CQURE Academy

MasterClass: Windows Server 2016

PKI

Version 1.2

Author: CQURE Team

Email: info@cqure.us | Twitter: @CQUREAcademy

http://cqure.us

Training Content

1 Network Setup – Important 3

2 PKI setup 3

3 Creating SSL Certificate 5

4 Code signing 6

5 PowerShell script signing 7

1 Network Setup – Important

Here are the control steps that need to me made before the training:

1. Passwords are set to P@ssw0rd – if you have US keyboard layout (for example for Nano machines) the @ sign may be obtained by pressing Shift+2
2. Addresses for machines in labs are:
    a. DC: 10.10.10.10 netmask 255.0.0.0
    b. SRV1: 10.10.10.101 netmask 255.0.0.0
    c. SRV: 10.10.10.102 netmask 255.0.0.0
    d. Nano1: 10.10.10.111 netmask 255.0.0.0 -it will be set during one of labs
    e. NAT: 10.10.10.1 – there is no need to logon on this machine. It works as NAT to provide Internet access when needed.
3. Machines have automatic updates disabled through gpedit console. It makes labs lighter and faster if you do not have to face with "you have to restart now" messages. Machines have updates till March 2017.
4. Local administrator account name is localadmin.

2 PKI setup

1. Install Root CA
    a. Logon to the SRV2 machine
    b. Start Server Manager
    c. Start "Add roles and features" wizard
    d. Select "Active Directory Certificate Services" role.
    e. Accept all suggested roles and features.
    f. Under the "Role Services" leave only the "Certificate Authority" option checked.
    g. Finish the wizard
2. Configure Root CA
    a. Click on the yellow exclamation mark icon on the toolbar of Server Manager
    b. Select "Configure Active Directory Certificate Services"
    c. Leave default user context and click "Next".
    d. Check "Certificate Authority" option and click "Next".
    e. Select "Standalone CA" – the root certificate authority should not be integrated with Active Directory. Click "Next".
    f. Select "Root CA" and click "Next".
    g. Select "Create new private key" and click "Next".
    h. Confirm default set of cryptographic options and click "Next".
    i. Change the name to "ROOT-CA" and click "Next".
    j. Set the validity period to 10 years and click "Next".
    k. Confirm default database paths and finish the wizard.
    l. Best practices require a configuration of CDP and AIA now. We can skip this step for this lab.

3. Configure the domain to trust the Root CA
    a. Go to the C:\Windows\System32\CertSrv\CertEnroll and copy the SRV2.CQURE.LAB_ROOT-CA.crt file to the desktop of the DC machine.
    b. Login to DC
    c. Launch cmd.exe
    d. Issue a command: certutil -dspublish -f c:\users\administrator\desktop\SRV2.CQURE.LAB_ROOT-CA.crt RootCA
    e. Issue a command certutil -pulse
4. Install subordinate CA
    a. Switch to the SRV1 machine
    b. Start Server Manager
    c. Start “Add roles and features” wizard
    d. Select “Active Directory Certificate Services” role.
    e. Accept all suggested roles and features.
    f. Under the “Role Services” leave only the “Certificate Authority” option checked.
    g. Finish the wizard
5. Configure Sub-CA
    a. Click on the yellow exclamation mark icon on the toolbar of Server Manager
    b. Select “Configure Active Directory Certificate Services”
    c. Leave default user context and click “Next”.
    d. Check “Certificate Authority” option and click “Next”.
    e. Select “Enterprise CA” to integrate Sub-CA with domain and click “Next”.
    f. Select “Subordinate CA” and click “Next”.
    g. Select “Create new private key” and click “Next”.
    h. Confirm default set of cryptographic options and click “Next”.
    i. Change the name to “CQURE-SUB-CA” and click “Next”.
    j. Send the certificate request to the SRV2.CQURE.LAB machine.
    k. Confirm default database paths and finish the wizard. Pay attention at the warning.
6. Issue Sub-CA Certificate
    a. Switch to the SRV2 machine.
    b. Go to Windows Administrative Tools and launch Certification Authority console.
    c. Go to “Pending Requests” folder and find the request.
    d. Right-click the request and select “All Tasks” --> “Issue”.
    e. Go to the “Issued Certificates” folder and fond the certificate.
    f. Right-click the certificate and select “All Tasks” --> “Export Binary Data”.
    g. Select “Binary certificate” and “Save binary data to a file”
    h. Save the file on the desktop with the name SubCA.crt
    i. Copy the certificate file to the desktop of SRV1 machine.
7. Provide a certificate for the Sub-CA
    a. Switch to the SRV1 machine
    b. Go to Windows Administrative Tools and launch Certification Authority console.
    c. Right-click CQURE-SUB-CA, select “All tasks”and “Install CA Certificate”
    d. Find the certificate file you have on the desktop. Please pay attention at the file extension in the Open File dialog box.
    e. Trust the RootCA Certificate if prompted.

8. Right-click CQURE-SUB-CA, select “All Tasks” and “Start Service”
9. Switch to the cmd.exe console and type pkiview
10. Verify if your Public Key Infrastructure works properly.
11. Run cmd.exe and type “gpupdate /force” on SRV1 and SRV2.

