

OpenLDAP Database

DESCRIPTION



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2016, Mitel Networks Corporation

All rights reserved

1 INTRODUCTION

1.1 SCOPE

This document describes the general principle for how a replicated OpenLDAP directory is used as a (partly redundant) distributed configuration database in the MX-ONE Service Node. The document also describes the most important files stored in the file system using OpenLDAP, and the basic principle of the tree structure used for the data stored in OpenLDAP.

1.2 GENERAL OPENLDAP INFORMATION

This document provides information only on those aspects of the use of OpenLDAP that are unique to the MX-ONE Service Node. For information about general OpenLDAP use, you are recommended to read:

- The **OpenLDAP Software 2.3 Administrator's Guide** available for free downloading from <http://www.openldap.org/>
- **Deploying OpenLDAP** by Tom Jackiewicz. Apress 2005. ISBN: 1-59059-413-4
- **LDAP System Administration** by Gerald Carter. O Reilly 2003. ISBN: 1-56592-491-6
- **Understanding and Deploying LDAP Directory Services** by Timothy A. Howes, Mark C. Smith and Gordon S. Good. Second Edition. Addison-Wesley / Pearson Education Inc. 2003. ISBN: 0-672-32316-8
- **LDAP, Programming Directory-Enabled Applications with Lightweight Directory Access Protocol** by Timothy A Howes and Mark C. Smith. New Riders (Technology Series) 1997. ISBN: 1-57870-000-0

1.3 GLOSSARY AND ACRONYMS

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

2

OVERVIEW

2.1

ARCHITECTURE

The architectural model is to have an OpenLDAP server in every LIM serving the telephony applications of that LIM. Thus read requests are always directed to localhost and served locally.

One of the OpenLDAP servers is a read/write master, and all other OpenLDAP servers are read-only replicas. (Write operations need network access to the OpenLDAP master server.)

In a telephony system with small amounts of configuration changes, the OpenLDAP master server can be located on one of the LIMs as the OpenLDAP server of that LIM. (The other LIMs have read-only replica servers.)

In a telephony system with large amounts of configuration changes, the OpenLDAP master server must be located on a special external server. All LIMs will then have their own local read-only replica OpenLDAP server.

If the OpenLDAP master server is out of service for a long time (for instance due to hardware failure), it is possible to manually reconfigure one of the OpenLDAP replica servers to be the new master (without loss of data). This is seen as a manual service measure. This process will not be automated.

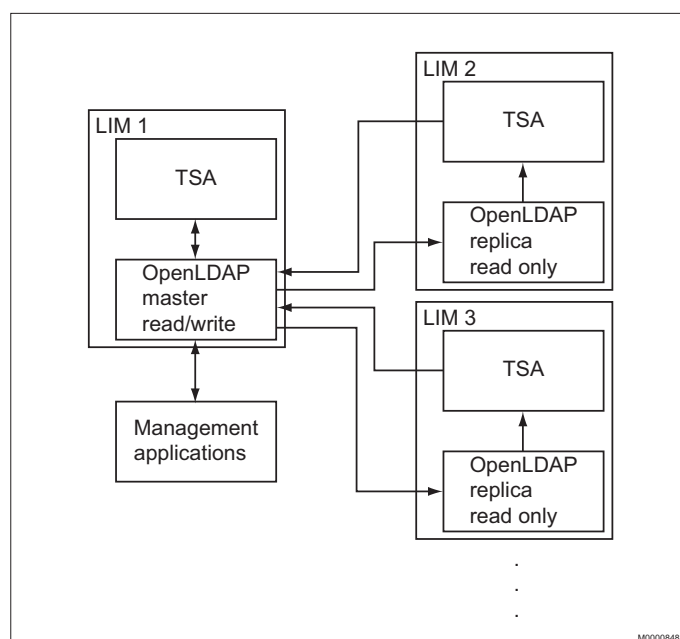


Figure 1: Sketch of architecture for system with low volume of configuration changes. Arrow direction indicates data flow direction.

