HSM(Hardware Security Module)과 FND의 통합 문제 해결

목차

소개

이 문서에서는 HSM(Hardware Security Module), FAN(Field Area Network) 솔루션과의 통합 및 일반적인 문제 해결에 대해 설명합니다.

하드웨어 보안 모듈(HSM)

HSM(Hardware Security Module)은 어플라이언스, PCI 카드, 클라우드 오퍼링의 세 가지 형태로 제공됩니다. 대부분의 구축은 어플라이언스 버전을 선택합니다.

SSM(Software Security Module)

반면, SSM(Software Security Module)은 HSM과 유사한 목적을 수행하는 소프트웨어 패키지입니다. FND 소프트웨어와 번들로 제공되며 어플라이언스 대신 간단한 대안을 제공합니다.

HSM과 SSM은 모두 FND 구축의 선택적 구성 요소이며 필수 구성 요소가 아닙니다.

HSM의 기능

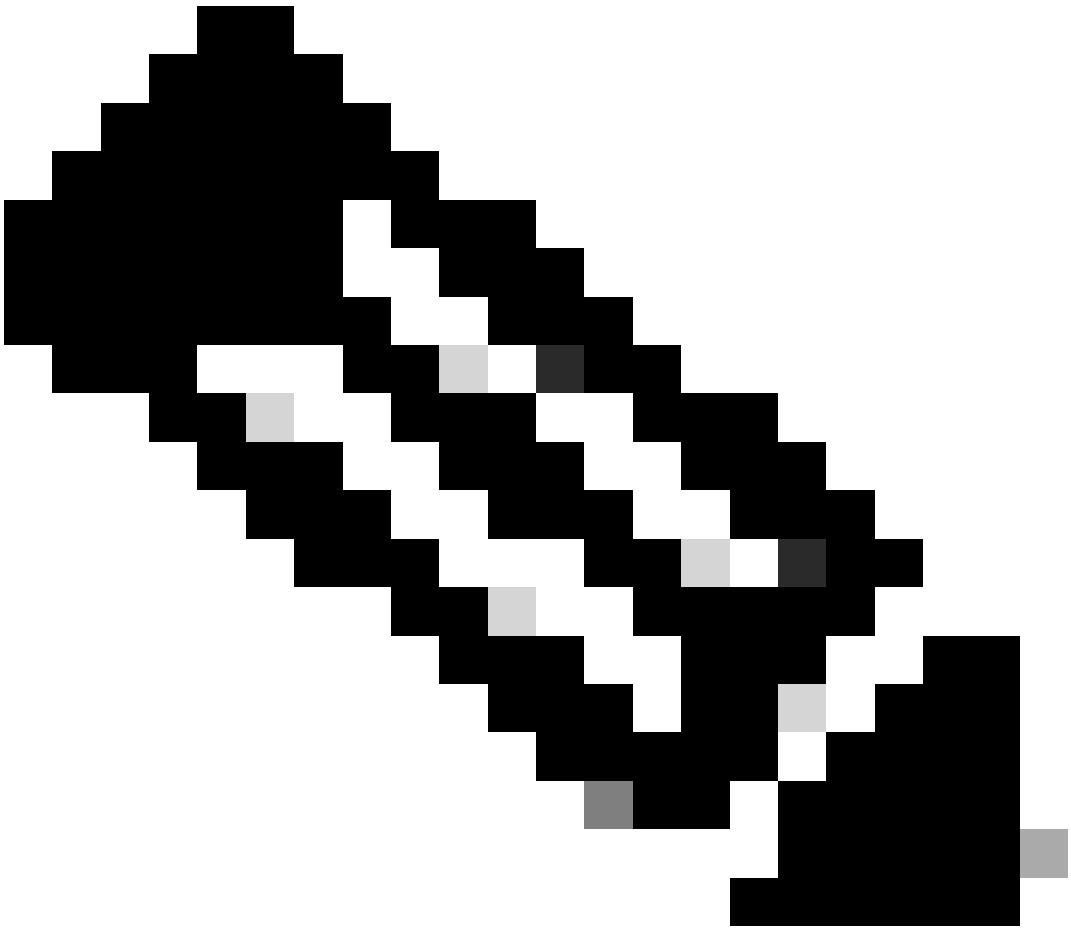
FND 솔루션에서 HSM과 SSM의 기본 기능은 PKI 키 쌍과 CSMP 인증서를 안전하게 저장하는 것입니다. 특히 계량기와 같은 CSMP 엔드포인트를 사용하는 경우 더욱 그렇습니다.

