THALES

CyberArk Vault: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-000134-001
Revision	D
Release Date	25 November 2020

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

At the core of CyberArk Privileged Account Security Solution is the CyberArk Digital Vault that contains a highly secure database for storing privileged account credentials, access control policies, credential management policies, and audit information. To protect both the Digital Vault database and the data stored within the database, CyberArk has designed a multi-layered encryption hierarchy that uses FIPS 140-2 compliant encryption. Each individual file and safe within the Digital Vault database is encrypted with its own unique encryption key. The Digital Vault Server uses key-hierarchy for protecting each object in the Vault. Based on this unique and highly secure approach, CyberArk has the top-level encryption key (server key) required to start the Digital Vault.

This document describes how to store encryption key (server key) on Thales Luna HSMs. Using Luna HSMs to secure the server key provides the following benefits:

- Secure generation, storage and protection of the Identity signing private key on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- HSM audit trail*.
- Significant performance improvements by off-loading cryptographic operations from application servers

*Luna Cloud HSM services do not have access to the secure audit trail.

Certified Platforms

This integration is certified on the following platforms.

HSM Type	Platforms Tested	CyberArk Vault Server	PrivateArk Client
Luna HSM, Luna Cloud HSM	Windows Server 2012R2	10.3	8.0
Luna HSM, Luna Cloud HSM	Windows Server 2016	11.6	8.0

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic

Luna Cloud HSM: Luna Cloud HSM platform provides on-demand, cloud-based HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an

Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

Configure Luna HSM Device

To configure a Luna HSM device:

1. Ensure that the HSM is set up, initialized, provisioned and ready for deployment. Refer to the HSM product documentation for help.
2. Create a partition that will be later used by CyberArk Vault.
3. Create and exchange certificate between the Luna Network HSM and Client system. Register client and assign partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe

lunacm.exe (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights
reserved.

Available HSMs:

   Slot Id ->              0

   Label ->                CyberArk

   Serial Number ->        1238696044904

   Model ->                LunaSA 7.4.0

   Firmware Version ->     7.4.0

   Configuration ->        Luna User Partition With SO (PW) Signing With
   Cloning Mode

   Slot Description ->     Net Token Slot

   FM HW Status ->         Non-FM
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to Luna HSM documentation for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

To configure Luna HSM HA (High-Availability)

Please refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM appliances on Windows and UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stop functioning for some reason, all calls automatically routed to secondary till primary starts functioning again.

NOTE: This integration is tested in both HA and FIPS mode.

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

```
[Windows]
cvclient-min.zip
[Linux]
cvclient-min.tar
# tar -xvf cvclient-min.tar
```

4. Run the **setenv** script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Windows]
Right-click setenv.cmd and select Run as Administrator.
[Linux]
Source the setenv script.
# source ./setenv
```

5. Run the **LunaCM** utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

6. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
7. Extract the .zip file into a directory on your client workstation.
8. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

```
[Windows]
cvclient-min.zip
[Linux]
cvclient-min.tar
# tar -xvf cvclient-min.tar
```

9. Run the **setenv** script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Windows]
Right-click setenv.cmd and select Run as Administrator.
[Linux]
Source the setenv script.
# source ./setenv
```

10. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

Cloud HSM Certificates:

```
server-certificate.pem
partition-ca-certificate.pem
partition-certificate.pem
```

LunaClient Certificate Directory:

```
[Windows default location for Luna Client]
C:\Program Files\Safenet\Lunaclient\cert\
[Linux default location for Luna Client]
/usr/safenet/lunaclient/cert/
```

> **NOTE:** Skip this step for Luna Client v10.2 or higher.

11. Open the configuration file from the Cloud HSM service client directory and copy the **XTC** and **REST** section.

```
[Windows]
crystoki.ini
[Linux]
Chrystoki.conf
```

12. Edit the Luna Client configuration file and add the **XTC** and **REST** sections copied from Cloud HSM service client configuration file.
13. Change server and partition certificates path from step 5 in **XTC** and **REST** sections. Do not change any other entries provided in these sections.

[XTC]

```
. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .

[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .
```

> **NOTE:** Skip this step for Luna Client v10.2 or higher.

14. Edit the following entry from the **Misc** section and update the correct path for the **plugins** directory:

```
Misc]
PluginModuleDir=<LunaClient_plugins_directory>

[Windows Default]

C:\Program Files\Safenet\Lunaclient\plugins\

[Linux Default]

/usr/safenet/lunaclient/plugins/
```

Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

15. Reset the **ChrystokiConfigurationPath** environment variable and point back to the location of the Luna Client configuration file.

