CyberArk Conjur

nShield® HSM Integration Guide

2024-04-05

Table of Contents

Chapter 1. Introduction

CyberArk Conjur offers secrets management for applications and services. There are four different deployment models. The model tested in this Integration Guide is the Dynamic Access Provider (DAP). For more information, see Conjur Secrets Manager Enterprise features in the CyberArk Conjur online documentation.

The base product is provided as a containerized appliance and can be executed in Docker or Kubernetes. The testing in this Integration Guide uses a basic deployment of nCOP in Docker.

1.1. Container images

Two container images were created for the purpose of this integration: a hardserver container and a CyberArk Conjur application container. These images are stored in an external registry:

- `nshield-hwsp`

  A hardserver container image that controls communication between the HSM(s) and the application containers.

- `conjur-appliance`

  An Application Access Manager (AAM) container image from CyberArk that will host the Master DAP Server.

1.2. Product configurations

Entrust has successfully tested nShield HSM integration with CyberArk Conjur in the following configurations:

Software	Version
nCOP	1.1.2
Operating System	Ubuntu 22.04 LTS
CyberArk Conjur Appliance Image	12.3.0, 12.7.0, 13.2.0

1.3. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.3.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
12.71.0	12.50.11 (FIPS Certified)	12.60.10	✓	✓	✓
12.80.4	12.50.11 (FIPS Certified)	12.80.4	✓	✓	✓
12.80.4	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓
13.4.5	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓

1.3.2. nShield 5c

Security World Software	Firmware	Image	OCS	Softcard	Module
13.4.5	13.2.2 (FIPS Pending)	13.3.2	✓	✓	✓

1.4. Supported nShield HSM functionality

Feature	Support
Module-only key	Yes
OCS cards	Yes
Softcards	Yes
nSaaS	Yes
FIPS 140 Level 3 mode support	Yes (FIPS Pending)

1.5. Requirements

Before installing these products, read the associated documentation:

- For the nShield HSM: *Installation Guide* and *User Guide*.
- If nShield Remote Administration is to be used: *nShield Remote Administration User Guide*.
- *nShield Container Option Pack User Guide*.
- DAP Deployment, refer to Conjur Secrets Manager Enterprise v13.2 in the CyberArk online documentation.
- HSM Master Key Encryption, refer to Encrypt the master key using an HSM in the CyberArk online documentation.

Furthermore, the following design decisions have an impact on how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140 Level 3 standards.

  If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. For information about limitations on FIPS authorization, see the *Installation Guide* of the nShield HSM.

- Whether to instantiate the Security World as recoverable or not.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.6. More information

For more information about OS support, contact your CyberArk sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Chapter 2. Procedures

2.1. Prerequisites

Before you can use nCOP and run the container images, complete the following steps:

1. Install Docker. For information, see Get Docker in the Docker online documentation.
2. Gain access to the Conjur appliance image. The following command can be used to load the `conjur-appliance` .tar file into the local Docker repository:

```
% docker load -i conjur-appliance-13.2.0.tar.gz
```

3. Request the nCOP and Security World software from Entrust.
4. Set up the HSM. See the *Installation Guide* for your HSM.
5. Configure the HSM(s) to use the IP address of your container host machine as a client.
6. Load an existing Security World or create a new one on the HSM.
7. Copy the Security World and module files to your container host machine at a directory of your choice.
8. Create or edit the `cknfastrc` file in `/opt/nfast` and add one of the following config settings:
9. For OCS or Softcard protection:

```
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
```

10. For Module protection:

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

11. Optionally, the following can be added to generate PKCS #11 debug logs at the example location:

```
CKNFAST_DEBUG=10
CKNFAST_DEBUGFILE=/opt/ncop/pkcs11.log
```

12. Create a `pkcs11.yml` file with the following content:

```
library: /opt/nfast/toolkits/pkcs11/libcknfast.so
wrapping_key: <wrapping_key name>
pin: <passphrase of ocs/softcard if required>
slot: <slot number for the intended key protection type>
```

By the default, the slot number for module protection is 0, for softcard protection 1, and for OCS protection 2. This can change depending on your HSM deployment. The pin passphrase is not required if you are using module protection.

