أستكشاف أخطاء تكامل وحدات أمان الأجهزة (HSM) وإصلاحها باستخدام FND

المحتويات

المقدمة

يصف هذا المستند وحدة أمان الأجهزة (HSM) والدمج مع حل شبكة المنطقة (FAN) واستكشاف المشكلات الشائعة وإصلاحها.

وحدة أمان الأجهزة (HSM)

تتوفر وحدات أمان الأجهزة (HSM) في ثلاثة أشكال: الجهاز وبطاقة PCI وعرض الشبكة. تختار معظم عمليات النشر إصدار الجهاز.

وحدات أمان البرامج (SSM)

وحدات أمان البرامج (SSM)، من ناحية أخرى، هي حزم برامج تخدم غرضا مماثلا لـ HSM. فهي موزعة ببرنامج الصندوق الوطني للتنمية المستدامة وتوفر بديلا بسيطا بدلا من الجهاز.

من المهم ملاحظة أن كلا من HSM و SSM هما مكونان اختياريان في عمليات نشر القوات الخاصة وهما ليسا إلزاميين.

وظائف الجهاز

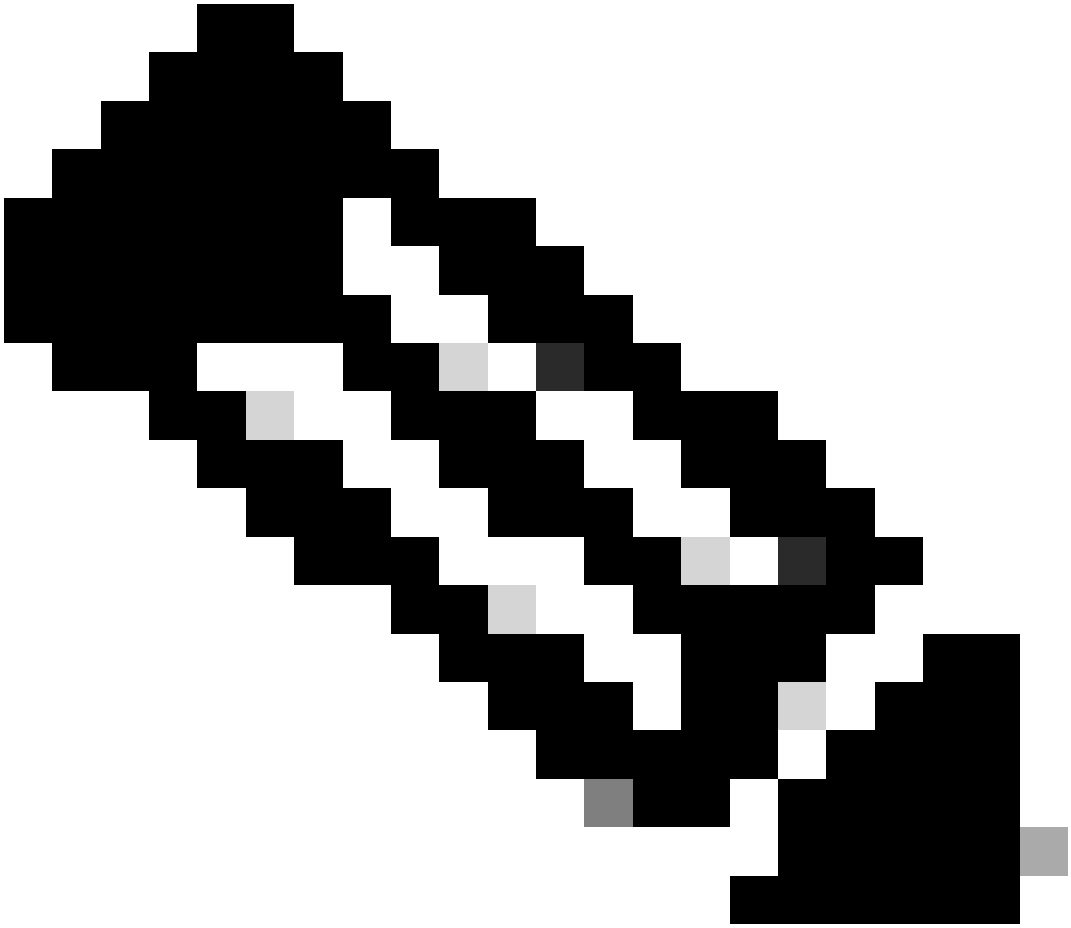
الوظيفة الأساسية لكل من HSM و SSM في حل FND هي تخزين زوج مفاتيح PKI بشكل آمن وشهادة CSMP، خاصة عندما يتم إستخدام نقاط نهاية CSMP مثل الأمتار.

