# Resolución de problemas de integración de los módulos de seguridad de hardware (HSM) con FND

## Contenido



## Introducción

Este documento describe el Módulo de seguridad de hardware (HSM), la integración con la solución Red de área de campo (FAN) y la resolución de problemas comunes.

## Módulo de seguridad de hardware (HSM)

Los módulos de seguridad de hardware (HSM) están disponibles de tres formas: dispositivo, tarjeta PCI y oferta de nube. La mayoría de las implementaciones optan por la versión del dispositivo.

## Módulos de seguridad de software (SSM)

Por otro lado, los módulos de seguridad de software (SSM) son paquetes de software que tienen un propósito similar al de HSM. Se incluyen con el software FND y proporcionan una alternativa sencilla en lugar del dispositivo.

Es importante tener en cuenta que tanto HSM como SSM son componentes opcionales en implementaciones FND y no son obligatorios.

## Funciones del HSM

La función principal de HSM y SSM en una solución FND es almacenar de forma segura el par de

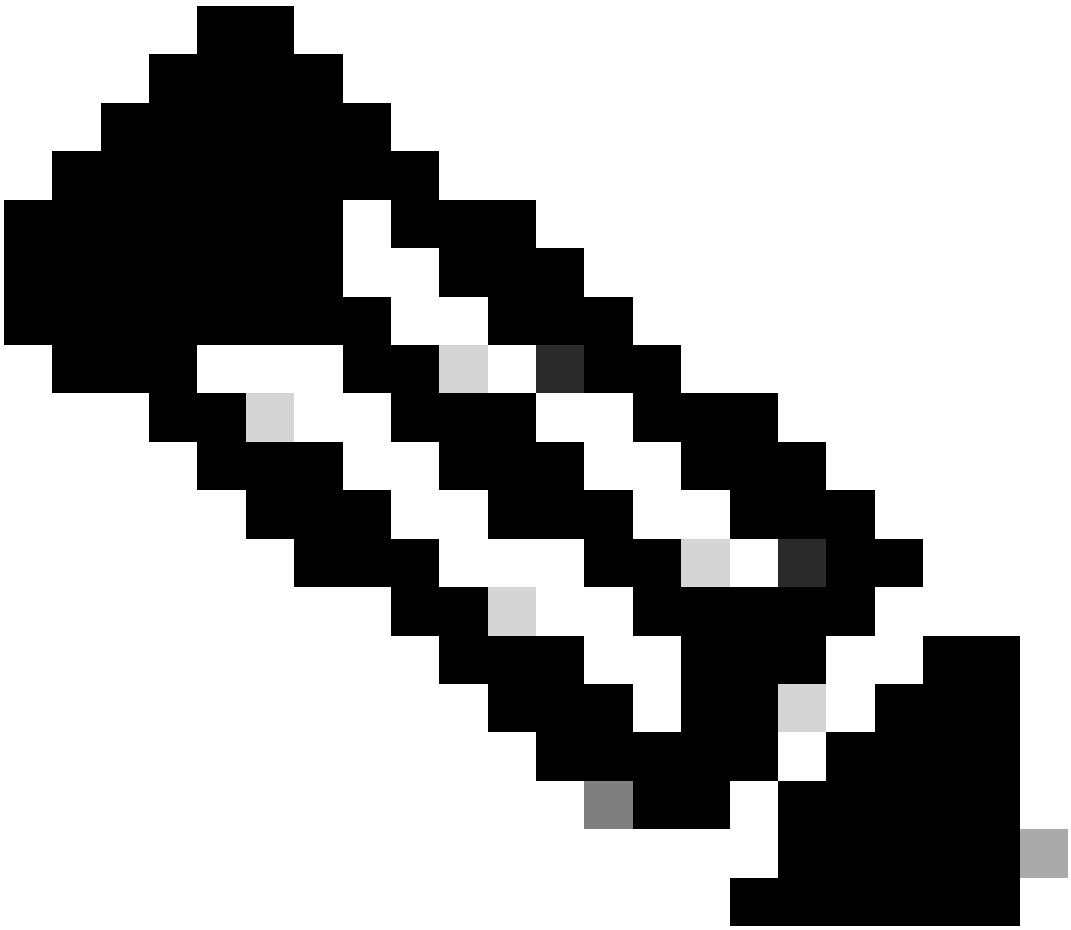
claves PKI y el certificado CSMP, especialmente cuando se utilizan terminales CSMP como medidores.

Estas claves y certificados son esenciales para cifrar la comunicación entre FND y los terminales CSMP.

