Fehlerbehebung: Integration von Hardware-Sicherheitsmodulen (HSM) in FND

Inhalt

Einleitung

Hardware-Sicherheitsmodul (HSM)

Software-Sicherheitsmodule (SSM)

Funktionen des HSM

Installation des HSM-Clients

Pfad für HSM-Client-Installationsdateien, Konfigurationsdateien und Bibliotheken:

HSM-Server

Fehlerbehebung

- Kommunikation zwischen HSM-Client und HSM-Server

Auf HSM-Appliance oder HSM-Server:

Einleitung

In diesem Dokument werden das Hardware Security Module (HSM), die Integration mit Field Area Network (FAN) und die Behebung gängiger Probleme beschrieben.

Hardware-Sicherheitsmodul (HSM)

Hardware Security Modules (HSM) sind in drei Formen erhältlich: Appliance, PCI-Karte und Cloud-Angebot. Die meisten Bereitstellungen entscheiden sich für die Appliance-Version.

Software-Sicherheitsmodule (SSM)

Software Security Modules (SSM) hingegen sind Softwarepakete, die einen ähnlichen Zweck wie HSM erfüllen. Sie sind im Paket mit der FND-Software erhältlich und bieten eine einfache Alternative anstelle der Appliance.

Beachten Sie, dass sowohl HSM als auch SSM optionale Komponenten in FND-Bereitstellungen sind und nicht obligatorisch sind.

Funktionen des HSM

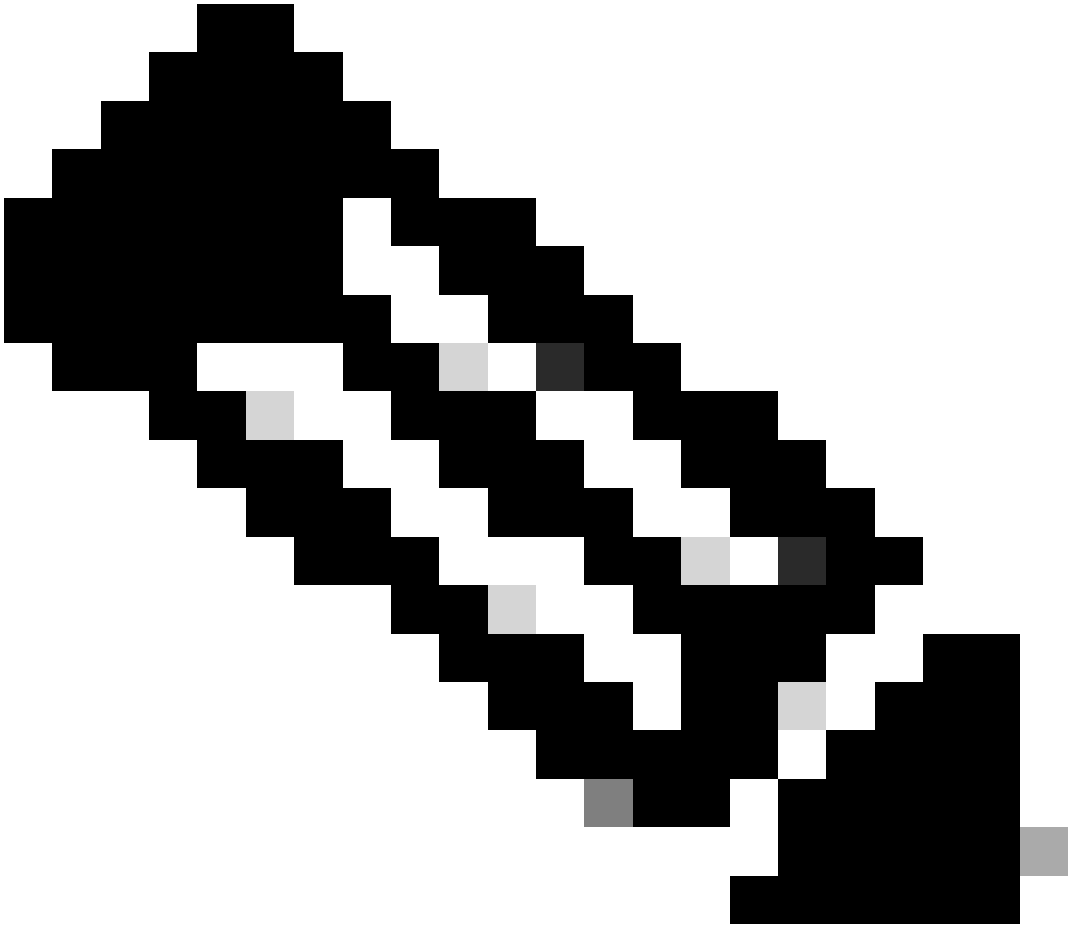
Die Hauptfunktion von HSM und SSM in einer FND-Lösung besteht darin, das PKI-Schlüsselpaar und das CSMP-Zertifikat sicher zu speichern, insbesondere wenn CSMP-Endpunkte wie Messgeräte verwendet werden.

