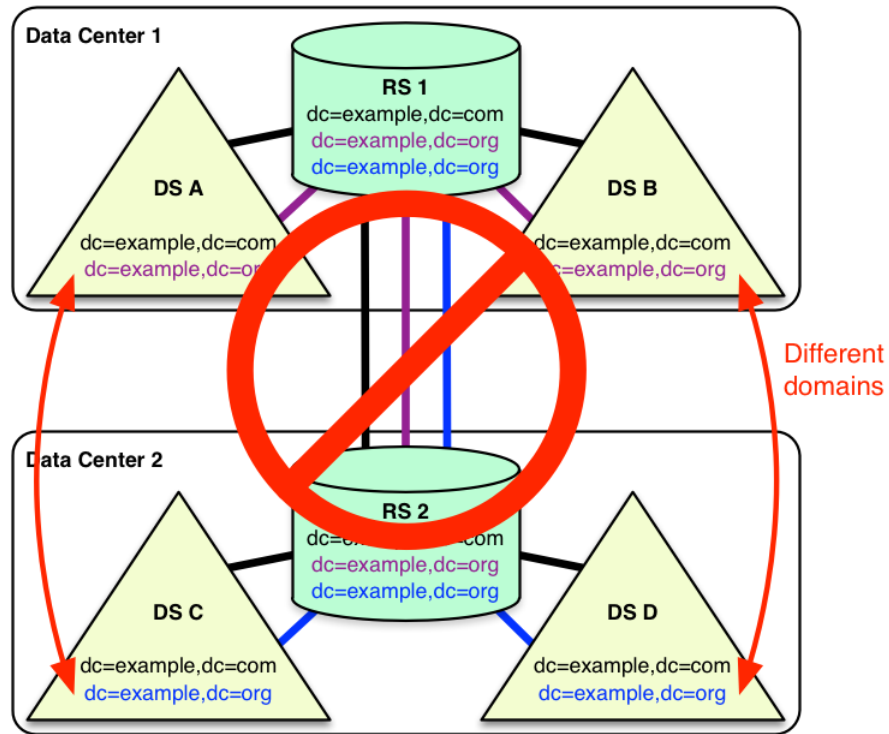
The primary unit of replication is the suffix, specified by a base DN such as `dc=example,dc=com`.² Replication also depends on the directory schema, defined on `cn=schema`, and the `cn=admin` data suffix with administrative identities and certificates for protecting communications. Thus that content gets replicated as well.

The set of OpenDJ servers replicating data for a given suffix is called a replication topology. You can have more than one replication topology. For example, one topology could be devoted to `dc=example,dc=com`, and another to `dc=example,dc=org`. OpenDJ servers serve more than one suffix, and participate in more than one replication topology.

²When you configure partial and fractional replication, however, you can replicate only part of a suffix, or only certain attributes on entries. Also, if you split your suffix across multiple backends, then you need to set up replication separately for each part of suffix in a different backend.



Within a replication topology, the suffixes being replicated are identified to the replication servers by their DNs. All the replication servers are fully connected in a topology. Consequently it is impossible to have multiple separate, independent topologies for data under the same DN within the overall set of servers. This is illustrated in the following diagram.



8.2.3 Replication Connection Selection

In order to understand what happens when individual servers stop responding due to a network partition or a crash, know that OpenDJ can offer both directory service and also replication service, and the two services are not the same, even if they can run alongside each other in the same OpenDJ server in the same Java Virtual Machine.

Replication relies on the replication service provided by OpenDJ replication servers, where OpenDJ directory servers publish changes made to their data, and subscribe to changes published by other OpenDJ directory servers. A replication server manages replication data only, handling replication traffic with directory servers and with other replication servers, receiving, sending, and storing only changes to directory data rather than directory data itself. Once a replication server is connected to a replication topology, it maintains connections to all other replication servers in that topology.

A directory server handles directory data. It responds to requests, stores directory data and historical information. For each replicated suffix, such as `dc=example,dc=com`, `cn=schema` and `cn=admin` data, the directory server publishes changes to a replication server, and subscribes to changes from that replication server. (Directory servers do not publish changes to other directory servers.) A directory server also resolves any conflicts that arise when reconciling changes from other directory servers, using the historical information about changes to resolve the conflicts. (Conflict resolution is the responsibility of the directory server rather than the replication server.)

Once a directory server is connected to a replication topology for a particular suffix, it connects to one replication server at a time for that suffix. The replication server provides the directory server with a list of all replication servers for that suffix. Given the list of possible replication servers to which it can connect, the directory server can determine which replication server to connect to when starting up, or when the current connection is lost or becomes unresponsive.

For each replicated suffix, a directory server prefers to connect to a replication server:

1. In the same group as the directory server
2. Had the same initial data for the suffix as the directory server
3. If initial data was the same, has all the latest changes from the directory server
4. Runs in the same Java Virtual Machine as the directory server
5. Has the most available capacity relative to other eligible replication servers

Available capacity depends on how many directory servers in the topology are already connected to a replication server, and what proportion of all directory servers in the topology ought to be connected to the replication server.

To determine what proportion of the total number of directory servers should be connected to a replication server, OpenDJ uses replication server weight. When configuring a replication server, you can assign it a weight (default: 1). The weight property takes an integer that indicates capacity to provide replication service relative to other servers. For example, a weight of 2 would indicate a replication server that can handle twice as many connected servers as a replication server with weight 1.

The proportion of directory servers in a topology that should be connected to a given replication server is equal to $(\text{replication server weight}) / (\text{sum of replication server weights})$. In other words, if there are four replication servers in a topology each with default weights, the proportion for each replication server is $1/4$.

Consider a situation where seven directory servers are connected to replication servers A, B, C, and D for `dc=example,dc=com` data. Suppose two directory servers each are connected to A, B, and C, and once directory server is connected to replication server D. Replication server D is therefore the server with the most available capacity relative to other replication servers in the topology. All other criteria being equal, replication server D is the server to connect to when an eighth directory server joins the topology.

The directory server regularly updates the list of replication servers in case it must reconnect. As available capacity of replication servers for each replication topology can change dynamically, a directory server can potentially reconnect to another replication server to balance the replication load in the topology. For this reason the server can also end up connected to different replication servers for different suffixes.

8.3 Configuring Replication

This section shows how to configure replication with command-line tools, such as the **dsreplication** command, described in `dsreplication(1)` in the *OpenDJ Reference*.

8.3.1 Enabling Replication

You can start the replication process by using the **dsreplication enable** command:

```
$ dsreplication \  
enable \  
--adminUID admin \  
--adminPassword password \  
--baseDN dc=example,dc=com \  
--host1 opendj.example.com \  
--port1 4444 \  
--bindDN1 "cn=Directory Manager" \  
--bindPassword1 password \  
--replicationPort1 8989 \  
--host2 opendj2.example.com \  
--port2 4444 \  
--bindDN2 "cn=Directory Manager" \  
--bindPassword2 password \  
--replicationPort2 8989 \  
--trustAll \  
--no-prompt  
  
Establishing connections ..... Done.  
Checking registration information ..... Done.  
Updating remote references on server opendj.example.com:4444 ..... Done.  
Configuring Replication port on server opendj2.example.com:4444 ..... Done.  
Updating replication configuration for baseDN dc=example,dc=com on server  
opendj.example.com:4444 ..... Done.  
Updating replication configuration for baseDN dc=example,dc=com on server  
opendj2.example.com:4444 ..... Done.  
Updating registration configuration on server  
opendj.example.com:4444 ..... Done.  
Updating registration configuration on server  
opendj2.example.com:4444 ..... Done.  
Updating replication configuration for baseDN cn=schema on server  
opendj.example.com:4444 ..... Done.  
Updating replication configuration for baseDN cn=schema on server  
opendj2.example.com:4444 ..... Done.  
Initializing registration information on server opendj2.example.com:4444 with  
the contents of server opendj.example.com:4444 ..... Done.  
Initializing schema on server opendj2.example.com:4444 with the contents of  
server opendj.example.com:4444 ..... Done.  
  
Replication has been successfully enabled. Note that for replication to  
work you must initialize the contents of the base DN's that are being  
replicated (use dsreplication initialize to do so).  
  
See  
/var/.../opens-replication-7958637258600693490.log  
for a detailed log of this operation.
```

To enable secure connections for replication use the `--secureReplication1` and `--secureReplication2` options, which are equivalent to selecting **Configure as Secure** in the replication topology options screen of the setup wizard.

As you see in the command output, replication is set up to function once enabled. You must, however, initialize replication in order to start the process.



Tip

When scripting the configuration to set up multiple replicas in quick succession, use the same initial replication server each time you run the command. In other words, pass the same `--host1`, `--port1`, `--bindDN1`, `--bindPassword1`, and `--replicationPort1` options for each of the other replicas that you set up in your script.

If you need to add another OpenDJ directory server to participate in replication, use the **dsreplication enable** with the new server as the second server.

8.3.2 Initializing Replicas

You can initialize replication between servers by performing initialization over the network after you have enabled replication, or by importing the same LDIF data on all servers and then enabling replication. You can also add a new server by restoring a backup from an existing replica onto the new server and then enabling replication with an existing replica.

The alternatives are described step-by-step in the following procedures:

- [Procedure 8.1, "To Initialize Replication Over the Network"](#)
- [Procedure 8.2, "To Initialize All Servers From the Same LDIF"](#)
- [Procedure 8.3, "To Create a New Replica From an Existing Backup"](#)
- [Procedure 8.4, "To Restore All Replicas to a Known State"](#)

Procedure 8.1. To Initialize Replication Over the Network

Initialization over the network while the server is online works well when you have no initial data, or when your network bandwidth is large compared to the initial amount of data to replicate.

1. Enable replication on all servers.

See [Section 8.3.1, "Enabling Replication"](#) for instructions.

2. Start replication with the **dsreplication initialize-all** command:

```
$ dsrepllication \
  initialize-all \
  --adminUID admin \
  --adminPassword password \
  --baseDN dc=example,dc=com \
  --hostname opendj.example.com \
  --port 4444 \
  --trustAll \
  --no-prompt

Initializing base DN dc=example,dc=com with the contents from
opendj.example.com:4444: 160 entries processed (100 % complete).
Base DN initialized successfully.

See
/var/.../opens-replication-5020375834904394170.log
for a detailed log of this operation.
```

Procedure 8.2. To Initialize All Servers From the Same LDIF

This procedure can be useful when you are starting with a large amount of directory data that is available locally to all directory servers.

1. Import the same LDIF on all servers as described in [Procedure 4.2, "To Import LDIF Data"](#).

Do not yet accept updates to the directory data. [Section 8.3.7, "Read-Only Replicas"](#) shows how to prevent replicas from accepting updates from clients.

2. Enable replication for all servers.

See [Section 8.3.1, "Enabling Replication"](#) for instructions.

3. Allow updates to the directory data by setting writability-mode:enabled using a command like the one you found in [Section 8.3.7, "Read-Only Replicas"](#).

Procedure 8.3. To Create a New Replica From an Existing Backup

You can create a new replica from a backup of a server in the existing topology.

1. Install a new server to use as the new replica.
2. Backup the database on an existing server as described in [Section 9.1, "Backing Up Directory Data"](#).

At this point, other servers in the topology can continue to process updates.

3. Enable replication on the new replica:


```
$ dsrepllication \
enable \
--adminUID admin \
--adminPassword password \
--baseDN dc=example,dc=com \
--host1 opendj.example.com \
--port1 4444 \
--bindDN1 "cn=Directory Manager" \
--bindPassword1 password \
--replicationPort1 8989 \
--host2 opendj3.example.com \
--port2 4444 \
--bindDN2 "cn=Directory Manager" \
--bindPassword2 password \
--replicationPort2 8989 \
--trustAll \
--no-prompt

Establishing connections ..... Done.
Checking registration information ..... Done.
Updating remote references on server opendj.example.com:4444 ..... Done.
Configuring Replication port on server opendj3.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
opendj3.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
opendj2.example.com:4444 ..... Done.
Updating remote references on server opendj2.example.com:4444 ..... Done.
Updating registration configuration on server
opendj.example.com:4444 ..... Done.
Updating registration configuration on server
opendj3.example.com:4444 ..... Done.
Updating registration configuration on server
opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
opendj3.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
opendj2.example.com:4444 ..... Done.
Initializing registration information on server opendj3.example.com:4444 with
the contents of server opendj.example.com:4444 ..... Done.

Replication has been successfully enabled. Note that for replication to
work you must initialize the contents of the base DN's that are being
replicated (use dsrepllication initialize to do so).

See
/var/.../opensd-replication-1672058070147419978.log
for a detailed log of this operation.
```

Contrary to the message from the command, you do not need to use the **dsrepllication initialize** command at this point.

4. On the new server, restore the database from the backup archive as described in [Procedure 9.5, "To Restore a Replica"](#).

As long as you restore the database on the new replica before the replication purge delay runs out, updates processed by other servers after you created the backup are replicated to the new server after you restore the data.

Procedure 8.4. To Restore All Replicas to a Known State

OpenDJ replication is designed to make directory data converge across all replicas in a topology. Directory replication mechanically applies new changes to ensure that replicated data is the same everywhere, with newer changes taking precedence over older changes.

When you restore older backup data, for example, directory replication applies newer changes to the older data. This behavior is a good thing when the newer changes are correct.

This behavior can be problematic in the following cases:

- A bug or serious user error results in unwanted new changes that are hard to fix.
- The data in a test or proof-of-concept environment must regularly be reinitialized to a known state.

The **dsreplication** command has the following subcommands that let you reinitialize directory data, preventing replication from replaying changes that occurred before reinitialization:

- The **dsreplication pre-external-initialization** command removes the setting for the *generation ID* across the topology for a specified base DN. The generation ID is an internal-use identifier that replication uses to determine what changes to apply. This halts replication.
- The **dsreplication post-external-initialization** command sets a new generation ID across the topology, effectively resuming replication.



Caution

The steps in this procedure reinitialize the replication changelog, eliminating the history of changes that occurred before replication resumed. The replication changelog is described in [Section 8.4, "Change Notification For Your Applications"](#). Applications that depend on the changelog for change notifications must be reinitialized after this procedure is completed.

1. Prevent changes to the affected data during the procedure, as such changes are lost for the purposes of replication.

For example, make each replica read-only as described in [Section 8.3.7, "Read-Only Replicas"](#).

2. On a single server in the topology, run the **dsreplication pre-external-initialization** command for the base DN holding the relevant data, as shown in the following example:

```
$ dsreplication \
pre-external-initialization \
--adminUID admin \
--adminPassword password \
--baseDN dc=example,dc=com \
--hostname opendj.example.com \
--port 4444 \
--trustAll \
--no-prompt
```

Preparing base DN dc=example,dc=com to be initialized externally Done.

Now you can proceed to the initialization of the contents of the base DNs on all the replicated servers. You can use the command `import-ldif` or the binary copy to do so. You must use the same LDIF file or binary copy on each server.

When the initialization is completed you must use the subcommand 'post-external-initialization' for replication to work with the new base DNs contents.

Replication halts as the command takes effect.

Changes made at this time are not replicated, even after replication resumes.

3. On each server in the topology, restore the data in the topology to the known state in one of the following ways:
 - Import the data from LDIF as described in [Procedure 4.2, "To Import LDIF Data"](#).
 - Restore the data from backup as described in [Procedure 9.4, "To Restore a Stand-alone Server"](#).
4. On a single server in the topology, run the **dsreplication post-external-initialization** command for the base DN holding the relevant data, as shown in the following example:

```
$ dsreplcation \  
post-external-initialization \  
--adminUID admin \  
--adminPassword password \  
--baseDN dc=example,dc=com \  
--hostname opendj.example.com \  
--port 4444 \  
--trustAll \  
--no-prompt  
  
Updating replication information on base DN dc=example,dc=com ..... Done.  
  
Post initialization procedure completed successfully.
```

Replication resumes as the command takes effect.

5. If you made replicas read-only, make them read-write again by setting `writability-mode:enabled`.

8.3.3 Stopping Replication

How you stop replication depends on whether the change is meant to be temporary or permanent.

Procedure 8.5. To Stop Replication Temporarily For a Replica

If you must stop a server from replicating temporarily, you can do so by using the **dsconfig** command.



Warning

Do not allow modifications on the replica for which replication is disabled, as no record of such changes is kept, and the changes cause replication to diverge.

1. Disable the multimaster synchronization provider:

```
$ dsconfig \
  set-synchronization-provider-prop \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --set enabled:false \
  --trustAll \
  --no-prompt
```

2. When you are ready to resume replication, enable the multimaster synchronization provider:

```
$ dsconfig \
  set-synchronization-provider-prop \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --set enabled:true \
  --trustAll \
  --no-prompt
```

Procedure 8.6. To Stop Replication Permanently For a Replica

If you need to stop a server from replicating permanently, for example in preparation to remove a server, you can do so with the **dsreplication disable** command.

1. Stop replication using the **dsreplication disable** command:

```

$ dsreplication \
  disable \
  --disableAll \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --adminPassword password \
  --trustAll \
  --no-prompt
Establishing connections ..... Done.
Disabling replication on base DN cn=admin data of server
opendj2.example.com:4444 ..... Done.
Disabling replication on base DN dc=example,dc=com of server
opendj2.example.com:4444 ..... Done.
Disabling replication on base DN cn=schema of server
opendj2.example.com:4444 ..... Done.
Disabling replication port 8989 of server
opendj2.example.com:4444 ..... Done.
Removing registration information ..... Done.
Removing truststore information ..... Done.

See
/var/.../opens-125248191132797765.log
for a detailed log of this operation.

```

The **dsreplication disable** as shown completely removes the replication configuration information from the server.

2. If you want to restart replication for the server, you need to run the **dsreplication enable** and **dsreplication initialize** commands again.

8.3.4 Standalone Replication Servers

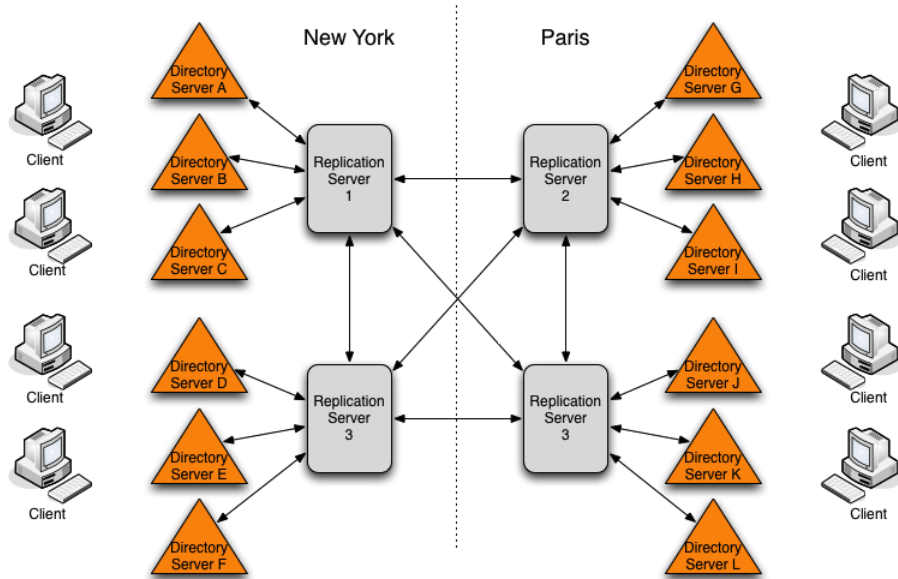
Replication in OpenDJ is designed to be both easy to implement in environments with a few servers, and also scalable in environments with many servers. You can enable the replication service on each OpenDJ directory server in your deployment, for example, to limit the number of servers you deploy. Yet in a large deployment, you can use standalone replication servers—OpenDJ servers that do nothing but relay replication messages—to configure (and troubleshoot) the replication service separately from the directory service. You only need a few standalone replication servers publishing changes to serve many directory servers subscribed to the changes. Furthermore, replication is designed such that you need only connect a directory server to the nearest replication server for the directory server to replicate with all others in your topology. Yet only the standalone replication servers participate in fully meshed replication.

All replication servers in a topology are connected to all other replication servers. Directory servers are connected only to one replication server at a time, and their connections should be to replication servers on the same LAN. Therefore the total number of replication connections, $Total_{conn}$ is expressed as follows.

$$\text{Total}_{\text{conn}} = (N_{\text{RS}} * (N_{\text{RS}} - 1)) / 2 + N_{\text{DS}} \quad (8.1)$$

Here, N_{RS} is the number of replication servers, and N_{DS} is the number of standalone directory servers. In other words, if you have only three servers, then $\text{Total}_{\text{conn}}$ is three with no standalone servers. However, if you have two data centers, and need 12 directory servers, then with no standalone directory servers $\text{Total}_{\text{conn}}$ is $(12 * 11) / 2$ or 66. Yet, with four standalone replication servers, and 12 standalone directory servers, $\text{Total}_{\text{conn}}$ is $(4 * 3) / 2 + 12$, or 18, with only four of those connections needing to go over the WAN. (By running four directory servers that also run replication servers and eight standalone directory servers, you reduce the number of replication connections to 14 for 12 replicas.)

Figure 8.1. Deployment For Multiple Data Centers



Tip

If you set up OpenDJ directory server to replicate by using the Quick Setup wizard, then the wizard activated the replication service for that server. You can turn off the replication service on OpenDJ directory server, and then configure the server to work with a separate, standalone replication server instead. Start by using the **dsreplication disable --**

disableReplicationServer command to turn off the replication service on the server.

Procedure 8.7. To Set Up a Standalone Replication Server

This example sets up a standalone replication server to handle the replication traffic between two directory servers that do not handle replication themselves.

Here the replication server is `rs.example.com`. The directory servers are `opendj.example.com` and `opendj2.example.com`.

In a real deployment, you would have more replication servers to avoid a single point of failure.

1. Set up the replication server as a directory server that has no database.
2. Set up the directory servers as standalone directory servers.
3. Enable replication with `--noReplicationServer` or `--onlyReplicationServer` options:


```
$ dsreplication \
enable \
--adminUID admin \
--adminPassword password \
--baseDN dc=example,dc=com \
--host1 opendj.example.com \
--port1 4444 \
--bindDN1 "cn=Directory Manager" \
--bindPassword1 password \
--noReplicationServer1 \
--host2 rs.example.com \
--port2 4444 \
--bindDN2 "cn=Directory Manager" \
--bindPassword2 password \
--replicationPort2 8989 \
--onlyReplicationServer2 \
--trustAll \
--no-prompt
Establishing connections ..... Done.
Only one replication server will be defined for the following base DN's:
dc=example,dc=com
It is recommended to have at least two replication servers (two changelogs) to
avoid a single point of failure in the replication topology.

Checking registration information ..... Done.
Configuring Replication port on server rs.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
opendj.example.com:4444 ..... Done.
Updating registration configuration on server
opendj.example.com:4444 ..... Done.
Updating registration configuration on server
rs.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
opendj.example.com:4444 ..... Done.
Initializing registration information on server rs.example.com:4444 with
the contents of server opendj.example.com:4444 ..... Done.

Replication has been successfully enabled. Note that for replication to work
you must initialize the contents of the base DN's that are being
replicated (use dsreplication initialize to do so).

See
/var/.../opens-replication-1720959352638609971.log
for a detailed log of this operation.

$ dsreplication \
enable \
--adminUID admin \
--adminPassword password \
--baseDN dc=example,dc=com \
--host1 opendj2.example.com \
--port1 4444 \
--bindDN1 "cn=Directory Manager" \
--bindPassword1 password \
--noReplicationServer1 \
--host2 rs.example.com \
--port2 4444 \
--bindDN2 "cn=Directory Manager" \
--bindPassword2 password \
--replicationPort2 8989 \
--onlyReplicationServer2 \
--trustAll \
--no-prompt

Establishing connections ..... Done.
Only one replication server will be defined for the following base DN's:
dc=example,dc=com
It is recommended to have at least two replication servers (two changelogs) to
avoid a single point of failure in the replication topology.
```

4. Initialize replication from one of the directory servers:

```
$ dsreplication \  
  initialize-all \  
  --adminUID admin \  
  --adminPassword password \  
  --baseDN dc=example,dc=com \  
  --hostname opendj.example.com \  
  --port 4444 \  
  --trustAll \  
  --no-prompt  
  
Initializing base DN dc=example,dc=com with the contents from  
opendj.example.com:4444: 160 entries processed (100 % complete).  
Base DN initialized successfully.  
  
See  
/var/.../opens-replication-7677303986403997574.log  
for a detailed log of this operation.
```

8.3.5 Standalone Directory Server Replicas

When you configure replication for an OpenDJ directory server, you can give the directory server the capability to handle replication traffic as well. As described in [Section 8.3.4, "Standalone Replication Servers"](#), OpenDJ servers can also be configured to handle only replication traffic.

Alternatively you can configure an OpenDJ directory server to connect to a remote replication server of either variety, but to remain only a directory server itself. This sort of standalone directory server replica is shown in [Figure 8.1, "Deployment For Multiple Data Centers"](#).

Furthermore, you can make this standalone directory server replica read-only for client applications, accepting only replication updates.

Procedure 8.8. To Set Up a Standalone Directory Server Replica

The following steps show how to configure the server as a standalone, directory server-only replica of an existing replicated directory server.

1. Set up replication between other servers.
2. Install the directory server without configuring replication, but creating at least the base entry to be replicated.
3. Enable replication with the appropriate `--noReplicationServer` option:

```
$ dsrepllication \  
enable \  
--adminUID admin \  
--adminPassword password \  
--baseDN dc=example,dc=com \  
--host1 master.example.com \  
--port1 4444 \  
--bindDN1 "cn=Directory Manager" \  
--bindPassword1 password \  
--host2 ds-only.example.com \  
--port2 4444 \  
--bindDN2 "cn=Directory Manager" \  
--bindPassword2 password \  
--noReplicationServer2 \  
--trustAll \  
--no-prompt  
  
Establishing connections ..... Done.  
Checking registration information ..... Done.  
Updating remote references on server master.example.com:4444 ..... Done.  
Updating replication configuration for baseDN dc=example,dc=com  
on server master.example.com:4444 ..... Done.  
Updating replication configuration for baseDN dc=example,dc=com  
on server ds-only.example.com:4444 ..... Done.  
Updating replication configuration for baseDN dc=example,dc=com  
on server master2.example.com:4444 ..... Done.  
Updating remote references on server master2.example.com:4444 ..... Done.  
Updating registration configuration  
on server master.example.com:4444 ..... Done.  
Updating registration configuration  
on server ds-only.example.com:4444 ..... Done.  
Updating registration configuration  
on server master2.example.com:4444 ..... Done.  
Updating replication configuration for baseDN cn=schema  
on server master.example.com:4444 ..... Done.  
Updating replication configuration for baseDN cn=schema  
on server ds-only.example.com:4444 ..... Done.  
Updating replication configuration for baseDN cn=schema  
on server master2.example.com:4444 ..... Done.  
Initializing registration information on server ds-only.example.com:4444  
with the contents of server master.example.com:4444 ..... Done.  
Initializing schema on server ds-only.example.com:4444  
with the contents of server master.example.com:4444 ..... Done.  
  
Replication has been successfully enabled. Note that for replication to work  
you must initialize the contents of the base DN's that are being replicated  
(use dsrepllication initialize to do so).  
  
See  
/var/.../opendj-replication-859181866587327450.log  
for a detailed log of this operation.
```

Here the existing server is both directory server and replication server.
If the existing server is a standalone replication server, then also use the
appropriate `--onlyReplicationServer` option.

4. Initialize data on the new directory server replica:

```
$ dsreplation \  
  initialize \  
    --adminUID admin \  
    --adminPassword password \  
    --baseDN dc=example,dc=com \  
    --hostSource master.example.com \  
    --portSource 4444 \  
    --hostDestination ds-only.example.com \  
    --portDestination 4444 \  
    --trustAll \  
    --no-prompt  
  
Initializing base DN dc=example,dc=com with the contents  
  from master.example.com:4444:  
0 entries processed (0 % complete).  
176 entries processed (100 % complete).  
Base DN initialized successfully.  
  
See  
/var/.../opendj-replication-4326340645155418876.log  
for a detailed log of this operation.
```

5. If you want to make the directory server replica read-only for client application traffic, see [Section 8.3.7, "Read-Only Replicas"](#).

8.3.6 Replication Groups

Replication lets you define groups so that replicas communicate first with replication servers in the group before going to replication servers outside the group. Groups are identified with unique numeric group IDs.

Replication groups are designed for deployments across multiple data centers, where you aim to focus replication traffic on the LAN rather than the WAN. In multi-data center deployments, group nearby servers together.

Procedure 8.9. To Set Up Replication Groups

For each group, set the appropriate group ID for the topology on both the replication servers and the directory servers.

The example commands in this procedure set up two replication groups, each with a replication server and a directory server. The directory servers are `opendj.example.com` and `opendj2.example.com`. The replication servers are `rs.example.com` and `rs2.example.com`. In a full-scale deployment, you would have multiple servers of each type in each group, such as all the replicas and replication servers in each data center being in the same group.

1. Pick a group ID for each group.

The default group ID is 1.

2. Set the group ID for each group by replication domain on the directory servers:

```
$ dsconfig \
set-replication-domain-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--domain-name "dc=example,dc=com" \
--set group-id:1 \
--trustAll \
--no-prompt

$ dsconfig \
set-replication-domain-prop \
--port 4444 \
--hostname opendj2.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--domain-name "dc=example,dc=com" \
--set group-id:2 \
--trustAll \
--no-prompt
```

3. Set the group ID for each group on the replication servers:

```
$ dsconfig \
set-replication-server-prop \
--port 4444 \
--hostname rs.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--set group-id:1 \
--trustAll \
--no-prompt

$ dsconfig \
set-replication-server-prop \
--port 4444 \
--hostname rs2.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--set group-id:2 \
--trustAll \
--no-prompt
```

8.3.7 Read-Only Replicas

By default all directory servers in a replication topology are read-write. You can, however, choose to make replicas take updates only from the replication protocol, and refuse updates from client applications:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set writability-mode:internal-only \
  --trustAll \
  --no-prompt
```

8.3.8 Assured Replication

In standard replication, when a client requests an update operation the directory server performs the update and, if the update is successful, sends information about the update to the replication service, and sends a result code to the client application right away. As a result, the client application can conclude that the update was successful, *but only on the replica that handled the update*.

Assured replication lets you force the replica performing the initial update to wait for confirmation that the update has been received elsewhere in the topology before sending a result code to the client application. You can configure assured replication either to wait for one or more replication servers to acknowledge having received the update, or to wait for all directory servers to have replayed the update.

As you might imagine, assured replication is theoretically safer than standard replication, yet it is also slower, potentially waiting for a timeout before failing when the network or other servers are down.

Procedure 8.10. To Ensure Updates Reach Replication Servers

Safe data mode requires the update be sent to `assured-sd-level` replication servers before acknowledgement is returned to the client application.

- For each directory server, set safe data mode for the replication domain, and also set the safe data level:

```
$ dsconfig \
  set-replication-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name "dc=example,dc=com" \
  --set assured-type:safe-data \
  --set assured-sd-level:1 \
  --trustAll \
  --no-prompt

$ dsconfig \
  set-replication-domain-prop \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name "dc=example,dc=com" \
  --set assured-type:safe-data \
  --set assured-sd-level:1 \
  --trustAll \
  --no-prompt
```

Procedure 8.11. To Ensure Updates Are Replayed Everywhere

Safe read mode requires the update be replayed on all directory servers before acknowledgement is returned to the client application.

- For each directory server, set safe read mode for the replication domain:

```
$ dsconfig \
  set-replication-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name "dc=example,dc=com" \
  --set assured-type:safe-read \
  --trustAll \
  --no-prompt

$ dsconfig \
  set-replication-domain-prop \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name "dc=example,dc=com" \
  --set assured-type:safe-read \
  --trustAll \
  --no-prompt
```

When working with assured replication, the replication server property `degraded-status-threshold` (default: 5000), sets the number of operations allowed to build up in the replication queue before the server is assigned degraded status. When a replication server has degraded status, assured replication ceases to have an effect.

8.3.9 Subtree Replication

OpenDJ can perform subtree replication, for example, replicating `ou=People,dc=example,dc=com`, but not the rest of `dc=example,dc=com`, by putting the subtree in a separate backend from the rest of the suffix.

For example, in this case you might have a `userRoot` backend containing everything in `dc=example,dc=com` except `ou=People,dc=example,dc=com`, and a separate `peopleRoot` backend for `ou=People,dc=example,dc=com`. Then you replicate `ou=People,dc=example,dc=com` in its own topology.

8.3.10 Fractional Replication

OpenDJ can perform fractional replication, whereby you specify the attributes to include in or to exclude from the replication process.

You set fractional replication configuration as `fractional-include` or `fractional-exclude` properties for a replication domain. When you include attributes, the attributes that are required on the relevant object classes are also included,

whether you specify them or not. When you exclude attributes, the excluded attributes must be optional attributes for the relevant object classes. Fractional replicas still respect schema definitions.

Fractional replication filters objects at the replication server level. Initialize replication as you would normally. Of course, you cannot create a full replica from a replica with only a subset of the data. If you must prevent data from being replicated across a national boundary, split the replication server handling the updates from the directory servers receiving the updates as described in [Procedure 8.7, "To Set Up a Standalone Replication Server"](#).

For example, you might configure an externally facing fractional replica to include only some inetOrgPerson attributes:

```
$ dsconfig \
  set-replication-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name "dc=example,dc=com" \
  --trustAll \
  --no-prompt \
  --set \
  fractional-include:inetorgperson:cn,givenname,mail,mobile,sn,telephonenumber
```

As another example, you might exclude a custom attribute called sessionToken from being replicated:

```
$ dsconfig \
  set-replication-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name "dc=example,dc=com" \
  --set fractional-exclude:*:sessionToken \
  --trustAll \
  --no-prompt
```

This last example only works if you first define a sessionToken attribute in the directory server schema.

8.3.11 Breaking a Multi-Role Server Into Standalone Components

As described in [Section 8.2, "About Replication"](#), a replication topology is made up of servers playing the role of directory server, and servers playing the role

of replication server. By default, each replicated OpenDJ server plays both roles. Some deployments call for standalone directory servers and standalone replication servers, however.³

If possible avoid breaking apart an existing multi-role server. Instead, set up standalone servers as described in [Section 8.3.4, "Standalone Replication Servers"](#) and [Section 8.3.5, "Standalone Directory Server Replicas"](#).

The following procedure breaks a multi-role server into two standalone servers while preserving existing data. It does require disk space initially to hold copies of existing data.

Procedure 8.12. To Break a Multi-Role Server Into Standalone Components

The following steps show how to break a multi-role OpenDJ server into a standalone directory server and a standalone replication server.

While you carry out this procedure, do not allow any client traffic to the servers you modify.

1. Make sure you have already set up at least a couple of OpenDJ servers that replicate user data.

This example starts with the following multi-role servers:

- `/path/to/dsrs1` (ports: 1389, 1636, 4444, 8989; replicating user data for `dc=example,dc=com`)
- `/path/to/dsrs2` (ports: 2389, 2636, 5444, 9989; replicating user data for `dc=example,dc=com`)

`/path/to/dsrs1` is the target server to be broken into standalone components.

When you begin, the target server has both directory server and replication server components.

Before you proceed:

- Read the rest of the procedure, and make sure you understand the steps.
- Direct client traffic away from the target server.
- Back up the target server.

2. Run the **`dsreplication status`** command before making changes:

³ In practice, "standalone" technically usually refers only to the role with respect to replication of user data. In fact standalone servers generally continue to play both roles for server configuration data under `cn=admin` data and `cn=schema`. The update traffic to these suffixes is, however, generally orders of magnitude lower than update traffic for user data.