En cuanto a la implementación, HSM es un dispositivo independiente, mientras que SSM se puede instalar en el mismo servidor Linux que FND o en un servidor Linux independiente. La configuración para SSM se especifica en el archivo cgms.properties.

Durante el arranque, FND comprueba las bibliotecas de clientes HSM, independientemente de si la información relacionada con HSM se especifica en cgms.properties. Cualquier registro perteneciente a bibliotecas de clientes HSM perdidas durante el arranque puede ignorarse si HSM no se incluye en la solución.

---



Nota: la información relacionada con HSM se debe especificar en el archivo cgms.properties, que se encuentra en directorios diferentes en función de si FND se instala mediante OVA o ISO.

---

# Instalación del cliente HSM

El cliente HSM debe estar instalado en el mismo servidor Linux en el que se encuentra el servidor FND. Los clientes pueden descargar el software cliente de HSM desde el sitio web de Thales o a través de un contrato de asistencia de Cisco.

Las notas de la versión del software FND documentan el software necesario en el cliente HSM y el software HSM para la implementación. Aparece en la sección Tabla de actualización de HSM para las notas de la versión.

# Ruta para archivos de instalación, archivos de configuración y bibliotecas del cliente HSM:

La ubicación de instalación predeterminada es /usr/safenet/lunaclient/bin . La mayoría de los comandos, como lunacm, vtl o ckdemo, se ejecutan desde esta ruta (/usr/safenet/lunaclient/bin).

El archivo de configuración se encuentra en /etc/Chrystoki.conf .

La ruta a los archivos de biblioteca de cliente HSM Luna que necesita el servidor FND en los servidores Linux es /usr/safenet/lunaclient/jsp/lib/ .

# Servidor HSM

La mayoría de las implementaciones utilizan el servidor HSM como dispositivo.

Es necesario particionar el servidor HSM y los clientes HSM solo tienen acceso a la partición específica a la que están asignados. El servidor HSM se puede autenticar mediante PED o mediante contraseña.

En la autenticación de contraseña, un nombre de usuario y una contraseña son suficientes para realizar cambios de configuración en el servidor HSM.

Sin embargo, el HSM autenticado por PED es un método de autenticación multifactor en el que, además de una contraseña, la persona que realiza los cambios necesita acceder a una clave PED.

La clave PED funciona como un mecanismo de seguridad, mostrando un PIN que el usuario debe introducir junto con la contraseña para realizar cualquier cambio en la configuración.

Para ciertos comandos como los comandos show y el acceso de sólo lectura, la clave PED no es necesaria. Sólo los cambios de configuración específicos, como la creación de particiones, requieren la clave PED.

Cada partición de servidor puede tener varios clientes asignados y todos los clientes asignados a una partición tienen acceso a los datos de dicha partición.

El servidor HSM ofrece varias funciones de usuario, siendo especialmente importantes las de

administrador y responsable de seguridad criptográfica. Además, existe el papel de oficial de seguridad de la partición.

# Resolución de problemas

FND utiliza el cliente HSM para acceder al hardware HSM. Por lo tanto, la integración consta de dos partes.

1. Comunicación de cliente HSM a servidor HSM
2. Comunicación de cliente FND a HSM

Ambas partes deben funcionar para que la integración de HSM tenga éxito.

## Comunicación de cliente HSM a servidor HSM

Para determinar si el cliente HSM puede leer correctamente la información de clave y certificado almacenada en la partición HSM del servidor HSM mediante un solo comando, utilice el comando /cmu list de la ubicación /usr/safenet/lunaclient/bin.

La ejecución de este comando proporciona una salida que indica si el cliente HSM puede acceder a la clave y al certificado almacenados en la partición HSM.

Tenga en cuenta que este comando solicita una contraseña, que debe ser la misma que la contraseña de la partición HSM.

Una salida exitosa se asemeja a este resultado:

[root@fndblr23 bin]# ./cmu list
Utilidad de administración de certificados (64 bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Todos los derechos reservados.