هذه المفاتيح والشهادات ضرورية لتشفير الاتصال بين FND ونقاط نهاية CSMP.

وفيما يتعلق بالنشر، فإن HSM هو جهاز مستقل، بينما يمكن تثبيت SSM إما على نفس

خادم Linux مثل FND أو على خادم Linux منفصل. تم تحديد تكوين SSM في ملف cgms.properties.

أثناء بدء التشغيل، يتحقق FND من مكتبات عملاء HSM، بغض النظر عما إذا كانت المعلومات المتعلقة ب HSM محددة في cgms.properties. يمكن تجاهل أي سجلات متعلقة بمكتبات عملاء HSM المفقودة أثناء بدء التشغيل إذا لم يتم تضمين HSM في الحل.



ملاحظة: يجب تحديد المعلومات المتعلقة ب HSM في ملف cgms.properties الموجود في دليل مختلف وفقا لما إذا كان FND مثبتا عبر OVA أو ISO.

تثبيت عميل HSM

يجب تثبيت عميل HSM على خادم Linux نفسه حيث يوجد خادم FND. يمكن للعملاء تنزيل برنامج عميل HSM من موقع Thales على الويب أو من خلال عقد دعم Cisco.

يقوم إصدار برنامج FND بتوثيق البرنامج المطلوب على عميل HSM وبرنامج HSM للنشر. وقد تم إدراجه ضمن قسم جدول ترقية HSM لملاحظات الإصدار.

مسار ملفات تثبيت عميل HSM وملفات التكوين والمكتبات:

موقع التثبيت الافتراضي هو /usr/safenet/lunaclient/bin . يتم تشغيل معظم الأوامر، مثل lunacm أو vtl أو ckdemo، من هذا المسار (/usr/safenet/lunaclient/bin).

يوجد ملف التكوين في /etc/Chrystoki.conf .

مسار ملفات مكتبة HSM Luna Client Library التي يحتاج إليها خادم FND على خوادم Linux هو /usr/safenet/lunaclient/jsp/lib/ .

خادم HSM

تستخدم معظم عمليات النشر خادم HSM كجهاز.

يجب تقسيم خادم HSM، والوصول إلى العملاء HSM إلى القسم المحدد المعين لهم. يمكن مصادقة خادم HSM أو مصادقته بكلمة مرور.

في مصادقة كلمة المرور، يكون اسم المستخدم وكلمة المرور كافيين لتغييرات التكوين في خادم HSM.

ومع ذلك، فإن HSM المصادق عليها هي طريقة مصادقة متعددة العوامل حيث يحتاج الشخص الذي يجري التغييرات، بالإضافة إلى كلمة المرور، إلى الوصول إلى مفتاح PED.

يعمل المفتاح PED مثل مفتاح، ويعرض رقم التعريف الشخصي (PIN) الذي يجب على المستخدم إدخاله مع كلمة المرور لإجراء أي تغييرات في التكوين.

بالنسبة لأوامر معينة مثل أوامر العرض والوصول للقراءة فقط، لا يكون مفتاح PED ضروري. تتطلب تغييرات التكوين المحددة فقط مثل إنشاء الأقسام المفتاح PED.

يمكن أن يحتوي كل قسم خوادم على عملاء متعددين تم تعيينهم له، كما يمكن لجميع العملاء المعينين لقسم ما الوصول إلى البيانات الموجودة داخل ذلك القسم.

يوفر خادم HSM أدوارا مختلفة للمستخدم، حيث تكون أدوار المسؤول ومسؤول أمان التشفير مهمة بشكل خاص. وبالإضافة إلى ذلك، هناك دور موظف أمن القسم.

استكشاف الأخطاء وإصلاحها

يستخدم FND عميل HSM للوصول إلى أجهزة HSM. وبالتالي، هناك جزء للتكامل.

