Dépannage de l'intégration des modules matériels de sécurité (HSM) avec FND

Table des matières

Introduction

Ce document décrit le module matériel de sécurité (HSM), l'intégration à la solution de réseau de zone (FAN) et le dépannage des problèmes courants.

Module de sécurité matériel (HSM)

Les modules matériels de sécurité (HSM) sont disponibles sous trois formes : appliance, carte PCI et offre cloud. La plupart des déploiements optent pour la version de l'appliance.

Modules de sécurité logicielle (SSM)

Les modules de sécurité logicielle (SSM), quant à eux, sont des progiciels qui remplissent une fonction similaire à celle du module HSM. Ils sont fournis avec le logiciel FND et constituent une alternative simple à la solution matérielle-logicielle.

Il est important de noter que les modules HSM et SSM sont des composants facultatifs dans les déploiements FND et ne sont pas obligatoires.

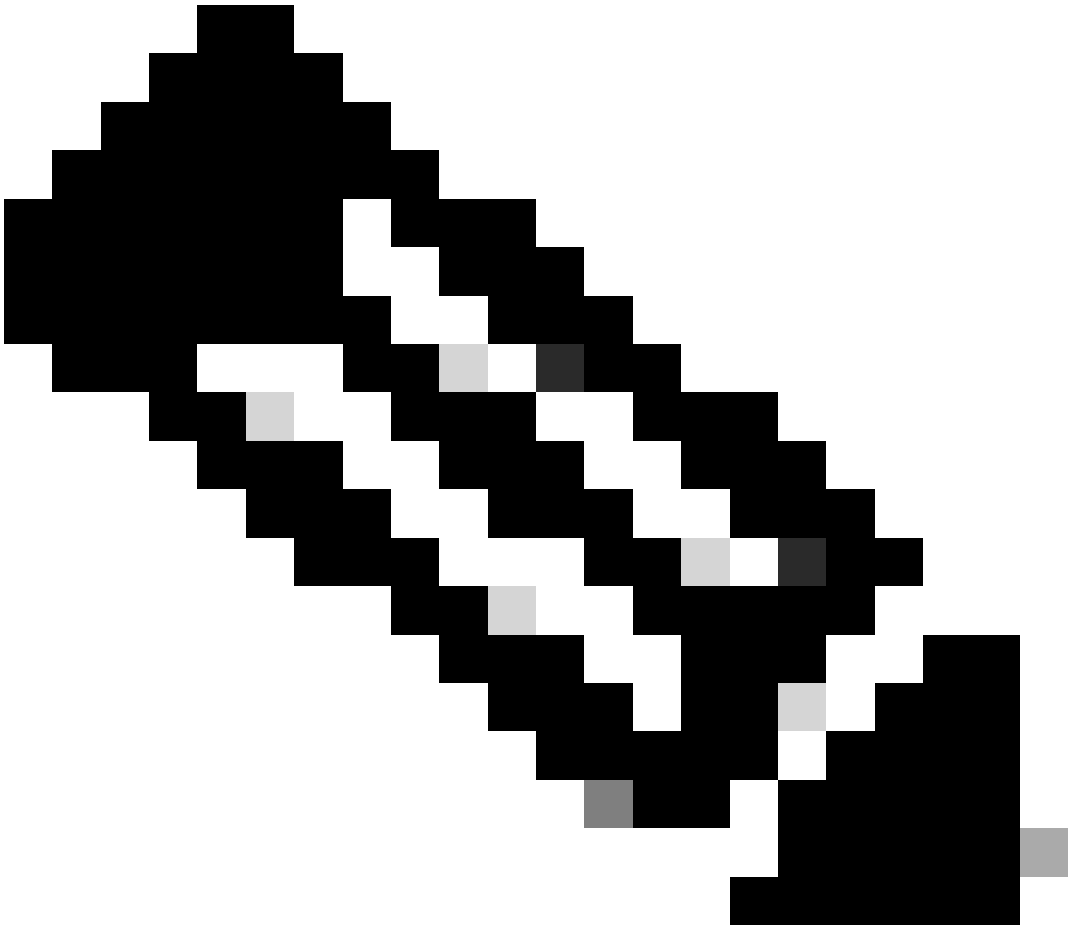
Fonctions du module HSM

La fonction principale des modules HSM et SSM dans une solution FND est de stocker de manière sécurisée la paire de clés PKI et le certificat CSMP, en particulier lorsque des points d'extrémité CSMP tels que des compteurs sont utilisés.

Ces clés et certificats sont essentiels pour chiffrer la communication entre FND et les terminaux CSMP.

