排除Hardware Security Modules (HSM)与FND集成的故障

目录

简介

本文档介绍Hardware Security Module (HSM)、与现场区域网络(FAN)解决方案的集成，以及常见问题的故障排除。

Hardware Security Module (HSM)

Hardware Security Modules (HSM)有三种形式：设备、PCI卡和云产品。大多数部署选择设备版本。

软件安全模块(SSM)

而软件安全模块(SSM)则是一种用途与HSM类似的软件包。它们与FND软件捆绑在一起，并提供简单的替代方案而不是设备。

请注意，HSM和SSM都是FND部署中的可选组件，不是必需的。

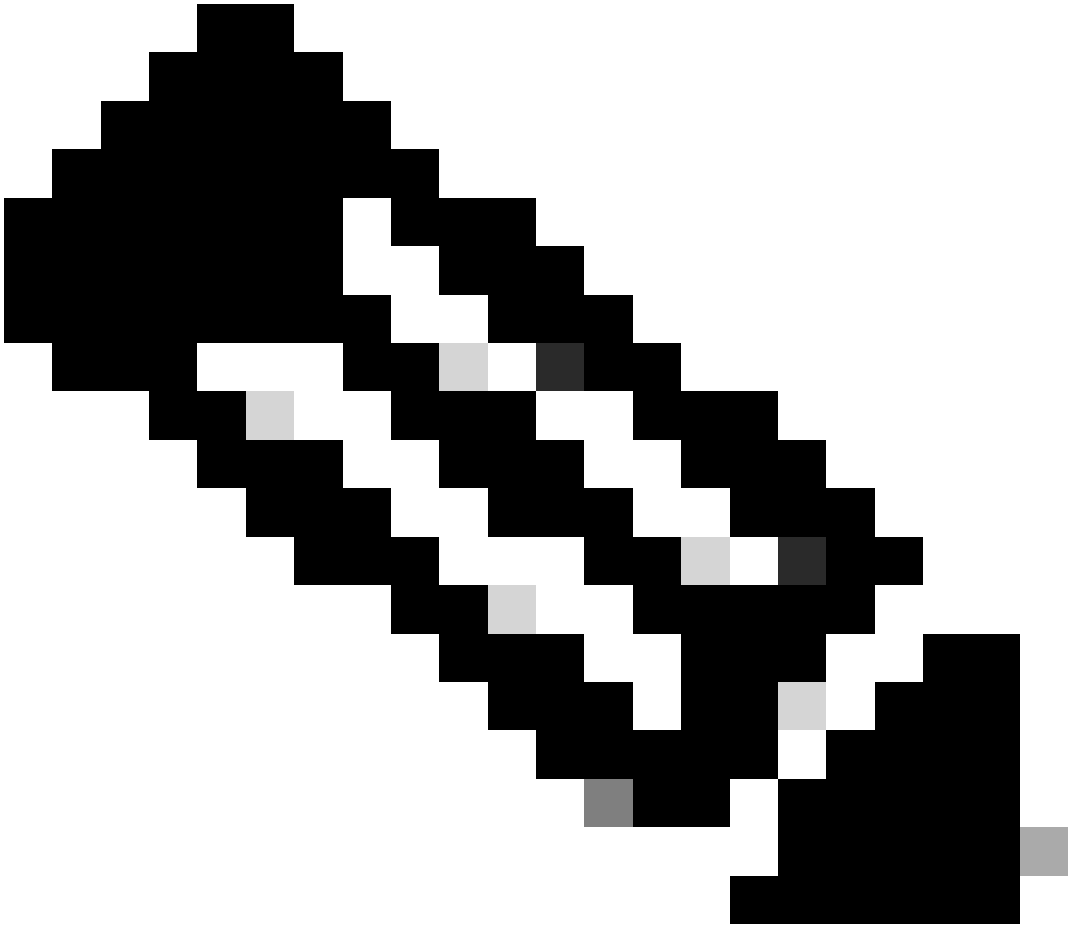
HSM的功能

在FND解决方案中，HSM和SSM的主要功能是安全地存储PKI密钥对和CSMP证书，特别是在使用米表等CSMP终端时。

这些密钥和证书对于加密FND和CSMP终端之间的通信至关重要。

在部署方面，HSM是独立设备，而SSM可以与FND安装在同一Linux服务器上，也可以安装在单独的Linux服务器上。SSM的配置在cgms.properties文件中指定。

