Microsoft Cloud Workshop

Building a resilient IaaS architecture

Hands-on lab step-by-step

December 2017

Contents

Building a resilient IaaS architecture hands-on lab step-by-step

Abstract and learning objectives

The student will assist a large organization in evaluating their current infrastructure deployments in Azure, and help identify single points of failure. Attention will be given to making the customer's current deployments more resilient and communicating best practices to ensure future deployments will follow best practices.

Attendees will be better able to design resilient applications in Azure, for high availability and disaster recovery. Specific attention will be given to:

- The use of availability sets
- The use of Managed Disks
- Design principles when provisioning storage to VMs
- Effective employment of Azure Backup to provide point-in-time recovery

Overview

Litware has asked you to deploy their infrastructure in a resilient manner to insure their infrastructure will be available for their users and gain an SLA from Microsoft.

Requirements

1. Microsoft Azure Subscription
2. Virtual Machine Built during this hands-on lab or local machine with the following:
    a. Visual Studio 2017 Community or Enterprise Edition
    b. Azure SDK 2.9.+
    c. Latest Azure PowerShell Cmdlets
    d. https://azure.microsoft.com/en-us/downloads/
    e. Ensure you reboot after installing the SDK or Azure PowerShell will not work correctly

Help References

Description	Links
Authoring ARM Templates	https://azure.microsoft.com/en-us/documentation/articles/resource-group-authoring-templates/
Azure Resource Manager templates with VS 2015	http://blogs.msdn.com/b/kaevans/archive/2015/07/06/azure-resource-manager-templates-with-visual-studio-2015.aspx
Virtual Machine Scale Set Samples	https://github.com/gbowerman/azure-myriad
Azure Quick Start Templates	https://github.com/Azure/azure-quickstart-templates
Network Security Groups	https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/

Before the hands-on lab

Duration: 30 minutes

In this exercise, you build a Lab VM followed by preparing an Azure infrastructure containing several issues needing to be addressed from a resiliency standpoint. You will create an Active Directory environment, a SQL database tier, and a web tier for a Web Application.

Prerequisites

1. Microsoft Azure subscription: http://azure.microsoft.com/en-us/pricing/free-trial/

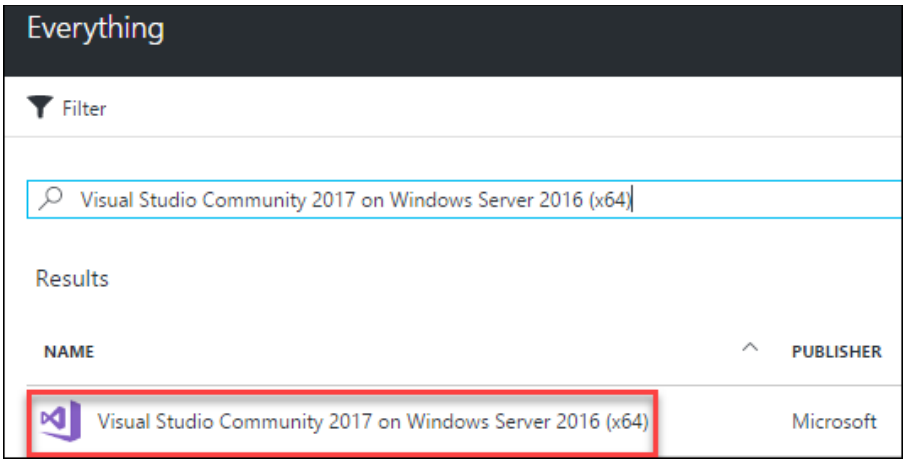
Task 1: Create a Virtual Machine using the Azure portal

1. Launch a browser and navigate to https://portal.azure.com. Once prompted, login with your Microsoft Azure credentials. If prompted, choose whether your account is an organization account or just a Microsoft Account.

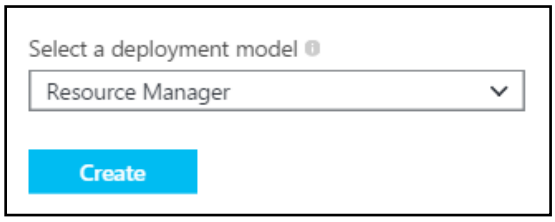
   Note: You may need to launch an "in-private" session in your browser if you have multiple Microsoft Accounts.

2. Click on **+NEW**, and in the search box, type in **Visual Studio Community 2017 on Windows Server 2016 (x64)** and press Enter. Click the Visual Studio Community 2017 image running on Windows Server 2016 and with the latest update.

3. In the returned search results, click the image name.



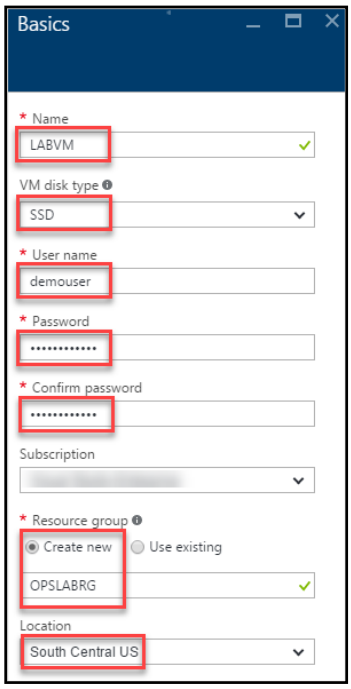
4. At the bottom of the page in the Marketplace solution blade, keep the deployment model set to **Resource Manager**, and click **Create**.



5. Set the following configuration on the Basics tab, and click **OK**.

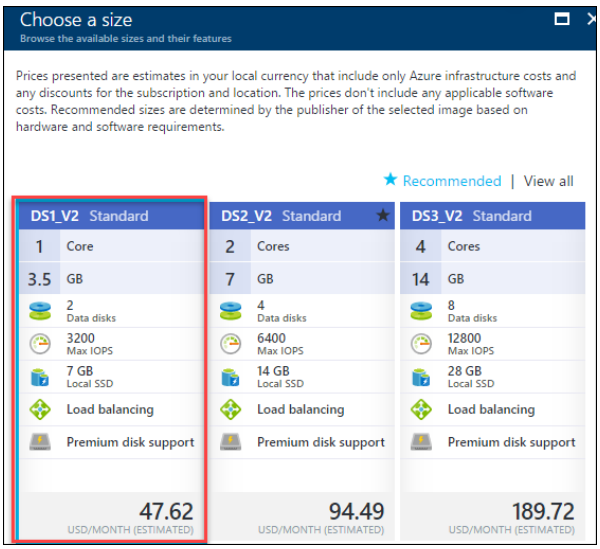
   a. Name: **LABVM**

b. VM disk type: **SSD**
c. User name: **demouser**
d. Password: **demo@pass123**
e. Subscription: **If you have multiple subscriptions choose the subscription to execute your labs in.**
f. Resource Group: **OPSLABRG**
g. Location: **Choose the closest Azure region to you.**



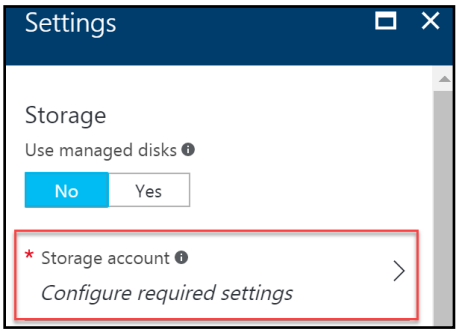
6. Choose the **DS1_V2 Standard** instance size on the Size blade.

Note: You may have to click the View All link to see the instance sizes.

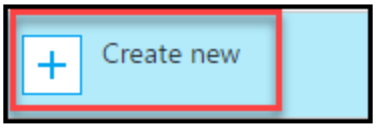


Note: If the Azure Subscription you are using is NOT a trial Azure subscription, you may want to choose the DS2_V2 to have more power in this LABMV. If you are using a trial subscription or one that you know has a restriction on the number of cores, stick with the DS1_V2.

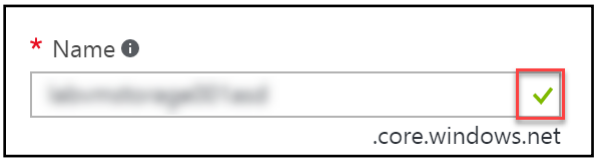
7. Click **Configure required settings** to specify a storage account for your virtual machine if a storage account name is not automatically selected for you.



8. Click **Create new**.

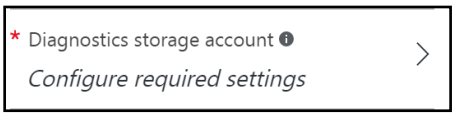


9. Specify a unique name for the storage account (all lower letters and alphanumeric characters), and ensure the green checkmark showing the name is valid.

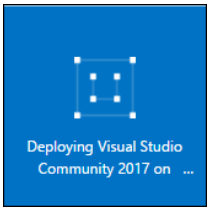


10. Click **OK** to continue.

11. Click **Configure required settings** for the Diagnostics storage account if a storage account name is not automatically selected for you. Repeat the previous steps to select a unique storage account name. This storage account will hold diagnostic logs about your virtual machine that you can use for troubleshooting purposes.



