THALES

Deploy Luna Minimal Client 10.4 with DPoD Service in Docker

Pre-Requisites

- Obtain the luna client minimal 10.4 (LunaClient-Minimal-10.4.0-417.x86_64.tar)
- Download the zip file from your DPoD service (in our case: setup-HSM_pki_client.zip)
- Docker installed and configured
- Environment: Centos 7.8

Note: the steps are based on official documents "Install luna minimal client on Linux using docker" and "From Linux Minimal Client Create a Docker Container to Access a DPOD Luna Cloud HSM Service"

1. Luna Minimal Client deploy into Docker

1.1. Create a directory. In this example:

```
mkdir $HOME/luna-docker
```

1.2. Create the following subdirectories under that first directory:

```
mkdir $HOME/luna-docker/config

mkdir $HOME/luna-docker/config/certs
```

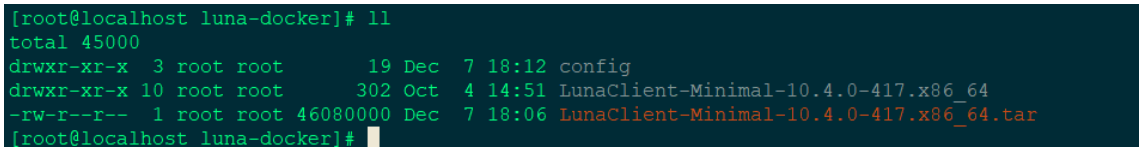
1.3. Copy the Luna Minimal Client tarball to $HOME/luna-docker.

```
cp LunaClient-Minimal-10.4.0-417.x86_64.tar $HOME/luna-docker
```

1.4. Untar the Luna Minimal Client tarball.

```
cd  $HOME/luna-docker

tar -xf LunaClient-Minimal-10.4.0-417.x86_64.tar
```

Result: folder called equal as tar file (without extension)



1.5. Copy the Chrystoki.conf file from the Minimal Client directory to $HOME/luna-docker/config

```
cd  $HOME/luna-docker

cp LunaClient-Minimal-10.4.0-417.x86_64/Chrystoki-template.conf  $HOME/luna-docker/config/Chrystoki.conf
```

1.6. Define the following environment variable:

```
export ChrystokiConfigurationPath=$HOME/luna-docker/config
```

1.7. Update the Chrystoki.conf file paths so the tools work as expected (execute all the following commands as it)

```
MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-10.4.0-417.x86_64

$MIN_CLIENT_DIR/bin/64/configurator setValue -s Chrystoki2 -e LibUNIX -v $MIN_CLIENT_DIR/libs/64/libCryptoki2.so

$MIN_CLIENT_DIR/bin/64/configurator setValue -s Chrystoki2 -e LibUNIX64 -v $MIN_CLIENT_DIR/libs/64/libCryptoki2_64.so

$MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e ToolsDir -v $MIN_CLIENT_DIR/bin/64

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e SSLConfigFile -v $MIN_CLIENT_DIR/openssl.cnf

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ClientPrivKeyFile -v $HOME/luna-docker/config/certs/dockerlunaclientKey.pem

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ClientCertFile -v $HOME/luna-docker/config/certs/dockerlunaclient.pem

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ServerCAFile -v $HOME/luna-docker/config/certs/CAFile.pem

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e ClientTokenLib -v $MIN_CLIENT_DIR/libs/64/libSoftToken.so

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e SoftTokenDir -v $HOME/luna-docker/config/stc/token

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e ClientIdentitiesDir -v $HOME/luna-docker/config/stc/client_identities

$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e PartitionIdentitiesDir -v $HOME/luna-docker/config/stc/partition_identities
```

