Hardware Security Modules (HSM)與FND整合的故障排除

目錄

簡介

本文檔介紹Hardware Security Module (HSM)、與現場區域網路(FAN)解決方案的整合，以及常見問題的故障排除。

Hardware Security Module (HSM)

Hardware Security Modules (HSM)有三種形式：裝置、PCI卡和雲產品。大多數部署都選擇裝置版本。

軟體安全模組(SSM)

而軟體安全模組(SSM)則是一種與HSM具有類似用途的軟體套件。它們與FND軟體捆綁在一起，提供了一種簡單的替代方案而不是裝置。

請注意，HSM和SSM都是FND部署中的可選元件，不是必需的。

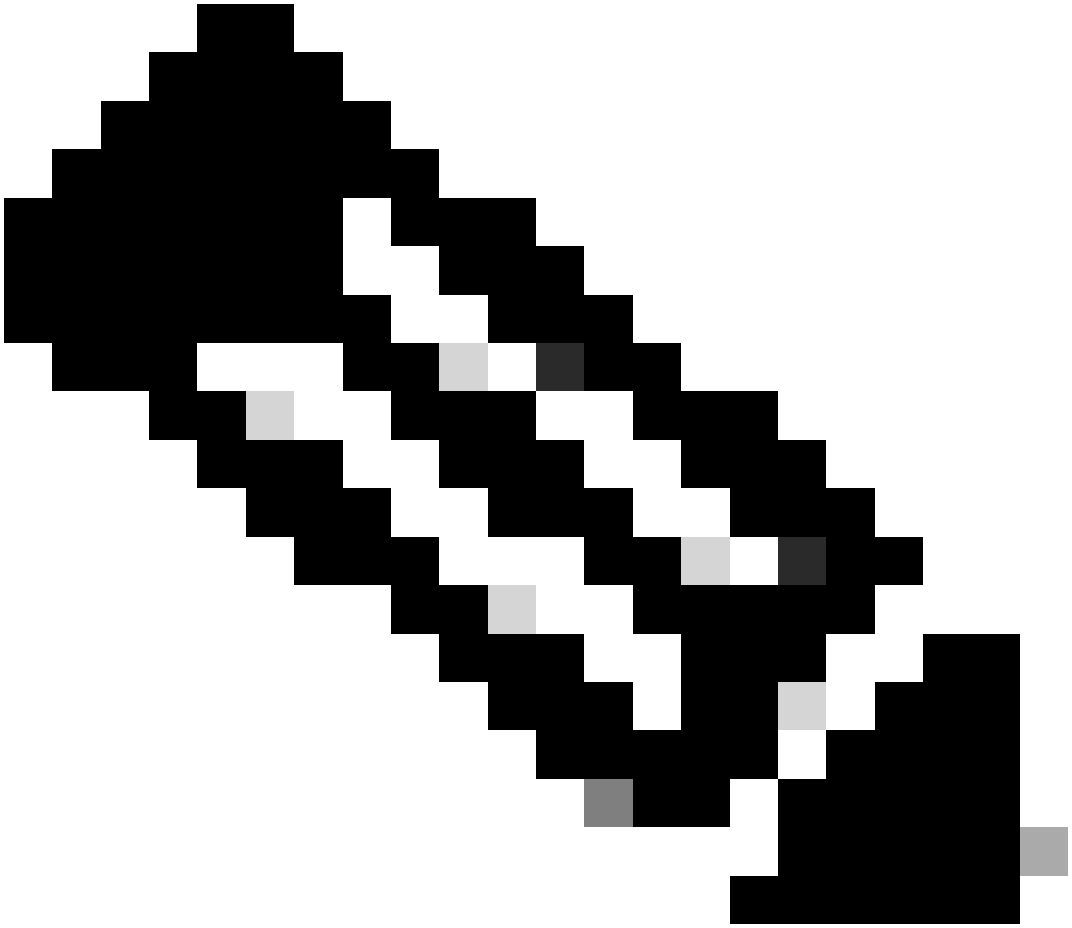
HSM的功能

在FND解決方案中，HSM和SSM的主要功能是安全儲存PKI金鑰對和CSMP證書，特別是在使用儀表等CSMP端點時。

這些金鑰和證書對於加密FND和CSMP終端之間的通訊至關重要。

在部署方面，HSM是獨立裝置，而SSM可以安裝在與FND相同的Linux伺服器上，也可以安裝在單獨的Linux伺服器上。SSM的配置在cgms.properties檔案中指定。

