Solução de problemas de integração do HSM (Hardware Security Modules) com o FND

Contents

Introdução

Este documento descreve o Hardware Security Module (HSM), a integração com a solução Field Area Network (FAN) e a solução de problemas comuns.

Módulo de segurança de hardware (HSM)

Os módulos de segurança de hardware (HSM) estão disponíveis em três formas: dispositivo, placa PCI e oferta de nuvem. A maioria das implantações opta pela versão do dispositivo.

Módulos de segurança de software (SSM)

Os módulos de segurança de software (SSM), por outro lado, são pacotes de software que servem a uma finalidade semelhante ao HSM. Eles são fornecidos com o software FND e fornecem uma alternativa simples em vez do dispositivo.

É importante observar que o HSM e o SSM são componentes opcionais nas implantações do FND e não são obrigatórios.

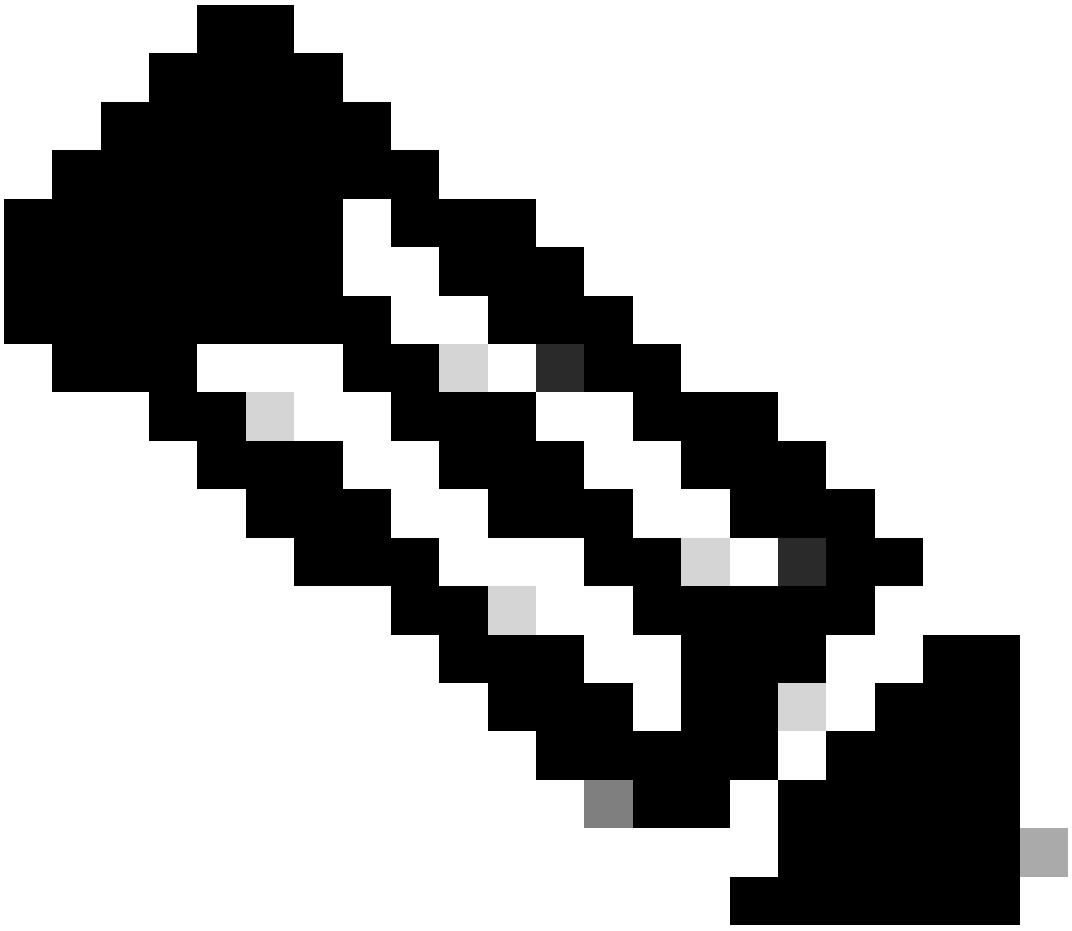
Funções do HSM

A principal função do HSM e do SSM em uma solução FND é armazenar com segurança o par de chaves PKI e o certificado CSMP, particularmente quando endpoints CSMP, como medidores, são utilizados.

Essas chaves e certificados são essenciais para criptografar a comunicação entre o FND e os endpoints do CSMP.

