Oracle Unified Directory

Integration Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-012599-001, Rev. C

Release Date: March 2016

Contents

Preface

This guide provides instructions for setting up a small test lab with OUD as Directory Server running with Luna HSM for securing the SSL private keys.

Scope

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of Oracle Unified Directory as LDAP Directory Server. Administrators are expected to understand Oracle Unified Directory Server concepts.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: Command-line commands and options (Type **dir /p**.) Button names (Click **Save As**.) Check box and radio button names (Select the **Print Duplex** check box.) Window titles (On the **Protect Document** window, click **Yes**.) Field names (**User Name:** Enter the name of the user.) Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1 Introduction

Overview

Oracle Unified Directory is a comprehensive next generation directory service. It is designed to address large deployments and to provide high performance, and is highly extensive. Oracle Unified Directory includes:

- LDAP directory server, used for storing data
- Proxy server, where the server acts as an interface between the client and the directory server that contains the data
- Replication gateway between Oracle Unified Directory and Oracle Directory Server Enterprise Edition

Oracle Unified Directory provides several mechanisms to secure traffic between the client and the server.

This document helps administrators through the steps to integrate Oracle Unified Directory as LDAP Directory server with SafeNet Network HSM.

SafeNet Network HSM provides a secure repository for storing key information. This significantly reduces the likelihood that sensitive key information will be exposed and helps protect the overall integrity of the secure communication mechanisms.

Scope

This guide provides instructions for setting up a small test lab with OUD as Directory Server running with SafeNet Network HSM for securing the SSL private keys. This guide explains how to install and configure software that is required for setting up a SSL on Oracle Unified Directory as LDAP Server while storing private key on SafeNet Network HSM.

3rd Party Application Details

- Oracle Unified Directory

Supported Platforms

Red Hat Enterprise Linux 6.5 (64 bit)

Third Party Application	Luna Client Software Version	SafeNet Luna HSM Appliance Software & Firmware Version
OUD 11.1.2.3	Luna Client 6.2 Luna Client 6.1	Luna SA v6.2.0 F/w 6.10.9

Red Hat Enterprise Linux 6.3 (64 bit)

Third Party Application	Luna Client Software Version	SafeNet Luna HSM Appliance Software & Firmware Version
OUD 11.1.2.2.0	Luna client 5.3.1(64 bit)	Luna SA v5.4.1 F/w 6.21.0

Solaris 10 SPARC (64 bit)

Third Party Application	Luna Client Software Version	SafeNet Luna HSM Appliance Software & Firmware Version
OUD 11.1.2.2.0	Luna client 5.3.1 (32 bit)	Luna SA v5.4.1 F/w 6.21.0

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for the installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started, ensure the following:

- SafeNet Network HSM appliance and a secure admin password
- SafeNet Network HSM, and a hostname, suitable for your network
- SafeNet Network HSM network parameters are set to work with your network
- Initialize SafeNet Network HSM.
- Create and exchange certificates between SafeNet Network HSM and Client system.
- Create a partition on SafeNet Network HSM. Remember the partition password that will be later used by Oracle Unified Directory.

- Register the client with the partition. Run the "vtl verify" command on the client system to display a registered partition. The general form of command for Windows is

  ```
  C:\Program Files\SafeNet\LunaClient > vtl verify.
  ```

- Enable partition policies 22 and 23: Activation and Auto Activation respectively.

Oracle Unified Directory Setup

It is recommended that you should familiarize yourself with the Oracle Unified Directory server. Refer to the Installation Guide for Oracle Unified Directory for more information to install and pre-installation requirements. After installation create OUD instance and start directory server from <OUD instance location>/bin directory.

Before you install

Before installing the WebLogic Server you need to install the JDK. Download the JDK software from Oracle support site and install it. You can use the following JDK software available at Oracle Technology Network.

- Java Development Kit 7

Start the Oracle Universal Installer (OUI) by running the runInstaller script, specifying the location of a valid Java Installation Java 7).

NOTE: Ensure that you do not run the Oracle Unified Directory installer as the root user.

For this integration, you need to install OUD server and create an instance of it using oud-setup and use below configurations:

OUD instance name: asinst1

Administration port: 4444

Default root user: "cn=directory manager"

Created following two files:

key-store-pin-file: Contains keystore password which will be generated in “Generate the Private Key” section of second chapter.

bindPasswordFile: Contains the password of "cn=directory manager".

