Risoluzione dei problemi di integrazione dei moduli di sicurezza hardware (HSM) con FND

Sommario

Introduzione

Modulo di sicurezza hardware (HSM)

Moduli di sicurezza software (SSM)

Funzioni dell'HSM

Installazione del client HSM

Percorso file di installazione, file di configurazione e librerie del client HSM:

Server HSM

Risoluzione dei problemi

- Comunicazione tra il client HSM e il server HSM

Sull'accessorio HSM o sul server HSM:

Introduzione

Questo documento descrive il Modulo di sicurezza hardware (HSM), l'integrazione con la soluzione Field Area Network (FAN) e la risoluzione dei problemi comuni.

Modulo di sicurezza hardware (HSM)

I moduli di sicurezza hardware (HSM) sono disponibili in tre forme: appliance, scheda PCI e offerta cloud. La maggior parte delle installazioni opta per la versione dell'accessorio.

Moduli di sicurezza software (SSM)

I moduli di sicurezza software (SSM), d'altra parte, sono pacchetti software che hanno uno scopo simile a quello di HSM. Sono forniti in bundle con il software FND e forniscono una semplice alternativa al dispositivo.

È importante notare che sia HSM che SSM sono componenti facoltativi nelle distribuzioni FND e non sono obbligatori.

Funzioni dell'HSM

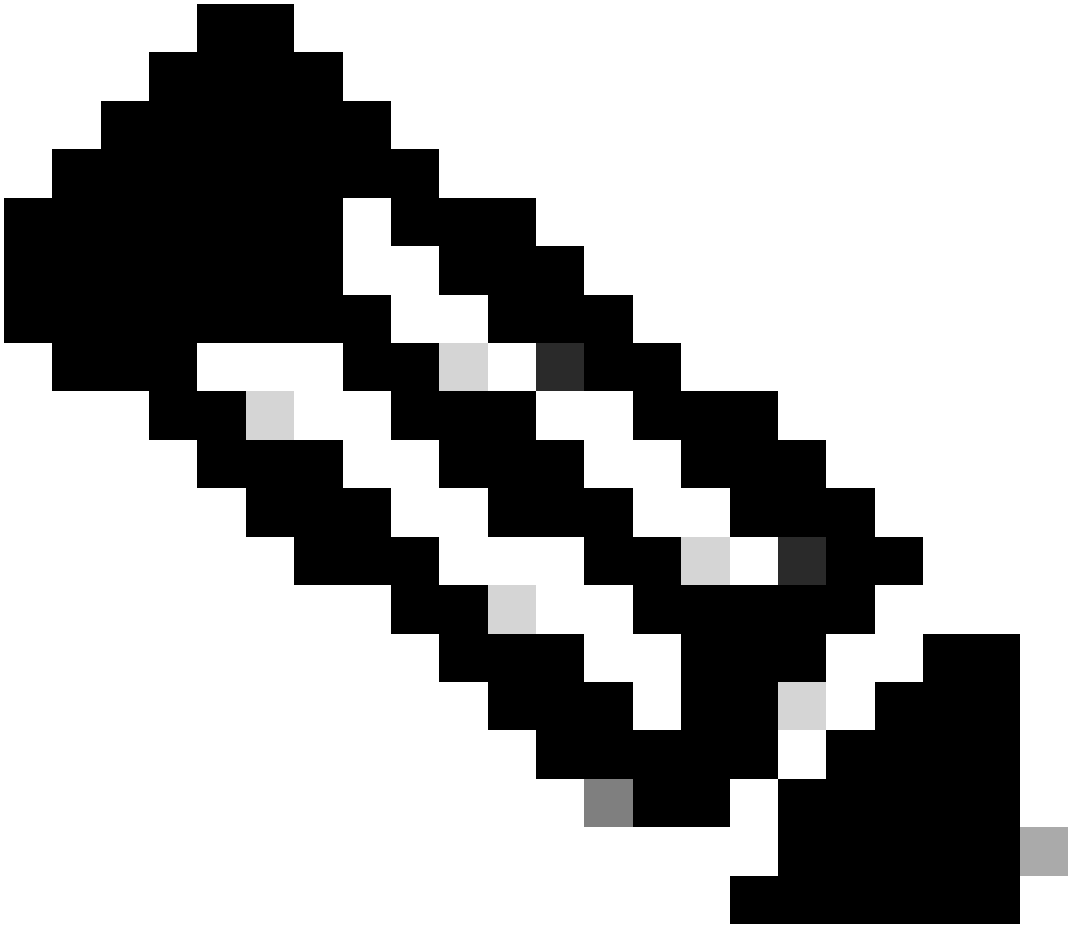
La funzione principale di HSM e SSM in una soluzione FND è quella di archiviare in modo sicuro la coppia di chiavi PKI e il certificato CSMP, in particolare quando vengono utilizzati endpoint CSMP come i contatori.

