Azure Virtual Networks – Practice Exercises

Overview

This course includes optional practical exercises where you can try out the techniques demonstrated in the course for yourself. This guide lists the steps for the individual practical exercises.

See the Overview page under Practical Exercises in your course for information about getting started.
Assign a Static IP Address

In this exercise, you will assign a static IP address to an existing Windows Server 2012 R2 VM using PowerShell. By default, all VMs have dynamic IP addresses. You can use a static IP address for specific use cases such as building a domain controller.

1. If you already have a test VM deployed with the Resource Manager model, use it for this exercise and skip to step 11. Otherwise, perform the following steps to create a new Windows Server 2012 R2 VM with the Resource Manager model.
2. Navigate to the Azure Portal and sign in.
5. In the search results, click Windows Server 2012 Datacenter.
6. On the Windows Server 2012 R2 Datacenter blade, notice the default deployment model is set to Resource Manager. Click Create.
7. On the Create Virtual Machine blade, fill in the following values for basic settings (substituting your information for the user name, subscription, and location) and click OK.
   - Name: SERVER-01
   - VM disk type: HDD
   - User name: <Your first name>
   - Password: Pa$$w0rd12345
   - Subscription: <Your subscription>
   - Resource group: Create a new one named “Server2012R2-RG”
   - Location: <Your location>
8. On the Choose a size blade, click View all. Click the A0 Standard size and then click Select. Note that we are choosing a larger size VM to support multiple NICs in a later exercise.
9. On the Settings blade, review the default options for storage, network, extensions, high availability, and monitoring. Click OK.
10. On the Summary blade, review the configuration and then click OK.
11. Open an elevated PowerShell prompt. If you already have the Azure PowerShell modules installed skip to step 20. Otherwise, perform the following steps to download and install the Azure PowerShell modules.
12. Run the Install-Module AzureRM command. This will install the AzureRM module which represents resource management.
13. If you get prompted to install and import the NuGet provider, Type Y and then press the Enter key.
14. If you are notified that the repository is untrusted, confirm that you want to install the modules by typing Y and then pressing the Enter key. The installation process will take several minutes as packages are downloaded and installed.
15. After the download and installation is finished, run the Import-Module AzureRM command.
16. Run the Install-Module Azure command. This will install the Azure module which represents service management.
17. If you are notified that the repository is untrusted, confirm that you want to install the modules by typing Y and then pressing the Enter key.

18. Once the download and installation is finished, run the Import-Module Azure command.

19. Run the Get-Module -All command to verify that you see the Azure related modules.

20. Run the Login-AzureRmAccount command and then authenticate with your Azure administrative credentials.

21. Run the Get-AzureRmVM command to list all of the VMs deployed with the Resource Manager model. Locate SERVER-01 (or your existing test VM). Note the values for ResourceGroupName and NetworkInterfaceIDs.


23. Run the following commands in sequence to update the PrivateIpAllocationMethod to static and assign a new private IP address:
   - $NIC = Get-AzureRmNetworkInterface -Name <NetworkInterfaceID> -ResourceGroupName "Server-RG"
   - $NIC.IpConfigurations[0].PrivateIpAllocationMethod = "Static"
   - $NIC.IpConfigurations[0].PrivateIpAddress = "10.0.0.50"
   - Set-AzureRmNetworkInterface -NetworkInterface $NIC

24. Run Get-AzureRmNetworkInterface -Name <NetworkInterfaceID> -ResourceGroupName "Server-RG". Review the output and confirm that the PrivateIPAddress and PrivateIpAllocationMethod have been updated.

25. When you are finished with this exercise, run the Get-AzureRmVM -Name "SERVER-01" -ResourceGroupName "Server-RG" | Stop-AzureRmVM command to shut down the VM.

---

Create and Manage Virtual Networks by Using Azure Portal

In this exercise, you will be working with virtual networks within the Azure Portal. You will create a new virtual network and explore the various management options.

1. Navigate to the Azure Portal and sign in.
3. Type virtual networks in the filter to reveal the available options for managing virtual networks in the Azure Portal. Mark Virtual networks as a favorite to add it to your Hub menu.
4. Click Virtual networks. If you have any existing virtual networks they should appear in this list. Click Add.
5. On the Create virtual network blade, fill in the following values to create a new virtual network. Click Create when you are finished entering the information
   - Name: Server-VNET
   - Address space: 172.168.0.0/16
   - Subnet name: Server-Subnet
- Subnet address range: **172.168.0.0/24**
- Subscription: `<Your subscription>`
- Resource group: Create a new one named “Server-VNET”
- Location: `<Your location>`

6. On the menu bar, monitor the alerts for progress as the new virtual network is created.
7. On the Hub menu, click **Virtual networks**. Confirm that the new virtual network has been created. Click **Server-VNET**.
8. On the Server-VNET blade, review the list of available management options under Settings, such as address space, connected devices, subnets, DNS servers, and peerings.
9. When you are finished exploring the new virtual network, close the web page.
Deploy a Virtual Machine into a virtual network

In this exercise, you will deploy a new Windows Server 2012 R2 VM to a new virtual network within the Azure Portal.

