CQURE Academy

MasterClass: Windows Server 2016

PART 1

Version 1.2

Author: CQURE Team

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

http://cqure.us

Training Content

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 Windows Server Installation

1. Mount the Windows Server 2016 Installation Image to the SRV1 Machine.
2. Make sure your VM will try to boot from DVD first.
3. Turn on the machine and press a key when prompted.
4. Follow through the installation wizard until the "Select the operating system you want to install" screen appears.
5. Note the set of installation options. Can you find the purpose for each of these options?
6. Shut down the VM and boot it from the disk.
7. Question: What is the difference between Windows Server 2012 R2 and Windows Server 2016?
8. Start DC machine and wait till it boots up.
9. Logon to the DC machine as CQURE\Administrator
10. Wait until Server Manager starts
11. Click on "Manage" and select "Remove Roles and Features"
12. Try to locate GUI related options. Do not remove them – it is possible to install them back but it may take up to one hour.
13. Close the wizard without making any changes.
14. Logon to the SRV1 machine as CQURE\Administrator
15. Repeat steps you just have performed on the DC machine.
16. Question: What is the difference? Can you explain how may it affect your work?

3 Nano Server Image generation

1. Logon to the SRV1 machine as CQURE\administrator
2. Make sure the Windows Server 2016 Installation Image is mounted to the VM
3. Copy all the content of the d:\NanoServer to the C:\NanoServer
4. Launch PowerShell ISE
5. Import PowersShell Nano Server Image Generator by typing: Import-Module C:\NanoServer\NanoServerImageGenerator\NanoServerImageGenerator.psm1
6. Create new Nano Server image by typing: New-NanoServerImage -Edition Datacenter -MediaPath D:\ -BasePath C:\NanoServer -TargetPath C:\NanoServer\nano1.vhdx -DeploymentType Guest -ComputerName NANO1 -Storage -Package Microsoft-NanoServer-IIS-Package
7. Provide a password for your new machine when prompted.
8. Locate the VHDX file you have just created. How can you use it?
9. Locate the Logs folder and observe type of logs you have.

4 Managing Nano Server Image with PowerShell

1. Locate you Nano Server VHDX file and “Packages” folder.
2. Find the package Microsoft-NanoServer-DNS-Package
3. Launch PowerShell ISE
4. Create a mounting point: md c:\MountDir
5. Mount the VHDX file by using the command: Mount-WindowsImage -ImagePath C:\NanoServer\Nano1.vhdx -Path c:\MountDir -Index 1
6. Add the package: Add-WindowsPackage -Path c:\MountDir -PackagePath C:\NanoServer\Packages\Microsoft-NanoServer-DNS-Package.cab
7. Dismount the image: Dismount-WindowsImage -Path c:\MountDir -Save

5 Managing Nano Server Image with DISM

1. Locate you Nano Server VHDX file and “Packages” folder.
2. Find the package Microsoft-NanoServer-ShieldedVM-Package
3. Launch cmd.exe
4. Make sure c:\MountDir exists by typing: dir c:\MountDir
5. Mount the image: dism.exe /Mount-Image /ImageFile:C:\NanoServer/Nano1.vhdx /Index:1 /MountDir:C:\MountDir
6. Add the package: dism.exe /Image:C:\MountDir /Add-Package /PackagePath: C:\NanoServer\Packages\Microsoft-NanoServer-ShieldedVM-Package.cab
7. Dismount the image: dism.exe /Unmount-Image /MountDir:C:\MountDir /Commit