1. عميل HSM إلى اتصال خادم HSM
2. اتصال عميل FND إلى HSM

يحتاج كل الجزيئين إلى العمل من أجل نجاح تكامل HSM.

عميل HSM إلى اتصال خادم HSM

لتحديد ما إذا كان يمكن لعميل HSM قراءة معلومات المفتاح والشهادة المخزنة في قسم
HSM على خادم HSM باستخدام رمز واحد بنجاح، أستخدم الأمر /cmu list من موقع
/usr/safenet/lunaclient/bin.

يوفر تنفيذ هذا الأمر إخراج يشير إلى ما إذا كان يمكن لعميل HSM الوصول إلى المفاتيح
والشهادة المخزنة في قسم HSM.

الرجاء ملاحظة أن هذا الأمر يطلب كلمة مرور، والتي يجب أن تكون نفس كلمة المرور الخاصة
بتقسيم HSM.

المخرج الناجح يتشابه مع هذه النتيجة:

[root@fndblr23 bin]# ./cmu قائمة
إدارة الشهادات المساعدة (64 بت) الإصدار 7. 3. 0-165. حقوق النشر (c) 2018 SafeNet. جميع
الحقوق محفوظة.

يرجى إدخال كلمة مرور للرمز المميز في الفتحة 0 : ******

handle=200001 label=NMS_SOUTHBOUND_KEY
handle=200002 label=NMS_SOUTHBOUND_KEY-cert0
[root@fndblr23 bin]#

ملاحظة:

إذا لم يتذكر العميل كلمة المرور، فقم بفك تشفير كلمة المرور المدرجة في ملف
cgms.properties كما هو موضح أنه:

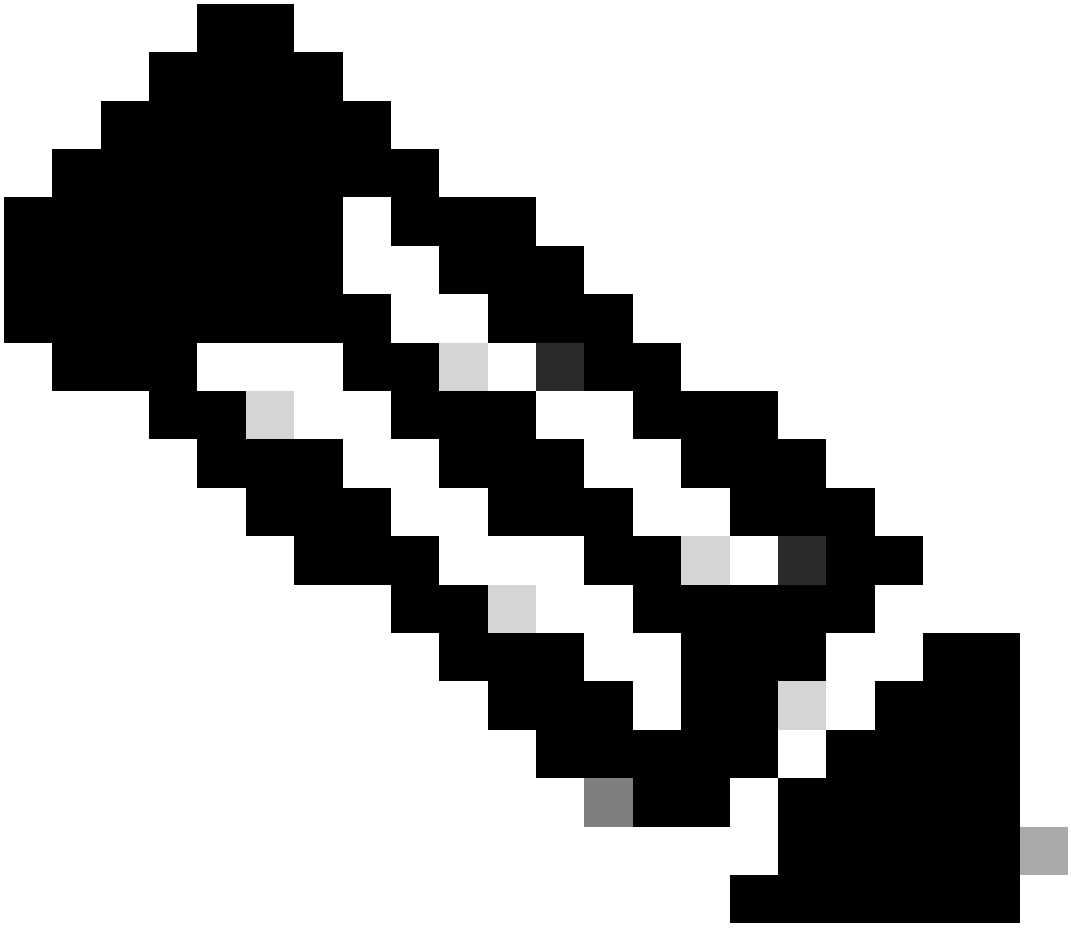
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | غرب إتش إس إم
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
hsm-keystore-name=TEST2Group
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
كلمة المرور
[root@fndblr23 ~]#