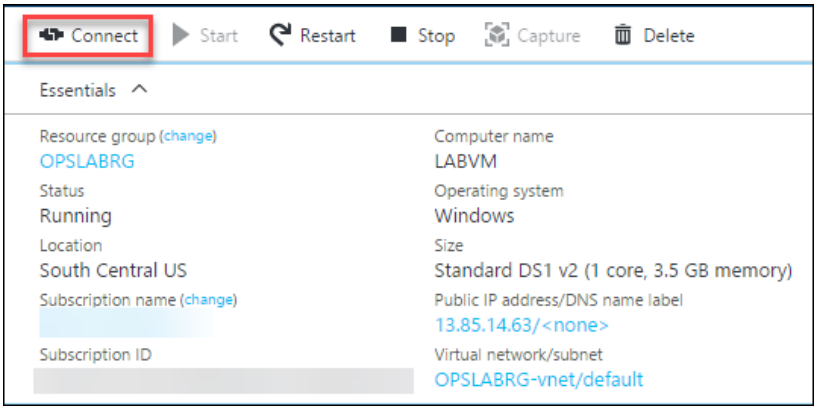
12. Accept the remaining default values on the Settings blade, and click **OK**. On the Summary page, click **OK**. The deployment should begin provisioning. It may take more than 10 minutes for the virtual machine to complete provisioning.



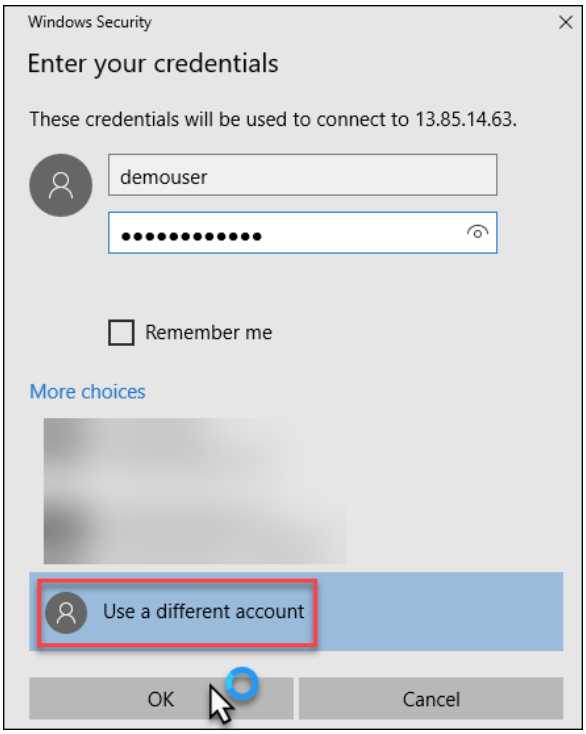
Note: Once the deployment is complete, move on to the next exercise.

Task 2: Connect to the VM and download the student files

1. Move back to the portal page on your local machine, and wait for **LABVM** to show the Status of **Running**. Click **Connect** to establish a new remote desktop session.



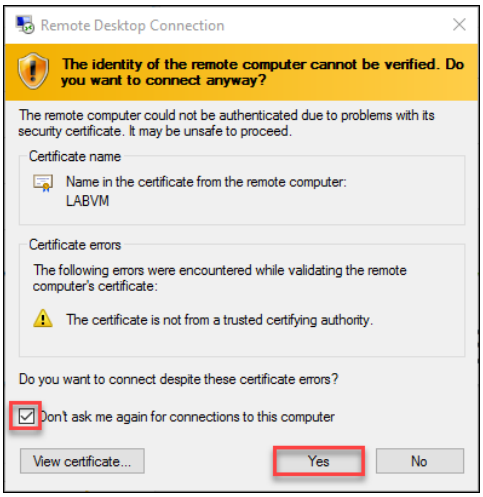
2. Depending on your remote desktop protocol client and browser configuration, you will either be prompted to open an RDP file, or you will need to download it followed by opening it up separately to connect. You may also be required to click, **Use a different account**.



3. Login with the credentials specified during creation:

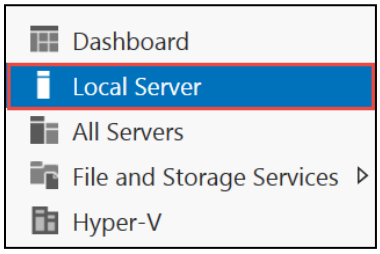
    a. User: **demouser**
    b. Password: **demo@pass123**

4. You will be presented with a remote desktop connection warning because of a certificate trust issue. Click, **Don't ask me again for connections to this computer** followed by **Yes** to continue with the connection.

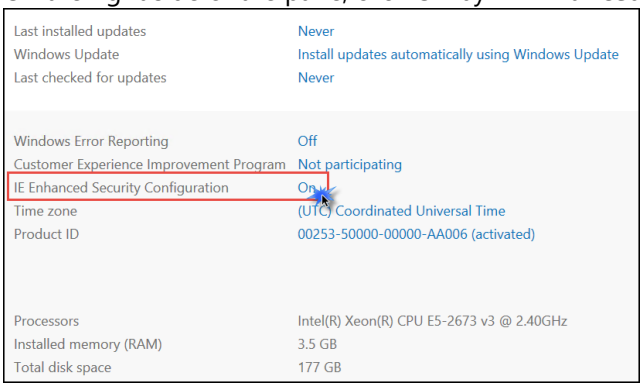


5. When logging on for the first time, you will see a prompt on the right asking about network discovery. Click **No**.

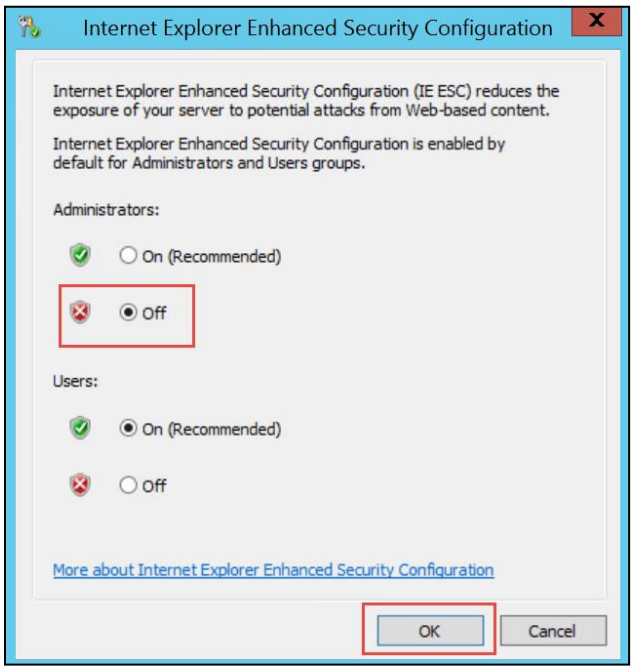
6. Notice that Server Manager opens by default. On the left, click **Local Server**.



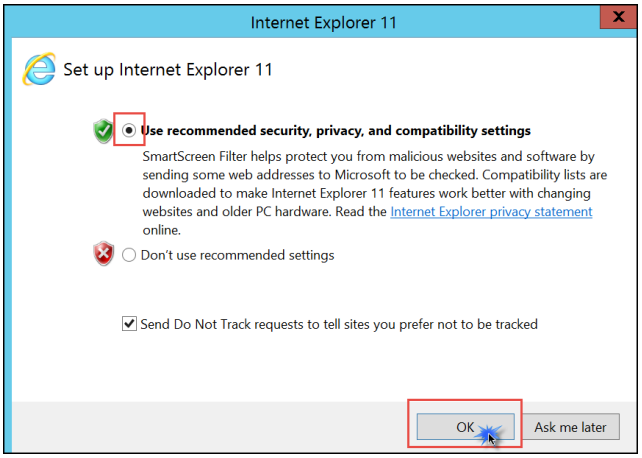
7. On the right side of the pane, click **On** by **IE Enhanced Security Configuration**.



8. Change to **Off** for Administrators, and click **OK**.



9. In the lower left corner, click Internet Explorer to open it. On first use, you will be prompted about security settings. Accept the defaults by clicking **OK**.

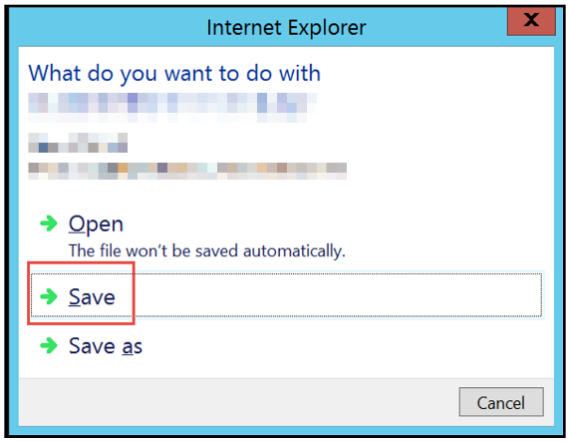


10. If prompted, click **Don't show this again** regarding protected mode.

11. To download the exercise files for the hands-on lab, paste this URL into the browser.

```
https://cloudworkshop.blob.core.windows.net/resilient-iaas-hackathon/Building_Resilient_Iaas_Hackathon_Student_Files.zip
```

12. You will be prompted about what you want to do with the file. Select **Save**.



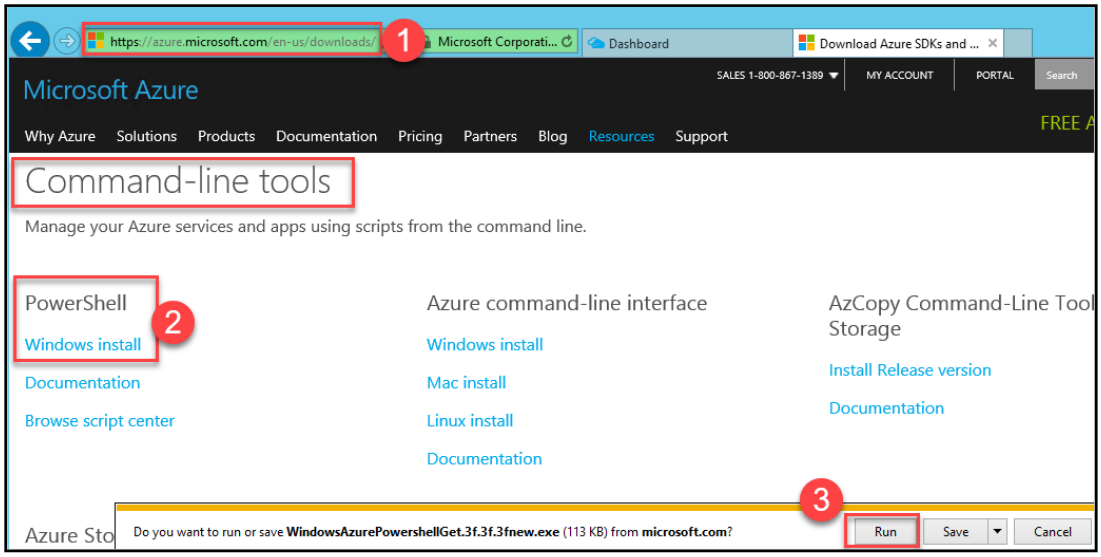
13. Download progress is shown at the bottom of the browser window. When the download is complete, click **Open folder**.

