Yubico YubiHSM 2 Setup

CBOM Secure · HSM Sensor (Discover_HSM)

Overview

This guide configures a Yubico YubiHSM 2 for read-only discovery by the CBOM Secure Discover_HSM sensor. The sensor connects via the yubihsm-connector daemon and the PKCS#11 library (yubihsm_pkcs11.so) and enumerates:

- Asymmetric keys - RSA and EC pairs (metadata only: key ID, algorithm, label, domains, capabilities)
- Opaque objects - X.509 certificates and raw binary blobs
- HMAC keys - symmetric HMAC objects (metadata only: key ID, algorithm, label)

No private key material or secret values are extracted. The sensor uses a dedicated authentication key with the minimum required capabilities.

Prerequisites

- A YubiHSM 2 connected to the target host via USB.
- A supported Linux distribution (Ubuntu 20.04+, Debian 11+, or RHEL/CentOS 8+).
- root/sudo access on the host.
- The admin authentication key credentials (factory default key ID 1, password 'password').
- Reachability to the connector endpoint (default http://localhost:12345; open TCP 12345 if the sensor is remote).
- pkcs11-tool available (from opensc).
- The CBOM platform deployed with access to the sensor configuration interface.

Step-by-Step Guide

Step 1: Install the Connector, Shell, and PKCS#11 Library

```
curl -fsSL https://developers.yubico.com/Software_Projects/Yubico_APT_repo/Release.key \
  | gpg --dearmor | sudo tee /usr/share/keyrings/yubico-archive-keyring.gpg > /dev/null
echo "deb [signed-by=/usr/share/keyrings/yubico-archive-keyring.gpg]
https://developers.yubico.com/Software_Projects/Yubico_APT_repo/Debian/stable/ stable
main" | sudo tee /etc/apt/sources.list.d/yubico.list
sudo apt-get update && sudo apt-get install -y yubihsm-connector yubihsm-shell yubihsm-
pkcs11 opensc
sudo systemctl enable --now yubihsm-connector
curl -s http://localhost:12345/connector/status      # expect status=OK
```

Step 2: Create a Read-Only Authentication Key

Open an admin session and create a key limited to the five capabilities the sensor needs:

```
yubihsm-shell --connector http://localhost:12345
yubihsm> connect
yubihsm> session open 1 password
yubihsm> put authkey 0 0 "cbom-readonly" 1 \
  get-pseudo-random:get-log-entries:get-opaque:list-objects:get-public-key \
  none cbomReadOnly!Sensor1
yubihsm> list objects 0 0 any any any any any      # confirm the new authentication-key
yubihsm> session close 0
yubihsm> quit
```

Note Record the assigned object ID (e.g. 0x0002) - it is the auth_key_id in the sensor config. Adjust the domain bitmask (1) to cover all domains the sensor must inspect.

Step 3: Configure the PKCS#11 Module

```
sudo tee /etc/yubihsm_pkcs11.conf > /dev/null <<EOF
connector = http://localhost:12345
debug = 0
EOF
ls -l /usr/lib/x86_64-linux-gnu/pkcs11/yubihsm_pkcs11.so    # record this path
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_HSM
    enabled: true
    type: hsm
    vendor: yubico
    model: yubihsm2
    connection:
      connector_url: "http://localhost:12345"
      pkcs11_library_path: "/usr/lib/x86_64-linux-gnu/pkcs11/yubihsm_pkcs11.so"
      pkcs11_conf_path: "/etc/yubihsm_pkcs11.conf"
    authentication:
      auth_key_id: "0x0002"
      auth_key_password: "${YUBIHSM_AUTH_PASSWORD}"
      domain: 1
    discovery:
      object_types: [asymmetric-key, opaque, hmac-key]
      all_domains: true
      include_public_key_metadata: true
      include_opaque_metadata: true
      include_hmac_metadata: true
    scheduling:
      interval_minutes: 60
      run_on_start: true
```

Step 5: Validate

```
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/pkcs11/yubihsm_pkcs11.so --list-slots
# PIN format is <key-id-decimal>:<password>  (0x0002 -> 2)
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/pkcs11/yubihsm_pkcs11.so \
  --login --pin "2:cbomReadOnly!Sensor1" --list-objects
journalctl -u cbom-sensor -f
```

Slot enumeration plus an object list confirms the library, connector, and auth key are functional. Then trigger a manual Discover_HSM run and confirm object metadata appears with no errors.

Common Errors

Connector not reachable (connection refused)

Cause: yubihsm-connector is not running or the device is not attached.

Resolution: Confirm lsusb | grep Yubico, restart the connector, and check journalctl -u yubihsm-connector for USB errors.

C_Login failed: CKR_PIN_INCORRECT

Cause: The PIN is not in <key-id-decimal>:<password> form, or the key password does not match.

Resolution: Use the decimal key ID (0x0002 -> 2), verify the password; if lost, recreate the auth key per Step 2.

InsufficientPermissions / CKR_USER_NOT_LOGGED_IN

Cause: The auth key is missing a required capability, or its domain mask excludes the target objects.

Resolution: Run get objectinfo to check capabilities and domains; if incomplete, delete and recreate the key with the five capabilities and correct domains.

Security Recommendations

- Use a dedicated authentication key with only the five minimum capabilities - never share it.
- Keep yubihsm-connector bound to localhost; if remote, tunnel over WireGuard/SSH rather than exposing port 12345.
- Inject the auth key password from a secrets manager, not plaintext config.
- Rotate the read-only auth key on the same cadence as other service credentials.
- Independently export and review the YubiHSM audit log to detect access outside normal sensor activity.

Conclusion

With the connector installed, a least-privilege authentication key created, and the PKCS#11 module configured, the Discover_HSM sensor continuously enumerates asymmetric keys, opaque certificate objects, and HMAC keys on the YubiHSM 2 - metadata only, no secret material - giving CBOM Secure full visibility into HSM-resident cryptographic assets.