Google Cloud HSM Setup

CBOM Secure · HSM Sensor (Discover_HSM)

Overview

This guide configures the CBOM Secure HSM Sensor to discover cryptographic assets managed by Google Cloud HSM — GCP's hardware-backed key management delivered through Cloud KMS with HSM protection level. Discovery is performed entirely through the Cloud KMS REST/gRPC API; Cloud HSM does not expose a PKCS#11 interface, so no library path or slot configuration is required.

- HSM-protected symmetric keys (AES-128/256) for envelope encryption
- HSM-protected asymmetric keys (RSA-2048/3072/4096, EC P-256/P-384) for signing and decryption
- Key ring metadata, key version states, rotation schedules, and key purpose classifications

Prerequisites

- A GCP project with one or more Cloud KMS key rings using PROTECTION_LEVEL: HSM.
- A GCP account with Project IAM Admin (or equivalent) to create service accounts and assign roles.
- The Google Cloud Console or an authenticated gcloud CLI.
- The CBOM platform able to reach https://cloudkms.googleapis.com outbound on port 443.

Step-by-Step Guide

Step 1: Enable the Cloud KMS API

```
gcloud services enable cloudkms.googleapis.com --project=YOUR_PROJECT_ID
gcloud services list --enabled --filter="name:cloudkms.googleapis.com" --
project=YOUR_PROJECT_ID
```

Step 2: Confirm HSM Key Rings Exist

```
gcloud kms keyrings list --location=us-east1 --project=YOUR_PROJECT_ID
gcloud kms keys list --keyring=YOUR_KEY_RING_NAME --location=us-east1 \
  --project=YOUR_PROJECT_ID --filter="versionTemplate.protectionLevel=HSM"
```

Step 3: Create a Dedicated Service Account

```
gcloud iam service-accounts create cbom-hsm-sensor \
  --display-name="CBOM HSM Sensor" \
  --project=YOUR_PROJECT_ID
```

Step 4: Grant Read-Only Cloud KMS Access

Assign roles/cloudkms.viewer — read-only access to list key rings, keys, key versions, and metadata. It does not permit encrypt, decrypt, or sign operations.

```
gcloud projects add-iam-policy-binding YOUR_PROJECT_ID \
  --member="serviceAccount:cbom-hsm-
sensor@YOUR_PROJECT_ID.iam.gserviceaccount.com" \
  --role="roles/cloudkms.viewer"
```

To scope to a single key ring instead, bind the role at the key ring resource level with gcloud kms keyrings add-iam-policy-binding.

Step 5: Generate a JSON Key File

```
gcloud iam service-accounts keys create /etc/cbom/credentials/gcp-hsm-sensor-key.json \
  --iam-account=cbom-hsm-sensor@YOUR_PROJECT_ID.iam.gserviceaccount.com \
  --project=YOUR_PROJECT_ID
chmod 600 /etc/cbom/credentials/gcp-hsm-sensor-key.json
```

Note In production, prefer Workload Identity Federation over a long-lived JSON key, or retrieve the key from GCP Secret Manager at startup. Never commit it to source control.

Step 6: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_HSM
    type: gcp_cloud_hsm
    enabled: true
    connection:
      project_id: "my-production-project-123456"
      credentials_file: "/etc/cbom/credentials/gcp-hsm-sensor-key.json"
    scope:
      locations: ["us-east1", "us-central1", "global"]
      protection_levels: ["HSM"]
    discovery:
      collect_rotation_schedule: true
      collect_key_purpose: true
      collect_algorithm: true
    schedule:
      interval_hours: 24
```

Step 7: Validate

```
export GOOGLE_APPLICATION_CREDENTIALS=/etc/cbom/credentials/gcp-hsm-sensor-
key.json
cbom sensor run --config /etc/cbom/sensors/gcp-cloud-hsm.yaml --dry-run
cbom sensor run --config /etc/cbom/sensors/gcp-cloud-hsm.yaml
```

Confirm a table of key rings, keys, protection levels, and algorithms appears, then verify HSM-protected keys under Assets → HSM Keys filtered by sensor_source: gcp-cloud-hsm.

Common Errors

403 Permission Denied on cloudkms.keyRings.list

Cause: The service account lacks roles/cloudkms.viewer on the project, or the role was bound only at key-ring level while a project-wide list is attempted.

Resolution: Confirm/assign the binding (Step 4); if using key-ring-scoped permissions, list each key ring explicitly in scope.key_rings.

Could not load credentials file

Cause: The credentials_file path is wrong or unreadable by the CBOM user.

Resolution: Confirm the file exists and is readable; fix ownership/permissions (chown cbom-service, chmod 600).

Cloud KMS API has not been enabled

Cause: The Cloud KMS API is not enabled in the project.

Resolution: Run gcloud services enable cloudkms.googleapis.com and allow 30-60s for propagation.

Security Recommendations

- Use roles/cloudkms.viewer exclusively — never admin or encrypter/decrypter roles.
- Prefer Workload Identity Federation over JSON keys where CBOM runs on GKE/Compute.
- Rotate the JSON key at least every 90 days; store it in Secret Manager.
- Enable Cloud Audit Logs (DATA_READ) for Cloud KMS and review the service account's activity.
- Use VPC Service Controls / Private Service Connect for cloudkms.googleapis.com where possible.

Conclusion

With the Cloud KMS API enabled, a read-only cloudkms.viewer service account, and credentials supplied to the sensor, the CBOM Secure HSM Sensor enumerates all HSM-protected key rings and keys — including algorithm, purpose, version state, and rotation schedule — on the configured schedule.