Microsoft AD CS Setup

CBOM Secure · PKI Sensor (Discover_PKI)

Overview

This guide configures the CBOM Secure Discover_PKI sensor to connect read-only to a Microsoft Active Directory Certificate Services (AD CS) Certificate Authority and discover all issued certificates in the CA database:

- Issued X.509 certificates (Disposition = 20), serial numbers, and validity periods
- Subject distinguished names and email addresses
- Key algorithm, key size, and signature algorithm
- Certificate templates and intended purposes (EKU extensions)
- Revocation status and CRL distribution points

Prerequisites

- A Windows Server running AD CS with the Certification Authority role service.
- Domain Admin / Enterprise Admin privileges, or delegated rights to create service accounts and modify CA security.
- The CA reachable from the sensor host over DCOM/RPC (TCP 135 + dynamic high ports) or via certutil.
- RSAT installed on the sensor host, or certutil.exe available in PATH.
- The CA Common Name and server hostname known (e.g. CASERVER01\MyEnterpriseCA).
- PowerShell 5.1+ for service account creation, and the Discover_PKI sensor module present.

Step-by-Step Guide

Step 1: Create a Dedicated Service Account

```
New-ADUser `
  -Name "svc-cbom-pki" `
  -SamAccountName "svc-cbom-pki" `
  -UserPrincipalName "svc-cbom-pki@contoso.com" `
  -Path "OU=ServiceAccounts,DC=contoso,DC=com" `
  -AccountPassword (ConvertTo-SecureString "P@ssw0rd_ChangeMe!" -AsPlainText -Force) `
  -PasswordNeverExpires $true -CannotChangePassword $true -Enabled $true `
  -Description "CBOM PKI Sensor read-only service account"
```

Harden the account via GPO: add it to Deny log on locally and Deny log on through Remote Desktop Services so it can never be used interactively.

Step 2: Grant Read-Only Access to the CA

Grant only the Read permission on the CA. Do not grant Issue and Manage Certificates.

GUI (certsrv.msc)

- Open the Certification Authority MMC snap-in, right-click the CA name → Properties → Security tab.
- Click Add, select svc-cbom-pki, and check Allow for Read only.
- Ensure Issue and Manage Certificates is unchecked/Deny. Click OK.

CLI (certutil)

```
certutil -config "CASERVER01\MyEnterpriseCA" -setreg CA\Security ^
  "+CIADMIN:CONTOSO\svc-cbom-pki:Read"
net stop certsvc && net start certsvc
```

Step 3: Verify Certificate Enumeration

As (or impersonating) svc-cbom-pki, list issued certificates (Disposition 20 = Issued):

```
certutil -view -config "CASERVER01\MyEnterpriseCA" ^
  -restrict "Disposition=20" ^
  -out "SerialNumber,NotAfter,SubjectDN,CertificateTemplate"
```

If a table of issued certificates is returned, connectivity and permissions are confirmed.

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_PKI
  enabled: true
  description: "Read-only discovery of issued certificates from Microsoft AD CS"
connection:
  type: adcs
  ca_config: "CASERVER01\\MyEnterpriseCA"    # Server\CAName (escape backslash in
YAML)
  host: "CASERVER01.contoso.com"
  port: 135
  transport: rpc_dcom
authentication:
  method: windows_service_account
  domain: "CONTOSO"
  username: "svc-cbom-pki"
  password_secret_ref: "cbom-vault://adcs/svc-cbom-pki"
discovery:
  scope: issued_certificates
  disposition_filter: 20                # 20 = Issued
  fields: [SerialNumber, NotAfter, NotBefore, SubjectDN, SubjectEmail,
           CertificateTemplate, SignatureAlgorithm, PublicKeyAlgorithm,
           PublicKeyLength, Disposition, RevokedReason]
  include_revoked: false
schedule:
  interval: "6h"
output:
  format: cbom_json
  api_endpoint: "https://cbom.contoso.internal/api/v1/ingest"
  api_key_secret_ref: "cbom-vault://api/ingest-key"
```

Note Backslashes must be escaped in YAML as \\ — for example ca_config: "CASERVER01\\MyEnterpriseCA".

Step 5: Validate

```
sudo systemctl reload cbom-agent        # or: Restart-Service -Name CBOMAgent
tail -f /var/log/cbom/discover_pki_adcs.log
```

Confirm log lines such as Connected to CA … and Enumerated 4,821 issued certificates, then verify the certificates appear under Assets → Certificates filtered by the CA source.

Common Errors

Access Denied (0x80070005) on certutil -view

Cause: The service account lacks Read on the CA, or certsvc was not restarted after the change.

Resolution: Confirm Read is allowed in CA Properties → Security, then restart certsvc and re-run the query as the service account.

RPC Server Unavailable (0x800706ba)

Cause: The sensor host cannot reach the CA over DCOM/RPC; a firewall is blocking TCP 135 or the dynamic high ports.

Resolution: Enable the Certification Authority (DCOM-In) firewall rule, open TCP 135 and 49152-65535 from the sensor host, and test with certutil -ping.

CA configuration string not found (0x80070057)

Cause: The ca_config CA name is incorrect — it must match the registered name exactly, including casing.

Resolution: Run certutil -dump to find the exact Server\CAName, update ca_config, and remember to escape the backslash as \\ in YAML.

Security Recommendations

- Use a dedicated, non-interactive service account; integrate with a secrets manager for rotation.
- Reference credentials via password_secret_ref — never plaintext in YAML.
- Grant only the CA Read permission; audit the CA ACL quarterly.
- Restrict DCOM/RPC to the sensor host IP only.
- Enable CA audit logging (certutil -setreg CA\AuditFilter 127) for traceability.

Conclusion

Following the least-privilege model here, the Discover_PKI sensor maintains a continuously updated inventory of all PKI-issued certificates without any ability to modify the CA or its database. Regular validation runs and audit-log reviews keep the integration healthy and compliant.