Lab: Deploy ADCS Enterprise Root CA

itpro.outsidesys.com/2017/10/28/lab-deploy-adcs-enterprise-root-ca

Some notes for deploying a single online Enterprise Root Certification Authority (CA) using Active Directory Certificate Services (ADCS) in a lab environment.

For this lab deployment, ADCS is installed on a Windows Server 2016 domain controller (do not do this in production) using contoso.com. PowerShell and the CertUtil commands are used whenever possible to complete the deployment.

The user account performing the deployment is an **Enterprise Admin**.

Prerequisites

Create a DNS Record for the CDP/AIA HTTP Location

This is a CNAME record for **pki.contoso.com** pointing to the domain controller dc1.contoso.com.

```
Add-DnsServerResourceRecordCName -Name "pki" -HostNameAlias "dc1.contoso.com" -
ZoneName "contoso.com"
```

Install IIS

IIS will host the CDP/AIA HTTP location.

```
Install-WindowsFeature Web-WebServer -IncludeManagementTools
```

Create a CertData Folder and CPS Text File

The CertData folder will contain the certificate and CRL files. The CPS text file is a placeholder for creating a certificate policy statement.

```
New-Item -Path C:\inetpub\wwwroot\CertData -Type Directory

Write-Output "Placeholder for Certificate Policy Statement (CPS). Modify as needed
by your organization." | Out-File C:\inetpub\wwwroot\CertData\cps.txt
```

New IIS Virtual Directory

```
$vDirProperties = @{

    Site         = "Default Web Site"
    Name         = "CertData"
    PhysicalPath = 'C:\inetpub\wwwroot\CertData'
}

New-WebVirtualDirectory @vDirProperties
```

Allow IIS Directory Browsing & Double Escaping

Directory browsing allows a user to view and download certificate files using their Internet browser (Firefox, IE, Chrome, etc.). **Double escaping** allows for the download of the CRL delta files, which has a "+" in the file name. Even if you're not using a CRL delta file, you should allow double escaping in case this changes in the future.

```
Set-WebConfigurationProperty -filter /system.webServer/directoryBrowse -name
enabled -Value $true -PSPath
"IIS:\Sites\$($vDirProperties.site)\$($vDirProperties.name)"

Set-WebConfigurationProperty -filter /system.webServer/Security/requestFiltering -
name allowDoubleEscaping -value $true -PSPath "IIS:\Sites\$($vDirProperties.site)"
```

New Share for the CertData Directory

Optional. The share allows domain users to retrieve copies of the root certificate for devices that need it. They can use the HTTP location too.

```
New-SmbShare -Name CertData -Path C:\inetpub\wwwroot\CertData -ReadAccess
"Contoso\domain users"
```

NTFS Permissions for the CertData Directory

Security (tab) > Edit > Add

- Required: Cert Publishers
  Permissions: Allow Modify
- Optional: Domain Users
  Permissions: [Defaults]
- OK > Close

Create the CA Policy File

The CAPolicy.inf file is read when the CA role service is installed. Additional settings can be defined in this file that are not included in the installation wizard or PowerShell command.

```
Notepad C:\windows\CAPolicy.inf
```

Paste in the following, save, and close.

```
[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies=AllIssuancePolicy
Critical=False

[AllIssuancePolicy]
OID=2.5.29.32.0
URL=http://pki.contoso.com/certdata/cps.txt

[BasicConstraintsExtension]
PathLength=0
Critical=True

[certsrv_server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=0
```

Install Active Directory Certificate Services

Install the ADCS Role

```
Install-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools
```

Install the ADCS Certification Authority Role Service

```
$CaProperties = @{

    CACommonName        = "Contoso-Root-CA"
    CAType              = "EnterpriseRootCA"
    CryptoProviderName  = 'RSA#Microsoft Software Key Storage Provider'
    HashAlgorithmName   = "SHA256"
    KeyLength           = 4096
    ValidityPeriod      = "Years"
    ValidityPeriodUnits = 10
}

Install-AdcsCertificationAuthority @CaProperties -force
```

Review the Configuration

```
Certutil -CAInfo
```

Review the Database and Log Locations

```
Certutil -getreg
```

Configure Max Validity Period of Certificates Issued by this CA

```
Certutil -setreg ca\ValidityPeriodUnits 5
Certutil -setreg ca\ValidityPeriod "Years"
```

Configure the CRL Validity Periods

- Base CRL: 6 Days
- Overlap: 3 Days
- No Delta CRL

```
Certutil -setreg CA\CRLPeriodUnits 6
Certutil -setreg CA\CRLPeriod "Days"
Certutil -setreg CA\CRLDeltaPeriodUnits 0
Certutil -setreg CA\CRLDeltaPeriod "Hours"
Certutil -setreg ca\CRLOverlapUnits 3
Certutil -setreg ca\CRLOverlapPeriod "Days"
```

