Active Directory Federation Services (AD FS) Setup

CBOM Secure · WinCerts Sensor (Discover_WinCerts)

Overview

This guide configures the CBOM Secure Discover_WinCerts sensor to discover AD FS cryptographic certificates:

- Token-signing certificates — sign security tokens issued to relying parties
- Token-decryption certificates — decrypt incoming encrypted assertions
- Service-communications certificates — secure communication between AD FS components

AD FS does not expose these via LDAP. The sensor runs with scan_adfs: true, invoking Get-AdfsCertificate via PowerShell remoting or locally on the AD FS host.

Prerequisites

- Access to a Domain Controller (ADUC or the ActiveDirectory PowerShell module).
- Access to the AD FS server (local admin, or remote via WinRM/RDP). Verify the service with Get-Service adfssrv.
- The sensor host is the AD FS server itself, or a Windows host with RSAT-AD-Tools and network access.
- PowerShell 5.1+ on the sensor host.
- WinRM enabled on the AD FS server for remote runs.
- The Discover_WinCerts sensor package downloaded.

Step-by-Step Guide

Step 1: Create a Service Account

```
Import-Module ActiveDirectory
$SecurePassword = ConvertTo-SecureString "P@ssw0rd!Str0ng#2024" -AsPlainText -Force
New-ADUser `
  -Name "CBOM ADFS Sensor" `
  -SamAccountName "cbom-adfs-sensor" `
  -UserPrincipalName "cbom-adfs-sensor@corp.example.com" `
  -Path "OU=Service Accounts,DC=corp,DC=example,DC=com" `
  -AccountPassword $SecurePassword `
  -PasswordNeverExpires $true -CannotChangePassword $true -Enabled $true
```

Step 2: Grant Read Access to AD FS Certificates

Get-AdfsCertificate requires membership in the local AD FS Readers group on the AD FS server. On the AD FS server as a local administrator:

```
Add-LocalGroupMember -Group "AD FS Readers" -Member "CORP\cbom-adfs-sensor"
Get-LocalGroupMember -Group "AD FS Readers"
```

Step 3: Install RSAT on the Sensor Host (Remote Runs Only)

```
Add-WindowsFeature RSAT-AD-Tools
# On the AD FS server, enable remoting:
Enable-PSRemoting -Force
# From the sensor host, verify:
Test-WSMan -ComputerName adfs-server.corp.example.com -Credential (Get-Credential)
```

Step 4: Verify Access to AD FS Certificates

```
$Credential = Get-Credential -UserName "CORP\cbom-adfs-sensor" -Message "service
account password"
Invoke-Command -ComputerName adfs-server.corp.example.com -Credential $Credential
-ScriptBlock {
    Import-Module ADFS
    Get-AdfsCertificate
}
```

Confirm at least three certificate types are returned: Token-Signing, Token-Decrypting, and Service-Communications.

Step 5: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_WinCerts
    enabled: true
    schedule: "0 2 * * *"          # daily at 02:00 UTC
    scan_adfs: true
    adfs:
      host: adfs-server.corp.example.com
      port: 5985                   # WinRM HTTP; 5986 for HTTPS
      use_ssl: false               # true if WinRM HTTPS is configured
      auth_method: negotiate       # negotiate | kerberos | ntlm | basic
      domain: corp.example.com
      username: cbom-adfs-sensor
      password_env: CBOM_ADFS_PASSWORD
    certificate_types: [Token-Signing, Token-Decrypting, Service-Communications]
    output:
      format: cbom-json
      destination: /var/cbom/output/adfs
    tags: { environment: production, platform: adfs, team: identity }
```

Note Set CBOM_ADFS_PASSWORD via a secrets manager at runtime rather than in shell profiles.

Step 6: Validate

```
cbom-sensor run --sensor Discover_WinCerts --config /etc/cbom/sensors/adfs.yaml --dry-run
grep -i "CertificateType" /var/cbom/output/adfs/adfs-server_certificates_<timestamp>.json
```

Confirm the output contains Token-Signing, Token-Decrypting, and Service-Communications entries.

Common Errors

Access is denied calling Get-AdfsCertificate (0x80070005)

Cause: The service account is not in the local AD FS Readers group, or the token has not refreshed.

Resolution: Confirm membership with Get-LocalGroupMember; start a fresh session to refresh the token; re-add the account if missing.

WinRM connection failure (remote host)

Cause: WinRM is not enabled on the AD FS server, or a firewall blocks TCP 5985/5986.

Resolution: Run Enable-PSRemoting -Force, allow the WinRM firewall rule, and verify with Test-NetConnection -Port 5985.

Get-AdfsCertificate cmdlet not found

Cause: The PowerShell ADFS module is not present on the sensor host.

Resolution: Run the sensor on the AD FS server, or install RSAT-AD-Tools and confirm with Get-Module -ListAvailable -Name ADFS.

Security Recommendations

- Use Kerberos authentication for WinRM to enforce mutual auth and prevent relay attacks.
- Enable WinRM over HTTPS (port 5986) with a valid certificate.
- Store the service account password in a secrets manager and inject it as a short-lived variable.
- Deny interactive and Remote Desktop logon for the service account via GPO.
- Audit logon events (4624/4625) for cbom-adfs-sensor and forward to your SIEM.

Conclusion

The Discover_WinCerts sensor with scan_adfs: true provides read-only discovery of all AD FS token-signing, token-decryption, and service-communications certificates — material not accessible over LDAP — keeping the CBOM Secure inventory current with AD FS certificate rotations for compliance and crypto-agility.