

**HSM nShield Connect**

Índice

[1. Estrutura do sistema 3](#_Toc47023401)

[1.1. Relação Client-nShield-RFS. 4](#_Toc47023402)

[2. Diretórios base 5](#_Toc47023403)

[2.1. Diretório /opt/nfast/bin 5](#_Toc47023404)

[2.2. Diretório /opt/nfast/sbin 5](#_Toc47023405)

[2.3. Diretório /opt/nfast/kmdata 5](#_Toc47023406)

[2.4. Diretório /opt/nfast/log 5](#_Toc47023407)

[3. Procedimento de troubleshooting 6](#_Toc47023408)

[3.1. Tabela de comandos para troubleshooting: 6](#_Toc47023409)

[3.2. Coleta de informações troubleshooting: 7](#_Toc47023410)

[4. Procedimento de instalação de um servidor Client 10](#_Toc47023411)

[5. Procedimento para habilitação do uso da API JAVA 10](#_Toc47023412)

[6. Health Check do ambiente nShield 11](#_Toc47023413)

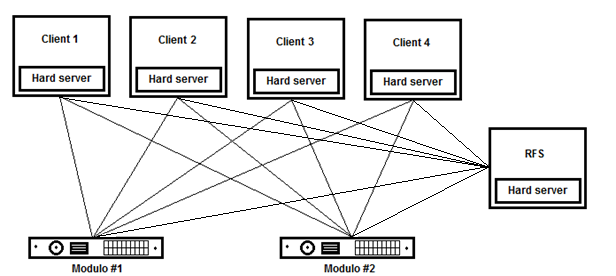
[6.1. Tabela de comando para Health Check 11](#_Toc47023414)

[7. Rease Notes 12](#_Toc47023415)

# Estrutura do sistema

O nShield Connect é um HSM de propósitos genéricos que trabalha na rede e é acessado a partir de servidores Clients pré-selecionados que fazem parte de um ambiente seguro chamado “*Security World*”.

Esta estrutura servidor Client-HSM nShield se dá da seguinte maneira:



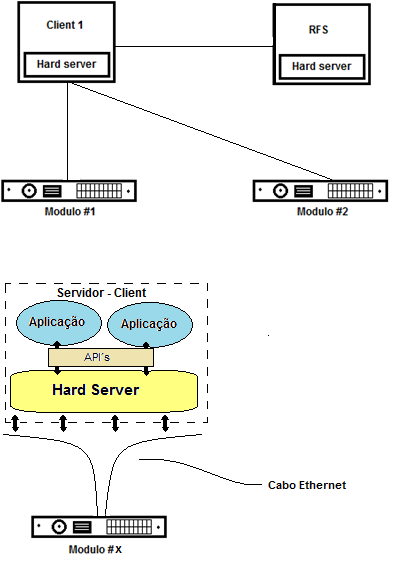
Na figura acima podemos observar um ambiente em que todos os servidores C*lients* tem um serviço “*Hard server*” ativo que simula a interface de comunicação com o HSM nShield, sem este serviço não há conexão, consequentemente não há resposta a nenhum comando de criptografia, assinatura, verificação de link ou verificação do Security World. É muito importante que este ambiente esteja em harmonia para que todo o sistema funcione de maneira correta.

Na figura podemos observar também um elemento chamado RFS (*Remote File System*). Toda unidade deve ter um servidor Remote File System onde são armazenados os arquivos de LOGs, os arquivos de configurações dos servidores HSM´s, as feature-enebling dos equipamentos, o Security World e os dados de chaves deste Security World. O servidor RFS pode ou não ser um servidor Client do servidor HSM, sendo assim, qualquer computador que esteja na mesma rede do HSM pode servir como um servidor RFS.

Um servidor RFS pode conter dados de vários appliance nShields, porém um appliance nShield tem somente um servidor RFS.

## Relação Client-nShield-RFS.

Abaixo podemos observar um ecossistema onde temos 01 servidor Client, 01 servidor RFS e 02 appliance nShields.



O servidor Client se comunica com o appliance nShield a partir do serviço Hardserver, que faz a comunicação e interface de suas aplicações com as funcionalidades do aparelho. Quando é gerado algum tipo de Log, alteração de configuração, geração de chave etc. o servidor Client se reporta ao servidor RFS que faz suas devidas alterações em seus diretórios.

# Diretórios base

|  |  |
| --- | --- |
| Comandos de teste | /opt/nfast/bin |
| Comandos do sistema | /opt/nfast/sbin |
| Aplicação JAVA | /opt/nfast/java |
| Key Management Data | /opt/nfast/kmdata/ |
| Log Files | /opt/nfast/log/ |

Pode-se tomar os Diretórios acima como diretórios base para procurarmos evidências e informações do aparelho, da conexão do ambiente, dos logs e das features e licenças.

