

**Company Name: Contoso**

### Subnets:

|  |  |
| --- | --- |
|  |  |
| **Contoso Virtual Network Configuration** | Address Space: 192.168.10.0/24  **Production** Subnet: 192.168.10.0/25  **Development** Subnet: **192.168.10.128/26**  **Gateway** Subnet: 192.168.10.192/26 or the default subnet shown during the creation |
| **VNet Gateway** | 192.168.20.0 / 25 |
| Storage Account Type | Page Blobs with Diagnostics enabled |
| VM DSC Configuration  VM1 – Web Server | **CONTOSOPOCVM01** |
| VM2 – Non-Web Server | **CONTOSOPOCVM02** |

### Naming Conventions

|  |  |
| --- | --- |
| **Resource Group Name** | ContosoPOC |
| **VNetName** | ContosoVNET - 192.168.10.0/24 |
| **Production Subnet name** | Production - 192.168.10.0/25 |
| **Development Subnet Name** | Development - 192.168.10.0/26 |
| **Gateway Subnet Name** | GatewaySubnet |
| **Location** | US East 2 |
| **GWName** | CONTOSOGW |
| **Location** | US East 2 |
| **Gateway address pool** | 192.168.20.0/25 |

# Start Lab

## Configure First

Copy and extract “Cloud and Proud V2 Live Delivery Files.zip” file into “C:\ Cloud and Proud V2 Live Delivery Files” directory. This is to ensure the scripts provided in the lab run without any issues. Variable in the scripts refer to the “C:\ Cloud and Proud V2 Live Delivery Files”.

|  |  |
| --- | --- |
|  | Scripts : Contain scripts required for the lab  Website: Website template for Webapp lab  Makecert.exe: Create root and client certificate for point to site VPN  Putty.exe: Connect Linux VM (may not be required in this lab) |

### Configure PowerShell (if not already configured)

1. [Install PowerShell](https://msdn.microsoft.com/en-us/powershell/scripting/setup/installing-windows-powershell) if not installed. Lab environment on “Labs on Demand” is pre-configured with PowerShell and PowerShell ISE
2. Open PowerShell or PowerShell ISE “as an Administrator”
3. **OPTIONAL:** Ensure the Set-ExecutionPolicy cmdlet is run to allow your computer to run scripts. Windows PowerShell has four different execution policies:
   1. *Run “Set-ExecutionPolicy RemoteSigned” to allow scripts to run in the PowerShell environment*

### Configure Azure Cmdlets and Subscription

1. [Install-Module AzureRM](https://msdn.microsoft.com/en-us/library/mt125356.aspx) -Force
2. Import-Module AzureRM
3. Add-AzureRmAccount

*Note: The first command installs the AzureRM module from the PowerShell Gallery. The second command installs all the component modules of Azure Resource Manager in the module version range specified in the AzureRM module.*

### Create Resource Group

1. Create Resource Group named “ContosoPOC” , location “US East 2”
2. Review various options in the left-hand pane

### Build Virtual Network

1. Search for “Virtual Network” from the search bar and select “Virtual Network”
2. Name it as “ContosoVNET”, Address space of **192.168.10.0/24**
3. Name subnet as “**Production” 192.168.10.0/25**
4. Select resource group “ContosoPOC”
5. Review various options in the left-hand pane

### Create Additional Subnets in the Virtual Network

1. From the “Subnets” section in the left-hand side pane, create subnet “Development”
2. IP subnet address space “**192.168.10.64/26”**
3. While in the subnet menu, from the top pane click on “Gateway Subnet” address space “**192.168.10.192/28”**

Verify various options from the left-hand pane, such as “DNS Server”, Peering, Automation Script, Diagram etc.

### Create Virtual Network Gateway

1. Click on resource group
2. Add -> search -> Virtual Network Gateway -> Select “Virtual Network Gateway” from the search results
3. Name is as “ContosoGW”
4. Select “VPN”, “Route Based VPN” Basic
5. In the virtual networks Select “ContosoVNet”
6. Choose a public IP address -> Create New -> OK “ContosoGWIP”
7. Location “US East 2”
8. Create

**It may take “20-30 minutes” to create the gateway VM. Create the VMs now while the VPN Gateway is being created**

### Configure the Gateway

1. Click on the “ContosoGW” gateway just created
2. “Point to Site Configuration” from left hand pane
3. In the address pool select “192.168.20.0/25”
4. Save the configuration

### Start Building VMs

**While the VPN Gateway is being created, start creating the VMs so that you can connect using the VPN client from the lab machine.**

