NetIQ eDirectory Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

Overview

This guide configures NetIQ eDirectory as a source for the CBOM Secure Discover_LDAP sensor, which connects over LDAPS (port 636) and performs read-only enumeration of cryptographic assets in the directory tree:

- ndspkiPublicKey - public keys on user and server objects managed by Novell PKI Services
- ndspkiCertificateChain - full certificate chains on PKI-enabled objects
- userCertificate - X.509 certificates on user objects
- cACertificate - CA certificates on organizational or container objects

Prerequisites

- NetIQ eDirectory 9.x or later, operational.
- LDAP Services enabled and listening on port 636 (LDAPS), with a valid TLS certificate bound and its CA exportable.
- iManager access (https://<server>/nps/iManager.html) with an admin account.
- Network access from the sensor host to eDirectory on TCP 636.
- The CBOM platform installed with the Discover_LDAP module.
- The target tree and base DN known (e.g. o=corp).

Step-by-Step Guide

Step 1: Create a Read-Only Service Account in iManager

Log in to iManager as an administrator. Under Users -> Create User, create cn=cbom-reader,o=corp (First Name cbom, Last Name reader, Context o=corp) with a strong random password stored in your secrets manager. Do not assign it to any role groups. Do not reuse an administrative account.

Step 2: Grant Attribute-Level Trustee Rights

Browse to Directory Administration -> Modify Object for the target container (e.g. o=corp) -> NDS Rights -> Trustees of this Object -> Add Trustee, and add cn=cbom-reader,o=corp. Under Assigned Rights -> Attribute Rights, add each target attribute with Read and Compare checked (Write and Add Self unchecked): ndspkiPublicKey, ndspkiCertificateChain, userCertificate, cACertificate. Check Inherit so rights propagate to child containers and leaf objects, then Save.

Verify via Rights -> View Effective Rights on a sample user object: Read should be listed for all four attributes and Write should not be granted.

Step 3: Export the eDirectory CA Certificate

In iManager under NetIQ Certificate Server -> Server Certificates, export the tree CA (or the LDAP service certificate) as PEM to /etc/cbom/certs/edirectory-ca.pem. Or export it directly from the sensor host:

```
openssl s_client -connect edirectory.corp.example.com:636 -showcerts </dev/null 2>/dev/null
\
  | openssl x509 -outform PEM > /etc/cbom/certs/edirectory-ca.pem
```

Step 4: Validate LDAP Connectivity

```
ldapsearch \
  -H ldaps://edirectory.corp.example.com:636 \
  -D "cn=cbom-reader,o=corp" -W \
  -b "o=corp" -s sub "(objectClass=*)" \
  userCertificate ndspkiPublicKey ndspkiCertificateChain cACertificate
```

A result set containing the target attributes in Base64 confirms the account and rights are configured correctly.

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_LDAP
  display_name: "NetIQ eDirectory - LDAP Crypto Discovery"
  enabled: true
  schedule: "0 2 * * *"
connection:
  host: edirectory.corp.example.com
  port: 636
  use_tls: true
  tls_mode: ldaps
  ca_cert: /etc/cbom/certs/edirectory-ca.pem
  verify_cert: true
bind:
  dn: "cn=cbom-reader,o=corp"
  password_env: CBOM_LDAP_BIND_PASSWORD
search:
  base_dn: "o=corp"
  scope: sub
  filter: "(objectClass=*)"
  page_size: 500
  attributes: [ndspkiPublicKey, ndspkiCertificateChain, userCertificate, cACertificate]
discovery:
  parse_certificates: true
  include_expired: true
  min_key_size_rsa: 2048
output:
  tags: { directory_vendor: netiq-edirectory, sensor_type: ldap }
```

Set the bind password via CBOM_LDAP_BIND_PASSWORD (or a systemd EnvironmentFile) sourced from a secrets manager.

Step 6: Validate

```
systemctl restart cbom-sensor
journalctl -u cbom-sensor -f
cbom-ctl scan run --sensor Discover_LDAP
```

Confirm a successful bind (cn=cbom-reader,o=corp) and a completed search with a crypto-asset count. In the dashboard, filter Assets -> Certificates by directory_vendor: netiq-edirectory and confirm subject/expiry/key metadata. Review the eDirectory audit log to confirm no write operations occurred.

Common Errors

LDAP bind failure - Invalid credentials (49)

Cause: Wrong password, a locked account, or an expired password (NDS error -669).

Resolution: Reset the password in iManager, ensure CBOM_LDAP_BIND_PASSWORD matches exactly, and set Password Never Expires on the service object if a policy applies.

TLS handshake failure - certificate verify error

Cause: The sensor host does not trust the eDirectory LDAP CA, or the exported CA is malformed.

Resolution: Re-export the CA (openssl x509 -noout -subject -dates to validate), confirm the ca_cert path, and append any intermediate CA to the same PEM.

Attributes not returned despite being set

Cause: The trustee rights were not saved with Inherit, or were assigned at the wrong scope.

Resolution: Confirm cbom-reader has Read on the four attributes with Inherit checked; use View Effective Rights on a leaf object before re-running.

Security Recommendations

- Use a dedicated non-privileged account - never the tree admin or a supervisory object.
- Grant rights only on the four target attributes; avoid [All Attributes Rights].
- Store the bind password in a secrets manager via password_env - never plaintext YAML.
- Enforce LDAPS only (disable/firewall port 389); keep verify_cert: true in production.
- Enable eDirectory auditing and alert on binds/searches from cbom-reader outside scan windows.

Conclusion

With a scoped read-only service account in iManager and attribute-level trustee rights, the Discover_LDAP sensor enumerates PKI public keys, certificate chains, and CA certificates across the eDirectory tree on schedule - giving CBOM Secure continuous, read-only visibility into directory-based cryptographic assets.