```
$ dsreplication \
status \
--port 4444 \
--hostname opendj.example.com \
--adminUID admin \
--adminPassword password \
--baseDN "cn=admin data" \
--baseDN cn=schema \
--baseDN dc=example,dc=com \
--trustAll \
--no-prompt

Suffix DN      :...: DS ID : RS ID :...
-----:-----:-----:
cn=admin data  :...: 29388 : 32560 :...
cn=admin data  :...: 7044  : 29137 :...
cn=schema      :...: 24612 : 32560 :...
cn=schema      :...: 22295 : 29137 :...
dc=example,dc=com :...: 20360 : 32560 :...
dc=example,dc=com :...: 12164 : 29137 :...
...
```

Keep the output of the command for the IDs shown. The information is used later in this procedure.

3. Temporarily disable the multimaster synchronization provider on the target server:

```
$ dsconfig \
set-synchronization-provider-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--set enabled:false \
--trustAll \
--no-prompt
```

This step is also shown in [Procedure 8.5, "To Stop Replication Temporarily For a Replica"](#).

4. Temporarily disable the backend holding the replicated data:

```
$ dsconfig \
  set-backend-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --backend-name userRoot \
    --set enabled:false \
    --trustAll \
    --no-prompt
```

5. Stop the target server:

```
$ stop-ds
Stopping Server...
... msg=The Directory Server is now stopped
```

6. Make two copies of the server files:

```
$ cd /path/to/
```

One copy will be the standalone directory server:

```
$ cp -r dsrs1 ds
```

The other copy will be the standalone replication server:

```
$ cp -r dsrs1 rs
```

7. Start the copy that will become the standalone directory server, remove the replication server and changelog configuration, enable the user data backend, and then enable the multimaster synchronization provider on the directory server:

```
# The following command removes the replication server configuration.

dsconfig \
  delete-replication-server \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --provider-name "Multimaster Synchronization" \
```

```
--trustAll \  
--no-prompt  
  
# The following command disables the changelog for the user data  
# in dc=example,dc=com.  
  
dsconfig \  
  set-external-changelog-domain-prop \  
  --port 4444 \  
  --hostname opendj.example.com \  
  --bindDN "cn=Directory Manager" \  
  --bindPassword password \  
  --provider-name "Multimaster Synchronization" \  
  --domain-name dc=example,dc=com  
  --set enabled:false  
  --trustAll \  
  --no-prompt  
  
# The following command enables the user data backend.  
  
dsconfig \  
  set-backend-prop \  
  --port 4444 \  
  --hostname opendj.example.com \  
  --bindDN "cn=Directory Manager" \  
  --bindPassword password \  
  --backend-name userRoot \  
  --set enabled:true \  
  --trustAll \  
  --no-prompt  
  
# The following command enables the multimaster synchronization provider.  
  
dsconfig \  
  set-synchronization-provider-prop \  
  --port 4444 \  
  --hostname opendj.example.com \  
  --bindDN "cn=Directory Manager" \  
  --bindPassword password \  
  --provider-name "Multimaster Synchronization" \  
  --set enabled:true \  
  --trustAll \  
  --no-prompt
```

You can then remove the files for the changelog on the directory server:

```
$ rm /path/to/ds/changelogDb/*
```

8. If the replication server is on the same host as the directory server, carefully change the connection handler port numbers and the administration port number in the configuration file before starting the replication server. Before making any changes, make sure that the new port numbers you use are available, and not in use by any other services on the system.

Change the port numbers for the LDAP and LDAPS connection handlers as described in [Procedure 5.1, "To Change the LDAP Port Number"](#).

The following example changes the administration port to 6444. After this command succeeds, you must restart the server in order to use the **dsconfig** command again:

```
$ dsconfig \
  set-administration-connector-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set listen-port:6444 \
  --trustAll \
  --no-prompt
```

Restart the server to be able to connect on the new administration port:

```
$ stop-ds --restart
Stopping Server...
...
...The Directory Server has started successfully
```

9. Change the server ID values for the cn=admin data and cn=schema replication domains on the copy that is to become the standalone replication server.

Replication uses unique server IDs to distinguish between different directory server replicas. When you make identical copies of the original multi-role server, the server IDs on the new standalone directory server and on the new standalone replication server are identical.

For the user data replication domains, such as dc=example,dc=com, you are going to fix the duplicate server ID problem as part of this procedure. When you remove the replication domain configuration information from the new standalone replication server for user data, part of the configuration information that you remove is the server ID. For the administrative data and directory schema, however, the new standalone replication server must maintain its administrative and schema data in sync with other servers, so it still holds that data like any other directory server. The server IDs for the cn=admin data and cn=schema replication domains must therefore be changed so as not to conflict with other existing server IDs.

If you try to edit server IDs by using the **dsconfig** command, you encounter an error:

The Replication Domain property "server-id" is read-only and cannot be modified

You must instead edit the server ID values directly in the configuration file while the new standalone replication server is stopped.

Before editing the configuration file, refer to the information you gather in [Step 2](#) for the list of IDs that are in use in the replication topology. You must choose server ID values that are unique, and that are between 0 and 65535 inclusive.

After choosing two valid, unused server ID values, carefully edit the configuration file, /path/to/rs/config/config.ldif, to change the ds-cfg-server-id values for the entries with DNs cn=cn=admin data,cn=domains,cn=Multimaster Synchronization,cn=Synchronization Providers,cn=config and cn=cn=schema,cn=domains,cn=Multimaster Synchronization,cn=Synchronization Providers,cn=config.

For example, if the duplicate server IDs were 29388 and 24612, and you edited the configuration file to use 12345 and 23456 instead, the result might appear as follows:

```
$ grep -B 1 ds-cfg-server-id /path/to/rs/config/config.ldif
cn: cn=admin data
#ds-cfg-server-id: 29388
ds-cfg-server-id: 12345
--
cn: cn=schema
#ds-cfg-server-id: 24612
ds-cfg-server-id: 23456
```

10. Start the copy that is to become the standalone replication server, remove the user data backend configuration, remove the replication domain for the user data, and then enable the multimaster synchronization provider on the directory server:

```
# The following command removes the user data backend configuration.

dsconfig \
  delete-backend \
    --port 6444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --backend-name userRoot \
    --trustAll \
    --no-prompt

# The following command removes the replication domain for the user data.
```

```
dsconfig \
  delete-replication-domain \
  --port 6444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name dc=example,dc=com \
  --trustAll \
  --no-prompt

# The following command enables the multimaster synchronization provider.

dsconfig \
  set-synchronization-provider-prop \
  --port 6444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --set enabled:true \
  --trustAll \
  --no-prompt
```

You can then remove the files for the user data backend on the replication server:

```
$ rm -rf /path/to/rs/db/userRoot
```

11. If you have moved servers with secure ports configured, the host names in the server certificates might no longer correspond to the new host names.

For details see [Chapter 20, "Changing Server Certificates"](#).

12. After testing that everything is working to your satisfaction, you can allow normal client traffic to the new directory server, and retire the old multi-role server (**rm -rf /path/to/dsrs1** in this example).

8.4 Change Notification For Your Applications

Some applications require notification when directory data updates occur. For example, an application might need to sync directory data with another database, or the application might need to kick off other processing when certain updates occur.

In addition to supporting persistent search operations, OpenDJ provides an external change log mechanism to allow applications to be notified of changes to directory data.

This section includes the following procedures:

- [Procedure 8.13, "To Enable the External Change Log"](#)
- [Procedure 8.14, "To Use the External Change Log"](#)
- [Procedure 8.15, "To Include Unchanged Attributes in the External Change Log"](#)
- [Procedure 8.16, "To Limit External Change Log Content"](#)
- [Procedure 8.17, "To Align Draft Change Numbers"](#)

Procedure 8.13. To Enable the External Change Log

OpenDJ directory servers without replication cannot expose an external change log. The OpenDJ server that exposes the change log must function both as a directory server, and also as a replication server for the suffix whose changes you want logged.

- Enable replication without using the `--noReplicationServer` or `--onlyReplicationServer` options.

With replication enabled, the data is under `cn=changelog`. The user reading the changelog must however have access to read and search the changelog and must have the `changelog-read` privilege. By default, Directory Manager has this privilege:

```
$ ldapsearch \
--hostname opendj.example.com \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--baseDN cn=changelog \
"(objectclass=*)" \
\* +
dn: cn=changelog
cn: changelog
objectClass: top
objectClass: container
subschemaSubentry: cn=schema
hasSubordinates: false
entryDN: cn=changelog
```

To allow other users to read the changelog, add the `changelog-read` privilege to their entries. For details on how to add a privilege, see [Section 6.3, "Configuring Privileges"](#).

Procedure 8.14. To Use the External Change Log

You read the external change log over LDAP. In addition, when you poll the change log periodically, you can get the list of updates that happened since your last request.

The external change log mechanism uses an LDAP control with OID 1.3.6.1.4.1.26027.1.5.4 to allow the exchange of cookies for the client application to bookmark the last changes seen, and then start reading the next set of changes from where it left off on the previous request.

This procedure shows the client reading the change log as `cn=Directory Manager`. Make sure your client application reads the changes with sufficient access and privileges to view all the changes it needs to see.

1. Send an initial search request using the LDAP control with no cookie value.

Notice the value of the `changeLogCookie` attribute for the last of the two changes:

Change Notification For Your Applications

```
$ ldapsearch \
--baseDN cn=changelog \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--control "1.3.6.1.4.1.26027.1.5.4:false" \
"(objectclass=*)" \
\* +
dn: cn=changelog
cn: changelog
objectClass: top
objectClass: container
subschemaSubentry: cn=schema
hasSubordinates: true
entryDN: cn=changelog

# Public changelog exchange control(1.3.6.1.4.1.26027.1.5.4):
dc=example,dc=com:0000013087cbc28212d100000001;
dn: replicationCSN=0000013087cbc28212d100000001,dc=example,dc=com,cn=changelog
targetDN: cn=arsene lupin,ou=special users,dc=example,dc=com
changeNumber: 0
changes:: b2JqZWNOQ2xhc3M6IHBlcnNvbGpvYmplY3RDbGFzc2ogdG9wCmNuOiBBcnNlbnUgTHVwaW
4KdGVsZXBob25lTnVtYmVyOiArMzMgMSAyMyA0NSA2NyA40QpzbjogTHVwaW4KZW50cnllVUUE0iA5M
GM3MTNmNy00ODZlLTRkNDctOTQwOS1iNDRkMTlkZWZzMWUKY3JlYXRlVGltZXN0YW1wOiAyMDExMDYx
MzA2NTg1NVokY3JlYXRvcnNOYW10iBjbj1EaXJlY3RvcnkgTWFuYWdlcixxbj1Sb290IER0cyxbj1
jb25maWck
changeType: add
changeTime: 20110613065855Z
objectClass: top
objectClass: changeLogEntry
targetEntryUUID: 90c714f7-486b-4d47-9409-b44d19dea31e
replicationCSN: 0000013087cbc28212d100000001
numSubordinates: 0
replicaIdentifier: 4817
changeLogCookie: dc=example,dc=com:0000013087cbc28212d100000001;
changeInitiatorsName: cn=Directory Manager,cn=Root DNs,cn=config
subschemaSubentry: cn=schema
hasSubordinates: false
entryDN: replicationCSN=0000013087cbc28212d100000001,dc=example,dc=com,cn=change
log

# Public changelog exchange control(1.3.6.1.4.1.26027.1.5.4):
dc=example,dc=com:0000013087cbc34a12d100000002;
dn: replicationCSN=0000013087cbc34a12d100000002,dc=example,dc=com,cn=changelog
targetDN: cn=horace velmont,ou=special users,dc=example,dc=com
changeNumber: 0
changes:: b2JqZWNOQ2xhc3M6IHBlcnNvbGpvYmplY3RDbGFzc2ogdG9wCmNuOiBiB3JhY2UgVmVsbn
9udAp0ZWxlcnGhbnV0dW1lZXI6ICszMyAxIDEyIDZlIDM0IDQ1CnNuOiBhZWZwxb250CmVudHJ5VWVJR
DogNmIyMjQ0MGEtNzZkMC00MDMxLTk0YjctMzViMmQ0NmYwNjdlCmNyZWZ0ZVRpbWVzdGFtcDogMjAx
MTA2MThwNjU4NTVaCmNyZWZ0b3JzTmFtZTogY249RGlyZWNO0b3J5IE1hbmFnZXIsY249Um9vdCBETnM
sY249Y29uZmlnCG==
changeType: add
changeTime: 20110613065855Z
objectClass: top
objectClass: changeLogEntry
targetEntryUUID: 6b22440a-76d0-4031-94b7-35b1d86f067e
replicationCSN: 0000013087cbc34a12d100000002
numSubordinates: 0
replicaIdentifier: 4817
changeLogCookie: dc=example,dc=com:0000013087cbc34a12d100000002;
changeInitiatorsName: cn=Directory Manager,cn=Root DNs,cn=config
subschemaSubentry: cn=schema
hasSubordinates: false
entryDN: replicationCSN=0000013087cbc34a12d100000002,dc=example,dc=com,cn=change
log
```

In this example, two new users were added to another replica before the change log request was made.

Here the changes are base64-encoded, so you can decode them using the **base64** command:

```
$ base64 decode --encodedData b2JqZW...Zm1nCg==
objectClass: person
objectClass: top
cn: Horace Velmont
telephoneNumber: +33 1 12 23 34 45
sn: Velmont
entryUUID: 6b22440a-76d0-4031-94b7-35b1d86f067e
createTimestamp: 20110613065855Z
creatorsName: cn=Directory Manager,cn=Root DNs,cn=config
```

2. For the next search, provide the cookie to start reading where you left off last time.

In this example, a description was added to Babs Jensen's entry:

```
$ ldapsearch \
--baseDN cn=changelog \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--control "1.3.6.1.4.1.26027.1.5.4:false:dc=example, \
dc=com:0000013087cbc34a12d100000002;" \
"(objectclass=*)" \
\* +
dn: cn=changelog
cn: changelog
objectClass: top
objectClass: container
subschemaSubentry: cn=schema
hasSubordinates: true
entryDN: cn=changelog

# Public changelog exchange control(1.3.6.1.4.1.26027.1.5.4):
dc=example,dc=com:0000013087d7e27f12d100000003;
dn: replicationCSN=0000013087d7e27f12d100000003,dc=example,dc=com,cn=changelog
targetDN: uid=bjensen,ou=people,dc=example,dc=com
changeNumber: 0
changes:: YWRkOiBkZXNjcmlwdGlvbgpkZXNjcmlwdGlvbjogQSB0aGlyZCBjaGFuZ2UKLQpyZXBsYW
NlOiBtb2RpZmllcnNOYW1lCm1vZGlmawVyc05hbWU6IGNuPURpcmVjdG9yeSB5BNW5hZ2VylGNuPVJvb
3QgRE5zLGNuPWVbmZpZwotCnJlcGxhY2U6IGlvZGlmVVRpbWVzdGFtcAptb2RpZnluUaW1lc3RhbXA6
IDIwMTcwNjEzMDcxMjEwWgotCg==
changeType: modify
changeTime: 20110613071210Z
objectClass: top
objectClass: changeLogEntry
targetEntryUUID: fc252fd9-b982-3ed6-b42a-c76d2546312c
replicationCSN: 0000013087d7e27f12d100000003
numSubordinates: 0
replicaIdentifier: 4817
changeLogCookie: dc=example,dc=com:0000013087d7e27f12d100000003;
changeInitiatorsName: cn=Directory Manager,cn=Root DNs,cn=config
subschemaSubentry: cn=schema
hasSubordinates: false
entryDN: replicationCSN=0000013087d7e27f12d100000003,dc=example,dc=com,cn=change
log
```

If we base64-decode the changes, we see the following:

```
$ base64 decode --encodedData YWRkOiBkZXNjcmlwdGlvbjogQSB0aGlyZCBjaGFuZ2UKLQpyZXBsYW
NlOiBtb2RpZmllcnNOYW1lCm1vZGlmawVyc05hbWU6IGNuPURpcmVjdG9yeSB5BNW5hZ2VylGNuPVJvb
3QgRE5zLGNuPWVbmZpZwotCnJlcGxhY2U6IGlvZGlmVVRpbWVzdGFtcAptb2RpZnluUaW1lc3RhbXA6
IDIwMTcwNjEzMDcxMjEwWgotCg==
add: description
description: A third change
-
replace: modifiersName
modifiersName: cn=Directory Manager,cn=Root DNs,cn=config
-
replace: modifyTimestamp
modifyTimestamp: 20110613071210Z
-
```

3. If for some reason you lose the cookie, you can start over from the earliest available change by sending a search request with no value for the cookie.

Procedure 8.15. To Include Unchanged Attributes in the External Change Log

As shown above, the changes returned from a search on the external change log include only what was actually changed. If you have applications that need additional attributes published with every change log entry, regardless of whether or not the attribute itself has changed, then specify those using `ecl-include` and `ecl-include-for-deletes`.

1. Set the attributes to include for all update operations with `ecl-include`:

```
$ dsconfig \
  set-external-changelog-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name dc=example,dc=com \
  --set ecl-include:"@person" \
  --trustAll \
  --no-prompt
```

2. Set the attributes to include for deletes with `ecl-include-for-deletes`:

```
$ dsconfig \
  set-external-changelog-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name dc=example,dc=com \
  --add ecl-include-for-deletes:"*" \
  --add ecl-include-for-deletes:"+" \
  --trustAll \
  --no-prompt
```

Procedure 8.16. To Limit External Change Log Content

You can limit external change log content by disabling the domain for a base DN. By default, `cn=schema` and `cn=admin` data are not enabled.

- Prevent OpenDJ from logging changes by disabling the domain:

```
$ dsconfig \
  set-external-changelog-domain-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --provider-name "Multimaster Synchronization" \
  --domain-name dc=example,dc=com \
  --set enabled:false \
  --trustAll \
  --no-prompt
```

Procedure 8.17. To Align Draft Change Numbers

The external change log can be used by applications that follow the *Internet-Draft: Definition of an Object Class to Hold LDAP Change Records*, and that cannot use change log cookies shared across the replication topology. Nothing special is required to get the objects specified for this legacy format, but there are steps you must perform to align change numbers across replicas.

Change numbers described in the Internet-Draft are simple numbers, not cookies. When change log numbers are aligned across replicas, applications fail over from one replica to another when necessary.

If you do not align the change numbers, each server keeps its own count. The same change numbers can refer to different changes on different replicas.

For example, if you install a new replica and initialize replication from an existing server, the last change numbers are likely to differ. The following example shows different last change numbers for an existing server and for a new replica that has just been initialized from the existing replica:

```
$ ldapsearch \  
--hostname existing.example.com \  
--port 1389 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--baseDN "" \  
--searchScope base \  
"(&)" lastChangeNumber  
dn:  
lastChangeNumber: 285924
```

Result Code: 0 (Success)

```
$ ldapsearch \  
--hostname new.example.com \  
--port 1389 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--baseDN "" \  
--searchScope base \  
"(&)" lastChangeNumber  
dn:  
lastChangeNumber: 198643
```

Result Code: 0 (Success)

When you add a new replica to an existing topology, follow these steps to align the change numbers with those of an existing server.

These steps can also be used at any time to align the change numbers:

1. Make sure that the new replica has the same replication configuration as the existing replica.

Specifically, both replicas must replicate the same suffixes in order for the change number calculations to be the same on both replicas. If the suffix configurations differ, the change numbers cannot be aligned.

2. If you must start the new replica's change numbering from a specific change, determine the changeNumber to use.

The changeNumber must be from a change that has not yet been purged according to the replication purge delay, which by default is three days.

3. Using the **dsreplication** command installed with the new replica, reset the change number on the new replica to the change number from the existing replica.

The following example does not specify the change number to use. By default, the new replica uses the last change number from the existing replica:


```
$ dsreplication \  
  reset-change-number \  
  --adminUID admin \  
  --adminPassword password \  
  --hostSource existing.example.com \  
  --portSource 4444 \  
  --hostDestination new.example.com \  
  --portDestination 4444 \  
  --trustAll \  
  --no-prompt  
  
Change-log change number reset task has finished successfully.  
  
See /path/to/opensdj-replication-....log  
for a detailed log of this operation.
```

At this point, the new replica's change log starts with the last change number from the existing replica. Earlier change numbers are no longer present in the new replica's change log.

8.5 Recovering From User Error

Changes to a replicated OpenDJ directory service are similar to those made with the Unix **rm** command, but with a twist. With the **rm** command, if you make a mistake you can restore your files from backup, and lose only the work done since the last backup. If you make a mistake with an update to the directory service however, then after you restore a server from backup, replication efficiently replays your mistake to the server you restored.

There is more than one way to recover from user error. None of the ways involve simply changing OpenDJ settings. All of the ways instead involve manually fixing mistakes.

Consider these alternatives:

- Encourage client applications to provide end users with undo capability if necessary. In this case, client applications take responsibility for keeping an undo history.
- Maintain a record of each update to the service, so that you can manually "undo" mistakes.

You can use the external change log. A primary advantage to the external change log is that the change log is enabled with replication, and so it does not use additional space.

See [Section 8.4, "Change Notification For Your Applications"](#) for instructions on enabling, using, and configuring the external change log. In particular, see

[Procedure 8.15, "To Include Unchanged Attributes in the External Change Log"](#) for instructions on saving not only what is changed, but also all attributes when an entry is deleted.

OpenDJ also provides a file-based audit log, but the audit log does not help with a general solution in this case. The OpenDJ audit log records changes to the data. When you delete an entry however, the audit log does not record the entry before deletion. The following example shows the audit log records of some changes made to Barbara Jensen's entry:

```
# 30/Apr/2014:16:23:29 +0200; conn=7; op=10
dn: uid=bjensen,ou=People,dc=example,dc=com
changetype: modify
replace: description
description: This is the description I want.
-
replace: modifiersName
modifiersName: cn=Directory Manager,cn=Root DNs,cn=config
-
replace: modifyTimestamp
modifyTimestamp: 20140430142329Z

# 30/Apr/2014:16:23:46 +0200; conn=7; op=14
dn: uid=bjensen,ou=People,dc=example,dc=com
changetype: modify
replace: description
description: I never should have changed this!
-
replace: modifiersName
modifiersName: cn=Directory Manager,cn=Root DNs,cn=config
-
replace: modifyTimestamp
modifyTimestamp: 20140430142346Z

# 30/Apr/2014:16:24:53 +0200; conn=7; op=27
dn: uid=bjensen,ou=People,dc=example,dc=com
changetype: delete
```

You can use these records to fix the mistaken update to the description, but the audit log lacks the information needed to restore Barbara Jensen's deleted entry.

- For administrative errors that involve directory data, if you have properly configured the external change log, then use it.

If not, an alternative technique consists of restoring backup to a separate server not connected to the replication topology. (Do not connect the server to the topology as replication replays mistakes, too.) Compare data on the separate restored server to the live servers in the topology, and then fix the mistakes manually.

A more drastic alternative consists of rebuilding the entire service from backup, by disabling replication and restoring all servers from backup (or restoring one server and initializing all servers from that one). This alternative is only recommended in the case of a major error where you have a very fresh backup (taken immediately before the error), and no client applications are affected.

- For administrative configuration errors that prevent servers from starting, know that OpenDJ keeps a copy of the last configuration that OpenDJ could use to start the server in the file `/path/to/openssl/config/config.ldif.startok`.

OpenDJ also backs up earlier versions of the configuration under `/path/to/openssl/config/archived-configs/`.

You can therefore compare the current configuration with the earlier configurations, and repair mistakes manually (avoiding trailing white space at the end of LDIF lines) while the server is down.

Chapter 9

Backing Up and Restoring Data

This chapter covers management of directory data backup archives. For information on managing directory data in an interoperable format that is portable between directory server products, see [Chapter 4, "Importing and Exporting LDIF Data"](#) instead. In this chapter you will learn to:

- Create backup archives
- Restore data from backup archives

OpenDJ lets you back up and restore your data either in compressed, binary format, or in LDIF. This chapter shows you how to back up and to restore OpenDJ data from archives, and explains portability of backup archives, as well as backing up server configuration information.

9.1 Backing Up Directory Data

A `bak/` directory is provided when you install OpenDJ, as a location to save binary backups. When you create a backup, the `bak/backup.info` contains information about the archive.

Archives produced by the **backup** command contain backups only of the directory data. Backups of server configuration are found in `config/archived-configs/`.

This section includes the following procedures:

- [Procedure 9.1, "To Back Up Data Immediately"](#)

- [Procedure 9.2, "To Schedule Data Backup"](#)
- [Procedure 9.3, "To Schedule Incremental Data Backup"](#)

Procedure 9.1. To Back Up Data Immediately

To perform online backup, you start backup as a task by connecting to the administrative port and authenticating as a user with the backend-backup privilege, and also setting a start time for the task by using the `--start` option.

To perform offline backup when OpenDJ directory server is stopped, you run the **backup** command, described in `backup(1)` in the *OpenDJ Reference*, without connecting to the server, authenticating, or requesting a backup task.

- Use one of the following alternatives:
 - Back up only the database for Example.com, where the data is stored in the backend named `userRoot`.

The following example requests an online backup task that starts immediately, backing up only the `userRoot` backend:

```
$ backup \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--backendID userRoot \  
--backupDirectory /path/to/openssl/bak \  
--start 0  
Backup task 20110613143715983 scheduled to start Jun 13, 2011 2:37:15 PM CEST
```

- Stop the server to back up Example.com data offline.

The following example stops OpenDJ, runs offline backup, and starts the server after backup has completed:

```
$ stop-ds
Stopping Server...

[13/Jun/2011:14:31:00 +0200] category=BACKEND severity=NOTICE msgID=9896306
msg=The backend userRoot is now taken offline
[13/Jun/2011:14:31:00 +0200] category=CORE severity=NOTICE msgID=458955
msg=The Directory Server is now stopped
$ backup --backendID userRoot -d /path/to/opensl/bak
[13/Jun/2011:14:33:48 +0200] category=TOOLS severity=NOTICE msgID=10944792
msg=Starting backup for backend userRoot
...
[13/Jun/2011:14:33:48 +0200] category=TOOLS severity=NOTICE msgID=10944795
msg=The backup process completed successfully
$ start-ds
... The Directory Server has started successfully
```

- Back up all user data on the server.

The following example requests an online backup task that starts immediately, backing up all backends:

```
$ backup \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--backUpAll \
--backupDirectory /path/to/opensl/bak \
--start 0
Backup task 20110613143801866 scheduled to start Jun 13, 2011 2:38:01 PM CEST
```

Procedure 9.2. To Schedule Data Backup

You can schedule online data backup using **crontab** format.

- Back up all user data every night at 2 AM, and notify diradmin@example.com when finished, or on error:

```
$ backup \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--backUpAll \
--backupDirectory /path/to/opensl/bak \
--recurringTask "00 02 * * *" \
--completionNotify diradmin@example.com \
--errorNotify diradmin@example.com
Recurring Backup task BackupTask-988d6adf-4d65-44bf-8546-6ea74a2480b0
scheduled successfully
```

Procedure 9.3. To Schedule Incremental Data Backup

You can schedule an incremental backup by using the `--incremental` option. If you do not set the `--incrementalBaseID` option, then OpenDJ increments based on the last backup taken.

- Back up userRoot backend data incrementally every night at 3 AM, and notify `diradmin@example.com` when finished, or on error:

```
$ backup \  
--port 4444 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--backupDirectory /path/to/openssl/bak \  
--backendID userRoot \  
--incremental \  
--recurringTask "00 03 * * *" \  
--completionNotify diradmin@example.com \  
--errorNotify diradmin@example.com  
Recurring Backup task BackupTask-6988c19d-9afc-4f50-89b7-d3e167255d3e  
scheduled successfully
```

9.2 Restoring Directory Data From Backup

When you restore data, the procedure to follow depends on whether the OpenDJ directory server is replicated.

Procedure 9.4. To Restore a Stand-alone Server

To restore OpenDJ when the server is online, you start a restore task by connecting to the administrative port and authenticating as a user with the `backend-restore` privilege, and also setting a start time for the task by using the `--start` option.

To restore data when OpenDJ directory server is stopped, you run the **restore** command, described in `restore(1)` in the *OpenDJ Reference*, without connecting to the server, authenticating, or requesting a restore task.

- Use one of the following alternatives:
 - Stop the server to restore data for Example.com.

The following example stops OpenDJ, restores data offline from one of the available backups, and then starts the server after the restore is complete:


```
$ stop-ds
Stopping Server...

[13/Jun/2011:15:44:06 +0200] category=BACKEND severity=NOTICE msgID=9896306
msg=The backend userRoot is now taken offline
[13/Jun/2011:15:44:06 +0200] category=CORE severity=NOTICE msgID=458955
msg=The Directory Server is now stopped
$ restore --backupDirectory /path/to/opendj/bak --listBackups
Backup ID:      20110613080032
Backup Date:    13/Jun/2011:08:00:45 +0200
Is Incremental: false
Is Compressed:  false
Is Encrypted:   false
Has Unsigned Hash: false
Has Signed Hash: false
Dependent Upon: none
$ restore --backupDirectory /path/to/opendj/bak --backupID 20110613080032
[13/Jun/2011:15:47:41 +0200] ... msg=Restored: 00000000.jdb (size 341835)
$ start-ds
... The Directory Server has started successfully
```

- Schedule the restore as a task to begin immediately.

The following example requests an online restore task, scheduled to start immediately:

```
$ restore \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--backupDirectory /path/to/opendj/bak \
--backupID 20110613080032 \
--start 0
Restore task 20110613155052932 scheduled to start Jun 13, 2011 3:50:52 PM CEST
```

Procedure 9.5. To Restore a Replica

After you restore a replica from backup, replication brings the replica up to date with changes that happened after you created the backup. In order to bring the replica up to date, replication must apply changes that happened after the backup was made. Replication uses internal change log records to determine what changes to apply.

Internal change log records are not kept forever, though. Replication is configured to purge the change log of old changes, preventing the log from growing indefinitely. Yet, for replication to determine what changes to apply to a restored replica, it must find change log records dating back at least to the last change in the backup. In other words, replication can bring the restored replica

up to date *as long as the change log records used to determine which changes to apply have not been purged.*

Therefore, when you restore a replicated server from backup, make sure the backup you use is newer than the last purge of the replication change log (default: 3 days). If all your backups are older than the replication purge delay, do not restore from a backup, but instead initialize a new replica as described in [Section 8.3.2, "Initializing Replicas"](#).

- Restore the server database from the backup archive that you are sure is newer than the last purge of the replication change log:

```
$ stop-ds
Stopping Server...

[13/Jun/2011:15:44:06 +0200] category=BACKEND severity=NOTICE msgID=9896306
msg=The backend userRoot is now taken offline
[13/Jun/2011:15:44:06 +0200] category=CORE severity=NOTICE msgID=458955
msg=The Directory Server is now stopped
$ restore --backupDirectory /path/to/openssl/bak --listBackups
Backup ID:      20110613080032
Backup Date:    13/Jun/2011:08:00:45 +0200
Is Incremental: false
Is Compressed:  false
Is Encrypted:   false
Has Unsigned Hash: false
Has Signed Hash: false
Dependent Upon: none
$ restore --backupDirectory /path/to/openssl/bak --backupID 20110613080032
[13/Jun/2011:15:47:41 +0200] ... msg=Restored: 00000000.jdb (size 341835)
$ start-ds
... The Directory Server has started successfully
```

Chapter 10

Configuring Password Policy

This chapter covers password policy including examples for common use cases. In this chapter you will learn to:

- Decide what type of password policy is needed
- Discover which password policy applies for a given user
- Configure server-based and subentry-based password policies
- Assign password policies to users and to groups
- Configure automated password generation, password storage schemes, and validation of new passwords to reject invalid passwords before they are set

If you want to synchronize password policy across your organization and your applications go to the directory for authentication, then the directory can be a good place to enforce your password policy uniformly. Even if you do not depend on the directory for all your password policy, you no doubt still want to consider directory password policy if only to choose the appropriate password storage scheme.

10.1 About OpenDJ Password Policies

OpenDJ password policies govern not only passwords, but also account logout, and how OpenDJ provides notification about account status.

OpenDJ supports password policies as part of the server configuration, and also subentry password policies as part of the (replicated) user data.

10.1.1 Server-Based Password Policies

You manage server-based password policies in the OpenDJ configuration by using the **dsconfig** command. As they are part of the server configuration, such password policies are not replicated. You must instead apply password policy configuration updates to each replica in your deployment.

By default, OpenDJ includes two password policy configurations, one default for all users, and another for directory root DN users, such as `cn=Directory Manager`. You can see all the default password policy settings using the **dsconfig** command as follows:

```
$ dsconfig \
get-password-policy-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Default Password Policy" \
--advanced
Property                                : Value(s)
-----
account-status-notification-handler      : -
allow-expired-password-changes          : false
allow-multiple-password-values           : false
allow-pre-encoded-passwords             : false
allow-user-password-changes             : true
default-password-storage-scheme         : Salted SHA-1
deprecated-password-storage-scheme       : -
expire-passwords-without-warning        : false
force-change-on-add                     : false
force-change-on-reset                   : false
grace-login-count                       : 0
idle-lockout-interval                   : 0 s
last-login-time-attribute                : -
last-login-time-format                  : -
lockout-duration                        : 0 s
lockout-failure-count                   : 0
lockout-failure-expiration-interval      : 0 s
max-password-age                        : 0 s
max-password-reset-age                  : 0 s
min-password-age                        : 0 s
password-attribute                      : userpassword
password-change-requires-current-password : false
password-expiration-warning-interval     : 5 d
password-generator                      : Random Password Generator
password-history-count                  : 0
password-history-duration                : 0 s
password-validator                      : -
previous-last-login-time-format         : -
require-change-by-time                  : -
require-secure-authentication           : false
require-secure-password-changes         : false
skip-validation-for-administrators       : false
state-update-failure-policy              : reactive
```

For detailed descriptions of each property, see the section called “Password Policy” in the *OpenDJ Reference*.

Notice that many capabilities are not set by default: no lockout, no password expiration, no multiple passwords, no password validator to check that passwords contain the appropriate mix of characters. This means that if you decide to use the directory to enforce password policy, you must configure at least the default password policy to meet your needs.

Yet a few basic protections are configured by default. When you import LDIF with userPassword values, OpenDJ hashes the values before storing them. When a user provides a password value during a bind for example, the server hashes the

value provided to compared it with the stored value. Even the directory manager cannot see the plain text value of a user's password:

```
$ ldapsearch \  
--port 1389 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--baseDN dc=example,dc=com \  
uid=bjensen \  
userpassword  
dn: uid=bjensen,ou=People,dc=example,dc=com  
userpassword: {SSHA}QWAtw8ch/9850HNFRqLNMIQc1YhxCn0oGmk1g==
```

In addition, users can change their passwords provided you have granted them access to do so. OpenDJ uses the `userPassword` attribute to store passwords by default, rather than the `authPassword` attribute, which is designed to store passwords hashed by the client application.

10.1.2 Subentry-Based Password Policies

You manage subentry password policies by adding the subentries alongside the user data. Thus, OpenDJ can replicate subentry password policies across servers.

Subentry password policies support the Internet-Draft [Password Policy for LDAP Directories](#) (version 09). A subentry password policy effectively overrides settings in the default password policy defined in the OpenDJ configuration. Settings not supported or not included in the subentry password policy are thus inherited from the default password policy.

As a result, the following Internet-Draft password policy attributes override the default password policy when you set them in the subentry:

- `pwdAllowUserChange`, corresponding to the OpenDJ password policy property `allow-user-password-changes`
- `pwdMustChange`, corresponding to the OpenDJ password policy property `force-change-on-reset`
- `pwdGraceAuthNLimit`, corresponding to the OpenDJ password policy property `grace-login-count`
- `pwdLockoutDuration`, corresponding to the OpenDJ password policy property `lockout-duration`
- `pwdMaxFailure`, corresponding to the OpenDJ password policy property `lockout-failure-count`
- `pwdFailureCountInterval`, corresponding to the OpenDJ password policy property `lockout-failure-expiration-interval`

- `pwdMaxAge`, corresponding to the OpenDJ password policy property `max-password-age`
- `pwdMinAge`, corresponding to the OpenDJ password policy property `min-password-age`
- `pwdAttribute`, corresponding to the OpenDJ password policy property `password-attribute`
- `pwdSafeModify`, corresponding to the OpenDJ password policy property `password-change-requires-current-password`
- `pwdExpireWarning`, corresponding to the OpenDJ password policy property `password-expiration-warning-interval`
- `pwdInHistory`, corresponding to the OpenDJ password policy property `password-history-count`

The following Internet-Draft password policy attributes are not taken into account by OpenDJ:

- `pwdCheckQuality`, as OpenDJ has password validators. You can set password validators to use in the default password policy.
- `pwdMinLength`, as this is handled by the length-based password validator. You can configure this as part of the default password policy.
- `pwdLockout`, as OpenDJ can deduce whether lockout is configured based on the values of other lockout-related password policy attributes.

Values of the following properties are inherited from the default password policy for Internet-Draft based password policies:

- `account-status-notification-handlers`
- `allow-expired-password-changes`
- `allow-multiple-password-values`
- `allow-pre-encoded-passwords`
- `default-password-storage-schemes`
- `deprecated-password-storage-schemes`
- `expire-passwords-without-warning`
- `force-change-on-add`

- `idle-lockout-interval`
- `last-login-time-attribute`
- `last-login-time-format`
- `max-password-reset-age`
- `password-generator`
- `password-history-duration`
- `password-validators`
- `previous-last-login-time-formats`
- `require-change-by-time`
- `require-secure-authentication`
- `require-secure-password-changes`
- `skip-validation-for-administrators`
- `state-update-failure-policy`

If you would rather specify password validators for your policy, you can configure password validators for a subentry password policy by adding the auxiliary object class `pwdValidatorPolicy` and setting the multi-valued attribute, `ds-cfg-password-validator`, to the DN of the password validator configuration entries.

The following example shows a subentry password policy that references two password validator configuration entries. The Character Set password validator determines whether a proposed password is acceptable by checking whether it contains a sufficient number of characters from one or more user-defined character sets and ranges. The length-based password validator determines whether a proposed password is acceptable based on whether the number of characters it contains falls within an acceptable range of values. Both are enabled in the default OpenDJ directory server configuration:


```
dn: cn=Subentry Password Policy with Validators,dc=example,dc=com
objectClass: top
objectClass: subentry
objectClass: pwdPolicy
objectClass: pwdValidatorPolicy
cn: Subentry Password Policy with Validators
pwdAttribute: userPassword
pwdLockout: TRUE
pwdMaxFailure: 3
pwdFailureCountInterval: 300
pwdLockoutDuration: 300
pwdAllowUserChange: TRUE
pwdSafeModify: TRUE
ds-cfg-password-validator: cn=Character Set,cn=Password Validators,cn=config
ds-cfg-password-validator: cn=Length-Based Password Validator,
    cn=Password Validators,cn=config
subtreeSpecification: {base "ou=people", specificationFilter
    "(isMemberOf=cn=Directory Administrators,ou=Groups,dc=example,dc=com)" }
```

If a referenced password validator cannot be found, then OpenDJ directory server logs an error message when the password policy is invoked. This can occur, for example, when a subentry password policy is replicated to a directory server where the password validator is not (yet) configured. In that case when a user attempts to change their password, the server fails to find the referenced password validator.

See also [Procedure 10.3, "To Create a Subentry-Based Password Policy"](#).

10.1.3 Applying Password Policies to Users

The password policy that applies to a user is identified by the operational attribute, `pwdPolicySubentry`:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com uid=bjensen pwdPolicySubentry
dn: uid=bjensen,ou=People,dc=example,dc=com
pwdPolicySubentry: cn=Default Password Policy,cn=Password Policies,cn=config
```

10.2 Configuring Password Policies

You configure server-based password policies by using the **dsconfig** command. Notice that server-based password policies are part of the server configuration, and therefore not replicated. Alternatively, you can configure a subset of password policy features by using subentry-based password policies that are stored with the replicated server data. This section covers both server-based and subentry-based password policies.