14. The **Downloads** folder will open, ***Right-click*** the zip file, and click **Extract All**. In the **Extract Compressed (Zipped) Folders** window, enter **C:\Hackathon** in the **Files will be extracted to this folder** dialog. Click the **Extract** button.

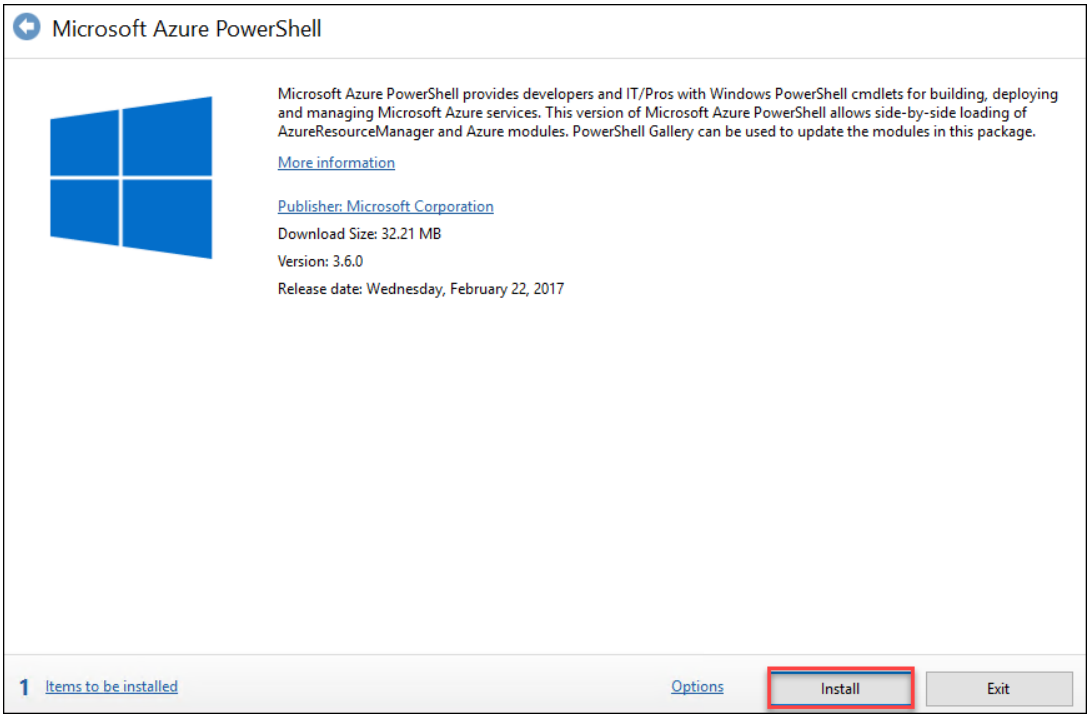
Task 3: Update the Azure PowerShell CmdLets

Note: The LABVM you created already has the Azure PowerShell cmdlets installed, but you should update the version to ensure the labs work well.

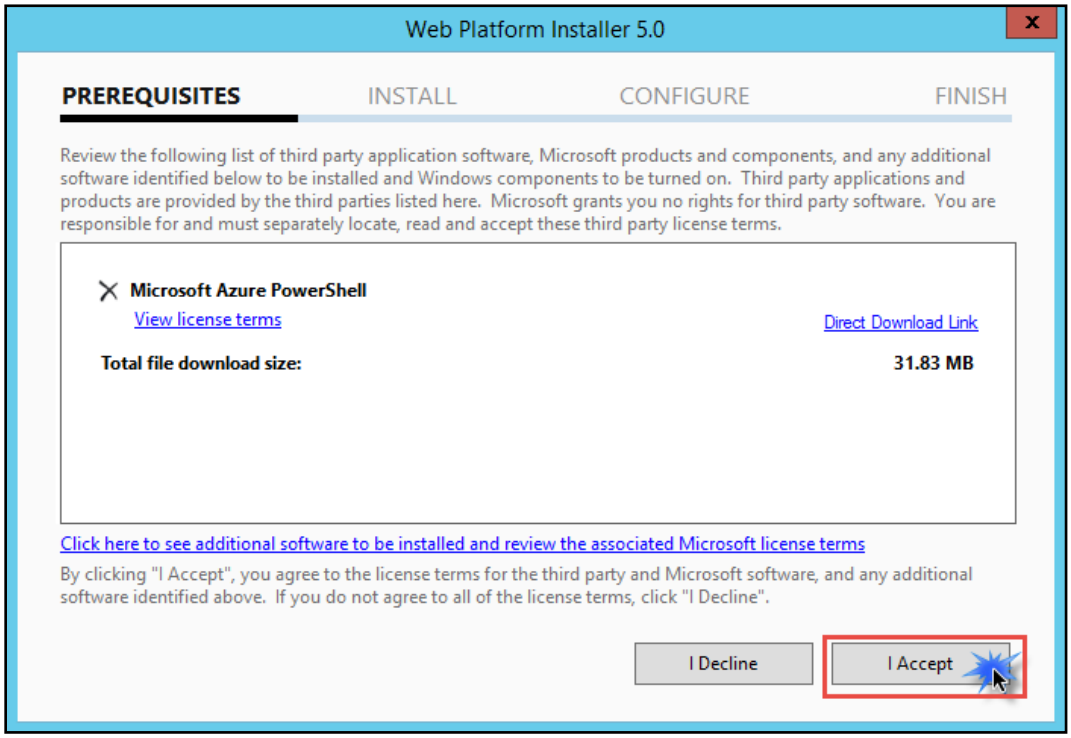
1. In Internet Explorer, navigate to https://azure.microsoft.com/en-us/downloads/. In the **PowerShell** section, click **Windows install**, and choose **Run.**



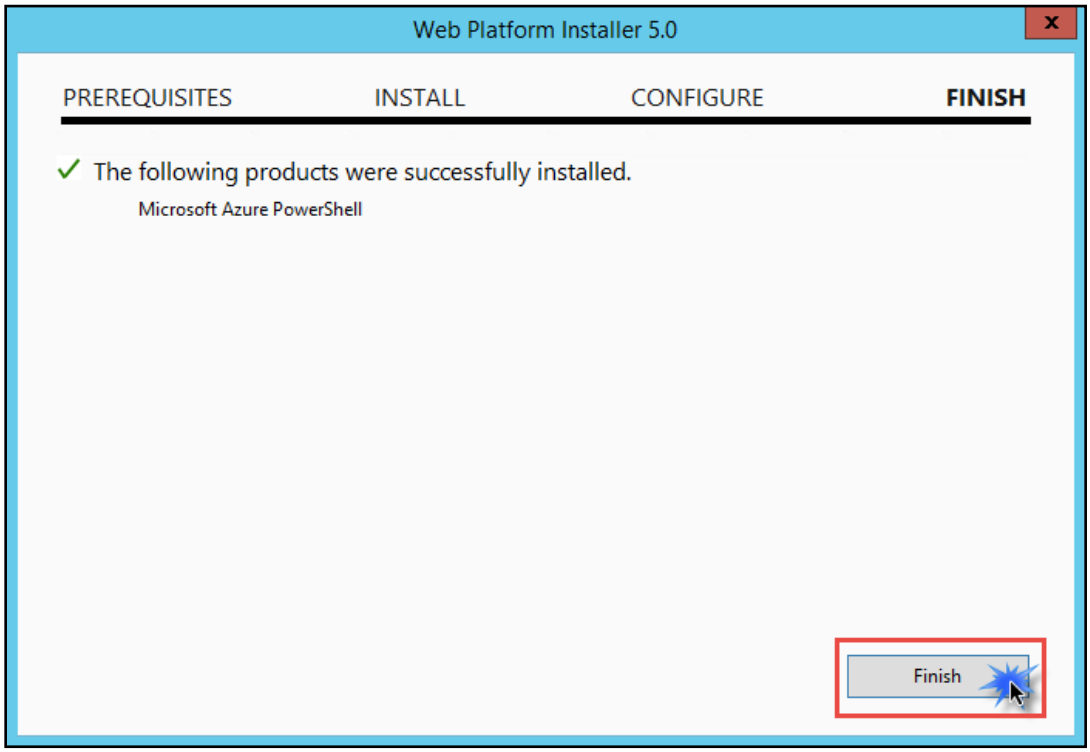
2. A Web Platform Installer dialog box will open showing the latest version of the Azure PowerShell modules. Click **Install**.