## Diretório /opt/nfast/bin

Neste diretório concentra os comandos de teste e checagem dos módulos e serviço Hardserver, criptografia, assinatura, geração de chaves, geração de *Security Wolrd*, entre outros

## Diretório /opt/nfast/sbin

Neste Diretório encontram-se os comandos relacionados ao sistema como reinicialização do hardserver init.c-ncipher restart.

## Diretório /opt/nfast/kmdata

A infra-estrutura do *Security World* armazena material de chaves criptografados no servidor RFS e nos servidores Clients*.* Para multiplos clients utilizarem o mesmo *Security World* o administrador do sistema deve garantir que estes arquivos serão copiados para todos os clientes e atualizado quando necessário.

Se um Security World é feito em um modulo, os arquivos relacionados a este ambiente são gerados automaticamente e enviados para um diretório especifico /opt/nfast/kmdata/local, neste diretório também são gerados arquivos temporários, e configurações gerais referentes ao *Security World,* como informações do OCS (operation card system).

## Diretório /opt/nfast/log

Todos os logs dos módulos como tampers, reboots, mudanças de configuração, ações do servidor Hard Server etc., são armazenados neste diretório.

Existem dois tipos de Logs.:

* **System Log**
* **Hardserver log**

Os **System Logs** são informações como diretórios que foram gerados pelo módulo no servidor RFS, configurações que foram alteradas em config.files ou qualquer hash do *Security World,* reboots, comandos que não foram executados devido a não privilégio de usuário e ação de algum executável.

Os **Hardserver logs** armazenam informações sobre sockets privilegiados ou não (priv port 9001, non-priv port 9000) utilizados pelo serviço *Hardserver* para realizar comunicações, quando este foi reinicializado (ou resetado) e quantas vezes e demais eventos relacionados ao serviço. Estes logs são gerados e enviados para o diretório Log caso configure o modulo como “**Append**”, caso contrário estes poderão ser vistos somente no painel frontal do appliance nShield.

# Procedimento de troubleshooting

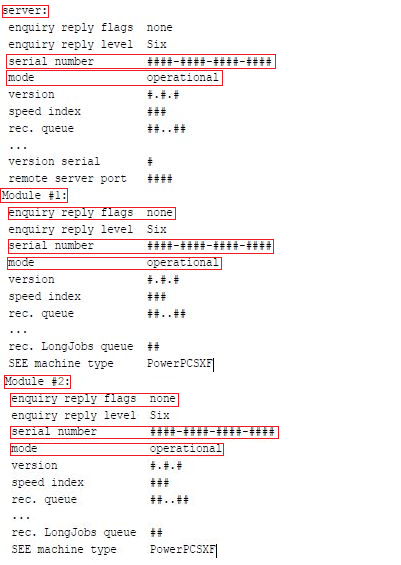
Conhecendo a infraestrutura do ambiente, devemos utilizar os procedimentos de troubleshooting abaixo para detectar de forma eficiente a causa do problema testando todos os módulos que compõem o sistema:

## Tabela de comandos para troubleshooting:

|  |  |
| --- | --- |
| Utilitário | Função |
| enquiry | Obter informações sobre o serviço *Hardserver* e os módulos conectados  Use esta ferramenta para:   * Checar se o software está instalado corretamente. * Checar a versão do firmware * Checar se o Remote Operator está habilitado. |
| Ncversions | Obter e verificar as versões dos componentes do Security World instalados. Este utilitário lista as seguintes informações:   * Versão de todos os componentes, independentemente se estão instalados individualmente ou como parte de um pacote de componentes. * Versão de cada pacote de componentes. |
| stattree | Obter as estatísticas colhidas pelo Security World dos servers e módulos. |
| fwcheck | Verificar o firmware instalado em um módulo |
| nfkminfo | Obtém informações sobre um Security World e seus cartões e chaves associados. |
| kmfile-dump | Obter informações sobre a gerência das chaves do arquivo de gerência de chaves do Security World. |