Procedure 10.1. To Adjust the Default Password Policy

You can reconfigure the default password policy, for example, to enforce password expiration, check that passwords do not match dictionary words, and prevent password reuse. This default policy is a server-based password policy.

1. Enable the appropriate password validator:

```
$ dsconfig \
  set-password-validator-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --validator-name Dictionary \
  --set enabled:true \
  --set check-substrings:true \
  --set min-substring-length:4 \
  --trustAll \
  --no-prompt
```

2. Apply the changes to the default password policy:

```
$ dsconfig \
  set-password-policy-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --policy-name "Default Password Policy" \
  --set max-password-age:90d \
  --set min-password-age:4w \
  --set password-history-count:7 \
  --set password-validator:Dictionary \
  --trustAll \
  --no-prompt
```

3. Check your work:

```
$ dsconfig \
  get-password-policy-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --policy-name "Default Password Policy"
Property                                     : Value(s)
-----
account-status-notification-handler          : -
allow-expired-password-changes              : false
allow-user-password-changes                : true
default-password-storage-scheme             : Salted SHA-1
deprecated-password-storage-scheme          : -
expire-passwords-without-warning            : false
force-change-on-add                         : false
force-change-on-reset                      : false
grace-login-count                           : 0
idle-lockout-interval                       : 0 s
last-login-time-attribute                   : -
last-login-time-format                     : -
lockout-duration                           : 0 s
lockout-failure-count                      : 0
lockout-failure-expiration-interval         : 0 s
max-password-age                           : 12 w 6 d
max-password-reset-age                     : 0 s
min-password-age                           : 4 w
password-attribute                         : userpassword
password-change-requires-current-password  : false
password-expiration-warning-interval        : 5 d
password-generator                         : Random Password Generator
password-history-count                     : 7
password-history-duration                   : 0 s
password-validator                         : Dictionary
previous-last-login-time-format            : -
require-change-by-time                     : -
require-secure-authentication              : false
require-secure-password-changes            : false
```

Procedure 10.2. To Create a Server-Based Password Policy

You can add a password policy, for example, for new users who have not yet used their credentials to bind.

1. Create the new password policy:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "New Account Password Policy" \
--set default-password-storage-scheme:"Salted SHA-1" \
--set force-change-on-add:true \
--set password-attribute:userPassword \
--type password-policy \
--trustAll \
--no-prompt
```

2. Check your work:

```
$ dsconfig \
get-password-policy-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "New Account Password Policy"
Property                                : Value(s)
-----
account-status-notification-handler      : -
allow-expired-password-changes           : false
allow-user-password-changes              : true
default-password-storage-scheme          : Salted SHA-1
deprecated-password-storage-scheme       : -
expire-passwords-without-warning         : false
force-change-on-add                      : true
force-change-on-reset                    : false
grace-login-count                        : 0
idle-lockout-interval                    : 0 s
last-login-time-attribute                 : -
last-login-time-format                   : -
lockout-duration                         : 0 s
lockout-failure-count                    : 0
lockout-failure-expiration-interval       : 0 s
max-password-age                         : 0 s
max-password-reset-age                   : 0 s
min-password-age                         : 0 s
password-attribute                       : userpassword
password-change-requires-current-password : false
password-expiration-warning-interval      : 5 d
password-generator                       : -
password-history-count                   : 0
password-history-duration                 : 0 s
password-validator                       : -
previous-last-login-time-format           : -
require-change-by-time                   : -
require-secure-authentication             : false
require-secure-password-changes           : false
```

If you use a password policy like this, you might want to change the user's policy again when the new user successfully updates the password.

Procedure 10.3. To Create a Subentry-Based Password Policy

You can add a subentry to configure a password policy that applies to Directory Administrators.

1. Create the entry that specifies the password policy:

```
$ cat /path/to/subentry-pwp.ldif
dn: cn=Subentry Password Policy,dc=example,dc=com
objectClass: top
objectClass: subentry
objectClass: pwdPolicy
cn: Subentry Password Policy
pwdAttribute: userPassword
pwdLockout: TRUE
pwdMaxFailure: 3
pwdFailureCountInterval: 300
pwdLockoutDuration: 300
pwdAllowUserChange: TRUE
pwdSafeModify: TRUE
subtreeSpecification: {base "ou=people", specificationFilter
  "(isMemberOf=cn=Directory Administrators,ou=Groups,dc=example,dc=com)" }
```

2. Add the policy to the directory:

```
$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename /path/to/subentry-pwp.ldif
Processing ADD request for cn=Subentry Password Policy,dc=example,dc=com
ADD operation successful for DN cn=Subentry Password Policy,dc=example,dc=com
```

3. Check that the policy applies as specified.

In the example, the policy should apply to a Directory Administrator, while a normal user has the default password policy. Here, Kirsten Vaughan is a member of the Directory Administrators group, and Babs Jensen is not a member:

```
$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
uid=kvaughan \
pwdPolicySubentry
dn: uid=kvaughan,ou=People,dc=example,dc=com
pwdPolicySubentry: cn=Subentry Password Policy,dc=example,dc=com

$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
uid=bjensen \
pwdPolicySubentry
dn: uid=bjensen,ou=People,dc=example,dc=com
pwdPolicySubentry: cn=Default Password Policy,cn=Password Policies,cn=config
```

10.3 Assigning Password Policies

You assign subentry-based password policies for a subtree of the DIT by adding the policy to an LDAP subentry whose immediate superior is the root of the subtree. In other words you can add the subtree based password policy under `ou=People,dc=example,dc=com`, to have it apply to all entries under `ou=People,dc=example,dc=com`. You can further use the capabilities of LDAP [subentries](#) to refine the scope of application.

You assign server-based password policies by using the `ds-pwp-password-policy-dn` attribute.

Procedure 10.4. To Assign a Password Policy to a User

1. Prevent users from selecting their own password policy:

```
$ cat protectpwp.ldif
dn: ou=People,dc=example,dc=com
changetype: modify
add: aci
aci: (target ="ldap:///uid=*,ou=People,dc=example,dc=com")(targetattr =
"ds-pwp-password-policy-dn")(version 3.0;acl "Cannot choose own pass
word policy";deny (write)(userdn = "ldap:///self");)

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename protectpwp.ldif
Processing MODIFY request for ou=People,dc=example,dc=com
MODIFY operation successful for DN ou=People,dc=example,dc=com
```

2. Update the user's ds-pwp-password-policy-dn attribute:

```
$ cat newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: changeme
ds-pwp-password-policy-dn: cn=New Account Password Policy,cn=Password Policies,
cn=config

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename newuser.ldif
Processing ADD request for uid=newuser,ou=People,dc=example,dc=com
ADD operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

3. Check your work:

```
$ ldapsearch \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--baseDN dc=example,dc=com \
uid=newuser \
pwdPolicySubentry
dn: uid=newuser,ou=People,dc=example,dc=com
pwdPolicySubentry: cn=New Account Password Policy,cn=Password Policies,cn=config
```

Procedure 10.5. To Assign a Password Policy to a Group

1. Create a subentry defining the collective attribute that sets the ds-pwp-password-policy-dn attribute for group members' entries:

```
$ cat pwp-coll.ldif
dn: cn=Password Policy for Dir Admins,dc=example,dc=com
objectClass: collectiveAttributeSubentry
objectClass: extensibleObject
objectClass: subentry
objectClass: top
cn: Password Policy for Dir Admins
ds-pwp-password-policy-dn;collective: cn=Root Password Policy,cn=Password Policies,cn=config
subtreeSpecification: { base "ou=People", specificationFilter "(isMemberOf=cn=Directory Administrators,ou=Groups,dc=example,dc=com)"}

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename pwp-coll.ldif
Processing ADD request for cn=Password Policy for Dir Admins,dc=example,dc=com
ADD operation successful for DN cn=Password Policy for Dir Admins,dc=example,dc=com
```

2. Check your work:

```
$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
uid=kvaughan \
pwdPolicySubentry
dn: uid=kvaughan,ou=People,dc=example,dc=com
pwdPolicySubentry: cn=Root Password Policy,cn=Password Policies,cn=config
```

Procedure 10.6. To Assign Password Policy for an Entire Branch

You can use a collective attribute to assign a password policy to the entries under a base DN.

1. Create a password policy and collective attribute subentry to assign the policy to all entries under a base DN.

The following example creates a password policy, and then assigns that policy to entries under `ou=People,dc=example,dc=com`:


```
$ cat collective-pwp.ldif
dn: cn=People Password Policy,dc=example,dc=com
objectClass: top
objectClass: subentry
objectClass: pwdPolicy
cn: People Password Policy
pwdAttribute: userPassword
pwdLockout: TRUE
pwdMaxFailure: 3
pwdFailureCountInterval: 300
pwdLockoutDuration: 300
pwdAllowUserChange: TRUE
pwdSafeModify: TRUE
subtreeSpecification: {}

dn: cn=Assign People Password Policy,dc=example,dc=com
objectClass: top
objectClass: subentry
objectClass: extensibleObject
objectClass: collectiveAttributeSubentry
cn: Assign People Password Policy
ds-pwp-password-policy-dn;collective: cn=People Password Policy,dc=example,dc=com
subtreeSpecification: { base "ou=people" }

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename collective-pwp.ldif
Processing ADD request for cn=People Password Policy,dc=example,dc=com
ADD operation successful for DN cn=People Password Policy,dc=example,dc=com
Processing ADD request for cn=Assign People Password Policy,dc=example,dc=com
ADD operation successful for DN
cn=Assign People Password Policy,dc=example,dc=com
```

Notice the subtree specification used to assign the policy, { base "ou=people" }. You can relax the subtree specification value to {} to apply the password policy to all entries the parent of the subentry, dc=example,dc=com, or further restrict the subtree specification by adding a specificationFilter. See Section 5.2, “Collective Attributes” in the *OpenDJ Directory Server Developer's Guide* for more information.

2. Check your work:

```
$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
"(uid=alutz)" \
pwdPolicySubentry
dn: uid=alutz,ou=People,dc=example,dc=com
pwdPolicySubentry: cn=People Password Policy,dc=example,dc=com
```

If everything is correctly configured, then the password policy should be assigned to users whose entries are under `ou=People,dc=example,dc=com`.

10.4 Configuring Password Generation

Password generators are used by OpenDJ during the [LDAP Password Modify extended operation](#) to construct a new password for the user. In other words, a directory administrator resetting a user's password can have OpenDJ directory server generate the new password by using the `ldappasswordmodify` command, described in `ldappasswordmodify(1)` in the *OpenDJ Reference*:

```
$ ldappasswordmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--authzID "u:bjensen"
The LDAP password modify operation was successful
Generated Password: eak77qdi
```

The default password policy shown in [Procedure 10.1, "To Adjust the Default Password Policy"](#) uses the Random Password Generator, described in the section called "Random Password Generator" in the *OpenDJ Reference*:

```
$ dsconfig \
get-password-policy-prop \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Default Password Policy" \
--property password-generator
Property          : Value(s)
-----
password-generator : Random Password Generator

$ dsconfig \
get-password-generator-prop \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--generator-name "Random Password Generator" \
--property password-generator
Property          : Value(s)
-----
enabled           : true
password-character-set : alpha:abcdefghijklmnopqrstuvwxyz, numeric:0123456789
password-format    : "alpha:3,numeric:2,alpha:3"
```

Notice that the default configuration for the Random Password Generator defines two password-character-set values, and then uses those definitions in the password-format so that generated passwords have eight characters: three from the alpha set, followed by two from the numeric set, followed by three from the alpha set. The password-character-set name must be ASCII.

To set the password generator that OpenDJ employs when constructing a new password for a user, set the password-generator property for the password policy that applies to the user.

The following example does not change the password policy, but instead changes the Random Password Generator configuration, and then demonstrates a password being generated upon reset:

```
$ dsconfig \
  set-password-generator-prop \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --generator-name "Random Password Generator" \
    --remove password-character-set:alpha:abcdefghijklmnopqrstuvwxyz \
    --add \
      password-character-set:alpha:ABCDEFGHIJKLMNOPQRSTUVWXYZWabcdefghijklmnopqrstuvwxyz \
    --add password-character-set:punct:.,./\`!@#\$%^&*~\;[]\"'\'(\)+=-_~\ \
    --set \
      password-format:alpha:3,punct:1,numeric:2,punct:2,numeric:3,alpha:3,punct:2 \
    --no-prompt

$ ldapmodify \
  --port 1389 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --authzID "u:bjensen"
The LDAP password modify operation was successful
Generated Password: pld^06:)529HTq$'
```

If you also set up a password validator in the password policy as shown in [Procedure 10.1, "To Adjust the Default Password Policy"](#) and further described in [Section 10.6, "Configuring Password Validation"](#), make sure the generated passwords are acceptable to the validator.

10.5 Configuring Password Storage

Password storage schemes, described in `dsconfig create-password-storage-scheme(1)` in the *OpenDJ Reference*, encode new passwords provided by users so that they are stored in an encoded manner. This makes it difficult or impossible to determine the cleartext passwords from the encoded values. Password storage schemes also determine whether a cleartext password provided by a client matches the encoded value stored by the server.

OpenDJ offers a variety of both reversible and one-way password storage schemes. Some schemes make it easy to recover the cleartext password, whereas others aim to make it computationally hard to do so:

```
$ dsconfig \
  list-password-storage-schemes \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password
```

Password Storage Scheme	Type	: enabled
3DES	: triple-des	: true
AES	: aes	: true
Base64	: base64	: true
Blowfish	: blowfish	: true
Clear	: clear	: true
CRYPT	: crypt	: true
MD5	: md5	: true
PBKDF2	: pbkdf2	: true
PKCS5S2	: pkcs5s2	: true
RC4	: rc4	: true
Salted MD5	: salted-md5	: true
Salted SHA-1	: salted-sha1	: true
Salted SHA-256	: salted-sha256	: true
Salted SHA-384	: salted-sha384	: true
Salted SHA-512	: salted-sha512	: true
SHA-1	: sha1	: true

As shown in [Procedure 10.1, "To Adjust the Default Password Policy"](#), the default password storage scheme for users in Salted SHA-1. When you add users or import user entries with userPassword values in cleartext, OpenDJ hashes them with the default password storage scheme. Root DN users have a different password policy by default, shown in [Procedure 10.5, "To Assign a Password Policy to a Group"](#). The Root Password Policy uses Salted SHA-512 by default.

You change the default password policy storage scheme for users by changing the applicable password policy, as shown in the following example:

```
$ dsconfig \
  set-password-policy-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --policy-name "Default Password Policy" \
  --set default-password-storage-scheme:pbkdf2 \
  --no-prompt
```

Notice that the change in default password storage scheme does not cause OpenDJ to update any stored password values. By default, OpenDJ only stores

a password with the new storage scheme the next time that the password is changed.

OpenDJ prefixes passwords with the scheme used to encode them, which means it is straightforward to see which password storage scheme is in use. After the default password storage scheme is changed to PBKDF2, old user passwords remain encoded with Salted SHA-1:

```
$ ldapsearch \
--port 1389 \
--bindDN uid=bjensen,ou=people,dc=example,dc=com \
--bindPassword hifalutin \
--baseDN dc=example,dc=com \
"(uid=bjensen)" userPassword
dn: uid=bjensen,ou=People,dc=example,dc=com
userPassword: {SSHA}Rc3tkAjlqP5zGiRkwDIWDFxrxpGg08Fwh3aibg==
```

When the password is changed, the new default password storage scheme takes effect, as shown in the following example:

```
$ ldappasswordmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--authzID "u:bjensen" \
--newPassword changeit
The LDAP password modify operation was successful

$ ldapsearch \
--port 1389 \
--bindDN uid=bjensen,ou=people,dc=example,dc=com \
--bindPassword changeit \
--baseDN dc=example,dc=com \
"(uid=bjensen)" userPassword
dn: uid=bjensen,ou=People,dc=example,dc=com
userPassword: {PBKDF2}10000:03V6G7y7n7Aef0kRGNKQ5ukrMu05uf+iEQ9ZLg==
```

When you change the password storage scheme for users, realize that the user passwords must change in order for OpenDJ to encode them with the chosen storage scheme. If you are changing the storage scheme because the old scheme was too weak, then you no doubt want users to change their passwords anyway.

If, however, the storage scheme change is not related to vulnerability, you can use the deprecated-password-storage-scheme property of the password policy to have OpenDJ store the password in the new format after successful authentication. This makes it possible to do password migration for active users without forcing users to change their passwords:

```

$ ldapsearch \
--port 1389 \
--bindDN uid=kvaughan,ou=people,dc=example,dc=com \
--bindPassword bribery \
--baseDN dc=example,dc=com \
"(uid=kvaughan)" userPassword
dn: uid=kvaughan,ou=People,dc=example,dc=com
userPassword: {SSHA}hDgK44F2GhIIZj913b+29Ak7phb9oU3Lz4ogkg==

$ dsconfig \
set-password-policy-prop \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Default Password Policy" \
--set deprecated-password-storage-scheme:"Salted SHA-1" \
--no-prompt

$ ldapsearch \
--port 1389 \
--bindDN uid=kvaughan,ou=people,dc=example,dc=com \
--bindPassword bribery \
--baseDN dc=example,dc=com \
"(uid=kvaughan)" userPassword
dn: uid=kvaughan,ou=People,dc=example,dc=com
userPassword: {PBKDF2}10000:L4dCYqSsNnf47YZ3a6aC8K2E3DChhHHhpcoUzg==

```

Notice that with `deprecated-password-storage-scheme` set appropriately, Kirsten Vaughan's password was hashed again after she authenticated successfully.

10.6 Configuring Password Validation

Password validators, described in `dsconfig create-password-validator(1)` in the *OpenDJ Reference*, are responsible for determining whether a proposed password is acceptable for use. Validators can run checks like ensuring that the password meets minimum length requirements, that it has an appropriate range of characters, or that it is not in the history of recently used passwords. OpenDJ directory server provides a variety of password validators:

```
$ dsconfig \
  list-password-validators \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password
```

Password Validator	: Type	: enabled
Attribute Value	: attribute-value	: true
Character Set	: character-set	: true
Dictionary	: dictionary	: false
Length-Based Password Validator	: length-based	: true
Repeated Characters	: repeated-characters	: true
Similarity-Based Password Validator	: similarity-based	: true
Unique Characters	: unique-characters	: true

The password policy for a user specifies the set of password validators that should be used whenever that user provides a new password. By default no password validators are configured. You can see an example setting the Default Password Policy to use the Dictionary validator in [Procedure 10.1, "To Adjust the Default Password Policy"](#). The following example shows how to set up a custom password validator and assign it to the default password policy.

The custom password validator ensures passwords meet at least three of the following four criteria. Passwords are composed of:

- English lowercase characters (a through z)
- English uppercase characters (A through Z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, \$, #, %)

Notice how the character-set values are constructed. The initial 0: means the set is optional, whereas 1: would mean the set is required:

```
$ dsconfig \
create-password-validator \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--validator-name "Custom Character Set Password Validator" \
--set allow-unclassified-characters:true \
--set enabled:true \
--set character-set:0:abcdefghijklmnopqrstuvwxyz \
--set character-set:0:ABCDEFGHIJKLMNOPQRSTUVWXYZ \
--set character-set:0:0123456789 \
--set character-set:0:!"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~ \
--set min-character-sets:3 \
--type character-set \
--no-prompt

$ dsconfig \
set-password-policy-prop \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Default Password Policy" \
--set password-validator:"Custom Character Set Password Validator" \
--no-prompt

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--authzID "u:bjensen" \
--newPassword '!ABcd%^'
```

In the preceding example, the character set of ASCII punctuation, `!"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~`, is hard to read because of all the escape characters. In practice it can be easier to enter sequences like that by using **dsconfig** in interactive mode, and letting it do the escaping for you. You can also use the `--commandFilePath {path}` option to save the result of your interactive session to a file for use in scripts later.

An attempt to set an invalid password fails as shown in the following example:

```
$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--authzID "u:bjensen" \
--newPassword hifalutin
The LDAP password modify operation failed with result code 19
Error Message: The provided new password failed the validation checks defined
in the server: The provided password did not contain characters from at least
3 of the following character sets or ranges: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ',
'!"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~', '0123456789', 'abcdefghijklmnopqrstuvwxyz'
```


Validation does not affect existing passwords, but only takes effect when the password is updated.

You can reference password validators from subentry password policies. See [Section 10.1.2, "Subentry-Based Password Policies"](#) for an example.

10.7 Sample Password Policies

The sample password policies in this section demonstrate OpenDJ server-based password policies for several common cases:

- [Example 10.1, "Enforce Regular Password Changes"](#)
- [Example 10.2, "Track Last Login Time"](#)
- [Example 10.3, "Deprecate a Password Storage Scheme"](#)
- [Example 10.4, "Lock Idle Accounts"](#)
- [Example 10.5, "Allow Grace Log In to Change Expired Password"](#)
- [Example 10.6, "Require Password Change on Add or Reset"](#)

Example 10.1. Enforce Regular Password Changes

The following commands configure an OpenDJ server-based password policy that sets age limits on passwords, requiring that they change periodically. It also sets the number of passwords to keep in the password history of the entry, thereby preventing users from reusing the same password on consecutive changes:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Enforce Regular Password Changes" \
--type password-policy \
--set default-password-storage-scheme:"Salted SHA-1" \
--set password-attribute:userPassword \
--set max-password-age:13w \
--set min-password-age:4w \
--set password-history-count:7 \
--trustAll \
--no-prompt
```

See also [Section 10.3, "Assigning Password Policies"](#) for instructions on using the policy.

Example 10.2. Track Last Login Time

The following commands configure an OpenDJ server-based password policy that keeps track of the last successful login.

First, set up an attribute to which OpenDJ directory server can write a timestamp value on successful login. For additional information also see Example 2.6, “Search: Listing Active Accounts” in the *OpenDJ Directory Server Developer's Guide*:

```
$ ldapmodify \  
--port 1389 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password  
dn: cn=schema  
changetype: modify  
add: attributeTypes  
attributeTypes: ( lastLoginTime-oid  
    NAME 'lastLoginTime'  
    DESC 'Last time the user logged in'  
    EQUALITY generalizedTimeMatch  
    ORDERING generalizedTimeOrderingMatch  
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.24  
    SINGLE-VALUE  
    NO-USER-MODIFICATION  
    USAGE directoryOperation  
    X-ORIGIN 'OpenDJ example documentation' )  
  
Processing MODIFY request for cn=schema  
MODIFY operation successful for DN cn=schema
```

Next, create the password policy that causes OpenDJ directory server to write the timestamp to the attribute on successful login:

```
$ dsconfig \  
create-password-policy \  
--port 4444 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--policy-name "Track Last Login Time" \  
--type password-policy \  
--set default-password-storage-scheme:"Salted SHA-1" \  
--set password-attribute:userPassword \  
--set last-login-time-attribute:lastLoginTime \  
--set last-login-time-format:"yyyyMMddHH'Z'" \  
--trustAll \  
--no-prompt
```

See also [Section 10.3, "Assigning Password Policies"](#) for instructions on using the policy.

Example 10.3. Deprecate a Password Storage Scheme

The following commands configure an OpenDJ server-based password policy that you can use when deprecating a password storage scheme. This policy uses elements from [Example 10.1, "Enforce Regular Password Changes"](#), as OpenDJ directory server only employs the new password storage scheme to hash or to encrypt passwords when a password changes:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Deprecate a Password Storage Scheme" \
--type password-policy \
--set deprecated-password-storage-scheme:Crypt \
--set default-password-storage-scheme:"Salted SHA-1" \
--set password-attribute:userPassword \
--set max-password-age:13w \
--set min-password-age:4w \
--set password-history-count:7 \
--trustAll \
--no-prompt
```

See also [Section 10.3, "Assigning Password Policies"](#) for instructions on using the policy.

Example 10.4. Lock Idle Accounts

The following commands configure an OpenDJ server-based password policy that locks idle accounts. This policy extends the example from [Example 10.2, "Track Last Login Time"](#) as OpenDJ directory server must track last successful login time in order to calculate how long the account has been idle. You must first add the `lastLoginTime` attribute type in order for OpenDJ directory server to accept this new password policy:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Lock Idle Accounts" \
--type password-policy \
--set default-password-storage-scheme:"Salted SHA-1" \
--set password-attribute:userPassword \
--set last-login-time-attribute:lastLoginTime \
--set last-login-time-format:"yyyyMMddHH'Z'" \
--set idle-lockout-interval:13w \
--trustAll \
--no-prompt
```

See also [Section 10.3, "Assigning Password Policies"](#), and [Section 11.1, "Configuring Account Lockout"](#).

Example 10.5. Allow Grace Log In to Change Expired Password

The following commands configure an OpenDJ server-based password policy that allows users to log in after their password has expired in order to choose a new password:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Allow Grace Login" \
--type password-policy \
--set default-password-storage-scheme:"Salted SHA-1" \
--set password-attribute:userPassword \
--set grace-login-count:2 \
--trustAll \
--no-prompt
```

See also [Section 10.3, "Assigning Password Policies"](#) for instructions on using the policy.

Example 10.6. Require Password Change on Add or Reset

The following commands configure an OpenDJ server-based password policy that requires new users to change their password after logging in for the first time, and also requires users to change their password after their password is reset:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--policy-name "Require Password Change on Add or Reset" \
--type password-policy \
--set default-password-storage-scheme:"Salted SHA-1" \
--set password-attribute:userPassword \
--set force-change-on-add:true \
--set force-change-on-reset:true \
--trustAll \
--no-prompt
```

See also [Section 10.3, "Assigning Password Policies"](#) for instructions on using the policy.

Chapter 11

Implementing Account Lockout and Notification

This chapter covers configuration of account lockout and account status notification. In this chapter you will learn to:

- Configure password policies to manage account lockout automatically
- Manage lockout with the **manage-account** command
- Set up email notification of account status

OpenDJ directory server supports automatic account lockout. The aim of account lockout is not to punish users who mistype their passwords, but instead to protect the directory against attacks in which the attacker attempts to guess a user password, repeatedly attempting to bind until success is achieved.

Account lockout disables a user account after a specified number of successive authentication failures. When you implement account lockout, you can opt to have OpenDJ directory server unlock the account after a specified interval, or you can leave the account locked until the password is reset.



Note

You configure account lockout as part of password policy. OpenDJ locks an account after the specified number of

consecutive authentication failures. Account lockout is not transactional across a replication topology. Under normal circumstances, replication propagates lockout quickly. If replication is ever delayed, an attacker with direct access to multiple replicas could try to authenticate up to the specified number of times on each replica before being locked out on all replicas.

This chapter shows you how to set up account lockout policies by using the **dsconfig** command, described in `dsconfig(1)` in the *OpenDJ Reference*, and how to intervene manually to lock and unlock accounts by using the **manage-account** command, described in `manage-account(1)` in the *OpenDJ Reference*.

11.1 Configuring Account Lockout

Account lockout is configured as part of password policy. This section demonstrates configuring account lockout as part of the default password policy. Users are allowed three consecutive failures before being locked out for five minutes. Failures themselves also expire after five minutes.

Change the default password policy to activate lockout using the **dsconfig** command. As the password policy is part of the server configuration, you must manually apply the changes to each replica in a replication topology:

```
$ dsconfig \
  set-password-policy-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --policy-name "Default Password Policy" \
  --set lockout-failure-count:3 \
  --set lockout-duration:5m \
  --set lockout-failure-expiration-interval:5m \
  --trustAll \
  --no-prompt
```

Users having the default password policy are then locked out after three failed attempts in succession:


```
$ ldapsearch \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword hifalutin \
--baseDN dc=example,dc=com \
uid=bjensen \
mail
dn: uid=bjensen,ou=People,dc=example,dc=com
mail: bjensen@example.com

$ ldapsearch \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword fatfngrs \
--baseDN dc=example,dc=com \
uid=bjensen \
mail
The simple bind attempt failed
Result Code: 49 (Invalid Credentials)

$ ldapsearch \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword fatfngrs \
--baseDN dc=example,dc=com \
uid=bjensen \
mail
The simple bind attempt failed
Result Code: 49 (Invalid Credentials)

$ ldapsearch \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword fatfngrs \
--baseDN dc=example,dc=com \
uid=bjensen \
mail
The simple bind attempt failed
Result Code: 49 (Invalid Credentials)

$ ldapsearch \
--port 1389 \
--bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
--bindPassword hifalutin \
--baseDN dc=example,dc=com \
uid=bjensen \
mail
The simple bind attempt failed
Result Code: 49 (Invalid Credentials)
```

11.2 Managing Accounts Manually

This section covers disabling and enabling accounts by using the **manage-account** command. Password reset is covered in the chapter on performing LDAP operations.

For the following examples, the directory admin user, Kirsten Vaughan, has `ds-privilege-name: password-reset`, and the following ACI on `ou=People,dc=example,dc=com`:

```
(target="ldap:///ou=People,dc=example,dc=com") (targetattr="*|+")(
  version 3.0;acl "Admins can run amok"; allow(all) groupdn =
  "ldap:///cn=Directory Administrators,ou=Groups,dc=example,dc=com";)
```

Procedure 11.1. To Disable an Account

- Set the account status to disabled with the **manage-account** command:

```
$ manage-account \
  set-account-is-disabled \
  --port 4444 \
  --bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
  --bindPassword bribery \
  --operationValue true \
  --targetDN uid=bjensen,ou=people,dc=example,dc=com \
  --trustAll
Account Is Disabled: true
```

Procedure 11.2. To Activate a Disabled Account

- Clear the disabled status using the **manage-account** command:

```
$ manage-account \
  clear-account-is-disabled \
  --port 4444 \
  --bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
  --bindPassword bribery \
  --targetDN uid=bjensen,ou=people,dc=example,dc=com \
  --trustAll
Account Is Disabled: false
```

11.3 Managing Account Status Notification

OpenDJ can send mail about account status changes. OpenDJ needs an SMTP server to send messages, and needs templates for the mail it sends. By default, message templates are in English, under `/path/to/opendj/config/messages/`.

OpenDJ generates notifications only when OpenDJ writes to an entry or evaluates a user entry for authentication. OpenDJ generates account enabled and account disabled notifications when the user account is enabled or disabled with the

manage-account command, which writes to the entry. OpenDJ generates password expiration notifications when a user tries to bind.

For example, if you set up OpenDJ directory server to send a notification about password expiration, that notification gets triggered when the user authenticates during the password expiration warning interval. OpenDJ directory server does not automatically scan entries to send password expiry notifications. OpenDJ directory server does implement controls that you can pass in an LDAP search to determine whether a user's password is about to expire. See Appendix F, in the *OpenDJ Reference* for a list. You can send notifications based on the results of your search.

Procedure 11.3. To Mail Users About Account Status

The following steps demonstrate how to set up notifications. Whether OpenDJ sends notifications depends on the settings in the password policy, and on account activity as described above.

1. Identify the SMTP server to which OpenDJ sends messages:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set smtp-server:smtp.example.com \
  --trustAll \
  --no-prompt
```

2. Set up OpenDJ to be able to mail users about account status:

```
$ dsconfig \
  set-account-status-notification-handler-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "SMTP Handler" \
  --set enabled:true \
  --set email-address-attribute-type:mail \
  --trustAll \
  --no-prompt
```

Notice that OpenDJ finds the user's mail address on the attribute on the user's entry, specified by `email-address-attribute-type`.

You can also configure the `message-subject` and `message-template-file` properties. Try interactive mode if you plan to do so.

You find templates for messages by default under the `config/messages` directory. You can edit the templates to suit your purposes.

3. Adjust applicable password policies to use the account status notification handler you configured:

```
$ dsconfig \
  set-password-policy-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --policy-name "Default Password Policy" \
  --set account-status-notification-handler:"SMTP Handler" \
  --trustAll \
  --no-prompt
```

About Notification Message Templates

When editing the `config/messages` templates to suit your purposes, you can use the following tokens to have OpenDJ update the message text dynamically.

`%%notification-type%%`

This token is replaced with the name of the account status notification type for the notification.

`%%notification-message%%`

This token is replaced with the message for the account status notification.

`%%notification-user-dn%%`

This token is replaced with the string representation of the DN for the user who is the target of the account status notification.

`%%notification-user-attr:attrname%%`

This token is replaced with the value of the attribute specified by *attrname* from the user's entry. If the specified attribute has multiple values, then OpenDJ uses the first value encountered. If the specified attribute does not have any values, then OpenDJ replaces it with an empty string.

