Oracle Unified Directory Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

Overview

This guide configures Oracle Unified Directory (OUD) - or Oracle Directory Server Enterprise Edition - so the CBOM Secure Discover_LDAP sensor can connect over LDAPS and perform read-only discovery of cryptographic assets stored in the directory:

- userCertificate - X.509 certificates bound to user or service accounts
- cACertificate - CA certificates stored on organizational unit or root entries
- sshPublicKey - SSH public keys associated with user identities

OUD is built on the OpenDJ codebase and supports LDAP (389) and LDAPS (636). The sensor uses a dedicated, least-privilege service account over LDAPS for search and compare operations only - no write access is granted at any point.

Prerequisites

- Oracle Unified Directory 11g Release 2 (11.1.2.x) or later, or Oracle Directory Server Enterprise Edition 11g, installed and running.
- Administrative access via the OUD Control Panel or shell access to $OUD_INSTANCE_ROOT/bin.
- The ldapmodify and ldapsearch tools (bundled under $OUD_INSTANCE_ROOT/bin).
- The base DN of the directory tree (e.g. dc=corp,dc=example,dc=com).
- An OU for service accounts such as ou=ServiceAccounts,dc=corp,dc=example,dc=com (create it if absent).
- A valid TLS certificate on the LDAPS listener (port 636).
- The Discover_LDAP sensor module deployed with network connectivity to port 636 (or 389).

Step-by-Step Guide

Step 1: Create the CBOM Service Account

Prepare an LDIF entry under ou=ServiceAccounts. Replace the password with a strong value and store it in your secrets manager.

```
cat > /tmp/cbom-reader-add.ldif << 'EOF'
dn: cn=cbom-reader,ou=ServiceAccounts,dc=corp,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: cbom-reader
sn: CBOMReader
uid: cbom-reader
```

```
description: Read-only service account for CBOM discovery
userPassword: <CBOM_SERVICE_ACCOUNT_PASSWORD>
EOF
```

Add the entry with an administrative bind DN:

```
$OUD_INSTANCE_ROOT/bin/ldapmodify --hostname oud.corp.example.com \
  --port 636 --useSSL --trustAll \
  --bindDN "cn=Directory Manager" --bindPassword "<ADMIN_PASSWORD>" \
  --defaultAdd --filename /tmp/cbom-reader-add.ldif
```

Step 2: Apply a Read-Only Access Control Instruction (ACI)

This ACI grants read/search/compare on the three cryptographic attributes across the tree rooted at the base DN.

```
cat > /tmp/cbom-aci.ldif << 'EOF'
dn: dc=corp,dc=example,dc=com
changetype: modify
add: aci
aci: (targetattr="userCertificate || cACertificate || sshPublicKey")
 (version 3.0; acl "CBOM Read - cryptographic attributes";
  allow(read,search,compare)
  userdn="ldap:///cn=cbom-reader,ou=ServiceAccounts,dc=corp,dc=example,dc=com";)
EOF

$OUD_INSTANCE_ROOT/bin/ldapmodify --hostname oud.corp.example.com \
  --port 636 --useSSL --trustAll \
  --bindDN "cn=Directory Manager" --bindPassword "<ADMIN_PASSWORD>" \
  --filename /tmp/cbom-aci.ldif
```

Note ACIs take effect immediately in OUD - no restart required. Use || (double pipe) as the attribute separator, and ensure no trailing spaces on continuation lines.

Step 3: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_LDAP
    enabled: true
    description: "CBOM LDAP sensor for Oracle Unified Directory"
    connection:
      host: oud.corp.example.com
      port: 636
      use_ssl: true
      verify_ssl: true
      ca_cert_path: /etc/cbom/certs/oud-ca-chain.pem
    authentication:
      method: simple
      bind_dn: "cn=cbom-reader,ou=ServiceAccounts,dc=corp,dc=example,dc=com"
      bind_password_env: CBOM_OUD_BIND_PASSWORD
    discovery:
      base_dn: "dc=corp,dc=example,dc=com"
      scope: sub
      page_size: 500
      attributes: [userCertificate, cACertificate, sshPublicKey]
      filter: "(|(userCertificate=*)(cACertificate=*)(sshPublicKey=*))"
    schedule:
      interval_hours: 24
      start_time: "02:00"
    output:
```

```
    tags: { source: oracle-oud, environment: production }
```

Inject the bind password from a secrets manager into CBOM_OUD_BIND_PASSWORD; do not store it in the YAML.

Step 4: Validate

```
# 1. TLS handshake
openssl s_client -connect oud.corp.example.com:636 -CAfile /etc/cbom/certs/oud-ca-chain.pem
# 2. Bind + read as the service account
$OUD_INSTANCE_ROOT/bin/ldapsearch --hostname oud.corp.example.com --port 636 --
useSSL \
  --trustStorePath /etc/cbom/certs/oud-ca-chain.pem \
  --bindDN "cn=cbom-reader,ou=ServiceAccounts,dc=corp,dc=example,dc=com" \
  --bindPassword "<CBOM_SERVICE_ACCOUNT_PASSWORD>" \
  --baseDN "dc=corp,dc=example,dc=com" --searchScope sub "(userCertificate=*)" dn
userCertificate
# 3. Manual sensor run
cbom sensor run --name Discover_LDAP --config /etc/cbom/sensors/oud.yaml
```

A handshake returning Verify return code: 0 (ok) and a successful bind confirm the setup. Then filter by source: oracle-oud in Inventory > Certificates.

Common Errors

LDAP Result Code 49 - Invalid Credentials

Cause: The bind DN or password does not match the OUD entry, or the account was not created successfully.

Resolution: Verify the entry exists, confirm CBOM_OUD_BIND_PASSWORD, and reset with a replace: userPassword change if needed.

SSL Handshake Failed - PKIX Path Building Failed

Cause: The sensor's JVM/TLS library does not trust the OUD CA chain.

Resolution: Export the CA to oud-ca-chain.pem, set ca_cert_path, and (for Java sensors) keytool -importcert into the JVM truststore, then restart.

LDAP Result Code 50 - Insufficient Access Rights

Cause: The ACI did not apply, targeted the wrong base DN, or has a syntax error.

Resolution: Re-verify the ACI on the base DN, check $OUD_INSTANCE_ROOT/logs/errors for aci warnings, use || as separator, and match the userdn exactly.

Security Recommendations

- Use LDAPS exclusively - never connect over plain LDAP (389) in any environment.
- Scope the ACI to specific attributes; never use (targetattr="*") which would expose userPassword.
- Rotate the cbom-reader password at least every 90 days and update the secret store immediately.

- Apply a password policy preventing interactive/self-service use of the account.
- Enable OUD access logging for the cbom-reader bind DN and forward to your SIEM.

Conclusion

With a least-privilege cbom-reader account, a scoped ACI, and an LDAPS connection, CBOM Secure continuously enumerates certificates, CA certificates, and SSH public keys in Oracle Unified Directory - read-only and fully auditable - populating the inventory with expiry and algorithm metadata for ongoing posture tracking.