En ce qui concerne le déploiement, HSM est une appliance autonome, tandis que SSM peut être installé soit sur le même serveur Linux que FND, soit sur un serveur Linux distinct. La configuration de SSM est spécifiée dans le fichier cgms.properties.

Pendant le démarrage, FND recherche les bibliothèques clientes HSM, que les informations relatives à HSM soient spécifiées ou non dans cgms.properties. Tous les journaux relatifs aux bibliothèques clientes HSM manquantes pendant le démarrage peuvent être ignorés si HSM n'est pas inclus dans la solution.



Remarque : les informations relatives au module HSM doivent être spécifiées dans le fichier cgms.properties, qui se trouve dans des répertoires différents selon que FND est installé via OVA ou ISO.

Installation du client HSM

Le client HSM doit être installé sur le même serveur Linux que le serveur FND. Les clients peuvent télécharger le logiciel client HSM depuis le site Web de Thales ou via un contrat d'assistance Cisco.

Les notes de version du logiciel FND documentent le logiciel requis sur le client HSM et le logiciel HSM pour le déploiement. Il est répertorié dans la section Tableau de mise à niveau HSM pour les notes de version.

Chemin d'accès aux fichiers d'installation, aux fichiers de configuration et aux bibliothèques du client HSM :

L'emplacement d'installation par défaut est /usr/safenet/lunaclient/bin . La plupart des commandes, telles que lunacm, vtl, ou ckdemo, sont exécutées à partir de ce chemin (/usr/safenet/lunaclient/bin).

Le fichier de configuration se trouve à l'adresse /etc/Chrystoki.conf .

Le chemin d'accès aux fichiers de bibliothèque cliente Luna HSM requis par le serveur FND sur les serveurs Linux est /usr/safenet/lunaclient/jsp/lib/ .

Serveur HSM

La plupart des déploiements utilisent le serveur HSM en tant qu'appliance.

Le serveur HSM doit être partitionné et les clients HSM n'ont accès qu'à la partition spécifique à laquelle ils sont affectés. Le serveur HSM peut être authentifié PED ou par mot de passe.

Dans l'authentification par mot de passe, un nom d'utilisateur et un mot de passe sont suffisants pour les modifications de configuration dans le serveur HSM.

Cependant, le module HSM authentifié PED est une méthode d'authentification multifacteur dans laquelle, en plus d'un mot de passe, la personne effectuant des modifications doit avoir accès à une clé PED.

La clé PED fonctionne comme un dongle, affichant un code PIN que l'utilisateur doit entrer avec le mot de passe pour effectuer des modifications de configuration.

Pour certaines commandes telles que les commandes show et l'accès en lecture seule, la touche PED n'est pas nécessaire. Seules des modifications de configuration spécifiques telles que la création de partitions nécessitent la clé PED.

Plusieurs clients peuvent être affectés à chaque partition de serveur, et tous les clients affectés à une partition ont accès aux données de cette partition.

Le serveur HSM offre différents rôles d'utilisateur, les rôles d'administrateur et de responsable de la sécurité cryptographique étant particulièrement importants. En outre, il y a le rôle d'agent de sécurité de partition.

Dépannage

FND utilise le client HSM pour accéder au matériel HSM. Par conséquent, il y a 2 parties à l'intégration.

1. Communication entre le client et le serveur HSM
2. Communication entre FND et HSM client

Les deux parties doivent fonctionner pour que l'intégration HSM réussisse.

Communication entre le client et le serveur HSM

Pour déterminer si le client HSM peut lire avec succès les informations de clé et de certificat stockées dans la partition HSM sur le serveur HSM à l'aide d'une seule commande, utilisez la commande /cmu list de l'emplacement /usr/safenet/lunaclient/bin.

L'exécution de cette commande fournit une sortie indiquant si le client HSM peut accéder à la clé et au certificat stockés dans la partition HSM.

Notez que cette commande vous invite à entrer un mot de passe, qui doit être identique au mot de passe de la partition HSM.

Une sortie réussie ressemble à ce résultat :

[root@fndblr23 bin]# ./cmu list
Utilitaire de gestion des certificats (64 bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Tous droits réservés.