`%%notification-property:propname%%`

This token is replaced with the value of the specified notification property from the account status notification. If the specified property has multiple values, then OpenDJ uses the first value encountered. If the specified property does not have any values, then OpenDJ replaces it with an empty string. Valid *propname* values include the following:

- `account-unlock-time`

- new-password
- old-password
- password-expiration-time
- password-policy-dn
- seconds-until-expiration
- seconds-until-unlock
- time-until-expiration
- time-until-unlock

Chapter 12

Setting Resource Limits

This chapter shows you how to set resource limits that prevent directory clients from using an unfair share of system resources. In this chapter you will learn to:

- Limit the resources used when a user searches the directory
- Limit how long connections can remain idle before they are dropped
- Limit the size of directory server requests

12.1 Limiting Search Resources

Well-written directory client applications limit the scope of their searches with filters that narrow the number of results returned. By default, OpenDJ only allows users with appropriate privileges to perform unindexed searches.

You can further adjust additional limits on search operations, such as the following:

- The *lookthrough limit* defines the maximum number of candidate entries OpenDJ considers when processing a search.

The default lookthrough limit, which is set by using the global server property `lookthrough-limit`, is 5000.

You can override the limit for a particular user by changing the operational attribute, `ds-rlim-lookthrough-limit`, on the user's entry.

- The *size limit* sets the maximum number of entries returned for a search.

The default size limit, which is set by using the global server property `size-limit`, is 1000.

You can override the limit for a particular user by changing the operational attribute, `ds-rlim-size-limit`, on the user's entry.

- The *time limit* defines the maximum processing time OpenDJ devotes to a search operation.

The default time limit, which is set by using the global server property `time-limit`, is 1 minute.

You can override the limit for a particular user by changing the operational attribute, `ds-rlim-time-limit`, on the user's entry. Times for `ds-rlim-time-limit` are expressed in seconds.

- The *idle time limit* defines how long OpenDJ allows idle connections to remain open.

No default idle time limit is set. You can set an idle time limit by using the global server property `idle-time-limit`.

You can override the limit for a particular user by changing the operational attribute, `ds-rlim-idle-time-limit`, on the user's entry. Times for `ds-rlim-idle-time-limit` are expressed in seconds.

- The maximum number of persistent searches can be set by using the global server property `max-psearches`.

Procedure 12.1. To Set Search Limits For a User

- Change the user entry to set the limits to override:

```
$ cat limit.ldif
dn: uid=bjensen,ou=People,dc=example,dc=com
changetype: modify
add: ds-rlim-size-limit
ds-rlim-size-limit: 10

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename limit.ldif
Processing MODIFY request for uid=bjensen,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=bjensen,ou=People,dc=example,dc=com
```


Now when Babs Jensen performs a search returning more than 10 entries, she sees the following message:

```
Result Code: 4 (Size Limit Exceeded)
Additional Information: This search operation has sent the maximum of
10 entries to the client
```

Procedure 12.2. To Set Search Limits For a Group

1. Create an LDAP subentry to specify the limits using collective attributes:

```
$ cat grouplim.ldif
dn: cn=Remove Administrator Search Limits,dc=example,dc=com
objectClass: collectiveAttributeSubentry
objectClass: extensibleObject
objectClass: subentry
objectClass: top
cn: Remove Administrator Search Limits
ds-rlim-lookthrough-limit;collective: 0
ds-rlim-size-limit;collective: 0
ds-rlim-time-limit;collective: 0
subtreeSpecification: {base "ou=people", specificationFilter "
(isMemberOf=cn=Directory Administrators,ou=Groups,dc=example,dc=com)" }
```

```
$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename grouplim.ldif
Processing ADD request for
cn=Remove Administrator Search Limits,dc=example,dc=com
ADD operation successful for DN
cn=Remove Administrator Search Limits,dc=example,dc=com
```

2. Check the results:

```
$ ldapsearch --port 1389 --baseDN dc=example,dc=com uid=kvaughan +|grep ds-rlim
ds-rlim-lookthrough-limit: 0
ds-rlim-time-limit: 0
ds-rlim-size-limit: 0
```

12.2 Limiting Idle Time

If you have applications that leave connections open for long periods, OpenDJ can end up devoting resources to maintaining connections that are no longer used. If your network does not drop such connections eventually, you can configure

OpenDJ to drop them by setting the global configuration property, `idle-time-limit`. By default, no idle time limit is set.

If your network load balancer is configured to drop connections that have been idle for some time, make sure you set the OpenDJ idle time limit to a lower value than the idle time limit for the load balancer. This helps to ensure that idle connections are shut down in orderly fashion. Setting the OpenDJ limit lower than the load balancer limit is particularly useful with load balancers that drop idle connections without cleanly closing the connection and notifying the client and server.



Note

OpenDJ does not enforce idle timeout for persistent searches:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set idle-time-limit:24h \
  --trustAll \
  --no-prompt
```

The example shown sets the idle time limit to 24 hours.

12.3 Limiting Maximum Request Size

The default maximum request size of 5 MB, set using the advanced connection handler property `max-request-size`, is sufficient to satisfy most client requests. Yet, there are some cases where you might need to raise the request size limit. For example, if clients add groups with large numbers of members, those add requests can go beyond the 5 MB limit:

```
$ dsconfig \
  set-connection-handler-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --handler-name "LDAP Connection Handler" \
  --set max-request-size:20mb \
  --trustAll \
  --no-prompt
```

The example shown sets the maximum request size on the LDAP connection handler to 20 MB.

12.4 Resource Limits and Proxied Authorization

Proxied authorization uses a standard LDAP control to permit an application to bind as one user and then carry out LDAP operations on behalf of other users.

When using proxied authorization as described in Section 2.8, “Configuring Proxied Authorization” in the *OpenDJ Directory Server Developer's Guide* know that the resource limits do not change when the user proxies as another user. In other words, resource limits depend on the bind DN, not the proxy authorization identity.

Chapter 13

Implementing Attribute Value Uniqueness

This chapter shows you how to enforce that specified attributes do not have repeated values in different directory entries. You can use attribute uniqueness, for example, to prevent two user entries sharing the same email address. In this chapter you will learn to:

- Enforce uniqueness for user IDs and other attributes
- Limit the scope of attribute value uniqueness
- Manage attribute value uniqueness across replicated directory servers

Some attribute values ought to remain unique. If you are using `uid` values as RDNs to distinguish between millions of user entries stored under `ou=People`, then you do not want your directory to contain two or more identical `uid` values. If your credit card or mobile number is stored as an attribute value on your directory entry, you certainly do not want to share that credit card or mobile number with another customer. The same is true for your email address.

The difficulty for you as directory administrator lies in implementing attribute value uniqueness without sacrificing the high availability that comes from using OpenDJ's loosely consistent, multi-master data replication. Indeed OpenDJ's replication model lets you maintain write access during network outages for directory applications. Yet, write access during a network outage can result in the same, theoretically unique attribute value getting assigned to two different entries at once. You do not notice the duplicate assignment until the network outage ends and replication resumes.

This chapter shows you how to set up attribute value uniqueness in your directory environment with the following procedures:

- [Procedure 13.1, "To Enable Unique UIDs"](#)
- [Procedure 13.2, "To Enable Unique Values For Other Attributes"](#)
- [Procedure 13.3, "To Limit The Scope of Uniqueness"](#)
- [Procedure 13.4, "To Ensure Unique Attribute Values With Replication"](#)

OpenDJ directory server uses the unique attribute plugin to handle attribute value uniqueness. As shown in the examples in this chapter, you can configure the unique attribute plugin to handle one or more attributes and to handle entries under one or more base DN's. You can also configure multiple instances of the plugin for the same OpenDJ directory server.

Procedure 13.1. To Enable Unique UIDs

OpenDJ provides a unique attribute plugin that you configure by using the **dsconfig** command. By default, the plugin is prepared to ensure attribute values are unique for uid attributes.

1. Set the base DN where uid should have unique values, and enable the plugin:

```
$ dsconfig \
  set-plugin-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --plugin-name "UID Unique Attribute" \
    --set base-dn:ou=people,dc=example,dc=com \
    --set enabled:true \
    --trustAll \
    --no-prompt
```

Alternatively, you can specify multiple base DN's for unique values across multiple suffixes:

```
$ dsconfig \
  set-plugin-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDn "cn=Directory Manager" \
    --bindPassword password \
    --plugin-name "UID Unique Attribute" \
    --set enabled:true \
    --add base-dn:ou=people,dc=example,dc=com \
    --add base-dn:ou=people,dc=example,dc=org \
    --trustAll \
    --no-prompt
```

2. Check that the plugin is working correctly:

```
$ cat bjensen.ldif
dn: uid=ajensen,ou=People,dc=example,dc=com
changetype: modify
add: uid
uid: bjensen

$ ldapmodify \
  --defaultAdd \
  --port 1389 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --filename bjensen.ldif
Processing MODIFY request for uid=ajensen,ou=People,dc=example,dc=com
MODIFY operation failed
Result Code: 19 (Constraint Violation)
Additional Information: A unique attribute conflict was detected for
attribute uid: value bjensen already exists in entry
uid=bjensen,ou=People,dc=example,dc=com
```

If you have set up multiple suffixes, you might try something like this:

```

$ cat bjensen.ldif
dn: uid=bjensen,ou=People,dc=example,dc=org
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Babs
sn: Jensen
uid: bjensen

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename bjensen.ldif
Processing ADD request for uid=bjensen,ou=People,dc=example,dc=org
ADD operation failed
Result Code: 19 (Constraint Violation)
Additional Information: A unique attribute conflict was detected for attribute
uid: value bjensen already exists in entry
uid=bjensen,ou=People,dc=example,dc=com

```

Procedure 13.2. To Enable Unique Values For Other Attributes

You can also configure the unique attribute plugin for use with other attributes, such as mail, mobile, or attributes you define, for example cardNumber.

1. Before you set up the plugin, index the attribute for equality.

See [Section 7.3, "Configuring and Rebuilding Indexes"](#) for instructions.

2. Set up the plugin configuration for your attribute.

You can either add the attribute to an existing plugin configuration, or create a new plugin configuration including the attribute.

When choosing between these alternatives, keep in mind that values must be unique across the attributes and base DNs specified in each plugin configuration. Therefore only group attributes together in the same configuration if you want each value to be unique for all attributes. For example, you might create a single plugin configuration for telephone, fax, mobile, and pager numbers. As an alternative example, suppose user IDs are numeric, that user entries also specify uidNumber, and that user IDs are normally the same as their uidNumbers. In that case you create separate unique attribute configurations for uid and uidNumber:

- If you want to add the attribute to an existing plugin configuration, do so as shown in the following example which uses the plugin configuration from [Procedure 13.1, "To Enable Unique UIDs"](#):

```
$ dsconfig \
  set-plugin-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --plugin-name "UID Unique Attribute" \
  --add type:mobile \
  --trustAll \
  --no-prompt
```

- If you want to create a new plugin configuration, do so as shown in the following example:

```
$ dsconfig \
  create-plugin \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --plugin-name "Unique mobile numbers" \
  --type unique-attribute \
  --set enabled:true \
  --set base-dn:ou=people,dc=example,dc=com \
  --set type:mobile \
  --trustAll \
  --no-prompt
```

3. Check that the plugin is working correctly:

```

$ cat mobile.ldif
dn: uid=ajensen,ou=People,dc=example,dc=com
changetype: modify
add: mobile
mobile: +1 828 555 1212

dn: uid=bjensen,ou=People,dc=example,dc=com
changetype: modify
add: mobile
mobile: +1 828 555 1212

$ ldapmodify \
--defaultAdd \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename mobile.ldif
Processing MODIFY request for uid=ajensen,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=ajensen,ou=People,dc=example,dc=com
Processing MODIFY request for uid=bjensen,ou=People,dc=example,dc=com
MODIFY operation failed
Result Code: 19 (Constraint Violation)
Additional Information: A unique attribute conflict was detected for
attribute mobile: value +1 828 555 1212 already exists in entry
uid=ajensen,ou=People,dc=example,dc=com

```

Procedure 13.3. To Limit The Scope of Uniqueness

In some cases you need attribute uniqueness separately for different base DNs in your directory. For example, you need all uid values to remain unique both for users in dc=example,dc=com and dc=example,dc=org, but it is not a problem to have one entry under each base DN with the same user ID as the organizations are separate. The following steps demonstrate how to limit the scope of uniqueness by creating separate configuration entries for the unique attribute plugin.

1. If the attribute you target is not indexed for equality by default, index the attribute for equality.

See [Section 7.3, "Configuring and Rebuilding Indexes"](#) for instructions.

The examples in this procedure target the user ID attribute, uid, which is indexed for equality by default.

2. For each base DN, set up a configuration entry that ensures the target attribute values are unique:

```
$ dsconfig \
create-plugin \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--plugin-name "Unique Example.com UIDs" \
--type unique-attribute \
--set enabled:true \
--set base-dn:dc=example,dc=com \
--set type:uid \
--trustAll \
--no-prompt

$ dsconfig \
create-plugin \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--plugin-name "Unique Example.org UIDs" \
--type unique-attribute \
--set enabled:true \
--set base-dn:dc=example,dc=org \
--set type:uid \
--trustAll \
--no-prompt
```

3. Check that the plugin is working correctly:

```

$ cat uniq-ids.ldif
dn: uid=unique,ou=People,dc=example,dc=com
uid: unique
givenName: Unique
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: Unique Person
sn: Person
userPassword: 1Mun1qu3

dn: uid=unique,ou=People,dc=example,dc=org
uid: unique
givenName: Unique
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: Unique Person
sn: Person
userPassword: 1Mun1qu3

dn: uid=copycat,ou=People,dc=example,dc=com
uid: unique
uid: copycat
givenName: Copycat
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: Copycat Person
sn: Person
userPassword: copycopy

$ ldapmodify \
--defaultAdd \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename uniq-ids.ldif
Processing ADD request for uid=unique,ou=People,dc=example,dc=com
ADD operation successful for DN uid=unique,ou=People,dc=example,dc=com
Processing ADD request for uid=unique,ou=People,dc=example,dc=org
ADD operation successful for DN uid=unique,ou=People,dc=example,dc=org
Processing ADD request for uid=copycat,ou=People,dc=example,dc=com
ADD operation failed
Result Code: 19 (Constraint Violation)
Additional Information: A unique attribute conflict was detected for
attribute uid: value unique already exists in entry
uid=unique,ou=People,dc=example,dc=com

```

Procedure 13.4. To Ensure Unique Attribute Values With Replication

The unique attribute plugin ensures unique attribute values on the directory server where the attribute value is updated. If client applications write the same

attribute value separately at the same time on different directory replicas, it is possible that both servers consider the duplicate value unique, especially if the network is down between the replicas.

1. Enable the plugin identically on all replicas.
2. To avoid duplicate values where possible, try one of the following solutions:
 - Use a load balancer or proxy technology to direct all updates to the unique attribute to the same directory server.

The drawback here is the need for an additional component to direct the updates to the same server, and to manage failover should that server go down.

- Configure safe read mode assured replication between replicas storing the unique attribute.

The drawbacks here are the cost of safe read assured replication, and the likelihood that assured replication can enter degraded mode during a network outage, thus continuing to allow updates during the outage.

Chapter 14

Managing Schema

This chapter describes how to manage Lightweight Directory Access Protocol (LDAP) schema definitions for directory data. In this chapter you will learn to:

- Understand LDAP schemas including the schema definitions delivered with OpenDJ directory server
- Change and extend OpenDJ LDAP schemas
- Relax schema checking when troubleshooting data that does not conform to schema definitions

Schema definitions describe the data, and especially the object classes and attribute types that can be stored in the directory. By default OpenDJ conforms strictly to LDAPv3 standards pertaining to schema definitions and attribute syntax checking, ensuring that data stored is valid and properly formed. Unless your data uses only standard schema present in OpenDJ when you install, then you must add additional schema definitions to account for the data your applications stored.

OpenDJ comes with many standard schema definitions out of the box. In addition you can update and extend schema definitions while OpenDJ is online. As a result you can add new applications requiring additional data without stopping your directory service.

14.1 About Directory Schema

Directory schema, described in [RFC 4512](#), defines the kinds of information you find in the directory, and can define how the information are related. This chapter focuses primarily on the following types of directory schema definitions:

- *Attribute type* definitions describe attributes of directory entries, such as `givenName` or `mail`.

Here is an example of an attribute type definition:

```
# Attribute type definition
attributeTypes: ( 0.9.2342.19200300.100.1.3 NAME ( 'mail' 'rfc822Mailbox' )
    EQUALITY caseIgnoreIA5Match SUBSTR caseIgnoreIA5SubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} X-ORIGIN 'RFC 4524' )
```

Attribute type definitions start with an OID, and generally a short name or names that are easier to remember than the OID. The attribute type definition can specify how attribute values should be collated for sorting, and what syntax they use. The X-ORIGIN is an extension to identify where the definition originated. When you define your own schema, you likely want to provide an X-ORIGIN to help you to track versions of definitions, and where the definitions came from.

- *Object class* definitions identify the attribute types that an entry must have, and may have. Examples of object classes include `person` and `organizationalUnit`.

Here is an example of an object class definition:

```
# Object class definition
objectClasses: ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL MUST ( sn $ cn )
    MAY ( userPassword $ telephoneNumber $ seeAlso $ description )
    X-ORIGIN 'RFC 4519' )
```

Entries all have an attribute identifying their object classes, called `objectClass`.

Object class definitions start with an object identifier (OID), and generally a short name that is easier to remember than the OID. The definition here says that the `person` object class inherits from the `top` object class, which is the top-level parent of all object classes. An entry's `objectClass` attribute lists the entry's object classes. An entry can have one STRUCTURAL object class inheritance branch, such as `top - person - organizationalPerson - inetOrgPerson`. Yet entries can have multiple AUXILIARY object classes. The object class then defines the attribute types that must be included, and the attribute types that may be included on entries having the object class.

- An *attribute syntax* constrains what directory clients can store as attribute values.

An attribute syntax is identified in an attribute type definition by its OID. String-based syntax OIDs are optionally followed by a number set between braces that represents a minimum upper bound on the number of characters in the attribute value. For example, in the attribute type definition shown above, the syntax is 1.3.6.1.4.1.1466.115.121.1.26{256}. The syntax is an IA5 string (composed of characters from the international version of the ASCII character set) that can contain at least 256 characters.

You can find a table matching attribute syntax OIDs with their human-readable names in RFC 4517, [Appendix A. Summary of Syntax Object Identifiers](#). The RFC describes attribute syntaxes in detail. Alternatively, you can see the attribute syntaxes that OpenDJ supports by opening the OpenDJ control panel and browsing to Schema > Manage Schema > Attribute Syntaxes. You can also list them by using the **dsconfig** command.

Although attribute syntaxes are often specified in attribute type definitions, directory servers do not always check that attribute values comply with attribute syntaxes. OpenDJ directory server does tend to enforce compliance by default, in particular for certificates, country strings, directory strings, JPEG photos, and telephone numbers. The aim is to avoid accumulating garbage in your directory data.

If you are trying unsuccessfully to import non-compliant data from a more lenient directory server, you can either clean the data before importing it, or if cleaning the data is not an option, read [Section 14.3, "Relaxing Schema Checking to Import Legacy Data"](#).

When creating your own attribute type definitions, use existing attribute syntaxes where possible. If you must create your own attribute syntax, then consider the extensions in [Extensions for Attribute Syntax Descriptions](#).

- Matching rules determine how the directory server compares attribute values to assertion values for LDAP search and LDAP compare operations.

For example, suppose you search with the filter (uid=bjensen). The assertion value in this case is bjensen.

OpenDJ has the following schema definition for the user ID attribute:

```
attributeTypes: ( 0.9.2342.19200300.100.1.1 NAME ( 'uid' 'userid' )
EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} X-ORIGIN 'RFC 4519' )
```

When finding an equality match for your search, OpenDJ uses the `caseIgnoreMatch` matching rule to check for user ID attribute values that equal bjensen without regard to case.

You can see the matching rules that OpenDJ supports by opening the OpenDJ control panel and browsing to Schema > Manage Schema > Matching Rules. Notice that many matching rules support string collation in languages other than English. You can also list matching rules by using the **dsconfig** command.

As you can read in examples such as Example 2.6, “Search: Listing Active Accounts” in the *OpenDJ Directory Server Developer's Guide*, OpenDJ matching rules enable directory clients to compare other values besides strings, for example.

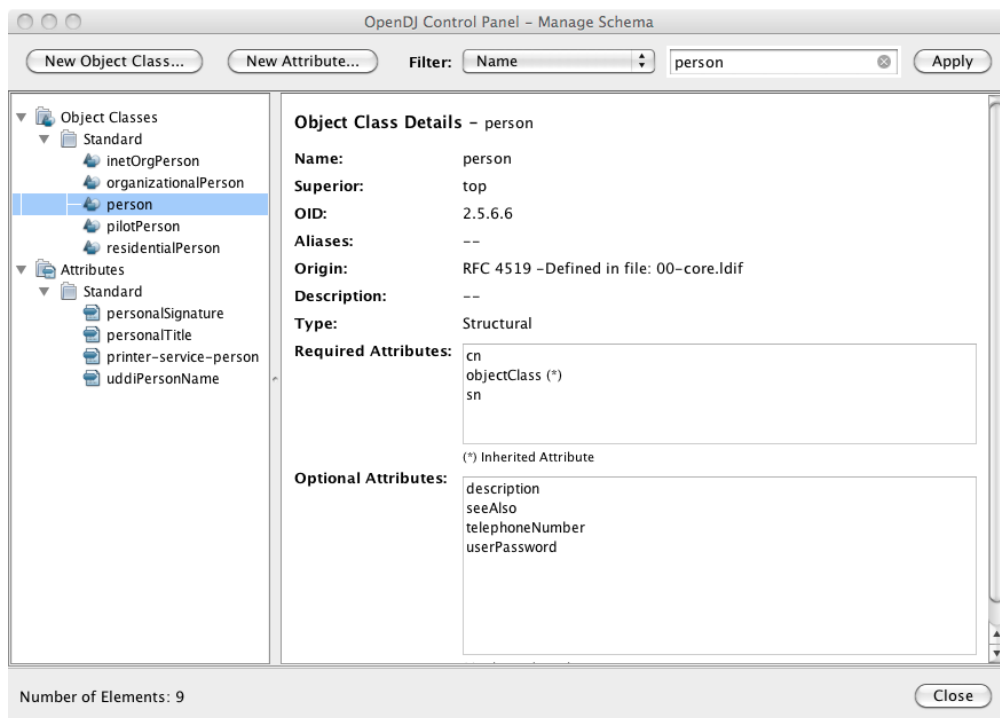
OpenDJ exposes schema over protocol through the `cn=schema` entry. OpenDJ stores the schema definitions corresponding to the entry in LDIF under the `config/schema/` directory. Many standard definitions and definitions pertaining to the server configuration are included at installation time.

14.2 Updating Directory Schema

OpenDJ directory server is designed to permit updating the list of directory schema definitions while the server is running. As a result you can add support for new applications that require new attributes or new kinds of entries without interrupting the directory service. OpenDJ also replicates schema definitions, so the schema you add on one replica is propagated to other replicas without the need for manual intervention.

As it is easy to introduce typos into schema definitions, the best way to start defining your own schema is with the OpenDJ Control Panel. Open the control panel > Schema > Manage Schema window to get started creating your custom object classes and attribute types.

Figure 14.1. Manage Schema Window



As object classes reference attribute types, you first create custom attribute types, and then create the object class that references the attribute types.

Create a custom attribute type through the New Attribute window.

Figure 14.2. New Attribute Window

OpenDJ Control Panel - New Attribute

* Indicates Required Field

Name: *

OID:

Description:

Syntax:

The syntax defines the type of value of the attribute

- ▶ Extra Options
- ▶ Attribute Type Options
- ▶ Matching Rule Options

OK Cancel

Using the New Object Class window, create an auxiliary object class that allows your new custom attribute type. You set the type to Auxiliary under Extra Options.

Figure 14.3. New Object Class Window

OpenDJ Control Panel - New Object Class

* Indicates Required Field

Name: * myCustomObjClass

OID: temporary-fake-oc-id

Description:

Superior: top Multiple Superiors...

Attributes:

Available Attributes:

- aci
- aclRights
- aclRightsInfo
- administratorsAddress
- aliasedObjectName
- altServer
- aRecord
- associatedDomain
- associatedName
- attributeMap
- attributeTypes
- audio
- authenticationMethod
- authorityRevocationList

(*) Inherited Attribute

Required Attributes:

- objectClass (*)

Optional Attributes:

- myCustomAttribute

► Extra Options

OK Cancel

When you finish, the schema changes show up by default in the file `config/schema/99-user.ldif`. Notice that the file name starts with a number, 99. This number is larger than the numbers prefixing other schema file names. In fact, OpenDJ reads the schema files in sorted order, reading schema definitions as they occur. If OpenDJ reads a schema definition for an object class before it has read the definitions of the attribute types mentioned in the object class definition, then it displays an error. Therefore, when naming your schema file, make sure the name appears in the sorted list of file names *after* all the schema files containing definitions that your schema definitions depends on. The default file name for your schema, `99-user.ldif`, ensures that your definitions load only after all of the schema files installed by default.

You can create this file in the lab using the control panel, and then apply the definitions in production by adapting the content for use with the **ldapmodify** command, for example:

```
$ cat config/schema/99-user.ldif
dn: cn=schema
objectClass: top
objectClass: ldapSubentry
objectClass: subschema
cn: schema
attributeTypes: ( temporary-fake-attr-id NAME 'myCustomAttribute' EQUALITY case
IgnoreMatch ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstrings
Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
objectClasses: ( temporary-fake-oc-id NAME 'myCustomObjClass
' SUP top AUXILIARY MAY myCustomAttribute )
modifiersName: cn=Directory Manager,cn=Root DNs,cn=config
modifyTimestamp: 20110620095948Z
```

To test your schema definition, add the object class and attribute to an entry:

```
$ cat custom-attr.ldif
dn: uid=bjensen,ou=People,dc=example,dc=com
changetype: modify
add: objectClass
objectClass: myCustomObjClass
-
add: myCustomAttribute
myCustomAttribute: Testing 1, 2, 3...

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename custom-attr.ldif
Processing MODIFY request for uid=bjensen,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=bjensen,ou=People,dc=example,dc=com

$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
uid=bjensen \
myCustomAttribute
dn: uid=bjensen,ou=People,dc=example,dc=com
myCustomAttribute: Testing 1, 2, 3...
```

In addition to supporting the standard schema definitions that are described in [RFC 4512, section 4.1](#), OpenDJ also supports the following extensions that you can use when adding your own definitions:

Extensions for All Schema Definitions

X-ORIGIN

Used to specify the origin of a schema element. Examples include X-ORIGIN 'RFC 4519', X-ORIGIN 'draft-ietf-ldup-subentry', and X-ORIGIN 'OpenDJ Directory Server'.

X-SCHEMA-FILE

Used to specify the relative path to the schema file containing the schema element such as X-SCHEMA-FILE '00-core.ldif'. Schema definitions are located by default in /path/to/openssl/config/schema/*.ldif files.

Extensions for Attribute Syntax Descriptions**X-ENUM**

Used to define a syntax that is an enumeration of values. The following attribute syntax description defines a syntax allowing four possible attribute values, for example:

```
ldapSyntaxes: ( security-label-syntax-oid DESC 'Security Label'
  X-ENUM ( 'top-secret' 'secret' 'confidential' 'unclassified' ) )
```

X-PATTERN

Used to define a syntax based on a regular expression pattern, where valid regular expressions are those defined for [java.util.regex.Pattern](#). The following attribute syntax description defines a simple, lenient SIP phone URI syntax check:

```
ldapSyntaxes: ( simple-sip-uri-syntax-oid DESC 'Lenient SIP URI Syntax'
  X-PATTERN '^sip:[a-zA-Z0-9.]+@[a-zA-Z0-9.]+(:[0-9]+)?$' )
```

X-SUBST

Used as a fallback to substitute a defined syntax for one that OpenDJ does not implement. The following example substitutes Directory String syntax, which has OID 1.3.6.1.4.1.1466.115.121.1.15, for a syntax that OpenDJ does not implement:

```
ldapSyntaxes: ( non-implemented-syntax-oid DESC 'Not Implemented in OpenDJ'
  X-SUBST '1.3.6.1.4.1.1466.115.121.1.15' )
```

Extension for Attribute Type Descriptions**X-APPROX**

X-APPROX is used to specify the approximate matching rule to use for a given attribute type when not using the default, which is the [double metaphone approximate match](#).

14.3 Relaxing Schema Checking to Import Legacy Data

By default, OpenDJ accepts data that follows the schema for allowable and rejected data. You might have legacy data from a directory service that is more lenient, allowing non-standard constructions such as multiple structural object classes per entry, not checking attribute value syntax, or even not respecting schema definitions.

For example, when importing data with multiple structural object classes defined per entry, you can relax schema checking to warn rather than reject entries having this issue:

```
$ dsconfig \
  set-global-configuration-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set single-structural-objectclass-behavior:warn \
  --trustAll \
  --no-prompt
```

You can allow attribute values that do not respect the defined syntax with the **dsconfig** command as well:

```
$ dsconfig \
  set-global-configuration-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set invalid-attribute-syntax-behavior:warn \
  --trustAll \
  --no-prompt
```

You can even turn off schema checking altogether, although turning off schema checking only really makes sense when you are absolutely sure that the entries and attribute values respect the schema definitions, and you simply want to turn off schema checking temporarily to speed up import processing:


```
$ dsconfig \
  set-global-configuration-prop \
  --hostname opendj.example.com \
  --port 4444 \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set check-schema:false \
  --trustAll \
  --no-prompt
```

14.4 Standard Schema Included With OpenDJ Server

OpenDJ directory server provides many standard schema definitions in these LDIF files under `/path/to/opendj/config/schema`:

00-core.ldif

This file contains a core set of attribute type and object class definitions from the following Internet-Drafts, RFCs, and standards:

- draft-ietf-boreham-numsubordinates
- draft-findlay-ldap-groupofentries
- draft-furuseth-ldap-untypedobject
- draft-good-ldap-changelog
- draft-ietf-ldup-subentry
- draft-wahl-ldap-adminaddr
- RFC 1274
- RFC 2079
- RFC 2256
- RFC 2798
- RFC 3045
- RFC 3296
- RFC 3671
- RFC 3672
- RFC 4512
- RFC 4519
- RFC 4523
- RFC 4524
- RFC 4530
- RFC 5020
- X.501

01-pwpolicy.ldif

This file contains schema definitions from [draft-behera-ldap-password-policy](#) (Draft 09), which defines a mechanism for storing password policy information in an LDAP directory server.

02-config.ldif

This file contains the attribute type and objectclass definitions for use with the directory server configuration.

03-changelog.ldif

This file contains schema definitions from [draft-good-ldap-changelog](#), which defines a mechanism for storing information about changes to directory server data.

03-rfc2713.ldif

This file contains schema definitions from [RFC 2713](#), which defines a mechanism for storing serialized Java objects in the directory server.

03-rfc2714.ldif

This file contains schema definitions from [RFC 2714](#), which defines a mechanism for storing CORBA objects in the directory server.

03-rfc2739.ldif

This file contains schema definitions from [RFC 2739](#), which defines a mechanism for storing calendar and vCard objects in the directory server. Note that the definition in RFC 2739 contains a number of errors, and this schema file has been altered from the standard definition in order to fix a number of those problems.

03-rfc2926.ldif

This file contains schema definitions from [RFC 2926](#), which defines a mechanism for mapping between Service Location Protocol (SLP) advertisements and LDAP.

03-rfc3112.ldif

This file contains schema definitions from [RFC 3112](#), which defines the authentication password schema.

03-rfc3712.ldif

This file contains schema definitions from [RFC 3712](#), which defines a mechanism for storing printer information in the directory server.

03-uddiv3.ldif

This file contains schema definitions from [RFC 4403](#), which defines a mechanism for storing UDDIv3 information in the directory server.

04-rfc2307bis.ldif

This file contains schema definitions from [draft-howard-rfc2307bis](#), which defines a mechanism for storing naming service information in the directory server.

05-rfc4876.ldif

This file contains schema definitions from [RFC 4876](#), which defines a schema for storing Directory User Agent (DUA) profiles and preferences in the directory server.

05-samba.ldif

This file contains schema definitions required when storing Samba user accounts in the directory server.

05-solaris.ldif

This file contains schema definitions required for Solaris and OpenSolaris LDAP naming services.

06-compat.ldif

This file contains the attribute type and objectclass definitions for use with the directory server configuration.

Chapter 15

Configuring Pass-Through Authentication

This chapter focuses on pass-through authentication (PTA), whereby you configure another server to determine the response to an authentication request. A typical use case for PTA involves passing authentication through to Active Directory for users coming from Microsoft Windows systems. In this chapter you will learn to:

- Configure password policies to use PTA
- Assign PTA policies to users and to groups

15.1 About Pass-through Authentication

You use *pass-through authentication* (PTA) when the credentials for authenticating are stored in a remote directory service instead of OpenDJ. In effect OpenDJ redirects the bind operation against a remote LDAP server.

The method OpenDJ uses to redirect the bind depends on the mapping from the user entry in OpenDJ to the corresponding user entry in the remote directory. OpenDJ provides you several choices to set up the mapping:

- When both the local entry in OpenDJ and the remote entry in the other server have the same DN, you do not have to set up the mapping. By default,

OpenDJ redirects the bind with the original DN and password from the client application.

- When the local entry in OpenDJ has been provisioned with an attribute holding the DN of the remote entry, you can specify which attribute holds the DN, and OpenDJ redirects the bind on the remote server using the DN value.
- When you cannot get the remote bind DN directly, you need an attribute and value on the OpenDJ entry that corresponds to an identical attribute and value on the remote server. In this case you also need the bind credentials for a user who can search for the entry on the remote server. OpenDJ performs a search for the entry using the matching attribute and value, and then redirects the bind with the DN from the remote entry.

You configure PTA as an authentication policy that you associate with a user's entry in the same way that you associate a password policy with a user's entry. Either a user has an authentication policy for PTA, or the user has a local password policy.

15.2 Setting Up Pass-Through Authentication

When setting up pass-through authentication, you need to know to which remote server or servers to redirect binds, and you need to know how you map user entries in OpenDJ to user entries in the remote directory.

Procedure 15.1. To Set Up SSL Communication For Testing

When performing PTA, you protect communications between OpenDJ and the server providing authentication. If you test using SSL with self-signed certificates, and you do not want the client to blindly trust the server, follow these steps to import the authentication server's certificate into the OpenDJ keystore.

1. Export the server certificate from the authentication server.

How you perform this step depends on the authentication directory server. With OpenDJ, you can export the certificate as shown here:

```
$ cd /path/to/PTA-Server/config
$ keytool \
  -exportcert \
  -rfc \
  -alias server-cert \
  -keystore keystore \
  -storepass `cat keystore.pin` \
  > /tmp/pta-srv-cert.pem
```

2. Make note of the host name used in the certificate.

You use the host name when configuring the SSL connection. With OpenDJ, you can view the certificate details as shown here:

```
$ keytool \  
-list \  
-v \  
-alias server-cert \  
-keystore keystore \  
-storepass `cat keystore.pin`  
Alias name: server-cert  
Creation date: Sep 12, 2011  
Entry type: PrivateKeyEntry  
Certificate chain length: 1  
Certificate[1]:  
Owner: CN=pta-server.example.com, O=OpenDJ Self-Signed Certificate  
Issuer: CN=pta-server.example.com, O=OpenDJ Self-Signed Certificate  
Serial number: 4e6dc429  
Valid from: Mon Sep 12 10:34:49 CEST 2011 until: Wed Sep 11 10:34:49 CEST 2013  
Certificate fingerprints:  
MD5: B6:EE:1C:A0:71:12:EF:6F:21:24:B9:50:EF:8B:4E:6A  
SHA1: 7E:A1:C9:07:D2:86:56:31:24:14:F7:07:A8:6B:3E:A1:39:63:F4:0E  
Signature algorithm name: SHA1withRSA  
Version: 3
```

3. Import the authentication server certificate into OpenDJ's keystore:

```
$ cd /path/to/opendj/config  
$ keytool \  
-importcert \  
-alias pta-cert \  
-keystore truststore \  
-storepass `cat keystore.pin` \  
-file /tmp/pta-srv-cert.pem  
Owner: CN=pta-server.example.com, O=OpenDJ Self-Signed Certificate  
Issuer: CN=pta-server.example.com, O=OpenDJ Self-Signed Certificate  
Serial number: 4e6dc429  
Valid from: Mon Sep 12 10:34:49 CEST 2011 until: Wed Sep 11 10:34:49 CEST 2013  
Certificate fingerprints:  
MD5: B6:EE:1C:A0:71:12:EF:6F:21:24:B9:50:EF:8B:4E:6A  
SHA1: 7E:A1:C9:07:D2:86:56:31:24:14:F7:07:A8:6B:3E:A1:39:63:F4:0E  
Signature algorithm name: SHA1withRSA  
Version: 3  
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

Procedure 15.2. To Configure an LDAP Pass-Through Authentication Policy

You configure authentication policies with the **dsconfig** command. Notice that authentication policies are part of the server configuration, and therefore not replicated.

