FNDとのハードウェアセキュリティモジュール(HSM)統合のトラブルシューティング

内容

はじめに

このドキュメントでは、ハードウェアセキュリティモジュール(HSM)、フィールドエリアネットワーク(FAN)ソリューションとの統合、および一般的な問題のトラブルシューティングについて説明します。

ハードウェアセキュリティモジュール(HSM)

ハードウェアセキュリティモジュール(HSM)は、アプライアンス、PCIカード、クラウドの3つの形式で提供されます。ほとんどの導入では、アプライアンスバージョンが選択されます。

ソフトウェアセキュリティモジュール(SSM)

一方、ソフトウェアセキュリティモジュール(SSM)は、HSMと同様の目的を果たすソフトウェアパッケージです。これらはFNDソフトウェアにバンドルされており、アプライアンスの代わりに単純な代替手段を提供します。

HSMとSSMはどちらもFND展開のオプションコンポーネントであり、必須ではないことに注意してください。

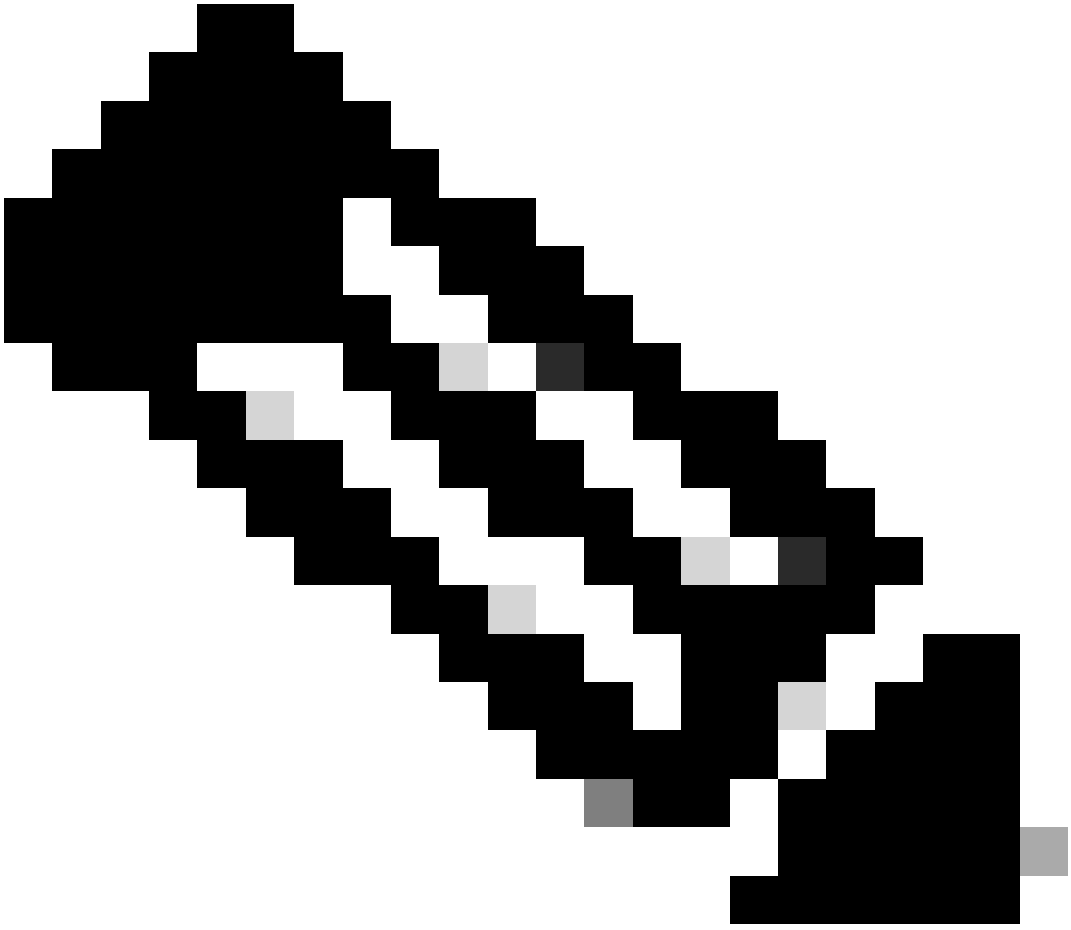
HSMの機能

FNDソリューションにおけるHSMとSSMの主な機能は、特にメーターなどのCSMPエンドポイントを使用する場合、PKIキーペアとCSMP証明書を安全に保存することです。

これらのキーと証明書は、FNDとCSMPエンドポイント間の通信を暗号化するために不可欠です。

導入に関して言えば、HSMはスタンドアロンアプライアンスですが、SSMはFNDと同じLinuxサーバまたは別のLinuxサーバにインストールできます。SSMの設定は、cgms.propertiesファイルで指定されます。