2 Integrating Oracle Unified Directory with SafeNet Luna HSM

Set up SafeNet Luna HSM with Oracle Unified Directory

To set up Luna HSM for Oracle Unified Directory, perform the following steps:

1. Copy the libLunaAPI.so and LunaProvider.jar file from the <Luna Installation Directory> to appropriate extension folder under <JDK Installation directory>.

   For Example:

   ```
   # cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so so <Path to JDK installation
   directory>/jdk1.7.0_60/jre/lib/ext/
   ```

   ```
   # cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar so <Path to JDK installation
   directory>/jdk1.7.0_60/jre/lib/ext/
   ```

   Edit the Java Security Configuration file java.security located in the security directory under <JDK Installation directory>.

   For Example:

   ```
   # vi /usr/jdk1.7.0_60/jre/lib/security/java.security
   ```

2. Add the Luna Provider in java.security file as shown below:

   ```
   ----------------------------------------------------------------------------------------------------------------------------------------
   security.provider.1=sun.security.provider.Sun
   security.provider.2=sun.security.rsa.SunRsaSign
   security.provider.3=sun.security.ec.SunEC
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider
   security.provider.5=com.sun.crypto.provider.SunJCE
   security.provider.6=sun.security.jgss.SunProvider
   security.provider.7=com.sun.security.sasl.Provider
   security.provider.8=org.jcp.xml.dsig.internal.dom.XMLDSigRI
   security.provider.9=sun.security.smartcardio.SunPCSC
   security.provider.10=com.safenetinc.luna.provider.LunaProvider
   ----------------------------------------------------------------------------------------------------------------------------------------
   ```

3. Save the changes in the java.security file.

4. Create a file manually at <OUD instance location>/config and name it as “luna-keystore”. This file should contain "tokenlabel:myPartition" in it. myPartition is label of the partition, for example:

   tokenlabel:part1

   Here part1 is label of partition registered with the machine and will be used to store keys and certificates created or used by OUD.

   This file will be used as keystore file in further commands.

5. Export the JAVA_HOME and PATH variables.

   For Example:

   ```
   # export JAVA_HOME= /usr/jdk1.7.0_60
   ```

   ```
   # export PATH=$JAVA_HOME/bin:$PATH
   ```

Generate the Private Key

Whether you use a self-signed certificate or generate a certificate signing request, you must first generate a private key. You can generate the private key by using the keytool utility with the -genkeypair option.

For example:

```
[oracle@localhost Oracle_OUD1]$ keytool -genkeypair -alias server-cert -keyalg rsa -keysize 2048 -
dname "CN=localhost.localdomain,O=SafeNet,C=IN" -keystore
/home/oracle/Oracle/Middleware/asinst_1/OUD/config/luna-keystore -storetype luna
```

Enter keystore password:

Re-enter new password:

Enter key password for <RHELserver-cert>

    (RETURN if same as keystore password):

Self-Sign the Certificate

```
[oracle@localhost Oracle_OUD1]$ keytool -selfcert -alias server-cert -validity 1825 -keystore
/home/oracle/Oracle/Middleware/asinst_1/OUD/config/luna-keystore -storetype luna
```

Enter keystore password:

Generate Certificate Request

In case not using self-signed certificate generate certificate request using keytool.

```
[oracle@localhost Oracle_OUD1]$ keytool -certreq -alias server-cert -file /tmp/server-cert.csr -
keystore /home/oracle/Oracle/Middleware/asinst_1/OUD/config/luna-keystore -keypass <password> -
storetype luna -storepass <password>
```

“keypass” is the password used for keystore and “storepass” is the partition password.

Send the certificate request to an external certificate authority. The certificate authority sends you a signed certificate file. Save the file in /tmp/cert.cer