Entrez le mot de passe du jeton dans le logement 0 : *******

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

Remarque :

Si le client ne se souvient pas du mot de passe, déchiffrez le mot de passe répertorié dans le fichier cgms.properties, comme indiqué ici :

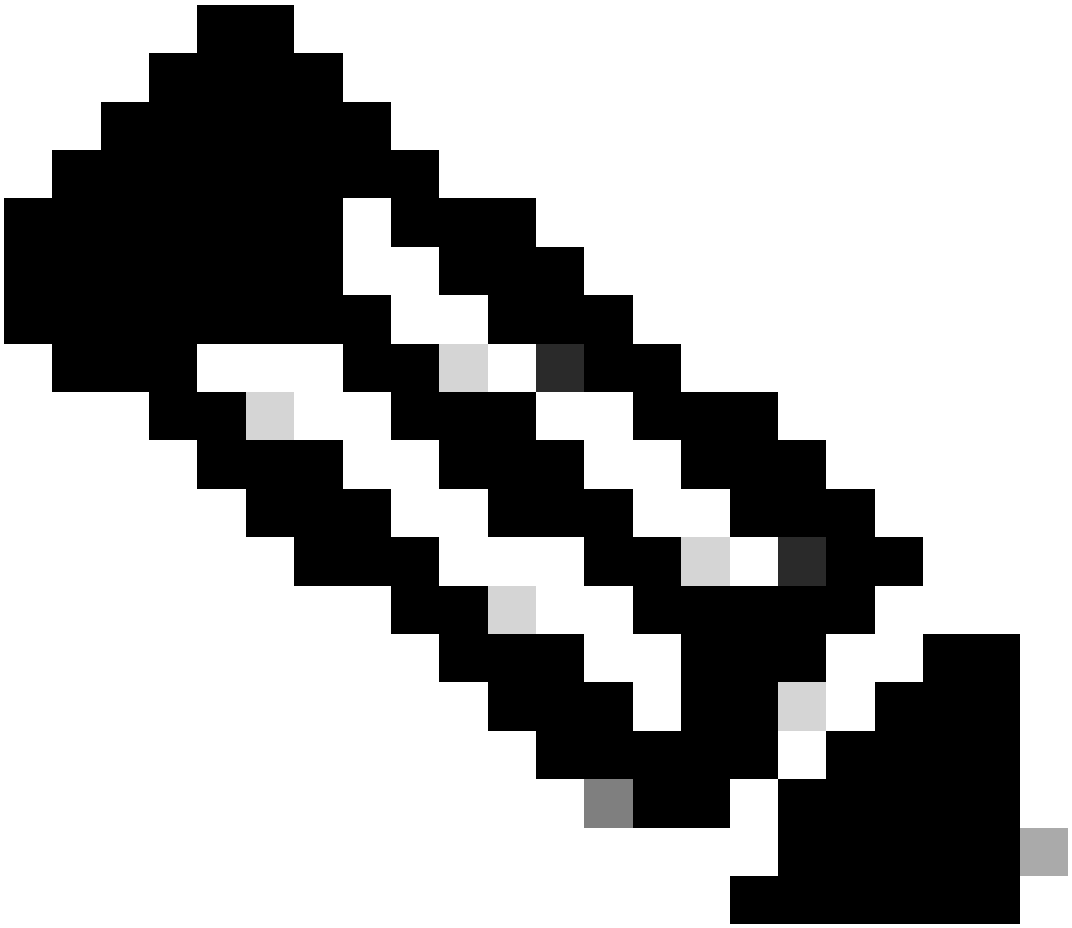
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | hsm grep
hsm-keystore-password=qnBC7WGvZB5ux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Groupe
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
Mot de passe exemple
[root@fndblr23 ~]#

Dans ce cas, le mot de passe déchiffré est Passwordexample

1. Vérification des communications NTLS :

Le client HSM communique avec le serveur HSM à l'aide du port bien connu 1792 pour les communications NTLS (Network Transport Layer Security), qui est dans l'état établi.

Pour vérifier l'état de la communication NTLS sur le serveur Linux exécutant le serveur FND et où le client HSM est installé, utilisez cette commande :



Remarque : "netstat" a été remplacé par la commande "ss" sous Linux

---

coup

Copier le code

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

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

Si la connexion n'est pas à l'état établi, cela indique un problème de communication NTLS de base.

Dans ce cas, conseillez au client de se connecter à son appareil HSM et vérifiez que le service NTLS est en cours d'exécution à l'aide de la commande « ntls information show ».

Assurez-vous également que les interfaces sont activées pour NTLS. Vous pouvez réinitialiser les compteurs à l'aide de la commande « ntls information reset », puis exécuter à nouveau la commande « show ».

Sur l'appliance HSM ou le serveur HSM :

yaml

Copier le code

[hsmlast] lunash:>ntls information show

Informations NTLS :

État opérationnel : 1 (actif)

Clients connectés : 1

Liens : 1

Connexions client réussies : 20095

Connexions client ayant échoué : 20150

Résultat de la commande : 0 (réussite)

[hsmlast] lunash : >

1. Identification du client Luna Safenet :

Le client HSM, également connu sous le nom de client Luna Safenet, peut être identifié à l'aide de la commande "./lunacm" à partir de l'emplacement "/usr/safenet/lunaclient/bin". Cette commande répertorie également la partition HSM attribuée au client et tout groupe haute disponibilité (HA) configuré.

