Troubleshoot Hardware Security Modules (HSM) Integration with FND

Contents

Introduction

This document describes the **Hardware Security Module** (HSM), integration with **Field Area Network** (FAN) solution, and troubleshooting common issues.

Hardware Security Module (HSM)

Hardware Security Modules (HSM) are available in three forms: appliance, PCI card, and cloud offering. Most deployments opt for the appliance version.

Software Security Modules (SSM)

Software Security Modules (SSM), on the other hand, are software packages that serve a similar purpose to HSM. They are bundled with FND software and provide a simple alternative instead of the appliance.

It is important to note that both HSM and SSM are optional components in FND deployments and are not mandatory.

Functions of the HSM

The primary function of both HSM and SSM in an FND solution is to securely store the PKI key pair and CSMP certificate, particularly when CSMP endpoints like meters are utilized.

These keys and certificates are essential for encrypting communication between FND and the CSMP endpoints.

Regarding deployment, HSM is a standalone appliance, while SSM can be installed either on the same Linux server as FND or on a separate Linux server. Configuration for SSM is specified in the cgms.properties file.

During bootup, FND checks for HSM client libraries, irrespective of whether HSM-related information is specified in cgms.properties. Any logs pertaining to missing HSM client libraries during bootup can be disregarded if HSM is not included in the solution.

Note: HSM-related information must be specified in the cgms.properties file, which is located in different directories depending on whether FND is installed via OVA or ISO.

HSM Client Installation

The HSM client must be installed on the same Linux server where the FND server is located. Customers can download the HSM client software from the Thales website or through a Cisco support contract.

The FND software release notes documents the required software on the HSM client and HSM software for the deployment. It is listed under the **HSM Upgrade Table** section for the release notes.

Path for HSM Client Installation Files, Configuration Files, and Libraries:

The default installation location is **/usr/safenet/lunaclient/bin** . Most commands, such as **lunacm**, **vtl**, or **ckdemo**, are run from this path (**/usr/safenet/lunaclient/bin**).

The configuration file is located at **/etc/Chrystoki.conf** .

The path to HSM Luna client library files needed by the FND server on Linux servers is **/usr/safenet/lunaclient/jsp/lib/** .

HSM Server

Most deployments utilize the HSM server as an appliance.

The HSM server needs to be partitioned, and HSM clients only have access to the specific partition they are assigned to. The HSM server can be PED authenticated or password-authenticated.

In password authentication, a username and password are sufficient for configuration changes in the HSM server.

However, PED authenticated HSM is a multifactor authentication method where, in addition to a password, the person making changes needs access to a PED key.

The PED key functions like a dongle, displaying a PIN that the user must enter along with the password to make any configuration changes.

For certain commands such as **show** commands and read-only access, PED key is not necessary. Only specific configuration changes like creating partitions require the PED key.

Each server partition can have multiple clients assigned to it, and all clients assigned to a partition have access to the data within that partition.

The HSM server offers various user roles, with the roles of admin and Crypto Security Officer being particularly important. Additionally, there is the role of partition security officer.

Troubleshooting

FND uses the HSM client to access the HSM hardware. Hence, there are 2 parts to the integration.

1. HSM client to HSM server communication
2. FND to HSM client communication

Both parts need to work for the HSM integration to be successful.

HSM client to HSM server communication

To determine whether the HSM client can successfully read the key and certificate information stored in the HSM partition on the HSM server using a single command, utilize the **/cmu list** command from the **/usr/safenet/lunaclient/bin** location.

Executing this command provides output indicating whether the HSM client can access the key and certificate stored in the HSM partition.

Please note that this command prompts for a password, which must be the same as the password for the HSM partition.

A successful output resembles this result:

```
[root@fndblr23 bin]# ./cmu list
Certificate Management Utility (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Please enter password for token in slot 0 : *******

handle=2000001 label=NMS_SOUTHBOUND_KEY
handle=2000002 label=NMS_SOUTHBOUND_KEY--cert0
[root@fndblr23 bin]#
```

Note:

If the customer does not remember the password, then decrypt the password that is listed in the cgms.properties file as shown here:

```
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
Passwordexample
[root@fndblr23 ~]#
```

In this case, the decrypted password is Passwordexample

1. NTLS Communication Check:

The HSM client communicates with the HSM server using the well-known port 1792 for NTLS (Network Transport Layer Security) communications, which is in the established state.

To check the status of NTLS communication on the Linux server running the FND server and where the HSM client is installed, use this command:

Note: "**netstat**" has been replaced with the "**ss**" command in Linux

bash

Copy code

```
[root@fndblr23 ~]# ss -natp | grep 1792

ESTAB      0      0         10.106.13.158:46336                 172.27.126.15:1792
users:(("java",pid=11943,fd=317))
```

If the connection is not in the established state, it indicates an issue with basic NTLS communication.

