Apache Directory Server (ApacheDS) Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

Overview

The CBOM Secure Discover_LDAP sensor connects to Apache Directory Server (ApacheDS) over LDAPS and performs read-only enumeration of cryptographic material:

```
userCertificate — X.509 certificates on user or service-account entries
cACertificate — CA certificates (typically on certificationAuthority or pkiCA entries)
```

This guide prepares a least-privilege bind account, grants read access to cryptographic attributes via a prescriptive ACI, and configures the sensor.

Prerequisites

- Apache Directory Server 2.0.0+ installed and running.
- Apache Directory Studio (GUI client) for administrative operations.
- LDAPS enabled (port 10636 in dev, 636 in production).
- The admin DN and password (default uid=admin,ou=system).
- The container ou=users,dc=example,dc=com exists, or permission to create entries.
- Access Control Subsystem (ACS) enabled (ads-enableAccessControl = TRUE).
- Sensor host reachable to the LDAPS port, and the server CA certificate available.

Step-by-Step Guide

Step 1: Create a CBOM Bind Account

Using Apache Directory Studio, create an inetOrgPerson entry cn=cbom-reader,ou=users,dc=example,dc=com with a strong userPassword. The account is read-only and used solely by the sensor.

Step 2: Grant Read Access via Prescriptive ACI

Add a prescriptiveACI on the suffix permitting cbom-reader to read userCertificate and cACertificate. Via ldapmodify with an LDIF file:

```
dn: dc=example,dc=com
changetype: modify
add: prescriptiveACI
prescriptiveACI: { identificationTag "CBOM-Read-Certs",
  precedence 10,
  authenticationLevel simple,
  itemOrUserFirst userFirst:
  { userClasses { name { "cn=cbom-reader,ou=users,dc=example,dc=com" } },
    userPermissions
    { { protectedItems { attributeType { userCertificate, cACertificate } },
```

```
      grantsAndDenials { grantRead, grantSearch, grantCompare, grantBrowse,
grantReturnDN } } } } }
ldapmodify -H ldaps://localhost:10636 \
  -D "uid=admin,ou=system" -W -f cbom-aci.ldif
```

Step 3: Verify the Bind Account and LDAPS

```
ldapwhoami -H ldaps://localhost:10636 \
  -D "cn=cbom-reader,ou=users,dc=example,dc=com" -W


ldapsearch -H ldaps://localhost:10636 \
  -D "cn=cbom-reader,ou=users,dc=example,dc=com" -W \
  -b "dc=example,dc=com" -s sub "(objectClass=*)" \
  userCertificate cACertificate
```

If the ApacheDS LDAPS listener uses a self-signed certificate, export the CA certificate for the sensor:

```
openssl s_client -connect localhost:10636 -showcerts </dev/null 2>/dev/null \
  | openssl x509 -outform PEM > apacheds-ca.pem
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_LDAP
    enabled: true
    type: ldap
    label: "ApacheDS - Production Directory"
    schedule: "0 2 * * *"
    connection:
      host: "ldaps://apacheds.example.com"
      port: 10636                # 636 in production
      use_tls: true
      tls_ca_cert: "/etc/cbom/certs/apacheds-ca.pem"
      verify_hostname: true
    bind:
      dn: "cn=cbom-reader,ou=users,dc=example,dc=com"
      password_env: "CBOM_LDAP_BIND_PASSWORD"
    discovery:
      base_dn: "dc=example,dc=com"
      scope: "subtree"
      filter: "(objectClass=*)"
      attributes: [userCertificate, cACertificate]
      page_size: 500
    output:
      include_raw_der: true
```

Step 5: Validate

```
cbom-sensor run --sensor Discover_LDAP --dry-run --verbose
```

Expected output confirms a successful TLS handshake and bind, a subtree search, and discovery counts such as Entries with userCertificate: 47, cACertificate: 3.

Common Errors

PKIX path building failed / certificate verify failed

Cause: The sensor does not trust the ApacheDS TLS certificate (self-signed or internal CA not in the trust store).

Resolution: Export the CA cert via openssl s_client, set tls_ca_cert to it, and run update-ca-certificates / update-ca-trust if using the system store.

LDAP error 49 — Invalid credentials

Cause: The bind DN does not exist, the password is wrong, or userPassword was not set.

Resolution: Confirm the entry exists, reset userPassword in Directory Studio, and verify CBOM_LDAP_BIND_PASSWORD matches.

LDAP error 50 — Insufficient access rights

Cause: The ACI was not applied, ACS is disabled, or the ACI targets the wrong bind DN.

Resolution: Confirm ads-enableAccessControl is TRUE, verify prescriptiveACI on the suffix, and ensure the userdn matches the bind DN exactly.

Security Recommendations

- Never hard-code credentials — supply the bind password via CBOM_LDAP_BIND_PASSWORD or a secrets manager.
- Enforce LDAPS with verify_hostname: true for all sensor connections.
- Keep the ACI scoped to userCertificate and cACertificate — never (targetattr="*").
- Rotate the bind account password on schedule and restart the sensor.
- Enable ApacheDS access logging and review for unexpected binds from cbom-reader.

Conclusion

With a least-privilege bind account, a targeted prescriptive ACI, and an LDAPS connection, the Discover_LDAP sensor maintains an up-to-date inventory of all X.509 certificates stored in ApacheDS — supporting visibility into certificate lifecycle, expiry, and algorithm posture across directory services.