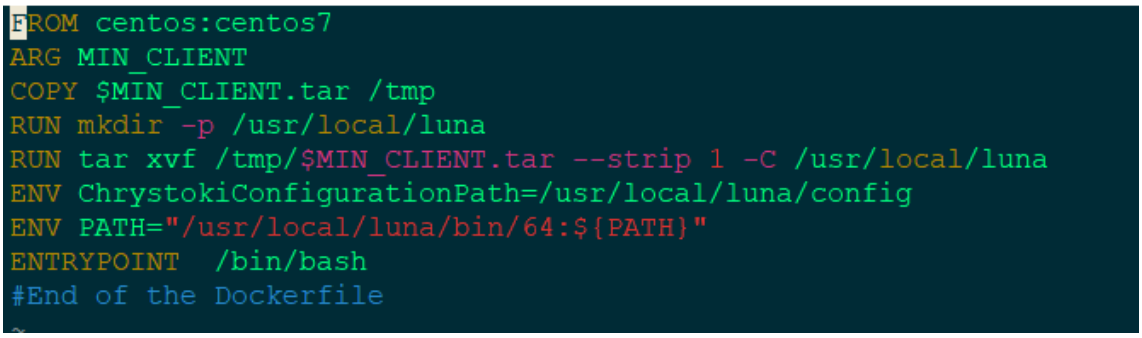
1.8. Update the paths of the libraries, certs and general fields to their future Docker image locations within the $ChrystokiConfigurationPath/Chrystoki.conf.

```
sed -i -e 's#'$HOME'/luna-docker/config#/usr/local/luna/config#g' -e 's#'$HOME'/luna-docker/LunaClient-Minimal-\([0-9\.-]\+\)x86_64#/usr/local/luna#g' $ChrystokiConfigurationPath/Chrystoki.conf
```

1.9. Create a file named Dockerfile with the following contents at $HOME/luna-docker, with the following content

```
FROM centos:centos7

ARG MIN_CLIENT

COPY $MIN_CLIENT.tar /tmp

RUN mkdir -p /usr/local/luna

RUN tar xvf /tmp/$MIN_CLIENT.tar --strip 1 -C /usr/local/luna

ENV ChrystokiConfigurationPath=/usr/local/luna/config

ENV PATH="/usr/local/luna/bin/64:${PATH}"

ENTRYPOINT  /bin/bash

#End of the Dockerfile
```

Result: it should looks like



1.10. Build a Docker image.

```
docker build . --build-arg MIN_CLIENT=LunaClient-Minimal-10.4.0-417.x86_64 -t lunaclient-image
```

Result: it should ends with successfully built, as shown in the image:

```
[root@localhost luna-docker]# docker build . --build-arg MIN_CLIENT=LunaClient-Minimal-10.4.0-417.x86_64 -t lunaclient-image
Sending build context to Docker daemon 92.16 MB
Step 1/8 : FROM centos:centos7
 ---> eeb6ee3f44bd
Step 2/8 : ARG MIN_CLIENT
 ---> Running in 1b4c3cfcff64
 ---> 24e04f10c2a4
Removing intermediate container 1b4c3cfcff64
Step 3/8 : COPY $MIN_CLIENT.tar /tmp
 ---> 0a96bec4192e
Removing intermediate container cffe671dcd89
Step 4/8 : RUN mkdir -p /usr/local/luna
 ---> Running in ae1066eef66a

 ---> 30219ef17dd1
Removing intermediate container ae1066eef66a
Step 5/8 : RUN tar xvf /tmp/$MIN_CLIENT.tar --strip 1 -C /usr/local/luna
 ---> Running in 43908ebb6a96
```

more output…..

```
LunaClient-Minimal-10.4.0-417.x86_64/stc/partition_identities/
LunaClient-Minimal-10.4.0-417.x86_64/Chrystoki-noncontainer-template.conf
 ---> edec9fc869b7
Removing intermediate container 43908ebb6a96
Step 6/8 : ENV ChrystokiConfigurationPath /usr/local/luna/config
 ---> Running in 1f0f75fccec7
 ---> 913de0c5c9b6
Removing intermediate container 1f0f75fccec7
Step 7/8 : ENV PATH "/usr/local/luna/bin/64:${PATH}"
 ---> Running in 689efba540ff
 ---> 82e3137779b9
Removing intermediate container 689efba540ff
Step 8/8 : ENTRYPOINT /bin/bash
 ---> Running in a159615308f4
 ---> 6c7e500d4fcf
Removing intermediate container a159615308f4
Successfully built 6c7e500d4fcf
```