3. On the next dialog, click **I Accept** to accept the license terms for Azure PowerShell.



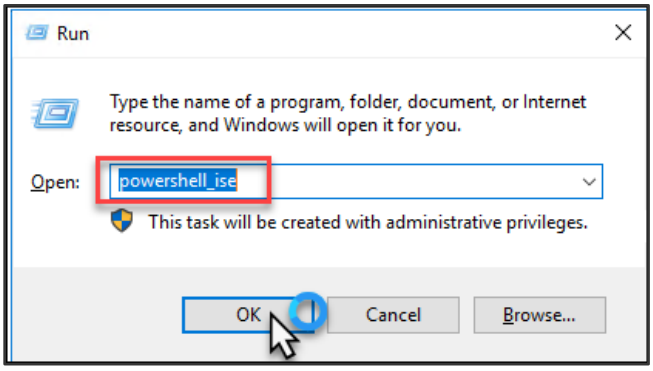
4. When the install is completed, click **Finish**.



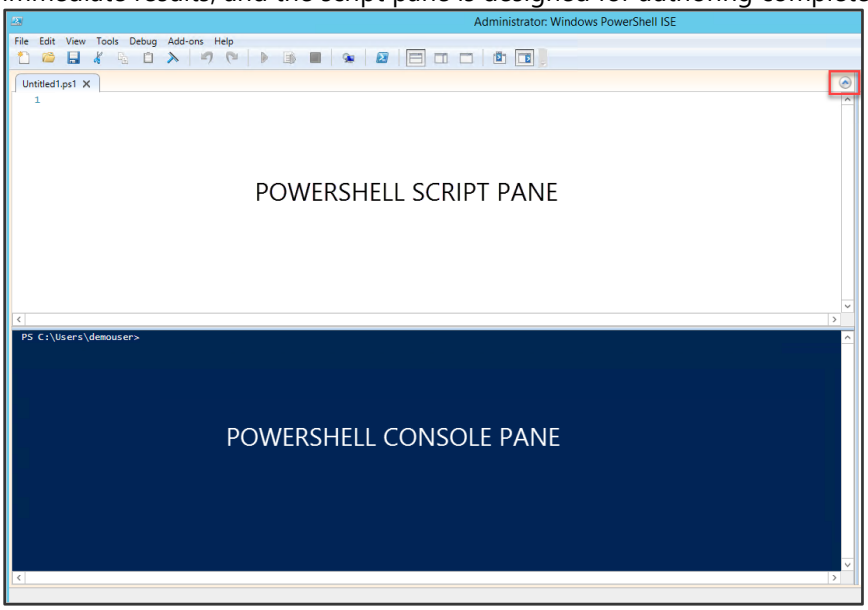
5. Once the installation for the Azure PowerShell tools are complete, click **Exit**, restart the LABVM, reconnect after it has been restarted, and continue.

6. Launch the PowerShell Integrated System Environment (ISE) by opening a Windows run prompt. To do this, **Right-click** on the **Start** button, and choose **Run**.

7. Launch the PowerShell Integrated System Environment (ISE) by typing in **PowerShell_ISE** in the Windows run prompt.



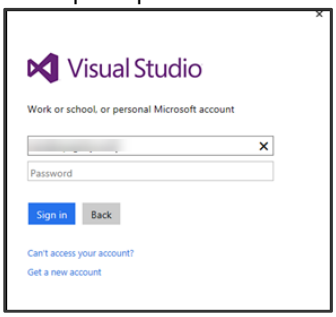
8. The ISE consists of two windows, the Script Pane and the Console Pane. If the Script Pane is not visible, click the ^ icon towards the top right of the window. The Console Pane is where you can execute individual commands with immediate results, and the script pane is designed for authoring complete scripts.



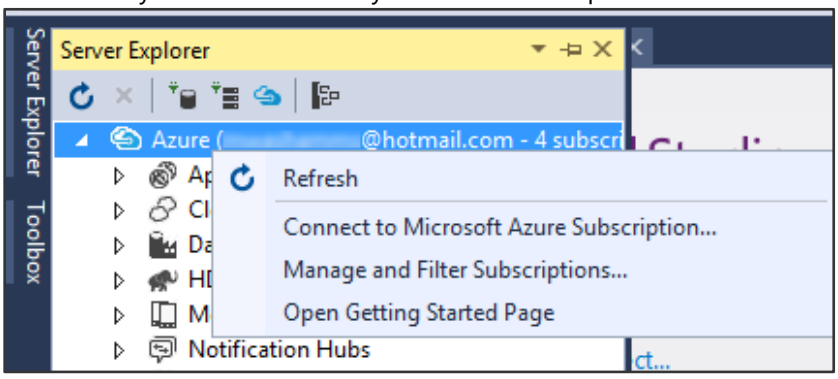
9. In the console pane execute the following command:

Task 4: Validate Connectivity to Azure

1. Within the virtual machine, launch Visual Studio 2017, and validate you can login with your Microsoft Account when prompted.

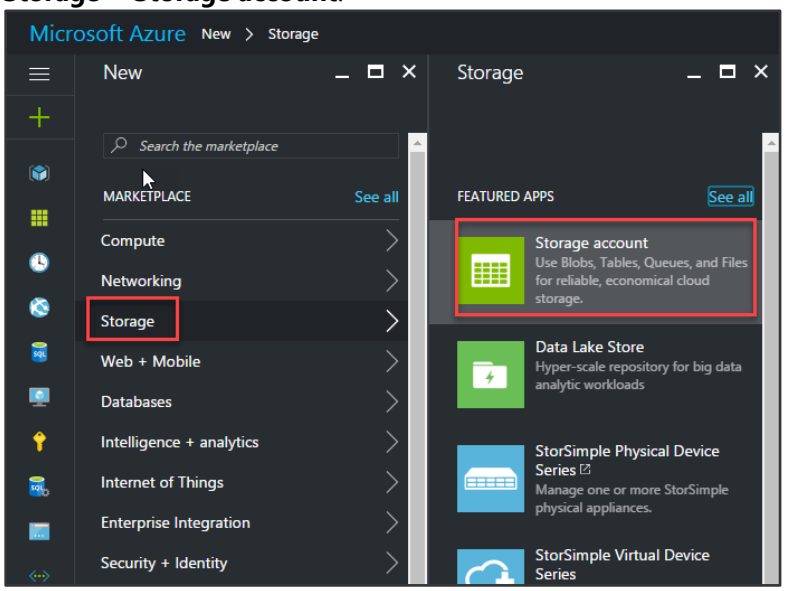


2. Validate connectivity to your Azure subscription. Launch Visual Studio, open Server Explorer from the View menu, and ensure you can connect to your Azure subscription.



Task 5: Create a Storage Account for Artifact Storage

1. Browse to the Azure portal, and authenticate at https://portal.azure.com.
2. Click **+ New**.
3. **Storage > Storage account**.



4. In the **Create storage account** blade, provide the following settings:
    a. Name: **litwareartifacts** (this name must be unique, so modify as appropriate)
    b. Replication: Change to **Locally-redundant storage (LRS)** via drop-down
    c. Resource Group: **Create new – ArtifactRG**
    d. Location: **Choose a location near you**
    e. Leave all other settings at the **Defaults**
    f. Click the **Create** button.

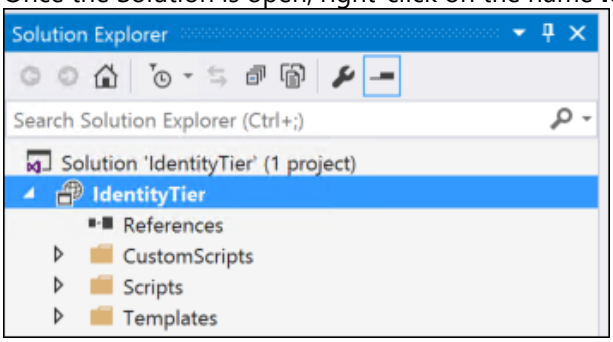
    Note: This will allow for storing of the scripts that will be run in the following tasks. Make sure to choose this for all deployments as the artifacts accounts or you will have issues.

Task 6: Run Script to create the Active Directory deployment

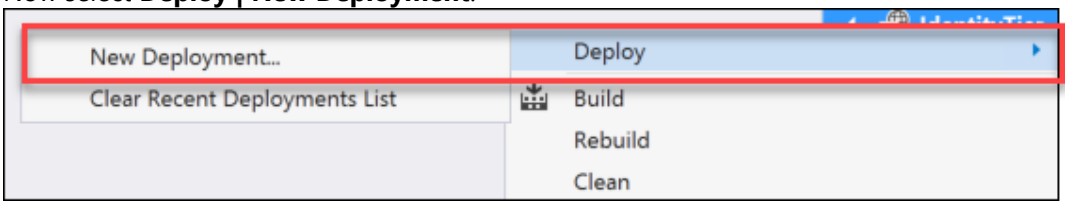
1. In Visual Studio, select **File | Open | Project/Solution**, browse to the files you previously downloaded and extracted to **C:\Hackathon**.

2. Open the **IdentityTier** folder, and select the Visual Studio Solution file: **IdentityTier.sln**.

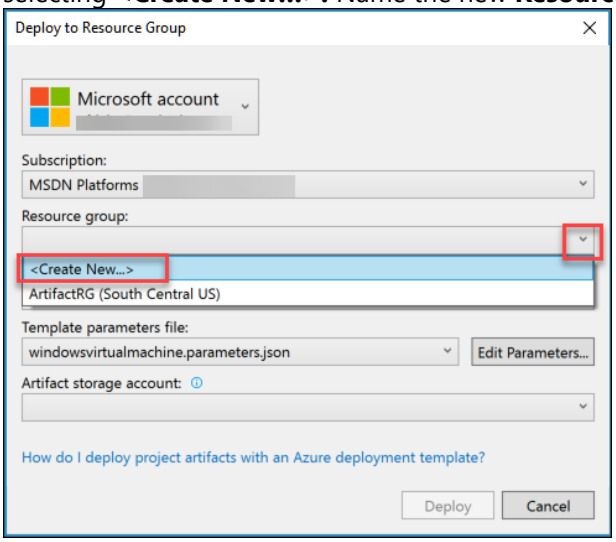
3. Once the Solution is open, right-click on the name **IdentityTier** in Solution Explorer.