1. Navigate to the Azure Portal and sign in.
2. On the Hub menu, click New.
4. In the search results, click Windows Server 2012 Datacenter.
5. On the Windows Server 2012 R2 Datacenter blade, notice the default deployment model is set to Resource Manager. Click Create.
6. On the Create Virtual Machine blade, fill in the following values for basic settings (substituting your information for the user name, subscription, and location) and click OK.
   - Name: SERVER-05
   - VM disk type: HDD
   - User name: <Your first name>
   - Password: Pa$$w0rd12345
   - Subscription: <Your subscription>
   - Resource group: Create a new one named “Server-RG”
   - Location: <Your location>
7. On the Choose a size blade, click View all. Click the A0 Basic size and then click Select.
8. On the Settings blade, click Network.
9. On the Choose virtual network blade, click Server-VNET (created in the previous exercise).
10. On the Settings blade, under Network, confirm that the Virtual network and Subnet reflect your selected network. Click OK.
11. On the Summary blade, review the configuration and then click OK.
12. On the menu bar, monitor the alerts for progress as the new virtual machine is created.
13. When the VM is created, click Virtual machines in the left pane.
14. In the Virtual machines blade, click the server name for the VM that you deployed.
15. In the Server-05 blade, click Stop at the top of the blade to stop the VM. This ensures that you don’t consume resources unnecessarily.

Add a new domain to DNS Zones

In this exercise, you will explore DNS zones in the Azure Portal, including how to add and manage them.

1. Navigate to the Azure Portal and sign in.
3. Type dns zones in the filter. Mark DNS zones as a favorite to add it to your Hub menu.
4. Click **DNS zones**. If you have any existing DNS zones they will appear in this list. Click **Add**.

5. On the Create DNS zone blade, fill in the following values to create a new DNS zone. Click **Create** when you are finished entering the information.
   - **Name**: CLD220test.com
   - **Subscription**: <Your subscription>
   - **Resource group**: Create a new one named “Server-DNS”
   - **Resource group location**: <Your location>

6. On the menu bar, monitor the alerts for progress as the new DNS zone is created.

7. On the Hub menu, click **DNS zones**. Confirm that the new DNS zone has been created. Click **CLD220test.com**.

8. On the CLD220test.com DNS zone blade, review the available options and information, such as the list of existing records sets. Click **+ Record set**.

9. On the Add record set blade, fill in the following values to add a new record for WWW. Click **OK** when you are finished entering the information.
   - **Name**: WWW
   - **Type**: A
   - **TTL**: 1
   - **TTL unit**: Hours
   - **IP address**: 10.50.50.99

10. On the menu bar, monitor the alerts for progress as the new DNS record set is created. Confirm that the new record set has been added by reviewing the CLD220test.com DNS zone blade.

11. On the CLD220test.com DNS zone blade, click Click **+ Record set**.

12. On the Add record set blade, fill in the following values to add a new record for syslog. Click **OK** when you are finished entering the information.
   - **Name**: Syslog
   - **Type**: A
   - **TTL**: 1
   - **TTL unit**: Hours
   - **IP address**: 10.50.50.110

13. On the menu bar, monitor the alerts for progress as the new DNS record set is created. Confirm that the new record set has been added by reviewing the CLD220test.com DNS zone blade.

14. When you are finished exploring the DNS zones, close the web page.
Create a Point-to-Site VPN

In this exercise, you will create a Point-to-Site VPN. At the time of this writing, you can create a Point-to-Site VPN by using the Azure classic portal or Windows PowerShell. We use the Windows PowerShell method here since the Azure classic portal is scheduled to be fazed out. Note that the steps shown below were used on a Windows 10 computer. If you use a different Windows operating system, some of the prompts and UI elements might be slightly different.