## Coleta de informações troubleshooting:

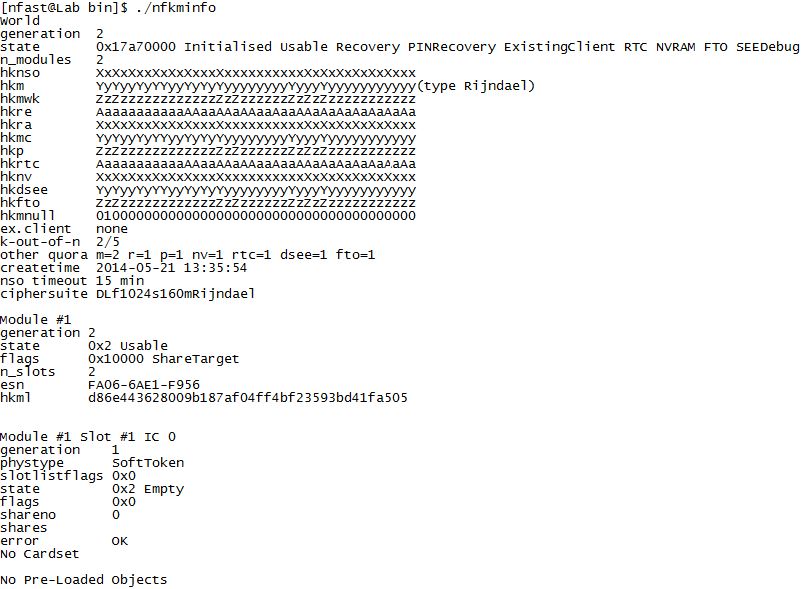
A partir o path **/opt/nfast/bin/** executar o comando **enquiry.** Este comando faz uma busca e retorna informações do serviço Hardserver e módulos conectados a ele. Ao executar este comando teremos um retorno semelhante à figura abaixo.



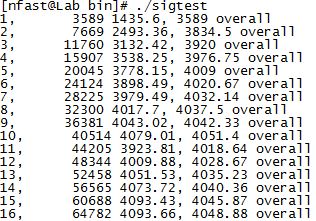
Verificar se o servidor se encontra em ***operacional***. Se estiver diferente deve-se reinicializar o serviço Hardserver (**path**: /opt/nfast/sbin/ | **comando**: ./init.d-ncipher restart).

Verificar se os módulos se encontram em ***operacional.*** Isto garante que os módulos estão se comunicando com o serviço H*ardserver.* No caso do modulo não estar em***Operacional*** deve-se inicializar um troubleshooting do HSM (módulo), para verificar os possíveis problemas.

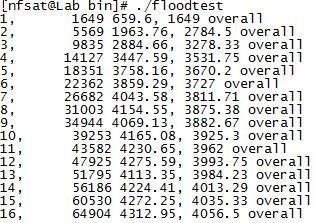
**./nfkminfo:** O serviço *Hardserver* faz uma busca nos documentos do servidor RFS (pasta local e pasta config) e checa o status do servidor Client em relação ao *Security World* em que ele está atrelado, evidenciando as chaves que o compõem, se o módulo está em estado *Usable* em relação ao servidor C*lient* ou não. Em resumo, com este comando podemos observar se o módulo #*X* está disponível para uso do servidor C*lient* e se os dados do *Security World* estão devidamente evidenciados.



**./sigtest**: Este é um teste de stress para assinaturas, com este comando o HSM irá executar uma serie de sucessivas assinaturas ao qual é incrementado o tamanho da chave conforme o teste roda. Pode-se observar a variação crescente do tamanho da assinatura pelo tempo de demora à medida que o teste corre, este teste possui o objetivo de testar a velocidade do módulo na utilização de chaves RSA e DSA.



**./floodtest:** Realiza um teste de rapidez do hardware utilizando a exponenciação modular, também é um comando para estressar o funcionamento do módulo aumentando a carga de teste ao passo que o comando se executa.



Para uma ação imediata de um troubleshooting podemos utilizar estes 4 comandos citados acima como os principais logs a serem coletados.

**/opt/nfast/bin/enquiry:** Comando que nos fornece informações sobre o link do servidor C*lient* até os módulos (HSM nShield) e sobre o serviço *Hardserver* no servidor.

**/opt/nfast/bin/nfkminfo:** Comando que nos fornece informações sobre o *Security World* e à disponibilização dos módulos quando a este Security World.

**/opt/nfast/bin/sigtest:** Comando que nos fornece informações quanto ao desempenho do hardware no que se diz respeito a assinaturas RSA e DSA, também podemos verificar a partir deste comando qual dos módulos estão e não estão respondendo à comandos de stress.

**/opt/nfast/bin/floodtest:** Comando que nos fornece informações quando ao desempenho do hardware no que se diz respeito à stress test de exponenciação modular, também utilizado no teste de qual módulo está respondendo aos comandos vindos do client e quais não estão.

**OBS:** Para todos os comandos acima é essencialmente necessário que o serviço **H*ardserver*** que realiza a intermediação dos servidores Clients com os módulos esteja sendo executado, caso contrário não teremos esta comunicação e consequentemente não teremos nenhum resultado, por mais saudável que esteja o nShield. Caso seja necessário o serviço *hard server* pode ser reiniciado utilizando o comando **init.d-ncipher restart,** este levará à reinicialização do serviço Hardserver.