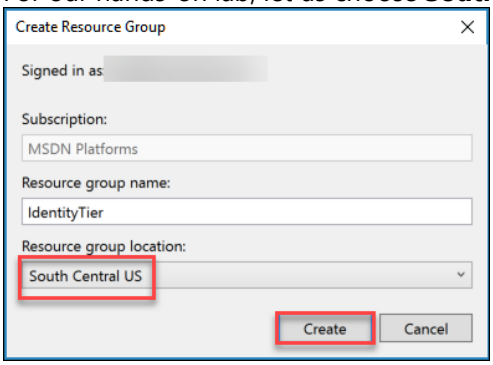
4. Now select **Deploy | New Deployment**.



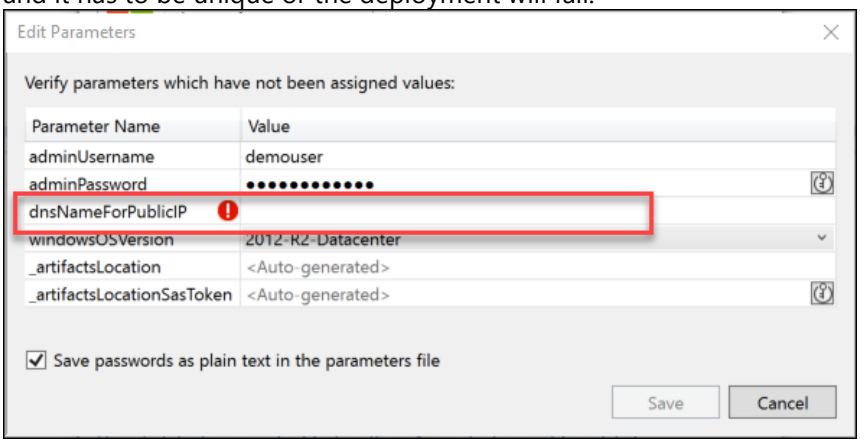
5. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New...>.** Name the new **Resource group "IdentityTier."**



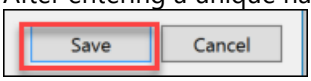
6. In the **Create Resource Group** window, leave everything at the **Defaults**, and choose a **Resource group location**. For our hands-on lab, let us choose **South Central US** and click the **Create** button to continue.



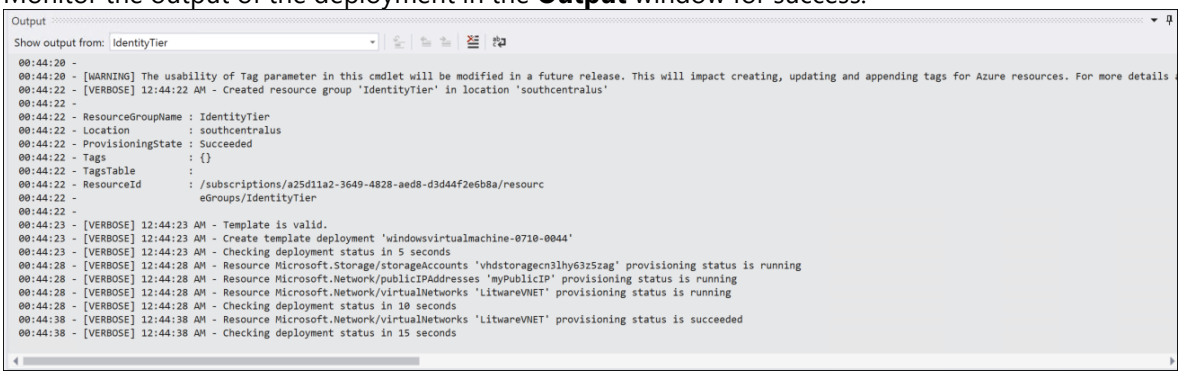
7. When prompted by the **Edit Parameters** window, enter a **dnsNameForPublicIP** making sure it is all lower-case, and it has to be unique or the deployment will fail.



8. After entering a unique name, click the **Save** button to start the deployment.

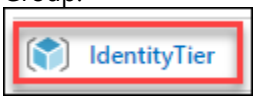


9. Monitor the output of the deployment in the **Output** window for success.

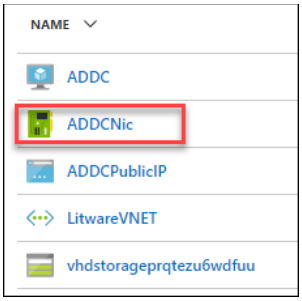


Note: This will take 10 minutes to deploy a Virtual Network, Storage Account, Subnets, other resources, and a domain controller Virtual Machine. It will also promote the DC as the primary DC for Litware.com.

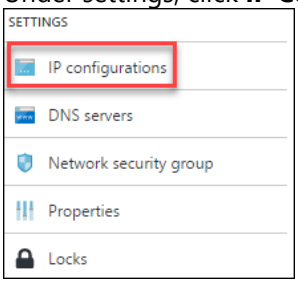
10. Before continuing to the next task, some network settings need to change. Open the **IdentityTier** Resource Group.



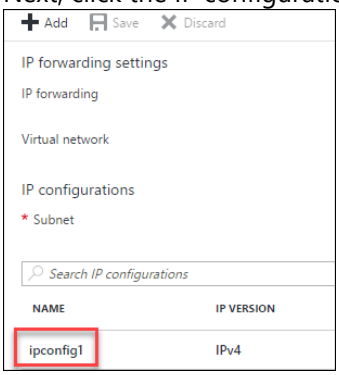
11. Click the **ADDCNic** Network Interface Card in the list.



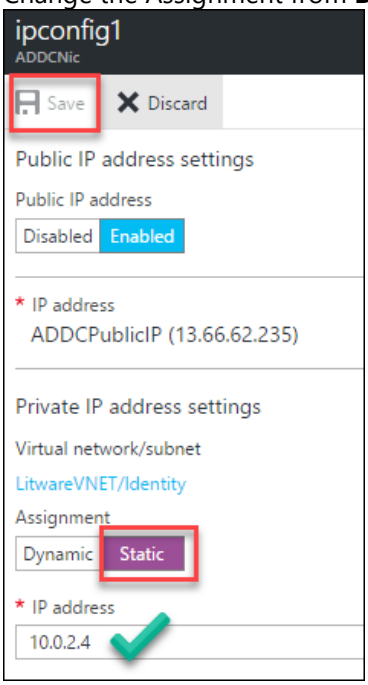
12. Under settings, click **IP Configurations**.



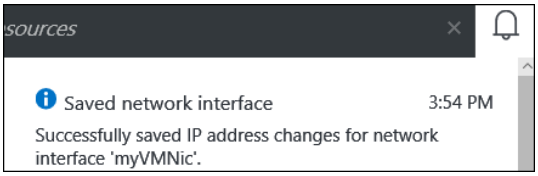
13. Next, click the IP configuration named **ipconfig1**.



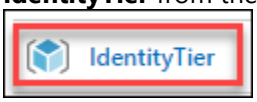
14. Change the Assignment from **Dynamic** to **Static**, verify that the address is **10.0.2.4**, and click **Save**.



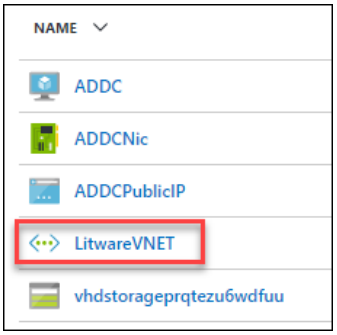
15. Once the Azure notification occurs for **Saved network interface**, continue for the VNET.



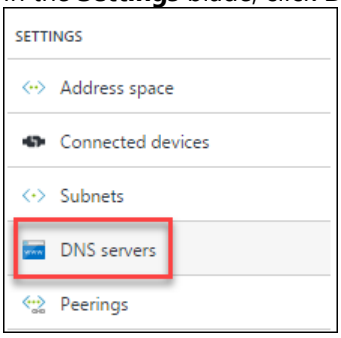
16. In the Azure portal, browse to **Resource Groups** in the left-hand menu. Click on the line with the name **IdentityTier** from the list of Resource Groups.



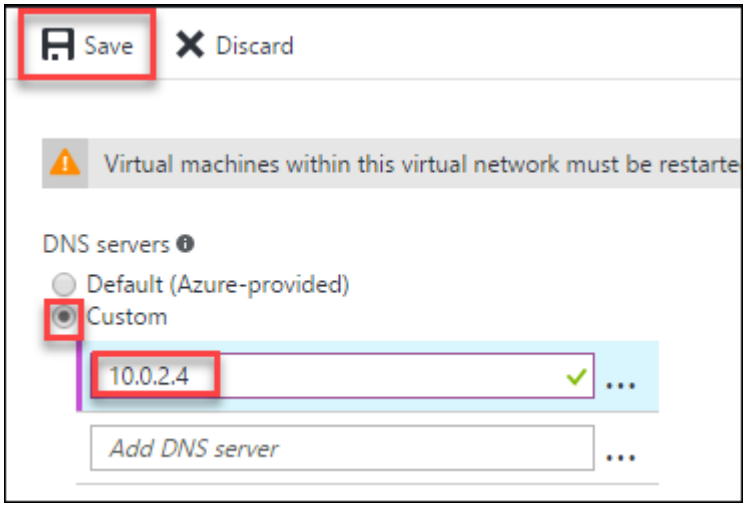
17. Click on **LitwareVNET** in the list of resources to open the VNET Resource.