Queste chiavi e questi certificati sono essenziali per crittografare la comunicazione tra FND e gli

endpoint CSMP.

Per quanto riguarda l'installazione, HSM è un'appliance standalone, mentre SSM può essere installato sullo stesso server Linux di FND o su un server Linux separato. La configurazione per SSM è specificata nel file cgms.properties.

Durante l'avvio, FND controlla le librerie client HSM, indipendentemente dal fatto che le informazioni relative a HSM siano specificate in cgms.properties. Se HSM non è incluso nella soluzione, è possibile ignorare tutti i registri relativi alle librerie client HSM mancanti durante l'avvio.



> Nota: le informazioni relative a HSM devono essere specificate nel file cgms.properties, che si trova in directory diverse a seconda che FND sia installato tramite OVA o ISO.

Installazione del client HSM

Il client HSM deve essere installato sullo stesso server Linux in cui si trova il server FND. I clienti

possono scaricare il software client HSM dal sito Web Thales o tramite un contratto di assistenza Cisco.

Le note di rilascio del software FND documentano il software richiesto sul client HSM e il software HSM per l'installazione. È elencato nella sezione HSM Upgrade Table delle note sulla versione.

Percorso file di installazione, file di configurazione e librerie del client HSM:

Il percorso di installazione predefinito è /usr/safenet/lunaclient/bin. La maggior parte dei comandi, ad esempio lunacm, vtl o ckdemo, viene eseguita da questo percorso (/usr/safenet/lunaclient/bin).

Il file di configurazione si trova in /etc/Chrystoki.conf .

Il percorso dei file della libreria client HSM Luna richiesto dal server FND sui server Linux è /usr/safenet/lunaclient/jsp/lib/ .

Server HSM

La maggior parte delle implementazioni utilizza il server HSM come appliance.

Il server HSM deve essere partizionato e i client HSM hanno accesso solo alla partizione specifica a cui sono assegnati. Il server HSM può essere autenticato tramite il comando PED o tramite l'autenticazione tramite password.

Nell'autenticazione tramite password, un nome utente e una password sono sufficienti per le modifiche alla configurazione nel server HSM.

Tuttavia, l'HSM autenticato PED è un metodo di autenticazione a più fattori in cui, oltre a una password, l'utente che apporta le modifiche deve accedere a una chiave PED.

Il tasto PED funziona come un dongle e visualizza un PIN che l'utente deve immettere insieme alla password per apportare modifiche alla configurazione.

Per alcuni comandi, ad esempio i comandi show e l'accesso in sola lettura, non è necessario utilizzare il tasto PED. La chiave PED è necessaria solo per le modifiche di configurazione specifiche, ad esempio la creazione di partizioni.

A ogni partizione server possono essere assegnati più client e tutti i client assegnati a una partizione hanno accesso ai dati all'interno di tale partizione.

Il server HSM offre diversi ruoli utente, con i ruoli di amministratore e Crypto Security Officer particolarmente importanti. Inoltre, esiste il ruolo di responsabile della sicurezza delle partizioni.

Risoluzione dei problemi

FND utilizza il client HSM per accedere all'hardware HSM. L'integrazione si compone quindi di due

parti.

1. Comunicazione tra il client HSM e il server HSM
2. Comunicazione tra FND e client HSM

Entrambe le parti devono lavorare per il successo dell'integrazione HSM.

Comunicazione tra il client HSM e il server HSM

Per determinare se il client HSM è in grado di leggere correttamente le informazioni relative alla chiave e al certificato archiviate nella partizione HSM sul server HSM utilizzando un unico comando, utilizzare il comando /cmu list dalla posizione /usr/safenet/lunaclient/bin.

L'esecuzione di questo comando fornisce un output che indica se il client HSM può accedere alla chiave e al certificato archiviati nella partizione HSM.

Questo comando richiede una password, che deve essere uguale alla password della partizione HSM.

Un output corretto è simile al risultato seguente:

```
[root@fndblr23 bin]# ./cmu list
Certificate Management Utility (64 bit) v7.3.0-165. Copyright (c) 2018 SafeNet. Tutti i diritti sono riservati.

Immettere la password per il token nello slot 0 : *******

handle=2000001 label=NMS_SOUTHBOUND_KEY
handle=200002 label=NMS_SOUTHBOUND_KEY—cert0
[root@fndblr23 bin]#
```

Nota:

Se il cliente non ricorda la password, decrittografare la password elencata nel file cgms.properties come mostrato di seguito:

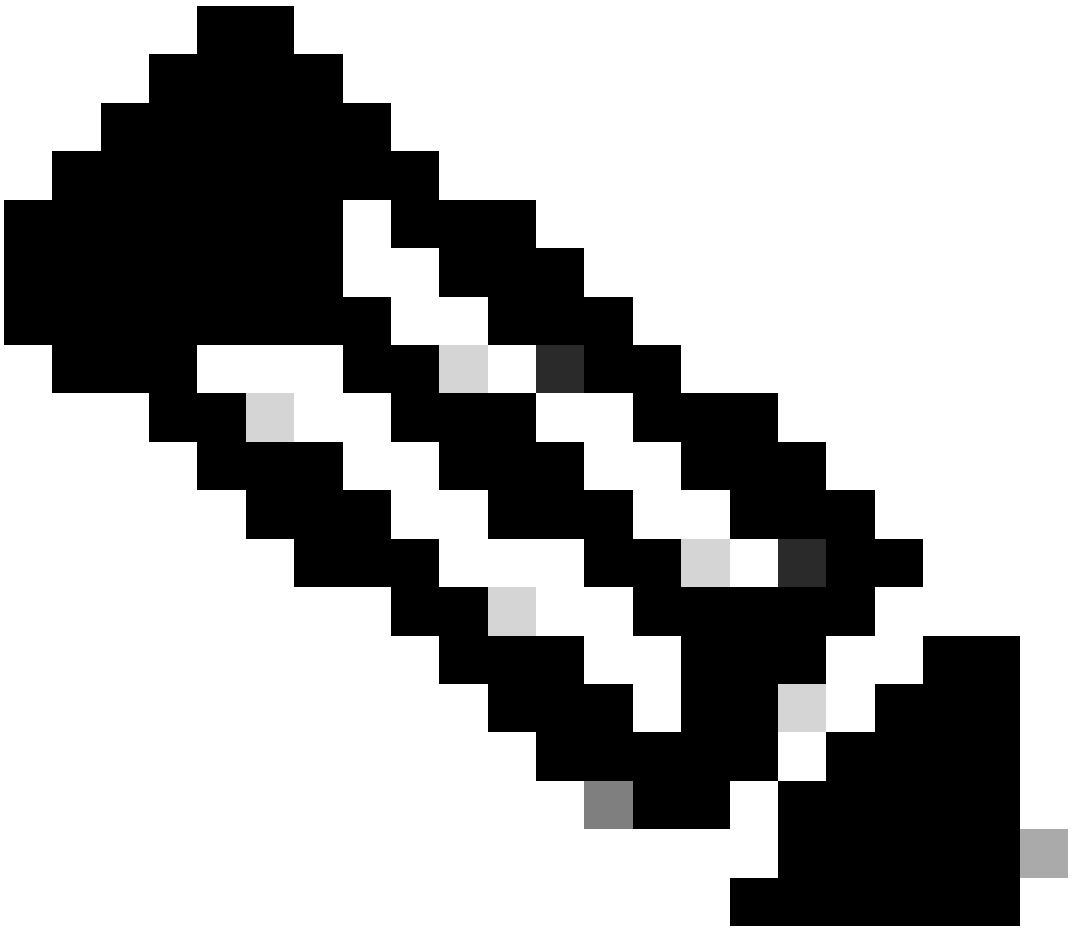
```
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrittografare qnBC7WGvZB5iux4BnnDplTWzcmAxhuISQLmVRXtHBeBWF4=
Esempio di password
[root@fndblr23 ~]#
```

In questo caso, la password decrittografata è Passwordexample

1. Controllo comunicazione NTLS:

Il client HSM comunica con il server HSM utilizzando la nota porta 1792 per le comunicazioni NTLS (Network Transport Layer Security), che si trova nello stato stabilito.

Per controllare lo stato della comunicazione NTLS sul server Linux su cui è in esecuzione il server FND e dove è installato il client HSM, utilizzare questo comando:



Nota: "netstat" è stato sostituito dal comando "ss" in Linux

---

sbattere

Copia codice

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

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

Se la connessione non è nello stato stabilito, indica un problema con la comunicazione NTLS di base.

In questi casi, consigliare al cliente di accedere al proprio accessorio HSM e verificare che il servizio NTLS sia in esecuzione utilizzando il comando "ntls information show".

Verificare inoltre che le interfacce siano abilitate per NTLS. È possibile ripristinare i contatori usando "reimpostazione informazioni ntls" e poi usare di nuovo il comando "show".

Sull'accessorio HSM o sul server HSM:

yaml

Copia codice

[hsmlast] lunash:>informazioni ntls

Informazioni NTLS:

Stato operativo: 1 (attivo)

Client connessi: 1

Collegamenti: 1

Connessioni client riuscite: 20095

Connessioni client non riuscite: 20150

Risultato comando: 0 (riuscito)

[hsmlast] lunash:>

1. Identificazione client Luna Safenet:

Il client HSM, noto anche come client Luna Safenet, può essere identificato utilizzando il comando "./lunacm" dalla posizione "/usr/safenet/lunaclient/bin". Con questo comando vengono inoltre elencate la partizione HSM assegnata al client e qualsiasi gruppo ad alta disponibilità (HA) configurato.