ブートアップ時に、FNDはHSM関連の情報がcgms.propertiesで指定されているかどうかに関係なく、HSMクライアントライブラリをチェックします。HSMがソリューションに含まれていない場合、ブートアップ中に見つからないHSMクライアントライブラリに関するログは無視できます。



注: HSM関連の情報は、cgms.propertiesファイルで指定する必要があります。このファイルは、FNDがOVAまたはISOのどちらを介してインストールされているかによって異なるディレクトリに配置されています。

HSMクライアントのインストール

HSMクライアントは、FNDサーバと同じLinuxサーバにインストールする必要があります。HSMクライアントソフトウェアは、ThalesのWebサイトまたはシスコのサポート契約からダウンロードできます。

FNDソフトウェアのリリースノートには、展開に必要なHSMクライアントおよびHSMソフトウェアのソフトウェアが記載されています。リリースノートの「HSMアップグレードテーブル」セクションに一覧されています。

HSMクライアントインストールファイル、構成ファイル、およびライブラリのパス：

デフォルトのインストール場所は/usr/safenet/lunaclient/binです。lunacm、vtl、ckdemoなどのほとんどのコマンドは、このパス(/usr/safenet/lunaclient/bin)から実行されます。

コンフィギュレーションファイルは、/etc/Chrystoki.confにあります。

Linuxサーバ上のFNDサーバで必要なHSM Lunaクライアントライブラリファイルへのパスは、/usr/safenet/lunaclient/jsp/lib/です。

HSMサーバー

ほとんどの導入では、HSMサーバをアプライアンスとして使用します。

HSMサーバはパーティション化する必要があり、HSMクライアントは割り当てられている特定のパーティションにのみアクセスできます。HSMサーバーは、PED認証またはパスワード認証できます。

パスワード認証では、ユーザー名とパスワードはHSMサーバー内の構成を変更するのに十分です。

ただし、PED認証されたHSMは、パスワードに加えて、変更を行うユーザーがPEDキーにアクセスする必要がある多要素認証方式です。

PEDキーはドングルのように機能し、設定を変更するためにユーザがパスワードとともに入力する必要があるPINを表示します。

showコマンドや読み取り専用アクセスなどの特定のコマンドでは、PEDキーは必要ありません。PEDキーが必要なのは、パーティションの作成などの特定の設定変更だけです。

各サーバパーティションには複数のクライアントを割り当てることができ、パーティションに割り当てられたすべてのクライアントは、そのパーティション内のデータにアクセスできます。

HSMサーバーは、さまざまなユーザーの役割を提供します。特に重要なのは、adminとCrypto Security Officerの役割です。さらに、パーティションセキュリティ担当者の役割があります。

トラブルシューティング

FNDは、HSMクライアントを使用してHSMハードウェアにアクセスします。したがって、統合には2つの部分があります。

1. HSMクライアントからHSMサーバへの通信
2. FNDからHSMクライアントへの通信

HSM統合を成功させるには、両方の要素が機能する必要があります。

HSMクライアントからHSMサーバへの通信

HSMクライアントが、HSMサーバー上のHSMパーティションに格納されたキーと証明書の情報を1つのコマンドで正常に読み取れるかどうかを確認するには、/usr/safenet/lunaclient/binにある/cmu listコマンドを使用します。

このコマンドを実行すると、HSMクライアントがHSMパーティションに格納されているキーと証明書にアクセスできるかどうかを示す出力が表示されます。

このコマンドでは、パスワードの入力を求められます。パスワードは、HSMパーティションのパスワードと同じである必要があります。

正常な出力は、次の結果のようになります。

[root@fndblr23 bin]# ./cmu list
Certificate Management Utility（64ビット）v7.3.0-165著作権(c) 2018 SafeNet。All rights reserved.

スロット0のトークンのパスワードを入力してください：*******

ハンドル=2000001 label=NMS_SOUTHBOUND_KEY
handle=2000002 label=NMS_SOUTHBOUND_KEY：証明書0
[root@fndblr23 bin]#

