Setup Server 2019 Enterprise CA 3/5: Subordinate CA

Setup Subordinate CA

1. Start the Server manager and select “Add roles and features”

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

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

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

5. Select “Active Directory Certificate Services”

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

7. Select “Web Server (IIS)

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

9. Press “Next” to continue

10. Press “Next” to continue.

11. Check if the Servername before you start, this cannot be changed after the AD CS role has been installed and press “Next” to continue.

12. Keep the default role services (Certication Authority) and press “Next”

13. On the Web Server Role (IIS) page press “Next”

14. On the Role Services page select “Basic Authentication” and “Windows Authentication”. Press “Next” to continue.

15. In the confirmation screen press “Install” to start the installation.

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

17. Make sure your Domain credentials have been entered and not your local admin credentials. Otherwise you will not be able to configure a Enterprise CA. Press “Next” to continue.

18. Select the box “Certification Authority” and press “Next” to continue.

19. Select “Enterprise CA” and press “Next” to continue. (if Enterprise CA is not available check if the server is domain joined and the credentials entered in step 17)

20. Select “Subordinate CA” and press “Next” to continue.

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

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

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

24. Select the folder to save the Certificate Request and press “Next” to continue. (default is “c:\”)

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

26. Press “Configure” to apply the configuration.

27. When the configuration has succeeded a warning is shown. This is just a notification that the untill a certificate of the RootCA has been obtained and applied to the subordinate ca the Configuration is not completed.

28. Switch over to the Offline Root CA (OFFENT-CA01) and browse to the folder “c:\windows\system32\certsrv\certenroll”. There should be three files, select and copy all files.

29. Switch back to the Subordinate CA (SUBENT-CA02) and browse to the folder “c:\windows\system32\certsrv\certenroll”. Paste all the files copied in the previous step.

30. Rightclick the Root CA certificate which you just copied and select “Install Certificate”

31. Select “Local Machine” and press “Next”

32. Press “Browse” and select the “Trusted Root Certification Authorities” store. Press “Next” to continue.

33. Press “Finish” to continue.

34. After some time a popup will appear when the import has finished. Press “OK” to continue

35. Create a new folder in “C:\inetpub\wwwroot” with the name “CertEnroll”

36. Copy the RootCA Certificate and Certifate Revocation List from “C:\Windows\System32\CertSrv\CertEnroll” to “C:\inetpub\wwwroot\CertEnroll”

37. Browse to the location entered in step 20 (default “c:\”) and copy the “*.Req” file to the C: Drive on RootCA server.

38. On the Root CA Server open ” Certification Authority” rightclick the servername and select “All Tasks” -> Submit new request…”

39. Browse to the request file on the C: driver and press “Open”

40. Select “Pending Requests”. Rightclick the pending request and select “All Tasks” -> “Issue”

41. Select “Issued Certificates”. Rightclick the issued certificate and select “Open”

42. Select “Details” and press “Copy to file...”

43. Press “Next” to continue

44. Select “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)” and check the box “Include all certificates in the certification path if possible”. Press “Next” to continue.

45. Press “Browse…”

46. Enter a name for the certificate and press “Save” (the default location is the Documents folder)

47. Press “Next” to continue.

48. Press “Finish” to export the CA Certificate.

49. After some time a popup will appear when the export has finished. Press “OK” to continue.

50. Copy the CA Certificate from the RootCA (step 46) and switch to the subordinate server to paste the file.

51. On the Subordinate CA open the Certification Authority. Rightclick the Servername and select “All Tasks” -> “Install CA Certificate”

52. Select the copied CA Certificate and press “Open”

53. Rightclick the Servername and select “All Tasks” -> “Start Service”

The setup of the Subordinate CA is now completed

Unieke FAQ ID: #1082
Auteur: diode
Laatst bijgewerkt:02-03-2021 11:26