[Windows]

In the Control Panel, search for "environment" and select **Edit the system environment variables**. Click **Environment Variables**. In both list boxes for the current user and system variables, edit **ChrystokiConfigurationPath** and point to the **crystoki.ini** file in the Luna client install directory.

[Linux]

Either open a new shell session, or export the environment variable for the current session pointing to the location of the **Chrystoki.conf** file:

```
# export ChrystokiConfigurationPath=/etc/
```

16. Run the **LunaCM** utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

> **NOTE:** Follow the Luna Cloud HSM documentation for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

To use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Set up CyberArk Vault

CyberArk Vault and PrivateArk Client must be installed on the target machine to carry on with the integration process. For a detailed installation procedure, refer to the *CyberArk Documentation*.

Integrating Luna HSM with CyberArk Vault

This document contains detailed instructions and procedures to integrate CyberArk Vault with a Luna HSM or HSM on Demand service. This integration contains the following topics:

Configure CyberArk Vault

To configure the CyberArk Vault:

1. Configure the firewall to allow communication to the HSM device if you are using Thales Luna Network HSM. Open the dbparam.ini file in a text editor. It is located at C:\Program Files(x86)\PrivateArk\Server.

   Edit or add the AllowNonStandardFWAddresses parameter to open the firewall and allow access to the HSM device:

   ```
   AllowNonStandardFWAddresses= [HSM-
   IP],Yes,1792:inbound/tcp,1792:outbound/tcp
   ```

NOTE: When editing firewall rules in dbparm.ini file, the separator between two rules is a comma. For example:

```
AllowNonStandardFWAddresses=
[IP],Yes,3389:outbound/tcp,3389:inbound/tcp,[IP],Yes,1792:inbound
/tcp,1792:outbound/tcp
```

NOTE: If you are using Luna Cloud HSM service, the firewall file configuration is not required.

2. Configure the PKCS#11 provider DLL and specify it in the PKCS11ProviderPath parameter in dbparam.ini file in the `[main]` section.

   ```
   PKCS11ProviderPath=<path_to_PKCS#11_provider_library >
   ```

   For example:

   ```
   PKCS11ProviderPath="C:\Program Files\SafeNet\LunaClient\cryptoki.dll"
   ```

3. Navigate to C:\Program Files(x86)\PrivateArk\Server. Execute the CAVaultManager command and specify the partition password that will be used to access the server key:

   ```
   CAVaultManager.exe SecureSecretFiles /SecretType HSM /Secret
   <partition_password>
   ```

   ```
   PS C:\Program Files (x86)\PrivateArk\Server> .\CAVaultManager.exe SecureSecretFiles /SecretType HSM /Secret userpin1

   ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol
   Integrity), SHA2-512 (Files Integrity).

   CAVLT146I HSM secret was secured successfully.
   ```

   Open dbparam.ini file and verify that the HSMPinCode parameter was added with the encrypted value of the PIN code.

4. Restart the CyberArk Server to apply the changes.
5. Shutdown the CyberArk Server.

Generate Server Key in HSM

To generate the Server Key in the HSM:

1. Ensure that the Vault Server is not running.
2. Navigate to C:\Program Files(x86)\PrivateArk\Server and run the CAVaultManager command to generate a new server key on the HSM:

   ```
   CAVaultManager.exe GenerateKeyOnHSM /ServerKey
   ```

   ```
   PS C:\Program Files (x86)\PrivateArk\Server> .\CAVaultManager.exe GenerateKeyOnHSM /ServerKey
   ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol Integrity),
    SHA2-512 (Files Integrity).
   ITADM114I Successfully connected to Database, Database id 0.
   CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#1).
   ```

   The above command generates a new key for the Vault Server, stores it in the HSM device, and returns the key generation id. For example: `HSM#1`.

3. Verify that the server key has been generated on HSM using CMU utility that comes with LunaClient.

   ```
   cmu.exe list
   ```

   Provide the partition password when prompted.