启动期间，无论是否在cgms.properties中指定与HSM相关的信息，FND都会检查HSM客户端库。如果HSM未包括在解决方案中，则启动过程中丢失的HSM客户端库相关的任何日志都可被忽略。



注意：必须在cgms.properties文件中指定与HSM相关的信息，该文件位于不同的目录中，具体取决于FND是通过OVA还是ISO安装。

HSM客户端安装

HSM客户端必须安装在FND服务器所在的同一Linux服务器上。客户可以从Thales网站或通过Cisco支持合同下载HSM客户端软件。

FND软件发行版本注释记录了部署所需的HSM客户端软件和HSM软件。它在发行版本注释的HSM升级表部分列出。

HSM客户端安装文件、配置文件和库的路径：

默认安装位置是/usr/safenet/lunaclient/bin。大多数命令(如lunacm、vtl或ckdemo)都是从此路径(/usr/safenet/lunaclient/bin)运行的。

配置文件位于/etc/Chrystoki.conf。

Linux服务器上的FND服务器所需的HSM Luna客户端库文件的路径为/usr/safenet/lunaclient/jsp/lib/。

HSM服务器

大多数部署都使用HSM服务器作为设备。

HSM服务器需要分区，而HSM客户端只能访问它们所分配到的特定分区。HSM服务器可以通过PED验证或密码验证。

在密码验证中，用户名和密码足以应对HSM服务器中的配置更改。

但是，PED身份验证HSM是一种多因素身份验证方法，在该方法中，除密码外，进行更改的人员还需要访问PED密钥。

PED密钥的功能类似于转换器，显示用户必须输入的PIN和密码才能进行配置更改。

对于某些命令(如show命令和只读访问)，不需要PED密钥。只有特定配置更改（如创建分区）才需要PED密钥。

每个服务器分区可以分配多个客户端，并且分配给分区的所有客户端都可以访问该分区内的数据。

HSM服务器提供多种用户角色，管理员和加密安全管理人员这两个角色尤其重要。此外，还有分区安全管理员的角色。

故障排除

基金使用HSM客户端访问HSM硬件。因此，集成有2个部分。

1. HSM客户端到HSM服务器的通信
2. FND到HSM客户端通信

两个部分都需要工作，HSM集成才能成功。

HSM客户端到HSM服务器的通信

要确定HSM客户端是否可以使用单个命令成功读取存储在HSM服务器上的HSM分区中的密钥和证书信息，请从/usr/safenet/lunaclient/bin位置使用/cmu list命令。

执行此命令会提供指示HSM客户端是否可以访问存储在HSM分区中的密钥和证书的输出。

请注意，此命令会提示输入密码，密码必须与HSM分区的密码相同。

成功输出类似于以下结果：

[root@fndblr23 bin]# ./cmu list
证书管理实用程序（64位） v7.3.0-165。版权所有(c) 2018 SafeNet。保留所有权利。