Import Certificate

Use the -importcert to import the signed certificate.

```
[oracle@localhost bin]$ keytool -importcert -alias server-cert -file /tmp/cert.cer -keystore
/home/oracle/Oracle/Middleware/asinst_1/OUD/config/luna-keystore -storetype luna -storepass temp123#

Top-level certificate in reply:

Owner: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Issuer: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Serial number: 168164a428ca12dfab12f19fb1b93554

Valid from: Wed Apr 01 05:30:00 IST 2009 until: Sun Apr 01 05:29:59 IST 2029

Certificate fingerprints:

         MD5:  E0:19:F5:FC:C0:9A:13:0E:38:B7:BF:0D:02:40:D3:C2

         SHA1: 51:51:B8:63:8A:4C:1F:15:54:56:ED:37:C9:10:35:CA:D3:01:B9:36

         SHA256:
89:DD:5C:3D:FE:28:13:87:45:1F:A3:A0:F7:8C:1A:B6:77:DB:18:63:9E:71:72:AD:B2:52:91:CF:BE:F7:8D:19

         Signature algorithm name: SHA1withRSA

         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.5.5.7.1.12 Criticality=false
0000: 30 5F A1 5D A0 5B 30 59   30 57 30 55 16 09 69 6D  0_.].[0Y0W0U..im
0010: 61 67 65 2F 67 69 66 30   21 30 1F 30 07 06 05 2B  age/gif0!0.0...+
0020: 0E 03 02 1A 04 14 8F E5   D3 1A 86 AC 8D 8E 6B C3  ..............k.
0030: CF 80 6A D4 48 18 2C 7B   19 2E 30 25 16 23 68 74  ..j.H.,...0%.#ht
0040: 74 70 3A 2F 2F 6C 6F 67   6F 2E 76 65 72 69 73 69  tp://logo.verisi
0050: 67 6E 2E 63 6F 6D 2F 76   73 6C 6F 67 6F 2E 67 69  gn.com/vslogo.gi
0060: 66                                                 f


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 48 19 E7 92 6F 92 9D 34   63 99 C0 F0 99 C8 D6 A5  H...o..4c.......
0010: 8C 8C 7F 65                                        ...e
]
]
```

```
... is not trusted. Install reply anyway? [no]:  yes
Certificate reply was installed in keystore
```

Check the Certificate

```
[oracle@localhost bin]$ keytool -list -v -storetype luna –keystore
/home/oracle/Oracle/Middleware/asinst_1/OUD/config/luna-keystore

Enter keystore password:


Keystore type: LUNA

Keystore provider: LunaProvider


Your keystore contains 1 entries


Alias name: server-cert

Creation date: Jun 12, 2014

Entry type: PrivateKeyEntry

Certificate chain length: 3

Certificate[1]:

Owner: CN=RHEL.com, OU=HSM, O=SafeNet, L=Noida, ST=UP, C=IN

Issuer: CN=VeriSign Trial Secure Server CA - G2, OU=Terms of use at
https://www.verisign.com/cps/testca (c)09, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Serial number: 2388db46f0c171a443ec4f34d01e5fda

Valid from: Fri Jun 13 05:30:00 IST 2014 until: Mon Jul 14 05:29:59 IST 2014

Certificate fingerprints:

         MD5:  13:F9:C7:98:8C:30:F9:98:DD:95:CC:3E:E9:7F:01:55

         SHA1: 53:46:5C:FB:3F:8A:F5:CC:41:67:13:C6:3F:B2:31:85:32:9D:64:2C

         SHA256:
3C:61:EC:C3:1A:26:55:D6:18:A0:86:F7:39:91:21:04:36:FA:7C:B6:92:49:46:22:A1:3A:41:55:10:2D:21:B1

         Signature algorithm name: SHA1withRSA

         Version: 3

Certificate[2]:

Owner: CN=VeriSign Trial Secure Server CA - G2, OU=Terms of use at
https://www.verisign.com/cps/testca (c)09, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Issuer: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Serial number: 7e3bb784bbc654abd2b8d677ecc394a8

Valid from: Wed Apr 01 05:30:00 IST 2009 until: Mon Apr 01 05:29:59 IST 2019
```

```
Certificate fingerprints:

         MD5:  71:13:D9:3A:CD:21:F2:EE:9F:59:17:8D:A6:F9:AE:14

         SHA1: BE:D1:D1:4E:25:A7:94:36:83:9E:4B:A7:CD:84:48:96:B7:0A:7F:B0

         SHA256:
A0:E4:92:AB:5B:3D:CA:80:12:6F:89:A8:54:9A:D6:1A:F3:F6:ED:BD:87:54:32:9E:C0:51:89:69:74:A7:36:0B

         Signature algorithm name: SHA1withRSA

         Version: 3

Certificate[3]:

Owner: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Issuer: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

Serial number: 168164a428ca12dfab12f19fb1b93554

Valid from: Wed Apr 01 05:30:00 IST 2009 until: Sun Apr 01 05:29:59 IST 2029

Certificate fingerprints:

         MD5:  E0:19:F5:FC:C0:9A:13:0E:38:B7:BF:0D:02:40:D3:C2

         SHA1: 51:51:B8:63:8A:4C:1F:15:54:56:ED:37:C9:10:35:CA:D3:01:B9:36

         SHA256:
89:DD:5C:3D:FE:28:13:87:45:1F:A3:A0:F7:8C:1A:B6:77:DB:18:63:9E:71:72:AD:B2:52:91:CF:BE:F7:8D:19

         Signature algorithm name: SHA1withRSA

         Version: 3

*******************************************

*******************************************
```

