FIRST TECH®

Construindo relações duradouras

HSM nShield Connect

Índice

1. RFS

1.1. Configuração

Essa etapa consiste em configurar o endereço IP do HSM nShield.

NSHIELD - configuração do endereço IPv4 HSM nShield.

```
1-1-1-1-1-2

Static IPv4 Address
       <IP_NSHIELD>
       <MASCARA_NSHIELD>
       Next – Finish
```

1.2. Instalação

Essas etapas consistem no processo de instalação do software da nCipher no Servidor RFS.

RFS – liberando o acesso no firewall na porta 9004

```
$ sudo firewall-cmd --zone=public --add-port=9004/tcp --permanent
$ sudo firewall-cmd --reload
$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: dhcpv6-client ssh
  ports: 9004/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

RFS – montando o arquivo ISO para poder instalar os softwares necessários.

```
$ sudo mount /dev/cdrom /mnt/
```

RFS – acessando o diretório raiz do GNU/Linux.

```
$ cd /
```

RFS – visualizando o conteúdo do diretório.

```
$ ls /mnt/linux/libc6_11/amd64/nfast/

ctls dsserv hwcrhk hwsp javasp jcecsp nhfw pkcs11 ratls snmp version.txt
```

```
```

RFS – descompactando os softwares.

```
$ sudo find /mnt/linux/libc6_11/amd64/nfast/ -type f | egrep '.tar' | sudo xargs -I {} sudo tar xf {}
```

RFS – executando o software de instalação.

```
$ sudo /opt/nfast/sbin/install
```

1.3. Sincronismo

Essas etapas consistem no sincronismo das informações entre o HSM nShield e servidor RFS.

RFS – coletando o ESN do HSM nShield.

```
$ /opt/nfast/bin/anonkneti <IP_NSHIELD>
      ESN
```

RFS – configurando a relação de confiança entre o servidor RFS e HSM nShield.

```
$ sudo /opt/nfast/bin/rfs-setup <IP_NSHIELD> <ESN>
```

NSHIELD – configurando no HSM nShield, o endereço IP do servidor RFS.

```
1-1-3-1

      Define IPv4 RFS
      <IP_RFS>
      Finish
```

2. Client

2.1. Instalação

Essas etapas consistem no processo de instalação do software da nCipher no Servidor RFS.

CLIENT – liberando o acesso no firewall na porta 9004

```
$ sudo firewall-cmd --zone=public --add-port=9004/tcp --permanent
$ sudo firewall-cmd --reload
$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: dhcpv6-client ssh
  ports: 9004/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

CLIENT – montando o arquivo ISO para poder instalar o software.

```
$ sudo mount /dev/cdrom /mnt/
```

CLIENT – acessando o diretório raiz.

```
$ cd /
```

CLIENT – visualizando o conteúdo do diretório do software de instalação.

```
$ ls /mnt/linux/libc6_11/amd64/nfast/
ctls dsserv hwcrhk hwsp javasp jcecsp nhfw pkcs11 ratls snmp version.txt
```

CLIENT – descompactando os softwares para a instalação.

```
$ sudo find /mnt/linux/libc6_11/amd64/nfast/ -type f | egrep '.tar' | sudo xargs -I {} sudo tar xf {}
```

CLIENT – executando o software de instalação.

```
$ sudo /opt/nfast/sbin/install
```

2.2. Sincronismo nShield => Client

CLIENT – coletando o ESN do HSM nShield.

```
$ /opt/nfast/bin/anonkneti <IP_NSHIELD>
      ESN
```

CLIENT – configurando a relação de confiança entre o servidor Client e o HSM nShield.

```
$ sudo /opt/nfast/bin/nethsmenroll <IP_NSHIELD> <ESN>
```

NO NSHIELD – configurando o endereço IP do servidor Client.

```
1-1-4-1
      <IP_CLIENT> - <Unprivileged>
```

CLIENT – inicializando o serviço.

```
$ sudo /opt/nfast/bin/config-serverstartup -s
```

CLIENT – reinicializando o serviço Hardserver.

```
$ sudo /opt/nfast/sbin/init.d-ncipher restart
```

2.3. Sincronismo RFS => Client

RFS – configurando a relação de confiança entre o servidor Client com o servidor RFS.

```
$ sudo /opt/nfast/bin/rfs-setup --gang-client --write-noauth <IP_CLIENT>
```

CLIENT – indicando o endereço IP do servidor RFS.

```
$ sudo /opt/nfast/bin/rfs-sync --setup --no-authenticate <IP_RFS>
```

CLIENT – executando o sincronismo entre os servidores Client e o servidor RFS.

```
$ sudo /opt/nfast/bin/rfs-sync --update
```

3. Security World

3.1. Criação do Security World

NSHIELD – criação do Security World no HSM nShield.

```
3-2-1-(1/1)
```

3.2. Sincronismo nShield => Client

CLIENT – executando o sincronismo entre o servidor Client e o servidor RFS.

```
$ sudo /opt/nfast/bin/rfs-sync --update
```

CLIENT – validando as configurações.

```
$ sudo /opt/nfast/bin/enquiry
$ sudo /opt/nfast/bin/nfkminfo
```

4. Teste

4.1. Chaves de criptografia

Criação de chaves de criptografia para teste.

CLIENT – criando chaves de criptografia para teste.

```
$ sudo /opt/nfast/bin/generatekey --generate simple
      client_a
      client_b
```

CLIENT – visualizando as chaves de criptografia que foram criadas no passo anterior e que ainda estão armazenadas no servidor Client.

```
$ sudo /opt/nfast/bin/nfkminfo -k simple
      Key listing AppName simple (2 keys):
      AppName simple               Ident client_b
      AppName simple               Ident client_a
```

RFS – visualizando as chaves de criptografia que foram criadas

Não existe nenhuma chave de criptografia no servidor RFS pois as chaves ainda estão armazenadas no servidor Client.

```
$ sudo /opt/nfast/bin/nfkminfo -k simple
      Key listing AppName simple (0 keys):
```

CLIENT – executando o comando de sincronismo entre o servidor Client com o servidor RFS.

```
$ sudo /opt/nfast/bin/rfs-sync --update
$ sudo /opt/nfast/bin/rfs-sync --commit
$ sudo /opt/nfast/bin/rfs-sync --update
```

RFS – visualizando as chaves de criptografia que foram criadas no servidor Client e foram sincronizadas com o servidor RFS.

```
$ sudo /opt/nfast/bin/nfkminfo -k simple
      Key listing AppName simple (2 keys):
      AppName simple               Ident client_a
      AppName simple               Ident client_b
```

CLIENT – visualizando as chaves de criptografia que estão armazenadas.

```
$ sudo /opt/nfast/bin/nfkminfo -k simple
      Key listing AppName simple (2 keys):
      AppName simple               Ident client_a
      AppName simple               Ident client_b
```

5. Rease Notes

Autor	Descrição	Data
Caio Ferreira	Primeira versão	30/06/2020
Caio Ferreira	Tabela nos comandos para simular um terminal	06/07/2020
Caio Ferreira	Firewall	20/01/2021