1. Set up an authentication policy for pass-through authentication to the authentication server:

```
$ dsconfig \
  create-password-policy \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --type ldap-pass-through \
  --policy-name "PTA Policy" \
  --set primary-remote-ldap-server:pta-server.example.com:636 \
  --set mapped-attribute:uid \
  --set mapped-search-base-dn:"dc=PTA Server,dc=com" \
  --set mapping-policy:mapped-search \
  --set use-ssl:true \
  --set trust-manager-provider:JKS \
  --trustAll \
  --no-prompt
```

The policy shown here maps identities with this this password policy to identities under `dc=PTA Server,dc=com`. Users must have the same `uid` values on both servers. The policy here also uses SSL between OpenDJ and the authentication server.

2. Check that your policy has been added to the list:

```
$ dsconfig \
  list-password-policies \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --property use-ssl

Password Policy      : Type      : use-ssl
-----:-----:-----
Default Password Policy : password-policy : -
PTA Policy           : ldap-pass-through : true
Root Password Policy  : password-policy : -
```

Procedure 15.3. To Configure Pass-Through Authentication To Active Directory

The steps below demonstrate how to set up PTA to Active Directory. Here is some information to help you make sense of the steps.

Entries on the OpenDJ side use `uid` as the naming attribute, and entries also have `cn` attributes. Active Directory entries use `cn` as the naming attribute. User entries on both sides share the same `cn` values. The mapping between entries therefore uses `cn`.

Consider the example where an OpenDJ account with `cn=LDAP PTA User` and DN `uid=ldapptauser,ou=People,dc=example,dc=com` corresponds to an Active Directory account with DN `CN=LDAP PTA User,CN=Users,DC=internal,DC=forgerock,DC=com`. The steps below enable the user with `cn=LDAP PTA User` on OpenDJ authenticate through to Active Directory:

```
$ ldapsearch \
--hostname opendj.example.com \
--baseDN dc=example,dc=com \
uid=ldapptauser \
cn
dn: uid=ldapptauser,ou=People,dc=example,dc=com
cn: LDAP PTA User

$ ldapsearch \
--hostname ad.example.com \
--baseDN "CN=Users,DC=internal,DC=forgerock,DC=com" \
--bindDN "cn=administrator,cn=Users,DC=internal,DC=forgerock,DC=com" \
--bindPassword password \
"(cn=LDAP PTA User)" \
cn
dn: CN=LDAP PTA User,CN=Users,DC=internal,DC=forgerock,DC=com
cn: LDAP PTA User
```

OpenDJ must map its `uid=ldapptauser,ou=People,dc=example,dc=com` entry to the Active Directory entry, `CN=LDAP PTA User,CN=Users,DC=internal,DC=forgerock,DC=com`. In order to do the mapping, OpenDJ has to perform a search for the user in Active Directory using the `cn` value it recovers from its own entry for the user. Active Directory does not allow anonymous searches, so part of the authentication policy configuration consists of the administrator DN and password OpenDJ uses to bind to Active Directory to be able to search.

Finally, before setting up the PTA policy, make sure OpenDJ can connect to Active Directory over a secure connection to avoid sending passwords in the clear.

1. Export the certificate from the Windows server.
 - a. Click start > All Programs > Administrative Tools > Certification Authority, then right-click the CA and select Properties.
 - b. In the General tab, select the certificate and click View Certificate.
 - c. In the Certificate dialog, click the Details tab, then click Copy to File...
 - d. Use the Certificate Export Wizard to export the certificate into a file, such as `windows.cer`.
2. Copy the exported certificate to the system running OpenDJ.
3. Import the server certificate into OpenDJ's keystore:

```
$ cd /path/to/openssl/config
$ keytool \
  -importcert \
  -alias ad-cert \
  -keystore truststore \
  -storepass 'cat keystore.pin' \
  -file ~/Downloads/windows.cer
Owner: CN=internal-ACTIVEDIRECTORY-CA, DC=internal, DC=forgerock, DC=com
Issuer: CN=internal-ACTIVEDIRECTORY-CA, DC=internal, DC=forgerock, DC=com
Serial number: 587465257200a7b14a6976cb47916b32
Valid from: Tue Sep 20 11:14:24 CEST 2011 until: Tue Sep 20 11:24:23 CEST 2016
Certificate fingerprints:
  MD5: A3:D6:F1:8D:0D:F9:9C:76:00:BC:84:8A:14:55:28:38
  SHA1: 0F:BD:45:E6:21:DF:BD:6A:CA:8A:7C:1D:F9:DA:A1:8E:8A:0D:A4:BF
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: A3 3E C0 E3 B2 76 15 DC   97 D0 B3 C0 2E 77 8A 11   .>...v.....w..
    0010: 24 62 70 0A                               $bp.
  ]
]

#4: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

Trust this certificate? [no]: yes
Certificate was added to keystore
```

At this point OpenDJ can connect to Active Directory over SSL.

4. Set up an authentication policy for OpenDJ users to authenticate to Active Directory:

```
$ dsconfig \
create-password-policy \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--type ldap-pass-through \
--policy-name "AD PTA Policy" \
--set primary-remote-ldap-server:ad.example.com:636 \
--set mapped-attribute:cn \
--set mapped-search-base-dn:"CN=Users,DC=internal,DC=forgerock,DC=com" \
--set mapped-search-bind-dn:"cn=adminstrator,cn=Users,DC=internal, \
DC=forgerock,DC=com" \
--set mapped-search-bind-password:password \
--set mapping-policy:mapped-search \
--set trust-manager-provider:JKS \
--set use-ssl:true \
--trustAll \
--no-prompt
```

5. Assign the authentication policy to a test user:

```
$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password
dn: uid=ldapptouser,ou=People,dc=example,dc=com
changetype: modify
add: ds-pwp-password-policy-dn
ds-pwp-password-policy-dn: cn=AD PTA Policy,cn=Password Policies,cn=config

Processing MODIFY request for uid=ldapptouser,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=ldapptouser,ou=People,dc=example,dc=com
```

6. Check that the user can bind using PTA to Active Directory:

```
$ ldapsearch \
--hostname opendj.example.com \
--port 1389 \
--baseDN dc=example,dc=com \
--bindDN uid=ldapptouser,ou=People,dc=example,dc=com \
--bindPassword password \
"(cn=LDAP PTA User)" \
userpassword cn
dn: uid=ldapptouser,ou=People,dc=example,dc=com
cn: LDAP PTA User
```

Notice that to complete the search, the user authenticated with a password to Active Directory, though no userpassword value is present on the entry on the OpenDJ side.

15.3 Assigning Pass-Through Authentication Policies

You assign authentication policies in the same way as you assign password policies, by using the `ds-pwp-password-policy-dn` attribute.



Note

Although you assign the pass-through authentication policy using the same attribute as for password policy, the authentication policy is not in fact a password policy. Therefore, the user with a pass-through authentication policy does not have a value for the operational attribute `pwdPolicySubentry`:

```
$ ldapsearch \
--port 1389 \
--baseDN dc=example,dc=com \
uid=user.0 \
pwdPolicySubentry
dn: uid=user.0,ou=People,dc=example,dc=com
```

Procedure 15.4. To Assign a Pass-Through Authentication Policy To a User

Users depending on PTA no longer need a local password policy, as they no longer authenticate locally.

Examples in the following procedure work for this user, whose entry on OpenDJ is as shown. Notice that the user has no password set. The user's password on the authentication server is password:

```
dn: uid=user.0,ou=People,dc=example,dc=com
cn: Aaccf Amar
description: This is the description for Aaccf Amar.
employeeNumber: 0
givenName: Aaccf
homePhone: +1 225 216 5900
initials: ASA
l: Panama City
mail: user.0@maildomain.net
mobile: +1 010 154 3228
objectClass: person
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: top
pager: +1 779 041 6341
postalAddress: Aaccf Amar$01251 Chestnut Street$Panama City, DE 50369
postalCode: 50369
sn: Amar
st: DE
street: 01251 Chestnut Street
telephoneNumber: +1 685 622 6202
uid: user.0
```

This user's entry on the authentication server also has `uid=user.0`, and the pass-through authentication policy performs the mapping to find the user entry in the authentication server.

1. Prevent users from changing their own password policies:

```
$ cat protect-pta.ldif
dn: ou=People,dc=example,dc=com
changetype: modify
add: aci
aci: (target = "ldap:///uid=*,ou=People,dc=example,dc=com")(targetattr =
  "ds-pwp-password-policy-dn")(version 3.0;acl "Cannot choose own pass
  word policy";deny (write)(userdn = "ldap:///self");)

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename protect-pta.ldif
Processing MODIFY request for ou=People,dc=example,dc=com
MODIFY operation successful for DN ou=People,dc=example,dc=com
```

2. Update the user's `ds-pwp-password-policy-dn` attribute:

```
$ ldapmodify \  
--port 1389 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password  
dn: uid=user.0,ou=People,dc=example,dc=com  
changetype: modify  
add: ds-pwp-password-policy-dn  
ds-pwp-password-policy-dn: cn=PTA Policy,cn=Password Policies,cn=config  
  
Processing MODIFY request for uid=user.0,ou=People,dc=example,dc=com  
MODIFY operation successful for DN uid=user.0,ou=People,dc=example,dc=com
```

3. Check that the user can authenticate through to the authentication server:

```
$ ldapsearch \  
--port 1389 \  
--baseDN dc=example,dc=com \  
--bindDN uid=user.0,ou=People,dc=example,dc=com \  
--bindPassword password \  
uid=user.0 \  
cn sn  
dn: uid=user.0,ou=People,dc=example,dc=com  
cn: Aaccf Amar  
sn: Amar
```

Procedure 15.5. To Assign a Pass-Through Authentication Policy To a Group

Examples in the following steps use the PTA policy as defined above. Kirsten Vaughan's entry has been reproduced on the authentication server under `dc=PTA Server,dc=com`.

1. Create a subentry to assign a collective attribute that sets the `ds-pwp-password-policy-dn` attribute for group members' entries:

```
$ cat pta-coll.ldif
dn: cn=PTA Policy for Dir Admins,dc=example,dc=com
objectClass: collectiveAttributeSubentry
objectClass: extensibleObject
objectClass: subentry
objectClass: top
cn: PTA Policy for Dir Admins
ds-pwp-password-policy-dn;collective: cn=PTA Policy,cn=Password Policies,
cn=config
subtreeSpecification: { base "ou=People", specificationFilter "(isMemberOf=
cn=Directory Administrators,ou=Groups,dc=example,dc=com)" }

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename pta-coll.ldif
Processing ADD request for cn=PTA Policy for Dir Admins,dc=example,dc=com
ADD operation successful for DN cn=PTA Policy for Dir Admins,dc=example,dc=com
```

2. Check that OpenDJ has applied the policy.
 - a. Make sure you can bind as the user on the authentication server:

```
$ ldapsearch \
--port 2389 \
--bindDN "uid=kvaughan,ou=People,dc=PTA Server,dc=com" \
--bindPassword password \
--baseDN "dc=PTA Server,dc=com" \
uid=kvaughan
dn: uid=kvaughan,ou=People,dc=PTA Server,dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
givenName: Kirsten
uid: kvaughan
cn: Kirsten Vaughan
sn: Vaughan
userPassword: {SSHA}x1BdtrJyRTw63kBSJFDvgvd4guzk66CV8L+t8w==
ou: People
mail: jvaughan@example.com
```

- b. Check that the user can authenticate through to the authentication server from OpenDJ directory server:

```
$ ldapsearch \  
--port 1389 \  
--bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \  
--bindPassword password \  
--baseDN dc=example,dc=com \  
uid=kvaughan \  
cn sn  
dn: uid=kvaughan,ou=People,dc=example,dc=com  
cn: Kirsten Vaughan  
sn: Vaughan
```

Chapter 16

Samba Password Synchronization

This chapter covers synchronization between directory passwords and Samba passwords. In this chapter you will learn to:

- Configure Samba for use with OpenDJ directory server
- Set up the OpenDJ directory sever Samba password plugin for synchronization

[Samba](#), the Windows interoperability suite for Linux and UNIX, stores accounts because UNIX and Windows password storage management is not interoperable. The default account storage mechanism is designed to work well with relatively small numbers of accounts and configurations with one domain controller. For larger installations, you can configure Samba to use OpenDJ for storing Samba accounts. See the Samba documentation for your platform for instructions on how to configure an LDAP directory server such as OpenDJ as a Samba passdb backend.

The rest of this chapter focuses on how you keep passwords in sync when using OpenDJ for Samba account storage.

When you store Samba accounts in OpenDJ, Samba stores its own attributes as defined in the Samba schema. Samba does not use the LDAP standard `userPassword` attribute to store users' Samba passwords. You can configure Samba to apply changes to Samba passwords to LDAP passwords as well, too. Yet, if a user modifies their LDAP password directly without updating the Samba password, the LDAP and Samba passwords get out of sync.

The OpenDJ Samba Password plugin resolves this problem for you. The plugin intercepts password changes to Samba user profiles, synchronizing Samba

password and LDAP password values. For an incoming Password Modify Extended Request or modify request changing the user password, the OpenDJ Samba Password plugin detects whether the user's entry reflects a Samba user profile (entry has object class `sambaSAMAccount`), hashes the incoming password value, and applies the password change to the appropriate password attribute, keeping the password values in sync. The OpenDJ Samba Password plugin can perform synchronization as long as new passwords values are provided in cleartext in the modification request. If you configure Samba to synchronize LDAP passwords when it changes Samba passwords, then the plugin can ignore changes by the Samba user to avoid duplicate synchronization.

Procedure 16.1. To Set Up a Samba Administrator Account

The Samba Administrator synchronizes LDAP passwords after changing Samba passwords by issuing a Password Modify Extended Request. In Samba's `smb.conf` configuration file, the value of `ldap admin dn` is set to the DN of this account. When the Samba Administrator changes a user password, the plugin ignores the changes, so choose a distinct account different from Directory Manager and other administrators.

1. Create or choose an account for the Samba Administrator:

```
$ cat samba.ldif
dn: uid=samba-admin,ou=Special Users,dc=example,dc=com
cn: Samba Administrator
givenName: Samba
mail: samba@example.com
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
sn: Administrator
uid: samba-admin
userPassword: password

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--defaultAdd \
--filename samba.ldif
Processing ADD request for uid=samba-admin,ou=Special Users,dc=example,dc=com
ADD operation successful for DN uid=samba-admin,ou=Special Users,
dc=example,dc=com
```

2. Ensure the Samba Administrator can reset user passwords:

```

$ cat samba-rights.ldif
dn: uid=samba-admin,ou=Special Users,dc=example,dc=com
changetype: modify
add: ds-privilege-name
ds-privilege-name: password-reset

dn: dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///dc=example,dc=com") (targetattr="*)(version 3.0; acl "
Samba Admin user rights"; allow(all) groupdn="ldap:///uid=samba-user,ou=
Special Users,dc=example,dc=com");)

$ ldapmodify \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename samba-rights.ldif
Processing MODIFY request for uid=samba-admin,ou=Special Users,dc=example,dc=com
MODIFY operation successful for DN
uid=samba-admin,ou=Special Users,dc=example,dc=com
Processing MODIFY request for dc=example,dc=com
MODIFY operation successful for DN dc=example,dc=com

```

Procedure 16.2. To Set Up the Samba Password Plugin

1. Determine whether the plugin must store passwords hashed like LanManager (sync-lm-password) or like Windows NT (sync-nt-password), based on how you set up Samba in your environment.
2. Enable the plugin:

```

$ dsconfig \
create-plugin \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--plugin-name "Samba Password Synchronisation" \
--type samba-password \
--set enabled:true \
--set pwd-sync-policy:sync-nt-password \
--set \
samba-administrator-dn:"uid=samba-admin,ou=Special Users,dc=example,dc=com" \
--trustAll \
--no-prompt

```

At this point the Samba Password plugin is active.

3. When troubleshooting Samba Password plugin issues, you can turn on debug logging as follows:

```
$ dsconfig \
  set-log-publisher-prop \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based Debug Logger" \
    --set enabled:true \
    --no-prompt \
    --trustAll

$ dsconfig \
  create-debug-target \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based Debug Logger" \
    --target-name org.opends.server.plugins.SambaPasswordPlugin \
    --set enabled:true \
    --trustAll \
    --no-prompt

$ tail -f /path/to/opendj/logs/debug
```

Chapter 17

Monitoring, Logging, and Alerts

This chapter covers OpenDJ monitoring capabilities. In this chapter you will learn to:

- Access monitoring information over LDAP, over SNMP, and through use of JMX.
- Monitor directory server status, including the status of directory server tasks
- Configure directory server logs and interpret the messages they contain
- Configure email settings for administrative alert notifications

OpenDJ control panel provides basic monitoring capabilities under Monitoring > General Information, Monitoring > Connection Handler, and Monitoring > Manage Tasks. This chapter covers the other options for monitoring OpenDJ.

17.1 LDAP-Based Monitoring

OpenDJ exposes monitoring information over LDAP under the entry `cn=monitor`. Many different types of information are exposed. The following example shows monitoring information about the `userRoot` backend holding `Example.com` data:

Interface stability: Evolving (See Section I.2, “ForgeRock Product Interface Stability” in the *OpenDJ Reference*)

```
$ ldapsearch --port 1389 --baseDN cn=monitor "(cn=userRoot backend)"
dn: cn=userRoot backend,cn=Disk Space Monitor,cn=monitor
disk-state: normal
objectClass: top
objectClass: ds-monitor-entry
objectClass: extensibleObject
disk-dir: /path/to/openssl/db/userRoot
disk-free: 343039315968
cn: userRoot backend

dn: cn=userRoot Backend,cn=monitor
objectClass: top
objectClass: ds-monitor-entry
objectClass: ds-backend-monitor-entry
cn: userRoot Backend
ds-backend-id: userRoot
ds-backend-base-dn: dc=example,dc=com
ds-backend-is-private: FALSE
ds-backend-entry-count: 176
ds-base-dn-entry-count: 176 dc=example,dc=com
ds-backend-writability-mode: enabled
```

You can set global ACIs on the Access Control Handler if you want to limit read access under `cn=monitor`.

17.2 SNMP-Based Monitoring

OpenDJ lets you monitor the server over SNMP with support for the Management Information Base described in [RFC 2605: Directory Server Monitoring MIB](#).

OpenDJ SNMP-based monitoring depends on OpenDMK, which you must [download separately](#). Install the [Full Binary Bundle](#) by using the GUI installer, which requires that you accept the [Binary License for Project OpenDMK](#). OpenDJ directory server that you download from ForgeRock is built with OpenDMK, but due to licensing OpenDMK is not part of OpenDJ. SNMP is therefore not enabled by default.

To run the OpenDMK installer, use the self-extracting `.jar`:

```
$ java -jar ~/Downloads/opendmk-1.0-b02-*.jar
```

If you install under `/path/to`, then the runtime library needed for SNMP is `/path/to/OpenDMK-bin/lib/jdmkrt.jar`.

Once you have installed OpenDMK, you can set up a connection handler for SNMP by enabling the connection handler, and pointing OpenDJ to your installation of the OpenDMK `jdmkrt.jar` library:

```
$ dsconfig \
  set-connection-handler-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "SNMP Connection Handler" \
    --set enabled:true \
    --set opendmk-jarfile:/path/to/OpenDMK-bin/lib/jdmkrt.jar \
    --trustAll \
    --no-prompt
```

By default, the SNMP connection handler listens on port 161 and uses port 162 for traps. On UNIX and Linux systems, only root can normally open these ports. Therefore if you install as a normal user, you might want to change the listen and trap ports:

```
$ dsconfig \
  set-connection-handler-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "SNMP Connection Handler" \
    --set listen-port:11161 \
    --set trap-port:11162 \
    --trustAll \
    --no-prompt
```

Restart the SNMP connection handler to take the port number changes into account.

To restart the connection handler, you disable it, then enable it again:

```
$ dsconfig \
  set-connection-handler-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "SNMP Connection Handler" \
    --set enabled:false \
    --trustAll \
    --no-prompt

$ dsconfig \
  set-connection-handler-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "SNMP Connection Handler" \
    --set enabled:true \
    --trustAll \
    --no-prompt
```

Use a command such as **snmpwalk** to check that the SNMP listen port works:

```
$ snmpwalk -v 2c -c OpenDJ@OpenDJ localhost:11161
SNMPv2-SMI::mib-2.66.1.1.1.1 = STRING: "OpenDJ 3.0.0..."
SNMPv2-SMI::mib-2.66.1.1.2.1 = STRING: "/path/to/opendj"
...
```

17.3 JMX-Based Monitoring

OpenDJ provides JMX-based monitoring. A number of tools support JMX, including **jconsole** and **jvisualvm**, which are bundled with the Sun/Oracle Java platform. JMX is not configured by default. Use the **dsconfig** command to configure the JMX connection handler:

Interface stability: Evolving (See Section I.2, “ForgeRock Product Interface Stability” in the *OpenDJ Reference*)

```
$ dsconfig \
  set-connection-handler-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "JMX Connection Handler" \
    --set enabled:true \
    --trustAll \
    --no-prompt
```


By default, no users have privileges to access the JMX connection. The following command adds JMX privileges for Directory Manager:

```
$ dsconfig \
  set-root-dn-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --add default-root-privilege-name:jmx-notify \
    --add default-root-privilege-name:jmx-read \
    --add default-root-privilege-name:jmx-write \
    --trustAll \
    --no-prompt
```

You must also configure security to login remotely. See the section on *Using SSL* in [Monitoring and Management Using JMX](#) for hints.

Alternatively, you can connect to a local server process by using the server process identifier:

```
$ cat ../logs/server.pid
3363
$ jvisualvm --openpid 3363 &
```

17.4 Server Operation and Tasks

OpenDJ comes with two commands for monitoring server processes and tasks. The **status** command, described in `status(1)` in the *OpenDJ Reference*, displays basic information about the local server, similar to what is seen in the default window of the control panel. The **manage-tasks** command, described in `manage-tasks(1)` in the *OpenDJ Reference*, lets you manage tasks scheduled on a server, such as nightly backup.

The **status** command takes administrative credentials to read the configuration, as does the control panel:

```
$ status --bindDN "cn=Directory Manager" --bindPassword password
```

```

    --- Server Status ---
Server Run Status:      Started
Open Connections:      1

    --- Server Details ---
Host Name:              localhost
Administrative Users:   cn=Directory Manager
Installation Path:      /path/to/openssl
Version:               OpenDJ 3.0.0
Java Version:           version
Administration Connector: Port 4444 (LDAPS)

```

```

    --- Connection Handlers ---
Address:Port : Protocol : State
-----
--           : LDIF    : Disabled
0.0.0.0:636   : LDAPS   : Disabled
0.0.0.0:1389  : LDAP    : Enabled
0.0.0.0:1689  : JMX     : Disabled

```

```

    --- Data Sources ---
Base DN:         dc=example,dc=com
Backend ID:      userRoot
Entries:         163
Replication:     Disabled

```

The **manage-tasks** command connects over the administration port, and so can connect to both local and remote servers:

```
$ manage-tasks \
--hostname opendj.example.com \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--trustAll \
--no-prompt
```

ID	Type	Status
example	Backup	Recurring
example-201106230300000000	Backup	Waiting on start time

17.5 Server Logs

By default OpenDJ stores access and errors logs, and a server process ID file under the logs/ directory. For the replication service, OpenDJ also keeps a replication log there. You can also configure a debug log. You can also configure policies about how logs are rotated, and how they are retained. You configure logging using the **dsconfig** command.

Each log depends on a *log publisher*, whose type corresponds to the type of log. OpenDJ provides a number of file-based log publishers out of the box, and supports the ForgeRock common audit event framework, sometimes referred to as Common Audit. The ForgeRock common audit event framework provides log handlers for publishing to CSV files, relational databases, and the UNIX system log (Syslog) as described in [Section 17.5.2, "Common ForgeRock Access Logs"](#). The framework makes it possible to plug in additional handlers as well.

17.5.1 Access Logs

The *access log* traces the operations the server processes including timestamps, connection information, and information about the operation itself. The access log can grow quickly, as each client request results in at least one new log message.

The following access log excerpt shows a search operation from the local host, with the first three lines wrapped for readability:

```
[21/Jun/2011:08:01:53 +0200] CONNECT conn=4 from=127.0.0.1:49708
to=127.0.0.1:1389 protocol=LDAP
[21/Jun/2011:08:01:53 +0200] SEARCH REQ conn=4 op=0 msgID=1
base="dc=example,dc=com" scope=wholeSubtree filter="(uid=bjensen)" attrs="ALL"
[21/Jun/2011:08:01:53 +0200] SEARCH RES conn=4 op=0 msgID=1
result=0 nentries=1 etime=3
[21/Jun/2011:08:01:53 +0200] UNBIND REQ conn=4 op=1 msgID=2
[21/Jun/2011:08:01:53 +0200] DISCONNECT conn=4 reason="Client Unbind"
```

Notice that by default OpenDJ directory server logs a message for the search request, and a message for the search response.¹ The server also logs request and response messages for other operations that have responses, such as bind and modify operations. The server does not log response messages for all operations, as some operations, such as persistent searches, abandon operations, unbind operations, and abandoned operations, do not have responses. In the preceding excerpt, notice that the log message for the unbind request is followed by a log message for the disconnection.

17.5.2 Common ForgeRock Access Logs

In addition to the default file-based access log formats, OpenDJ directory server supports the ForgeRock common audit event framework. OpenDJ uses the framework to write access logs in formats that are compatible with all products using the framework. The framework uses transaction IDs that make it easy to

¹ You can also configure the access logger to combine log messages by setting the property `log-format:combined`. The setting is useful when filtering messages based on response criteria. It causes the server to log one message per operation, rather than one message for the request and another for the response.

correlate requests as they traverse the platform. This makes it easier to monitor activity and to enrich reports.

Interface stability: Evolving (See Section I.2, “ForgeRock Product Interface Stability” in the *OpenDJ Reference*)

The ForgeRock common audit event framework is built around audit event handlers. Audit event handlers can encapsulate their own configurations. Audit event handlers are the same in each product in the ForgeRock platform. As a result, you can plug in custom handlers that comply with the framework without having to upgrade OpenDJ directory server.

The ForgeRock common audit event framework includes handlers for logging audit event messages to local files and facilities, as well as to remote systems. Handlers for the following are supported:

- CSV files, with support for tamper-evident logs.

OpenDJ supports LDAP and HTTP CSV access logs, which you must configure in order to use.

- Relational database using JDBC.

You configure the JDBC handler as an external log publisher that logs access messages to a relational database.

- The UNIX system log facility.

Although it is rarely used for access events, you can configure the Syslog handler as an external log publisher that logs access messages to the UNIX Syslog facility.

The ForgeRock common audit event framework supports a variety of audit event topics. OpenDJ currently supports handling for access events, which are system boundary events such as the initial request and final response to that request. In other words, the implementation in OpenDJ is focused only on access logging. Based on the connection handler for the request, OpenDJ divides access events into `ldap-access` events and `http-access` events.

To enable common audit-based logging, follow one of these procedures:

- [Procedure 17.1, "To Enable LDAP CSV Access Logs"](#)
- [Procedure 17.2, "To Enable HTTP CSV Access Logs"](#)
- [Procedure 17.4, "To Enable External LDAP or HTTP Access Logging"](#)

Procedure 17.1. To Enable LDAP CSV Access Logs

After you complete the following steps, OpenDJ directory server records LDAP access event messages in files named like `logs/ldap-access.csv`:

1. If you trust transaction IDs sent by client applications, and want monitoring and reporting systems consuming the logs to allow correlation of requests as they traverse multiple servers, update the global server configuration as described in [Procedure 17.5, "To Trust Transaction IDs"](#).
2. Create an enabled CSV File Access Log Publisher with optional rotation and retention policies as in the following example:

```
$ dsconfig \
create-log-publisher \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--publisher-name "Common Audit Csv File Access Logger" \
--type csv-file-access \
--set enabled:true \
--set "rotation-policy:24 Hours Time Limit Rotation Policy" \
--set "rotation-policy:Size Limit Rotation Policy" \
--set "retention-policy:File Count Retention Policy" \
--trustAll \
--no-prompt
```

You can view the log publisher properties to check your work as in the following example:

```
$ dsconfig \
  get-log-publisher-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --publisher-name "Common Audit Csv File Access Logger" \
  --trustAll \
  --no-prompt
Property          : Value(s)
-----
csv-delimiter-char : ","
enabled           : true
filtering-policy   : no-filtering
key-store-file     : -
key-store-pin-file : -
log-control-oids   : false
log-directory      : logs
retention-policy   : File Count Retention Policy
rotation-policy    : 24 Hours Time Limit Rotation Policy, Size Limit Rotation
tamper-evident     : false
```

Notice that when setting the CSV File Access Log Publisher properties, you can set the log directory, but you cannot change the log file name, which contains `ldap-access`.

3. If you require tamper-evident logs, prepare a keystore as described in [Procedure 17.3, "To Prepare a Keystore for Tamper-Evident Logs"](#). Then enable tamper-evident capability as in the following example:

```
$ dsconfig \
  set-log-publisher-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --publisher-name "Common Audit Csv File Access Logger" \
  --set tamper-evident:true \
  --set key-store-file:config/audit-keystore \
  --set key-store-pin-file:config/audit-keystore.pin \
  --trustAll \
  --no-prompt
```

Tamper-evident logging relies on digital signatures and regularly flushing messages to the log system. In high-volume directory deployments with heavy access patterns, signing log messages has a severe negative impact on server performance, reducing throughput by orders of magnitude.

Make certain that you test the performance impact of tamper-evident logging with realistic access patterns for your deployment before enabling the feature in production.

Procedure 17.2. To Enable HTTP CSV Access Logs

If you have enabled the HTTP connection handler as described in [Procedure 5.7, "To Set Up REST Access to OpenDJ Directory Server"](#), you might want to enable CSV-format HTTP access logs.

After you complete the following steps, OpenDJ directory server records HTTP access event messages in files named like `logs/http-access.csv`:

1. If you trust transaction IDs sent by client applications, and want monitoring and reporting systems consuming the logs to allow correlation of requests as they traverse multiple servers, update the global server configuration as described in [Procedure 17.5, "To Trust Transaction IDs"](#).
2. Create an enabled CSV File HTTP Access Log Publisher with optional rotation and retention policies as in the following example:

```
$ dsconfig \
  create-log-publisher \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --publisher-name "Common Audit Csv File HTTP Access Logger" \
  --type csv-file-http-access \
  --set enabled:true \
  --set "rotation-policy:24 Hours Time Limit Rotation Policy" \
  --set "rotation-policy:Size Limit Rotation Policy" \
  --set "retention-policy:File Count Retention Policy" \
  --trustAll \
  --no-prompt
```

You can view the log publisher properties to check your work as in the following example:

```
$ dsconfig \
get-log-publisher-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--publisher-name "Common Audit Csv File HTTP Access Logger" \
--trustAll \
--no-prompt
Property          : Value(s)
-----
csv-delimiter-char : ","
enabled            : true
key-store-file     : -
key-store-pin-file : -
log-directory      : logs
retention-policy   : File Count Retention Policy
rotation-policy    : 24 Hours Time Limit Rotation Policy, Size Limit Rotation
                   : Policy
tamper-evident     : false
```

Notice that when setting the CSV File HTTP Access Log Publisher properties, you can set the log directory, but you cannot change the log file name, which contains http-access.

3. If you require tamper-evident logs, prepare a keystore as described in [Procedure 17.3, "To Prepare a Keystore for Tamper-Evident Logs"](#). Then enable tamper-evident capability as in the following example:

```
$ dsconfig \
set-log-publisher-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--publisher-name "Common Audit Csv File HTTP Access Logger" \
--set tamper-evident:true \
--set key-store-file:config/audit-keystore \
--set key-store-pin-file:config/audit-keystore.pin \
--trustAll \
--no-prompt
```

Tamper-evident logging relies on digital signatures and regularly flushing messages to the log system. In high-volume directory deployments with heavy access patterns, signing log messages has a severe negative impact on server performance, reducing throughput by orders of magnitude.

Make certain that you test the performance impact of tamper-evident logging with realistic access patterns for your deployment before enabling the feature in production.

Procedure 17.3. To Prepare a Keystore for Tamper-Evident Logs

Tamper-evident logging depends on a public key/private key pair and on a secret key that are stored together in a JCEKS keystore. Follow these steps to prepare the keystore:

1. Create a password for the keystore.

The following example uses the default file name. If you use a different filename, then you must edit `key-store-pin-file` property when configuring the log publisher:

```
$ echo password > /path/to/opensj/config/audit-keystore.pin
$ chmod 400 /path/to/opensj/config/audit-keystore.pin
```

2. Generate a key pair in the keystore.

The CSV event handler expects a JCEKS-type keystore with a key alias of `Signature` for the signing key, where the key is generated with the RSA key algorithm and the SHA256withRSA signature algorithm.

The following example uses the default file name. If you use a different filename, then you must edit `key-store-file` property when configuring the log publisher:

```
$ keytool \
-genkeypair \
-keyalg RSA \
-sigalg SHA256withRSA \
-alias "Signature" \
-dname "CN=opensj.example.com,O=Example Corp,C=FR" \
-keystore /path/to/opensj/config/audit-keystore \
-storetype JCEKS \
-storepass `cat /path/to/opensj/config/audit-keystore.pin` \
-keypass `cat /path/to/opensj/config/audit-keystore.pin`
```

3. Generate a secret key in the keystore.

The CSV event handler expects a JCEKS-type keystore with a key alias of `Password` for the symmetric key, where the key is generated with the HmacSHA256 key algorithm and 256-bit key size.

The following example uses the default file name. If you use a different filename, then you must edit `key-store-file` property when configuring the log publisher:

```
$ keytool \  
-genseckey \  
-keyalg HmacSHA256 \  
-keysize 256 \  
-alias "Password" \  
-keystore /path/to/opendj/config/audit-keystore \  
-storetype JCEKS \  
-storepass `cat /path/to/opendj/config/audit-keystore.pin` \  
-keypass `cat /path/to/opendj/config/audit-keystore.pin`
```

4. Verify the contents of the keystore:

```
$ keytool \  
-list \  
-keystore /path/to/opendj/config/audit-keystore \  
-storetype JCEKS \  
-storepass `cat /path/to/opendj/config/audit-keystore.pin`  
  
Keystore type: JCEKS  
Keystore provider: SunJCE  
  
Your keystore contains 2 entries  
  
signature, Nov 27, 2015, PrivateKeyEntry,  
Certificate fingerprint (SHA1): 4D:CF:CC:29:...:8B:6E:68:D1  
password, Nov 27, 2015, SecretKeyEntry,
```

Procedure 17.4. To Enable External LDAP or HTTP Access Logging

External LDAP or HTTP access event logging lets you use a JDBC handler to log to a relational database, a Syslog handler to log to the UNIX Syslog facility, or a custom handler to consume the events in some other way. The configuration depends on the handler, and is provided as a JSON file that corresponds to the handler.