Introduzca la contraseña para el token en la ranura 0 : *******

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

Nota:

Si el cliente no recuerda la contraseña, descifre la contraseña que aparece en el archivo cgms.properties como se muestra a continuación:

[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=PRUEBA2Grupo
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=

Ejemplo de contraseña
[root@fndblr23 ~]#

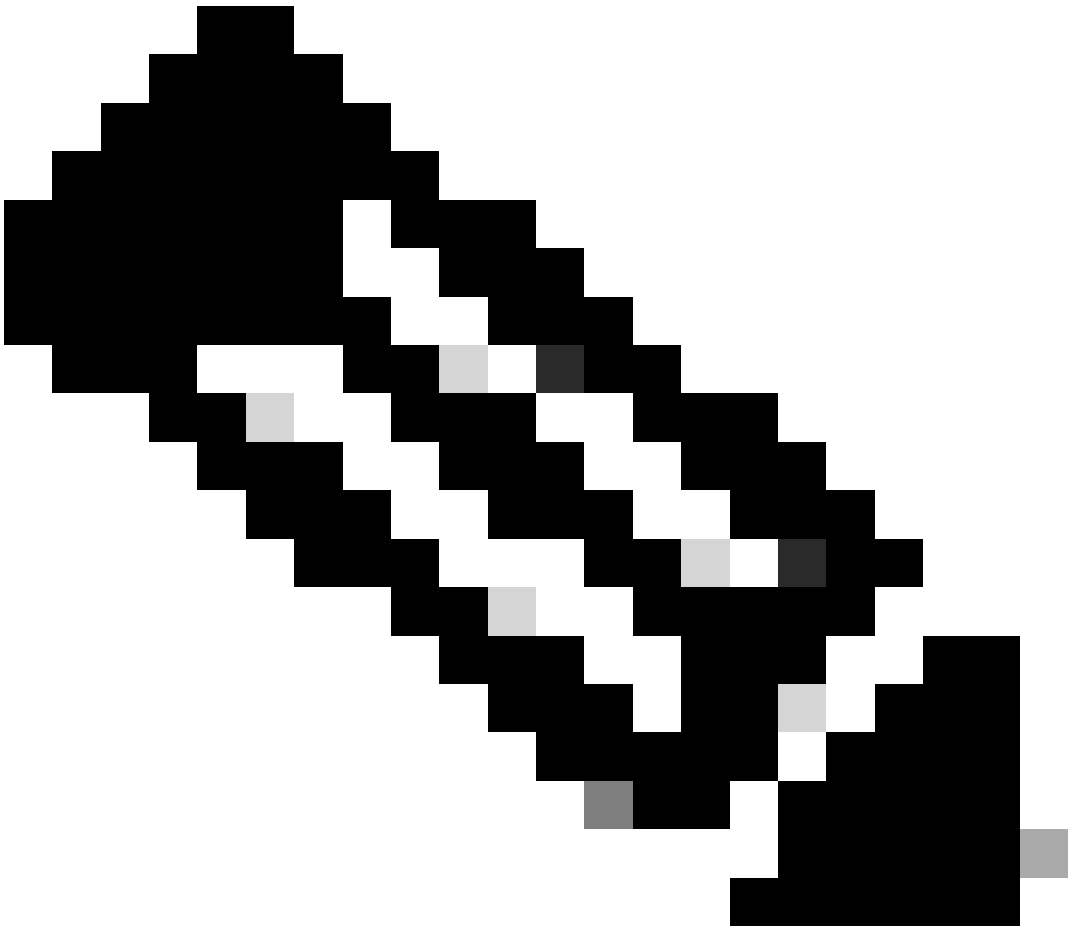
En este caso, la contraseña descifrada es Passwordeexample

1. Comprobación de la comunicación NTLS:

El cliente HSM se comunica con el servidor HSM mediante el conocido puerto 1792 para las comunicaciones NTLS (seguridad de la capa de transporte de red), que se encuentra en el estado establecido.

Para comprobar el estado de la comunicación NTLS en el servidor Linux que ejecuta el servidor FND y en el que está instalado el cliente HSM, utilice este comando:

---



Nota: "netstat" ha sido reemplazado por el comando "ss" en Linux

---

golpear

Copiar código

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

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

Si la conexión no se encuentra en el estado establecido, indica un problema con la comunicación NTLS básica.

En tales casos, aconseje al cliente que inicie sesión en su dispositivo HSM y verifique que el servicio NTLS se esté ejecutando mediante el comando "ntls information show".

Además, asegúrese de que las interfaces estén habilitadas para NTLS. Puede restablecer los contadores mediante "ntls information reset" y luego ejecutar el comando "show" nuevamente.

# En un dispositivo HSM o servidor HSM:

yaml

Copiar código

[hsmlatest] lunash:>ntls information show

Información de NTLS:

Estado operativo: 1 (arriba)

Clientes conectados: 1

Enlaces: 1

Conexiones de cliente correctas: 20095

Conexiones de cliente fallidas: 20150

Resultado del comando: 0 (correcto)

[hsmlatest] lunash:>

1. Identificación del cliente de Luna Safenet:

El cliente HSM, también conocido como cliente Luna Safenet, se puede identificar mediante el comando "./lunacm" desde la ubicación "/usr/safenet/lunaclient/bin". Este comando también enumera la partición HSM asignada al cliente y cualquier grupo de alta disponibilidad (HA) configurado.

