Renew Certificate Authority Certificates on Windows Server Core. No Problem!

Blog Post

Hi there! Rob and Jim are here from the Directory Services team. Today's blog strives to clearly elucidate an administrative procedure that comes along more frequently with PKI Hierarchies being deployed to Windows Server Core operating systems.

Installing the Certificate Services Role on Windows Server Core will not be covered in this blog, but this is good reference for this endeavor - https://learn.microsoft.com/en-us/powershell/module/adcsdeployment/install-adcscertificationauthority?view=windowsserver2022-ps

In our scenario we already have an OFFLINE ROOT and an Enterprise Subordinate CA certificate that needs to be renewed. Both of these PKI roles are installed on the Windows Server Core operating system.

1. To start the renewal process, validate if the customer has the following registry value in place so we know if / where the Certificate Signing Request (CSR) file is going to be written to.

```
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CA Name
Value Name:  RequestFileName
Value Name:  ParentCAMachine
Value Name:  ParentCAName
```

These registry settings control where the CSR file and name will be located if they are specified. Make sure that the folder path already exists before moving forward. GENERATING A CSR WILL NOT create a missing folder.

If the Root CA is an Enterprise Root CA (domain joined) the CSR creation will use the two Parent registry values to submit the certificate request to this Root CA. However, these values will not work and will probably not be present when utilizing an Offline (Standalone) Root CA.

2. In an elevated command prompt on the subordinate Issuing CA run the following command after deciding if reuse of the CA's existing private key is in order or if a new private key should be generated:

```
CertUtil -RenewCert [ReuseKeys]
```

If you want to generate a new private key for the Subordinate CA, then type:

If you want to generate a new private key for the Subordinate CA, then type: **CertUtil -RenewCert**

If you want to use the existing private key for the Subordinate CA, then type: **CertUtil -RenewCert ReuseKeys**

Additional information on CA certificate renewal options can be found here - Certification Authority Renewal - Win32 apps | Microsoft Learn

3. Copy the resultant CSR .req File over to the Root CA.

4. Now we can submit the request that we just copied to The Root CA which is also running on Windows Core OS. We are going to use the Certreq.exe command to submit this request to the Standalone Root CA.

CertReq -Submit -Config "*RootCAComputerDNSNameRootCAName*" *SubCACSRFIleName.req***

Example of the command line.

```
Root CA Computer name: FourthCoffeeCA01.FourthCoffee.com
Root CA Name:  FourthCoffee Root CA 01
Sub CA CSR File Name:  FourthCoffeeSubCARenewal01.req
```

CertReq -Submit -Config "FourthCoffeeCA01.FourthCoffee.com\FourthCoffee Root CA 01" FourthCoffeeSubCARenewal01.req

IMPORTANT: You should get a Request ID as part of the output. You will need to make a note of this for forthcoming steps.

5. If the CA Manager needs to approve the CSR, this can be accomplished via the certificate services management UI (cetsrv.msc) if possible as it is easier.
However, since the Root is also running the Windows Core OS, we must run the following command:

```
CertUtil -Resubmit RequestIDNumber
Example of the command line:  Request ID from step 4:  Request ID = 3

CertUtil -Config "FourthCoffeeCA01.FourthCoffee.com\FourthCoffee Root CA 01" -
resubmit 3
```

6. We next need to retrieve the CER/CRT file from the Root CA so that we can install the certificate on the Subordinate CA to complete the renewal.

```
CertUtil -View -Restrict "RequestID=RequestIDNumber" -out RawCertificate >
C:\FourthCoffeeSubCACert.cer
```

7. Assuming the Root CA's certificate has not been renewed, we just need to copy the resultant FourthCoffeeSubCACert.cer file back to the subordinate CA that is being renewed.

8. Back on the subordinate CA in an elevated command prompt we then need to install the subordinate CA's certificate. Using the following command:

```
CertUtil -InstallCert CACertFileName
Example:  Certutil -InstallCert FourthCoffeeSubCACert.cer
```

When this command is run the Certificate Service Service on the subordinate CA will start.

We hope this blog will take some of the mystery and challenge out of interacting with Microsoft PKI running on Windows Server Core.

Robert “what were you thinking” Greene and Jim “that’s for the birds” Tierney.

Updated Dec 13, 2023