Configure Oracle Unified Directory Server

This section describes the procedure to create key manager provider, configure trust manager, and configure connection handler for SSL.

“dsconfig” command provided by OUD is used to complete all the above tasks. It is located at “<OUD instance location>/bin” directory.

Create Key Manager Provider

```
[oracle@localhost bin]$ ./dsconfig create-key-manager-provider --set enabled:true --set key-store-
file:/home/oracle/Oracle/Middleware/asinst_1/OUD/config/luna-keystore --set key-store-type:luna --
set key-store-pin-file:/home/oracle/keyStorePin.txt --type file-based --provider-name Luna --
hostname localhost.localdomain --port 4444 --trustAll --bindDN cn=Directory\ Manager --
bindPasswordFile /home/oracle/pass.txt --no-prompt
```

Configure Trust Manager

Blind Trust Manager

```
[oracle@localhost bin]$ ./dsconfig -D "cn=directory manager" -j /home/oracle/pass.txt -X -n set-trust-manager-provider-prop --provider-name "Blind Trust" --set enabled:true
```

Configure Connection Handler for SSL

Create Connection Handler:

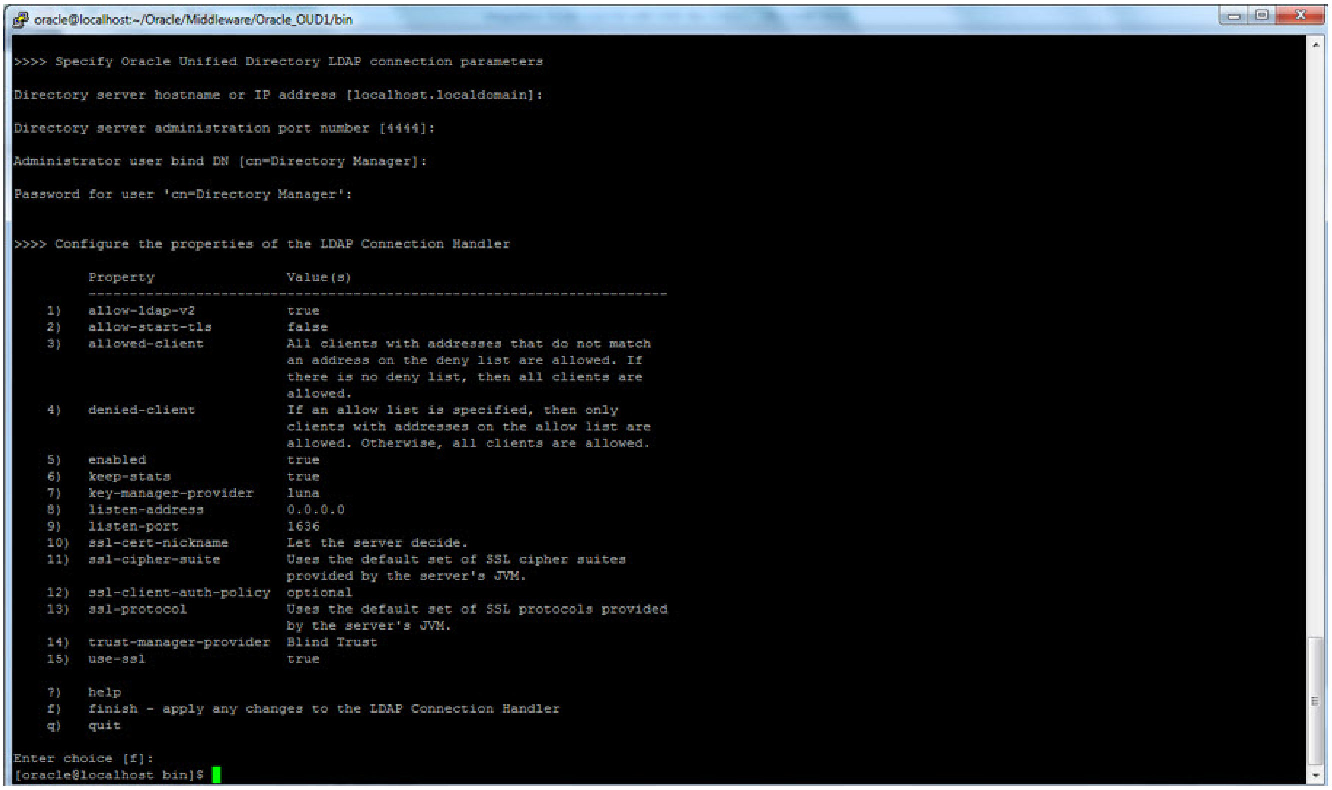
```
[oracle@localhost bin]$ ./dsconfig -h localhost.localdomain -p 4444 -D "cn=directory manager" -j /home/oracle/pass.txt -X -n create-connection-handler -t ldap --handler-name "Luna LDAPS Connection Handler" --set listen-port:1636 --set enabled:true
```

