Decommissioning an Old Certification Authority without affecting Previously Issued Certificates and then Switching Operations to a New One

https://blogs.technet.microsoft.com/pki/2012/01/27/decommissioning-an-old-certification-authority-without-affecting-previously-issued-certificates-and-then-switching-operations-to-a-new-one/

Jonathan Stephens posted an excellent Blog about this topic; however, it didn't include the steps. As a result, I decided to type this Blog detailing the steps required. The following assumptions have to be met before proceeding with these steps:

1- There is a new valid Certification Authority configured
2- There is a new distribution point configured for AIA and CDP locations named http://crl.contoso.com/CertData

Steps:

1- Logon to the old Enterprise Certification Authority as an Enterprise Administrator.
2- Identify the AIA and CDP distribution points
    a. Open the Certification Authority Console
    b. Right click the Certification Authority name and click Properties
    c. Click the "Extensions" tab
    d. Document the distribution points configured for CRL Distribution Point (CDP) – as an example http://<serverDNSnname>/CertEnroll/<CANAME>CRLNameSuffix><DeltaCRLAllowed>.crl which refers to local IIS installed on the server, or http://pki.contoso.com/Certenroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl

Note: Ignore the LDAP and C:\%windir% locations

    e. In the "Extensions" tab, select Authority Information Access (AIA) from the drop down menu
    f. Document the distribution points configured for the AIA extensions – as an example http://<ServerDNSName>/Certenroll/<ServerDNSName>_<CAName><CertificateName>.crt which refers to the local IIS installed on the server or http://pki.contoso.com/Certenroll/<ServerDNSName>_<CAName><CertificateName>.crt

Note: Ignore the LDAP and C:\%windir% locations

3- Disable Delta CRL and Issue a long Certificate Revocation List (CRL)
    a. Open the Certification Authority Console
    b. Right click "Revoked Certificates", and then click "Properties"
    c. Uncheck "Publish Delta CRL"
    d. Change the "CRL publication Interval" to 99 years and then click OK
    e. Open the command line with elevated privileges
    f. Run Certutil –crl to issue a new Certificate Revocation List (CRL)
4- Copy the old Certification Authority's certificate (CRT) and certificate revocation list (CRL) files to the server hosting website http://crl.contoso.com/CertData
    a. On the old Certification Authority, navigate to %windir%\System32\CertSrv\CertEnroll
    b. Copy the Certification Authority's certificate (CRT) and certificate revocation list (CRL) to the directory hosting http://crl.contoso.com/CertData
5- Redirect the Authority Information Access (AIA) and Certificate Revocation List (CRL) distribution points of the old Certification Authority to http://crl.contoso.com/certdata
    a. This can be done using an IIS redirect, or a DNS CNAME redirect to redirect Authority information Access (AIA) and Certificate Revocation List (CRL) of the old Certification Authority documented in steps 2.d and 2.f to the new web server http://crl.contoso.com/certdata
6- Document and remove all certificate templates available on the old Certification Authority to prevent it from issuing new certificates
    a. Open the command line with elevated privileges
    b. Run Certutil –catemplates > c:\catemplates.txt to document all available certificate templates at the d Certification Authority
    c. Launch the Certification Authority console

d. Navigate to “Certificate Templates”
e. Highlight all templates in the right pane, right click and then click “Delete”

At this point, the old Certification Authority can’t issue any certificates, and has all of its Authority Information Access (AIA) and Certificate Revocation List (CRL) redirected to a new web site http://crl.contoso.com/CertData The next steps will detail how to document the certificates issued by templates from the old Certification Authority and how to make them available at the new Certification Authority.

7- Identify and document the certificates issued based on certificate templates by sorting the Certification Authority database
   a. Highlight “Issued Certificates”
   b. Navigate to the right, and sort by “Certificate Templates”
   c. Identify the certificates issued by default certificate template types
   d. Identify the certificates issued by custom certificate templates – any template other than the default certificate templates mentioned earlier
8- Dump the certificates based on the default certificate template types:
   a. Open the command line with elevated privileges
   b. Run Certutil -view -restrict "Certificate Template=Template" -out "SerialNumber,NotAfter,DistinguishedName,CommonName" > c:\TemplateType.txt
   c. Examine the output of c:\TemplateType.txt and document all the certificates needing immediate action – i.e. requiring issuance from the new CA infrastructure if needed such as Web SSL.
   d. Consult with the application administrator using the certificates to determine the best approach to replace the certificates if needed

Note: Replace ***Template*** with the correct template name.

9- Dump the certificates based on the custom certificate template types:
   a. Open the Certification Authority Console
   b. Right click “Certificate Templates” and click “Manage”
   c. Double click the certificate template and click on “Extensions” tab
   d. Click on “Certificate Template Information”
   e. Copy the Object Identifier (OID) number – the number will look similar to 1.3.6.1.4.1.311.21.8.12531710.13924440.6111642.16676639.10714343.69.16212521.10022553
   f. Open the command line with elevated privileges
   g. Run Certutil -view -restrict "Certificate Template=OIDNumber" -out "SerialNumber,NotAfter,DistinguishedName,CommonName" > c:\CustomTemplateType.txt

Note: Replace ***OIDNumber*** with the number identified in step 9.e

   h. Examine the output of c:\CustomTemplateType.txt and document all the certificates needing immediate action – i.e. requiring issuance from the new CA infrastructure if needed such as custom SSL certificates.
   i. Consult with the application administrator using the certificates to determine the best approach to replace the certificates if needed

Note: You don’t need to take any action if the certificate was auto-enrolled because the certificate holder will renew the certificate when it expires from the new CA infrastructure.

10- Enable the Certificate Templates needed based on the results of steps 7-9 on the new Certification Authority
   a. Logon to the new Certification Authority as an Enterprise Administrator
   b. Right Click “Certificate Templates”, click “New” and then click “Certificate Template to Issue”
   c. Choose all the certificate templates needed in the “Enable Certificate Templates” window and click “OK”
11- <Optional> At this point you can uninstall the Certification Authority Role on the old Certification Authority
   a. Backup the old Certification Authority using the steps outlined in Disaster Recovery Procedures for Active Directory Certificate Services (ADCS)
   b. Uninstall Certificate Services from the old Certification Authority
   c. Decommission the server unless it is running other applications
12- Once all certificates are issued by the new infrastructure, you can safely remove all the Authority Information Access (AIA) and Certificate Revocation List (CRL) files from you infrastructure by following the steps in How to Decommission a Windows Enterprise Certification Authority and How to Remove All Related Objects and from the web server hosting http://crl.contoso.com