注：

お客様がパスワードを覚えていない場合は、次に示すように、cgms.propertiesファイルにリストされているパスワードを復号化します。

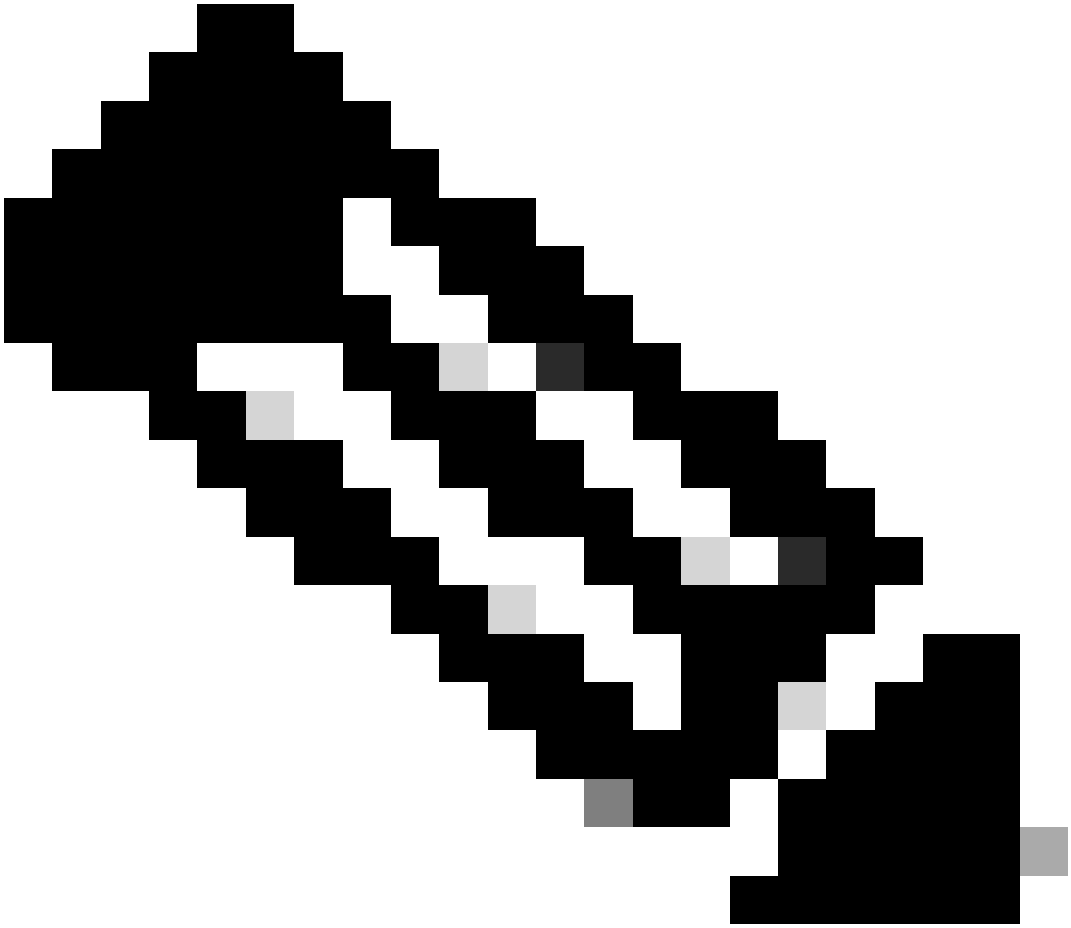
[root@fndblr23 ~]# cat /opt/cgms/server/cgms/conf/cgms.properties | grep hsm
hsm-keystore-password=qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=（必須）
hsm-keystore-name=TEST2グループ
[root@fndblr23 ~]#
[root@fndblr23 ~]# /opt/cgms/bin/encryption_util.sh decrypt qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
パスワード
[root@fndblr23 ~]#

この場合、復号化されたパスワードはPasswordexampleです

1. NTLS通信チェック：

HSMクライアントは、NTLS(Network Transport Layer Security)通信の既知のポート1792を使用してHSMサーバと通信します。このポートは確立状態にあります。

FNDサーバを実行しているLinuxサーバ上のNTLS通信のステータスと、HSMクライアントがインストールされている場所を確認するには、次のコマンドを使用します。



注:「netstat」はLinuxでは「ss」コマンドに置き換えられました

バッシュ

コードのコピー

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

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

接続が確立された状態でない場合は、基本的なNTLS通信に問題があることを示しています。

このような場合は、HSMアプライアンスにログインし、「ntls information show」コマンドを使用してNTLSサービスが実行されていることを確認するよう、お客様に伝えます。

さらに、インターフェイスでNTLSが有効になっていることを確認します。カウンタは「ntls information reset」を使用してリセットしてから、再度「show」コマンドを発行できます。

HSMアプライアンスまたはHSMサーバー：

ヤマル

コードのコピー

[hsmlatest] lunash:>ntls information show

NTLS情報：

動作ステータス：1（稼働中）

接続クライアント：1

リンク：1

成功したクライアント接続： 20095

失敗したクライアント接続： 20150

コマンドの結果：0（成功）

[hsmlatest]ルナッシュ：>

1. Luna SafenetクライアントId:

HSMクライアント(Luna Safenetクライアントとも呼ばれる)は、「/usr/safenet/lunaclient/bin」にある「。/lunacm」コマンドを使用して識別できます。このコマンドでは、クライアントに割り当てられているHSMパーティションと、設定されているハイアベイラビリティ(HA)グループも一覧表示されます。

コードのコピー

[root@fndblr23 bin]# ./lunacm

lunacm（64ビット）v7.3.0-165。著作権(c) 2018 SafeNet。All rights reserved.

