

**Luna**

Índice

[1. Info 3](#_Toc69831503)

[2. Partição 4](#_Toc69831504)

[3. Configuração 5](#_Toc69831505)

[3.1. Várias Etapas 5](#_Toc69831506)

[3.2. Única Etapa 7](#_Toc69831507)

[4. Partição e Inicialização PSO 11](#_Toc69831508)

[5. Inicialização CO 12](#_Toc69831509)

[6. Ativação 13](#_Toc69831510)

[7. Transporte 14](#_Toc69831511)

[7.1. Transport 14](#_Toc69831512)

[7.2. Recovery 14](#_Toc69831513)

[8. Release Notes 15](#_Toc69831514)

# Info

|  |
| --- |
| •the HSM Admin or SO (blue PED Key)  •the Partition Owner or Crypto Officer (black PED Key)  •the cloning Domain (red PED Key)  •the Remote PED Key (orange PED Key)  •the Secure Recovery Key (purple PED Key)  •the Audit key (white PED Key) |

# Partição

# login

|  |
| --- |
| [luna-ft] lunash:>hsm login  Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.  'hsm login' successful.  Command Result : 0 (Success) |

# criar

|  |
| --- |
| [luna-ft] lunash:>partition create -partition lunalab  Type 'proceed' to create the partition, or  'quit' to quit now.  > proceed  'partition create' successful.  Command Result : 0 (Success) |

# exibir

|  |
| --- |
| [luna-ft] lunash:>partition show -partition lunalab  Partition Name: lunalab  Partition SN: 1372869334793  Partition Label:  Partition SO is not initialized.  Crypto Officer is not initialized.  Crypto User is not initialized.  Legacy Domain Has Been Set: no  Partition Storage Information (Bytes): Total=3240938, Used=0, Free=3240938  Partition Object Count: 0  Command Result : 0 (Success) |

# Configuração

## Várias Etapas

# criar certificado no cliente

|  |
| --- |
| VTL.exe createcert -n 10.20.71.28  sudo /usr/safenet/lunaclient/bin/vtl createCert -n 10.20.60.79  vtl (64-bit) v7.4.0-226. Copyright (c) 2018 SafeNet. All rights reserved.  Private Key created and written to: /usr/safenet/lunaclient/cert/client/10.20.60 .79Key.pem  Certificate created and written to: /usr/safenet/lunaclient/cert/client/10.20.60 .79.pem |

# copia certificado do HSM para o client

|  |
| --- |
| PSCP.EXE admin@10.20.60.77:server.pem .  sudo /usr/safenet/lunaclient/bin/pscp admin@10.20.60.77:server.pem .  admin@10.20.60.77's password:  server.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100% |

# adicionar o HSM na lista de servidores local

|  |
| --- |
| VTL.exe addserver -n 10.20.60.77 -c server.pem  sudo /usr/safenet/lunaclient/bin/vtl addServer -n 10.20.60.77 -c server.pem  vtl (64-bit) v7.4.0-226. Copyright (c) 2018 SafeNet. All rights reserved.  New server 10.20.60.77 successfully added to server list. |

# cópia certificado do cliente para HSM

|  |
| --- |
| PSCP.EXE C:\Program Files\SafeNet\LunaClient\cert\client\10.20.60.77.pem [admin@10.20.60.77](mailto:admin@10.20.60.77):  sudo /usr/safenet/lunaclient/bin/pscp /usr/safenet/lunaclient/cert/client/10.20.60.79.pem [admin@10.20.60.77](mailto:admin@10.20.60.77):  admin@10.20.60.77's password:  10.20.60.79.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100% |

# adicionar um novo cliente no HSM

|  |
| --- |
| client register -client 10.20.60.79 -ip 10.20.60.79  'client register' successful.  Command Result : 0 (Success) |

# assinar a partição criada ao cliente

|  |
| --- |
| [luna-ft] lunash:>client assignPartition -client 10.20.60.79 -partition lunalab  'client assignPartition' successful.  Command Result : 0 (Success) |

# verificar o registro do cliente

|  |
| --- |
| [ft@lunaclient ~]$ sudo /usr/safenet/lunaclient/bin/vtl verify  vtl (64-bit) v7.4.0-226. Copyright (c) 2018 SafeNet. All rights reserved.  The following Luna SA Slots/Partitions were found:  Slot Serial # Label  ==== ================ =====  0 1372869334793 |