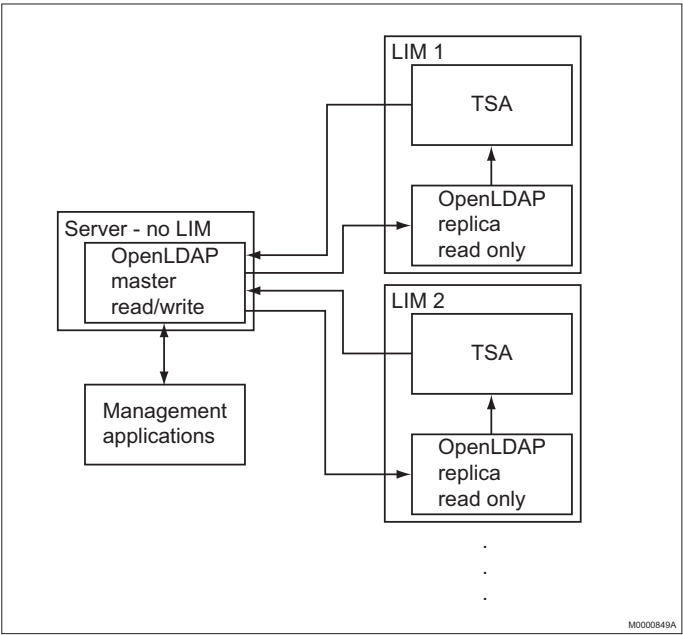


Figure 2: Sketch of architecture for system with high volume of configuration changes. Arrow direction indicates data flow direction.

2.2 LDAP DATA MODEL

2.2.1 LDAP SECTION ILLUSTRATION

This section briefly describes the intended data model.

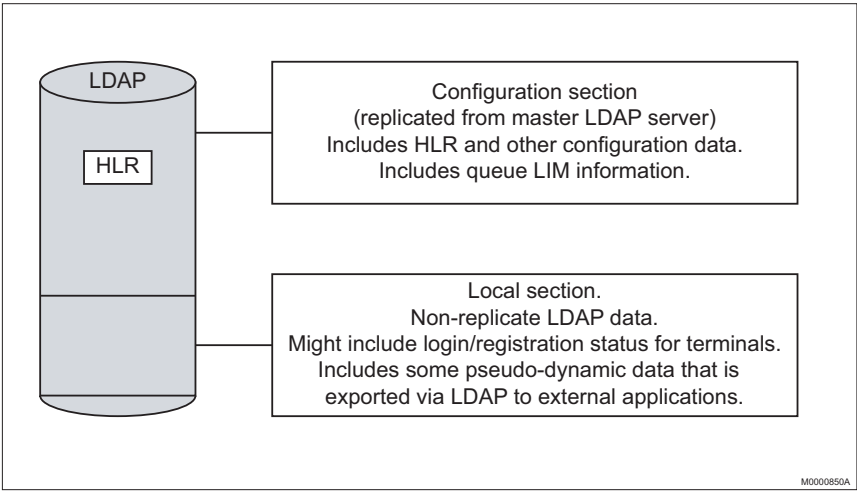


Figure 3: LDAP Sections

There are two sections in LDAP. Each section is implemented using its own back-end database. The configuration section (also known as the master section) is replicated (read-only) from the master LDAP server to the LDAP servers on every LIM. The local section holds data that exists only locally on the specific LIM.

Every LIM host has its own LDAP server, and every LDAP server has both the configuration and the local section.

2.2.2

LDAP SYNC-REPLICATION

The sync-replication protocol of OpenLDAP (refresh and persist) is used. In this way all the necessary information is available locally on every LIM. Every LDAP read operation is a local operation to localhost. In this way network disturbance cannot affect read operations.

The configuration section has one master LDAP server that holds the read/write copy of the configuration data. Using OpenLDAP sync-replication this is replicated to every LIM host.

The local section has data that is stored only locally on the current LIM host.

