IBM Cloud Hyper Protect Crypto Services Setup

CBOM Secure · Cloud Sensor (Discover_Cloud)

Overview

This guide configures the CBOM Secure Discover_Cloud sensor to connect to IBM Cloud Hyper Protect Crypto Services (HPCS) — a FIPS 140-2 Level 4 cloud HSM built on IBM Crypto Express — and enumerate, read-only via the IBM Cloud KMS API:

- Symmetric and asymmetric keys and their metadata
- Key states (active, suspended, deactivated, destroyed)
- Key policies, rotation schedules, and expiration dates
- Key rings, resource-group assignments, root keys, and standard keys

Prerequisites

- An IBM Cloud account able to create service instances and IAM resources.
- The IBM Cloud CLI installed; the TKE plugin for domain initialization.
- IAM permissions to create instances and API keys and assign policies.
- Connectivity from the sensor host to the regional KMS endpoint (e.g. us-south.kms.cloud.ibm.com).
- The Discover_Cloud sensor binary installed.

Step-by-Step Guide

Step 1: Provision an HPCS Instance

In the IBM Cloud catalog, create a Hyper Protect Crypto Services instance (region, plan, resource group, name e.g. cbom-hpcs-prod). Record the Instance ID (GUID), KMS API endpoint, and GREP11 endpoint from the instance overview.

Step 2: Initialize the Service Domain (TKE)

```
ibmcloud login --sso
ibmcloud target -g <resource-group-name> -r us-south
ibmcloud plugin install tke
ibmcloud tke cryptounits
ibmcloud tke domain-zeroize
ibmcloud tke domain-mk-clr
# load/commit/activate master key parts as prompted, then enable GREP11 in the console
```

Step 3: Create a Service ID and Read-Only Policy

Under Manage → Access (IAM) → Service IDs, create cbom-hpcs-readonly. Assign access to Hyper Protect Crypto Services scoped to the specific instance, with Platform role Viewer and Service access role Reader. Do not grant Writer, Manager, or Editor/Administrator.

Step 4: Create an API Key

On the service ID's API keys tab, create cbom-hpcs-sensor-key and copy the value immediately (shown once); store it in a secrets manager.

Step 5: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_Cloud
    enabled: true
    provider: ibm_hpcs
    schedule: "0 2 * * *"
    connection:
      region: "us-south"
      instance_id: "a1b2c3d4-e5f6-7890-abcd-ef1234567890"
      kms_endpoint: "https://us-south.kms.cloud.ibm.com"
      grep11_endpoint: "ep11.us-south.hs-crypto.cloud.ibm.com:13412"
    auth:
      type: iam_api_key
      api_key: "${IBM_CLOUD_API_KEY}"
    discovery:
      key_metadata: true
      key_rings: true
      key_policies: true
    tls:
      verify: true
export IBM_CLOUD_API_KEY="<paste-api-key-value>"
```

Step 6: Validate

```
systemctl restart cbom-sensor
journalctl -u cbom-sensor -n 100 --no-pager
ibmcloud kp keys -i <instance-id> --output json | jq ". | length"
```

Confirm a successful KMS connection and discovered key count. In Activity Tracker, only read-only API calls (e.g. kms.secrets.list) should appear from cbom-hpcs-readonly.

Common Errors

401 Unauthorized — Invalid IAM token

Cause: The API key is wrong/deleted, or the variable was not exported.

Resolution: Check IBM_CLOUD_API_KEY; recreate the key if deleted and restart.

403 Forbidden — Insufficient IAM permissions

Cause: The service ID lacks the Reader service-access role on the instance, or targets the wrong GUID.

Resolution: Confirm the policy targets the correct instance with Reader; allow up to 60s for propagation.

Connection timeout — KMS endpoint unreachable

Cause: A firewall/egress rule blocks the endpoint, or the URL is wrong.

Resolution: Test with curl -v https://us-south.kms.cloud.ibm.com; allow HTTPS to *.kms.cloud.ibm.com and confirm the endpoint.

Security Recommendations

- Use a dedicated service ID per environment; do not share API keys.
- Scope IAM policies to the specific HPCS instance GUID.
- Rotate the API key every 90 days (create new before deleting old).
- Store the key in a secrets manager and inject via env/EnvironmentFile (chmod 600).
- Alert in Activity Tracker on any write/delete events from the service ID.

Conclusion

With an initialized HPCS instance, a least-privilege IAM service ID, and the Discover_Cloud sensor, CBOM Secure maintains an up-to-date inventory of all keys managed in HPCS via the read-only KMS API — supporting compliance and posture assessment.