1.11. Use the following command to verify the Docker image has been created:

```
docker images
```

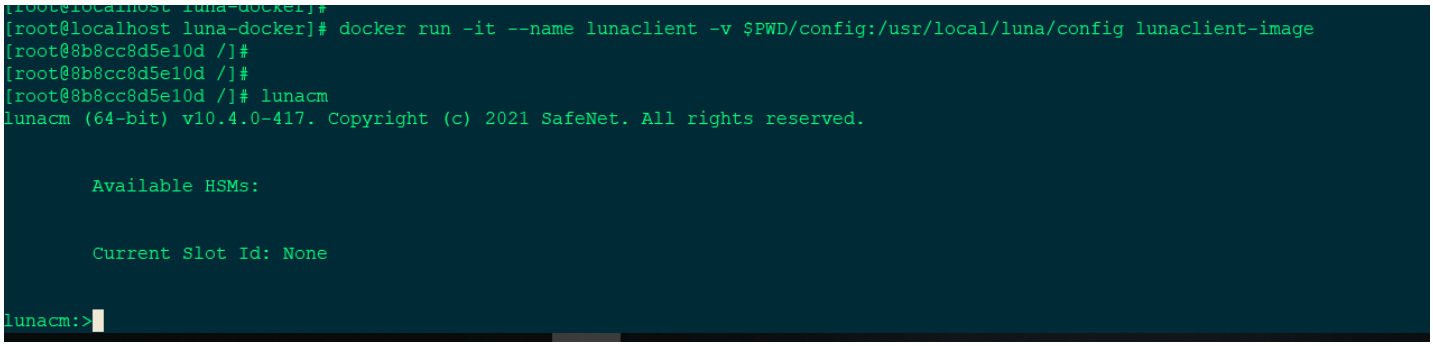
Result: it will shows the name of the docker image built (lunaclient-image)

```
[root@localhost luna-docker]#
[root@localhost luna-docker]# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
lunaclient-image    latest              6c7e500d4fcf        4 minutes ago       296 MB
```

1.12. Run the Docker container. Make the contents of the config directory available to the Containers when you create them, by mounting the config directory as a volume.

```
docker run -it --name lunaclient -v $PWD/config:/usr/local/luna/config lunaclient-image
```

Result: it should bring the linux container console, and after run the **lunacm** command it should open the luna client prompt (without partitions yet) but this means that luna minimal client was installed correctly.



Note: exit from the docker container to get in the OS linux folder $HOME/luna-docker

THALES

2. Luna Minimal Client deploy into Docker

2.1. Create a dpod folder into $HOME/luna-docker/

```
mkdir $HOME/luna-docker/dpod
```

2.2. Unzip the DPoD service zip file into it ($HOME/luna-docker/dpod)

```
unzip $HOME/setup-HSM_pki_client.zip  -d $HOME/luna-docker/dpod
```

Result of this is to deflate all service files into dpod folder

```
[root@localhost luna-docker]# unzip $HOME/setup-HSM_pki_client.zip  -d $HOME/luna-docker/dpod
Archive:  /root/setup-HSM_pki_client.zip
  inflating: /root/luna-docker/dpod/EULA.zip
  inflating: /root/luna-docker/dpod/cvclient-min.tar
  inflating: /root/luna-docker/dpod/cvclient-min.zip
  inflating: /root/luna-docker/dpod/partition-certificate.pem
  inflating: /root/luna-docker/dpod/partition-ca-certificate.pem
  inflating: /root/luna-docker/dpod/server-certificate.pem
  inflating: /root/luna-docker/dpod/Chrystoki.conf
  inflating: /root/luna-docker/dpod/crystoki-template.ini
[root@localhost luna-docker]#
```