في هذه الحالة، لا فك تشفير كلمة مرور تدقيق كلمة مرور

1. التحقق من اتصال NTLS:

يتصل عميل HSM بخادم HSM باستخدام المنفذ المعروف جيدا 1792 اتصالات طبقة
النقل عبر الشبكة (NTLS)، والتي تكون في الحالة المؤسسة.

للتحقق من حالة اتصال NTLS على خادم Linux الذي يقوم بتشغيل خادم FND وحيث يتم
تثبيت عميل HSM، أستخدم هذا الأمر:



ملاحظة: تم إستبدال "netstat" بالأمر "ss" في نظام التشغيل Linux

---

باش

نسخ الرمز

[root@fndblr23 ~]# ث ث -np | غورب 1792

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

إذا لم يكن الاتصال في الحالة المحددة، فإنه يشير إلى وجود مشكلة في اتصال NTLS الأساسي.

في مثل هذه الحالات، نصح العميل بتسجيل الدخول إلى جهاز HSM الخاص به والتحقق من تشغيل خدمة NTLS باستخدام الأمر ntls information show".

وبالإضافة إلى ذلك، تأكد من تمكين الواجهات ل NTLS. يمكنك إعادة ضبط العدادات باستخدام "إعادة تعيين معلومات NTLS" ثم إصدار الأمر show" مرة أخرى.

على جاهز HSM أو مداخ HSM:

لماي

نسخ الرمز

[hsmlatest] lunash:>ضرع تامولعم ntls

تامولعم NTLS:

حالة التشغيل: 1 (ألعلى)

الأجهزة العميلة المتصلة: 1

الروابط: 1

إتصاالت العمالء الناجحة: 20095

إتصاالت العميل الفاشلة: 20150

نتيجة الأمر: 0 (حاجن)

[hsmlatest] لوناش:>

1. تعريف عميل LUNA SAFENET:

يمكن تحديد عميل HSM، المعروف أيضا باسم عميل لونا Safenet، باستخدام الأمر ./LUNACM" من موقع /USR/SAFENET/Lunaclient/bin". كما يسرد هذا الأمر قسم HSM الذي تم تعيينه للعميل أو أي مجموعة عالية التوافر تم تكوينها (HA).

نسخ الرمز

[root@fndblr23 bin]# ./LUNACM

LUNACM (64 بت) الإصدار 7. 3. 0-165. حقوق النشر (c) 2018 SafeNet. جميع الحقوق محفوظة.

يتم الإشارة إلى إصدار عميل Luna المثبت هنا (في هذا المثال، الإصدار 7.3).

يعرض الإخراج أيضا معلومات حول HSMs المتوفرة، بما في ذلك أقسام HSM المعينة وتكوين مجموعة HA.

الكيتامثام

نسخ الرمز

معرف الفتحة -> 0

التسمية -> الاختبار 2

الرقم التسلسلي -> 1358678309716

الطراز -> LunaSA 7.4.0

إصدار البرنامج الثابت -> 7.4.2

التكوين -> قسم مستخدم LUN مع تصدير مفاتيح SO (PED) مع وضع النسخ

وصف الفتحة -> فتحة الرمز المميز ل Net

معرف الفتحة -> 4

تسمية HSM -> TEST2Group

الرقم التسلسلي HSM -> 11358678309716

طراز HSM -> LunaVirtual

إصدار البرنامج الثابت HSM -> 7.4.2

تكوين HSM -> تصدير مفاتيح HSM الظاهري (PED) لوان مع وضع النسخ

حالة HSM -> N/A - HA Group

تحقق من تعيين كل عميل HSM إلى قسم واحد على الأقل وفهم التكوينات المرتبطة بمجموعات HA لسيناريوهات التوفر العالي.