2.2.3

LDAP DATA TREE

The LDAP data is organized in a tree as follows:

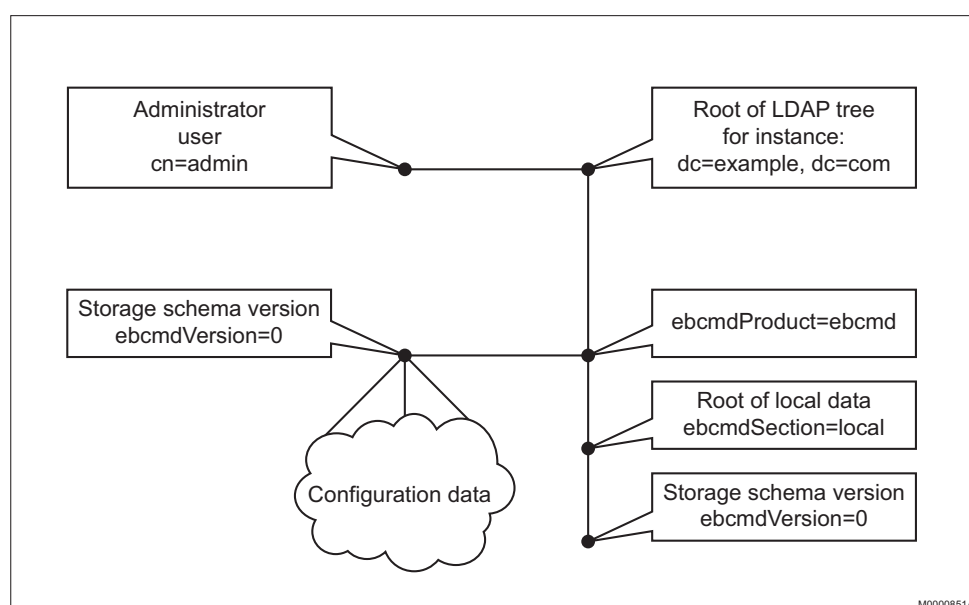


Figure 4: LDAP Data Organization

3

FILES

The files related to the use of OpenLDAP are data files, OpenLDAP configuration files, the start script and the slapd binary.

The start script we use is **/etc/init.d/eri_ldap**.

Never run the script **/etc/init.d/ldap** (if it exists on your system). That script is shipped by SuSE with their OpenLDAP version and does not work for the MX-ONE use of LDAP.

The OpenLDAP server binary is called **slapd** and is stored under **/opt/eri_sn/sbin**. There is also a non-optimized debug version of the server called **slapd_dbg**. (To run the debug version, type debug as the second argument to the **/etc/init.d/eri_ldap** start script.)

Under **/opt/eri_sn/sbin** you will also find some other programs with names starting with **slap**. These are utility commands shipped with OpenLDAP. There are also some programs with names starting with **db_**. These are utility commands shipped with the Berkeley Data Base backend used by OpenLDAP. There are also some programs with names starting with **ldap** and **ldap_**. The programs with names starting with **ldap_** are MX-ONE Service Node commands for the administration and debugging of the use of OpenLDAP. The programs with names starting with **ldap** (without the underscore **_**) are utility commands shipped with OpenLDAP.

3.1

DATA FILES

The binary database files that OpenLDAP store data in, are located in the directories: **/var/opt/eri_sn/ldap/master** and **/var/opt/eri_sn/ldap/local**.

The hot-backup files (which are used for fast recovery if the original binary database files get corrupted) are stored in the directory: **/var/opt/eri_sn/ldap/recovery**.

The backup files of the OpenLDAP data are in LDIF (Ldap Data Interchange Format) and are stored as **/var/opt/eri_sn/ldap/ldapBackup_*.ldif**. The LDIF files are human-readable ASCII, and data can be read back from LDIF independent of the LDAP server version. Only the master can read data from the LDIF files.

3.2

OPENLDAP CONFIGURATION FILE

The configuration file for the OpenLDAP server is **/etc/openldap/slapd.conf**.

The file **/etc/openldap/slapd.conf** is created by the command **ldap_config_create**. This is normally done by the MX-ONE Service Node installation.

The line **loglevel** in the file **/etc/openldap/slapd.conf** may be interesting to edit. A value of 0 means no logging. No logging gives the best performance, but makes debugging very hard. The default value is 64, which is a reasonable compromise between performance and debugging possibilities. Setting the value to -1 will give lots of logging for debugging, but very bad performance. See the OpenLDAP documentation for more information about **loglevel**.

