Samba4 Active Directory Setup

CBOM Secure · LDAP Sensor (Discover_LDAP)

Overview

This guide configures a Samba4 Active Directory domain controller so the CBOM Secure Discover_LDAP sensor can perform read-only discovery over LDAPS:

```
userCertificate — X.509 certificates on user and computer objects
cACertificate — CA certificates on certification authority objects
altSecurityIdentities — SSH public keys and Kerberos principal mappings
```

Samba4 implements the full AD LDAP schema and is fully compatible with the LDAP sensor.

Prerequisites

- A running Samba4 AD domain controller (4.14+ recommended).
- Admin access to run samba-tool; the domain DNS name and base DN.
- LDAPS (636) enabled, or LDAP with STARTTLS; connectivity from the sensor host.
- The Discover_LDAP sensor available; Python 3.8+ with ldap3 for the Python variant.

Step-by-Step Guide

Step 1: Create a Read-Only Service Account

```
samba-tool user create cbom-reader --random-password
samba-tool user setpassword cbom-reader --newpassword='ReplaceWithStrongPassword!'
samba-tool user show cbom-reader
```

Step 2: Create a Delegation Group (Optional)

```
samba-tool group add CbomReaders
samba-tool group addmembers CbomReaders cbom-reader
```

Note Samba4's default AD ACL model grants authenticated users read access to userCertificate, cACertificate, and altSecurityIdentities — no extra delegation is needed unless custom ldb ACLs restrict attribute visibility.

Step 3: Confirm LDAPS and Test a Bind

Samba4 auto-generates a self-signed TLS cert at /var/lib/samba/private/tls/ (replace with an internal-CA cert for production). Test connectivity and an authenticated bind:

```
openssl s_client -connect dc1.corp.example.com:636 -showcerts

ldapsearch -H ldaps://dc1.corp.example.com:636 \
  -D "CN=cbom-reader,CN=Users,DC=corp,DC=example,DC=com" \
  -w 'ReplaceWithStrongPassword!' \
  -b "DC=corp,DC=example,DC=com" -s sub \
```

```
  "(objectClass=user)" userCertificate altSecurityIdentities
```

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_LDAP
  enabled: true
  schedule: "0 2 * * *"
connection:
  host: dc1.corp.example.com
  port: 636
  use_ssl: true
  verify_ssl: true
  ca_cert_path: /etc/cbom/certs/samba4-ca.pem
bind:
  dn: "CN=cbom-reader,CN=Users,DC=corp,DC=example,DC=com"
  password: "${CBOM_LDAP_PASSWORD}"
discovery:
  base_dn: "DC=corp,DC=example,DC=com"
  scope: subtree
  page_size: 500
  attributes: [userCertificate, cACertificate, altSecurityIdentities, distinguishedName,
sAMAccountName, objectClass]
  object_class_filters: [user, computer, certificationAuthority, pKIEnrollmentService]
output:
  format: cbom_json
  platform_url: https://cbom.corp.example.com
```

Step 5: Validate

```
cbom-sensor start --config /etc/cbom/sensors/samba4-ldap.yaml --log-level debug
```

Confirm a successful bind, subtree search, and discovered certificate/SSH-key counts; verify assets under Inventory → Directory Services. Re-run to confirm idempotency.

Common Errors

ldap_bind: Invalid credentials (49)

Cause: The password doesn't match, or the account is locked/expired.

Resolution: Reset with samba-tool user setpassword; clear expiry with --noexpiry; confirm CBOM_LDAP_PASSWORD is injected.

SSL: CERTIFICATE_VERIFY_FAILED

Cause: The DC's TLS CA is not trusted by the sensor host.

Resolution: Copy /var/lib/samba/private/tls/ca.pem to ca_cert_path, or add it to the system trust store.

Size limit exceeded (4)

Cause: The search exceeds the server-side size limit without correct paging.

Resolution: Set page_size to 500 or lower and confirm the sensor uses RFC 2696 paged results.

Security Recommendations

- Use LDAPS (636) or STARTTLS exclusively — never plain LDAP in production.
- Rotate the cbom-reader password every 90 days via a secrets manager.
- Restrict cbom-reader to LDAP bind only; block interactive logon via policy.
- Enable Samba4 LDAP access logging and alert on binds outside the scan window.
- Firewall the sensor host to reach only port 636 on domain controllers.

Conclusion

With a dedicated read-only account and an LDAPS connection, the Discover_LDAP sensor continuously inventories certificates, CA certificates, and SSH key mappings in Samba4 AD with minimal privilege and no impact on production.