Diese Schlüssel und Zertifikate sind für die Verschlüsselung der Kommunikation zwischen FND

und den CSMP-Endpunkten erforderlich.

Bei der Bereitstellung ist HSM eine Standalone-Appliance, während SSM entweder auf demselben Linux-Server wie FND oder auf einem separaten Linux-Server installiert werden kann. Die Konfiguration für SSM wird in der Datei "cgms.properties" angegeben.

Während des Bootvorgangs sucht FND nach HSM-Clientbibliotheken, unabhängig davon, ob HSM-bezogene Informationen in cgms.properties angegeben sind. Protokolle, die während des Bootvorgangs fehlende HSM-Clientbibliotheken betreffen, können ignoriert werden, wenn HSM nicht in der Lösung enthalten ist.



Hinweis: HSM-bezogene Informationen müssen in der Datei "cgms.properties" angegeben werden, die sich in verschiedenen Verzeichnissen befindet, je nachdem, ob FND über OVA oder ISO installiert ist.

Installation des HSM-Clients

Der HSM-Client muss auf demselben Linux-Server installiert werden, auf dem sich der FND-Server befindet. Kunden können die HSM-Client-Software von der Thales-Website oder über einen Cisco Supportvertrag herunterladen.

In den Versionshinweisen zur FND-Software wird die für die Bereitstellung erforderliche Software auf dem HSM-Client und der HSM-Software dokumentiert. Sie wird für die Versionshinweise im Abschnitt zur HSM-Upgrade-Tabelle aufgeführt.

Pfad für HSM-Client-Installationsdateien, Konfigurationsdateien und Bibliotheken:

Der Standard-Installationsstandort ist /usr/safenet/lunaclient/bin . Die meisten Befehle, wie lunacm, vtl oder ckdemo, werden von diesem Pfad aus ausgeführt (/usr/safenet/lunaclient/bin).

Die Konfigurationsdatei finden Sie unter /etc/Chrystoki.conf .

Der Pfad zu den vom FND-Server auf Linux-Servern benötigten HSM Luna-Client-Bibliotheksdateien lautet /usr/safenet/lunaclient/jsp/lib/ .

HSM-Server

In den meisten Bereitstellungen wird der HSM-Server als Appliance verwendet.

Der HSM-Server muss partitioniert werden, und HSM-Clients haben nur Zugriff auf die Partition, der sie zugewiesen sind. Der HSM-Server kann PED- oder kennwortauthentifiziert werden.

Bei der Passwortauthentifizierung reichen ein Benutzername und ein Passwort für Konfigurationsänderungen auf dem HSM-Server aus.

HSM mit PED-Authentifizierung ist jedoch eine mehrstufige Authentifizierungsmethode, bei der die Person, die Änderungen vornimmt, zusätzlich zu einem Kennwort Zugriff auf einen PED-Schlüssel benötigt.

Die PED-Taste funktioniert wie ein Dongle und zeigt eine PIN an, die der Benutzer zusammen mit dem Kennwort eingeben muss, um Konfigurationsänderungen vorzunehmen.

Bei bestimmten Befehlen wie show-Befehlen und schreibgeschütztem Zugriff ist die PED-Taste nicht erforderlich. Der PED-Schlüssel ist nur für bestimmte Konfigurationsänderungen erforderlich, z. B. für das Erstellen von Partitionen.

Jeder Serverpartition können mehrere Clients zugewiesen sein, und alle einer Partition zugewiesenen Clients haben Zugriff auf die Daten in dieser Partition.

Der HSM-Server bietet verschiedene Benutzerrollen, wobei die Rollen des Administrators und des Crypto Security Officers besonders wichtig sind. Darüber hinaus gibt es die Rolle der Partition Security Officer.

