Setup Server 2019 Enterprise CA 2/5: Offline Root CA

Setup Offline Root CA

First we will create the CApolicy.inf. This is a configuration file that defines multiple settings that are applied to the root CA certificate and all other certificates issued by the root CA. This file needs to be created before the ADCS is installed on the root CA. For more information about the Syntax go here.

1. Start powershell and type the following line and press “enter”:

```
notepad c:\windows\capolicy.inf
```

2. Select “yes” to create the new file

3. Because this is a lab setup I will only setup some basic settings for the Root CA. I will configure the following settings:

- Renewalinformation for the CA certificate.
- The validity period for the base CRL.
- Disable the AlternateSignatureAlgorithm (more info on why can be found here).
- Disable the DefaultTemplates, these are not used because this is an offline CA.

For this lab I will use a random generated OID which is based on the Microsoft OID. Because these generated OID may not be unique you should request a private enterprise number at IANA (link). This number can be added to the CAPolicy.inf.

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

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=Years
CRLPeriodUnits=1
AlternateSignatureAlgorithm=0
LoadDefaultTemplates=0
```

4. Save the file as “capolicy.inf” using “All files” and “ANSI” Encoding.

5. Now we the role can be added and configured. Start the Server manager and select “Add roles and features”

6. The “Add Roles and Features Wizard” will start, press “Next” to continue.

7. Select “Role-based or feature-based installation” and press “Next”

8. Use the default settings and press “Next” to continue.

9. Select “Active Directory Certificate Services”

10. A pop-up will appear, press “Add Features” to continue.

11. Press “Next” to continue

12. Press “Next” to continue.

13. Check if the Servername is correct and press “Next” to continue.

14. Use the default settings, for the Root CA only the “Certification Authority” role is needed.

15. Press “install” to add the Active Directory Certificate Services to the server.

16. When the installation has completed, press the link “Configure Active Directory Certificate Services on the destination server”

17. Use the default settings and press “Next”

18. Select “Certification Authority” and press “Next”

19. Because this server is non-domain joined only Standalone CA can be selected. Press “Next” to continue.

20. As this server is the root of the PKI hierarchy select “Root CA” and press “Next”

21. Select “Create a new private key” and press “Next” to continue.

22. Because this is the Root CA Certificate I use a longer Key length of 4096. This will increase the security.

23. Use the default settings and press “Next” to continue.

24. Because this server will be used in a Test Environment I extend the validity period to 10 years. Press “Next” to continue.

25. Use the default settings and press “Next” to continue.

26. Press “Configure” to configure the server.

27. Press “Close” to continue.

28. Press “Tools” in the Server Manager and select “Certification Authority”

29. Right click the Servername and select “Properties”

30. Select the “Extensions” tab

31. In the “Extensions tab” select the extension “CRL Distribution Point (CDP) and remove all locations except the “C:\*” Location.

32. Because this server will be offline it cannot be contacted, therefore a location needs to be added to the subordinate server. Press “Add” to add the CDP on the Subordinate Server.

33. Enter the following location and press “OK”

http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

Replace <serverDNSName> with the dnsname of the Subordinateserver in this demo the location will be:

http://SUBENT-CA02.vmlabblog.com/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

24. Check the boxes beginning with “Include in CRLs*” and “Include in the CDP*” and press “Apply”

35. Press “No” when asked to restart the service.

36. Select in “Select extension” the “Authority Information Access (AIA)” and remove all locations except the “C:\*” Location.

37. Press “Add” to add the AIA location on the Subordinate Server.

38. Enter the following location and press “OK”

```
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
```

Replace <serverDNSName> with the dnsname of the Subordinateserver in this demo the location will be:

```
http://SUBENT-CA02.vmlabblog.com/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
```

39. Check the box “Include in the AIA extension of issued certificates” and press “Apply”

40. Press “Yes” when asked to restart the service.

41. Select the “General” and select the Root Certificate and press “View Certificate”.

42. Select the tab “Details” and press “Copy to File…”.

43. In the Certificate Export Wizard press “Next”.

44. Select “DER encoded binary X.509 (.CER)” and press “Next”.

45. In File name enter “C:\Windows\System32\CertSrv\CertEnroll\<CA-NAME>-CA.cer” and press “Next”.

46. Press “Finish” to export the RootCA Certificate.

47. A popup will appear when the export was successful, press “OK” to continue.

The setup of the Offline RootCA is now completed.

Unieke FAQ ID: #1081
Auteur: diode
Laatst bijgewerkt:02-03-2021 11:24