In such cases, advise the customer to log in to their HSM appliance and verify that the NTLS service is running using the "**ntls information show**" command.

Additionally, ensure that the interfaces are enabled for NTLS. You can reset the counters using "ntls information reset" and then issue the "**show**" command again.

On HSM Appliance or HSM Server:

yaml

Copy code

```
[hsmlatest] lunash:>ntls information show

NTLS Information:

Operational Status: 1 (up)

Connected Clients: 1

Links: 1

Successful Client Connections: 20095

Failed Client Connections: 20150

Command Result : 0 (Success)

[hsmlatest] lunash:>
```

1. Luna Safenet Client Identification:

The HSM client, also known as Luna **Safenet** client, can be identified by using the "**./lunacm**" command from the "**/usr/safenet/lunaclient/bin**" location. This command also lists the HSM partition assigned to the client and any configured **High Availability** (HA) Group.

Copy code

```
[root@fndblr23 bin]# ./lunacm

lunacm (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
```

The version of the Luna client installed is indicated here (in this example, version 7.3).

The output also displays information about the available HSMs, including the assigned HSM partitions and HA Group configuration.

mathematica

Copy code

```
Slot Id -> 0

Label -> TEST2

Serial Number -> 1358678309716

Model -> LunaSA 7.4.0

Firmware Version -> 7.4.2

Configuration -> Luna User Partition With SO (PED) Key Export With Cloning Mode
```

Slot Description -> Net Token Slot

Slot Id -> 4

HSM Label -> TEST2Group

HSM Serial Number -> 11358678309716

HSM Model -> LunaVirtual

HSM Firmware Version -> 7.4.2

HSM Configuration -> Luna Virtual HSM (PED) Key Export With Cloning Mode

HSM Status -> N/A - HA Group

Verify that each HSM client is assigned to at least one partition and understand the configurations related to HA Groups for high availability scenarios.

d. To list the HSM servers that are configured with the luna client, use the **./vtl** listServers in the location **/usr/safenet/lunaclient/bin**

```
[root@fndblr23 bin]# ./vtl listServers
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Server: 172.27.126.15
You have new mail in /var/spool/mail/root
[root@fndblr23 bin]#
```

e. If we type **./vtl** and then hit enter in the location **/usr/safenet/lunaclient/bin**, it shows the list of options available with **vtl** command.

./vtl verify lists the HSM physical partitions that are visible to the Luna client.

./vtl listSlots lists all the physical as well as the virtual slots (HA Group) if HAGroup is confgured but disabled.

If HAGroup is configured and enabled, then it shows only the virtual group or the HAGroup information.

```
[root@fndblr23 bin]# ./vtl verify
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

The following Luna SA Slots/Partitions were found:
Slot Serial #        Label
==== =============== =====
-    1358678309716    TEST2

[root@fndblr23 bin]#
[root@fndblr23 bin]# ./vtl listSlots
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Number of slots: 1
The following slots were found:

Slot Description          Label                                Serial #             Status
```

```
==== =================== =============================== ================       ============
0    HA Virtual Card Slot TEST2Group                        11358678309716         Present
[root@fndblr23 bin]#
```

f. To find if HAGroup is enabled or not, we can use the **./vtl listSlots**. If it shows only the HAGroup, and does not show the physical slots, then we know HAGroup is enabled.

Another way to find out if HAGroup is enabled is to issue the **./lunacm from /usr/safenet/lunaclient/bin** and then issue ha l command

The password requested, is the password of the physical partition. In this notice that the only show HA Slots is yes. This means HA is active.

If it is **no**, then although HA is configured, it is not active.

HA can be activated using the command "**ha ha-only enable**" in the lunacm mode.

```
lunacm:>ha l

If you would like to see synchronization data for group TEST2Group,
please enter the password for the group members. Sync info
not available in HA Only mode.

Enter the password: *******

HA auto recovery: disabled
HA recovery mode: activeBasic
Maximum auto recovery retry: 0
Auto recovery poll interval: 60 seconds
HA logging: disabled
Only Show HA Slots: yes

HA Group Label: TEST2Group
HA Group Number: 11358678309716
HA Group Slot ID: 4
Synchronization: enabled
Group Members: 1358678309716
Needs sync: no
Standby Members: <none>

Slot #       Member S/N                MemberLabel     Status
======       ==========                ============    ======
------       1358678309716             TEST2           alive

Command Result : No Error
```

g. Customers have access to HSM servers. Usually HSM servers are hosted in DC and many of them are PED operated.