Em relação à implantação, o HSM é um dispositivo autônomo, enquanto o SSM pode ser instalado no mesmo servidor Linux como FND ou em um servidor Linux separado. A configuração do SSM é especificada no arquivo cgms.properties.

Durante a inicialização, o FND verifica as bibliotecas do cliente HSM, independentemente de as informações relacionadas ao HSM estarem especificadas em cgms.properties. Qualquer registro referente às bibliotecas do cliente HSM ausentes durante a inicialização poderá ser ignorado se o HSM não estiver incluído na solução.



Observação: as informações relacionadas ao HSM devem ser especificadas no arquivo cgms.properties, localizado em diretórios diferentes, dependendo se o FND está instalado via OVA ou ISO.

Instalação do cliente HSM

O cliente HSM deve ser instalado no mesmo servidor Linux em que o servidor FND está localizado. Os clientes podem fazer o download do software cliente HSM do site Thales ou através de um contrato de suporte da Cisco.

As notas de versão do software FND documentam o software necessário no cliente HSM e o software HSM para a implantação. Ele está listado na seção Tabela de upgrade do HSM para obter as notas de versão.

Caminho para arquivos de instalação, arquivos de configuração e bibliotecas do cliente HSM:

O local de instalação padrão é /usr/safenet/lunaclient/bin . A maioria dos comandos, como lunacm, vtl ou ckdemo, são executados a partir desse caminho (/usr/safenet/lunaclient/bin).

O arquivo de configuração está localizado em /etc/Chrystoki.conf .

O caminho para os arquivos de biblioteca do cliente Luna do HSM necessários pelo servidor FND em servidores Linux é /usr/safenet/lunaclient/jsp/lib/ .

Servidor HSM

A maioria das implantações utiliza o servidor HSM como um dispositivo.

O servidor HSM precisa ser particionado, e os clientes HSM têm acesso somente à partição específica à qual estão atribuídos. O servidor HSM pode ser autenticado por PED ou por senha.

Na autenticação de senha, um nome de usuário e uma senha são suficientes para alterações de configuração no servidor HSM.

No entanto, o HSM autenticado por PED é um método de autenticação multifator em que, além de uma senha, a pessoa que faz as alterações precisa acessar uma chave PED.

A tecla PED funciona como um dongle, exibindo um PIN que o usuário deve inserir junto com a senha para fazer qualquer alteração na configuração.

Para determinados comandos como show e acesso somente leitura, a tecla PED não é necessária. Somente alterações de configuração específicas, como a criação de partições, exigem a chave PED.

Cada partição de servidor pode ter vários clientes atribuídos a ela, e todos os clientes atribuídos a uma partição têm acesso aos dados dentro dessa partição.

O servidor HSM oferece várias funções de usuário, com as funções de administrador e de Crypto Security Officer sendo particularmente importantes. Além disso, há a função de diretor de segurança da partição.

Troubleshooting

O FND usa o cliente HSM para acessar o hardware HSM. Portanto, há duas partes na integração.

1. Comunicação entre cliente HSM e servidor HSM
2. FND para comunicação de cliente HSM

Ambas as partes precisam trabalhar para que a integração do HSM seja bem-sucedida.

Comunicação entre cliente HSM e servidor HSM

Para determinar se o cliente HSM pode ler com êxito as informações de chave e certificado armazenadas na partição HSM no servidor HSM usando um único comando, utilize o comando /cmu list no local /usr/safenet/lunaclient/bin.

A execução desse comando fornece saída indicando se o cliente HSM pode acessar a chave e o certificado armazenados na partição HSM.

Observe que esse comando solicita uma senha, que deve ser igual à senha da partição HSM.

Uma saída bem-sucedida se parece com este resultado:

[root@fndblr23 bin]# ./cmu list
Utilitário de Gerenciamento de Certificados (64 bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Todos os direitos reservados.

Insira a senha para o token no slot 0: *******

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

Note:

Se o cliente não se lembrar da senha, descriptografe a senha listada no arquivo cgms.properties, como mostrado aqui:

[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 descriptografar
qnBC7WGvZB5iux4BnnDDplTWzcmAxhuISQLmVRXtHBeBWF4=
Exemplo desenha
[root@fndblr23 ~]#