2.3. Copy the Luna Cloud HSM service certificates into the certificate directory on the shared volume so that the Docker container can use them.

```
cp $HOME/luna-docker/dpod/server-certificate.pem $HOME/luna-docker/config/certs/
cp $HOME/luna-docker/dpod/partition-ca-certificate.pem $HOME/luna-docker/config/certs/
cp $HOME/luna-docker/dpod/partition-certificate.pem $HOME/luna-docker/config/certs/
```

2.4. Copy over the entire REST and XTC sections from the unzipped Chrystoki.conf located at $HOME/luna-docker/dpod/Chrystoki.conf:

cat $HOME/luna-docker/dpod/Chrystoki.conf

Extract the Rest and Xtc information showed like:

```
XTC = {
 Enabled = 1;
 TimeoutSec = 600;
 PartitionCAPath = ./partition-ca-certificate.pem;
 PartitionCertPath00 = ./partition-certificate.pem;
}
REST = {
 AuthTokenConfigURI = https://josemendez-tenantuser.uaa.system.snakefly.dpsas.io/.well-known/openid-configuration;
 AuthTokenClientId = 67309ba1-8d6a-4583-8c35-893758d57006;
 AuthTokenClientSecret = iru4pLO0ucplY49pKsVSO9gboKLW3G3D;
 RestClient = 1;
 ClientTimeoutSec = 120;
 ClientPoolSize = 32;
 ClientEofRetryCount = 15;
 ClientConnectRetryCount = 900;
 ClientConnectIntervalMs = 1000;
 PartitionData00 = 1285325060503, na.hsm.dpondemand.io, 443;
 SSLClientSideVerifyFile = ./server-certificate.pem;
}
```

Paste (using vi or vim) into $HOME/luna-docker/config/Chrystoki.conf at the end of the document and it should looks like:

```
Secure Trusted Channel = {
   ClientTokenLib = /usr/local/luna/libs/64/libSoftToken.so;
   SoftTokenDir = /usr/local/luna/config/stc/token;
   ClientIdentitiesDir = /usr/local/luna/config/stc/client_identities;
   PartitionIdentitiesDir = /usr/local/luna/config/stc/partition_identities;
}

XTC = {
  Enabled = 1;
  TimeoutSec = 600;
  PartitionCAPath = ./partition-ca-certificate.pem;
  PartitionCertPath00 = ./partition-certificate.pem;
}

REST = {
  AuthTokenConfigURI = https://josemendez-tenantuser.uaa.system.snakefly.dpsas.io/.well-known/openid-configuration;
  AuthTokenClientId = 67309ba1-8d6a-4583-8c35-893758d57006;
  AuthTokenClientSecret = iru4pLO0ucplY49pKsVSO9gboKLW3G3D;
  RestClient = 1;
  ClientTimeoutSec = 120;
  ClientPoolSize = 32;
  ClientEofRetryCount = 15;
  ClientConnectRetryCount = 900;
  ClientConnectIntervalMs = 1000;
  PartitionData00 = 1285325060503, na.hsm.dpondemand.io, 443;
  SSLClientSideVerifyFile = ./server-certificate.pem;
}
"config/Chrystoki.conf" 65L, 1874C written
```

IMPORTANT:

- Line
  PartitionData00 = 1285325060503, na.hsm.dpondemand.io, 443;
- Must be deleted and create in place two new lines

  ServerName=na.hsm.dpondemand.io

  ServerPort=443

Resulting file must show as shown in the red square

```
XTC = {
  Enabled = 1;
  TimeoutSec = 600;
   PartitionCAPath = /usr/local/luna/config/certs/partition-ca-certificate.pem;
   PartitionCertPath00 = /usr/local/luna/config/certs/partition-certificate.pem;
}

REST = {
  AuthTokenConfigURI = https://josemendez-tenantuser.uaa.system.snakefly.dpsas.io/.well-known/openid-configuration;
  AuthTokenClientId = 67309ba1-8d6a-4583-8c35-893758d57006;
  AuthTokenClientSecret = iru4pLO0ucplY49pKsVSO9gboKLW3G3D;
  RestClient = 1;
  ClientTimeoutSec = 120;
  ClientPoolSize = 32;
  ClientEofRetryCount = 15;
  ClientConnectRetryCount = 900;
  ClientConnectIntervalMs = 1000;
  ServerName=na.hsm.dpondemand.io
  ServerPort=443
  SSLClientSideVerifyFile = /usr/local/luna/config/certs/server-certificate.pem;
}
```