请输入插槽0中令牌的密码：*******

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

注意：

如果客户不记得密码，则解密cgms.properties文件中列出的密码，如下所示：

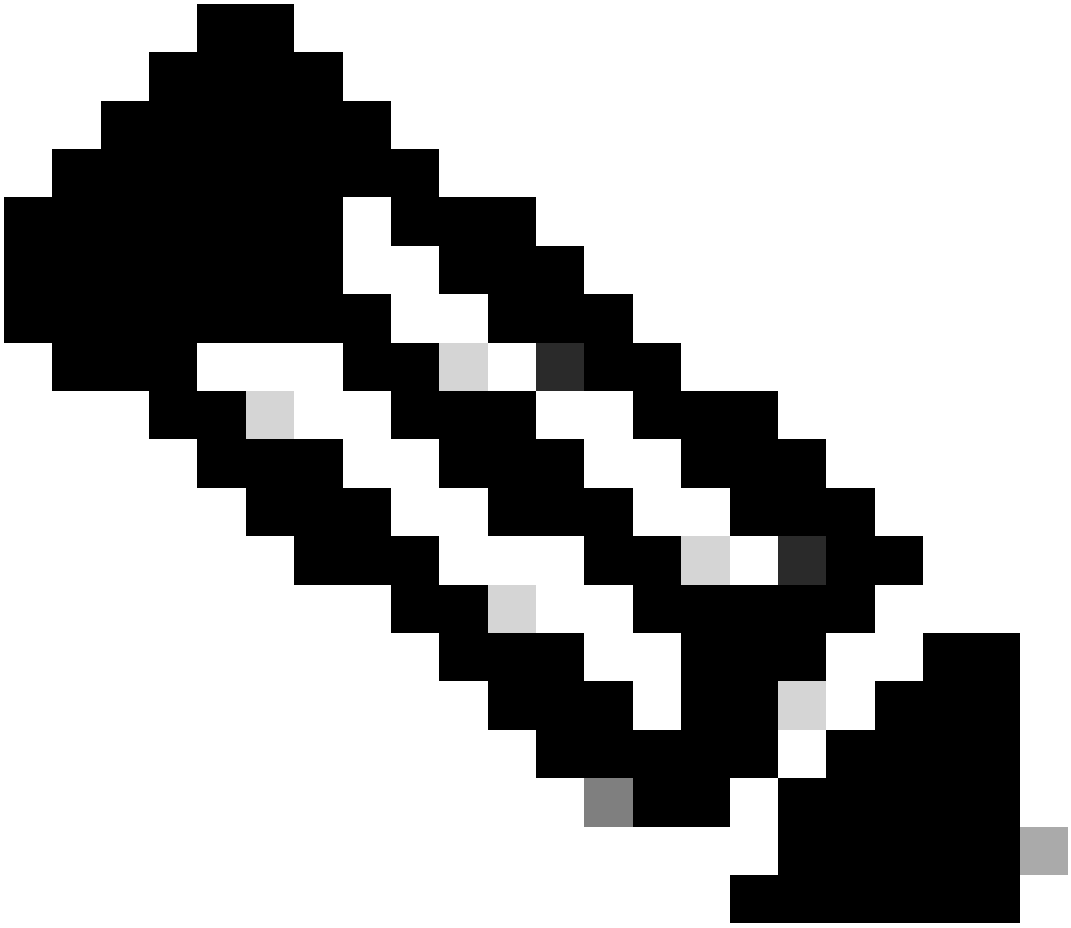
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=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

在这种情况下，解密的密码是Passworexample

1. NTLS通信检查：

HSM客户端使用公认的NTLS（网络传输层安全）通信端口1792与HSM服务器通信，该端口处于已建立状态。

要检查运行FND服务器的Linux服务器上以及HSM客户端的安装位置上的NTLS通信状态，请使用以下命令：



注意：在Linux中，“netstat”已替换为“ss”命令

---

bash

复制代码

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

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

如果连接未处于已建立状态，则表明基本NTLS通信存在问题。

在这种情况下，建议客户登录到其HSM设备，并使用“ntls information show”命令验证NTLS服务正在运行。

此外，请确保为NTLS启用接口。您可以使用“ntls information reset”重置计数器，然后再次发出“show”命令。

在HSM设备或HSM服务器上：

yaml

复制代码

[hsmlatest] lunash：>ntls信息显示

NTLS信息：

运行状态：1 (up)