PED is like a small dongle that displays security token information which is multi factor authentication for additional security, unless the user has both password and the token, then certain access like **admin** or **config** access is not allowed.

The single command that lists all the server information is hsm show

In this output, we can see that the name of the hsm appliance is **hsmlatest**. The **lunash** prompt tells us it is the HSM server.

We can see the HSM software version which is 7.4.0-226. We can see other information like serial number of the appliance, and what is the authentication method, whether it is PED or password, and we can see the total number of partitions on that HSM. Note as we saw earlier that HSM clients are associated with partitions in the appliance.

```
[hsmlatest] lunash:>
[hsmlatest] lunash:>hsm show

Appliance Details:
==================
Software Version: 7.4.0-226

HSM Details:
============
HSM Label: HSMLatest
Serial #: 583548
Firmware: 7.4.2
HSM Model: Luna K7
HSM Part Number: 808-000066-001
Authentication Method: PED keys
HSM Admin login status: Not Logged In
HSM Admin login attempts left: 3 before HSM zeroization!
RPV Initialized: No
Audit Role Initialized: No
Remote Login Initialized: No
Manually Zeroized: No
Secure Transport Mode: No
HSM Tamper State: No tamper(s)

Partitions created on HSM:
==============================
Partition: 1358678309715, Name: Test1
Partition: 1358678309716, Name: TEST2

Number of partitions allowed: 5
Number of partitions created: 2

FIPS 140-2 Operation:
=====================
The HSM is NOT in FIPS 140-2 approved operation mode.

HSM Storage Information:
========================
Maximum HSM Storage Space (Bytes): 16252928
Space In Use (Bytes): 6501170
Free Space Left (Bytes): 9751758

Environmental Information on HSM:
=================================
Battery Voltage: 3.115 V
Battery Warning Threshold Voltage: 2.750 V
System Temp: 39 deg. C
System Temp Warning Threshold: 75 deg. C
```

```
Functionality Module HW: Non-FM
=======================
Command Result : 0 (Success)
[hsmlatest] lunash:>
```

Other useful commands on the HSM server include **partition show** command.

The fields that we must reference are the partition name, the serial number, the partition object count. The partition object count is 2 here.

That is, one object stored in the parititon is the key pair for CSMP message encryption and another object stored is the CSMP certificate.

client list command:

The client we are checking for is listed in the registered client list in the **client list** command.

client show -c <client name> only lists that client information, the hostname, IP address and the partition to which this client is assigned. Successful outputs look like this.

Here, we can look at the partition name, serial number and also the Partition objects. In this case, the partition object = 2, the two objects being the private key and the CSMP certificate.

```
[hsmlatest] lunash:>partition show

Partition Name: Test1
Partition SN: 1358678309715
Partition Label: Test1
Partition SO PIN To Be Changed: no
Partition SO Challenge To Be Changed: no
Partition SO Zeroized: no
Partition SO Login Attempts Left: 10
Crypto Officer PIN To Be Changed: no
Crypto Officer Challenge To Be Changed: no
Crypto Officer Locked Out: no
Crypto Officer Login Attempts Left: 10
Crypto Officer is activated: yes
Crypto User is not initialized.
Legacy Domain Has Been Set: no
Partition Storage Information (Bytes): Total=3240937, Used=1036, Free=3239901
Partition Object Count: 2


Partition Name: TEST2
Partition SN: 1358678309716
Partition Label: TEST2
Partition SO PIN To Be Changed: no
Partition SO Challenge To Be Changed: no
Partition SO Zeroized: no
Partition SO Login Attempts Left: 10
Crypto Officer PIN To Be Changed: no
Crypto Officer Challenge To Be Changed: no
Crypto Officer Locked Out: no
Crypto Officer Login Attempts Left: 10
Crypto Officer is activated: yes
Crypto User is not initialized.
Legacy Domain Has Been Set: no
```

```
Partition Storage Information (Bytes): Total=3240937, Used=1036, Free=3239901
Partition Object Count: 2

Command Result : 0 (Success)
[hsmlatest] lunash:>
[hsmlatest] lunash:>client list

registered client 1: ELKSrv.cisco.com
registered client 2: 172.27.171.16
registered client 3: 10.104.188.188
registered client 4: 10.104.188.195
registered client 5: 172.27.126.209
registered client 6: fndblr23

Command Result : 0 (Success)
[hsmlatest] lunash:>
[hsmlatest] lunash:>client show -c fndblr23

ClientID: fndblr23
IPAddress: 10.106.13.158
Partitions: "TEST2"

Command Result : 0 (Success)
[hsmlatest] lunash:>
```