Follow these steps:

1. If you trust transaction IDs sent by client applications, and want monitoring and reporting systems consuming the logs to allow correlation of requests as they traverse multiple servers, update the global server configuration as described in [Procedure 17.5, "To Trust Transaction IDs"](#).
2. Create the JSON configuration file for the external handler, and copy it to the config directory for the OpenDJ directory server.

For details, see [Section 17.5.2.1, "JDBC Audit Event Handler Configuration"](#) and [Section 17.5.2.2, "Syslog Audit Event Handler Configuration"](#).

3. For LDAP access logging, create the External Access Log Publisher as in the following example, which creates a JDBC LDAP access log publisher:

```
$ dsconfig \
create-log-publisher \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--publisher-name "JDBC LDAP Access Log Publisher" \
--type external-access \
--set enabled:true \
--set config-file:config/jdbc-handler.json \
--trustAll \
--no-prompt
```

4. For HTTP access logging, create the External HTTP Access Log Publisher as in the following example, which creates a JDBC HTTP access log publisher:

```
$ dsconfig \
create-log-publisher \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--publisher-name "JDBC HTTP Access Log Publisher" \
--type external-http-access \
--set enabled:true \
--set config-file:config/jdbc-handler.json \
--trustAll \
--no-prompt
```

5. For a custom access logger, follow these general steps:
 - a. Copy the .jar file for the custom audit event handler to /path/to/opendj/lib/extensions.
 - b. Prepare the JSON configuration file for the custom handler.
 - c. Create an External Access Log Publisher or External HTTP Access Log Publisher configuration as appropriate for the custom access logger.

Procedure 17.5. To Trust Transaction IDs

Client applications using the ForgeRock common audit event framework send transaction IDs with their requests. The transaction IDs are used to correlate audit events for monitoring and reporting that trace the request through multiple applications.

Transaction IDs are sent over LDAP using an internal OpenDJ request control. They are sent over HTTP in an HTTP header.

By default, OpenDJ directory server is configured not to trust transaction IDs sent with client application requests. The default transaction ID is used instead. The default transaction ID is zero: 0.

- Set the advanced global server property, `trust-transaction-ids`, to `true`:

```
$ dsconfig \
  set-global-configuration-prop \
  --advanced \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set trust-transaction-ids:true \
  --trustAll \
  --no-prompt
```

At this point transaction IDs are trusted, and can be written to the logs.

17.5.2.1 JDBC Audit Event Handler Configuration

The JDBC audit event handler that responds to events by logging messages to an appropriately configured relational database table. This section briefly describes the JSON configuration file for the handler.

The JSON file has the following format:

```
{
  "class": "org.forgerock.audit.handlers.jdbc.JdbcAuditEventHandler",
  "config": {
    "name": string,
    "topics": array,
    "databaseType": string,
    "enabled": boolean,
    "buffering": {
      "enabled": boolean,
      "writeInterval": duration,
      "autoFlush": boolean,
      "maxBatchedEvents": number,
      "maxSize": number,
      "writerThreads": number
    },
    "connectionPool": {
      "dataSourceClassName": string,
      "jdbcUrl": string,
      "username": string,
      "password": string,
      "autoCommit": boolean,
      "connectionTimeout": number,

```

```
        "idleTimeout": number,
        "maxLifetime": number,
        "minIdle": number,
        "maxPoolSize": number,
        "poolName": string
    },
    "tableMappings": [
        {
            "event": string,
            "table": string,
            "fieldToColumn": {
                "event-field": "database-column"
            }
        }
    ]
}
```

The class field identifies the handler.

The "config" object has the following properties:

"name": *string, required*

The name of the event handler.

"topics": *array of strings, required*

The topics that this event handler intercepts.

OpenDJ supports handling access events that occur at the system boundary, such as arrival of the initial request and departure of the final response.

Set this to "topics": ["access"].

"databaseType": *string, required*

The database type name.

Built-in support is provided for oracle, mysql, and h2. Unrecognized database types rely on a GenericDatabaseStatementProvider.

"enabled": *boolean, optional*

Whether this event handler is active.

Default: true.

"buffering": *object, optional*

Buffering settings for sending messages to the database. The default is for messages to be written to the log file for each event.

The buffering object has the following fields:

"enabled": *boolean, optional*

Whether log buffering is enabled.

Default: false.

"writeInterval": *duration, required*

The interval at which to send buffered event messages to the database.

This interval must be greater than 0 if buffering is enabled.

A duration is a lapse of time expressed in English, such as 23 hours 59 minutes and 59 seconds.

Durations are not case sensitive.

Negative durations are not supported.

The following units can be used in durations:

- indefinite, infinity, undefined, unlimited: unlimited duration
- zero, disabled: zero-length duration
- days, day, d: days
- hours, hour, h: hours
- minutes, minute, min, m: minutes
- seconds, second, sec, s: seconds
- milliseconds, millisecond, millisec, millis, milli, ms: milliseconds
- microseconds, microsecond, microsec, micros, micro, us: microseconds
- nanoseconds, nanosecond, nanosec, nanos, nano, ns: nanoseconds

"autoFlush": *boolean, optional*

Whether the events are automatically flushed after being written.

Default: true.

"maxBatchedEvents": *number, optional*

The maximum number of event messages batched into a [PreparedStatement](#).

Default: 100.

"maxSize": *number, optional*

The maximum size of the queue of buffered event messages.

Default: 5000.

"writerThreads": *number, optional*

The number of threads to write buffered event messages to the database.

Default: 1.

"connectionPool": *object, required*

Connection pool settings for sending messages to the database.

The connection pool object has the following fields:

"dataSourceClassName": *string, optional*

The class name of the data source for the database.

"jdbcUrl": *string, required*

The JDBC URL to connect to the database.

"username": *string, required*

The username identifier for the database user with access to write the messages.

"password": *number, optional*

The password for the database user with access to write the messages.

"autoCommit": *boolean, optional*

Whether to commit transactions automatically when writing messages.

Default: true.

"connectionTimeout": *number, optional*

The number of milliseconds to wait for a connection from the pool before timing out.

Default: 30000.

"idleTimeout": *number, optional*

The number of milliseconds to allow a database connection to remain idle before timing out.

Default: 600000.

"maxLifetime": *number, optional*

The number of milliseconds to allow a database connection to remain in the pool.

Default: 1800000.

"minIdle": *number, optional*

The minimum number of idle connections in the pool.

Default: 10.

"maxPoolSize": *number, optional*

The maximum number of connections in the pool.

Default: 10.

"poolName": *string, optional*

The name of the connection pool.

"tableMappings": *array of objects, required*

Table mappings for directing event content to database table columns.

A table mappings object has the following fields:

"event": *string, required*

The audit event that the table mapping is for.

Set this to access.

"table": *string, required*

The name of the database table that corresponds to the mapping.

"fieldToColumn": *object, required*

This object maps the names of audit event fields to database columns, where the keys and values are both strings.

Audit event fields use JSON pointer notation, and are taken from the JSON schema for the audit event content.

17.5.2.2 Syslog Audit Event Handler Configuration

The Syslog audit event handler that responds to events by logging messages to the UNIX system log as governed by RFC 5424, [The Syslog Protocol](#). This section briefly describes the JSON configuration file for the handler.

The JSON file has the following format:


```
{
  "class": "org.forgerock.audit.handlers.syslog.SyslogAuditEventHandler",
  "config": {
    "name": string,
    "topics": array,
    "protocol": string,
    "host": string,
    "port": number,
    "connectTimeout": number,
    "facility": "string",
    "buffering": {
      "enabled": boolean,
      "maxSize": number
    },
    "severityFieldMappings": [
      {
        "topic": string,
        "field": string,
        "valueMappings": {
          "field-value": "syslog-severity"
        }
      }
    ]
  }
}
```

The class field identifies the handler.

The "config" object has the following properties:

"name": *string, required*

The name of the event handler.

"topics": *array of strings, required*

The topics that this event handler intercepts.

OpenDJ supports handling access events that occur at the system boundary, such as arrival of the initial request and departure of the final response.

Set this to "topics": ["access"].

"protocol": *string, required*

The transport protocol used to send event messages to the Syslog daemon.

Set this to TCP for Transmission Control Protocol, or to UDP for User Datagram Protocol.

"host": *string, required*

The hostname of the Syslog daemon to which to send event messages. The hostname must resolve to an IP address.

"port": *number, required*

The port of the Syslog daemon to which to send event messages.

The value must be between 0 and 65535.

"connectTimeout": *number, required when using TCP*

The number of milliseconds to wait for a connection before timing out.

"facility": *string, required*

The Syslog facility to use for event messages.

Set this to one of the following values:

kern

Kernel messages

user

User-level messages

mail

Mail system

daemon

System daemons

auth

Security/authorization messages

syslog

Messages generated internally by syslogd

lpr

Line printer subsystem

news

Network news subsystem

uucp

UUCP subsystem

cron

Clock daemon

authpriv

Security/authorization messages

ftp

FTP daemon

ntp

NTP subsystem

logaudit

Log audit

logalert
Log alert

clockd
Clock daemon

local0
Local use 0

local1
Local use 1

local2
Local use 2

local3
Local use 3

local4
Local use 4

local5
Local use 5

local6
Local use 6

local7
Local use 7

"buffering": *object, optional*

Buffering settings for writing to the system log facility. The default is for messages to be written to the log for each event.

The buffering object has the following fields:

"enabled": *boolean, optional*

Whether log buffering is enabled.

Default: false.

"maxSize": *number, optional*

The maximum number of buffered event messages.

Default: 5000.

"severityFieldMappings": *object, optional*

Severity field mappings set the correspondence between audit event fields and Syslog severity values.

The severity field mappings object has the following fields:

"topic": *string, required*

The audit event topic to which the mapping applies.

Set this to access.

"field": *string, required*

The audit event field to which the mapping applies.

Audit event fields use JSON pointer notation, and are taken from the JSON schema for the audit event content.

"valueMappings": *object, required*

The map of audit event values to Syslog severities, where both the keys and the values are strings.

Syslog severities are one of the following values:

emergency

System is unusable.

alert

Action must be taken immediately.

critical

Critical conditions.

error

Error conditions.

warning

Warning conditions.

notice

Normal but significant condition.

informational

Informational messages.

debug

Debug-level messages.

17.5.3 Error Logs

The *errors log* traces server events, error conditions, and warnings, categorized and identified by severity.

The following errors log excerpt shows log entries for a backup task, with lines wrapped for readability:

```
[06/Oct/2015:16:58:15 +0200] category=... severity=NOTICE msgID=...
msg=Backup task 20151006165815904 started execution
[06/Oct/2015:16:58:15 +0200] category=TASK severity=NOTICE msgID=...
msg=Starting backup for backend userRoot
[06/Oct/2015:16:58:16 +0200] category=UTIL severity=NOTICE msgID=...
msg=Archived backup file: dj
...
[06/Oct/2015:16:58:16 +0200] category=UTIL severity=NOTICE msgID=...
msg=Archived backup file: tasks.ldif
[06/Oct/2015:16:58:16 +0200] category=TASK severity=NOTICE msgID=...
msg=The backup process completed successfully
[06/Oct/2015:16:58:16 +0200] category=... severity=NOTICE msgID=...
msg=Backup task 20151006165815904 finished execution in the state
    Completed successfully
```

17.5.4 HTTP Access Logs

For the HTTP Connection Handler, OpenDJ maintains a separate access log in `logs/http-access`. This access log, by default configured as the File Based HTTP Access Log Publisher, uses a different format than the LDAP access log. This HTTP access log uses [Extended Log File Format](#) with fields described in [Microsoft's implementation](#) as well.

Interface stability: Evolving (See Section I.2, “ForgeRock Product Interface Stability” in the *OpenDJ Reference*)

The following default fields are shown here in the order they occur in the log file:

`cs-host`

Client host name

`c-ip`

Client IP address

`cs-username`

Username used to authenticate

`x-datetime`

Completion timestamp for the HTTP request, which you can configure using the `log-record-time-format` property

`cs-method`

HTTP method requested by the client

`cs-uri-query`

Path and query string requested by the client

cs-version
HTTP version requested by the client

sc-status
HTTP status code for the operation

cs(User-Agent)
User-Agent identifier

x-connection-id
Connection ID used for OpenDJ internal operations

When using this field to match HTTP requests with internal operations in the LDAP access log, first set the access log advanced property, `suppress-internal-operations`, to `false`. By default, internal operations do not appear in the LDAP access log.

x-etime
Execution time in milliseconds needed by OpenDJ to service the HTTP request

x-transaction-id
ForgeRock common audit event framework transaction ID for the request

This defaults to 0 unless you configure OpenDJ to trust transaction IDs as described in [Procedure 17.5, "To Trust Transaction IDs"](#).

Missing values are replaced with -. Tabs separate the fields, and if a field contains a tab character, then the field is surrounded with double quotes. OpenDJ then doubles double quotes in the field to escape them.

The following example shows an excerpt of an HTTP access log with the default configuration. Lines are folded and space reformatted for the printed page:

```
- 192.168.0.15 bjensen 22/May/2013:10:06:18 +0200
GET /users/bjensen?_prettyPrint=true HTTP/1.1 200
curl/7.21.4 3 40
- 192.168.0.15 bjensen 22/May/2013:10:06:52 +0200
GET /groups/Directory%20Administrators?_prettyPrint=true HTTP/1.1 200
curl/7.21.4 4 41
- 192.168.0.12 bjensen 22/May/2013:10:07:07 +0200
GET /users/missing?_prettyPrint=true HTTP/1.1 200
curl/7.21.4 5 9
- 192.168.0.12 - 22/May/2013:10:07:46 +0200
GET /users/missing?_prettyPrint=true HTTP/1.1 401
curl/7.21.4 6 0
- 192.168.0.15 kvaughan 22/May/2013:10:09:10 +0200
POST /users?_action=create&_prettyPrint=true HTTP/1.1 200
curl/7.21.4 7 120
```

You can configure the log-format for the access log using the **dsconfig** command.

In addition to the default fields, the following standard fields are supported:

- c-port
Client port number
- s-computername
Server name where the access log was written
- s-ip
Server IP address
- s-port
Server port number

17.5.5 Replication Logs

The *replication log* traces replication events, with entries similar to the errors log. The following excerpt has lines wrapped for readability:

```
[22/Jun/2011:14:37:34 +0200] category=SYNC severity=NOTICE msgID=15139026
msg=Finished total update: exported domain "dc=example,dc=com" from this
directory server DS(24065) to all remote directory servers.
[22/Jun/2011:14:37:35 +0200] category=SYNC severity=MILD_WARNING msgID=14745663
msg=Replication server RS(23947) at opendj.example.com/10.10.0.168:8989 has
closed the connection to this directory server DS(24065). This directory
server will now try to connect to another replication server in order to
receive changes for the domain "dc=example,dc=com"
[22/Jun/2011:14:37:35 +0200] category=SYNC severity=NOTICE msgID=15138894
msg=The generation ID for domain "dc=example,dc=com" has been reset to 3679640
```

Notice that the replication log does not trace replication operations. Use the external change log instead to get notifications about changes to directory data over protocol. You can alternatively configure an audit log, which is a type of access log that dumps changes in LDIF.

17.5.6 Debug Logs

A *debug log* traces details needed to troubleshoot a problem in the server. Debug logs can grow large quickly, and therefore no debug logs are enabled by default.

For debug logging, you must set a *debug target* to control what gets logged.

17.5.7 Log Rotation and Retention

Each file-based log can be associated with a *log rotation policy*, and a *log retention policy*. The former can specify when, after how much time, or at what

maximum size a log is rotated. The latter can specify a maximum number or size of logs to retain, or an amount of free disk space to maintain. The design allows for custom policies as well.

By default the file-based logs are subject to rotation and retention policies that you can list with **dsconfig list-log-rotation-policies** and **dsconfig list-log-retention-policies**.

For example, view the log rotation policies with the following command:

```
$ dsconfig \
list-log-rotation-policies \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password
```

Log Rotation Policy	Type	file-size-limit	rotation-interval	time-of-day
24 Hours Time Limit Rotation Policy	time-limit	-	1 d	-
7 Days Time Limit Rotation Policy	time-limit	-	1 w	-
Fixed Time Rotation Policy	fixed-time	-	-	2359
Size Limit Rotation Policy	size-limit	100 mb	-	-

View the log retention policies with the following command:

```
$ dsconfig \
list-log-retention-policies \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password
```

Log Retention Policy	Type	disk-space-used	free-disk-space	number-of-files
File Count Retention Policy	file-count	-	-	10
Free Disk Space Retention Policy	free-disk-space	-	500 mb	-
Size Limit Retention Policy	size-limit	500 mb	-	-

Use the **dsconfig get-log-publisher-prop** command to examine the policies that apply to a particular logger:


```
$ dsconfig \
  get-log-publisher-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --publisher-name "File-Based Access Logger" \
  --property retention-policy \
  --property rotation-policy
Property      : Value(s)
-----
retention-policy : File Count Retention Policy
rotation-policy  : 24 Hours Time Limit Rotation Policy, Size Limit Rotation
                  : Policy
```

In other words, by default OpenDJ keeps 10 access log files, rotating the access log each day, or when the log size reaches 100 MB.

The **dsconfig** command offers a number of subcommands for creating and deleting log rotation and retention policies, and for setting policy properties. You can update which policies apply to a logger by using the **dsconfig set-log-publisher-prop** command.

17.5.8 Log Filtering

Each time a client application sends a request to OpenDJ, the server writes to its access log. As shown above, a simple search operation results in five messages written to the access log. This volume of logging gives you the information to analyze overall access patterns, or to audit access when you do not know in advance what you are looking for.

When you do know what you are looking for, log filtering lets you limit what the server logs, and focus on what you want to see. You define the filter criteria, and also set the filtering policy.

You can filter both access and also audit logs.

Log filtering lets you define rules based these criteria:

- Client IP address, bind DN, group membership
- Port number
- Protocol used (such as LDAP, LDAPS, JMX)
- Response times
- Result codes (only log error results, for example)

- Search response criteria (number of entries returned, whether the search was indexed)
- Target DN
- Type of operation (connect, bind, add, delete, modify, rename, search, etc.)

The filtering policy in the log publisher configuration specifies whether to include or exclude log messages that match the criteria you define. OpenDJ does not filter logs until you update the log publisher configuration.

Example 17.1. Example: Exclude Control Panel-Related Messages

A common development troubleshooting technique consists of sending client requests while tailing the access log:

```
$ tail -f /path/to/openssl/logs/access
```

The trouble is, when OpenDJ control panel is running, or when you are also adapting your configuration using the **dsconfig** command, OpenDJ writes access log messages related to administration. These might prevent you from noticing the messages that interest you.

This example demonstrates how to filter out access log messages due to administrative connections over LDAPS on ports 1636 and 4444.

Create access log filtering criteria rules:

```
$ dsconfig \
  create-access-log-filtering-criteria \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --publisher-name "File-Based Access Logger" \
  --criteria-name "Exclude LDAPS on 1636 and 4444" \
  --type generic \
  --set connection-port-equal-to:1636 \
  --set connection-port-equal-to:4444 \
  --set connection-protocol-equal-to:ldaps \
  --trustAll \
  --no-prompt
```

Activate filtering to exclude messages from the default access log according to the criteria you specified:

```
$ dsconfig \
  set-log-publisher-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --publisher-name "File-Based Access Logger" \
  --set filtering-policy:exclusive \
  --trustAll \
  --no-prompt
```

At this point, OpenDJ filters out connections over LDAPS to ports 1636 and 4444. While performing operations in OpenDJ control panel, if you perform a simple **ldapsearch --port 1389 --baseDN dc=example,dc=com uid=bjensen cn**, then all you see in the access log is the effect of the **ldapsearch** command:

```
$ tail -f /path/to/opendj/logs/access
[19/Oct/2011:16:37:16 +0200] CONNECT conn=8 from=127.0.0.1:54165
to=127.0.0.1:1389 protocol=LDAP
[19/Oct/2011:16:37:16 +0200] SEARCH REQ conn=8 op=0 msgID=1
base="dc=example,dc=com" scope=wholeSubtree filter="(uid=bjensen)" attrs="cn"
[19/Oct/2011:16:37:16 +0200] SEARCH RES conn=8 op=0 msgID=1 result=0 nentries=1
etime=14
[19/Oct/2011:16:37:16 +0200] UNBIND REQ conn=8 op=1 msgID=2
[19/Oct/2011:16:37:16 +0200] DISCONNECT conn=8 reason="Client Unbind"
```

In addition to the filtering policy, you can also adjust how OpenDJ writes log messages. By default, OpenDJ writes one log message for a request, and another for a response. You can set the log publisher property `log-format` to `combined` to have OpenDJ write a single message per operation. This can be helpful, for example, when evaluating response times. In addition, you can change the log message time stamps with `log-record-time-format`, and specify whether to log LDAP control OIDs for operations by setting `log-control-oids` to `true`.

17.6 Alert Notifications

OpenDJ can send alerts to provide notifications of significant server events. Yet alert notifications are not enabled by default. You can use the **dsconfig** command to enable alert notifications:

```
$ dsconfig \
  set-alert-handler-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "JMX Alert Handler" \
    --set enabled:true \
    --trustAll \
    --no-prompt
```

OpenDJ can also send mail over SMTP instead of JMX notifications. Before you set up the SMTP-based alert handler, you must identify an SMTP server to which OpenDJ sends messages:

```
$ dsconfig \
  set-global-configuration-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --set smtp-server:smtp.example.com \
    --trustAll \
    --no-prompt

$ dsconfig \
  create-alert-handler \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --handler-name "SMTP Alert Handler" \
    --type smtp \
    --set enabled:true \
    --set message-subject:"OpenDJ Alert, Type: %%alert-type%%, ID: %%alert-id%%" \
    --set message-body:"%%alert-message%%" \
    --set recipient-address:kvaughan@example.com \
    --set sender-address:opendj@example.com \
    --trustAll \
    --no-prompt
```

Alert Types

OpenDJ directory server uses the following types when sending alerts. For alert types that indicate server problems, check `OpenDJ/logs/errors` for details.

`org.opens.server.AccessControlDisabled`
The access control handler has been disabled.

`org.opens.server.AccessControlEnabled`
The access control handler has been enabled.

`org.opensds.server.authentication.dseecompat.ACIParseFailed`

The dseecompat access control subsystem failed to correctly parse one or more ACI rules when the server first started.

`org.opensds.server.BackendRunRecovery`

The pluggable backend has thrown a `RunRecoveryException`. The directory server needs to be restarted.

`org.opensds.server.CannotCopySchemaFiles`

A problem has occurred while attempting to create copies of the existing schema configuration files before making a schema update, and the schema configuration has been left in a potentially inconsistent state.

`org.opensds.server.CannotRenameCurrentTaskFile`

The directory server is unable to rename the current tasks backing file in the process of trying to write an updated version.

`org.opensds.server.CannotRenameNewTaskFile`

The directory server is unable to rename the new tasks backing file into place.

`org.opensds.server.CannotScheduleRecurringIteration`

The directory server is unable to schedule an iteration of a recurring task.

`org.opensds.server.CannotWriteConfig`

The directory server is unable to write its updated configuration for some reason and therefore the server may not exhibit the new configuration if it is restarted.

`org.opensds.server.CannotWriteNewSchemaFiles`

A problem has occurred while attempting to write new versions of the server schema configuration files, and the schema configuration has been left in a potentially inconsistent state.

`org.opensds.server.CannotWriteTaskFile`

The directory server is unable to write an updated tasks backing file for some reason.

`org.opensds.server.DirectoryServerShutdown`

The directory server has begun the process of shutting down.

`org.opensds.server.DirectoryServerStarted`

The directory server has completed its startup process.

`org.opensds.server.DiskFull`

Free disk space has reached the full threshold.

Default is 20 MB.

- `org.opens.server.DiskSpaceLow`
Free disk space has reached the low threshold.

Default is 100 MB.
- `org.opens.server.EnteringLockdownMode`
The directory server is entering lockdown mode, wherein only root users are allowed to perform operations and only over the loopback address.
- `org.opens.server.LDAPHandlerDisabledByConsecutiveFailures`
Consecutive failures have occurred in the LDAP connection handler and have caused it to become disabled.
- `org.opens.server.LDAPHandlerUncaughtError`
Uncaught errors in the LDAP connection handler that have caused it to become disabled.
- `org.opens.server.LDIFBackendCannotWriteUpdate`
An LDIF backend was unable to store an updated copy of the LDIF file after processing a write operation.
- `org.opens.server.LDIFConnectionHandlerIOError`
The LDIF connection handler encountered an I/O error that prevented it from completing its processing.
- `org.opens.server.LDIFConnectionHandlerParseError`
The LDIF connection handler encountered an unrecoverable error while attempting to parse an LDIF file.
- `org.opens.server.LeavingLockdownMode`
The directory server is leaving lockdown mode.
- `org.opens.server.ManualConfigEditHandled`
The directory server detects that its configuration has been manually edited with the server online and those changes were overwritten by another change made through the server. The manually edited configuration will be copied to another location.
- `org.opens.server.ManualConfigEditLost`
The directory server detects that its configuration has been manually edited with the server online and those changes were overwritten by another change made through the server. The manually edited configuration could not be preserved due to an unexpected error.
- `org.opens.server.replication.UnresolvedConflict`
Multimaster replication cannot resolve a conflict automatically.
- `org.opens.server.UncaughtException`
A directory server thread has encountered an uncaught exception that caused that thread to terminate abnormally. The impact that this problem has

on the server depends on which thread was impacted and the nature of the exception.

`org.opens.server.UniqueAttributeSynchronizationConflict`

A unique attribute conflict has been detected during synchronization processing.

`org.opens.server.UniqueAttributeSynchronizationError`

An error occurred while attempting to perform unique attribute conflict detection during synchronization processing.

Chapter 18

Tuning Servers For Performance

This chapter suggests ways to measure and improve directory service performance. In this chapter you will learn to:

- Define directory server performance goals operationally in accordance with the needs of client applications
- Identify constraints that might limit achievable performance goals
- Design and execute appropriate performance tests with the help of OpenDJ command-line tools
- Adjust OpenDJ and system settings to achieve performance goals

Server tuning refers to the art of adjusting server, JVM, and system configuration to meet the service-level performance requirements of directory clients. In the optimal case you achieve service-level performance requirements without much tuning at all, perhaps only setting JVM runtime options when installing OpenDJ.

If you are reading this chapter, however, you are probably not facing an optimal situation. Instead you are looking for trade offs that maximize performance for clients given the constraints of your deployment.

18.1 Defining Performance Requirements and Constraints

Your key performance requirement is most likely to satisfy your users or customers with the resources available to you. Before you can solve potential performance problems, define what those users or customers expect, and determine what resources you will have to satisfy their expectations.

18.1.1 Service-Level Agreements

Service-level agreement (SLA) is a formal name for what directory client applications and the people who run them expect from your service in terms of performance.

SLAs might cover many aspects of the directory service. Whether or not your SLA is formally defined, you ought to know what is expected, or at least what you provide, in the following four areas:

- Directory service *response times*

Directory service response times range from less than a millisecond on average across a low latency connection on the same network to however long it takes your network to deliver the response. More important than average or best response times is the response time distribution, because applications set timeouts based on worst case scenarios. For example, a response time performance requirement might be defined as, *Directory response times must average less than 10 milliseconds for all operations except searches returning more than 10 entries, with 99.9% of response times under 40 milliseconds.*

- Directory service *throughput*

Directory service throughput can range up to many thousands of operations per second. In fact there is no upper limit for read operations such as searches, because only write operations must be replicated. To increase read throughput, simply add additional replicas. More important than average throughput is peak throughput. You might have peak write throughput in the middle of the night when batch jobs update entries in bulk, and peak binds for a special event or first thing Monday morning. For example, a throughput performance requirement might be expressed as, *The directory service must sustain a mix of 5,000 operations per second made up of 70% reads, 25% modifies, 3% adds, and 2% deletes.*

Even better is to mimic the behavior of key operations for performance testing, so that you understand the patterns of operations in the throughput you need to provide.

- Directory service *availability*

OpenDJ is designed to let you build directory services that are basically available, including during maintenance and even upgrade of individual servers. Yet, in order to reach very high levels of availability, you must make sure not only that the software is designed for availability, but also that your operations execute in such a way as to preserve availability. Availability requirements can be as lax as best effort, or as stringent as 99.999% or more uptime.

Replication is the OpenDJ feature that allows you to build a highly available directory service.

- Directory service administrative support

Be sure to understand how you support your users when they run into trouble. While directory services can help you turn password management into a self-service visit to a web site, some users still need to know what they can expect if they need your help.

Creating an SLA, even if your first version consists of guesses, helps you reduce performance tuning from an open-ended project to a clear set of measurable goals for a manageable project with a definite outcome.

18.1.2 Available Resources

With your SLA in hand, inventory the server, networks, storage, people, and other resources at your disposal. Now is the time to estimate whether it is possible to meet the requirements at all.

If, for example you are expected to serve more throughput than the network can transfer, maintain high-availability with only one physical machine, store 100 GB of backups on a 50 GB partition, or provide 24/7 support all alone, no amount of tweaking available resources is likely to fix the problem.

When checking that the resources you have at least theoretically suffice to meet your requirements, do not forget that high availability in particular requires at least two of everything to avoid single points of failure. Be sure to list the resources you expect to have, when and how long you expect to have them, and why you need them. Also make note of what is missing and why.

In addition to the suggestions in this section, also read Section 2.6, “Hardware” in the *OpenDJ Release Notes*.

18.1.2.1 Server Hardware Recommendations

OpenDJ runs on systems with Java support, and is therefore very portable. OpenDJ tends to perform best on single-board, x86 systems due to low memory latency.

18.1.2.2 Storage Recommendations

OpenDJ is designed to work with local storage for the database, not for network file systems such as NFS.

High-performance storage is essential if you need to handle high write throughput.

The Berkeley Java Edition DB, which is the underlying storage for the je backend type, works well with traditional disks as long as the database cache size allows the DB to stay fully cached in memory. This is the case because the database transaction log is append only. When the DB is too big to stay cached in memory, however, then cache misses lead to random disk access, slowing OpenDJ performance.

You might mitigate this effect by using solid-state disks for persistent storage, or for file system cache.

Regarding database size on disk, if you have sustained write traffic then the database grows to about twice its initial size on disk. This is normal, a result of how the database manages its logs. The size on disk does not impact the DB cache size requirements.

In order to avoid directory database file corruption after crashes or power failures on Linux systems, enable file system write barriers and make sure that the file system journaling mode is ordered. For details on how to enable write barriers and how to set the journaling mode for data, see the options for your file system in the **mount** command manual page.

18.2 Testing Performance

Even if you do not need high availability, you still need two of everything, because your test environment needs to mimic your production environment as closely as possible if you want to avoid unwelcome surprises.

In your test environment, you set up OpenDJ as you will later in production, and then conduct experiments to determine how best to meet the requirements defined in the SLA.

Use the **make-ldif** command, described in `make-ldif(1)` in the *OpenDJ Reference*, to generate sample data that match what you expect to find in production.

The OpenDJ LDAP Toolkit provides command-line tools to help with basic performance testing:

- The **addrate** command measures add and delete throughput and response time.
- The **authrate** command measures bind throughput and response time.
- The **modrate** command measures modification throughput and response time.
- The **searchrate** command measures search throughput and response time.

All these commands show you information about the response time distributions, and allow you to perform tests at specific levels of throughput.

If you need additional precision when evaluating response times, use the global configuration setting `etime-resolution`, to change elapsed processing time resolution from milliseconds (default) to nanoseconds:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set etime-resolution:nanoseconds \
  --no-prompt
```

18.3 Tweaking OpenDJ Performance

When your tests show that OpenDJ performance is lacking even though you have the right underlying network, hardware, storage, and system resources in place, you can tweak OpenDJ performance in a number of ways. This section covers the most common tweaks.

18.3.1 Maximum Open Files

OpenDJ needs to be able to open many file descriptors, especially when handling thousands of client connections. Linux systems in particular often set a limit of 1024 per user, which is too low to handle many client connections to OpenDJ.

When setting up OpenDJ for production use, make sure OpenDJ can use at least 64K (65536) file descriptors. For example, when running OpenDJ as user `opendj` on a Linux system that uses `/etc/security/limits.conf` to set user level limits, you can set soft and hard limits by adding these lines to the file:

```
opendj soft nfile 65536
opendj hard nfile 131072
```

The example above assumes the system has enough file descriptors available overall. You can check the Linux system overall maximum as follows:

```
$ cat /proc/sys/fs/file-max
204252
```

18.3.2 Java Settings

Default Java settings let you evaluate OpenDJ using limited system resources. If you need high performance for production system, test with the following JVM options. These apply to the Sun/Oracle JVM.



Tip

To apply JVM settings for your server, edit `config/java.properties`, and apply the changes with the **dsjavaproperties** command, described in `dsjavaproperties(1)` in the *OpenDJ Reference*:

-server

Use the C2 compiler and optimizer (HotSpot Server VM).

-d64

Use this option on 64-bit systems for heaps larger than 3.5 GB.

-Xms, -Xmx

Set both minimum and maximum heap size to the same value to avoid resizing. Leave space for the entire DB cache and more.

Use at least a 2 GB heap (`-Xms2G -Xmx2G`) unless your data set is small.

-Xmn

Set the new generation size between 1-4 GB for high-throughput deployments, but leave enough overall JVM heap to avoid overlaps with the space used for DB cache.

-XX:MaxTenuringThreshold=1

Force OpenDJ directory server to only create objects that have either a short lifetime, or a long lifetime.

-XX:NewSize

If OpenDJ directory server handles high throughput, set the new generation size large enough for the JVM to avoid promoting short-lived objects into the old generation space (`-XX:NewSize=512M`).

-XX:+UseConcMarkSweepGC

The CMS garbage collector tends to give the best performance characteristics with the lowest garbage collection pause times.

Consider using the G1 garbage collector only if CMS performance characteristics do not fit your deployment, and testing shows G1 performs better.

-XX:+UseCompressedOops

Set this option when you have a 64-bit JVM, and `-Xmx` less than 32 GB. Java object pointers normally have the same size as native machine pointers. If you run a small 64-bit JVM, then compressed object pointers can save space.

-XX:+PrintGCDetails

-XX:+PrintGCTimeStamps

Use these options when diagnosing JVM tuning problems. You can turn them off when everything is running smoothly.

18.3.3 Data Storage Settings

By default, OpenDJ compresses attribute descriptions and object class sets to reduce data size. This is called compact encoding.

By default, OpenDJ does not, however, compress entries stored in its backend database. If your entries hold values that compress well—such as text, and not JPEG photos or MP3 audio — you can gain space by setting the backend property `entries-compressed`, to `true` before you (re-)import data from LDIF. With `entries-compressed: true` OpenDJ compresses entries before writing them to the database:¹

¹ OpenDJ does not proactively rewrite all entries in the database after you change the settings. Instead, to force OpenDJ to compress all entries, import the data from LDIF.