이러한 키와 인증서는 FND와 CSMP 엔드포인트 간의 통신을 암호화하는 데 필수적입니다.

구축과 관련하여 HSM은 독립형 어플라이언스이지만, SSM은 FND와 동일한 Linux 서버 또는 별도의 Linux 서버에 설치할 수 있습니다. SSM에 대한 컨피그레이션은 cgms.properties 파일에 지정되

어 있습니다.

부팅 과정에서 FND는 HSM 관련 정보가 cgms.properties에 지정되었는지 여부와 상관없이 HSM 클라이언트 라이브러리를 확인합니다. HSM이 솔루션에 포함되지 않은 경우 부팅 중에 누락된 HSM 클라이언트 라이브러리와 관련된 모든 로그는 무시할 수 있습니다.



> 참고: HSM 관련 정보는 OVA를 통해 FND를 설치하는지 ISO를 통해 설치하는지에 따라 다른 디렉토리에 있는 cgms.properties 파일에 지정해야 합니다.

HSM 클라이언트 설치

HSM 클라이언트는 FND 서버가 있는 동일한 Linux 서버에 설치해야 합니다. 고객은 Thales 웹 사이트 또는 Cisco 지원 계약을 통해 HSM 클라이언트 소프트웨어를 다운로드할 수 있습니다.

FND 소프트웨어 릴리스는 구축을 위해 HSM 클라이언트 및 HSM 소프트웨어에 필요한 소프트웨어를 기록합니다. 릴리스 정보의 HSM 업그레이드 테이블 섹션 아래에 나열됩니다.

HSM 클라이언트 설치 파일, 구성 파일 및 라이브러리의 경로:

기본 설치 위치는 /usr/safenet/lunaclient/bin입니다. lunacm, vtl, ckdemo와 같은 대부분의 명령은 이 경로(/usr/safenet/lunaclient/bin)에서 실행됩니다.

구성 파일은 /etc/Chrystoki.conf에 있습니다.

Linux 서버의 FND 서버에 필요한 HSM Luna 클라이언트 라이브러리 파일의 경로는 /usr/safenet/lunaclient/jsp/lib/입니다.

HSM 서버

대부분의 구축에서는 HSM 서버를 어플라이언스로 사용합니다.

HSM 서버는 분할해야 하며 HSM 클라이언트는 할당된 특정 파티션에만 액세스할 수 있습니다. HSM 서버는 PED 인증 또는 비밀번호 인증이 가능합니다.

비밀번호 인증에서 사용자 이름과 비밀번호는 HSM 서버의 컨피그레이션 변경에 충분합니다.

그러나 PED authenticated HSM은 비밀번호 외에도 변경을 수행하는 사람이 PED 키에 액세스해야 하는 다단계 인증 방법입니다.

PED 키는 동글과 같이 작동하며 사용자가 비밀번호를 입력하여 컨피그레이션을 변경해야 하는 PIN을 표시합니다.

show 명령 및 읽기 전용 액세스와 같은 특정 명령의 경우 PED 키가 필요하지 않습니다. 파티션 생성과 같은 특정 컨피그레이션 변경에만 PED 키가 필요합니다.

각 서버 파티션에는 여러 클라이언트가 할당될 수 있으며, 파티션에 할당된 모든 클라이언트는 해당 파티션 내의 데이터에 액세스할 수 있습니다.

HSM 서버는 다양한 사용자 역할을 제공하며 관리자 및 암호화 보안 담당자의 역할이 특히 중요합니다. 또한, 파티션 보안 책임자의 역할도 있습니다.