Copier le code

[root@fndblr23 bin]# ./lunacm

lunacm (64 bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Tous droits réservés.

La version du client Luna installé est indiquée ici (dans cet exemple, la version 7.3).

Le résultat affiche également des informations sur les HSM disponibles, y compris les partitions HSM attribuées et la configuration du groupe haute disponibilité.

mathématique

Copier le code

ID de logement -> 0

Libellé -> TEST2

Numéro de série -> 1358678309716

Modèle -> LunaSA 7.4.0

Version du micrologiciel -> 7.4.2

Configuration -> Exportation de la partition utilisateur Luna avec clé SO (PED) en mode clonage

Description du logement -> Logement de jeton réseau

ID de logement -> 4

Libellé HSM -> TEST2Group

Numéro de série HSM -> 11358678309716

Modèle HSM -> LunaVirtual

Version du micrologiciel HSM -> 7.4.2

Configuration HSM -> Exportation de clé Luna Virtual HSM (PED) avec mode de clonage

État HSM -> S/O - Groupe haute disponibilité

Vérifiez que chaque client HSM est attribué à au moins une partition et comprenez les configurations liées aux groupes HA pour les scénarios de haute disponibilité.

d. Pour répertorier les serveurs HSM configurés avec le client luna, utilisez la commande ./vtl listServers dans l'emplacement /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 nous tapons ./vtl et que nous tapons ensuite entrée dans la zone location

/usr/safenet/lunaclient/bin, la liste des options disponibles avec la commande vtl s'affiche.

./vtl verify répertorie les partitions physiques HSM qui sont visibles par le client Luna.

./vtl listSlots répertorie tous les emplacements physiques ainsi que les emplacements virtuels (groupe HA) si HAGroup est configuré mais désactivé.

Si HAGroup est configuré et activé, il affiche uniquement le groupe virtuel ou les informations 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. Pour savoir si HAGroup est activé ou non, nous pouvons utiliser le ./vtl listSlots. S'il affiche uniquement le groupe HAGroup et n'affiche pas les emplacements physiques, nous savons que le groupe HAGroup est activé.

Une autre façon de savoir si HAGroup est activé est d'émettre la commande ./lunacm à partir de /usr/safenet/lunaclient/bin puis d'émettre la commande ha l

Le mot de passe demandé est le mot de passe de la partition physique. Dans cet avis, la seule option show HA Slots est yes. Cela signifie que HA est actif.

Si ce n'est pas le cas, bien que la haute disponibilité soit configurée, elle n'est pas active.

HA peut être activé en utilisant la commande "ha ha-only enable" en mode 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. Les clients ont accès aux serveurs HSM. En général, les serveurs HSM sont hébergés dans un data center et bon nombre d'entre eux sont exploités par PED.

PED est comme un petit dongle qui affiche des informations de jeton de sécurité qui est l'authentification multifacteur pour une sécurité supplémentaire, à moins que l'utilisateur ait à la fois le mot de passe et le jeton, alors certains accès comme admin ou config access n'est pas autorisé.

La commande unique qui répertorie toutes les informations du serveur est hsm show

Dans ce résultat, nous pouvons voir que le nom de l'appliance hsm est hsmlast. L'invite lunash nous indique qu'il s'agit du serveur HSM.

Nous pouvons voir la version du logiciel HSM qui est 7.4.0-226. Nous pouvons voir d'autres informations comme le numéro de série de l'appliance, et quelle est la méthode d'authentification, si c'est PED ou mot de passe, et nous pouvons voir le nombre total de partitions sur ce HSM. Comme nous l'avons vu précédemment, les clients HSM sont associés à des partitions dans l'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:>
```

D'autres commandes utiles sur le serveur HSM incluent la commande partition show.

Les champs que nous devons référencer sont le nom de la partition, le numéro de série, le nombre d'objets de la partition. Le nombre d'objets de partition est ici égal à 2.

En d'autres termes, un objet stocké dans la partition est la paire de clés pour le cryptage des messages CSMP et un autre objet stocké est le certificat CSMP.

commande client list :

Le client que nous recherchons est répertorié dans la liste des clients enregistrés dans la commande client list.

client show -c <nom du client> répertorie uniquement les informations du client, le nom d’hôte,

l'adresse IP et la partition à laquelle ce client est affecté. Les résultats positifs ressemblent à ceci.

Ici, nous pouvons regarder le nom de la partition, le numéro de série et aussi les objets Partition. Dans ce cas, l'objet partition = 2, les deux objets étant la clé privée et le certificat 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:>
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.