4

BACKUP STRATEGY

The backup strategy for OpenLDAP-based data is integrated with the backup strategy for old style reload data in the MX-ONE Service Node. There is no separate backup or restore done for LDAP data. The *data_backup* and *data_restore* commands affect both reload and LDAP data.

4.1

THE DATA_BACKUP COMMAND

When the *data_backup* command is issued, the LDAP data in every LIM is dumped to an LDIF (Ldap Data Interchange Format) file. The LDIF file is stored locally in the LIM just as the .D files for reload data.

When a data reload is executed (either as a result of the *data_restore* command or as a system measure), the data in the master LDAP server is rolled back to match the LDIF file. (This is done by running an *ldap_rollback* command behind the scenes. The *ldap_rollback* command compares the data in the LDAP server to the data in the LDIF file. Then it does only the necessary changes to make the data in the LDAP server match the LDIF file.)

Only the master LDAP server can read data from the LDIF file, but the LDIF file is created on every LIM in case the master has to be moved due to hardware failure.

Whenever the *data_backup* command is issued a hot-backup (see 4.3 Hot-backup on page 8) is also created.

4.2

SAFETY BACKUP

The data dumped to the local hard disk by the *data_backup* command has to be backed up to some external storage as a safety backup. This procedure is not described here as it is not LDAP-specific. The LDAP data that needs to be included in the safety backup are the LDIF files (*/var/opt/eri_sn/ldap/ldapBackup_*.ldif*) and the OpenLDAP server configuration file (*/etc/openldap/slapd.conf*).

4.3

HOT-BACKUP

At every clean shutdown of the OpenLDAP server a hot-backup is created. A hot-backup is also created when the *data_backup* command is run. The hot-backup creates a consistent binary copy of the OpenLDAP binary database files. The hot-backup files are stored in */var/opt/eri_sn/ldap/recovery*

The hot-backup is used for fast recovery if the OpenLDAP binary database files get corrupted. Recovery from the hot-backup files can be done on any OpenLDAP server (both master and replica).

5

STARTING AND STOPPING OPENLDAP

OpenLDAP should always be started and stopped using the start script **/etc/init.d/eri_ldap**.

The start script **/etc/init.d/eri_ldap** creates a hot-backup at every clean shutdown.

The start script **/etc/init.d/eri_ldap** checks the consistency of the OpenLDAP binary database files before starting OpenLDAP. If the binary database files are corrupt, they are recovered from the hot-backup. If recovery from the hot-backup is not possible, the master is recreated from the LDIF file, and the replicas are recreated by replicating all data from the master.

Arguments to the start script **/etc/init.d/eri_ldap** can be used to force a replica to do a complete resync to the master, and to force the use of the debug version of the OpenLDAP server.

6

ALARMS

The LDAP operation is supervised and alarms are generated for the following error conditions:

- Fault Code 1:24 Cannot write to master LDAP
- Fault Code 1:25 Broken connection to master LDAP
- Fault Code 1:26 Broken connection to local LDAP
- Fault Code 1:27 Local LDAP out of order
- Fault Code 1:28 Master LDAP out of order
- Fault Code 1:29 Local LDAP server not running

7

REFERENCES

The following **RFC standards** of the Internet Engineering Task Force (IETF <http://www.ietf.org/>) are relevant:

RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol
RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models
RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
RFC 4515	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters
RFC 4516	Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator
RFC 4517	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
RFC 4518	Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
RFC 4519	Lightweight Directory Access Protocol (LDAP): Schema for User Applications
RFC 4520	Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)
RFC 4521	Considerations for Lightweight Directory Access Protocol (LDAP) Extensions
RFC 4525	Lightweight Directory Access Protocol (LDAP) Modify- Increment Extension
RFC 4530	Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute
RFC 4531	Lightweight Directory Access Protocol (LDAP) Turn Operation
RFC 4533	The Lightweight Directory Access Protocol (LDAP) Content Synchronization Operation
RFC 3928	Lightweight Directory Access Protocol (LDAP) Client Update Protocol (LCUP)

See also the document *Fault location on OpenLDAP*.