CQURE Academy

MasterClass: Windows Server 2016

PowerShell

Version 1.2

Please respect the authored content – copying prohibited.

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 JEA - Step by Step

1. Logon to the DC machine as CQURE\Administrator
2. Open Active Directory Users and Computers console
3. Create new user Freddy Krueger (login: fkrueger)
4. Create new Group: JEA
5. Add fkrueger to the JEA group
6. Sign in to SRV1 as Freddy
7. Open PowerShell and try to connect to SRV2 with command:
```
Enter-PSSession -ComputerName SRV2
```
8. Go back to DC as CQURE\Administrator
9. Open PowerShell
10. Create two folders:
```
md $env:ProgramData\JEAConfiguration\Transcripts
md $env:ProgramFiles\WindowsPowerShell\Modules\JEA
```

11. Create new Manifest
```
New-ModuleManifest -Path
$env:ProgramFiles\WindowsPowerShell\Modules\JEA\Mod1.psd1
```

12. Define role capabilities as variable:
```
$MaintenanceRoleCapabilityCreationParams = @{
   Author = 'CQURE Admin'
   CompanyName = 'CQURE'
   VisibleCmdlets = 'Restart-Service'
   FunctionDefinitions =
           @{ Name = 'Get-UserInfo'; ScriptBlock = { $PSSenderInfo }}
}
```

13. Create Role Capability file *.psrc for module:
```
New-PSRoleCapabilityFile -Path
"$env:ProgramFiles\WindowsPowerShell\Modules\JEA\RoleCapabilities\Mai
ntenance.psrc" @MaintenanceRoleCapabilityCreationParams
```

14. Create *.pssc (PowerShell Session Configuration) file skeleton
```
New-PSSessionConfigurationFile -Path
"$env:ProgramData\JEAConfiguration\JEADemo.pssc"
```
15. Open file for edition:
```
Notepad "$env:ProgramData\JEAConfiguration\JEADemo.pssc"
```
16. Make adjustments:
    a. Change SessionType = 'RestrictedRemoteServer'
    b. Change and uncomment TranscriptDirectory = "C:\ProgramData\JEAConfiguration\Transcripts"
    c. Uncomment RunAsVirtualAccount = $true
    d. Change and uncomment RoleDefinitions = @{'CQURE\JEA' = @{ RoleCapabilities = 'Maintenance'}}
17. Save and close notepad
18. Register the configuration:
```
Register-PSSessionConfiguration -Name 'JEADemo' -Path
"$env:ProgramData\JEAConfiguration\JEADemo.pssc"
```

19. Restart WinRM
```
Restart-Service WinRM
```

20. Switch to SRV1 as Freddy
21. Try to connect to SRV2
```
Enter-PSSession -ComputerName SRV2
```

22. Try to do it with
```
Enter-PSSession -ComputerName SRV2 -ConfigurationName JEADemo
```

23. Try to run commands that are listed: `Get-Command`
24. Try to run `Get-Service`
25. `Run Restart-Service -Name WinRM`
26. Go to SRV2 and open transcript files

3 PowerShell and Azure

1. Start NAT virtual machine and sign in to it with Administrator account
2. Test network connectivity: ping 8.8.8.8
3. Switch to SRV1 and sign in as CQURE\Administrator
4. Disable IE ESC
5. Test network connectivity and wait until it will be working
6. Open PowerShell as admin

7. Import module:
   `Install-Module AzureRM`

8. Sign in to Azure
   `Login-AzureRmAccount`

9. Check if you have active subscription
   Get-AzureRmSubscription

10. Check if you have active context
    Get-AzureRmContext

11. Create new resource group
    New-AzureRmResourceGroup -Name "RG2" -Location "West Europe"

12. Create a new Subnet
    $subnetConfig = New-AzureRmVirtualNetworkSubnetConfig -Name mySubnet -AddressPrefix 192.168.1.0/24

13. Create virtual network
    $vnet = New-AzureRmVirtualNetwork -ResourceGroupName RG2 -Location westeurope -Name myVnet -AddressPrefix 192.168.0.0/16 -Subnet $subnetConfig

14. Create public IP for my
    $pip = New-AzureRmPublicIpAddress -ResourceGroupName RG2 -Location westeurope -AllocationMethod Static -IdleTimeoutInMinutes 4 -Name "cqlabs$(Get-Random)"

15. Create a security rule
    $nsgRuleRDP = New-AzureRmNetworkSecurityRuleConfig -Name myNetSecRule -Protocol Tcp -Direction Inbound -Priority 1000 -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389 -Access Allow

16. Create a network security group
    $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName RG2 -Location westeurope -Name myNetSecGroup -SecurityRules $nsgRuleRDP

17. Create vNIC
    $nic = New-AzureRmNetworkInterface -Name myNic -ResourceGroupName RG2 -Location westeurope -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -NetworkSecurityGroupId $nsg.Id

18. Prepare credentials for new VM
    $cred = Get-Credential

19. Prepare VM Config
    $vmConfig = New-AzureRmVMConfig -VMName myVM -VMSize Standard_D1 | Set-AzureRmVMOperatingSystem -Windows -ComputerName myVM -Credential $cred | Set-AzureRmVMSourceImage -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-Datacenter -Version latest | Add-AzureRmVMNetworkInterface -Id $nic.Id

20. Create VM
    New-AzureRmVM -ResourceGroupName RG2 -Location westeurope -VM $vmConfig

21. Check IP of new VM
    Get-AzureRmPublicIpAddress -ResourceGroupName myResourceGroup | Select IpAddress

22. Connect to VM via RDP
23. Go to http://portal.azure.com and verify that there is new VM
24. Remove VM and all reasources
    Remove-AzureRmResourceGroup -Name RG2