MySQL Setup

CBOM Secure · Database TDE Sensor (Discover_DB)

Overview

This guide connects the CBOM Secure Discover_DB sensor to a MySQL 8.0+ instance using InnoDB data-at-rest encryption. Using a dedicated least-privilege user, the sensor discovers, read-only:

- Encryption keys registered in the keyring (keyring_file, keyring_okv, keyring_hashicorp)
- InnoDB tablespace encryption status and associated key identifiers
- Active keyring plugin metadata and configuration state

No data is modified and no key material is extracted — metadata only.

Prerequisites

- MySQL 8.0 or later, running with InnoDB data-at-rest encryption and a supported keyring plugin.
- performance_schema enabled (default in 8.0+).
- A MySQL account with GRANT privileges (root or a DBA account).
- Connectivity from the sensor host to the MySQL port (default 3306).
- The CBOM agent installed with the Discover_DB module.
- SSL/TLS configured on the server if the connection crosses an untrusted network.

Step-by-Step Guide

Step 1: Create the CBOM Reader Account

Create a dedicated user (scope the host to the sensor IP in production):

```
CREATE USER 'cbom_reader'@'%' IDENTIFIED BY 'StrongPassword123!';
-- or restrict the origin:
CREATE USER 'cbom_reader'@'192.168.10.50' IDENTIFIED BY 'StrongPassword123!';
```

Step 2: Grant the Minimum Privileges

```
GRANT SELECT ON performance_schema.keyring_keys TO 'cbom_reader'@'%';        -- keyring key metadata
GRANT PROCESS ON *.* TO 'cbom_reader'@'%';                                   -- process/session state
GRANT SELECT ON information_schema.INNODB_TABLESPACES TO 'cbom_reader'@'%';
-- tablespace encryption status
FLUSH PRIVILEGES;

SHOW GRANTS FOR 'cbom_reader'@'%';
```

Step 3: Verify the Keyring Plugin and Metadata

```
SHOW PLUGINS;                        -- expect a KEYRING plugin with Status ACTIVE
```

```
SELECT * FROM performance_schema.keyring_keys;
SELECT SPACE, NAME, ENCRYPTION FROM information_schema.INNODB_TABLESPACES
WHERE ENCRYPTION = 'Y' LIMIT 10;
```

Returned keyring rows and encrypted tablespaces confirm the sensor will be able to collect key identifiers. An empty keyring set means encryption is configured but no keys are generated yet.

Step 4: (Recommended) Configure SSL/TLS

Confirm SSL is available (SHOW VARIABLES LIKE '%ssl%' — have_ssl = YES), optionally enforce it for the account, and stage the CA certificate on the sensor host:

```
ALTER USER 'cbom_reader'@'%' REQUIRE SSL;    -- optional hardening
# copy the server CA (default /var/lib/mysql/ca.pem) to the sensor host:
#   /etc/cbom/certs/mysql-ca.pem
```

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_DB
  enabled: true
  schedule: "0 */6 * * *"        # every 6 hours
target:
  type: mysql
  host: "mysql.internal.example.com"
  port: 3306
  database: "performance_schema"
credentials:
  username: "cbom_reader"
  password: "${CBOM_MYSQL_PASSWORD}"
tls:
  enabled: true
  ca_cert: "/etc/cbom/certs/mysql-ca.pem"
  verify_server_cert: true
discovery:
  keyring: { enabled: true, source_table: performance_schema.keyring_keys }
  tablespaces: { enabled: true, source_table: information_schema.INNODB_TABLESPACES,
filter_encrypted_only: true }
  plugins: { enabled: true, query: SHOW PLUGINS, filter_type: KEYRING }
output:
  format: "cbom-json"
  destination: "/var/cbom/output/mysql-tde/"
```

Inject CBOM_MYSQL_PASSWORD from a secrets manager rather than a plain environment variable in production.

Step 6: Validate

```
cbom sensor run --name Discover_DB --config /etc/cbom/sensors/mysql-tde.yaml --dry-run
cbom sensor run --name Discover_DB --config /etc/cbom/sensors/mysql-tde.yaml
```

Confirm authentication, an ACTIVE keyring plugin, and discovered keyring-key and encrypted-tablespace counts. Verify assets under Sensors -> Discover_DB -> MySQL in the CBOM console.

Common Errors

Access denied for user 'cbom_reader'

Cause: The account is missing for the connecting host, the password is wrong, or the host restriction does not match the sensor IP.

Resolution: Confirm the user/host in mysql.user, align the account host with the sensor origin, and reset the password with ALTER USER if needed.

Table 'performance_schema.keyring_keys' doesn't exist

Cause: The table exists only in MySQL 8.0.16+ and only when a keyring plugin is loaded.

Resolution: Confirm the version (SELECT VERSION()) and an ACTIVE KEYRING plugin; load one via early-plugin-load in my.cnf and restart.

SSL is required but the server doesn't support it

Cause: tls.enabled is true but the server has SSL disabled or was built without it.

Resolution: Confirm have_ssl = YES; enable ssl-ca/ssl-cert/ssl-key in my.cnf and restart. Only set tls.enabled: false as a documented temporary workaround on trusted networks.

Security Recommendations

- Use a dedicated read-only account with only the three grants above — never a DBA or root account.
- Restrict the account origin to the sensor host IP rather than '%'.
- Store the password in a secrets manager and rotate on schedule.
- Enforce SSL (REQUIRE SSL) with a valid CA certificate to prevent credential interception.
- Enable the MySQL audit log plugin for cbom_reader and review query patterns periodically.

Conclusion

By querying performance_schema.keyring_keys and information_schema.INNODB_TABLESPACES with a least-privilege user, the Discover_DB sensor builds a complete inventory of active encryption keys and encrypted tablespaces in MySQL 8.0+ — without accessing application data or extracting key material — keeping the CBOM Secure inventory current for compliance and risk assessment.