Copiar código

[root@fndblr23 bin]# ./lunacm

lunacm (64 bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Todos los derechos reservados.

Aquí se indica la versión del cliente Luna instalado (en este ejemplo, la versión 7.3).

El resultado también muestra información sobre los HSM disponibles, incluidas las particiones HSM asignadas y la configuración del grupo HA.

matemática

Copiar código

ID de ranura -> 0

Etiqueta -> PRUEBA2

Número de serie -> 1358678309716

Modelo -> LunaSA 7.4.0

Versión del firmware -> 7.4.2

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

Descripción de la Ranura -> Net Token Slot

ID de ranura -> 4

Etiqueta HSM -> TEST2Group

Número de serie de HSM -> 11358678309716

Modelo HSM -> LunaVirtual

Versión del firmware de HSM -> 7.4.2

Configuración de HSM -> Exportación de claves Luna Virtual HSM (PED) con modo de clonación

Estado de HSM -> N/A - Grupo HA

Verifique que cada cliente HSM esté asignado a al menos una partición y comprenda las configuraciones relacionadas con los grupos HA para escenarios de alta disponibilidad.

d. Para enumerar los servidores HSM que se configuran con el cliente luna, utilice la lista ./vtl Servers en la ubicación /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. Si escribimos ./vtl y luego presionamos enter en la ubicación /usr/safenet/lunaclient/bin, muestra la lista de opciones disponibles con el comando vtl.

./vtl verify enumera las particiones físicas HSM que son visibles para el cliente Luna.

./vtl listSlots enumera todas las ranuras físicas y virtuales (grupo HA) si HAGroup está configurado pero deshabilitado.

Si HAGroup está configurado y habilitado, solo mostrará la información del grupo virtual o del grupo HAGroup.

```
[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. Para encontrar si HAGroup está habilitado o no, podemos utilizar el ./vtl listSlots. Si muestra solamente el HAGroup, y no muestra las ranuras físicas, entonces sabemos que HAGroup está habilitado.

Otra manera de averiguar si HAGroup está habilitado es ejecutar el comando ./lunacm de /usr/safenet/lunaclient/bin y luego ejecutar el comando ha l

La contraseña solicitada es la contraseña de la partición física. En este aviso que el único show HA Ranuras es sí. Esto significa que HA está activo.

Si es no, aunque ha sido configurado, no está activo.

HA se puede activar usando el comando "ha ha-only enable" en el modo lunacm.

```
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. Los clientes tienen acceso a los servidores HSM. Normalmente, los servidores HSM se alojan en DC y muchos de ellos funcionan con PED.

PED es como un pequeño mecanismo de seguridad que muestra información de token de seguridad que es autenticación de varios factores para seguridad adicional, a menos que el usuario tenga la contraseña y el token, entonces cierto acceso como admin o config no está permitido.

El único comando que enumera toda la información del servidor es hsm show

En esta salida, podemos ver que el nombre del dispositivo hsm es hsmlatest. El mensaje lunash nos dice que es el servidor HSM.

Podemos ver la versión del software HSM 7.4.0-226. Podemos ver otra información como el número de serie del dispositivo y cuál es el método de autenticación, si es PED o contraseña, y podemos ver el número total de particiones en ese HSM. Tenga en cuenta, como hemos visto anteriormente, que los clientes HSM están asociados a particiones en el dispositivo.

```
[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:>
```

Otros comandos útiles en el servidor HSM incluyen el comando partition show.

Los campos a los que debemos hacer referencia son el nombre de la partición, el número de serie y el número de objetos de la partición. El conteo de objetos de partición es 2 aquí.

Es decir, un objeto almacenado en la partición es el par de claves para el cifrado de mensajes CSMP y otro objeto almacenado es el certificado CSMP.

comando client list:

El cliente que estamos comprobando aparece en la lista de clientes registrados en el comando client list.

client show -c <client name> sólo enumera esa información de cliente, el nombre de host, la

dirección IP y la partición a la que está asignado este cliente. Las salidas exitosas se ven así.

Aquí, podemos ver el nombre de la partición, el número de serie y también los objetos Partition. En este caso, el objeto de partición = 2, siendo los dos objetos la clave privada y el certificado CSMP.

```
[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:>
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).