

Oracle Database (TDE) Setup

CBOM Secure - Database Sensor (Discover_DB)

Overview

This guide configures Oracle Database so the CBOM Secure Discover_DB sensor can discover Transparent Data Encryption (TDE) assets read-only, by querying data dictionary views:

- TDE wallet keys - master key metadata from V\$ENCRYPTION_KEYS and V\$ENCRYPTION_WALLET
- Encrypted tablespaces - status and algorithm via V\$ENCRYPTED_TABLESPACES
- Encrypted columns - column-level metadata via DBA_ENCRYPTED_COLUMNS

The sensor reads key metadata only - never raw key material, wallet passwords, or plaintext data - through a dedicated least-privilege database account.

Prerequisites

- Oracle Database 12c Release 2 (12.2) or later, reachable from the sensor host.
- TDE enabled with the wallet OPEN (V\$ENCRYPTION_WALLET.STATUS = 'OPEN' or 'OPEN_NO_MASTER_KEY').
- A DBA-privileged account (SYS AS SYSDBA or a DBA grantee) to create the reader and assign grants.
- Network reachability to the Oracle listener (default 1521); verify with telnet <host> 1521.
- The Oracle JDBC thin driver (ojdbc8.jar or ojdbc11.jar) on the sensor host if using JDBC.
- The target service name or SID.

Step-by-Step Guide

Step 1: Create the CBOM Reader Database User

Connect as a privileged user (for a PDB, connect to the PDB service):

```
sqlplus sys/<sys_password>@//<oracle-host>:1521/<service_name> AS SYSDBA
CREATE USER cbom_reader IDENTIFIED BY "<strong_password>"
  DEFAULT TABLESPACE USERS
  TEMPORARY TABLESPACE TEMP
  ACCOUNT UNLOCK;

GRANT CREATE SESSION TO cbom_reader;
```

Step 2: Grant Least-Privilege SELECT Access

Grant SELECT on the underlying V_\$ synonyms (not V\$, which returns ORA-02030), plus the data dictionary view and catalog role:

```
GRANT SELECT ON V_$ENCRYPTION_WALLET TO cbom_reader;
```

```
GRANT SELECT ON V_$ENCRYPTED_TABLESPACES TO cbom_reader;
GRANT SELECT ON V_$ENCRYPTION_KEYS TO cbom_reader;
GRANT SELECT ON DBA_ENCRYPTED_COLUMNS TO cbom_reader;
GRANT SELECT CATALOG_ROLE TO cbom_reader;
```

Verify the grants:

```
SELECT PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE GRANTEE =
'CBOM_READER' ORDER BY TABLE_NAME;
SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'CBOM_READER';
```

Step 3: Verify Reader Account Access

Log in as cbom_reader and confirm each view returns without ORA- errors:

```
sqlplus cbom_reader/<strong_password>@//<oracle-host>:1521/<service_name>

SELECT * FROM V$ENCRYPTION_WALLET;
SELECT TABLESPACE_NAME, ENCRYPTEDTS, ENCRYPTIONALG, STATUS FROM
V$ENCRYPTED_TABLESPACES;
SELECT KEY_ID, CREATION_TIME, CREATOR FROM V$ENCRYPTION_KEYS;
SELECT OWNER, TABLE_NAME, COLUMN_NAME, ENCRYPTION_ALG FROM
DBA_ENCRYPTED_COLUMNS FETCH FIRST 10 ROWS ONLY;
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
- name: Discover_DB
  type: oracle_tde
  enabled: true
  schedule: "0 2 * * *"
  connection:
    host: "oracle-db.internal.example.com"
    port: 1521
    service_name: "ORCLPDB1"      # use service_name OR sid
    username: "cbom_reader"
    password: "${CBOM_ORACLE_PASSWORD}"
    connection_timeout_seconds: 30
    query_timeout_seconds: 120
  ssl:
    enabled: true
    wallet_path: "/opt/cbom/oracle/wallet"
  discovery:
    include_encrypted_tablespaces: true
    include_encrypted_columns: true
    include_wallet_keys: true
    column_sample_limit: 1000
  output:
    cbom_tag: "oracle-tde"
```

Inject the password via \${CBOM_ORACLE_PASSWORD} from a secrets manager - never hard-code it.

Step 5: Validate

```
cbom-sensor run --sensor Discover_DB --dry-run --log-level DEBUG
# then persist to inventory:
cbom-sensor run --sensor Discover_DB
```

A successful dry run reports rows returned for each view and the asset count. Confirm assets under Inventory > Database > Oracle TDE.

Common Errors

ORA-01031 - Insufficient Privileges

Cause: The grant was issued on V\$ENCRYPTION_WALLET instead of the underlying V_\$ENCRYPTION_WALLET synonym.

Resolution: Re-issue grants on the V_\$ objects and confirm with SESSION_PRIVS as cbom_reader.

ORA-28365 - Wallet Is Not Open

Cause: The TDE wallet is closed; V\$ENCRYPTION_KEYS requires an OPEN wallet.

Resolution: Have a DBA run ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN, or verify cwallet.sso exists for auto-login, then re-check STATUS.

IO Error - Network Adapter Could Not Establish the Connection

Cause: The sensor host cannot reach the listener - wrong host/port, firewall, or listener down.

Resolution: Confirm lsnrctl status, test telnet <host> 1521, open TCP 1521 from the sensor host, and match host/port/service_name.

Security Recommendations

- Use a dedicated cbom_reader account exclusively - never reuse application or DBA accounts.
- Rotate the reader password every 90 days and update the secret store.
- Restrict the listener with Oracle Net or security-group rules to the sensor host IP only.
- Enable Oracle Unified Auditing on cbom_reader SELECT activity.
- Never grant DBA, INSERT, UPDATE, DELETE, DROP, or ALTER; audit grants for privilege creep.

Conclusion

With a least-privilege cbom_reader account and SELECT-only grants on TDE views, the Discover_DB sensor builds a continuous, read-only inventory of TDE master keys, encrypted tablespaces, and encrypted columns across the Oracle fleet - giving the security team ongoing visibility into TDE posture without ever touching raw key material.