```
$ dsconfig \
  set-backend-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --backend-name userRoot \
  --set entries-compressed:true \
  --trustAll \
  --no-prompt

$ import-ldif \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --ldifFile /path/to/Example.ldif \
  --backendID userRoot \
  --includeBranch dc=example,dc=com \
  --start 0
Import task 20120917100628767 scheduled to start Sep 17, 2012 10:06:28 AM CEST
```

18.3.4 LDIF Import Settings

You can tweak OpenDJ to speed up import of large LDIF files.

By default, the temporary directory used for scratch files is `import-tmp` under the directory where you installed OpenDJ. Use the **import-ldif** command, described in `import-ldif(1)` in the *OpenDJ Reference*, with the `--tmpdirectory` option to set this directory to a `tmpfs` file system, such as `/tmp`.

In some cases, you can improve performance by using the `--threadCount` option with the **import-ldif** command to set the thread count larger than the default, which is twice the number of CPUs.

If you are certain your LDIF contains only valid entries with correct syntax, because the LDIF was exported from OpenDJ with all checks active, for example, you can skip schema and DN validation. Use the `--skipSchemaValidation` and `--skipDNValidation` options with the **import-ldif** command to skip validation.

18.3.5 Database Cache Settings

Database cache size is, by default, set as a percentage of the JVM heap by using the backend property `db-cache-percent`. Alternatively, you use the backend property `db-cache-size`, to set the size. If you set up multiple database backends, the total percent of JVM heap used must remain less than 100, and must leave space for other uses. Default settings work for servers with one user data backend JVM heaps up to 2 GB. For heaps larger than 2 GB, you can allocate a larger percentage of heap space to DB cache.

Depending on the size of your database, you have a choice to make about database cache settings.

By caching the entire database in the JVM heap, you can get more deterministic response times and limit disk I/O. Yet, caching the whole DB can require a very large JVM, which you must pre-load on startup, and which can result in long garbage collections and a difficult-to-manage JVM. Test database pre-load on startup by setting the `preload-time-limit` for the backend:

```
$ dsconfig \
  set-backend-prop \
    --port 4444 \
    --hostname opendj.example.com \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --backend-name userRoot \
    --set preload-time-limit:30m \
    --trustAll \
    --no-prompt
```

Database pre-load is single-threaded, and loads each database one at a time.

By allowing file system cache to hold the portion of database that does not fit in the DB cache, you trade less deterministic and slightly slower response times for not preloading the DB and not pausing for long garbage collections with large JVMs. How you configure the file system cache depends on your operating system.

18.3.6 Caching Large, Frequently Used Entries

OpenDJ implements an entry cache designed for deployments with a few large entries that are regularly updated or accessed. The common use case is a deployment with a few large static groups that are updated or accessed regularly. An entry cache is used to keep such groups in memory in a format that avoids the need to constantly read and deserialize the large entries.

When configuring an entry cache, take care to include only the entries that need to be cached by using the configuration properties `include-filter` and `exclude-filter`. The memory devoted to the entry cache is not available for other purposes.

The following example adds a Soft Reference entry cache to hold entries that match the filter (`ou=Large Static Groups`). A Soft Reference entry cache allows cached entries to be released if the JVM is running low on memory. A Soft Reference entry cache has no maximum size setting, so the number of entries cached is limited only by the `include-filter` and `exclude-filter` settings:

```
$ dsconfig \
create-entry-cache \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--cache-name "Large Group Entry Cache" \
--type soft-reference \
--set cache-level:1 \
--set include-filter:"(ou=Large Static Groups)" \
--set enabled:true \
--trustAll \
--no-prompt
```

The entry cache configuration takes effect when the entry cache is enabled.

18.3.7 Logging Settings

Debug logs trace the internal workings of OpenDJ, and therefore generally should be used sparingly, especially in high performance deployments.

In general leave other logs active for production environments to help troubleshoot any issues that arise.

For OpenDJ servers handling very high throughput, however, such as 100,000 operations per second or more, the access log constitute a performance bottleneck, as each client request results in multiple access log messages. Consider disabling the access log in such cases:

```
$ dsconfig \
set-log-publisher-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--publisher-name "File-Based Access Logger" \
--set enabled:false \
--trustAll \
--no-prompt
```

Chapter 19

Securing and Hardening OpenDJ Directory Server

By default OpenDJ directory server is set up for ease of evaluation and deployment. When you deploy OpenDJ in production, there are specific precautions you should take to minimize risks. This chapter recommends the key precautions to take. In this chapter you will learn to:

- Set up a special system account for OpenDJ directory server, and appropriately protect access to directory server files
- Enforce use of the latest Java security updates
- Enable only directory services that are actually used
- Use appropriate log configuration, global access control, password storage, and password policy settings
- Avoid overuse of the default directory root user account
- Use appropriate global access control settings
- Secure connections to the directory

After following the recommendations in this chapter, make sure that you test your installation to verify that it behaves as expected before putting the server into production.

19.1 Set Up a System Account for OpenDJ Directory Server

Do not run OpenDJ directory server as the system superuser (root). When applications run as superuser, the system effectively does not control their actions. When running the server as superuser, a bug in the server could affect other applications or the system itself.

After setting up a system account for the server, and using that account only to run OpenDJ directory server, you can use system controls to limit user access.

The user running OpenDJ directory server must have access to use the configured ports. Make sure you configure the system to let the user access privileged ports such as 389 and 636 if necessary. Make sure you configure the firewall to permit access to the server ports.

The user running OpenDJ directory server must have access to all server files, including configuration files, data files, log files, keystores, truststores and their password files, and other files. By default OpenDJ lets users in the same group as the user running the server read server files, though not directory data files.

The user running OpenDJ directory server does not, however, need access to login from a remote system or to perform actions unrelated to OpenDJ.

Set up the user account to prevent other users from reading configuration files. On UNIX, set an appropriate umask such as 027 to prevent users in other groups from accessing server files. On Windows, use file access control to do the same. Do consider letting all users to run command-line tools. What a user can do with tools depends on server access control mechanisms.

On UNIX and Linux, the group for the user running OpenDJ directory server has access by default to read files, including log files. You can restrict this after installation by setting the `log-file-permissions` property on each active log publisher.

You can create a UNIX service script to start the server at system startup and stop the server at system shutdown by using the **create-rc-script** command. For details see `create-rc-script(1)` in the *OpenDJ Reference*.

You can use the **windows-service** command to register OpenDJ directory server as a Windows service. For details see `windows-service(1)` in the *OpenDJ Reference*.

19.2 Install and Use Java Security Updates

Security updates are occasionally released for the Java runtime environment.

Make sure that your operational plans provide for deploying Java security updates to systems where you run OpenDJ software.

After you update the Java runtime environment, edit the `default.java-home` setting in the file `/path/to/openssl/config/java.properties` to use the path to the update release, and then use the **dsjavaproperties** command for the changes to be taken into account. Then restart OpenDJ directory server. For details see `dsjavaproperties(1)` in the *OpenDJ Reference*.

19.3 Only Enable Necessary Services

By default, OpenDJ directory server enables an LDAP connection handler and an administration connector. If the LDAP connection handler is not used, either because only LDAPS is used or because applications access directory data only over HTTPS, then set the LDAP connection handler property to `enabled:false` by using the **dsconfig set-connection-handler-prop** command.

Likewise, if you have enabled other connection handlers that are not used, you can also disable them by using the **dsconfig** command. Use the **status** command to check which connection handlers are enabled.

19.4 Configure Logging Appropriately

By default, OpenDJ directory server writes log messages to files when an error is encountered and when the server is accessed. Access logs tend to be much more intensively updated than error logs. You can also configure debug logging, generally too verbose for continuous use in production, and audit logging, which uses the access log mechanism to record changes. Debug and audit logs are not enabled by default. For details see [Section 17.5, "Server Logs"](#).

The default OpenDJ directory server error log levels and log rotation and retention policies are set to prevent the logs from harming performance or filling up the disk while still making it possible to perform basic troubleshooting. If you must set a more verbose error log level or if you must activate debug logging on a production system for more advanced troubleshooting, be aware that extra logging can negatively impact performance and generate large files on heavily used servers. When finished troubleshooting, reset the log configuration for more conservative logging.

The audit log in OpenDJ directory server is not for security audits. Instead it records changes in LDIF. The audit log is intended to help you as server administrator diagnose problems in the way applications change directory data. For change notification as a service use the external change log instead. For details about the external change log see [Section 8.4, "Change Notification For Your Applications"](#).

19.5 Limit Use of the cn=Directory Manager Account

Directory root DN accounts are stored in the server configuration under `cn=Root DNs,cn=config`. In order to bootstrap the system, the default root DN administrator, `cn=Directory Manager`, is not subject to access control and has privileges to perform almost every administrative operation, including changing privileges.

Use this account like you use the superuser (root) account on UNIX or the Administrator account on Windows: Use it only when you must.

Instead of allowing other applications to perform operations as the root DN administrator `cn=Directory Manager`, either create alternative root DN administrators with limited privileges, or explicitly assign directory administrator rights to specific accounts.

When creating alternative root DN administrators, you can limit their inherited privileges to prevent them from inheriting `bypass-acl` and `privilege-change` privileges. For an example of how to do this see [Procedure 6.3, "To Add Privileges For a Group of Administrators"](#).

To explicitly assign rights to specific accounts, create a directory administrator group and add administrators as members. Use the group to assign privileges to the administrators. For details see [Procedure 6.3, "To Add Privileges For a Group of Administrators"](#). Create multiple administrator groups if necessary for your deployment.

In both cases, explicitly set up access control instructions (ACIs) to allow administrators to perform administrative actions. For details see [Chapter 6, "Configuring Privileges and Access Control"](#). This prevents administrators from accidentally or intentionally overstepping their authority when managing directory servers and directory data, and you make it easier to audit what administrators can do.

19.6 Reconsider Default Global ACIs

Global ACIs are defined in the directory server configuration. Global ACIs apply whenever no other ACIs take precedence. Global ACIs allow applications to read the root DSE, to read directory server schema, to read directory data anonymously, to modify one's own entry, and to request extended operations and operations with certain controls. For details see [Table 6.1, "Default Global ACIs"](#).

If the default global ACIs do not match your requirements, make sure you change them on each server as the server configuration data is not replicated. Global ACIs have the same syntax as ACIs in the directory data. For details about ACIs see [Chapter 6, "Configuring Privileges and Access Control"](#).

Generally it is fine to allow applications at least to read the root DSE and schema operational attributes, to request the StartTLS extended operation over a cleartext connection, even if read access to most directory data requires authorization. The operational attributes on the root DSE indicate the server capabilities, allowing applications to discover interactively how to use the server. The schema operational attributes describe the data stored in the directory. The StartTLS extended operation lets an application initiate a secure session starting on a port that does not require encryption.

19.7 Protect Directory Server Network Connections

Directory server protocols like LDAP, HTTP, JMX, and replication rely on transport layer security to protect network connections. For evaluation and initial testing you might find it useful to be able to inspect the network traffic without decrypting messages. For final testing and production environments, secure the connections.

Transport layer security depends on public key infrastructure when negotiating encryption. OpenDJ directory server has multiple keystores and truststores for handling the key pairs and public key certificates as described in [Chapter 20](#), "*Changing Server Certificates*".

OpenDJ directory server can simplify installation by self-signing certificates for server key pairs. Self-signed certificates are not recognized by applications until you add them to the application's truststore. This is not a problem when you control both the service and the applications. Self-signed certificates are generally fine even in production systems for administrative and replication connections not used by other applications. For connection handlers that primarily serve applications you do not control, have the server public key certificate signed by a well-known CA so that the applications can recognize the certificate by default. For details on setting up connection handlers for secure communications, see [Chapter 5](#), "*Configuring Connection Handlers*".

You can use an ACI to require secure communications for most operations. Keep a global ACI that allows anonymous access to request the StartTLS extended operation. For all operations other than requesting StartTLS, use ACIs whose subject sets `authmethod = ssl`, and also sets `ssf` appropriately.

A security strength factor (`ssf`) is set when the server negotiates connection security with a client application. The `ssf` setting in an ACI subject indicates acceptable security strength factors for the target operation. The server can then check whether the security strength factor for the connection is acceptable according to ACIs that apply. The `ssf` setting in an ACI takes an integer between 0 and 1024. `ssf = 0` (or not set) means cleartext is acceptable. `ssf = 1` calls for integrity protection, meaning the connection should prevent messages from being corrupted between the sender and the receiver. `ssf >= integer`

where *integer* is two or more calls for integrity and confidentiality protection. Confidential messages are encrypted. Integers larger than one reflect the effective key size of the cipher negotiated between OpenDJ directory server and the LDAP client application. With the `ssf` setting, the aim is to achieve a balance. If not set, or set too low, the server and client can negotiate a connection that is not secure. If set too high, the server and some clients might not be able to negotiate connection settings at all.

When OpenDJ directory server and a client application negotiate connection security, they must agree on a security protocol and cipher suite. By default OpenDJ directory server supports all the SSL and TLS protocols and the cipher suites supported by the underlying Java virtual machine. The list can include protocols and ciphers that are not secure enough for the production environment. You can limit the security protocols and ciphers to those that are secure enough. For an example of how to change the settings for a connection handler, see [Section 5.6, "TLS Protocols and Cipher Suites"](#). You can also change the settings on the administration connector with the **`dsconfig set-administration-connector-prop`** command, and change the settings for replication by changing the crypto manager settings with the **`dsconfig set-crypto-manager-prop`** command.

19.8 Use Appropriate Password Storage and Password Policies

Make sure you keep passwords secret in production. OpenDJ directory server configuration includes files that hold passwords. Command-line tools allow users to provide password credentials. Passwords are also stored in directory data. This section looks at how to protect passwords in each situation.

19.8.1 Passwords in Configuration Files

OpenDJ directory server stores passwords in configuration files.

The `config.ldif` file stores hashes of the passwords for root DN users, such as `cn=Directory Manager`. Likewise for replicated servers the `admin-backend.ldif` file stores a password hash for the global administrator, such as `cn=admin`, `cn=Administrators`, `cn=admin` data. By default the password storage algorithm is Salted SHA512, a salted form of the 512-bit SHA-2 message digest algorithm. Permissions on the current copy of the file make it readable and writable only by the user running the server. A backup copy of the version used for the latest successful server startup, `config.ldif.startok`, can be readable to other users depending on the UNIX `umask` or Windows access control. Use a storage scheme that protects the passwords in server configuration files.

By default OpenDJ directory server stores passwords for keystores and truststores in configuration files with `.pin` extensions. These files contain the

cleartext, randomly generated passwords. Keep the PIN files readable and writable only by the user running the server. Alternatively, you can use the **dsconfig** command to configure the server to store keystore and truststore passwords in environment variables or Java properties if your procedures make these methods more secure in production. The settings to change are those of the Key Manager Providers and Trust Manager Providers.

19.8.2 Passwords as Command-Line Arguments

OpenDJ commands supply credentials for any operations that are not anonymous. Password credentials can be supplied as arguments such as the `--bindPassword password` option shown in many of the examples in the documentation. The passwords for keystores and truststores are handled in the same way. This is not recommended in production as the password appears in the command. Passwords can also be supplied interactively by using a `-` in the commands, as in `--bindPassword -`. The following example demonstrates a password supplied interactively:

```
$ ldapsearch \
--bindDN "cn=Directory Manager" \
--bindPassword - \
--port 1389 \
--hostname opendj.example.com \
--baseDN cn=config \
"(cn=Directory Manager)" \
userPassword
Password for user 'cn=Directory Manager':
dn: cn=Directory Manager,cn=Root DNs,cn=config
userPassword: {SSHA512}WiYWHyAa612EZwCMY7uGwN/WYp2Ne7EmV0QTPX5g6RrTKi8jZX3u5rBIW
OUY1DPK3TGYqDiF7d/BEhHnIjBmBtkotWkHIKMa
```

Notice that the password appears neither in the shell history, nor in the terminal session.

When using scripts where the password cannot be supplied interactively, passwords can be read from files. For example, the `--bindPasswordFile file` option takes a file that should be readable only by the user running the command. It is also possible to set passwords in the `tools.properties` file for the user. This file is located in the user's home directory, on UNIX `~/.opendj/tools.properties`, and on Windows typically `C:\Documents and Settings\username\.opendj\tools.properties`, though the location can depend on the Java runtime environment used. Here as well, make sure that the file is readable only by the user. Alternatively, use other approaches that work with scripts such as Java properties or environment variables, depending on what method is most secure in production.

19.8.3 Passwords in Directory Data

OpenDJ directory server encodes users' passwords before storing them. A variety of built-in password storage schemes are available, using either one-way (hash) or reversible algorithms. The default storage schemes use one-way algorithms to make it computationally difficult to recover the cleartext password values even when given full access to the files containing stored password values.

For details see [Section 10.5, "Configuring Password Storage"](#).

In OpenDJ directory server, password policies govern password storage schemes, valid password values, password term duration, account lockout, and others. For example, you can configure password policies that prevent users from setting weak passwords and from reusing passwords. OpenDJ provides a wide range of alternatives. For details see [Chapter 10, "Configuring Password Policy"](#).

19.9 Protect OpenDJ Directory Server Files

OpenDJ directory server does not encrypt directory server files. Other than passwords, OpenDJ directory server does not encrypt attribute values.

If you set up an appropriate user account for the server as described in [Section 19.1, "Set Up a System Account for OpenDJ Directory Server"](#), and unpacked the server files as that user, then the system should prevent other users from having overly permissive access to directory server files.

Included in the files that directory server does not encrypt are LDIF exports of directory data. LDIF export files are readable and writable depending on the UNIX umask or Windows file access control settings for the user who runs the command to export the LDIF. The **export-ldif** command can compress the LDIF, but does not have an option for encrypting LDIF.

Directory backup archives can be encrypted, but are not encrypted by default. Backup archive file permissions depend on the UNIX umask or Windows file access control settings. When using the **backup** command, run an online backup and supply the **--encrypt** option as shown in the following example:

```
$ backup \
--port 4444 \
--bindDN "cn=Directory Manager" \
--bindPassword - \
--backupAll \
--backupDirectory /path/to/openssl/bak \
--encrypt \
--start 0
Password for user 'cn=Directory Manager':
Backup task 20150810105606755 scheduled to start ...
```

The server uses its Crypto Manager configuration to determine how to encrypt the backup archive data. The `--encrypt` option is not available for offline back up. If you back up server data offline, plan to protect the files separately.

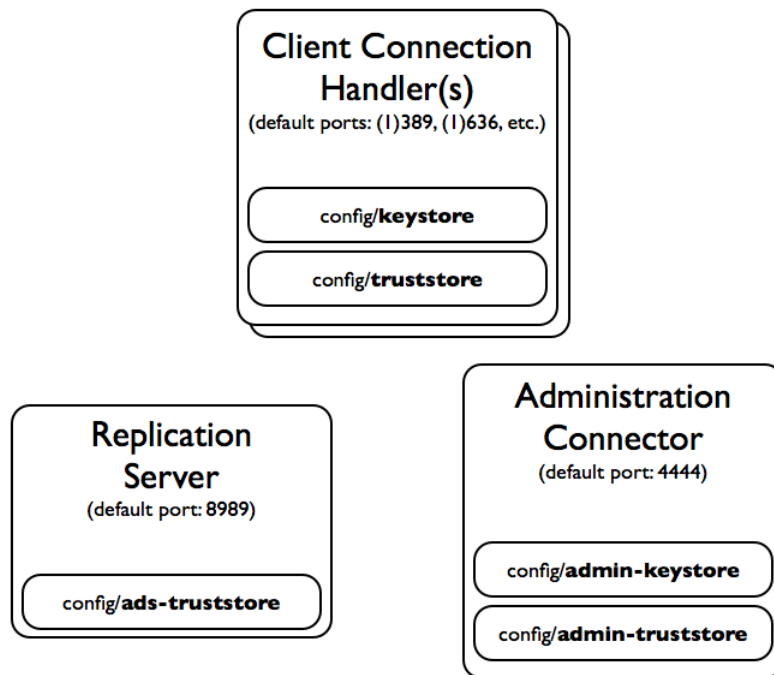
Chapter 20

Changing Server Certificates

This chapter covers how to replace OpenDJ key pairs and public key certificates. In this chapter you will learn to:

- Replace a key pair for securing a connection handler
- Replace a key pair used for replication

OpenDJ uses keystores (for private keys) and truststores (for public, signed certificates). Up to three sets of keystores are used, as shown in the following illustration.



OpenDJ uses different sets of public and private keys for different secure connections.

By default the keystores are located in the `/path/to/openssl/config` directory:

- The keystore and truststore hold keys for securing connections with client applications.
- The admin-keystore and admin-truststore hold keys for securing administrative connections, such as those used when connecting with the **dsconfig** command.
- The ads-truststore holds keys for securing replication connections with other OpenDJ servers in the replication topology.

Each keystore has a specific purpose:

admin-keystore

This Java Keystore holds the private key and administrative certificate for the server, admin-cert. This key pair is used to protect communications on the administration port. The password, stored in admin-keystore.pin, is also the key password for admin-cert.

admin-truststore

This Java Keystore holds a copy of the administrative certificate, `admin-cert`. The password is the same as for the `admin-keystore`, in other words the string in `admin-keystore.pin`.

ads-truststore

This Java Keystore holds public key certificates of all servers replicating with the current server. It also includes the `ads-certificate` key pair of the current server. The password is stored in `ads-truststore.pin`.

Do not change this keystore directly.

keystore

This Java Keystore holds the private key and server certificate, `server-cert`, used to protect TLS/SSL communications with client applications. The password, stored in `keystore.pin`, is also the key password for `server-cert`.

truststore

This Java Keystore holds a copy of the `server-cert` certificate from the keystore. This is also where you import certificates of client applications if you want OpenDJ to recognize them. The password is the same as for the keystore, in other words the string in `keystore.pin`.



Tip

Examples in this chapter use self-signed certificates, but you can also use certificates signed by a Certificate Authority (CA).

When importing a certificate (**keytool -import**) signed by a well-known CA, use the `-trustcacerts` option to trust the CA certificates delivered with the Java runtime environment.

Procedure 20.1. To Replace a Server Key Pair

This procedure shows how to replace a server key pair in the `admin-keystore` and copy of the administrative certificate in `admin-truststore`.

The examples also apply when replacing a key pair in the keystore and copy of the server certificate in truststore. Just adapt the commands to use the correct keystore, truststore, and PIN file names.

This procedure does not apply for replication key pairs. Instead, see [Procedure 20.2, "To Replace the Key Pair Used for Replication"](#).

1. Check the alias of the key pair and certificate copy to replace:

```
$ cd /path/to/openssl/config
$ keytool -list -keystore admin-keystore -storepass `cat admin-keystore.pin`

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

admin-cert, May 20, 2015, PrivateKeyEntry,
Certificate fingerprint (SHA1): 21:9F:F0:E8:A3:22:A3:62:1D:C7:04:BD:12:44:A6:FA:0C:3F:3A:35
$ keytool -list -keystore admin-truststore -storepass `cat admin-keystore.pin`

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

admin-cert, May 20, 2015, trustedCertEntry,
Certificate fingerprint (SHA1): 21:9F:F0:E8:A3:22:A3:62:1D:C7:04:BD:12:44:A6:FA:0C:3F:3A:35
```

This alias is also stored in the server configuration.

2. Remove the key pair and certificate copy to replace:

```
$ keytool \
-delete \
-alias admin-cert \
-keystore admin-keystore \
-storepass `cat admin-keystore.pin`

$ keytool \
-delete \
-alias admin-cert \
-keystore admin-truststore \
-storepass `cat admin-keystore.pin`
```

3. Generate a new key pair in the keystore:

```
$ keytool \
-genkey \
-alias admin-cert \
-keyalg RSA \
-validity 7300 \
-keysize 2048 \
-ext "san=dns:opendj.example.com" \
-dname "CN=opendj.example.com, O=Administration Connector Self-Signed Certificate" \
-keystore admin-keystore \
-storepass `cat admin-keystore.pin` \
-keypass `cat admin-keystore.pin`
```

Notice that the `-alias` option takes the same alias as before. This is because the `ssl-cert-nickname` for the Administration Connector is configured as `admin-cert`. Also, the `-dname` option has a CN value corresponding to the fully qualified domain name of the host where OpenDJ directory server is running.

4. Get the new key pair's certificate signed, using one of the following alternatives:

- Self-sign the certificate:

```
$ keytool \  
-selfcert \  
-alias admin-cert \  
-validity 7300 \  
-keystore admin-keystore \  
-storepass `cat admin-keystore.pin`
```

- Create a certificate signing request, have it signed by a CA, and import the signed certificate from the CA reply.

For examples of the **keytool** commands to use, see [Procedure 5.2, "To Request and Install a CA-Signed Certificate"](#).

5. Export a copy of the certificate from the keystore:

```
$ keytool \  
-export \  
-alias admin-cert \  
-keystore admin-keystore \  
-storepass `cat admin-keystore.pin` \  
-file admin-cert.crt  
Certificate stored in file <admin-cert.crt>
```

6. Import the copy of the certificate into the truststore:

```

$ keytool \
  -import \
  -alias admin-cert \
  -keystore admin-truststore \
  -storepass `cat admin-keystore.pin` \
  -file admin-cert.crt
Owner: CN=opendj.example.com, O=Administration Connector Self-Signed Certificate
Issuer: CN=opendj.example.com, O=Administration Connector Self-Signed Certificate
Serial number: 4cdd42a
Valid from: Thu May 28 11:32:05 CEST 2015 until: Wed May 23 11:32:05 CEST 2035
Certificate fingerprints:
  MD5:  40:38:24:5D:DD:BE:EC:D6:07:56:08:25:95:D9:61:FE
  SHA1: BC:3D:A9:26:CD:4E:71:04:44:16:1E:A5:79:DA:43:2A:65:E8:85:85
  SHA256: D3:41:EE:44:5A:54:74:11:5A:...9F:8F:08:13:09:DD:71:52:7E:35:66:7E
  Signature algorithm name: SHA256withRSA
  Version: 3

Extensions:

#1: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: opendj.example.com
]

#2: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 08 E3 D3 62 AA 68 E6 02   52 25 F8 22 C4 43 82 2D   ...b.h..R%.".C.-
0010: 20 C1 39 99                .9.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore

```

7. Restart OpenDJ to make sure it reloads the keystores:

```

$ cd /path/to/opendj/bin
$ stop-ds --restart

```

8. If you have client applications trusting the self-signed certificate, have them import the new one (admin-cert.crt in this example).

Procedure 20.2. To Replace the Key Pair Used for Replication

Follow these steps to replace the key pair that is used to secure replication connections.

1. Generate a new key pair for the server.

The changes you perform are replicated across the topology.

OpenDJ has an ads-certificate and private key, which is a local copy of the key pair used to secure replication connections.

To generate the new key pair, you remove the ads-certificate key pair, prompt OpenDJ to generate a new ads-certificate key pair, and then add a copy to the administrative data using the MD5 fingerprint of the certificate to define the RDN.

- a. Delete the ads-certificate entry:

```
$ ldapmodify \  
--port 1389 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password  
dn: ds-cfg-key-id=ads-certificate,cn=ads-truststore  
changetype: delete  
  
Processing DELETE request for ds-cfg-key-id=ads-certificate,cn=ads-truststore  
DELETE operation successful for DN ds-cfg-key-id=ads-certificate,  
cn=ads-truststore
```

- b. Prompt OpenDJ to generate a new, self-signed ads-certificate key pair.

You do this by adding an ads-certificate entry with object class ds-cfg-self-signed-cert-request:

```
$ ldapmodify \  
--port 1389 \  
--hostname opendj.example.com \  
--bindDN "cn=Directory Manager" \  
--bindPassword password  
dn: ds-cfg-key-id=ads-certificate,cn=ads-truststore  
changetype: add  
objectclass: ds-cfg-self-signed-cert-request  
  
Processing ADD request for ds-cfg-key-id=ads-certificate,cn=ads-truststore  
ADD operation successful for DN ds-cfg-key-id=ads-certificate,cn=ads-truststore
```

- c. Retrieve the ads-certificate entry:

```
$ ldapsearch \
--port 1389 \
--hostname opendj.example.com \
--baseDN cn=ads-truststore \
"(ds-cfg-key-id=ads-certificate)"
dn: ds-cfg-key-id=ads-certificate,cn=ads-truststore
ds-cfg-key-id: ads-certificate
ds-cfg-public-key-certificate;binary:: MIIB6zCCAUSgAwIBAgIEDKSUFjANBgkqhkiG9w0BA
QUFADA6MRswGQYDVQKExJCpGVuREogQ2VydGlmawNhdGUxGzAZBgNVBAMTEm9wZW5hbS5leGFtcGxl
LmNvbTAeFw0xMzAyMDcxMDMwMzNaFw0zMDIwMDIwMDMwMzNaMDoxGzAZBgNVBAoTEk9wZW5ESlB0ZXJ
0aWZpY2F0ZTEbMBkGA1UEAxMSb3BlbmFtLmV4YW1wbGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNAD
CBiQKBgQCfGLAiU0z4sC8CM9T5DPTk9V9ErNC8N59XwBt1aN7UjhQ14/JZZsetubtUrZBLS9cRrnYdZ
cpFgLQNEmXfS+PdZ0DJkaLNFmd8ZX0spX8++fb4SkkggkmNRmi1fccDQ/DHMLw17kk8841XummrzcD
GbZ7p4vnY7y7GmDlvZSP+wIDAQABMA0GCSqGSIb3DQEBAQUAA4GBAJciUzUP8T8A9VV6dQB0SYCNG1o
7IvpE7jGvZ6KvM0m5sBNX3wPbTVJQNi3TDm8nx6yhi6DUkpiAZfz/OBL5k+Wsw80TjpIZ2+klhPls
srsST4Um4fHzDX0XHR6NM83XxZBsR6MazYecL8CiGwnYW2AeBapzbAnGn1J831q1q
objectClass: top
objectClass: ds-cfg-instance-key
```

- d. Retrieve the MD5 fingerprint of the ads-certificate.

In this example, the MD5 fingerprint is
07:35:80:D8:F3:CE:E1:39:9C:D0:73:DB:6C:FA:CC:1C:

```
$ keytool \
-list \
-v \
-alias ads-certificate \
-keystore /path/to/opendj/config/ads-truststore \
-storepass `cat /path/to/opendj/config/ads-truststore.pin`
Alias name: ads-certificate
Creation date: Feb 7, 2013
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=opendj.example.com, O=OpenDJ Certificate
Issuer: CN=opendj.example.com, O=OpenDJ Certificate
Serial number: ca49416
Valid from: Thu Feb 07 11:30:33 CET 2013 until: Wed Feb 02 11:30:33 CET 2033
Certificate fingerprints:
  MD5:  07:35:80:D8:F3:CE:E1:39:9C:D0:73:DB:6C:FA:CC:1C
  SHA1: 56:30:F6:79:AA:C0:BD:61:88:3E:FB:38:38:9D:84:70:0B:E4:43:57
  SHA256: A8:4B:81:EE:30:2A:0C:09:2E:...:C1:41:F5:AB:19:C6:EE:AB:50:64
Signature algorithm name: SHA1withRSA
Version: 3
```

- e. Using the MD5 fingerprint and the certificate entry, prepare LDIF to update cn=admin data with the new server certificate:

```
$ cat /path/to/update-server-cert.ldif
dn: ds-cfg-key-id=073580D8F3CEE1399CD073DB6CFACC1C,cn=instance keys,
cn=admin data
changetype: add
ds-cfg-key-id: 073580D8F3CEE1399CD073DB6CFACC1C
ds-cfg-public-key-certificate;binary:: MIIB6zCCAUSgAwIBAgIEDKSUFjANBgkqhkiG9w0BA
QUFADA6MRswGQYDVQKEXJPcGVuREogQ2VydG1maWNhdGUxGzAZBgNVBAMTEm9wZW5hbS5leGFtcGxl
LmNvbTAeFw0xMzAyMDcxMDMwMzNaFw0zMzAyMDIxMDMwMzNaMDoxGzAZBgNVBAoTEK9wZW5ESiBDZXJ
0aWZpY2F0ZTEbMBkGA1UEAxMSb3BlbmFtLmV4YW1wbGUuY29tMIGfMA0GCSqGSIb3DQEBQUAA4GNAD
CBiQKBgQCfGLAiU0z4sC8CM9T5DPTk9V9ErNC8N59XwBt1aN7UjhQ14/JZZsetubtUrZBL59cRrnYdZ
cpFgLQNEmXifS+PdZ0DJkaLNFmd8ZX0spX8++fb45kkggkmNRmilfccDQ/DHMLwL7kk8841XummrzcD
GbZ7p4vnY7y7GmD1vZSP+wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJciUzUP8T8A9VV6dQ80SYCNG1o
7IvpE7jGVZh6KvM0m5sBNX3wPbTVJQNiJ3TDm8nx6yhi6DUkpiAZfz/0BL5k+WSw80TjpIZ2+klhPls
srsST4Um4fHzDX0XHR6NM83XxZBsR6MazYecL8CiGwnYW2AeBapzbAnGn1J831q1q
objectClass: top
objectClass: ds-cfg-instance-key

dn: cn=opendj.example.com:4444,cn=Servers,cn=admin data
changetype: modify
replace: ds-cfg-key-id
ds-cfg-key-id: 073580D8F3CEE1399CD073DB6CFACC1C
```

- f. Update the administrative data, causing OpenDJ to create a copy of the new ads-certificate with its MD5 signature as the alias in the ads-truststore:

```
$ ldapmodify \
--port 1389 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--filename /path/to/update-server-cert.ldif
Processing ADD request for ds-cfg-key-id=073580D8F3CEE1399CD073DB6CFACC1C,
cn=instance keys,cn=admin data
ADD operation successful for DN ds-cfg-key-id=073580D8F3CEE1399CD073DB6CFACC1C,
cn=instance keys,cn=admin data
Processing MODIFY request for cn=opendj.example.com:4444,cn=Servers,
cn=admin data
MODIFY operation successful for DN cn=opendj.example.com:4444,cn=Servers,
cn=admin data
```

2. Force OpenDJ to reopen replication connections using the new key pair.

Stop replication temporarily and then start it again as described in [Section 8.3, "Configuring Replication"](#):

```
$ dsconfig \
set-synchronization-provider-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--set enabled:false \
--no-prompt

$ dsconfig \
set-synchronization-provider-prop \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--provider-name "Multimaster Synchronization" \
--set enabled:true \
--no-prompt
```

Chapter 21

Moving Servers

This chapter explains how to move OpenDJ directory servers. In this chapter you will learn to:

- Prepare for the move, especially when the server is replicated, and when the directory service remains available during the move
- Perform the configuration needed to move the directory server

When you change where OpenDJ is deployed, you must take host names, port numbers, and certificates into account. The changes can also affect your replication configuration.

21.1 Overview

From time to time you might change server hardware, file system layout, or host names. At those times you move the services running on the system. You can move OpenDJ data between servers and operating systems. Most of the configuration is also portable.

Two aspects of the configuration are not portable:

1. Server certificates contain the host name of the system. Even if you did not set up secure communications when you installed the server, the server still has a certificate used for secure communications on the administrative port.

To resolve the issue with server certificates, you can change the server certificates during the move as described in this chapter.

2. Replication configuration includes the host name and administrative port numbers.

You can work around the issue with replication configuration by disabling replication for the server before the move, and then enabling and initializing replication again after the move.

21.2 Before You Move

Take a moment to determine whether you find it quicker and easier to move your server, or to recreate a copy. To recreate a copy, install a new server, set up the new server configuration to match the old, and then copy only the data from the old server to the new server, initializing replication from existing data, or even from LDIF if your database is not too large.

After you decide to move a server, start by taking it out of service. Taking it out of service means directing client applications elsewhere, and then preventing updates from client applications, and finally disabling replication. Directing client applications elsewhere depends on your network configuration and possibly on your client application configuration. The other two steps can be completed with the **dsconfig** and **dsreplication** commands.

Procedure 21.1. To Take the Server Out of Service

1. Direct client applications to other servers.

How you do this depends on your network and client application configurations.

2. Prevent the server from accepting updates from client applications:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj2.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set writability-mode:internal-only \
  --trustAll \
  --no-prompt
```

3. Disable replication for the server:


```
$ dsreplication \  
disable \  
--disableAll \  
--port 4444 \  
--hostname opendj2.example.com \  
--adminUID admin \  
--adminPassword password \  
--trustAll \  
--no-prompt  
Establishing connections ..... Done.  
Disabling replication on base DN dc=example,dc=com of server  
opendj2.example.com:4444 ..... Done.  
Disabling replication on base DN cn=admin data of server  
opendj2.example.com:4444 ..... Done.  
Disabling replication on base DN cn=schema of server  
opendj2.example.com:4444 ..... Done.  
Disabling replication port 8989 of server opendj2.example.com:4444 ..... Done.  
Removing registration information ..... Done.  
Removing truststore information ..... Done.  
  
See  
/var/.../opens-3173475478874782719.log  
for a detailed log of this operation.
```

4. With the server no longer receiving traffic or accepting updates from clients, and no longer replicating to other servers, you can shut it down in preparation for the move:

```
$ stop-ds  
Stopping Server...  
  
... msg=The Directory Server is now stopped
```

5. You might also choose to remove extra log files from the server logs/ directory before moving the server.

21.3 Moving a Server

Now that you have decided to move your server, and prepared for the move, you must not only move the files but also fix the configuration and the server certificates, and then enable replication.