문제 해결

FND는 HSM 클라이언트를 사용하여 HSM 하드웨어에 액세스합니다. 따라서 통합에는 두 가지 부분이 있습니다.

1. HSM 클라이언트와 HSM 서버 간 통신
2. HSM 클라이언트 통신에 대한 FND

두 부분 모두 HSM 통합이 성공적으로 이루어지기 위해 작동해야 합니다.

HSM 클라이언트와 HSM 서버 간 통신

HSM 클라이언트가 단일 명령을 사용하여 HSM 서버의 HSM 파티션에 저장된 키 및 인증서 정보를

성공적으로 읽을 수 있는지 확인하려면 /usr/safenet/lunaclient/bin 위치에서 /cmu list 명령을 사용합니다.

이 명령을 실행하면 HSM 클라이언트가 HSM 파티션에 저장된 키 및 인증서에 액세스할 수 있는지 여부를 나타내는 출력이 제공됩니다.

이 명령은 HSM 파티션의 비밀번호와 동일해야 하는 비밀번호를 입력하라는 프롬프트를 표시합니다.

성공적인 출력은 다음 결과와 유사합니다.

[root@fndblr23 bin]# ./cmu 목록
인증서 관리 유틸리티(64비트) v7.3.0-165. 저작권 (c) 2018 SafeNet. All rights reserved.

슬롯 0: *******에 토큰의 암호를 입력하십시오.

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

참고:

고객이 비밀번호를 기억하지 못하는 경우, cgms.properties 파일에 나와 있는 비밀번호를 해독합니다.

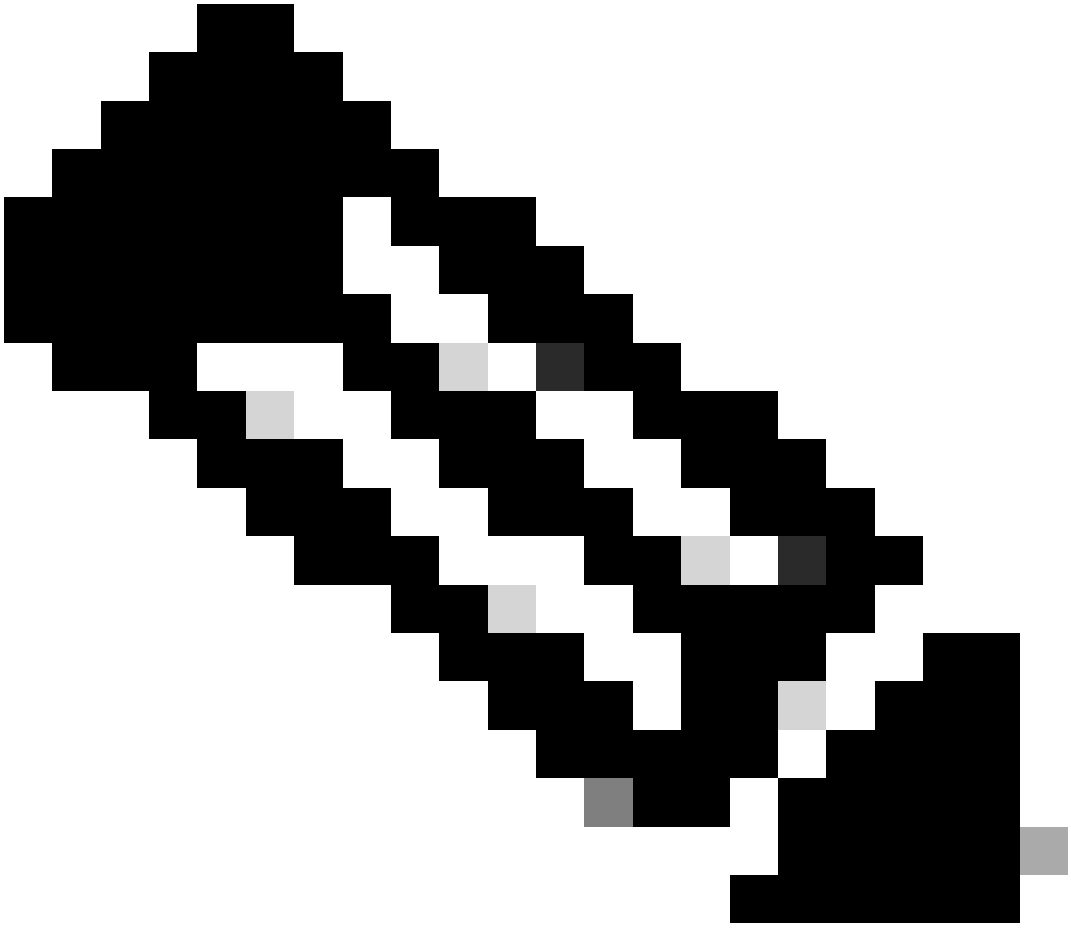
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2그룹
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
비밀번호샘플
[root@fndblr23 ~]#