Fehlerbehebung

FND verwendet den HSM-Client für den Zugriff auf die HSM-Hardware. Die Integration besteht also aus zwei Teilen.

1. Kommunikation zwischen HSM-Client und HSM-Server
2. Kommunikation zwischen FND und HSM-Client

Beide Komponenten müssen für eine erfolgreiche HSM-Integration geeignet sein.

Kommunikation zwischen HSM-Client und HSM-Server

Um festzustellen, ob der HSM-Client die Schlüssel- und Zertifikatinformationen, die in der HSM-Partition auf dem HSM-Server gespeichert sind, mithilfe eines einzigen Befehls lesen kann, verwenden Sie den Befehl /cmu list aus dem Speicherort /usr/safenet/lunaclient/bin.

Durch Ausführen dieses Befehls wird angegeben, ob der HSM-Client auf den in der HSM-Partition gespeicherten Schlüssel und das in der HSM-Partition gespeicherte Zertifikat zugreifen kann.

Beachten Sie, dass Sie bei diesem Befehl ein Kennwort eingeben müssen, das mit dem Kennwort für die HSM-Partition übereinstimmen muss.

Eine erfolgreiche Ausgabe ähnelt diesem Ergebnis:

[root@fndblr23 bin]# ./cmd list
Certificate Management Utility (64-Bit) v7.3.0-165. Copyright (c) 2018 SafeNet. Alle Rechte vorbehalten.

Geben Sie ein Kennwort für das Token in Steckplatz 0 ein: *******

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

Anmerkung:

Wenn sich der Kunde nicht an das Kennwort erinnert, entschlüsseln Sie das Kennwort, das in der Datei "cgms.properties" aufgeführt ist, wie hier gezeigt:

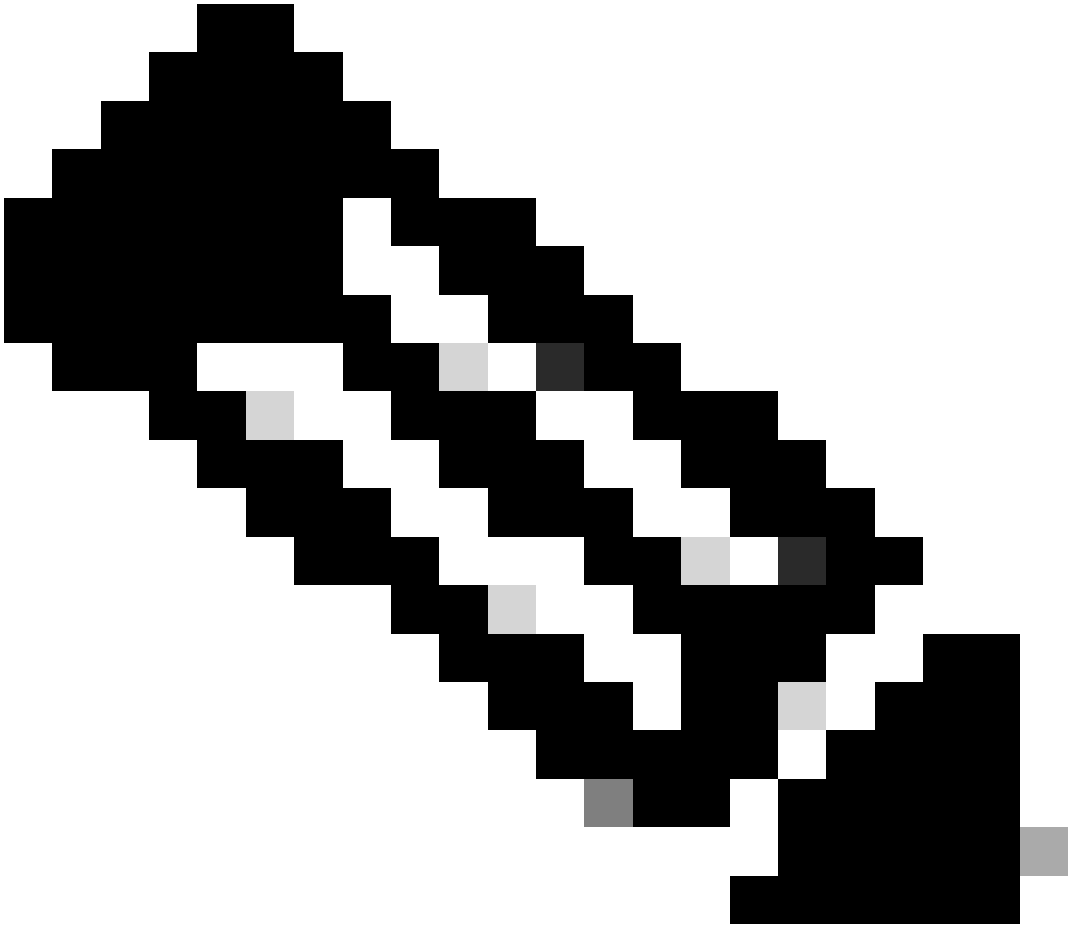
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | Grep HSM
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh entschlüsseln qnBC7WGvZB5iux4BnnDplTWzcmAxhuISQLmVRXtHBeBWF4=
KennwortBeispiel
[root@fndblr23 ~]#