3 Creating SSL Certificate

1. Switch to the SRV2.
2. Install IIS
    a. Launch Server Manager and start “Add roles and features” wizard.
    b. Install “Web Server (IIS)” role and add suggested features.
    c. In Role Services leave the default set of services.
    d. Finish the wizard.
3. Go to DC and try to open http://srv2.cqure.lab and https://srv2.cqure.lab with your browser
4. On the SRV2 go to Windows Administrative Tools and launch Internet Information Services management console.
5. Click on the “SRV2” node in the left pane and then double click “Server Certificates”
6. Click on the “Create Certificate Request” in the right pane.
7. Type srv2.cqure.lab as the common name and fill up other properties.
8. Leave default cryptographic service provider properties.
9. Save the request to the C:\Users\administrator.CQURE\Desktop\request1.txt file.
10. Copy the request1.txt file from the desktop of the SRV2 machine to the desktop of the SRV1 machine.
11. Switch to the SRV1 machine.
12. Launch the Certificate Autority Management console.
13. Right-click on the CQURE-SUB-CA and select “All tasks” and then “Submit new request”.
14. Select the request1.txt file from the desktop.
15. If you obtain an error message you can issue the same request from the command line and specifying the template name.
    a. Launch cmd.exe and type: certreq -submit -attrib "CertificateTemplate:WebServer" c:\users\administrator.cqure\desktop\request1.txt
    b. Select CQURE-SUB-CA when prompted.
    c. Save the result to the SRV2_SSL.cer on the desktop.
16. Copy the SRV2_SSL.cer from the desktop of SRV1 machine to the desktop of SRV2 machine.
17. Switch to the SRV2 machine.
18. Launch IIS manager and Click on the “SRV2” node in the left pane and then double click “Server Certificates”
19. Click on “Complete Certificate Request” in the right pane.
20. Select the SRV2_SSL.cer you have on the desktop.
21. Specify SRV2_SSL as a friendly name and finish the wizard
22. Expand the “Web sites” group in the left pane and select “Default Web Site”.
23. Click “Bindings” in the right pane.
24. Click “Add”

25. Switch type to “https”
26. Select the SRV2_SSL certificate.
27. Click OK and then Close.
28. Go to DC and try to open https://srv2.cqure.lab with your browser
29. Click on the padlock icon next to the URL and verify certificate properties including the path.

4 Code signing

1. Go to the SRV1 machine.
2. Open Certificate Authority management console.
3. Right-click on the “Certificate Templates” and select “Manage”.
4. Find the Code Signing template, right-click it and select “Duplicate template”.
5. Go to the “General” tab and specify “CQURE Signing” as a name.
6. Click OK.
7. Close the Certificate Templates console.
8. In the Certificate Authority management console right click on the “Certificate Templates” and select “New” --> “Certificate Template to Issue”.
9. Select the CQURE Signing template and click OK.
10. Go to the DC machine.
11. Copy tcpclient.exe to your desktop.
12. Right click the tcpclient.exe and verify if there is any digital signature.
13. Launch cmd.exe and then type “certmgr” to run the certificate management.
14. Go to Personal --> Certificates.
15. Right-click on “Certificates” and select “All tasks” --> “Request new certificate”.
16. Click “Next” twice and select the “CQURE Signing” template.
17. Click “Enroll” and then “Finish”.
18. Verify if you have the new certificate present.
19. Double click on the new certificate, go to the “Details” tab and scroll down to the “Thumbprint” property.Note first 4 characters.
20. Launch PowerShell ISE
21. List your certificates with “dir cert:\CurrentUser\My” Try to find the certificate with the thumbprint you have noted.
22. Assing the code signing certificate to the variable: “$cert1= dir cert:\CurrentUser\My\DEADBEEFDEADBEEF” – Remember about replacing the sample thumbprint with your one.
23. Sign the binary file: Set-AuthenticodeSignature -Certificate $cert1 -FilePath C:\Users\Administrator\Desktop\tcpclient.exe
24. Right click the tcpclient.exe on your desktop and verify if there is any digital signature.

5 PowerShell script signing

1. Sign in to DC
2. Lunch PowerShell console
3. List your certificates with “dir cert:\CurrentUser\My” Try to find the certificate with the thumbprint you have noted.
4. Assing the code signing certificate to the variable: $cert1= dir cert:\CurrentUser\My\DEADBEEFDEADBEEF – Remember about replacing the sample thumbprint with your one.
5. Create new PowerShell script on desktop script1.ps1 with code:
   Write-Host “Hello, CQURE World!”
6. Change script execution policy to AllSigned:
   Set-ExecutionPolicy -ExecutionPolicy AllSigned
7. Try to run script from desktop
8. Create signature for script
   Set-AuthenticodeSignature -Certificate $cert1 C:\Users\Administrator\Desktop\script.ps1
9. Run the script
10. Confirm to always trust the publisher
11. Open script in editor and search for signature
12. Add single space or modify file in any other way
13. Save file and try to run it again
14. Set Execution policy to remote signed
    Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
15. Try to run the script again
16. Copy the script to \\srv1\c$\script.ps1
17. Try to run it from network share