

**HSM nShield Connect**

Índice

[1. RFS 3](#_Toc63684013)

[1.1. Configuração 3](#_Toc63684014)

[1.2. Instalação 3](#_Toc63684015)

[1.3. Sincronismo 4](#_Toc63684016)

[2. Client 5](#_Toc63684017)

[2.1. Instalação 5](#_Toc63684018)

[2.2. Sincronismo nShield => Client 6](#_Toc63684019)

[2.3. Sincronismo RFS => Client 6](#_Toc63684020)

[3. Security World 7](#_Toc63684021)

[3.1. Criação do Security World 7](#_Toc63684022)

[3.2. Sincronismo nShield => Client 7](#_Toc63684023)

[4. Teste 8](#_Toc63684024)

[4.1. Chaves de criptografia 8](#_Toc63684025)

[5. Rease Notes 9](#_Toc63684026)

# RFS

## 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 |

## 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 |

## 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 |

# Client

## 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 |

## 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 |

## 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 |

# Security World

## Criação do Security World

# **NSHIELD** – criação do Security World no HSM nShield.

|  |
| --- |
| 3-2-1-(1/1) |

## 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 |

# Teste

## 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 |

# 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 |