StorageTek / Oracle Key Manager 3 Setup

CBOM Secure · KMIP Sensor (Discover_KMIP)

Overview

This guide configures StorageTek Oracle Key Manager 3 (OKM) — a KMIP-compliant KMS for tape drives and storage encryption — as a source for the CBOM Secure Discover_KMIP sensor, over KMIP 1.2+ on mutual TLS port 5696 in read-only Operator mode:

- Managed key objects (symmetric keys, private/public keys, secret data)
- Key metadata: UIDs, algorithm, length, state, activation/expiration dates
- Lifecycle attributes: creation/last-change dates, process start date, deactivation reason
- Certificate objects in the OKM certificate manager

Prerequisites

- Admin access to the OKM Manager GUI (https://<okm-primary-node>:7443/).
- OKM 3.2+ with a license including the KMIP feature module.
- Connectivity from the sensor host to TCP 5696; the OKM cluster CA (PEM).
- The CBOM agent installed with the Discover_KMIP plugin.

Step-by-Step Guide

Step 1: Create an OKM Operator User

In OKM Manager → Security → Users → Create, add cbom-sensor with Role Operator (read-only key metadata access) and a strong passphrase. Confirm the role and Enabled = Yes in the user detail.

Step 2: Enable KMIP on the Cluster

Under Cluster → Settings → KMIP, check Enable KMIP with Port 5696, Protocol Version 1.2+, Require Client Certificate = Yes, and the OKM Cluster CA. Apply, then confirm the listener:

```
openssl s_client -connect <okm-primary-node>:5696 \
  -CAfile /path/to/okm-cluster-ca.pem -showcerts
```

Step 3: Enroll and Export the Client Certificate

Under Security → Certificates → Create, enroll a certificate for user cbom-sensor (alias cbom-sensor-cert, RSA 2048, 730-day validity). Export it as PKCS#12, and export the OKM Cluster CA as PEM (Security → Certificate Authorities). Transfer both to the sensor host, then convert the P12 to PEM if needed:

```
openssl pkcs12 -in /etc/cbom/certs/cbom-sensor-cert.p12 -clcerts -nokeys \
  -out /etc/cbom/certs/cbom-sensor.crt.pem -passin pass:<export-pw>
openssl pkcs12 -in /etc/cbom/certs/cbom-sensor-cert.p12 -nocerts \
```

```
  -out /etc/cbom/certs/cbom-sensor.key.pem -passin pass:<export-pw> -passout pass:<key-pw>
chmod 600 /etc/cbom/certs/cbom-sensor.key.pem
chown cbom-agent:cbom-agent /etc/cbom/certs/cbom-sensor.key.pem
```

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_KMIP
  enabled: true
connection:
  host: okm-primary.example.internal
  port: 5696
  protocol: kmip
  kmip_version: "1.2"
  tls:
    enabled: true
    mutual_tls: true
    ca_cert: /etc/cbom/certs/okm-cluster-ca.pem
    client_cert: /etc/cbom/certs/cbom-sensor.crt.pem
    client_key: /etc/cbom/certs/cbom-sensor.key.pem
    client_key_passphrase_env: CBOM_OKM_KEY_PASSPHRASE
    verify_hostname: true
authentication:
  method: certificate
  username: cbom-sensor
discovery:
  object_types: [SymmetricKey, PrivateKey, PublicKey, Certificate, SecretData]
output:
  cbom_endpoint: https://cbom-server.example.internal:8443/api/v1/ingest
  tags: { source: storagetek-okm3 }
```

Step 5: Validate

```
sudo journalctl -u cbom-agent -n 100 | grep -i "okm\|kmip"
cbom-agent run-sensor --config /etc/cbom/sensors/okm3-kmip.yaml --dry-run
```

Confirm a KMIP session and an ingested-object count. In OKM Manager → Security → Audit Log, only Locate and Get Attribute operations should appear for cbom-sensor.

Common Errors

TLS handshake — certificate unknown

Cause: The client cert isn't issued by the OKM cluster CA, is revoked, or the user is disabled.

Resolution: Confirm cbom-sensor is enabled and the cert is associated; re-export if expired/revoked; ensure ca_cert is the OKM cluster CA.

Permission denied (Get)

Cause: The config requests an attribute implying key-material export (e.g. KeyValue/KeyBlock).

Resolution: Restrict the attributes list to metadata only (algorithm, state, dates); keep the user on the Operator role.

Connection refused on 5696

Cause: KMIP is not enabled/running, or a firewall blocks 5696.

Resolution: Enable KMIP under Cluster → Settings, check Cluster → Services, and open TCP 5696 to the sensor host.

Security Recommendations

- Use only the Operator role — never SecurityOfficer or Compliance Officer.
- Protect the client key (chmod 600, chown cbom-agent); supply the passphrase via env/secrets manager.
- Rotate the client certificate before its 730-day expiry (renew near day 700).
- Enforce TLS 1.2 minimum; reject TLS 1.0/1.1 in Cluster → Settings → TLS.
- Monitor the OKM audit log; alert on operations beyond Locate/Get Attribute.

Conclusion

With an Operator-role user, KMIP enabled cluster-wide, and a CA-signed client certificate, the Discover_KMIP sensor gains read-only access to OKM key metadata — supporting visibility into lifecycle states, algorithms, and expiration risk across the storage key management infrastructure.