

**HSM nShield – Instalação MS-Windows**

Índice

[1. RFS 3](#_Toc54373264)

[1.1. Configuração 3](#_Toc54373265)

[1.2. Instalação 3](#_Toc54373266)

[1.3. Sincronismo 4](#_Toc54373267)

[2. Client MS-Windows 5](#_Toc54373268)

[2.1. Instalação 5](#_Toc54373269)

[2.2. Sincronismo nShield => Client 5](#_Toc54373270)

[2.3. Sincronismo RFS => Client 5](#_Toc54373271)

[3. Security World 7](#_Toc54373272)

[3.1. Criação do Security World 7](#_Toc54373273)

[3.2. Sincronismo nShield => Client 7](#_Toc54373274)

[4. nCipher provider 8](#_Toc54373275)

[5. Rease Notes 8](#_Toc54373276)

# 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

<**10.20.60.73**>

<**255.255.255.0**>

Next – Finish

## Instalação

Essas etapas consistem no processo de instalação do software da nCipher no Servidor RFS. Esta sendo utilizado a distribuição GNU/Linux Debian como sistema operacional do computador ou máquina virtual.

# **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 10.20.60.73  **ESN** |

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

|  |
| --- |
| $ sudo /opt/nfast/bin/rfs-setup 10.20.60.73 <**ESN>** |

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

1-1-3-1

Define IPv4 RFS

<**10.20.60.74**>

Finish

# Client MS-Windows

## Instalação

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

# **CLIENT** – executando o software de instalação.

|  |
| --- |
| (…)\SecWorld-Win-12.40\nShield\_Win\setup.exe |

## Sincronismo nShield => Client

# **CLIENT** – coletando o ESN do HSM nShield.

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>anonkneti.exe 10.20.60.73  **ESN** |

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

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>nethsmenroll.exe --force 10.20.60.73 **<ESN>** |

# **NO NSHIELD –** configurando o endereço IP do servidor Client.

1-1-4-1

<**10.212.134.220**> - <**Unprivileged**>

# **CLIENT** – inicializando o serviço.

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>config-serverstartup.exe -s |

# **CLIENT** – reinicializando o serviço Hardserver.

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>net stop "nfast server"  C:\Program Files (x86)\nCipher\nfast\bin>net start "nfast server" |

## 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 10.212.134.220 |

# **CLIENT** – indicando o endereço IP do servidor RFS.

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>rfs-sync.exe --setup --no-authenticate 10.20.60.74 |

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

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>rfs-sync.exe –-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.

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>rfs-sync.exe –-update |

# **CLIENT** – validando as configurações.

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin>enquiry.exe  C:\Program Files (x86)\nCipher\nfast\bin>nfkminfo.exe |

# nCipher provider

1. copiar o arquivo nCipherKM.jar (C:\Program Files (x86)\nCipher\nfast\java\classes) para <caminho do Java>/jre/lib/ext; (exemplo: C:\Program Files (x86)\Java\jre1.8.0\_201\lib\ext)
2. editar o arquivo: <caminho Java/jre/lib/security/java.security> como primeiro provider: security.provider.1=com.ncipher.provider.km.nCipherKM
3. Testar com o comando: java com.ncipher.provider.InstallationTest
4. Testar com o comando: C:\Program Files (x86)\nCipher\nfast\bin>config-serverstartup.exe -sp
5. Restart do hardserver:

net stop "nfast server" / net start "nfast server"

# Rease Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 30/06/2020 |
| Caio Ferreira | Tabela nos comandos para simular um terminal | 06/07/2020 |