Configure the CDP Locations

- Default Local Server Location
- Location for CertData Folder in IIS
- HTTP Location (Added to Certificates)
- No LDAP Location

```
## Remove Existing CDP URIs
$CrlList = Get-CACrlDistributionPoint
ForEach ($Crl in $CrlList) { Remove-CACrlDistributionPoint $Crl.uri -Force }

## Add New CDP URIs
Add-CACRLDistributionPoint -Uri C:\Windows\System32\CertSrv\CertEnroll\%3%8.crl -
PublishToServer -PublishDeltaToServer -Force

Add-CACRLDistributionPoint -Uri C:\inetpub\wwwroot\CertData\%3%8.crl -
PublishToServer -PublishDeltaToServer -Force

Add-CACRLDistributionPoint -Uri "http://pki.contoso.com/certdata/%3%8.crl" -
AddToCertificateCDP -AddToFreshestCrl -Force
```

Configure the AIA Locations

- Default Local Server Location
- HTTP Location (Added to Certificates)
- No LDAP Location
- No OCSP Location
- No CA Server FQDN in the certificate file name

```
## Remove Existing AIA URIs
$AiaList = Get-CAAuthorityInformationAccess
ForEach ($Aia in $AiaList) { Remove-CAAuthorityInformationAccess $Aia.uri -Force }

## Add New AIA URIs
Certutil -setreg CA\CACertPublicationURLs
"1:C:\Windows\System32\CertSrv\CertEnroll\%3%4.crt"

Add-CAAuthorityInformationAccess -AddToCertificateAia -uri
"http://pki.contoso.com/certdata/%3%4.crt" -Force
```

Important Note: Even though there is no variable defining an FQDN in the certificate's file name, the CA service will add the FQDN to the name anyway.

Restart the CA Service & Publish a New CRL

```
Restart-Service certsvc
Start-Sleep(2)
Certutil -crl
```

Check the Status of the CA

```
Certutil -adca
```

Copy the Root Certificate File to the CertData Folder

```
Copy-Item "C:\Windows\System32\Certsrv\CertEnroll\DC1.contoso.com_Contoso-Root-
CA.crt" "C:\inetpub\wwwroot\CertData\DC1.contoso.com_Contoso-Root-CA.crt"
```

Rename the Root Certificate File

```
Rename-Item "C:\inetpub\wwwroot\CertData\DC1.contoso.com_Contoso-Root-CA.crt"
"Contoso-Root-CA.crt"
```

Note: The certificate file (.CRT) and CRL file (.CRL) should have the same name.

Verify the Enterprise PKI using PkiView

> Start > Run > pkiview.msc

Post Installation

Export the Root Certificate in PEM Format

Open the Certification Authority Console

- Right-click the CA Server object > Properties > View Certificate > Details (tab) > Copy to File…
- Select: Based-64 encoded X.509 (.CER)
- Browse To: C:\inetpub\wwwroot\CertData
- File Name: Contoso-Root-CA.cer
- Save > Next > Finish

Rename the newly generated certificate file:

```
Rename-Item "C:\inetpub\wwwroot\CertData\Contoso-Root-CA.cer" "Contoso-Root-
CA.pem"
```

Add the PEM MIME Type to IIS

Open the IIS Management Console

- Navigate to and select the CertData virtual directory
- Double-click MIME Types in the middle pane
- Click Add in the right-hand pane
  - File Name Extension: .pem
  - MIME type: text/plain
- OK

New GPO for Auto-Enrollment Linked to the Domain

```
New-GPO -Name "ADCS - Auto-Enrollment" | New-GpLink -Target "DC=contoso,DC=com" -
LinkEnabled Yes
```

Edit the Auto-Enrollment GPO

Computer Configuration > Windows Settings > Security Settings > Public Key Policies

- Enable: Certificate Services Client – Auto-Enrollment
- Select: Renew expired certificates, update pending certificates, and remove revoked certificates
- Select: Update certificates that use certificate templates
- OK

User Configuration > Windows Settings > Security Settings > Public Key Policies

- Enable: Certificate Services Client – Auto-Enrollment
- Select: Renew expired certificates, update pending certificates, and remove revoked certificates
- Select: Update certificates that use certificate templates
- OK

Add Certificate Templates for Domain Controllers

Server 2016 domain controllers use the following certificate templates:

- Kerberos Authentication
- Directory E-mail Replication

```
Add-CATemplate -Name KerberosAuthentication
Add-CATemplate -Name DirectoryEmailReplication
```

Duplicate and Issue Certificate Templates

At this point you’re ready to open the Certificate Templates console, duplicate some templates, and add them to the CA server.