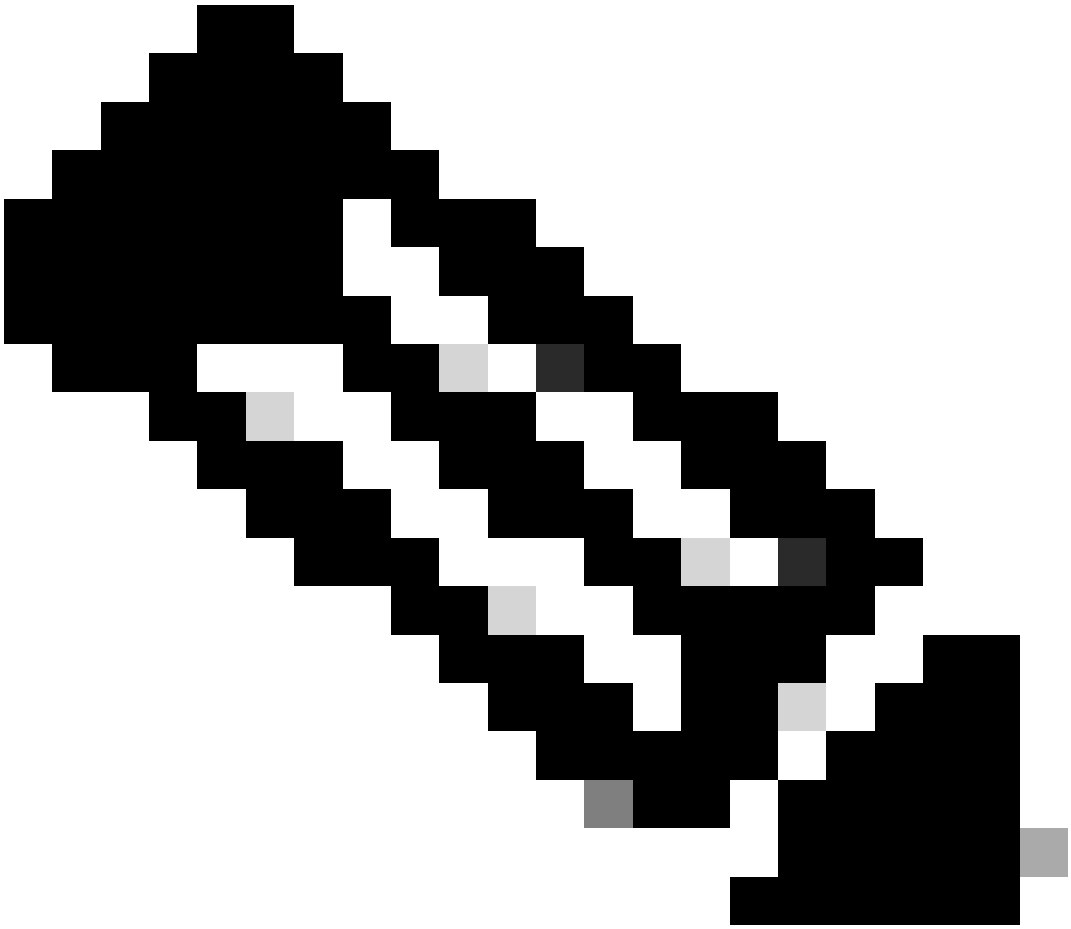
Nesse caso, a senha descriptografada é Passwordexample

1. Verificação de comunicação NTLS:

O cliente HSM se comunica com o servidor HSM usando a porta conhecida 1792 para

comunicações NTLS (Network Transport Layer Security), que está no estado estabelecido.

Para verificar o status da comunicação NTLS no servidor Linux executando o servidor FND e onde o cliente HSM está instalado, use este comando:



Observação: "netstat" foi substituído pelo comando "ss" no Linux

---

bash

Copiar código

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

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

Se a conexão não estiver no estado estabelecido, isso indica um problema com a comunicação NTLS básica.

Nesses casos, aconselhe o cliente a fazer login no dispositivo HSM e verifique se o serviço NTLS está em execução usando o comando "ntls information show".

Além disso, certifique-se de que as interfaces estejam ativadas para NTLS. Você pode redefinir os contadores usando "ntls information reset" e, em seguida, emitir o comando "show" novamente.

No dispositivo HSM ou no servidor HSM:

yaml

Copiar código

[hsmlatest] lunash:>exibição de informações ntls

Informações de NTLS:

Status operacional: 1 (ativado)

Clientes conectados: 1

Links: 1

Conexões de Clientes Bem-sucedidas: 20095

Conexões de Clientes com Falha: 20150

Resultado do Comando: 0 (Êxito)

[hsmlatest] lunash:>

1. Identificação do cliente Luna Safenet:

O cliente HSM, também conhecido como cliente Luna Safenet, pode ser identificado usando o comando "./lunacm" no local "/usr/safenet/lunaclient/bin". Esse comando também lista a partição HSM atribuída ao cliente e qualquer grupo de alta disponibilidade (HA) configurado.