在啟動期間，FND將檢查HSM客戶端庫，而無論HSM相關資訊是否在cgms.properties中指定。如果在解決方案中沒有HSM，則啟動期間與丟失的HSM客戶端庫有關的任何日誌都可能被忽略。



注意：與HSM相關的資訊必須在cgms.properties檔案中指定，該檔案位於不同的目錄中，具體取決於FND是透過OVA還是ISO安裝。

HSM客戶端安裝

HSM客戶端必須安裝在FND伺服器所在的同一Linux伺服器上。客戶可以從Thales網站或透過Cisco支援合約下載HSM客戶端軟體。

FND軟體版本說明中記錄了部署所需的HSM客戶端軟體和HSM軟體。在發行說明的HSM升級表部分中列出了該工具。

HSM客戶端安裝檔案、配置檔案和庫的路徑：

預設安裝位置是/usr/safenet/lunaclient/bin（Cisco IOS軟體）。大多數命令(如lunacm、vtl或ckdemo)都是從此路徑運行的(/usr/safenet/lunaclient/bin)。

配置檔案位於/etc/Chrystoki.conf。

Linux伺服器上的FND伺服器所需的HSM Luna客戶端庫檔案的路徑為/usr/safenet/lunaclient/jsp/lib/。

HSM伺服器

大多數部署都將HSM伺服器用作裝置。

HSM伺服器需要分割槽，而HSM客戶端僅能訪問它們被分配到的特定分割槽。HSM伺服器可以透過PED驗證或密碼驗證。

在密碼身份驗證中，使用者名稱和密碼足以在HSM伺服器中進行配置更改。

但是，PED驗證的HSM是一種多因素驗證方法，其中除了密碼之外，進行更改的人還需要訪問PED金鑰。

PED金鑰的功能類似於轉換器，顯示使用者必須輸入的PIN和密碼以進行任何配置更改。

對於某些命令(如show命令和只讀訪問)，不需要PED金鑰。只有特定配置更改（如建立分割槽）才需要PED金鑰。

每個伺服器分割槽可以分配多個客戶端，所有分配給某個分割槽的客戶端都可以訪問該分割槽內的資料。

HSM伺服器提供多種使用者角色，管理員和加密安全管理人員角色尤其重要。此外，還有分割槽安全管理員的角色。

疑難排解

FND使用HSM客戶端訪問HSM硬體。因此，整合有2個部分。

1. HSM客戶端與HSM伺服器之間的通訊
2. FND到HSM客戶端通訊

兩個部分都需要操作，HSM整合才能成功。

HSM客戶端與HSM伺服器之間的通訊

要確定HSM客戶端是否可以使用單個命令成功讀取儲存在HSM伺服器上的HSM分割槽中的金鑰和證書資訊，請從/usr/safenet/lunaclient/bin位置使用/cmu list命令。