In diesem Fall lautet das entschlüsselte Kennwort Kennwort KennwortBeispiel

1. NTLS-Kommunikationsprüfung:

Der HSM-Client kommuniziert mit dem HSM-Server über den bekannten Port 1792 für NTLS-Kommunikation (Network Transport Layer Security), der sich im etablierten Zustand befindet.

Verwenden Sie den folgenden Befehl, um den Status der NTLS-Kommunikation auf dem Linux-Server zu überprüfen, auf dem der FND-Server ausgeführt wird und auf dem der HSM-Client installiert ist:



Hinweis: "netstat" wurde in Linux durch den Befehl "ss" ersetzt.

Schlag

Code kopieren

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

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

Wenn sich die Verbindung nicht im gesicherten Zustand befindet, weist dies auf ein Problem mit der grundlegenden NTLS-Kommunikation hin.

Raten Sie dem Kunden in diesem Fall, sich bei seiner HSM-Appliance anzumelden und zu überprüfen, ob der NTLS-Dienst mit dem Befehl "ntls information show" ausgeführt wird.

Stellen Sie außerdem sicher, dass die Schnittstellen für NTLS aktiviert sind. Sie können die Zähler mit "ntls information reset" zurücksetzen und dann den Befehl "show" erneut eingeben.

Auf HSM-Appliance oder HSM-Server:

Yaml

Code kopieren

[hsmlatest] lunash:>ntls Informationen anzeigen

NTLS-Informationen:

Betriebsstatus: 1 (aktiv)

Verbundene Clients: 1

Links: 1

Erfolgreiche Clientverbindungen: 20095

Fehlgeschlagene Clientverbindungen: 20150

Befehlsergebnis: 0 (Erfolg)

[hsmneueste] Mittagspause:>

1. Luna Safenet Kundenidentifizierung:

Der HSM-Client, auch als Luna Safenet-Client bekannt, kann mithilfe des Befehls "./lunacm" vom Speicherort "/usr/safenet/lunaclient/bin" identifiziert werden. Mit diesem Befehl werden auch die dem Client zugewiesene HSM-Partition und jede konfigurierte HA-Gruppe (High Availability) aufgeführt.

Code kopieren

[root@fndblr23 bin]# ./lunacm

lunacm (64-Bit) v7.3.0-165. Copyright (c) 2018 SafeNet. Alle Rechte vorbehalten.

Die installierte Version des Luna-Clients ist hier angegeben (in diesem Beispiel Version 7.3).

Die Ausgabe zeigt außerdem Informationen über die verfügbaren HSMs an, einschließlich der

zugewiesenen HSM-Partitionen und der Konfiguration der HA-Gruppe.

Mathematik

Code kopieren

Steckplatz-ID -> 0

Label -> TEST2

Seriennummer -> 1358678309716

Modell -> LunaSA 7.4.0

Firmware-Version -> 7.4.2

Konfiguration -> LUNA Benutzerpartition mit SO (PED)-Schlüsselexport mit Klonmodus

Steckplatzbeschreibung -> Net Token Slot

Steckplatz-ID -> 4

HSM-Label -> TEST2Group

HSM-Seriennummer -> 11358678309716

HSM-Modell -> LunaVirtual

HSM-Firmwareversion -> 7.4.2

HSM-Konfiguration -> Luna Virtual HSM (PED) Key Export mit Klonmodus

HSM-Status -> k. A. - HA-Gruppe

Stellen Sie sicher, dass jeder HSM-Client mindestens einer Partition zugewiesen ist, und beziehen Sie sich auf die Konfigurationen der HA-Gruppen für Hochverfügbarkeitsszenarien.