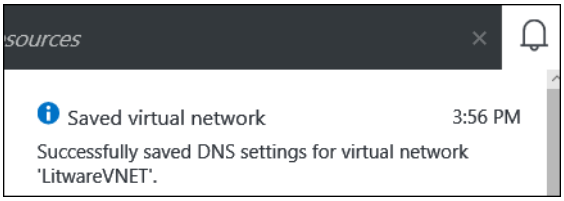
18. In the **Settings** blade, click **DNS servers.**



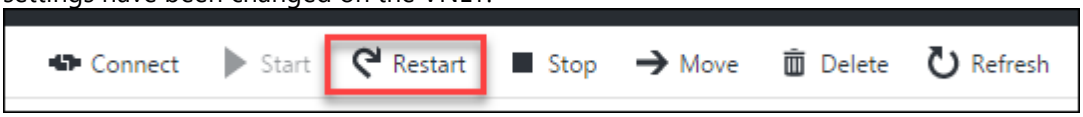
19. Change the setting to **Custom**, and for the **Primary DNS server**, enter the IP address of **10.0.2.4**, and click the **Save** icon.



20. Once the Azure notification occurs for **Saved virtual network**, continue to the next task.

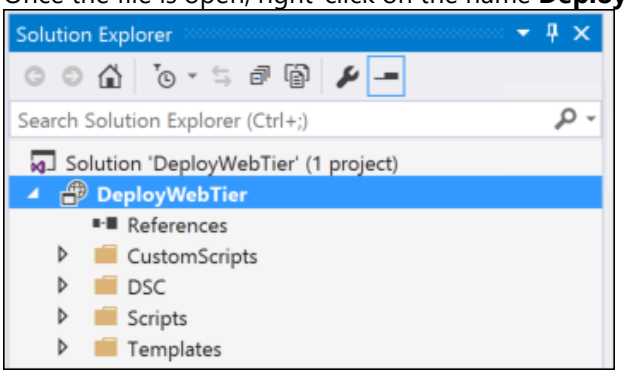


21. Move to the ADDC blade in the **IdentityTier** Resource Group, and click **Restart**. This is required since the DNS settings have been changed on the VNET.

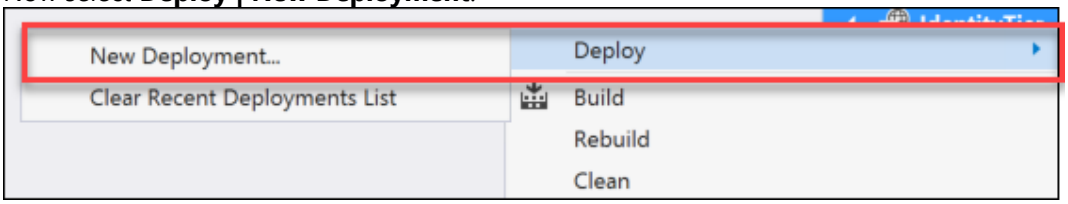


Task 7: Run Script to create the Web and SQL Tiers

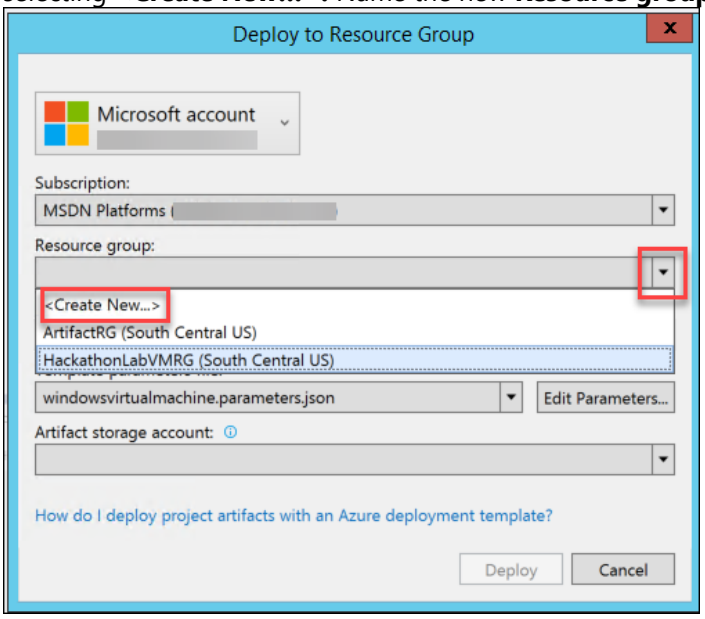
1. Move back to a RDP session into your LABVM.
2. In Visual Studio, select **File | Open | Project/Solution**, and browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **DeployWebTier** folder, and select the Visual Studio Solution file: **DeployWebTier.sln**.
4. Once the file is open, right-click on the name **DeployWebTier** in Solution Explorer.



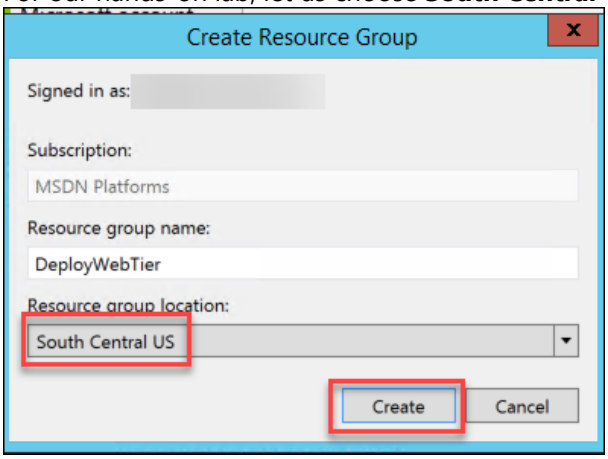
5. Now select **Deploy | New Deployment**.



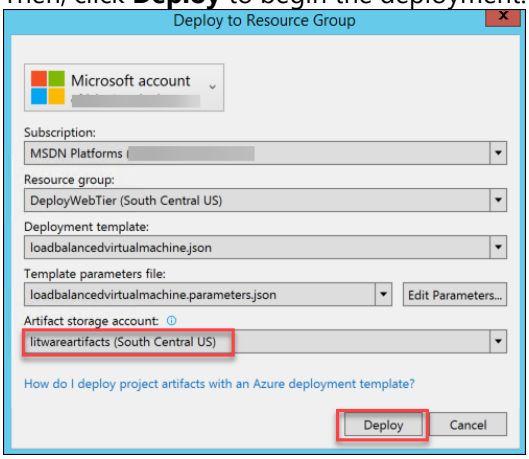
6. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New...>.** Name the new **Resource group** "**DeployWebTier**."



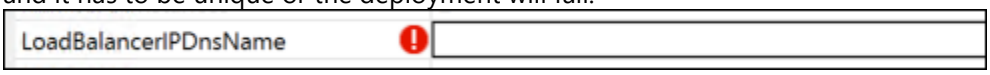
7. In the **Create Resource Group** window, leave everything at the **Defaults**, and choose a **Resource group location**. For our hands-on lab, let us choose **South Central US**, and click the **Create** button to continue.



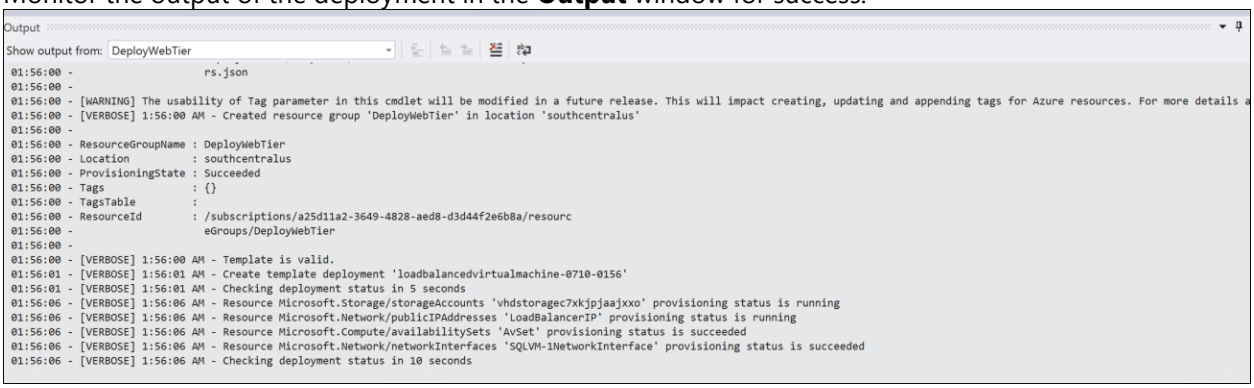
8. Back in the **Deploy to Resource Group** dialog, check to make sure that an **Artifact storage account** is selected. Then, click **Deploy** to begin the deployment.



9. When prompted by the **Edit Parameters** window, enter a **LoadBlancerIPDnsName**. Make sure it is all lower-case, and it has to be unique or the deployment will fail.