Copia codice

[root@fndblr23 bin]# ./lunacm

lunacm (64 bit) v7.3.0-165. Copyright (c) 2018 SafeNet. Tutti i diritti sono riservati.

La versione del client Luna installato è indicata qui (in questo esempio, versione 7.3).

Nell'output vengono inoltre visualizzate informazioni sugli HSM disponibili, incluse le partizioni HSM assegnate e la configurazione del gruppo HA.

matematica

Copia codice

ID slot -> 0

Etichetta -> TEST2

Numero di serie -> 1358678309716

Modello -> LunaSA 7.4.0

Versione firmware -> 7.4.2

Configurazione -> Partizione utente Luna con chiave SO (PED) Esportazione con modalità di clonazione

Descrizione slot -> slot token di rete

ID slot -> 4

Etichetta HSM -> TEST2Group

Numero di serie HSM -> 11358678309716

Modello HSM -> LunaVirtual

Versione firmware HSM -> 7.4.2

Configurazione HSM -> Esportazione chiave Luna Virtual HSM (PED) con modalità di clonazione

Stato HSM -> N/D - Gruppo HA

Verificare che ogni client HSM sia assegnato ad almeno una partizione e comprendere le configurazioni relative ai gruppi HA per scenari di elevata disponibilità.

d. Per elencare i server HSM configurati con il client luna, utilizzare il comando ./vtl listServers nel percorso /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. Se si digita ./vtl e quindi si preme invio in the location /usr/safenet/lunaclient/bin, viene visualizzato l'elenco di opzioni disponibili con il comando vtl.

./vtl verify elenca le partizioni fisiche HSM visibili al client Luna.

./vtl listSlots elenca tutti gli slot fisici e virtuali (gruppo HA) se HAGroup è configurato ma disabilitato.

Se HAGroup è configurato e abilitato, vengono visualizzate solo le informazioni sul gruppo virtuale o sul gruppo 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. Per verificare se HAGroup è abilitato o meno, è possibile utilizzare ./vtl listSlots. Se mostra solo il gruppo di HAG, e non mostra gli slot fisici, allora sappiamo che il gruppo di HAG è abilitato.

Un altro modo per scoprire se HAGroup è abilitato è usare il comando ./lunacm da /usr/safenet/lunaclient/bin e quindi eseguire il comando ha l

La password richiesta è la password della partizione fisica. In questo avviso, l'unica visualizzazione degli slot HA è sì. Ciò significa che HA è attivo.

Se è no, ha è configurato ma non è attivo.

Ha può essere attivato usando il comando "ha ha-only enable" nella modalità 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. I clienti hanno accesso ai server HSM. Di solito i server HSM sono ospitati in DC e molti di loro sono operati da PED.

Il PED è simile a un piccolo dongle che visualizza le informazioni sul token di sicurezza, ossia l'autenticazione a più fattori per una maggiore sicurezza, a meno che l'utente non abbia sia la password che il token, un accesso sicuro come l'accesso admin o config non è consentito.

Il comando singolo che elenca tutte le informazioni sul server è hsm show

In questo output è indicato che il nome dell'accessorio hsm è hsmlast. Il prompt lunash ci dice che è il server HSM.

È possibile vedere la versione del software HSM 7.4.0-226. È possibile visualizzare altre informazioni, ad esempio il numero di serie dell'accessorio e il metodo di autenticazione, se si tratta di un PED o di una password, nonché il numero totale di partizioni su tale modulo di sicurezza hardware. Si noti che i client HSM sono associati alle partizioni nell'accessorio.

```
[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:>
```

Altri comandi utili sul server HSM includono il comando partition show.

I campi a cui fare riferimento sono il nome della partizione, il numero di serie e il conteggio degli oggetti della partizione. Il conteggio degli oggetti di partizione è 2 qui.

In altre parole, un oggetto archiviato nella partizione è la coppia di chiavi per la crittografia dei messaggi CSMP e un altro oggetto archiviato è il certificato CSMP.

comando elenco client:

Il client che si sta verificando è elencato nell'elenco dei client registrati nel comando client list.

client show -c <nome client> elenca solo le informazioni sul client, il nome host, l'indirizzo IP e la partizione a cui è assegnato il client. Gli output di successo sono simili a quelli riportati di seguito.

Qui è possibile esaminare il nome della partizione, il numero di serie e gli oggetti Partition. In questo caso, l'oggetto partizione = 2, dove i due oggetti sono la chiave privata e il certificato 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:>
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).