2.5. Update $HOME/luna-docker/config/Chrystoki.conf with the expected paths that will be used by the Docker container.

Run the commands exact as is it

```
export ChrystokiConfigurationPath=$HOME/luna-docker/config

MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-10.4.0-417.x86_64

$MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCAPath -v /usr/local/luna/config/certs/partition-ca-certificate.pem

$MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCertPath00 -v /usr/local/luna/config/certs/partition-certificate.pem

$MIN_CLIENT_DIR/bin/64/configurator setValue -s REST -e SSLClientSideVerifyFile -v /usr/local/luna/config/certs/server-certificate.pem
```

2.6. The Luna Minimal Client now includes a Luna Cloud HSM service plugin which allows the LUNA client to be able to communicate with a Luna Cloud HSM service. That file can be located under $HOME/luna-docker/LunaClient-Minimal-<release_version>.x86_64/plugins/libdpod.plugin. This example uses the Dockerfile mentioned above which extracts the Luna Minimal Client tarball into the Docker image.

```
$MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e PluginModuleDir -v /usr/local/luna/plugins
```

Both 2.5 and 2.6 after execute should show the execution like this

```
[root@localhost luna-docker]#
[root@localhost luna-docker]# export ChrystokiConfigurationPath=$HOME/luna-docker/config
[root@localhost luna-docker]#
[root@localhost luna-docker]# MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-10.4.0-417.x86_64
[root@localhost luna-docker]#
[root@localhost luna-docker]# $MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCAPath -v /usr/local/luna/config/certs/partition-ca-certificate.pem
pass
[root@localhost luna-docker]# $MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCertPath00 -v /usr/local/luna/config/certs/partition-certificate.pem
pass
[root@localhost luna-docker]# $MIN_CLIENT_DIR/bin/64/configurator setValue -s REST -e SSLClientSideVerifyFile -v /usr/local/luna/config/certs/server-certificate.pem
pass
[root@localhost luna-docker]# $MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e PluginModuleDir -v /usr/local/luna/plugins
pass
[root@localhost luna-docker]#
```

2.7. Attach the Docker container. If it is stopped you must start the container first.

```
docker ps -a

docker start <container_id>

docker attach <container_id>
```

2.8. At this point you should be able to see the Luna Cloud HSM service

```
lunacm
```

After that it should list the DPoD tile information

```
[root@localhost luna-docker]#
[root@localhost luna-docker]# docker ps -a
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS
8b8cc8d5e10d        lunaclient-image    "/bin/sh -c /bin/bash"   39 minutes ago      Exited (0) 3 minut
[root@localhost luna-docker]# docker start 8b
8b
[root@localhost luna-docker]# docker attach 8b
[root@8b8cc8d5e10d /]# lunacm
lunacm (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.


        Available HSMs:

        Slot Id ->              6
        Label ->                DPoD_pki
        Serial Number ->        1285325060503
        Model ->                Cryptovisor7
        Firmware Version ->     7.3.0
        CV Firmware Version ->  1.4.2
        Plugin Version ->       Cloud 2.1.0-554
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM Not Supported


        Current Slot Id: 6


lunacm:>exit
[root@8b8cc8d5e10d /]# cmu list -slot 6
Certificate Management Utility (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.

Please enter password for token in slot 6 : ************

ouid=f94f08001800000131be0800   label=Generated RSA Private Key
ouid=f84f08001800000131be0800   label=Generated RSA Public Key
ouid=17240a0020000001706c0800   label=AesGcmKey
[root@8b8cc8d5e10d /]#
```