# Procedimento de instalação de um servidor Client

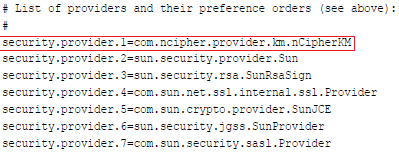
* **/opt/nfast/bin/anonkneti <IP do HSM>** **🡪** Irá gerar um <ESN> <hash>
* **/opt/nfast/bin/nethsmenroll - - force <IP do HSM> <ESN> <hash>** **🡪** Irá forçar a comunicação do client com o módulo.
* **/opt/nfast/bin/rfs-sync --setup --no-authenticate <rfs IP address> 🡪** Irá sincronizarcom o RFS.
* **/opt/nfast/bin/config-serverstartup –sp 🡪** Habilita a API Java se comunicar via TCP com os módulos.

# Procedimento para habilitação do uso da API JAVA

Para a utilização do JAVA como API temos que seguir os seguintes passos para a instalação do provider nCipher no diretório local JAVA do seu servidor de modo que o modulo possa reconhecê-lo.

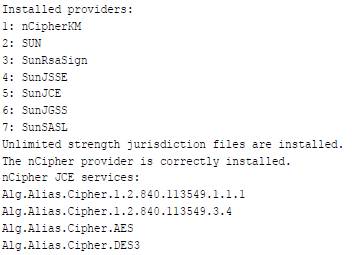
Primeiramente temos que copiar o arquivo **nCipherKM.jar** que se encontra no diretório /opt/nfast/java para o diretório local do seu servidor referente ao JAVA, se você utiliza JDK o diretório é .../jre/lib/ext se utiliza JRE o diretório é .../lib/ext.

Feito isso, o próximo passo é adicionar o provider nCipherKM no arquivo de configuração de segurança Java **java.security:**



Após as devidas mudanças nos diretórios do Java é necessário testar a instalação dele rodando o comando:

*java com.ncipher.provider.InstallationTest*



Quando o provider Java estiver aparecendo como o primeiro da lista em termos de prioridade o próximo passo é rodar o comando **/opt/nfast/bin/config-serverstartup -sp**

# Health Check do ambiente nShield

Para healthcheck do ambiente Security World basta observar se todas as pastas **/opt/nfast/kmdata/local** estão com os mesmos arquivos para assegurar a linearidade do sistema*.*

No comando **/opt/nfast/enquiry** deve-se observar a forma estrutural em que se apresentam os módulos e o servidor (Hardserver) se eles estão operacionais ou não.

🡪 **Server:** Se o servidor não estiver operacional deve-se checar:

1. Se o serviço do *Hardserver* está de fato “inicializado” na lista de serviços do servidor;
2. Se as regras de firewall para as portas lógicas 9000, 9001 e 9004 estão bidireccionalmente liberadas,
3. Se existe algum tamper relacionado à temperatura ou à reboot do nShield e executar o comando **init.d-ncipher restart** com usuário nfast.

🡪 **Modulo #X:** Se algum dos módulos não responder como o esperado será necessário observar:

1. O link até o ele (cabo Ethernet, ping, liberação das portas 9000 e 9001 bidireccionalmente, interface de redes do servidor, se o dispositivo se encontra de fato ligado etc.);
2. Se há alguma anormalidade nos logs de temperatura que possam vir a ter desligado ou rebotado o HSM;
3. Se houve alguma queda no sistema (servidor, rede, energia) que possam ter finalizado a comunicação ethernet a partir do switch onde está plugado o cabo host do nShield,
4. Checar se o serviço Hardserver está rodando.

## Tabela de comando para Health Check

|  |  |
| --- | --- |
| Utilitário | Função |
| cryptest | Testar os mecanismos de criptografia simétricos definidos. |
| des\_kat | Realizar testes DES de resposta sabida. Este utilitário indica se algum deles falhar. |
| floodtest | Realizar um teste de velocidade usando exponenciação modular. |
| kptest | Testar a consistência da encriptação e decriptação, ou de verificação de assinaturas, com algoritmos RSA e DSA. |
| ncthread-test | Teste de stress dos módulos e teste da API nCore para o suporte de conexões concorrentes. |
| perfcheck | Executar diversos testes para medir o desempenho de criptografia de um módulo. |
| sigtest | Medir a velocidade de um módulo usando assinaturas RSA ou DSA ou assinaturas de verificação. |

# Rease Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Vinícius Priori e Silva e Eduardo Campos | Primeira versão | 07/07/2015 |
|  |  |  |