Set properties of connection Handler

```
[oracle@localhost bin]$ ./dsconfig -D "cn=directory manager" -j /home/oracle/pass.txt -X -n set-connection-handler-prop --handler-name "Luna LDAPS Connection Handler" --set "trust-manager-provider:Blind Trust" --set key-manager-provider:luna
```

```
[oracle@localhost bin]$ ./dsconfig -X set-connection-handler-prop --handler-name "Luna LDAPS Connection Handler" --set use-ssl:true
```

This command displays all the applied properties for LDAP Connection Handler, if you want to change any property you can change it. Press **Enter** to finish and apply changes. Refer the below screenshot:



```
>>>> Specify Oracle Unified Directory LDAP connection parameters

Directory server hostname or IP address [localhost.localdomain]:

Directory server administration port number [4444]:

Administrator user bind DN [cn=Directory Manager]:

Password for user 'cn=Directory Manager':


>>>> Configure the properties of the LDAP Connection Handler

         Property                 Value(s)
         ----------------------------------------------------------------------
    1)   allow-ldap-v2            true
    2)   allow-start-tls          false
    3)   allowed-client           All clients with addresses that do not match
                                  an address on the deny list are allowed. If
                                  there is no deny list, then all clients are
                                  allowed.
    4)   denied-client            If an allow list is specified, then only
                                  clients with addresses on the allow list are
                                  allowed. Otherwise, all clients are allowed.
    5)   enabled                  true
    6)   keep-stats               true
    7)   key-manager-provider     luna
    8)   listen-address           0.0.0.0
    9)   listen-port              1636
    10)  ssl-cert-nickname        Let the server decide.
    11)  ssl-cipher-suite         Uses the default set of SSL cipher suites
                                  provided by the server's JVM.
    12)  ssl-client-auth-policy   optional
    13)  ssl-protocol             Uses the default set of SSL protocols provided
                                  by the server's JVM.
    14)  trust-manager-provider   Blind Trust
    15)  use-ssl                  true

    ?)   help
    f)   finish - apply any changes to the LDAP Connection Handler
    q)   quit

Enter choice [f]:
[oracle@localhost bin]$
```

Test SSL Connection

The server should now have a second listener that accepts SSL-based client connections. Test the configuration with the ldapsearch command, for example:

```
[oracle@localhost bin]$ ./ldapsearch --port 1636 --useSSL --baseDN "" --searchScope base
"(objectClass=*)"

The server is using the following certificate:

    Subject DN:  CN=RHEL.com, OU=HSM, O=SafeNet, L=Noida, ST=UP, C=IN

    Issuer DN : CN=VeriSign Trial Secure Server CA - G2, OU=Terms of use at
https://www.verisign.com/cps/testca (c)09, OU="For Test Purposes Only.  No assurances.",
O="VeriSign, Inc.", C=US

    Validity:  Tue Jun 03 16:35:16 IST 2014 through Mon Sep 01 16:35:16 IST 2014

Do you wish to trust this certificate and continue connecting to the server?

Please enter "yes" or "no":yes

dn:

objectClass: ds-root-dse

objectClass: top
```