1. Go to “Resource Groups” -> Search for “2012 R2 Datacenter” and select “Windows Server Datacenter 2012 R2” image
2. Name of the VM “ContosoPOCVM01”
3. VM Disk Type “SSD”
4. User name “student”
5. Password “Pass@word1234”
6. Resource Group “ContosoPOC”
7. Location “US East 2”
8. In the size select “DS2\_V2 Standard”
9. In the Settings section
   1. Create new storage account “contosohqvmdisks” -> Premium storage -> Redundancy LRS ->Virtual Network “Contso-VNet”
   2. Subnet “Production” -> Public IP Address “none” -> Network Security Group- default
   3. Extensions -> add-extension -> Select “Anti-malware”
   4. High availability – “none”
   5. Monitoring – “Disabled”
   6. Diagnostics “Enabled” -> create new storage -> “contosohqdiagdisk”
   7. Select “OK” to deploy
   8. Verify template options
   9. Virtual machine will be created in 10-15 mins
10. Connect to the VM using RDP, ensure you are connected to the VPN
11. Try to tag with certain tags “production”
12. Once the VM is created, verify various options in the left-hand side pane

* Add a second VM of same configuration “CONSTOSOPOCVM02”
* Verify ow to upload new disks etc in the VM configuration

### Configure Root Certificate for the VPN Client via PowerShell

Makecert.exe file is located in the “C:\ Cloud and Proud V2 Live Delivery Files”

|  |
| --- |
| cd 'C:\Cloud and Proud V2 Live Delivery Files'  makecert.exe -sky exchange -r -n "CN=CHQRoot" -pe -a sha256 -len 2048 -ss My "CHQRoot.cer"  makecert.exe -n "CN=CHQClient" -pe -sky exchange -m 96 -ss My -in "CHQRoot" -is my -a sha256  certutil -encode CHQRoot.cer CHQRoot2.cer |

### Configure VPN and Download VPN Client Using the Script Below

1. Run the VPN Script below
2. Download the VPN client (AMD64) from Azure Portal or by executing the last cmdlets and Install the VPN Client on the lab machine
3. Connect to the Azure VPN Gateway using the VPN Client
4. Verify client IP address using “ipconfig /all”

|  |
| --- |
| #Trimming the certificate  $Text = Get-Content -Path "D:\Ignite2016\AzureCSPWorkshop\Cloud and Proud V2 Live Delivery Files\CPOCRoot2.cer"  $CertificateText = for ($i=1; $i -lt $Text.Length -1 ; $i++){$Text[$i]}  # Uploading the root certificate to the Virtual Gateway: Verify the Azure resources names before running this script  $RG = "CONTOSOHQPOC"  $gwNAME = "CONTOSOPOCGW"  $P2SRootCertName = "CPOCRoot2.cer"  Add-AzureRmVpnClientRootCertificate -PublicCertData ($CertificateText | out-string) -ResourceGroupName $RG -VirtualNetworkGatewayName $GWName -VpnClientRootCertificateName $P2SRootCertName  # VPN client can be downloaded from the Azure Portal or by executing the command below  # Creating a download URL for the Windows VPN Client - simply copy and paste into a browser to download.  Get-AzureRmVpnClientPackage -ResourceGroupName $RG -VirtualNetworkGatewayName $GWName -ProcessorArchitecture X86  Add-AzureRmVpnClientRootCertificate -PublicCertData ($CertificateText | out-string) -ResourceGroupName -VirtualNetworkGatewayName $GWName -VpnClientRootCertificateName $P2SRootCertName |

### Automation and Desired State Configuration

1. Go to Market place -> automation -> Microsoft automation package
2. Name “ContosoPOCDSC”
3. Resource Group “ContosoOC”
4. Location “US East 2”
5. Create Azure Run as Account , select “Yes”
6. Click Create to create the automation account
7. Open the Automation Account “ContosoPOCDSC”
8. Click “DSC Configurations”
9. Click “Add a Configuration” -> upload the “DSCConfig.ps1” file from the script location
10. Click Ok to upload the file
11. Click on the file and verify the configuration of the file-> Click “Compile” from the top pane
12. This allows to select nodes that need DSC settings for automation
13. Select “CONTOSOPOCVM01” as the “Web server” in the configuration tab
14. Click Create
15. Select “CONTOSOPOCVM02” as the “Not Web server” in the configuration tab
16. After completing the webapp lab below, login to the VM01 and verify if the IIS Services have been installed inside the VM. If the IIS is installed, this indicates that the DSC has taken effect

## Adding Webapp

1. Go to Resource Group -> Market place -> Select WebApp -> Create
2. In the new blade “contosohqweb01”, resource group “ContosoPOC”
3. Create New Plan -> contosohqappplan01 -> select “S1 Standard” plan
4. Clieck Ok -> Create
5. Download publish profile to deploy website
   1. Visual Studio -> File -> Open ->Website -> Open from the deploy site
   2. Change the header name, and any other details
   3. Run the website to test
   4. Now the Webapp would have been created, verify the details from the left-hand pane
6. Go to ->Overview tab in the “contosoweb01” blade
7. More -> Get Publish Profile -> Download and save it locally
8. Visual Studio -> Publish ->import publish profile from local disk
9. Click Publish to publish the website to Azure

**>> Follow Instructor for demonstration on publishing websites from Visual Studio**