이 경우 암호 해독된 암호는 Passwordexample입니다

1. NTLS 통신 확인:

HSM 클라이언트는 설정된 상태의 NTLS(Network Transport Layer Security) 통신용 잘 알려진 포트 1792를 사용하여 HSM 서버와 통신합니다.

FND 서버를 실행 중인 Linux 서버 및 HSM 클라이언트가 설치된 위치에서 NTLS 통신의 상태를 확인하려면 다음 명령을 사용합니다.



참고: Linux에서 "netstat"가 "ss" 명령으로 대체되었습니다.

강타

코드 복사

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

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

연결이 설정된 상태가 아니면 기본 NTLS 통신에 문제가 있음을 나타냅니다.

그러한 경우 고객에게 HSM 어플라이언스에 로그인하고 "ntls information show" 명령을 사용하여 NTLS 서비스가 실행 중인지 확인하도록 안내합니다.

또한 인터페이스가 NTLS에 대해 활성화되어 있는지 확인합니다. "ntls information reset"을 사용하여 카운터를 재설정한 다음 "show" 명령을 다시 실행할 수 있습니다.

HSM 어플라이언스 또는 HSM 서버에서:

야말

코드 복사

[hsmlatest] lunash:>ntls 정보 표시

NTLS 정보:

작동 상태: 1(up)

연결된 클라이언트: 1

링크: 1

성공적인 클라이언트 연결: 20095

실패한 클라이언트 연결: 20150

명령 결과: 0(성공)

[hsmlatest] lunash:>

1. Luna Safenet 클라이언트 식별:

Luna Safenet 클라이언트라고도 하는 HSM 클라이언트는 "/usr/safenet/lunaclient/bin" 위치에서 "./lunacm" 명령을 사용하여 식별할 수 있습니다. 이 명령은 클라이언트에 할당된 HSM 파티션과 구성된 HA(고가용성) 그룹도 나열합니다.

코드 복사

[root@fndblr23 bin]# ./lunacm

lunacm(64비트) v7.3.0-165. 저작권 (c) 2018 SafeNet. All rights reserved.

설치된 Luna 클라이언트의 버전이 여기에 표시됩니다(이 예에서는 버전 7.3).

또한 할당된 HSM 파티션 및 HA 그룹 컨피그레이션을 포함하여 사용 가능한 HSM에 대한 정보도 표시됩니다.

수학자

코드 복사

슬롯 ID -> 0

레이블 -> TEST2

일련 번호 -> 1358678309716

모델 -> LunaSA 7.4.0

펌웨어 버전 -> 7.4.2

Configuration(컨피그레이션) -> Luna User Partition With SO (PED) Key Export With Cloning Mode(복제 모드를 사용하여 SO(PED) 키가 있는 Luna 사용자 파티션 내보내기)

슬롯 설명 -> Net Token Slot

슬롯 Id -> 4

HSM 레이블 -> TEST2Group

HSM 일련 번호 -> 11358678309716

HSM 모델 -> LunaVirtual

HSM 펌웨어 버전 -> 7.4.2

HSM Configuration(HSM 컨피그레이션) -> 복제 모드를 사용하여 Luna PED(Virtual HSM) 키 내보내기

HSM 상태 -> 해당 사항 없음 - HA 그룹

각 HSM 클라이언트가 하나 이상의 파티션에 할당되었는지 확인하고 고가용성 시나리오를 위한 HA 그룹과 관련된 컨피그레이션을 이해합니다.