## Única Etapa

# Limpeza

|  |
| --- |
| [ft@lunaclient ~]$ sudo /usr/safenet/lunaclient/bin/vtl deleteserver -n 10.20.60.77  vtl (64-bit) v7.4.0-226. Copyright (c) 2018 SafeNet. All rights reserved.  Server 10.20.60.77 successfully removed from server list. |

|  |
| --- |
| [root@lunaclient ft]# rm /usr/safenet/lunaclient/cert/client/\*  [root@lunaclient ft]# rm /usr/safenet/lunaclient/cert/server/\* |

|  |
| --- |
| [luna-ft] lunash:>client revokePartition -client 10.20.60.79 -partition lunalab  'client revokePartition' successful.  Command Result : 0 (Success) |

|  |
| --- |
| [luna-ft] lunash:>client delete -client 10.20.60.79  CAUTION: Are you sure you wish to delete client named:  10.20.60.79  Type 'proceed' to delete the client, or 'quit'  to quit now.  > proceed  'client delete' successful.  Command Result : 0 (Success) |

|  |
| --- |
| [luna-ft] lunash:>partition delete -partition lunalab  CAUTION: Are you sure you wish to delete the partition named:  lunalab  Type 'proceed' to delete the partition, or 'quit'  to quit now.  > proceed  'partition delete' successful.  Command Result : 0 (Success) |

# Instalação

|  |
| --- |
| [ft@lunaclient ~]$ sudo /usr/safenet/lunaclient/bin/lunacm  lunacm (64-bit) v7.4.0-226. Copyright (c) 2018 SafeNet. All rights reserved.  Available HSMs:  Slot Id -> 0  Label ->  Serial Number -> 1372869334793  Model -> LunaSA 7.0.0  Firmware Version -> 7.0.1  Configuration -> Luna User Partition With SO Signing With Cloning Mode  Slot Description -> Net Token Slot  FM HW Status -> FM Ready  Current Slot Id: 0 |

|  |
| --- |
| lunacm:>clientconfig deploy -server 10.20.60.77 -client 10.20.60.79 -partition lunalab -verbose  Please wait while we set up the connection to the HSM. This may take several minutes...  Using username "admin".  Please enter appliance admin role user's password:  Last login: Mon Apr 19 10:10:23 2021 from 10.20.71.20  Luna SA 7.0.0-956 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.  Using username "admin".  Last login: Mon Apr 19 10:47:38 2021 from 10.20.60.79  Luna SA 7.0.0-956 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.  sysconf forceSOLogin show  HSM Administrator Login Enforcement is NOT enabled.  Command Result : 0 (Success)  Using username "admin".  Last login: Mon Apr 19 10:47:51 2021 from 10.20.60.79  Luna SA 7.0.0-956 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.  client list  registered client 1: 10.20.71.20  registered client 2: 10.20.71.21  Command Result : 0 (Success)  Using username "admin".  Last login: Mon Apr 19 10:48:05 2021 from 10.20.60.79  Luna SA 7.0.0-956 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.  partition list  Storage (bytes)  ----------------------------  Partition Name Objects Total Used Free  ===========================================================================  1372869334790 prevenda 0 3240937 0 3240937  1372869334791 teste01 16 3240937 19408 3221529  1372869334793 lunalab 0 3240938 0 3240938  Command Result : 0 (Success)  Exiting...  Command Result : 0 (Success)  Exiting...  Private Key created and written to: /usr/safenet/lunaclient/cert/client/10.20.60.79Key.pem  Certificate created and written to: /usr/safenet/lunaclient/cert/client/10.20.60.79.pem  10.20.60.79.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%  server.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%  New server 10.20.60.77 successfully added to server list.  Using username "admin".  Last login: Mon Apr 19 10:48:18 2021 from 10.20.60.79  Luna SA 7.0.0-956 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.  client register -c 10.20.60.79 -i 10.20.60.79  'client register' successful.  client assignPartition -c 10.20.60.79 -p lunalab  'client assignPartition' successful.  Command Result : 0 (Success)  The following Luna SA Slots/Partitions were found:  Slot Serial # Label  ==== ================ =====  0 1372869334793 lunalab  Command Result : No Error  lunacm (64-bit) v7.4.0-226. Copyright (c) 2018 SafeNet. All rights reserved.  Available HSMs:  Slot Id -> 0  Label -> lunalab  Serial Number -> 1372869334793  Model -> LunaSA 7.0.0  Firmware Version -> 7.0.1  Configuration -> Luna User Partition With SO (PED) Signing With Cloning Mode  Slot Description -> Net Token Slot  FM HW Status -> FM Ready  Current Slot Id: 0 |