د. لسرد خوادم HSM التي تم تكوينها مع عميل LUNA، أستخدم قائمة /vtl. الموقع في الخوادم /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]#
```

ه. إذا قمنا بكتابة /vtl ثم وصلنا إلى الإدخال في الموقع /usr/safenet/lunaclient/bin، فإنه يعرض قائمة الخيارات المتوفرة باستخدام الأمر vtl.

/vtl تحقق من قوائم الأقسام المادية ل HSM التي تكون مرئية لعميل Luna.

/vtl listSlot تسرد جميع الفتحات المادية وكذلك الافتراضية (مجموعة HA) إذا كان HagGroup موجودًا ولكن معطل.

في حالة تكوين HAGgroup وتمكينها، فإنها تعرض معلومات المجموعة الظاهرية أو مجموعة الفرعية فقط للتنقل.

```
[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]#
```

طقف رهظت تناك إذا ./vtl listSlot. مادختسإ اننكمي ،ال مأ HAGgroup نيكمت مت إذا ام ةفرعمل .و
HagGroup والـ رهظت الفتحات الفعلية، فعندئذ نعلم أن HagGroup ممكنة.

طريقة أخرى لمعرفة ما إذا كانت مجموعة المشاركة ممكنة هي إصدار ./LUNACM من
/usr/safenet/lunaclient/bin ثم إصدار أمر ha l

كلمة المرور المطلوبة هي كلمة المرور الخاصة بالقسم الفعلي. في هذا الإشعار أن عرض
فتحات HA فقط هو نعم. هذا يعني أن HA نشط.

إذا كان لا، ثم على الرغم من أن HA تشكلت، فإنه ليس نشط.

يمكن تنشيط HA باستخدام الأمر HA-only enable" في وضع 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. يمكن للعملاء الوصول إلى خوادم HSM. وعادة ما تتم إستضافة خوادم HSM في DC وتتم تشغيل العديد منها.

PED هو مثل محول ملحق صغير يعرض معلومات رمز الأمان المميزة التي هي مصادقة متعددة العوامل الأمان إضافي، ما لم يكن للمستخدم كل من كلمة المرور والرمز المميز، ثم السماح بالوصول إلى بعض الوصول مثل admin وأ config.

الأمر المفرد الذي يسرد جميع معلومات الخادم هو HSM show

في هذه الإخراج، يمكننا أن نرى أن اسم جهاز HSM هو hsmlatest. تخبرنا المطالبة Lunash بأنه خادم HSM.

يمكننا رؤية إصدار برنامج HSM وهو 7.4.0-226. يمكن أن نرى معلومات أخرى مثل الرقم التسلسلي للجهاز، وهي طريقة المصادقة، أم إذا كانت PED وأ كلمة مرور، يمكننا أن نرى العدد الإجمالي للأقسام على HSM. لاحظ كما رأينا سابقا أن عملاء HSM مرتبطون بأقسام في الجهاز.

```
[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:>
```

وتتضمن الأوامر الأخرى المفيدة على خادم HSM أمر partition show.

الحقول التي يجب أن نشير إليها هي اسم القسم والرقم التسلسلي وعدد كائنات القسم. عدد كائنات القسم وه 2 هنا.

بمعنى أن أحد الكائنات المخزنة في Parititon وه زوج المفاتيح لتشفير رسائل CSMP والكائن الآخر المخزن وه شهادة CSMP.

أمر قائمة العملاء:

العميل الذي يتم التحقق منه مدرج في قائمة العملاء المسجلين في الأمر قائمة العملاء.

يقوم عرض العميل -c <client name>فقط بإدراج معلومات العميل واسم المضيف وعنوان IP والقسم الذي تم تعيين هذا العميل له. تبدو المخرجات الناتجة بهذا الشكل.

هنا، يمكننا النظر إلى اسم القسم، الرقم التسلسلي وكذلك إلى كائنات القسم. في هذه الحالة، كائن القسم = 2، يكون الكائنان هما المفتاح الخاص وشهادة 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:>
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).