6 Managing Nano Server

1. Launch Nano1 VM. Pay attention that it is pre-deployed machine, not the one you have just created.
2. Logon to the Nano1. Be careful as the keyboard layout is EN-US. The "@" sign may be obtained by pressing Shift+2.
3. Verify the IP Address and set it to 10.10.10.111, 255.0.0.0, gateway: 10.10.10.1
4. Question: How can you set DNS settings?
5. Go to the SRV1 machine
6. Launch PowerShell ISE and type: Set-Item WSMan:\localhost\Client\TrustedHosts "10.10.10.111" -Concatenate
7. Answer "Yes" when prompted if sure.
8. Use PowerShell variable to store your credentials: $Cred=Get-Credential
9. Enter the session: Enter-PSSession -ComputerName 10.10.10.111 -Credential $Cred
10. Try to verify the machine you are connected to: hostname
11. Try to verify the user you are using: whoami
12. Question: Does whoami command work as expected? What may be the reason?
13. Verify IP settings by typing: Netsh interface ipv4 show interfaces
14. Note the IDX property for the Ethernet adapter. Use it as "InterfaceIndex" in the next step.
15. Set the DNS with: Set-DNSClientServerAddress -InterfaceIndex 3 -ServerAddress 10.10.10.10
16. Verify the configuration with "ipconfig /all" command.
17. Do not close your machines, sessions and proceed to the next lab.

7 Adding Nano Server to the domain

1. On the DC machine launch Active Directory Users and Computers and verify the "Computers" container content.
2. On the SRV1 machine launch cmd.exe
3. Issue the command: djoin /provision /domain cqure.lab /machine nano1 /savefile c:\odjblob.txt
4. Re-check the content of the "Computers" container in Active Directory.
5. Switch back to the command prompt on the SRV1 machine
6. Authenticate against Nano Server: net use \\10.10.10.111 /u:Administrator *
7. Question: Does it work? Why?
8. Switch to the Nano1 machine and enable two firewall rules: NB-Session-In and SMB-In
9. Authenticate against Nano Server: net use \\10.10.10.111 /u:Administrator *
10. Copy the Offline Domain Join BLOB to the Nano1 machine: copy c:\odjblob.txt \\10.10.10.111\c$
11. Request domain join: Djoin /requestodj /loadfile c:\odjblob.txt /WindowsPath C:\Windows /localOS
12. Observe the result and restart the Nano Server: Restart-Computer
13. Logon to the Nano Server with Domain Admin credentials
14. Observe the computer configuration summary in the topmost part of the screen. Is everything configured properly here? What about time?
15. Do not close your machines, sessions and proceed to the next lab.

8 Setting Time Zone on Nano Server

1. Switch to SRV1 machine
2. From PowerShell ISE verify the host you are working on by typing “hostname”
3. If needed connect to the Nano1 machine by typing: Enter-PSSession -ComputerName 10.10.10.111 -Credential $Cred
4. Verify the timezone with “tzutil /g”. Does it need to be updated?
5. List available timezones with “tzutil /l” command
6. Find the right timezone and copy the name (second line)
7. Apply new timezone by typing tzutil /s "W. Europe Standard Time"
8. Verify the current setting using the command tzutil /g
9. Switch to the nano1 machine
10. Logoff by pressing Esc couple of times
11. Logon and observe the time information
12. Shut down the Nano1 machine.

9 Storage Replica

1. Create a snapshot of DC, SRV1 and SRV2.
2. Make sure all DC. SRV1 and SRV2 are running.
3. Logon into SRV1 as CQURE\Administrator
4. Launch Server Manager, click on “Add roles and features” and then add “Storage Replica”.
5. Accept feature management services offered to be installed.
6. Finish the wizard and restart the server.
7. Logon as CQURE\Administrator
8. Create volumes for data and log used for replication. Run cmd.exe and issue following commands:
    a. md c:\vhdx
    b. diskpart
    c. create vdisk file=c:\vhdx\data.vhdx type=expandable maximum=2048
    d. select vdisk file=c:\vhdx\data.vhdx
    e. attach vdisk
    f. convert gpt
    g. create partition primary
    h. format fs=ntfs quick
    i. assign letter=J
    j. create vdisk file=c:\vhdx\log.vhdx type=expandable maximum=2048
    k. select vdisk file=c:\vhdx\log.vhdx
    l. attach vdisk
    m. convert gpt
    n. create partition primary
    o. format fs=ntfs quick