   ```
   PS C:\Users\Administrator\Desktop\setup-ranjan> .\cmu.exe list
   Certificate Management Utility (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.

   Please enter password for token in slot 3 : ********

   ouid=24cf0500110000001ffa90800   label=Cyber-Ark Server Key
   ```

4. Verify that the `RecoveryPrvKey` parameter in dbparam.ini file points to the correct private recovery key (`recprv.key`).
5. Execute the ChangeServerKeys command to change the encryption keys that will be used for the Vault Server. This command re-encrypts the Vault data and metadata with the new encryption key generated on HSM. Press `y` on prompt.

```
ChangeServerKeys PathToKeys PathToEmergencyFile HSMKeyGenerationId
```

For Example:

```
ChangeServerKeys C:\Keys C:\Keys\VaultEmergency.pass HSM#1
```

```
PS C:\Program Files (x86)\PrivateArk\Server> .\ChangeServerKeys.exe C:\Users\Administrator\Desktop\Keys C:\Users\Administrator\Des
ktop\Keys\VaultEmergency.pass HSM#1
13/10/2020 12:20:29 CHSRVK041I ChangeServerKeys process started.ITADB399I Using encryption algorithms: Advanced Encryption Standar
d (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512 (Files Integrity).
ITADM114I Successfully connected to Database, Database id 0.
ITAQS031I Object cache is loaded.
HSM generation 1 was chosen, are you sure you want to change server keys to HSM (y/n)?
y
Verify that the current master key is at C:\Users\Administrator\Desktop\Keys\recprv.key, and press any key.

Verify new server's master key is at C:\Users\Administrator\Desktop\Keys, and press any key.

13/10/2020 12:21:13 CHSRVK043I Signing entropy file C:\PrivateArk\Safes\entropy.rnd with new keys.
13/10/2020 12:21:14 CHSRVK034I Encrypting server private key.
13/10/2020 12:21:14 CHSRVK058I Encrypting Backup key.
13/10/2020 12:21:14 CHSRVK057I Encrypting Database access passwords.
13/10/2020 12:21:20 CHSRVK020I Keys of Safe System changed successfully.
13/10/2020 12:21:20 CHSRVK040I Changing keys for Safe System.
.....
13/10/2020 12:21:21 CHSRVK020I Keys of Safe System changed successfully.
13/10/2020 12:21:21 CHSRVK040I Changing keys for Safe Pictures.

13/10/2020 12:21:21 CHSRVK020I Keys of Safe Pictures changed successfully.
13/10/2020 12:21:21 CHSRVK040I Changing keys for Safe VaultInternal.

13/10/2020 12:21:21 CHSRVK020I Keys of Safe VaultInternal changed successfully.
13/10/2020 12:21:21 CHSRVK040I Changing keys for Safe Notification Engine.
.....
13/10/2020 12:21:22 CHSRVK020I Keys of Safe Notification Engine changed successfully.
13/10/2020 12:21:22 CHSRVK054I ChangeServerKeys process was successful. DBParm.ini must be updated to point to new keys for Vault
to start.
13/10/2020 12:21:22 CHSRVK042I ChangeServerKeys process ended.
```

6. Open dbparam.ini file and change `ServerKey` parameter to specify the value of the key generation id of HSM. For example:

   ```
   ServerKey=HSM#1
   ```

7. Start the Vault Server and log in. This completes the integration of CyberArk Vault with Thales HSM.

Migrate Existing Server Key to HSM

To migrate existing server key to HSM:

1. Complete the steps given in Configure CyberArk Vault section.
2. Make sure that the Vault Server is not running.
3. Load the Server key to the HSM device: `CAVaultManager.exe LoadServerKeyToHSM /WrapKey`

   This will generate a new key pair. The public key will be used to encrypt the server key, and the private will decrypt it on the HSM device. The private key is deleted from HSM when the server key is unwrapped.

   ```
   PS C:\Program Files (x86)\PrivateArk\Server> .\CAVaultManager.exe LoadServerKeyToHSM /WrapKey
   ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol I
   ntegrity), SHA2-512 (Files Integrity).
   ITADM114I Successfully connected to Database, Database id 0.
   CAVLT143I Server Key was successfully uploaded to HSM device
   ```

4. Verify that the server key has been generated on HSM using CMU utility that comes with LunaClient.

   ```
   cmu.exe list
   ```

   Provide the partition password when prompted.

   ```
   PS C:\Users\Administrator\Desktop\setup-ranjan> .\cmu.exe list
   Certificate Management Utility (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.

   Please enter password for token in slot 3 : ********

   ouid=3acf0500110000001ffa90800   label=Cyber-Ark Server Key
   ```

5. Open dbparam.ini file and change the value of the ServerKey parameter as follows:

```
ServerKey=HSM
```

6. Start the PrivateArk Server and make sure you can log in to the Vault.

Contacting Customer Support

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.