1. Run the `Login-AzureRMAccount` command from a PowerShell prompt.
2. Type `Y` to enable data collection.
3. Authenticate with your administrative credentials.
4. Run the `Select-AzureRmSubscription -SubscriptionName "<YourSubscriptionName>"` command.
5. Run the following commands to declare your PowerShell variables using the following information. Note that you could opt to run through this exercise without relying heavily on variables but the reusability of the code is degraded in that scenario.
   - `$VNetName = "VNet1"
   - `$FESubName = "FrontEnd"
   - `$BESubName = "Backend"
   - `$GWSubName = "GatewaySubnet"
   - `$VNetPrefix1 = "192.168.0.0/16"
   - `$VNetPrefix2 = "10.254.0.0/16"
   - `$FESubPrefix = "192.168.1.0/24"
   - `$BESubPrefix = "10.254.1.0/24"
   - `$GWSubPrefix = "192.168.200.0/26"
   - `$VPNClienAddressPool = "172.16.201.0/24"
   - `$RG = "TestRG"
   - `$Location = "East US"
   - `$DNS = "8.8.8.8"
   - `$GWName = "GW"
   - `$GWIPName = "GWIP"
   - `$GWIPconfName = "gwipconf"
   - `$P2SRootCertName = "ARMP2SRootCert.cer"
6. Create a resource group by running the `New-AzureRmResourceGroup -Name $RG -Location $Location` command.
7. Run the `$fesub = New-AzureRmVirtualNetworkSubnetConfig -Name $FESubName -AddressPrefix $FESubPrefix` command.
8. Run the `$besub = New-AzureRmVirtualNetworkSubnetConfig -Name $BESubName -AddressPrefix $BESubPrefix` command.
9. Run the `\$gwsub = New-AzureRmVirtualNetworkSubnetConfig -Name $GWSubName - AddressPrefix $GWSubPrefix` command.
10. Run the `New-AzureRmVirtualNetwork -Name $VNetName -ResourceGroupName $RG - Location $Location -AddressPrefix $VNetPrefix1,$VNetPrefix2 -Subnet $fesub, $besub, $gwsub -DnsServer $DNS` command.
11. Run the `\$vnet = Get-AzureRmVirtualNetwork -Name $VNetName -ResourceGroupName $RG` command.
12. Run the `\$subnet = Get-AzureRmVirtualNetworkSubnetConfig -Name "GatewaySubnet" - VirtualNetwork $vnet` command.
13. Request a public IP address for the VPN gateway by running the `\$pip = New-AzureRmPublicIpAddress -Name $GWIPName -ResourceGroupName $RG -Location $Location -AllocationMethod Dynamic` command.
14. Run the `\$ipconf = New-AzureRmVirtualNetworkGatewayIpConfig -Name $GWIPconfName - Subnet $subnet -PublicIpAddress $pip` command.

**Note:** The makecert.exe tool is deprecated and its functionality will be replaced by Windows PowerShell.

16. Once the download has completed, begin the installation.
17. On the Specify Location page, click **Next**.
18. On the Windows Kits Privacy page, click **Next**.
19. On the License Agreement page, click **Accept**.
20. On the Select the feature you want to install page, update the feature selections so that only the .Net Framework 4.6.2 Software Development Kit and the Windows Software Development Kit are selected for installation.
21. Click **Install**. If you receive a User Account Control notification, click **Yes**.
22. When the installation is finished, click **Close**.
23. Open an elevated command prompt.
24. Change the directory to `C:\Program Files (x86)\Windows Kits\10\bin\x64`.
25. Generate the root certificate by running the `makecert -sky exchange -r -n "CN=ARMP2SRootCert" -pe -a sha1 -len 2048 -ss My "ARMP2SRootCert.cer"` command. The certificate will be installed in the Current User\Personal\Certificates store.
26. Open the Certificates MMC and export the certificate to `%SYSTEMDRIVE%\temp`. Export the certificate without the private key in Base-64 encoded X.509 (.CER) format.

**Note:** The next commands upload the exported certificate to Microsoft Azure and use it as the VPN client root certificate.

27. Run the `$filePathForCert = "%SYSTEMDRIVE%\temp\ARMP2SRootCert.cer"` command.
29. Run the `$CertBase64 = [system.convert]::ToBase64String($cert.RawData)` command.
30. Run the $p2srootcert = New-AzureRmVpnClientRootCertificate -Name $P2SRootCertName -PublicCertData $CertBase64 command.

**Note:** The next command creates the VPN gateway. It can take as many as 30 minutes to complete.

31. Run the New-AzureRmVirtualNetworkGateway -Name $GWName -ResourceGroupName $RG -Location $Location -IpConfigurations $ipconf -GatewayType Vpn -VpnType RouteBased -EnableBgp $false -GatewaySku Standard -VpnClientAddressPool $VPNClientAddressPool -VpnClientRootCertificates $p2srootcert command.

32. Run the Get-AzureRmVpnClientPackage -ResourceGroupName $RG -VirtualNetworkGatewayName $GWName -ProcessorArchitecture Amd64 command.

33. The PowerShell command will return a URL. Copy and paste the URL into your web browser to download the VPN client configuration package.

34. Once the package has been downloaded, run the installer.

35. You may receive a Windows SmartScreen security prompt. If so, click More info and then click Run anyway.

36. If a User Account Control window is displayed, click Yes.

37. In the installer confirmation window, click Yes install the VPN client.

38. On the client computer, navigate to Network Connections. You should see a new connection with the name of the virtual network you previously created.

39. Back at the elevated command prompt, run the following command to install a client certificate:

   `makecert.exe -n "CN=<YourCommonName>" -pe -sky exchange -m 96 -ss My -in "ARMP2SRootCert" -is my -a sha1`

40. On the VPN page of Network &Internet settings, select your virtual network and then click Connect.

41. On the Windows Azure Virtual Network prompt, click Connect and then click Continue.

42. Once connected, you will have full access to any service and virtual machine hosted in your virtual network. Verify your connection by running the `ipconfig /all` command and confirming that you have an IP address from the point-to-site network range.