For more information on configuring and managing nShield HSMs, Security Worlds, and Remote File Systems, see the *User Guide* for your HSM(s).

2.2. Create and configure the nshield-hwsp container

The nShield hardserver container has to be configured to enable it to communicate with the CyberArk Conjur Master DAP Server in a later step, see Create and configure the Conjur application container and the Master DAP Server.

To deploy an nCOP container image for use with CyberArk Conjur:

1. Log in to the container host machine server with `root` privileges and launch a terminal window.
2. Set up the nCOP working directory:

```
% mkdir -p /opt/ncop

% tar xf ncop-1.1.2.tar -C /opt/ncop
```

3. Mount the Security World:

```
% mkdir SecWorld-13.4.5

% mount -o loop SecWorld_Lin64-13.4.5.iso SecWorld-13.4.5
```

4. Set up the hardserver image:

```
% ./make-nshield-hwsp SecWorld-13.4.5
```

5. Configure `nshield-hwsp`:
    a. Set up the hardserver configuration file and directory:

```
% mkdir -p /opt/ncop/config1

% ./make-nshield-hwsp-config --output /opt/ncop/config1 config <hsm ip address>
```

b. Check that the configuration file information matches your HSM deployment:

```
% cat /opt/ncop/config1/config
```

c. Create a new socket so that application containers can use the hardserver:

```
% docker volume create socket1
```

d. Run the `nshield-hwsp` container:

```
% docker run -d -v /opt/ncop/config1:/opt/nfast/kmdata/config:ro -v socket1:/opt/nfast/sockets
nshield-hwsp:13.4.5
```

e. Check the status of `nshield-hwsp` using the `enquiry` command:

```
% NFAST_SERVER=/var/lib/docker/volumes/socket1/_data/nserver /opt/nfast/bin/enquiry
```

2.3. Create and configure the Conjur application container and the Master DAP Server

1. Extend the `conjur-appliance` image with the `nfast` utilities:

```
% ./extend-nshield-application --from registry.tld/conjur-appliance:13.2.2 --pkcs11 SecWorld-13.4.5
```

2. Tag the generated application image for convenience:

```
% docker tag <IMAGEID> conjor-appliance-wnfast:13.2.2
```

3. Run the `conjur-appliance` container with the `nfast` container:

```
% docker run --name dap-wnfast -d --restart=unless-stopped --security-opt seccomp=/path/to/conjur-
seccomp.json -p "443:443" -p "5432:5432" -p "1999:1999" -v /opt/nfast/kmdata:/opt/nfast/kmdata:rw -v
socket1:/opt/nfast/sockets conjur-appliance-wnfast:13.2.2
```

4. Perform the initial configuration of Conjur. The username is **admin**. For password requirements, see Configure the Conjur cluster in the CyberArk

online documentation.

```
% docker exec dap-wnfast evoke configure master --accept-eula --hostname dap-wnfast.example.com --admin
-password Mypassw0rD1! org1
```

5. Copy the `cknfastrc` and `pkcs11.yml` configuration files into the running container:

```
% docker cp cknfastrc dap-wnfast:/opt/nfast/cknfastrc

% docker cp pkcs11.yml dap-wnfast:/opt/conjur/etc/pkcs11.yml
```

6. Generate a new Key Encryption Key (KEK) for Conjur to be stored on the HSM:

```
% docker exec dap-wnfast evoke pkcs11 generate
```

7. Start the `conjur-appliance` container, which will act as the Master DAP Server, in Interactive mode:

```
% docker exec -i -t dap-wnfast /bin/bash
```

The KEK is now ready for use.

2.4. Example commands used with the KEK

```
% evoke pkcs11 wrap
% evoke keys lock
% evoke keys unlock
```

For more examples, see Server Key Encryption Methods in the CyberArk online documentation.

Chapter 3. Additional resources and related products

3.1. Video

3.2. nShield Connect

3.3. nShield as a Service

3.4. nShield Container Option Pack

3.5. Entrust digital security solutions

3.6. nShield product documentation