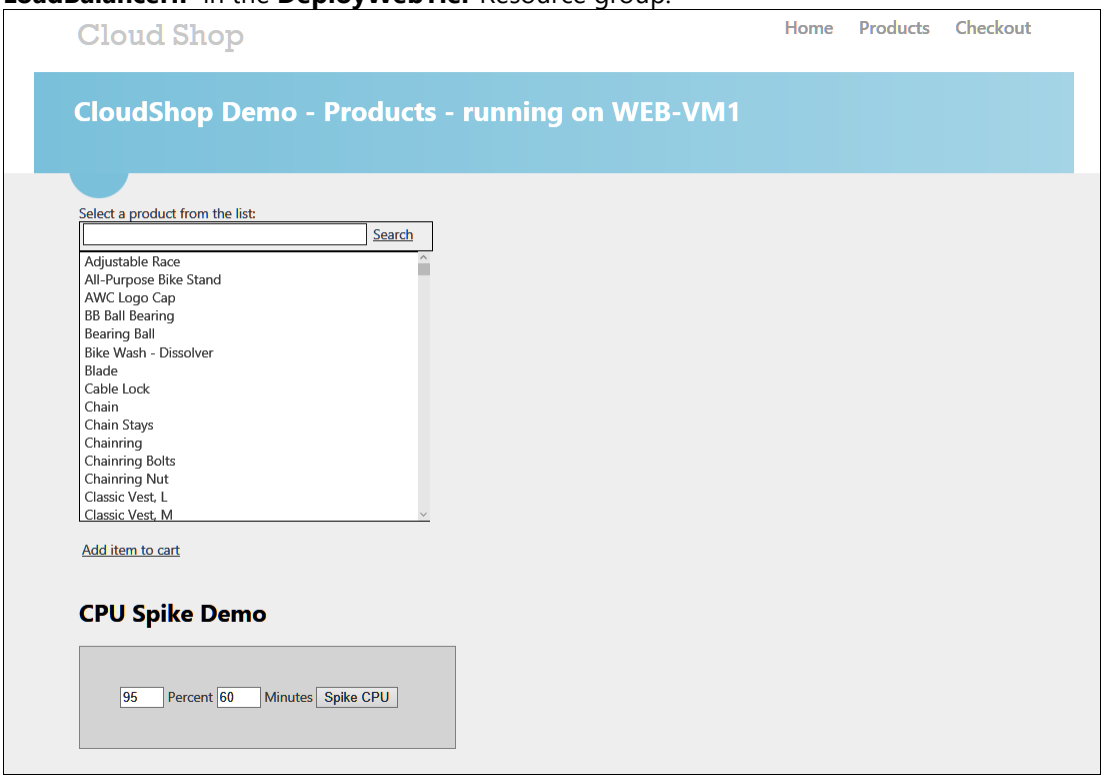


10. Monitor the output of the deployment in the **Output** window for success.



Note: This deployment deploys VMs for SQL Server, Web Servers, a load balancer, configures IIS and SQL among a number of other things. It will take 30-35 minutes to complete, so be patient and allow the script to complete fully so your environment will be ready for the hands-on lab.

11. Once deployment is successful, validate the deployment by browsing to the load balancer Public IP address previously created, and make sure you can see the **CloudShop** Demo Web Application. It will be the **LoadBalancerIP** in the **DeployWebTier** Resource group.



Feel free to log out of the development environment VM and the Azure portal. If need be, deallocate the machines to avoid any unnecessary charges before the hands-on lab.

Summary

In this exercise, you prepared an Azure infrastructure containing several issues needing to be addressed from a resiliency standpoint. You created an Active Directory environment, a SQL Database tier, and a web tier for a Web Application.

You should follow all steps provided *before* attending the Hands-on lab.

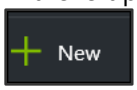
Exercise 1: Prepare the Infrastructure Region 2

Duration: 30 minutes

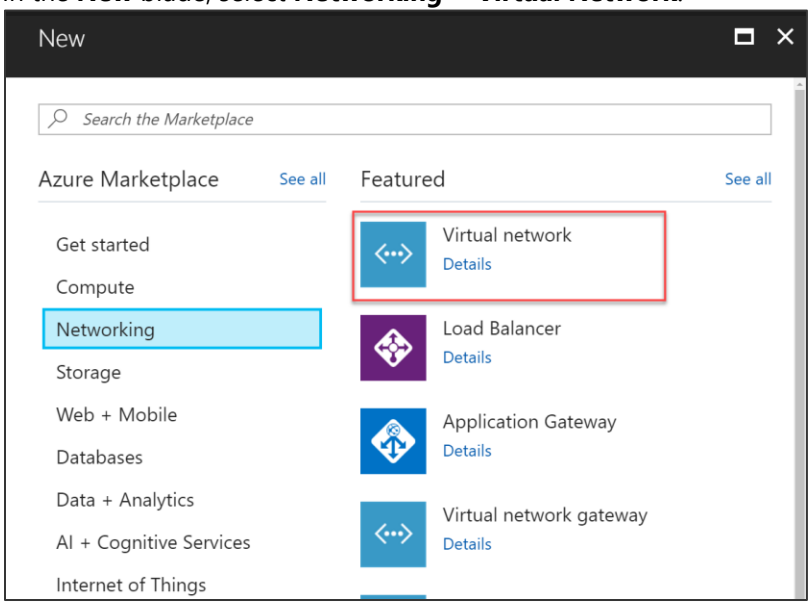
This portion of the lab is designed to help you if you are blocked or have limited experience with Azure Resource Manager. In this exercise, you will design and create IaaS resiliency options for an additional region to provide protection from a regional perspective. You will create a Virtual Network with subnets, a Gateway subnet, a VPN Gateway, and a Regional Backup Vault.

Task 1: Create a Virtual Network for the Azure Infrastructure (Region 2)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. In the left pane, click **+ New**.

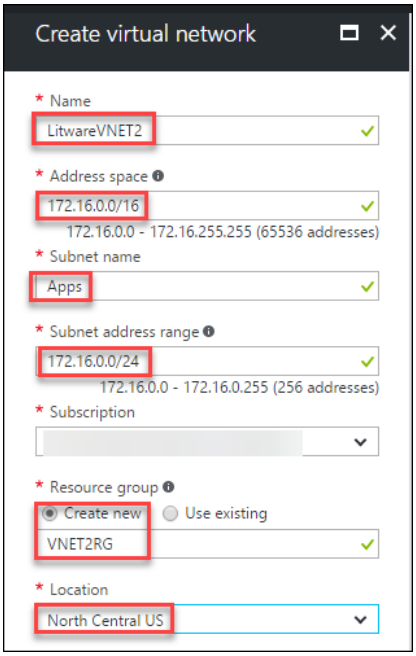


3. In the **New** blade, select **Networking > Virtual Network**.

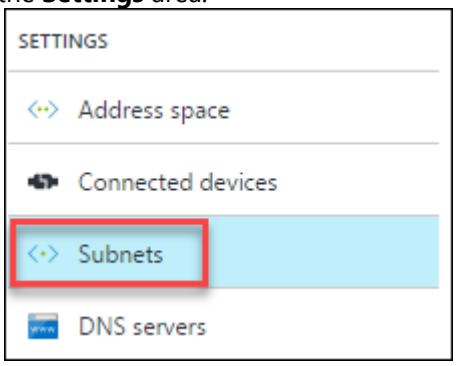


4. For the **Create virtual network** settings, enter the following information:
    a. Name: **LitwareVNET2**
    b. Address space: **172.16.0.0/16**
    c. Subnet name: **Apps**
    d. Subnet address range: **172.16.0.0/24**
    e. Subscription: **Choose your subscription**
    f. Resource group: **Create new – VNET2RG**
    g. Location: **North Central US**
    h. Pin to dashboard: **Check the checkbox**

i. Click the **Create** button to continue.



5. Once the deployment is complete, add two more subnets to the VNET. To do this, select the **Subnets >** icon in the **Settings** area.

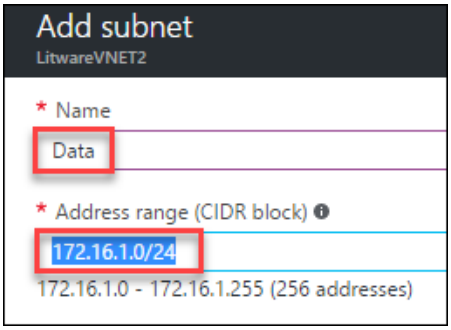


6. Click the **+ Subnet** option, and enter the following settings:

   a. Name: **Data**

   b. Address range (CIDR block): **172.16.1.0/24**

c. Click the **OK** button to add this subnet:

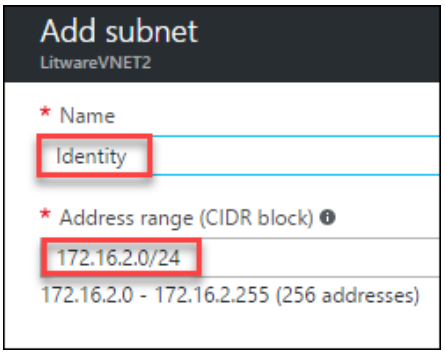


7. Once the subnet is created successfully, repeat the above step for an **Identity** subnet with the following settings:

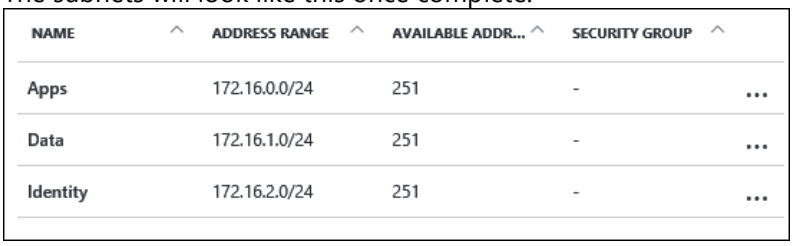
   a. Name: **Identity**

   b. Address range (CIDR block): **172.16.2.0/24**

   c. Click the **OK** button to add this subnet:



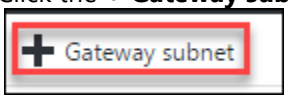
8. The subnets will look like this once complete:



NAME	ADDRESS RANGE	AVAILABLE ADDR...	SECURITY GROUP	
Apps	172.16.0.0/24	251	-	...
Data	172.16.1.0/24	251	-	...
Identity	172.16.2.0/24	251	-	...