   p. assign letter=L
   q. exit
9. Install Storage Replica and create volumes on SRV2. Repeat steps 3..8
10. Test your setup with the command: Test-SRTopology -SourceComputerName SRV1 -SourceVolumeName J: -SourceLogVolumeName L: -DestinationComputerName SRV2 -DestinationVolumeName J: -DestinationLogVolumeName L: -DurationInMinutes 1 -ResultPath c:\vhdx
11. Go to c:\vhdx and read the report.
12. Create replication partnership by issuing: New-SRPartnership -SourceComputerName srv1 -SourceRGName RG01 -SourceVolumeName J: -SourceLogVolumeName L: -DestinationComputerName SRV2 -DestinationRGName RG01 -DestinationVolumeName J: -DestinationLogVolumeName L: -LogSizeInBytes 1GB
13. Go to the SRV1 machine, open J: drive and create some files.
14. Go to the SRV2 machine, open J: drive and observe the result.
15. Question: can you explain the observed behavior?
16. Switch back to the SRV1 machine.
17. Find the driver responsible for the replication: driverquery | findstr /i replica

10 Monitoring Storage Replica

1. Switch to the SRV1 machine.
2. Launch eventvwr.
3. Locate the Microsoft-Windows-StorageReplica and then Admin and Operational Logs
4. Browse through entries (Start from the bottom where oldest entries are located) and try to analyze how the replica was set.
5. Launch perfmon
6. Select “Performance Monitor” in the left pane.
7. Click on the “+” button on the toolbar.
8. Expand “Storage Replica Statistics” group in the “Available counters” section.
9. Select the “Storage Replica Sent bytes per second” counter.
10. Select “J:\” as an instance and click “Add >>” and then “OK”.
11. Uncheck the checkbox next to the “% processor time” counter to clean up the graph.
12. Open cmd.exe and create some disk activity by typing: for /l %i in (1,1,1000) do @echo test >> j:\test.dat
13. Return to the perfmon window and wait the counter to drop to the zero for couple of seconds. Then use the “pause” button from the toolbar.
14. Right click on the “Storage Replica Sent Bytes per Sec” entry and select “Properties”
15. Set the “Scale” value to make the graph fill up the area optimally.

11 Changing Storage Replica parameters

1. Switch to the SRV1

2. Launch PowerShell ISE and type: Get-SRGroup
3. Observe the “ReplicationMode” and “AsyncRPO” attribute.
4. Switch the mode with command: Set-SRPartnership -SourceComputerName SRV1 -SourceRGName RG01 -DestinationComputerName SRV2 -DestinationRGName RG01 -ReplicationMode Asynchronous
5. Do the “Get-SRGroup” again and observe attributes mentioned above.

12 Destroying the Storage Replication Partnership

1. Switch to the SRV1
2. Launch PowerShell ISE
3. Remove all replication partnerships: Get-SRPartnership | Remove-SRPartnership
4. Switch to the SRV2 machine and try to open the J:\ drive.
5. Perform the cleanup:
    a. Launch diskmgmt.msc
    b. Right click and detach disks containing J: and L: volumes
    c. Delete c:\vhdx folder
6. Repeat steps above on the second server.

13 Data deduplication

1. Switch to the SRV1 machine
2. Create volumes deduplication tests. Run cmd.exe and issue following commands:
    a. md c:\vhdx
    b. diskpart
    c. create vdisk file=c:\vhdx\dedup.vhdx type=expandable maximum=2048
    d. select vdisk file=c:\vhdx\dedup.vhdx
    e. attach vdisk
    f. create partition primary
    g. format fs=ntfs quick
    h. assign letter=K
    i. exit
3. Create a test folder on the K: drive – md k:\test
4. Create a test file: for /l %i in (1,1,5000) do @echo test12345 >> k:\test\testfile.dat
5. Copy the test file: for /l %i in (1,1,1000) do @copy k:\test\testfile.dat k:\test\testfile_%i.dat
6. Open the K: drive, right-click the “test” folder and select “Properties”. Observe the size of files and the size on the disk. Is it clear why size on the disk is a bit larger?
7. Issue a “dir k:\” command in the cmd.exe window. Note the “bytes free” value.
8. Install data deduplication sub-role:
    a. Launch Server Manager
    b. Start “Add roles and features” wizard
    c. Select File and Storage Services \ File and iSCSI Services \ Data Deduplication