執行此命令會提供指示HSM客戶端是否可以訪問儲存在HSM分割槽中的金鑰和證書的輸出。

請注意，此命令會提示輸入密碼，密碼必須與HSM分割槽的密碼相同。

成功的輸出類似於以下結果：

```
[root@fndblr23 bin]# ./cmu list
憑證管理公用程式（64位元） v7.3.0-165。版權所有(c) 2018 SafeNet。版權所有。

請輸入插槽0中令牌的密碼： *******

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

附註：

如果客戶不記得密碼，請解密列在cgms.properties檔案中的密碼，如下所示：

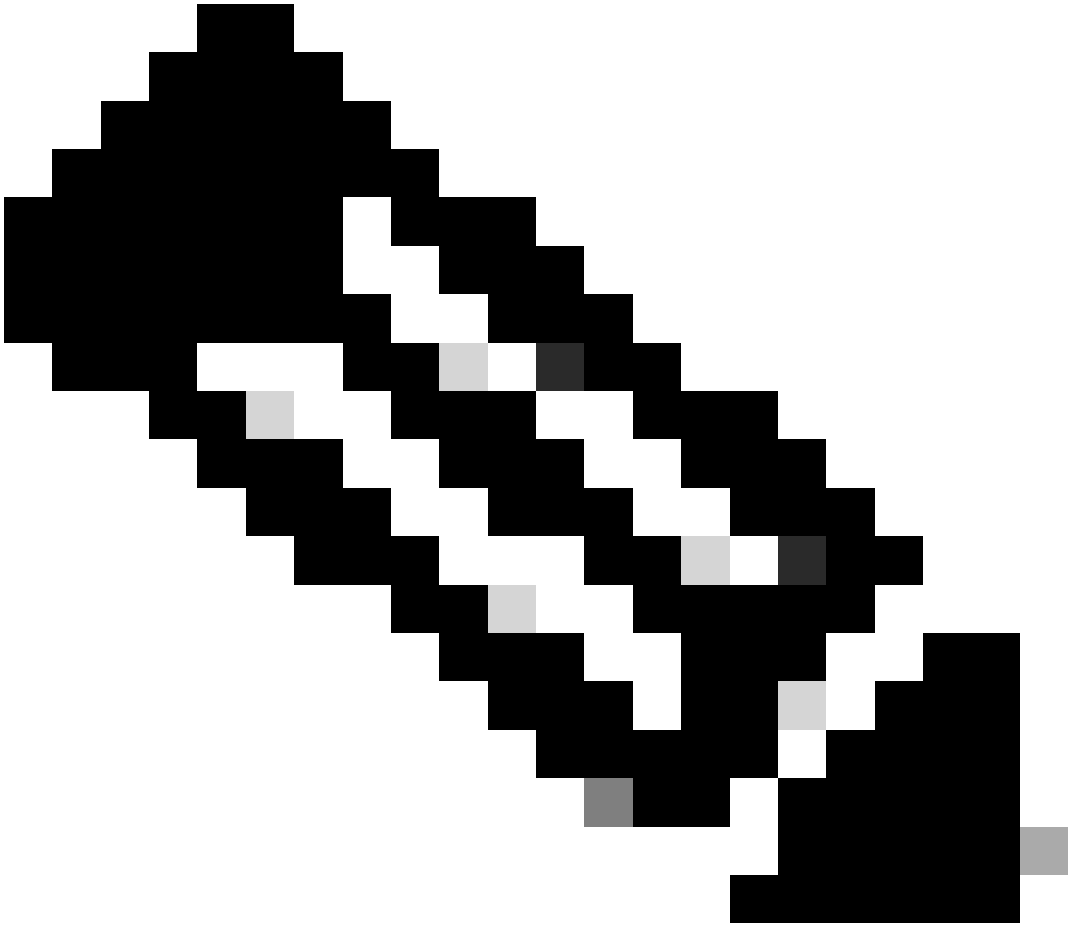
```
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=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

在這種情況下，解密的密碼為Passwordexample

1. NTLS通訊檢查：

HSM客戶端使用公認的NTLS（網路傳輸層安全）通訊埠1792與HSM伺服器通訊，該埠處於已建立狀態。

要檢查運行FND伺服器的Linux伺服器上的NTLS通訊狀態以及HSM客戶端的安裝位置，請使用以下命令：



註：在Linux中，netstat已替換為「ss」命令

bash

複製代碼

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

ESTAB 0 0 10.106.13.158：46336 172.27.126.15:1792使用者：((「java」，pid=11943，fd=317))

如果連線未處於已建立狀態，則表明基本NTLS通訊存在問題。

在這種情況下，建議客戶登入到其HSM裝置，並使用「ntls information show」命令驗證NTLS服務是否正在運行。

此外，請確保為NTLS啟用介面。您可以使用「ntls information reset」重置計數器，然後再次發出「show」命令。

在HSM裝置或HSM伺服器上：

yaml

複製代碼

[hsmlatest] lunash：>ntls資訊顯示

NTLS資訊：

運行狀態：1 (up)