d. Um die HSM-Server aufzulisten, die mit dem Luna-Client konfiguriert sind, verwenden Sie die ./vtl listServers im Verzeichnis /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. Wenn wir ./vtl eingeben und dann Enter im Verzeichnis/usr/safenet/lunaclient/bin drücken, zeigt es die Liste der Optionen an, die mit dem vtl-Befehl verfügbar sind.

./vtl verify listet die physischen HSM-Partitionen auf, die für den Luna-Client sichtbar sind.

./vtl listSlots listet alle physischen und virtuellen Steckplätze (HA-Gruppe) auf, wenn HAGroup konfiguriert, aber deaktiviert ist.

Wenn HAGroup konfiguriert und aktiviert ist, werden nur die Informationen der virtuellen Gruppe oder der HAGroup angezeigt.

```
[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. Um herauszufinden, ob HAGroup aktiviert ist oder nicht, können wir die ./vtl listSlots verwenden. Wenn nur die HAGroup angezeigt wird und die physischen Steckplätze nicht angezeigt werden, wissen wir, dass HAGroup aktiviert ist.

Eine andere Möglichkeit, herauszufinden, ob HAGroup aktiviert ist, besteht darin, den Befehl ./lunacm von /usr/safenet/lunaclient/bin auszugeben und dann den Befehl ha l auszugeben.

Das angeforderte Kennwort ist das Kennwort der physischen Partition. In diesem Hinweis, dass die einzige zeigen HA Slots ist ja. Das bedeutet, dass HA aktiv ist.

Ist dies nicht der Fall, ist die HA-Funktion zwar konfiguriert, aber nicht aktiv.

HA kann mit dem Befehl "ha ha-only enable" im lunacm-Modus aktiviert werden.

```
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. Kunden haben Zugriff auf HSM-Server. In der Regel werden HSM-Server im Rechenzentrum gehostet, und viele von ihnen werden per PED betrieben.

PED ist wie ein kleiner Dongle, der Sicherheitstokeninformationen anzeigt, die mehrstufige Authentifizierung für zusätzliche Sicherheit darstellen, es sei denn, der Benutzer hat sowohl das Kennwort als auch das Token, dann ist bestimmter Zugriff wie Admin- oder Konfigurationszugriff nicht erlaubt.

Der einzige Befehl, der alle Serverinformationen auflistet, lautet hsm show

In dieser Ausgabe können wir sehen, dass der Name der hsm-Appliance hsmlatest ist. Die Lunash-Eingabeaufforderung zeigt an, dass es sich um den HSM-Server handelt.

Die HSM-Softwareversion lautet 7.4.0-226. Es werden weitere Informationen angezeigt, z. B. die Seriennummer der Appliance und die Authentifizierungsmethode (PED oder Kennwort). Außerdem wird die Gesamtanzahl der Partitionen in diesem HSM angezeigt. Beachten Sie, dass HSM-Clients Partitionen in der Appliance zugeordnet sind.

```
[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:>
```

Weitere nützliche Befehle auf dem HSM-Server sind der Befehl partition show.

Die Felder, auf die verwiesen werden muss, sind der Partitionsname, die Seriennummer und die Partitionsobjektzahl. Die Anzahl der Partitionsobjekte ist hier 2.

Das heißt, ein in der Partition gespeichertes Objekt ist das Schlüsselpaar für die CSMP-Nachrichtenverschlüsselung, und ein anderes gespeichertes Objekt ist das CSMP-Zertifikat.

Befehl client list:

Der Client, den wir überprüfen, wird in der Liste der registrierten Clients im Befehl client list aufgeführt.

client show -c listet nur die Client-Informationen, den Hostnamen, die IP-Adresse und die Partition auf, der dieser Client zugewiesen ist. Erfolgreiche Ausgaben sehen so aus.

Hier können wir den Partitionsnamen, die Seriennummer und auch die Partitionsobjekte

betrachten. In diesem Fall ist das Partitionsobjekt = 2, wobei die beiden Objekte der private Schlüssel und das CSMP-Zertifikat sind.

```
[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:>
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.