Procedure 21.2. To Move the Server

1. Move the contents of the server installation directory to the new location.

2. If you must change port numbers, edit the port numbers in `config/config.ldif`, carefully avoiding changing any whitespace or other lines in the file.
3. Change server certificates as described in [Chapter 20, "Changing Server Certificates"](#).
4. Start the server:

```
$ start-ds
... The Directory Server has started successfully
```

5. Enable and initialize replication:

```
$ dsrepllication \  
enable \  
--adminUID admin \  
--bindPassword password \  
--baseDN dc=example,dc=com \  
--host1 opendj.example.com \  
--port1 4444 \  
--bindDN1 "cn=Directory Manager" \  
--bindPassword1 password \  
--replicationPort1 8989 \  
--host2 opendj2.example.com \  
--port2 4444 \  
--bindDN2 "cn=Directory Manager" \  
--bindPassword2 password \  
--replicationPort2 8989 \  
--trustAll \  
--no-prompt
```

Establishing connections Done.
Checking registration information Done.
Configuring Replication port on server opendj.example.com:4444 Done.
Updating remote references on server opendj2.example.com:4444 Done.
Updating replication configuration for baseDN dc=example,dc=com on server
opendj.example.com:4444 Done.
Updating replication configuration for baseDN dc=example,dc=com on server
opendj2.example.com:4444 Done.
Updating registration configuration on server
opendj.example.com:4444 Done.
Updating registration configuration on server
opendj2.example.com:4444 Done.
Updating replication configuration for baseDN cn=schema on server
opendj.example.com:4444 Done.
Updating replication configuration for baseDN cn=schema on server
opendj2.example.com:4444 Done.
Initializing registration information on server opendj.example.com:4444 with
the contents of server opendj2.example.com:4444 Done.
Initializing schema on server opendj2.example.com:4444 with the contents of
server opendj.example.com:4444 Done.

Replication has been successfully enabled. Note that for replication to work
you must initialize the contents of the base DN's that are being replicated
(use dsrepllication initialize to do so).

See /tmp/opensds-replication-1476402020764482023.log for a detailed log of this
operation.

```
$ dsrepllication \  
pre-external-initialization \  
--adminUID admin \  
--bindPassword password \  
--port 4444 \  
--baseDN dc=example,dc=com \  
--trustAll \  
--no-prompt
```

Preparing base DN dc=example,dc=com to be initialized externally Done.

Now you can proceed to the initialization of the contents of the base DN's on
all the replicated servers. You can use the command `import-ldif` or the binary
copy to do so. You must use the same LDIF file or binary copy on each server.

When the initialization is completed you must use the subcommand
'post-external-initialization' for replication to work with the new base DN's
contents.

```
$ dsrepllication \  
post-external-initialization \  
--adminUID admin \  
--bindPassword password \  
--port 4444 \  
--no-prompt
```

6. Accept updates from client applications:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set writability-mode:enabled \
  --trustAll \
  --no-prompt
```

7. Direct client applications to the server.

Chapter 22

Troubleshooting Server Problems

This chapter describes how to troubleshoot common server problems, and how to collect information necessary when seeking support help. In this chapter you will learn to:

- Identify directory server problems systematically as a first troubleshooting step
- Troubleshoot problems with installation and upgrade procedures, directory data import, data replication, and secure connections
- Reset lost administrator passwords
- Enable debug logging judiciously when solving problems
- Prevent applications from accessing the directory server when solving problems
- Troubleshoot problems with the way client applications access the directory
- Prepare evidence when asking a directory expert for help

22.1 Identifying the Problem

In order to solve your problem methodically, save time by defining the problem clearly up front. In a replicated environment with multiple directory servers and many client applications, it can be particularly important to pin down not only the

problem (difference in observed behavior compared to expected behavior), but also the circumstances and steps that lead to the problem occurring.

Answer the following questions:

- How do you reproduce the problem?
- What exactly is the problem? In other words, what is the behavior you expected? What is the behavior you observed?
- When did the problem start occurring? Under similar circumstances, when does the problem not occur?
- Is the problem permanent? Intermittent? Is it getting worse? Getting better? Staying the same?

Pinpointing the problem can sometimes indicate where you should start looking for solutions.

22.2 Troubleshooting Installation and Upgrade

Installation and upgrade procedures result in a log file tracing the operation. The log location differs by operating system, but look for lines in the command output of the following form:

See `/var/....log` for a detailed log of this operation.

Prevent antivirus and intrusion detection systems from interfering with OpenDJ directory server.

Antivirus and intrusion detection systems that do a deep inspection of database files are not compatible with OpenDJ directory server. Disable antivirus and intrusion detection systems, or at least prevent them from operating on OpenDJ directory server files.

22.3 Resetting Administrator Passwords

This section describes what to do if you forgot the password for Directory Manager or for the global (replication) administrator.

Procedure 22.1. Resetting the Directory Manager's Password

OpenDJ directory server stores the entry for Directory Manager in the LDIF representation of its configuration. You must be able to edit directory server files in order to reset Directory Manager's password.

1. Generate the encoded version of the new password using the OpenDJ **encode-password** command:

```
$ encode-password --storageScheme SSHA512 --clearPassword password
Encoded Password: "{SSHA512}yWqHnYV4a5l1PvE7wHLe5jzK27oZQWLI1Vcs9gySu4TyZJMg
NQNRtnR/Xx2xcslwuldVLI9jVVtl1W4BVsm0Kjyjr0rWrHt"
```

2. Stop OpenDJ directory server while you edit the configuration:

```
$ stop-ds
```

3. Find Directory Manager's entry, which has DN `cn=Directory Manager, cn=Root DNs, cn=config`, in `/path/to/openssl/config/config.ldif`, and carefully replace the `userpassword` attribute value with the encoded version of the new password, taking care not to leave any whitespace at the end of the line:

```
dn: cn=Directory Manager,cn=Root DNs,cn=config
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: ds-cfg-root-dn-user
objectClass: top
userpassword: {SSHA512}yWqHnYV4a5l1PvE7wHLe5jzK27oZQWLI1Vcs9gySu4TyZJMg
NQNRtnR/Xx2xcslwuldVLI9jVVtl1W4BVsm0Kjyjr0rWrHt
givenName: Directory
cn: Directory Manager
ds-cfg-alternate-bind-dn: cn=Directory Manager
sn: Manager
ds-pwp-password-policy-dn: cn=Root Password Policy,cn=Password Policies
,cn=config
ds-rlim-time-limit: 0
ds-rlim-lookthrough-limit: 0
ds-rlim-idle-time-limit: 0
ds-rlim-size-limit: 0
```

4. Start OpenDJ directory server again:

```
$ start-ds
```

5. Verify that you can administer the server as Directory Manager using the new password:

```
$ dsconfig -p 4444 -h opendj.example.com -D "cn=Directory Manager" -w password

>>>> OpenDJ configuration console main menu

What do you want to configure?

...

Enter choice: q
```

Procedure 22.2. To Reset the Global Administrator's Password

When you enable replication, part of the process involves creating a global administrator and setting that user's password. This user is present on all replicas. If you chose default values, this user has DN `cn=admin, cn=Administrators, cn=admin data`. You reset the password as you would for any other user, though you do so as Directory Manager.

1. Use the **ldappasswordmodify** command to reset the global administrator's password:

```
$ ldappasswordmodify \
--useStartTLS \
--port 1389 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--authzID "cn=admin,cn=Administrators,cn=admin data" \
--newPassword password
The LDAP password modify operation was successful
```

2. Let replication copy the password change to other replicas.

22.4 Enabling Debug Logging

OpenDJ can write debug information and stack traces to the server debug log. What is logged depends both on debug targets that you create, and on the debug level that you choose.

Procedure 22.3. To Configure Debug Logging

1. Enable the debug log, `opendj/logs/debug`, which is not enabled by default:


```
$ dsconfig \
  set-log-publisher-prop \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based Debug Logger" \
    --set enabled:true \
    --no-prompt \
    --trustAll
```

2. Create a debug target or targets.

No debug targets are enabled by default:

```
$ dsconfig \
  list-debug-targets \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based Debug Logger" \
    --no-prompt \
    --trustAll

Debug Target : enabled : debug-exceptions-only
-----:-----:-----

$
```

A debug target specifies a fully qualified OpenDJ Java package, class, or method for which to log debug messages at the level you specify:

```
$ dsconfig \
  create-debug-target \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based Debug Logger" \
    --type generic \
    --target-name org.opends.server.api \
    --set enabled:true \
    --no-prompt \
    --trustAll
```

3. Restart OpenDJ to see debug messages in the log:

```
$ stop-ds --restart
...
$ dsconfig \
  list-debug-targets \
    --hostname opendj.example.com \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword password \
    --publisher-name "File-Based Debug Logger" \
    --no-prompt \
    --trustAll

Debug Target          : enabled : debug-exceptions-only
-----
org.opends.server.api : true    : false

$ tail -f /path/to/opendj/logs/debug
...
```



Caution

OpenDJ directory server can generate a high volume of debug output. Use debug logging very sparingly on production systems.

22.5 Preventing Access While You Fix Issues

Misconfiguration can potentially put OpenDJ in a state where you must intervene, and where you need to prevent users and applications from accessing the directory until you are done fixing the problem.

OpenDJ provides a *lockdown mode* that allows connections only on the loopback address, and allows only operations requested by root users, such as `cn=Directory Manager`. You can use lockdown mode to prevent all but administrative access to OpenDJ in order to repair the server.

To put OpenDJ into lockdown mode, the server must be running. You cause the server to enter lockdown mode by using a task. Notice that the modify operation is performed over the loopback address (accessing OpenDJ on the local host):

```
$ ldapmodify \  
--port 1389 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--defaultAdd  
dn: ds-task-id=Enter Lockdown Mode,cn=Scheduled Tasks,cn=tasks  
objectClass: top  
objectClass: ds-task  
ds-task-id: Enter Lockdown Mode  
ds-task-class-name: org.opends.server.tasks.EnterLockdownModeTask  
  
Processing ADD request for  
ds-task-id=Enter Lockdown Mode,cn=Scheduled Tasks,cn=tasks  
ADD operation successful for DN  
ds-task-id=Enter Lockdown Mode,cn=Scheduled Tasks,cn=tasks
```

OpenDJ logs a notice message in logs/errors when lockdown mode takes effect:

```
[30/Jan/2012:17:04:32 +0100] category=BACKEND severity=NOTICE msgID=9896350  
msg=Lockdown task Enter Lockdown Mode finished execution
```

Client applications that request operations get a message concerning lockdown mode:

```
$ ldapsearch --port 1389 --baseDN "" --searchScope base "(objectclass=*)" +  
SEARCH operation failed  
Result Code: 53 (Unwilling to Perform)  
Additional Information: Rejecting the requested operation because the server  
is in lockdown mode and will only accept requests from root users over  
loopback connections
```

You also leave lockdown mode by using a task:

```
$ ldapmodify \  
--port 1389 \  
--bindDN "cn=Directory Manager" \  
--bindPassword password \  
--defaultAdd  
dn: ds-task-id=Leave Lockdown Mode,cn=Scheduled Tasks,cn=tasks  
objectClass: top  
objectClass: ds-task  
ds-task-id: Leave Lockdown Mode  
ds-task-class-name: org.opends.server.tasks.LeaveLockdownModeTask  
  
Processing ADD request for  
ds-task-id=Leave Lockdown Mode,cn=Scheduled Tasks,cn=tasks  
ADD operation successful for DN  
ds-task-id=Leave Lockdown Mode,cn=Scheduled Tasks,cn=tasks
```

OpenDJ also logs a notice message when leaving lockdown:

```
[30/Jan/2012:17:13:05 +0100] category=BACKEND severity=NOTICE msgID=9896350
msg=Leave Lockdown task Leave Lockdown Mode finished execution
```

22.6 Troubleshooting LDIF Import

By default OpenDJ requires that LDIF data you import respect standards. In particular, OpenDJ is set to check that entries to import match the schema defined for the server. You can temporarily bypass this check by using the `--skipSchemaValidation` with the **import-ldif** command.

OpenDJ also ensures by default that entries have only one structural object class. You can relax this behavior by using the advanced global configuration property, `single-structural-objectclass-behavior`. This can be useful when importing data exported from Sun Directory Server. For example, to warn when entries have more than one structural object class instead of reject such entries being added, set `single-structural-objectclass-behavior:warn` as follows:

```
$ dsconfig \
  set-global-configuration-prop \
  --port 4444 \
  --hostname opendj.example.com \
  --bindDN "cn=Directory Manager" \
  --bindPassword password \
  --set single-structural-objectclass-behavior:warn \
  --trustAll \
  --no-prompt
```

By default, OpenDJ also checks syntax for a number of attribute types. Relax this behavior by using the **dsconfig set-attribute-syntax-prop** command. Use the `--help` option for further information.

When running **import-ldif**, you can use the `-R rejectFile` option to capture entries that could not be imported, and the `--countRejects` option to return the number of rejected entries as the **import-ldif** exit code.

Once you work through the issues with your LDIF data, reinstate the default behavior to ensure automated checking.

22.7 Troubleshooting TLS/SSL Connections

In order to trust the server certificate, client applications usually compare the signature on certificates with those of the Certificate Authorities (CAs) whose certificates are distributed with the client software. For example, the Java environment is distributed with a keystore holding many CA certificates:

```
$ keytool -list -keystore $JAVA_HOME/lib/security/cacerts -storepass changeit \  
| wc -l  
334
```

The self-signed server certificates that can be configured during OpenDJ setup are not recognized as being signed by any CAs. Your software therefore is configured not to trust the self-signed certificates by default. You must either configure the client applications to accept the self-signed certificates, or else use certificates signed by recognized CAs.

You can further debug the network traffic by collecting debug traces. To see the traffic going over TLS/SSL in debug mode, configure OpenDJ to dump debug traces from `javax.net.debug` into the `logs/server.out` file:

```
$ OPENDJ_JAVA_ARGS="-Djavax.net.debug=all" start-ds
```

22.7.1 Troubleshooting Certificates and SSL Authentication

Replication uses SSL to protect directory data on the network. In some configurations, replica can fail to connect to each other due to SSL handshake errors. This leads to error log messages such as the following:

```
[21/Nov/2011:13:03:20 -0600] category=SYNC severity=NOTICE  
msgID=15138921 msg=SSL connection attempt from myserver (123.456.789.012)  
failed: Remote host closed connection during handshake
```

Notice these problem characteristics in the message above:

- The host name, `myserver`, is not fully qualified.

You should not see non-fully qualified host names in the error logs. Non-fully qualified host names are a sign that an OpenDJ server has not been configured properly.

Always install and configure OpenDJ using fully qualified host names. The OpenDJ administration connector, which is used by the **`dsconfig`** command, and also replication depend upon SSL and, more specifically, self-signed certificates for establishing SSL connections. If the host name used for connection establishment does not correspond to the host name stored in the SSL certificate then the SSL handshake can fail. For the purposes of establishing the SSL connection, a host name like `myserver` does not match `myserver.example.com`, and vice versa.

- The connection succeeded, but the SSL handshake failed, suggesting a problem with authentication or with the cipher or protocol negotiation. As

most deployments use the same Java Virtual Machine (JVM), and the same JVM configuration for each replica, the problem is likely not related to SSL cipher or protocol negotiation, but instead lies with authentication.

Follow these steps on each OpenDJ server to check whether the problem lies with the host name configuration:

1. Make sure each OpenDJ server uses only fully qualified host names in the replication configuration. You can obtain a quick summary by running the following command against each server's configuration:

```
$ grep ds-cfg-replication-server: config/config.ldif | sort | uniq
```

2. Make sure that the host names in OpenDJ certificates also contain fully qualified host names, and correspond to the host names found in the previous step:

```
# Examine the certificates used for the administration connector.
$ keytool -list -v -keystore config/admin-truststore \
-storepass `cat config/admin-keystore.pin` | grep "^Owner:"

# Examine the certificates used for replication.
$ keytool -list -v -keystore config/ads-truststore \
-storepass `cat config/ads-truststore.pin` | grep "^Owner:"
```

Sample output for a server on host `opendj.example.com` follows:

```
$ grep ds-cfg-replication-server: config/config.ldif | sort | uniq
ds-cfg-replication-server: opendj.example.com:8989
ds-cfg-replication-server: opendj.example.com:9989

$ keytool -list -v -keystore config/admin-truststore
-storepass `cat config/admin-keystore.pin` | grep "^Owner:"
Owner: CN=opendj.example.com, O=Administration Connector Self-Signed Certificate

$ keytool -list -v -keystore config/ads-truststore \
-storepass `cat config/ads-truststore.pin` | grep "^Owner:"
Owner: CN=opendj.example.com, O=OpenDJ Certificate
Owner: CN=opendj.example.com, O=OpenDJ Certificate
Owner: CN=opendj.example.com, O=OpenDJ Certificate
```

Unfortunately there is no easy solution to badly configured host names. It is often easier and quicker simply to reinstall your OpenDJ servers remembering to use fully qualified host names everywhere. Consider the following:

- When using the **setup** tool to install and configure a server ensure that the `-h` option is included, and that it specifies the fully qualified host name. Make

sure you include this option even if you are not enabling SSL/StartTLS LDAP connections.

If you are using the GUI installer, then make sure you specify the fully qualified host name on the first page of the wizard.

- When using the **dsreplication** tool to enable replication make sure that any --host options include the fully qualified host name.

If you cannot reinstall the server, follow these steps:

1. Disable replication in each replica:

```
$ dsreplication \  
disable \  
--disableAll \  
--port adminPort \  
--hostname hostName \  
--bindDN "cn=Directory Manager" \  
--adminPassword password \  
--trustAll \  
--no-prompt
```

2. Stop and restart each server in order to clear the in-memory ADS truststore backend.
3. Enable replication making certain that fully qualified host names are used throughout:

```
$ dsreplication \  
enable \  
--adminUID admin \  
--adminPassword password \  
--baseDN dc=example,dc=com \  
--host1 hostName1 \  
--port1 adminPort1 \  
--bindDN1 "cn=Directory Manager" \  
--bindPassword1 password \  
--replicationPort1 replPort1 \  
--host2 hostName2 \  
--port2 adminPort2 \  
--bindDN2 "cn=Directory Manager" \  
--bindPassword2 password \  
--replicationPort2 replPort2 \  
--trustAll \  
--no-prompt
```

4. Repeat the previous step for each remaining replica. In other words, host1 with host2, host1 with host3, host1 with host4, ..., host1 with hostN.
5. Initialize all remaining replica with the data from host1:

```
$ dsrepllication \  
  initialize-all \  
  --adminUID admin \  
  --adminPassword password \  
  --baseDN dc=example,dc=com \  
  --hostname hostName1 \  
  --port 4444 \  
  --trustAll \  
  --no-prompt
```

6. Check that the host names are correct in the configuration and in the keystores by following the steps you used to check for host name problems. The only broken host name remaining should be in the key and truststores for the administration connector:

```
$ keytool -list -v -keystore config/admin-truststore \  
  -storepass `cat config/admin-keystore.pin` |grep "^Owner:"
```

7. Stop each server, and then fix the remaining admin connector certificate as described in [Procedure 20.1, "To Replace a Server Key Pair"](#).

22.7.2 Handling Compromised Keys

As explained in [Chapter 20, "Changing Server Certificates"](#), OpenDJ directory server has different keys and keystores for different purposes. The public keys used for replication are also used to encrypt shared secret symmetric keys, for example, to encrypt and to sign backups. This section looks at what to do if either a key pair or secret key is compromised.

How you handle the problem depends on which key was compromised:

- For a key pair used for a client connection handler and with a certificate signed by a certificate authority (CA), contact the CA for help. The CA might choose to publish a certificate revocation list (CRL) that identifies the certificate of the compromised key pair.

Also make sure you replace the key pair. See [Procedure 20.1, "To Replace a Server Key Pair"](#) for specific steps.

- For a key pair used for a client connection handler and that has a self-signed certificate, follow the steps in [Procedure 20.1, "To Replace a Server Key Pair"](#), and make sure the clients remove the compromised certificate from their truststores, updating those truststores with the new certificate.

- For a key pair that is used for replication, mark the key as compromised as described below, and replace the key pair. See [Procedure 20.2, "To Replace the Key Pair Used for Replication"](#) for specific steps.

To mark the key pair as compromised, follow these steps:

1. Identify the key entry by searching administrative data on the server whose key was compromised.

The server in this example is installed on `opendj.example.com` with administration port 4444:

```
$ ldapsearch \  
--port 1389 \  
--hostname opendj.example.com \  
--baseDN "cn=admin data" \  
"(cn=opendj.example.com:4444)" ds-cfg-key-id  
dn: cn=opendj.example.com:4444,cn=Servers,cn=admin data  
ds-cfg-key-id: 4F2F97979A7C05162CF64C9F73AF66ED
```

The key ID, 4F2F97979A7C05162CF64C9F73AF66ED, is the RDN of the key entry.

2. Mark the key as compromised by adding the attribute, `ds-cfg-key-compromised-time`, to the key entry.

The attribute has generalized time syntax, and so takes as its value the time at which the key was compromised expressed in generalized time. In the following example, the key pair was compromised at 8:34 AM UTC on March 21, 2013:

```
$ ldapmodify  
--port 1389  
--hostname opendj.example.com  
--bindDN "cn=Directory Manager"  
--bindPassword password  
dn: ds-cfg-key-id=4F2F97979A7C05162CF64C9F73AF66ED,cn=instance keys,cn=admin data  
changetype: modify  
add: ds-cfg-key-compromised-time  
ds-cfg-key-compromised-time: 201303210834Z  
  
Processing MODIFY request for ds-cfg-key-id=4F2F97979A7C05162CF64C9F73AF66ED,  
cn=instance keys,cn=admin data  
MODIFY operation successful for DN ds-cfg-key-id=4F2F97979A7C05162CF64C9F73AF66ED  
,cn=instance keys,cn=admin data
```

3. If the server uses encrypted or signed data, then the shared secret keys used for encryption or signing and associated with the compromised key pair should also be considered compromised. Therefore, mark all shared secret keys encrypted with the instance key as compromised.

To identify the shared secret keys, find the list of secret keys in the administrative data whose `ds-cfg-symmetric-key` starts with the key ID of the compromised key:

```
$ ldapsearch \
--port 1389 \
--bindDN "cn=Directory Manager" \
--bindPassword password \
--baseDN "cn=secret keys,cn=admin data" \
"(ds-cfg-symmetric-key=4F2F979A7C05162CF64C9F73AF66ED*)" dn
dn: ds-cfg-key-id=fba16e59-2ce1-4619-96e7-8caf33f916c8,cn=secret keys,cn=admin d
ata

dn: ds-cfg-key-id=57bd8b8b-9cc6-4a29-b42f-fb7a9e48d713,cn=secret keys,cn=admin d
ata

dn: ds-cfg-key-id=f05e2e6a-5c4b-44d0-b2e8-67a36d304f3a,cn=secret keys,cn=admin d
ata
```

For each such key, mark the entry with `ds-cfg-key-compromised-time` as shown above for the instance key.

Changes to administration data are replicated to other OpenDJ servers in the replication topology.

- For a shared secret key used for data encryption that has been compromised, mark the key entry with `ds-cfg-key-compromised-time` as shown in the example above that demonstrates marking the instance key as compromised.

Again, changes to administration data are replicated to other OpenDJ servers in the replication topology.

22.8 Troubleshooting Client Operations

By default OpenDJ logs information about all LDAP client operations in `logs/access`, and all HTTP client operations in `logs/http-access`. The following lines are wrapped for readability, showing a search for the entry with `uid=bjensen` as traced in the LDAP access log. In the access log itself, each line starts with a time stamp:

```
[27/Jun/2011:17:23:00 +0200] CONNECT conn=19 from=127.0.0.1:56641
to=127.0.0.1:1389 protocol=LDAP
[27/Jun/2011:17:23:00 +0200] SEARCH REQ conn=19 op=0 msgID=1
base="dc=example,dc=com" scope=wholeSubtree filter="(uid=bjensen)" attrs="ALL"
[27/Jun/2011:17:23:00 +0200] SEARCH RES conn=19 op=0 msgID=1
result=0 nentries=1 etime=3
[27/Jun/2011:17:23:00 +0200] UNBIND REQ conn=19 op=1 msgID=2
[27/Jun/2011:17:23:00 +0200] DISCONNECT conn=19 reason="Client Unbind"
```

As you see, each client connection and set of LDAP operations are traced, starting with a time stamp and information about the operation performed, then including information about the connection, the operation number for the sequence of operations performed by the client, a message identification number, and additional information about the operation.

To match HTTP client operations with related internal server operations, first prevent OpenDJ from suppressing internal operations from the LDAP access log by using the **dsconfig** command to set the LDAP access log publisher `suppress-internal-operations` advanced property to `false`. Then match the values of the `x-connection-id` field in the HTTP access log with `conn=id` values in the LDAP access log.

For example, consider an HTTP GET request for the `_id` field of the user `newuser`, which is handled by connection 4 as shown in `logs/http-access`:

```
- 192.168.0.12 bjensen 22/May/2013:16:27:52 +0200
GET /users/newuser?_fields=_id HTTP/1.1 200
curl/7.21.4 4 12
```

With internal operations logged in `logs/access`, log lines for the related operations have `conn=4`:

```
[22/May/2013:16:27:52 +0200] CONNECT conn=4
  from=192.168.0.12:63593 to=192.168.0.12:8080 protocol=HTTP/1.1
[22/May/2013:16:27:52 +0200] SEARCH REQ conn=4
  op=0 msgID=0 base="ou=people,dc=example,dc=com" scope=wholeSubtree
  filter="(&(objectClass=inetOrgPerson)(uid=bjensen))" attrs="1.1"
[22/May/2013:16:27:52 +0200] SEARCH RES conn=4
  op=0 msgID=0 result=0 nentries=1 etime=5
[22/May/2013:16:27:52 +0200] BIND REQ conn=4
  op=1 msgID=1 version=3 type=SIMPLE
  dn="uid=bjensen,ou=People,dc=example,dc=com"
[22/May/2013:16:27:52 +0200] BIND RES conn=4
  op=1 msgID=1 result=0 authDN="uid=bjensen,ou=People,dc=example,dc=com"
  etime=3
[22/May/2013:16:27:52 +0200] SEARCH REQ conn=4
  op=2 msgID=2 base="uid=newuser,ou=people,dc=example,dc=com" scope=baseObject
  filter="(objectClass=*)" attrs="uid,etag"
[22/May/2013:16:27:52 +0200] SEARCH RES conn=4
  op=2 msgID=2 result=0 nentries=1 etime=4
[22/May/2013:16:27:52 +0200] UNBIND REQ conn=4
  op=3 msgID=3
[22/May/2013:16:27:52 +0200] DISCONNECT conn=4
  reason="Client Unbind"
```

To help diagnose errors due to access permissions, OpenDJ supports the get effective rights control. The control OID, 1.3.6.1.4.1.42.2.27.9.5.2, is not allowed by the default global ACIs. You must therefore add access to use the get effective rights control when not using it as Directory Manager.

22.8.1 Clients Need Simple Paged Results Control

For Solaris and some versions of Linux you might see a message in the OpenDJ access logs such as the following:

The request control with Object Identifier (OID) "1.2.840.113556.1.4.319" cannot be used due to insufficient access rights

This message means clients are trying to use the [simple paged results control](#) without authenticating. By default, OpenDJ includes a global ACI to allow only authenticated users to use the control:

```
$ dsconfig \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword "password" \
get-access-control-handler-prop

Property      : Value(s)
-----
enabled       : true
global-aci    : (extop="1.3.6.1.4.1.26027.1.6.1 || 1.3.6.1.4.1.26027.1.6.3 ||
...
               : (targetcontrol="1.3.6.1.1.12 || 1.3.6.1.1.13.1 || 1.3.6.1.1.13.2
               : || 1.2.840.113556.1.4.319 || 1.2.826.0.1.3344810.2.3 ||
               : 2.16.840.1.113730.3.4.18 || 2.16.840.1.113730.3.4.9 ||
               : 1.2.840.113556.1.4.473 || 1.3.6.1.4.1.42.2.27.9.5.9") (version
               : 3.0; acl "Authenticated users control access"; allow(read)
               : userdn="ldap:///all");, (targetcontrol="2.16.840.1.113730.3.4.2 ||
               : 2.16.840.1.113730.3.4.17 || 2.16.840.1.113730.3.4.19 ||
               : 1.3.6.1.4.1.4203.1.10.2 || 1.3.6.1.4.1.42.2.27.8.5.1 ||
               : 2.16.840.1.113730.3.4.16") (version 3.0; acl "Anonymous control
               : access"; allow(read) userdn="ldap:///anyone");)
```

To grant anonymous (unauthenticated) user access to the control, add the OID for the simple paged results control to the list of those in the Anonymous control access global ACI:

```
$ dsconfig \
--port 4444 \
--hostname opendj.example.com \
--bindDN "cn=Directory Manager" \
--bindPassword "password" \
set-access-control-handler-prop \
--remove global-aci:"(targetcontrol=\"2.16.840.1.113730.3.4.2 || \
2.16.840.1.113730.3.4.17 || 2.16.840.1.113730.3.4.19 || \
1.3.6.1.4.1.4203.1.10.2 || 1.3.6.1.4.1.42.2.27.8.5.1 || \
2.16.840.1.113730.3.4.16\") (version 3.0; acl \"Anonymous control access\"; \
allow(read) userdn=\"ldap:///anyone\";)" \
--add global-aci:"(targetcontrol=\"2.16.840.1.113730.3.4.2 || \
2.16.840.1.113730.3.4.17 || 2.16.840.1.113730.3.4.19 || \
1.3.6.1.4.1.4203.1.10.2 || 1.3.6.1.4.1.42.2.27.8.5.1 || \
2.16.840.1.113730.3.4.16 || 1.2.840.113556.1.4.319\") \
(version 3.0; acl \"Anonymous control access\"; allow(read) \
userdn=\"ldap:///anyone\";)" \
--no-prompt
```

Alternatively, stop OpenDJ, edit the corresponding ACI carefully in `/path/to/opendj/config/config.ldif`, and restart OpenDJ.¹

¹Unlike the **dsconfig** command, the `config.ldif` file is not a public interface, so this alternative should not be used in production.

22.9 Troubleshooting Replication

Replication can generally recover from conflicts and transient issues. Replication does, however, require that update operations be copied from server to server. It is therefore possible to experience temporary delays while replicas converge, especially when the write operation load is heavy. OpenDJ's tolerance for temporary divergence between replicas is what allows OpenDJ to remain available to serve client applications even when networks linking the replicas go down.

In other words, the fact that directory services are loosely convergent rather than transactional is a feature, not a bug.

That said, you may encounter errors. Replication uses its own error log file, `logs/replication`. Error messages in the log file have `category=SYNC`. The messages have the following form. Here the line is folded for readability:

```
[27/Jun/2011:14:37:48 +0200] category=SYNC severity=INFORMATION msgID=14680169
msg=Replication server accepted a connection from 10.10.0.10/10.10.0.10:52859
to local address 0.0.0.0/0.0.0.0:8989 but the SSL handshake failed. This is
probably benign, but may indicate a transient network outage or a
misconfigured client application connecting to this replication server.
The error was: Remote host closed connection during handshake
```

OpenDJ maintains historical information about changes in order to bring replicas up to date, and to resolve replication conflicts. To prevent historical information from growing without limit, OpenDJ purges historical information after a configurable delay (`replication-purge-delay`, default: 3 days). A replica can become irrevocably out of sync if you restore it from a backup archive older than the purge delay, or if you stop it for longer than the purge delay. If this happens to you, disable the replica, and then reinitialize it from a recent backup or from a server that is up to date.

22.10 Asking For Help

When you cannot resolve a problem yourself, and want to ask for help, clearly identify the problem and how you reproduce it, and also the version of OpenDJ you use to reproduce the problem. The version includes both a version number and also a build time stamp:

```
$ dsconfig --version
OpenDJ 3.0.0
Build yyyyymmddhhmmssZ
```

Be ready to provide the following additional information:

- The output from the **java -version** command.
- access and errors logs showing what the server was doing when the problem started occurring
- A copy of the server configuration file, `config/config.ldif`, in use when the problem started occurring
- Other relevant logs or output, such as those from client applications experiencing the problem
- A description of the environment where OpenDJ is running, including system characteristics, host names, IP addresses, Java versions, storage characteristics, and network characteristics. This helps to understand the logs, and other information.

Index

A

- Access control, 9, 55, 70
 - Debugging, 93
 - Disabling anonymous access, 89
 - Effective rights, 93
 - Evaluation, 76
 - Examples, 85
 - Operations, 77
 - Permissions, 73
 - Subjects, 74
 - Targets, 71
- Accounts
 - Activating, 200
 - Customizing notification messages, 202
 - Disabling, 200
 - Lockout, 198
 - Status notifications, 200
- Active Directory (see Pass-through authentication)
- Alerts, 281

B

- Backup, 29, 163, 166
 - Recovery from user error, 159

C

- Certificate revocation lists, 59
- Certificates, 41, 58, 307, 317, 334
- Commands, 16
- Control panel, 13

D

- Database backend
 - Creating, 34
 - Deleting, 38
 - Setting disk space thresholds, 36
 - Updating, 37
- Debug log, 326
- Directory services
 - About, 1
- DSML, 10, 64

E

- Exporting data, 29
- External change log, 150
 - Legacy format, 157

F

- File descriptors
 - Requirements, 291

H

- High availability (see Replication)
- HTTP, 60

I

- Importing data, 29
 - Performance, 294
 - Test data, 30
- Indexes, 97
 - Approximate, 98, 105
 - Configuring, 104
 - Debugging searches, 100
 - Default settings, 114
 - Entry limits, 110
 - Equality, 98
 - Extensible matching rule, 100, 106
 - Ordering, 98
 - Presence, 99
 - Rebuilding, 108
 - Substring, 99
 - Verifying, 113
 - Virtual list view (browsing), 100, 106

J

- JMX, 66, 254
- JSON, 60

L

- LDAP
 - About, 1
 - Data, 3
- LDAP controls
 - About, 7
- LDAP extended operations
 - About, 8

LDIF

- Export, 29
- File as backend, 67
- Import, 29
- Tools, 33

Lockdown mode, 328

Logs, 256

- Debug, 326
- Filtering, 279

M

Monitoring, 251

Moving servers, 317

P

Pass-through authentication, 235

Password policy, 169

- Behera Internet-Draft, 172
- Default, 176
- Samples, 191

Passwords

- Generating, 184
- Storage schemes, 185
- Validating, 188

Performance tuning, 287

Ports

- Configuring, 39

Privileges, 79

Provisioning, 29

R

Replication

- Assured, 140
- Change notification, 150
- Configuring, 123
- Crash recovery, 26
- Data access, 86
- Dedicated servers, 132, 136
- Fractional, 142
- Grouping servers, 138
- Log, 256
- Moving servers, 317
- Overview, 118
- Password policy, 172
- Quick setup, 117

Read-only servers, 140

Recovery from user error, 159

Restoring from backup, 167

Schema definitions, 224

Stopping, 130

Subtree, 142

Troubleshooting, 340

Unique attributes, 218

Write throughput, 288

Resetting passwords

- cn=Directory Manager, 324
- Global (replication) administrator, 326

Resource limits, 205

REST, 10, 60

Restart server, 25

Restoring

- From backup, 166
- From LDIF, 29

S

Samba, 247

Schema, 8, 221

Bundled definitions, 231

Legacy data, 230

Schema definition extensions, 228, 229, 229

SNMP, 252

SSL, 53, 334

Start server, 23

StartTLS, 52

Stop server, 25

T

TLS, 57

Troubleshooting, 323

Recovery from user error, 159

U

Unique attribute values, 211