Copiar código

[root@fndblr23 bin]# ./lunacm

lunacm (64 bits) v7.3.0-165. Copyright (c) 2018 SafeNet. Todos os direitos reservados.

A versão do cliente Luna instalado é indicada aqui (neste exemplo, versão 7.3).

A saída também exibe informações sobre os HSMs disponíveis, incluindo as partições HSM atribuídas e a configuração do grupo HA.

matemática

Copiar código

ID do Slot -> 0

Rótulo -> TESTE2

Número de série -> 1358678309716

Modelo -> LunaSA 7.4.0

Versão do firmware -> 7.4.2

Configuração -> Luna User Partition With SO (PED) Key Export With Cloning Mode (Exportação da partição do usuário com SO (PED) com modo de clonagem)

Descrição do slot -> Net Token Slot

ID do Slot -> 4

Rótulo de HSM -> TEST2Group

Número de série do HSM -> 11358678309716

Modelo HSM -> LunaVirtual

Versão do firmware do HSM -> 7.4.2

Configuração do HSM -> Exportação da chave do Luna Virtual HSM (PED) com modo de clonagem

Status do HSM -> N/D - Grupo HA

Verifique se cada cliente HSM está atribuído a pelo menos uma partição e compreenda as configurações relacionadas aos grupos HA para cenários de alta disponibilidade.

d. Para listar os servidores HSM configurados com o cliente luna, use ./vtl listServers no local /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 digitarmos ./vtl e pressionarmos enter no local /usr/safenet/lunaclient/bin, ele mostrará a lista de opções disponíveis com o comando vtl.

./vtl verify lista as partições físicas do HSM que são visíveis para o cliente Luna.

./vtl listSlots lista todos os slots físicos e virtuais (Grupo HA) se o HAGroup estiver configurado,

mas desabilitado.

Se o HAGroup estiver configurado e habilitado, ele mostrará apenas as informações do grupo virtual ou do 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. Para descobrir se o HAGroup está habilitado ou não, podemos usar ./vtl listSlots. Se ele mostrar apenas o HAGroup e não mostrar os slots físicos, saberemos que o HAGroup está habilitado.

Outra maneira de descobrir se o HAGroup está habilitado é emitir o comando ./lunacm de /usr/safenet/lunaclient/bin e, em seguida, emitir o comando ha l

A senha solicitada é a senha da partição física. Neste aviso, o único show HA Slots é yes. Isso significa que o HA está ativo.

Se for no, embora o HA esteja configurado, ele não está ativo.

O HA pode ser ativado usando o comando "ha ha-only enable" no modo 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. Os clientes têm acesso aos servidores HSM. Geralmente, os servidores HSM são hospedados em DC e muitos deles são operados por PED.

O PED é como um pequeno dongle que exibe informações de token de segurança, que são autenticação de vários fatores para segurança adicional, a menos que o usuário tenha a senha e o token, então determinados acessos, como admin ou config, não são permitidos.

O único comando que lista todas as informações do servidor é hsm show

Nesta saída, podemos ver que o nome do dispositivo hsm é hsmlatest. O prompt lunash nos diz que é o servidor HSM.

Podemos ver a versão do software HSM, que é 7.4.0-226. Podemos ver outras informações, como o número de série do dispositivo, e qual é o método de autenticação, se é PED ou senha, e podemos ver o número total de partições nesse HSM. Observe como vimos anteriormente que os clientes HSM estão associados a partições no dispositivo.

```
[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:>
```

Outros comandos úteis no servidor HSM incluem o comando partition show.

Os campos aos quais devemos fazer referência são o nome da partição, o número de série e a contagem de objetos da partição. A contagem de objetos da partição é 2 aqui.

Ou seja, um objeto armazenado na partição é o par de chaves para a criptografia de mensagens CSMP e outro objeto armazenado é o certificado CSMP.

comando lista de clientes:

O cliente que estamos procurando está listado na lista de clientes registrados no comando client list.

client show -c <nome do cliente> lista apenas as informações desse cliente, o nome do host, o endereço IP e a partição à qual esse cliente está atribuído. Saídas bem-sucedidas se parecem com isso.

Aqui, podemos observar o nome da partição, o número de série e também os objetos Partition. Nesse caso, o objeto de partição = 2, sendo os dois objetos a chave privada e o certificado 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:>
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.