d. luna 클라이언트로 구성된 HSM 서버를 나열하려면 /usr/safenet/lunaclient/bin 위치에서 ./vtl listServers를 사용합니다

```
[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. . /vtl을 입력한 다음 location/usr/safenet/lunaclient/bin에서 enter 키를 누르면 vtl 명령에서 사용할 수 있는 옵션 목록이 표시됩니다.

./vtl verify는 Luna 클라이언트에 표시되는 HSM 물리적 파티션을 나열합니다.

./vtl listSlots는 HAGroup이 구성되었지만 비활성화된 경우 모든 물리적 슬롯과 가상 슬롯(HA 그룹)을 나열합니다.

HAGroup이 구성되어 활성화된 경우 가상 그룹 또는 HAGroup 정보만 표시됩니다.

```
[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. HAGroup이 활성화되어 있는지 여부를 확인하려면 ./vtl listSlots를 사용합니다. HAGroup만 표시되고 물리적 슬롯은 표시되지 않으면 HAGroup이 활성화되어 있음을 알 수 있습니다.

HAGroup이 활성화되어 있는지 확인하는 또 다른 방법은 /usr/safenet/lunaclient/bin에서./lunacm을 실행한 다음 ha l 명령을 실행하는 것입니다

요청한 비밀번호는 실제 파티션의 비밀번호입니다. 이 알림에서는 HA 슬롯만 yes로 표시됩니다. 이는 HA가 활성 상태임을 의미합니다.

no인 경우 HA가 구성되더라도 활성화되지 않습니다.

HA는 lunacm 모드에서 "ha ha-only enable" 명령을 사용하여 활성화할 수 있습니다.

```
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. 고객은 HSM 서버에 액세스할 수 있습니다. 일반적으로 HSM 서버는 DC에서 호스팅되며 그중 상당수는 PED로 운영됩니다.

PED는 사용자가 비밀번호와 토큰을 모두 가지고 있지 않는 한, 추가 보안을 위해 다단계 인증인 보안 토큰 정보를 표시하는 작은 동글과 같으며, admin 또는 config 액세스와 같은 특정 액세스는 허용되지 않습니다.

모든 서버 정보를 나열하는 단일 명령은 hsm show입니다

이 출력에서는 hsm 어플라이언스의 이름이 hsmlatest임을 확인할 수 있습니다. lunash 프롬프트는 HSM 서버임을 알려줍니다.

HSM 소프트웨어 버전 7.4.0-226을 볼 수 있습니다. 어플라이언스의 일련 번호, 인증 방법, PED 또는 비밀번호 등 다른 정보도 볼 수 있으며, 해당 HSM의 총 파티션 수도 볼 수 있습니다. 앞에서 살펴본 것처럼 HSM 클라이언트는 어플라이언스의 파티션과 연결되어 있습니다.

```
[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 서버의 다른 유용한 명령에는 partition show 명령이 포함됩니다.

우리가 참조해야 하는 필드는 파티션 이름, 일련 번호, 파티션 개체 수입니다. 파티션 개체 수는 여기서 2입니다.

즉, 파티션에 저장된 한 객체는 CSMP 메시지 암호화를 위한 키 쌍이고, 다른 객체는 CSMP 인증서입니다.

client list 명령:

검사 중인 클라이언트는 client list 명령의 등록된 클라이언트 목록에 나열됩니다.

client show -c <client name>은(는) 해당 클라이언트 정보, 호스트 이름, IP 주소 및 이 클라이언트가 할당된 파티션만 나열합니다. 성공한 출력은 다음과 같습니다.

여기서는 파티션 이름, 일련 번호 및 파티션 개체를 확인할 수 있습니다. 이 경우 파티션 개체 = 2이며, 두 개체는 개인 키 및 CSMP 인증서입니다.

```
[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:>
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.