インストールされているLunaクライアントのバージョンを次に示します（この例ではバージョン7.3）。

この出力には、割り当てられたHSMパーティションやHAグループ構成など、使用可能なHSMに関する情報も表示されます。

数学者

コードのコピー

スロットId -> 0

ラベル – > TEST2

シリアル番号 – > 1358678309716

モデル – > LunaSA 7.4.0

ファームウェアバージョン – > 7.4.2

設定 – > SO(PED)キーエクスポートとクローニングモードを使用したLunaユーザパーティション

スロットの説明 – > Net Token Slot

スロットId -> 4

HSMラベル – > TEST2Group

HSMシリアル番号 – > 11358678309716

HSMモデル – > LunaVirtual

HSMファームウェアバージョン – > 7.4.2

HSM構成 – > Luna Virtual HSM(PED)キー・エクスポート（クローン・モードを使用）

HSMステータス – > N/A - HAグループ

各HSMクライアントが少なくとも1つのパーティションに割り当てられていることを確認し、高可用性シナリオのHAグループに関連する構成を理解します。

d. lunaクライアントで構成されているHSMサーバを一覧表示するには、/usr/safenet/lunaclient/binにある./vtlリストServersを使用します。

```
[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. ./vtlと入力して、/usr/safenet/lunaclient/binにあるEnterキーを押すと、vtlコマンドで使用可能なオプションのリストが表示されます。

./vtl verifyは、Lunaクライアントから認識できるHSM物理パーティションを一覧表示します。

./vtl listSlots:HAGroupが構成されているが無効になっている場合は、すべての物理スロット（HAグループ）と仮想スロット（HAグループ）を一覧表示します。

HAGroupが設定され、有効になっている場合は、仮想グループまたはHAGroup情報のみが表示されます。

```
[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. HAGroupが有効かどうかを確認するには、./vtl listSlotsを使用します。 HAGroupだけが表示され、物理スロットが表示されない場合は、HAGroupが有効であることがわかります。

HAGroupが有効になっているかどうかを確認するもう1つの方法は、/usr/safenet/lunaclient/binから./lunacmを発行してからha lコマンドを発行することです

要求されたパスワードは、物理パーティションのパスワードです。この注意では、「show HA Slots」だけが「yes」になっています。これは、HAがアクティブであることを意味します。

noの場合、HAは設定されていますが、アクティブではありません。

HAをアクティブにするには、lunacmモードでコマンド「ha ha-only enable」を使用します。

```
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. HSMサーバにアクセスできます。通常、HSMサーバはDCでホストされ、その多くはPEDで動作します。

PEDは、セキュリティトークン情報を表示する小さなドングルに似ています。これは、ユーザがパスワードとトークンの両方を持っていない限り、追加のセキュリティのための多要素認証であり、adminやconfigアクセスなどの特定のアクセスは許可されません。

すべてのサーバ情報を一覧表示する単一のコマンドは、hsm showです

この出力では、hsmアプライアンスの名前がhsmlatestであることがわかります。 lunashプロンプトから、これがHSMサーバであることがわかります。

HSMソフトウェアのバージョンは7.4.0-226です。アプライアンスのシリアル番号などの他の情報や、認証方法（PEDまたはパスワード）、そのHSM上のパーティションの総数などを確認できます。先ほど見たように、HSMクライアントはアプライアンス内のパーティションに関連づけられています。

```
[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サーバ上のその他の便利なコマンドには、partition showコマンドがあります。

ここで参照する必要があるフィールドは、パーティション名、シリアル番号、およびパーティションオブジェクトのカウントです。ここでは、パーティションオブジェクトのカウントは2です。

つまり、パーティションに保存されている1つのオブジェクトがCSMPメッセージ暗号化用のキーペアで、もう1つのオブジェクトがCSMP証明書です。

client listコマンドを使用します。

チェック対象のクライアントが、client listコマンドの登録済みクライアントリストにリストされます。

client show -c <client name>は、クライアント情報、ホスト名、IPアドレス、およびこのクライアントが割り当てられているパーティションをリストするだけです。正常な出力は次のようになります。

ここでは、パーティション名、シリアル番号、およびPartitionオブジェクトを確認できます。この場合、パーティションオブジェクトは2で、2つのオブジェクトは秘密キーとCSMP証明書です。

```
[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:>
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。