FreeIPA / Red Hat Identity Management Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

Overview

The CBOM Secure Discover_LDAP sensor connects to FreeIPA (and the downstream Red Hat Identity Management / IdM distribution) over LDAPS (port 636) to discover cryptographic assets stored in the directory:

```
ipaSshPubKey — user and host SSH public keys managed by FreeIPA
userCertificate — X.509 certificates issued to user principals
cACertificate — FreeIPA's integrated Dogtag CA and sub-CA certificates
ipaTokenOTPkey — TOTP/HOTP shared secrets assigned to user accounts
```

This guide creates a read-only service account, defines a scoped permission, groups it into a privilege and role, assigns the account, and configures the sensor.

Prerequisites

- A running FreeIPA 4.6+ or Red Hat IdM 7.x+ deployment reachable over the network.
- Administrative access to the FreeIPA web UI or CLI (kinit admin on an enrolled host).
- The FreeIPA LDAPS endpoint (port 636) reachable from the sensor host.
- The FreeIPA CA certificate (or full chain) available for download.
- The ipa CLI client installed on the setup host.
- Python 3.8+ and the CBOM sensor package installed on the scanning host.
- Your Kerberos realm and base DN noted (e.g. realm CORP.EXAMPLE.COM, base DN dc=corp,dc=example,dc=com).

Step-by-Step Guide

Step 1: Create the CBOM Service Account

Authenticate as admin, then create a dedicated read-only user:

```
kinit admin

ipa user-add cbom-reader \
   --first=CBOM \
   --last=Reader \
   --password

ipa passwd cbom-reader       # pre-set the password (no interactive reset)
ipa user-show cbom-reader
```

Step 2: Create the CBOM Read Permission

A permission defines which attributes can be accessed and under which subtree:

```
ipa permission-add "CBOM Read Certificates" \
   --attrs=userCertificate,caCertificate,ipaSshPubKey,ipaTokenOTPkey \
   --right=read,search,compare \
   --subtree="dc=corp,dc=example,dc=com"

ipa permission-show "CBOM Read Certificates"
```

Step 3: Create the CBOM Privilege

```
ipa privilege-add "CBOM Read" \
   --desc="Read-only access to cryptographic attributes for CBOM scanning"

ipa privilege-add-permission "CBOM Read" \
   --permissions="CBOM Read Certificates"
```

Step 4: Create the Role and Assign the Account

```
ipa role-add "CBOM Scanner" \
   --desc="Read-only role for CBOM cryptographic asset discovery"

ipa role-add-privilege "CBOM Scanner" --privileges="CBOM Read"
ipa role-add-member "CBOM Scanner" --users=cbom-reader
ipa role-show "CBOM Scanner"
```

Step 5: Export the FreeIPA CA Certificate

```
curl -k https://ipa.corp.example.com/ipa/config/ca.crt -o /etc/cbom/freeipa-ca.pem
# or copy from an enrolled client:
cp /etc/ipa/ca.crt /etc/cbom/freeipa-ca.pem
chmod 644 /etc/cbom/freeipa-ca.pem
```

Step 6: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_LDAP
  enabled: true
  description: "FreeIPA / Red Hat IdM LDAP sensor"
connection:
  host: ipa.corp.example.com
  port: 636
  use_ssl: true
  verify_ssl: true
  ca_cert_path: /etc/cbom/freeipa-ca.pem
authentication:
  method: simple_bind
  bind_dn: "uid=cbom-reader,cn=users,cn=accounts,dc=corp,dc=example,dc=com"
  bind_password_env: CBOM_LDAP_PASSWORD
discovery:
  base_dn: "dc=corp,dc=example,dc=com"
  scope: SUBTREE
  page_size: 500
  attributes: [ipaSshPubKey, userCertificate, cACertificate, ipaTokenOTPkey, uid, cn,
krbPrincipalName]
  filter: "(|(objectClass=inetOrgPerson)(objectClass=ipaHost)(objectClass=pkiCA))"
output:
  format: cbom_json
  destination: /var/lib/cbom/output/freeipa/
export CBOM_LDAP_PASSWORD='YourStrongPasswordHere'
```

Step 7: Validate

```
ldapsearch -H ldaps://ipa.corp.example.com:636 \
   -D "uid=cbom-reader,cn=users,cn=accounts,dc=corp,dc=example,dc=com" -W \
   -b "dc=corp,dc=example,dc=com" -s sub \
   "(objectClass=inetOrgPerson)" ipaSshPubKey userCertificate

cbom-sensor run --config /etc/cbom/sensors/freeipa.yaml --dry-run
```

A successful bind and reachable base DN confirm the configuration; run without --dry-run and confirm output files are generated.

Common Errors

Invalid credentials (49)

Cause: Wrong bind DN/password, or the cbom-reader password has expired (FreeIPA enforces password policy).

Resolution: Reset with ipa passwd cbom-reader and re-export the variable; add the account to a no-expiry service-account password policy if needed.

certificate verify failed

Cause: The FreeIPA CA certificate at ca_cert_path is missing, stale, or wrong (e.g. CA renewed).

Resolution: Re-export the CA cert, verify with openssl s_client -connect ipa…:636 -CAfile … (look for return code 0).

Insufficient access rights — attribute not returned

Cause: The permission did not propagate, or an extra ACI protects ipaTokenOTPkey (self-service only on some versions).

Resolution: Re-run ipa permission-mod with the attribute list, confirm role membership, and check the DS access log for the blocking ACI.

Security Recommendations

- Never store the bind password in YAML — inject via a secrets manager or a 0600 EnvironmentFile.
- Give cbom-reader no login shell; exclude it from VPN/SSH via an HBAC no-login rule.
- Rotate the service account password on schedule (90-day baseline) via your secrets manager.
- Forward FreeIPA DS access logs to your SIEM and alert on binds outside the scan window.
- Restrict port 636 access to the scanner host IP via firewall or FreeIPA host-based access control.

Conclusion

This least-privilege, read-only integration lets the Discover_LDAP sensor continuously inventory SSH public keys, X.509 user and CA certificates, and OTP token keys in FreeIPA / Red Hat IdM. For multi-replica environments, replicate the role/permission setup per domain and add connection entries to the sensor config.