# OpenLDAP Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

## Overview

The CBOM Secure Discover_LDAP sensor connects to OpenLDAP over LDAPS (636) or StartTLS (389) and performs read-only discovery of cryptographic material bound to directory entries:

- userCertificate - X.509 certificates on user or service accounts
- cACertificate - certificates held by certificate authority entries
- sshPublicKey - SSH public keys (requires the ldapPublicKey schema)
- crossCertificatePair - bilateral certificate pairs for cross-domain trust

Setup requires only a bind account entry and an ACL - no changes to existing data or schema.

## Prerequisites

- A running OpenLDAP (slapd 2.4+) reachable from the sensor host.
- root/sudo on the OpenLDAP server for ACL changes and restart.
- The client utilities ldapadd, ldapwhoami, ldapsearch.
- A valid TLS certificate for LDAPS/StartTLS (self-signed supported with the CA provided to the sensor).
- The base DN, and knowledge of whether the server uses slapd.conf or cn=config (OLC).
- The Discover_LDAP sensor installed with connectivity on 636 or 389.

## Step-by-Step Guide

### Step 1: Create the CBOM Bind Account

Create cbom-reader.ldif and add it to the directory:

```
dn: cn=cbom-reader,dc=corp,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: cbom-reader
description: CBOM read-only bind account for Discover_LDAP
userPassword: <password>
ldapadd -x -H ldap://localhost -D "cn=admin,dc=corp,dc=example,dc=com" -W -f cbom-reader.ldif
```

### Step 2: Apply a Read-Only ACL

cn=config (OLC) backend - create cbom-acl.ldif and apply it:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcAccess
```

```
olcAccess: {0}to *
  by dn.exact="cn=cbom-reader,dc=corp,dc=example,dc=com" read
  by * none

ldapmodify -Y EXTERNAL -H ldapi:/// -f cbom-acl.ldif
```

Classic slapd.conf backend - add the equivalent access rule after specific rules but before the global catch-all, then restart slapd:

```
access to *
    by self read
    by dn.exact="cn=cbom-reader,dc=corp,dc=example,dc=com" read
    by * none
```

### Step 3: Reload slapd and Confirm LDAPS

```
sudo systemctl restart slapd && sudo systemctl status slapd
sudo ss -tlnp | grep 636          # ensure LDAPS is listening
# if not: set SLAPD_SERVICES="ldap:/// ldaps:/// ldapi:///" in /etc/default/slapd and restart
```

For an internal CA, copy the CA PEM to the sensor host (e.g. /etc/cbom/tls/ldap-ca.pem).

### Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_LDAP
    enabled: true
    schedule: "0 2 * * *"
    connection:
      host: ldap.corp.example.com
      port: 636
      protocol: ldaps              # or starttls on 389
      tls:
        ca_cert: /etc/cbom/tls/ldap-ca.pem
        verify_hostname: true
    auth:
      bind_dn: "cn=cbom-reader,dc=corp,dc=example,dc=com"
      password_env: CBOM_LDAP_BIND_PASSWORD
    discovery:
      base_dn: "dc=corp,dc=example,dc=com"
      scope: subtree
      attributes: [userCertificate, cACertificate, sshPublicKey, crossCertificatePair]
      page_size: 500
    output:
      tags: { directory: openldap }
```

Set CBOM_LDAP_BIND_PASSWORD from a secrets manager; do not store it in the YAML.

### Step 5: Validate

```
ldapwhoami -H ldaps://ldap.corp.example.com \
  -D "cn=cbom-reader,dc=corp,dc=example,dc=com" -W
cbom sensor run --name Discover_LDAP --dry-run
sudo journalctl -u cbom-sensor --since "10 minutes ago" | grep Discover_LDAP
```

A successful ldapwhoami and a dry run reporting entries scanned and crypto attributes discovered confirm the setup.

## Common Errors

**ldap_bind: Invalid credentials (49)**

**Cause:** The password does not match userPassword for cn=cbom-reader, or the bind DN has a typo.

**Resolution:** Reset with ldappasswd as admin and update CBOM_LDAP_BIND_PASSWORD.

**Can't contact LDAP server (-1)**

**Cause:** The sensor host cannot reach port 636, or slapd is not listening on LDAPS.

**Resolution:** Confirm ss -tlnp | grep 636, check firewall rules, and ensure SLAPD_SERVICES includes ldaps:///.

**TLS: peer cert untrusted or revoked (0x42)**

**Cause:** The sensor does not trust the CA that signed the server's TLS certificate.

**Resolution:** Provide the CA PEM via ca_cert (or TLS_CACERT / -o tls_cacert for CLI tools).

## Security Recommendations

- Use LDAPS or enforced StartTLS - never send the bind password over plaintext.
- Scope the ACL narrowly (dn.subtree) to branches that hold crypto attributes where possible.
- Store the bind password in a secrets manager via password_env.
- Rotate the cbom-reader password at least quarterly and re-verify authentication.
- Enable the accesslog overlay or syslog and alert on cbom-reader binds outside scan windows.

## Conclusion

With a least-privilege bind account, a read-only ACL (slapd.conf or cn=config), and an encrypted connection, the Discover_LDAP sensor inventories X.509 certificates, CA certificates, SSH public keys, and cross-certificate pairs in OpenLDAP on each scheduled run.