# Partição e Inicialização PSO

# Inicializando Partição

|  |
| --- |
| lunacm:>partition init -label lunalab  You are about to initialize the partition.  All contents of the partition will be destroyed.  Are you sure you wish to continue?  Type 'proceed' to continue, or 'quit' to quit now ->proceed  Please attend to the PED.  Command Result : No Error |

Obs: tenha em mãos os pendrives que serão os SO e PO

# Inicialização CO

|  |
| --- |
| lunacm:>role login -name po  Please attend to the PED.  Command Result : No Error |

|  |
| --- |
| lunacm:>role init -name co  Please attend to the PED.  Command Result : No Error  a. Choose not to reuse an existing keyset.  b. Set M=1 and N=1.  c. Choose to use '1234' as PIN.  d. Choose not to duplicate the key. |

|  |
| --- |
| lunacm:>role login -name co  Please attend to the PED.  Command Result : No Error |

|  |
| --- |
| lunacm:>partition contents  The 'Crypto Officer' is currently logged in. Looking for objects  accessible to the 'Crypto Officer'.  Error in execution: CKR\_PIN\_EXPIRED.  Command Result : 0xa3 (CKR\_PIN\_EXPIRED) |

|  |
| --- |
| lunacm:>role changePW -name co  Please attend to the PED.  Command Result : No Error  lunacm:>partition contents  The 'Crypto Officer' is currently logged in. Looking for objects  accessible to the 'Crypto Officer'.  No objects viewable to 'Crypto Officer' are currently stored in the partition.  Command Result : No Error |

# Ativação

|  |
| --- |
| lunacm:>role login -name co  Please attend to the PED.  Command Result : No Error |

|  |
| --- |
| lunacm:>partition changepolicy -policy 22 -value 1  Command Result : No Error  lunacm:>partition changepolicy -policy 23 -value 1  Command Result : No Error |

|  |
| --- |
| lunacm:>role createchallenge -name co  Please attend to the PED.  enter new challenge secret: **AAaa00--**  re-enter new challenge secret: **AAaa00--**  Command Result : No Error  lunacm:>role changePW -name co -old AAaa00-- -newpw AAaa00--  This role has secondary credentials.  You are about to change the secondary credentials.  Are you sure you wish to continue?  Type 'proceed' to continue, or 'quit' to quit now ->proceed  Please attend to the PED.  Command Result : No Error  Your PED key is now cached and the CO can log in to the partition using only this password! |

# Transporte

Transportar físico do HSM Luna.

## Transport

|  |
| --- |
| [luna-ft] lunash:>hsm stm transport  WARNING !! You are about to configure the HSM in secure transport mode.  If you proceed, the HSM will be inoperable until it is recovered with hsm stm recover command.  If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.  > proceed  Proceeding...  Configuring the HSM for secure transport mode...  Record the displayed verification & random user strings. These are required to recover from Secure Transport Mode.  Verification String: /s/p-RLbp-SK4H-4KdM  Random User String: F3sT-p5FS-HtMM-RG5K  HSM is now in Secure Transport Mode.  Command Result : 0 (Success) |

## Recovery

|  |
| --- |
| [luna-ft] lunash:>hsm stm recover -randomuserstring F3sT-p5FS-HtMM-RG5K  Attempting to recover from Secure Transport Mode...  Calculating the verification string (may take a few seconds)...  Verification String: /s/p-RLbp-SK4H-4KdM  CAUTION: You are attempting to recover the HSM from Secure Transport Mode.  If the Verification string does not match the one you were provided out-of-band,  there may be an issue with the HSM. Type 'quit' at the prompt to remain in Secure Transport Mode.  If the verification strings match, or if you wish to bypass this check,  type 'proceed' to recover from Secure Transport Mode.  Type 'proceed' to continue, or 'quit' to quit now.  > proceed    Successfully recovered from Secure Transport Mode.  Command Result : 0 (Success) |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Versão Inicial | 19/04/2021 |
|  |  |  |