互联客户端：1

链接：1

成功的客户端连接：20095

失败的客户端连接： 20150

命令结果：0（成功）

[hsmlatest] lunash：>

1. Luna Safenet客户端标识：

HSM客户端也称为Luna Safenet客户端，可通过在/usr/safenet/lunaclient/bin”位置使用“。
/lunacm”命令进行识别。此命令还会列出分配给客户端和任何已配置高可用性(HA)组的HSM分区。

复制代码

[root@fndblr23 bin]# ./lunacm

lunacm （64位） v7.3.0-165。版权所有(c) 2018 SafeNet。保留所有权利。

此处指示安装的Luna客户端的版本（在本例中为7.3版）。

输出还显示可用HSM的信息，包括分配的HSM分区和HA组配置。

mathematica

复制代码

插槽Id -> 0

标签-> TEST2

序列号-> 1358678309716

型号-> LunaSA 7.4.0

固件版本-> 7.4.2

配置-> Luna用户分区SO (PED)密钥导出和克隆模式

Slot Description -> Net Token Slot

插槽Id -> 4

HSM标签-> TEST2Group

HSM序列号-> 11358678309716

HSM型号-> LunaVirtual

HSM固件版本-> 7.4.2

HSM配置-> Luna Virtual HSM (PED)密钥导出和克隆模式

HSM状态->不适用- HA组

确保每个HSM客户端至少分配到一个分区，并了解与高可用性场景的HA组相关的配置。

d.要列出使用luna客户端配置的HSM服务器，请使用位置/usr/safenet/lunaclient/bin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.如果我们键入./vtl，然后在位置/usr/safenet/lunaclient/bin中按enter键，则会显示通过vtl命令可用的选项列表。

./vtl verify列出了Luna客户端可见的HSM物理分区。

./vtl listSlots列出所有物理插槽和虚拟插槽（HA组）（如果已配置但禁用HAGroup）。

如果已配置并启用HAGroup，则它仅显示虚拟组或HAGroup信息。

```
[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.要查找HAGroup是否已启用，我们可以使用./vtl listSlots。 如果它只显示HAGroup，而不显示物理插槽，则我们知道HAGroup已启用。

要知道HAGroup是否已启用，另一种方法是从/usr/safenet/lunaclient/bin发出./lunacm，然后发出hal命令

请求的密码是物理分区的密码。在此通知中，唯一显示的高可用性插槽是是。这表示HA处于活动状态。

如果它为no，则虽然已配置HA，但它不处于活动状态。

在lunacm模式下，可使用ha ha-only enable命令激活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.客户有权访问HSM服务器。通常HSM服务器托管在DC中，其中许多服务器由PED运行。

PED就像一个小型转换器，显示安全令牌信息，这是增加安全性的多重身份验证，除非用户有密码和令牌，否则不允许进行某些访问，如admin或config访问。

列出所有服务器信息的单个命令是hsm show

在此输出中，我们可以看到hsm设备的名称为hsmlatest。 lunash提示符告诉我们它是HSM服务器。

我们可以看到HSM软件版本为7.4.0-226。我们可以看到其他信息，如设备的序列号、身份验证方法是什么（无论是PED还是密码），而且我们可以看到该HSM上的分区总数。请注意，如前所述，HSM客户端与设备中的分区相关联。

```
[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服务器上的其他有用命令包括partition show命令。

我们必须引用的字段是分区名称、序列号和分区对象计数。此处的分区对象计数为2。

也就是说，存储在协议中的一个对象是CSMP消息加密的密钥对，而存储的另一个对象是CSMP证书。

client list命令：

我们正在检查的客户端在client list命令的“registered client list”中列出。

client show -c <client name>仅列出客户端信息、主机名、IP地址以及为此客户端分配的分区。成功的输出如下所示。

在这里，我们可以查看分区名称、序列号以及分区对象。在这种情况下，分区对象= 2，两个对象是私钥和CSMP证书。

```
[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:>
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。