連線的使用者端：1

連結：1

成功的客戶端連線：20095

失敗的客戶端連線： 20150

命令結果：0（成功）

[hsmlatest] lunash：>

1. Luna Safenet客戶端標識：

HSM客戶端(也稱為Luna Safenet客戶端)可透過「/usr/safenet/lunaclient/bin」位置使用「。/lunacm」命令進行標識。此命令還會列出分配給客戶端的HSM分割槽和任何已配置的高可用性(HA)組。

複製代碼

[root@fndblr23 bin]# ./lunacm

lunacm （64位） v7.3.0-165。版權所有(c) 2018 SafeNet。版權所有。

此處指示安裝的Luna客戶端版本（在本例中為7.3版）。

輸出還顯示可用HSM的相關資訊，包括分配的HSM分割槽和HA組配置。

數學運算

複製代碼

插槽Id -> 0

標籤-> TEST2

序列號-> 1358678309716

型號-> LunaSA 7.4.0

韌體版本-> 7.4.2

配置->使用SO (PED)金鑰導出的Luna使用者分割槽（採用克隆模式）

插槽描述->網路令牌插槽

插槽Id -> 4

HSM標籤-> TEST2Group

HSM序列號-> 11358678309716

HSM型號-> LunaVirtual

HSM韌體版本-> 7.4.2

HSM配置-> Luna Virtual HSM (PED)金鑰導出，帶克隆模式

HSM狀態-> N/A - HA組

確保每個HSM客戶端至少分配給一個分割槽，並瞭解高可用性場景下與HA組相關的配置。

d.要列出使用luna客戶端配置的HSM伺服器，請使用/usr/safenet/lunaclient/bin位置中的./vtl listServers

```
[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.如果我們鍵入./vtl，然後點選位置/usr/safenet/lunaclient/bin中的enter鍵，則會顯示vtl命令中可用的選項清單。

./vtl verify列出了Luna客戶端可見的HSM物理分割槽。

./vtl listSlots列出所有物理插槽和虛擬插槽（HA組）（如果已配置但停用HAGroup）。

如果已配置並啟用HAGroup，則它只顯示虛擬組或HAGroup資訊。

```
[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.要查詢HAGroup是否已啟用，我們可以使用./vtl listSlots。 如果它只顯示HAGroup，而不顯示物理插槽，則我們知道HAGroup已啟用。

要知道HAGroup是否已啟用，另一種方法是：從/usr/safenet/lunaclient/bin發出./lunacm，然後發出ha l命令

請求的密碼是物理分割槽的密碼。在此注意事項中，唯一顯示的HA插槽是是。這表示HA處於活動狀態。

如果配置了no，則雖然配置了HA，但它並不處於活動狀態。

在lunacm模式下，可以使用ha ha-only enable命令啟用HA。

```
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.客戶可訪問HSM伺服器。通常HSM伺服器託管在DC中，並且其中很多由PED運行。

PED就像是顯示安全令牌資訊的小轉換器，這是用於提高安全性的多因素身份驗證，除非使用者同時具有密碼和令牌，否則不允許特定訪問(如admin或config)訪問。

列出所有伺服器資訊的單個命令是hsm show

在此輸出中，我們可以看到hsm裝置的名稱為hsmlatest。 lunash 提示符告訴我們它是HSM伺服器。

我們可以看到HSM軟體版本為7.4.0-226。我們可以看到其他資訊，例如裝置的序列號、身份驗證方法是什麼（無論是PED還是密碼），並且我們還可以看到該HSM上的分割槽總數。請注意，如前所述，HSM客戶端與裝置中的分割槽相關聯。

```
[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:>
```

HSM伺服器上的其他有用命令包括partition show命令。

我們必須參照的欄位是分割區名稱、序號、分割區物件計數。此處的分割槽對象計數為2。

也就是說，儲存在協定中的一個對象是CSMP消息加密的金鑰對，而另一個儲存的對象是CSMP證書。

client list命令：

我們正在檢查的客戶端在client list命令的「registered client list」中列出。

client show -c <client name>僅列出該客戶端的資訊、主機名、IP地址以及為其分配該客戶端的分割槽。成功的輸出如下所示。

在此，我們可以檢視分割槽名稱、序列號以及Partition對象。在這種情況下，分割槽對象= 2，兩個對象是私鑰和CSMP證書。

```
[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:>
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。