OpenDJ / ForgeRock DS / PingDS Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

Overview

This guide configures OpenDJ, ForgeRock Directory Services (DS), or PingDS - which share the same codebase - so the CBOM Secure Discover_LDAP sensor can discover cryptographic assets over LDAPS, read-only:

- userCertificate - X.509 certificates on user or device entries
- cACertificate - X.509 CA certificates on CA or configuration entries
- sshPublicKey - SSH public keys on user accounts (requires the openssh-lpk schema overlay)

Prerequisites

- A running OpenDJ 3.x+, ForgeRock DS 6.x+, or PingDS 8.x+ with administrative access.
- The dsconfig, ldapmodify, and ldapsearch tools available (bundled under bin/).
- The directory manager bind DN and password (e.g. cn=Directory Manager).
- LDAP (1389) and LDAPS (1636) reachable from the sensor host.
- The openssh-lpk schema loaded if sshPublicKey discovery is required.
- A valid TLS certificate on the server for LDAPS (recommended).

Step-by-Step Guide

Step 1: Create a Read-Only Service Account

```
ldapmodify --hostname localhost --port 1389 \
  --bindDN "cn=Directory Manager" --bindPassword "admin-password" \
  --addEntryToLdif << 'EOF'
dn: cn=cbom-reader,ou=ServiceAccounts,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: cbom-reader
sn: CBOMReader
userPassword: ChangeMeToAStrongPassword123!
EOF
```

Step 2: Create and Rebuild an Index on userCertificate

Without an index, searches on userCertificate require a full scan. Create an equality index in the userRoot backend and rebuild it:

```
dsconfig create-local-db-index --hostname localhost --port 4444 \
  --bindDN "cn=Directory Manager" --bindPassword "admin-password" \
  --backend-name userRoot --index-name userCertificate \
  --set index-type:equality --trustAll --no-prompt
```

```
rebuild-index --hostname localhost --port 4444 \
  --bindDN "cn=Directory Manager" --bindPassword "admin-password" \
  --baseDN "dc=example,dc=com" --index userCertificate --trustAll
```

Step 3: Grant a Read-Only Global ACI

```
dsconfig set-access-control-handler-prop --hostname localhost --port 4444 \
  --bindDN "cn=Directory Manager" --bindPassword "admin-password" \
  --add 'global-aci:(targetattr="userCertificate||cACertificate||sshPublicKey")(version 3.0;acl
"CBOM Read";allow(read,search,compare) userdn="ldap:///cn=cbom-
reader,ou=ServiceAccounts,dc=example,dc=com";)' \
  --trustAll --no-prompt
```

Then test as the service account over LDAPS to confirm the ACI works:

```
ldapsearch --hostname localhost --port 1636 --useSsl --trustAll \
  --bindDN "cn=cbom-reader,ou=ServiceAccounts,dc=example,dc=com" \
  --bindPassword "ChangeMeToAStrongPassword123!" \
  --baseDN "dc=example,dc=com" --searchScope sub \
  "(userCertificate=*)" userCertificate cACertificate sshPublicKey
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_LDAP
    type: ldap
    enabled: true
    label: "OpenDJ-Production"
    connection:
      host: ldap.example.com
      port: 1636
      use_ssl: true
      verify_ssl: true
      ca_cert_path: /etc/cbom/certs/ldap-ca.pem
    bind:
      dn: "cn=cbom-reader,ou=ServiceAccounts,dc=example,dc=com"
      password_env: CBOM_LDAP_PASSWORD
    discovery:
      base_dn: "dc=example,dc=com"
      scope: sub
      page_size: 500
      attributes: [userCertificate, cACertificate, sshPublicKey]
      filter: "(|(userCertificate=*)(cACertificate=*)(sshPublicKey=*))"
    output:
      tags: { directory_vendor: opendj }      # opendj | forgerock-ds | pingds
```

Set the bind password via CBOM_LDAP_PASSWORD sourced from a secrets manager.

Step 5: Validate

```
cbom-sensor start --config /etc/cbom/sensors/opendj.yaml --log-level info
cbom-sensor scan --sensor OpenDJ-Production --once
cbom-sensor logs --sensor OpenDJ-Production --tail 100
```

Confirm the sensor connects and that userCertificate/cACertificate/sshPublicKey assets appear in the inventory under the correct tag.

Common Errors

LDAP Result Code 49 - Invalid Credentials

Cause: The bind DN/password does not match, or the account has not replicated yet.

Resolution: Verify the exact bind DN and password, test with ldapsearch, and allow replication to propagate.

LDAP Result Code 50 - Insufficient Access Rights

Cause: The global ACI was not applied, has a syntax error, or the userdn does not exactly match the service account DN.

Resolution: Re-verify the CBOM Read ACI, match the userdn exactly, and check for higher-precedence deny ACIs.

TLS handshake - certificate verify failed

Cause: The server's private-CA certificate is not trusted by the sensor.

Resolution: Export the CA (keytool -exportcert -rfc), set ca_cert_path, and only use verify_ssl: false in non-production.

Security Recommendations

- Use LDAPS exclusively in production (use_ssl: true, port 1636).
- Store the service account password in a secrets manager via password_env; rotate on schedule.
- Restrict base_dn to the subtree that holds crypto assets to limit access scope.
- Enable access logging (logs/access) and alert on cbom-reader activity outside scan windows.
- Keep the ACI to read/search/compare only - never write, delete, or modify.

Conclusion

With a read-only service account, a userCertificate index, and a scoped global ACI, the Discover_LDAP sensor enumerates certificates, CA certificates, and SSH public keys across OpenDJ / ForgeRock DS / PingDS on schedule - least-privilege and auditable throughout.