   d. Accept additional roles and features to be installed.
   e. Finish the wizard
9. Go to cmd.exe and type ddpeval – try to use this tool to evaluate potential storage savings on the K:\test folder
10. Enable deduplication for the K: drive
   a. Start Server Manager
   b. Select “File and Storage Services”
   c. Select “Disks”
   d. Select Disk 1 in the “DISKS” (upper) section
   e. Select K: in the “VOLUMES” (lower) section
   f. Right-click the K: drive and select “Configure Data Deduplication”
   g. Set the deduplication to “General purpose file server”
   h. Click OK
11. Open the K: drive, right-click the “test” folder and select “Properties”. Can you see any difference here? And within the “dir k:\” result? Why?
12. Launch PowerShell ISE and list deduplication related cmdlets with “get-command *dedup*”
13. Verify the current state of the K: drive: Get-DedupProperties -DriveLetter k
14. Try to use another command for very similar result: Get-DedupStatus -Volume k:
15. Start the deduplication: Start-DedupJob -Type Optimization -Volume k:
16. Try to quickly type “Get-DedupJob” and observe if job is running. Repeat this command every couple of seconds until the list of jobs is empty which means your deduplication jobs are finished.
17. Verify the effect: Get-DedupStatus -Volume k: - can you explain why it is like this? If it is not clear, switch to the Server Manager and open deduplication properties for the volume. Does it look reasonable now?
18. Change the minimum file age: Set-DedupVolume -Volume k: -MinimumFileAgeDays 0
19. Repeat steps 15 to 17. Can you see the difference?
20. Verify the folder size and size on the disk. Verify the free disk space reported by dir command. Can you explain all observed values?
21. Open the cmd.exe console and do “dir k:\ /a” Observe the “System Volume Information” folder. Try to see the content of this folder. Verify permissions with icacls “k:\System Volume Information”
22. Find the psexec.exe utility and launch psexec.exe -i -d -s cmd.exe
23. Verify your identity with “whoami” command.
24. Browse through the System Volume information. In the cmd.exe window type:
   a. k:
   b. dir /a
   c. cd "System Volume Information"
   d. dir /a
   e. cd Dedup
   f. dir . /a/s/p
25. Press space to view the result page by page. Try to guess which file extension indicates the deduplicated data storage?
26. Return to the Administrator’s command prompt.
27. Remove the “test” folder content: del k:\test*.* /q
28. How many bytes of the free disk space this operation restored? Why?
29. Open PowerShell ISE and type again: “Get-DedupStatus -Volume k:” – Observe the result and try to answer how could be this possible

30. You can quickly test the dedup folder content by issuing the command from localsystem cmd.exe console: dir "k:\system volume information\dedup*.ccc" /a/s
31. Cleanup the unused (not related to any existing file) deduplicated data from PowerShell ISE: Start-DedupJob -Type GarbageCollection -Volume k:
32. Observe the Get-DedupJob result to figure out when your job finishes.
33. Try again with the Get-DedupStatus command and analyze the result.

14 Partition resize

1. If you started this lab without doing the previous one, you should issue the set of commands described in step 2 in lab 13.
2. Launch diskmgmt.msc
3. Right-click the K: drive and select “Shrink volume”. Read the information displayed.
4. Click “Shrink”
5. Launch eventvwr.
6. Go to the Application Event Log and try to find Defrag Event 259
7. Read the information about the file blocking your volume from shrinking.
8. Try to copy and paste suggested fsutil command to the cmd.exe console.
9. Issue “fsutil volume querycluster” command to see the explanation of attributes used.
10. Test limits of the partition size with PowerShell: Get-Partition -DriveLetter K | Get-PartitionSupportedSize
11. Use PowerShell to extend the partition back to the original size: “Resize-Partition -DriveLetter K” Specify the SizeMax property from the previous command as the new size.
12. Switch to the disk management console to see if there is any free space left after the partition.
13. Clean up the environment:
    a. Right click and detach disk containing K: volume
    b. Delete c:\vhdx folder content