Task 2: Add Gateway subnet to the VNET (Region 2)

1. Click the **+ Gateway subnet** icon to add a gateway subnet in preparation for the VPN gateway deployment.



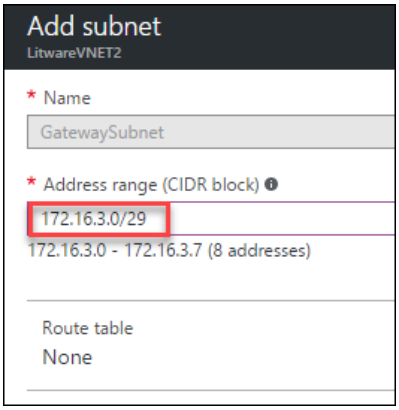
2. In the **Add subnet** blade, configure the following:

   a. Name: **GatewaySubnet (Default)**

   b. Address range (CIDR block): **172.16.3.0/29**

   c. Route table: **None**

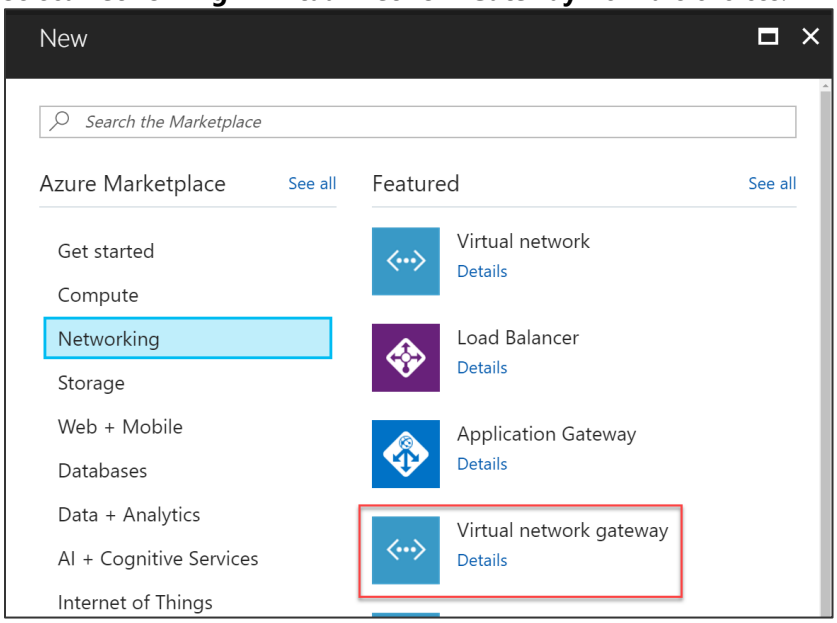
d. Click the **OK** button to add this Gateway.



3. Once complete, you will see four subnets defined for **LitwareVNET2**.

Task 3: Deploy VPN Gateway (Region 2)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.
3. Select **Networking > Virtual Network Gateway** from the choices.

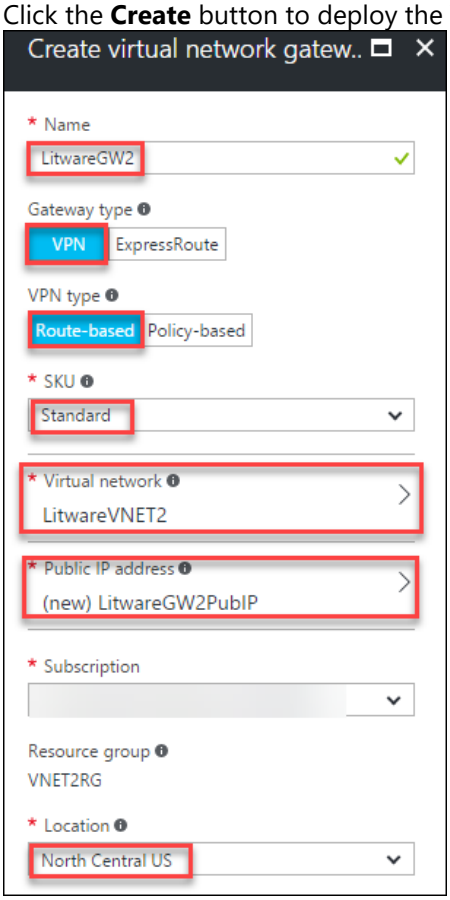


4. In the settings for **Create virtual network gateway**, enter the following:
   a. Name: **LitwareGW2**
   b. Gateway Type: **VPN**
   c. VPN type: **Route-based**
   d. SKU: **Basic**
   e. Virtual network: **LitwareVNET2**
   f. Public IP address: **Choose a Public IP address, + Create new,** name it **LitwareGW2Pubip**
   g. Subscription: **Select your subscription**
   h. Resource group: **VNET2RG (Default)**

i. Location: **North Central US**

j. Pin to dashboard: **Check the checkbox**

k. Click the **Create** button to deploy the VPN Gateway.



Note: This will take up to 45 minutes to deploy, so continue with the following steps while waiting on the deployment to complete.

Task 4: Create a Backup Vault (Region 2)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.
3. In the **Search the marketplace** window, type **Backup and Site Recovery (OMS)** then hit Enter.
4. In the resulting **Everything** blade, choose **Backup and Site Recovery (OMS)**, and then click the **Create** button to continue.

5. In the **Recovery Services vault** configuration blade, enter the following settings:

   a. Name: **LitwareVault2**

   b. Subscription: **Select your subscription**

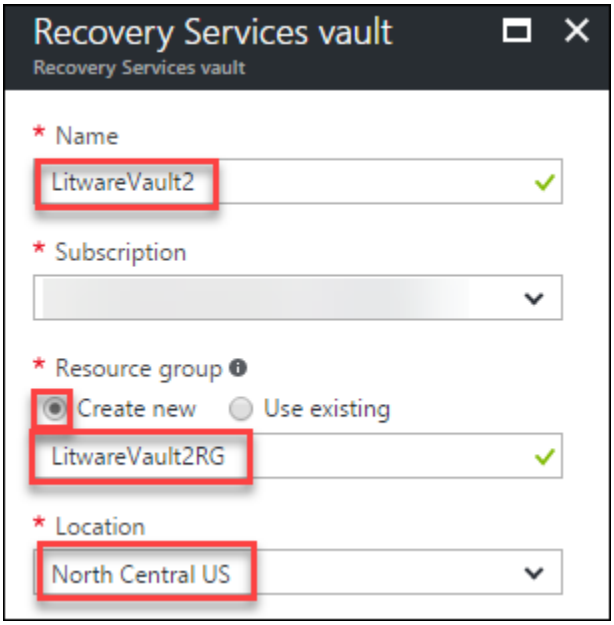
c. Resource group: **Create new – LitwareVault2RG**

d. Location: **North Central US**

Note: This Vault must be created in the same region to be able to see the VMs in the region for backup configuration.

e. Pin to dashboard: **Check the checkbox**

f. Click the **Create** button to continue and create the vault.



Summary

In this exercise, you designed and created IaaS resiliency options for an additional region to provide protection from a regional perspective. You created a Virtual Network with subnets, a Gateway subnet, a VPN Gateway, and a Regional Backup Vault.

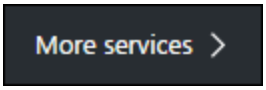
Exercise 2: Resilient Infrastructure Options Region 1

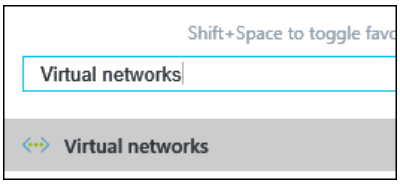
Duration: 45 minutes

In this exercise, you will design and create IaaS resiliency options for the current Azure environment you deployed before the hands-on lab.

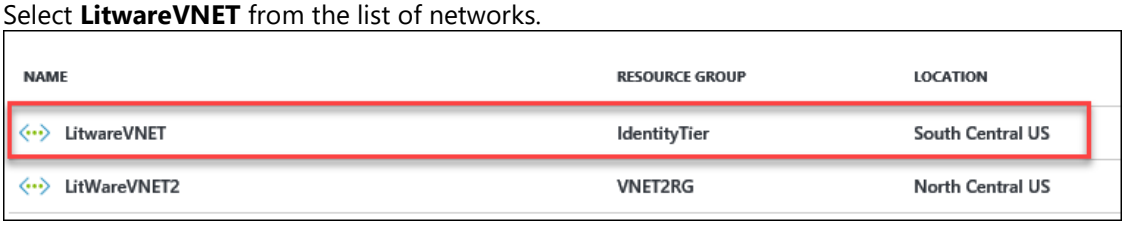
Task 1: Add Gateway subnet to existing VNET (Region 1)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Browse for **Virtual Networks** by clicking the **More Services>** menu item in the left pane and typing **Virtual networks** in the filter.

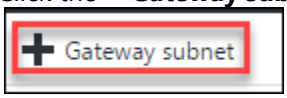




3. Select **LitwareVNET** from the list of networks.

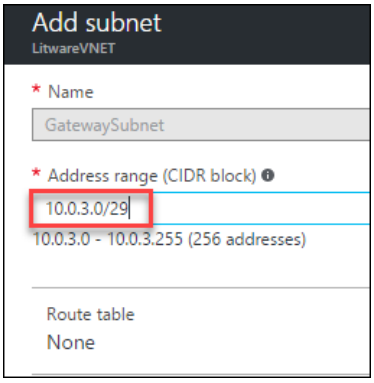


4. Click **Subnets** to display current subnets.
5. Click the **+ Gateway subnet** icon to add a gateway subnet in preparation for the VPN gateway deployment.



6. In the **Add subnet** blade, configure the following:
    a. Name: **GatewaySubnet (Default)**
    b. Address range (CIDR block): **10.0.3.0/29**
    c. Route table: **None**

d. Click the **OK** button to add this subnet:

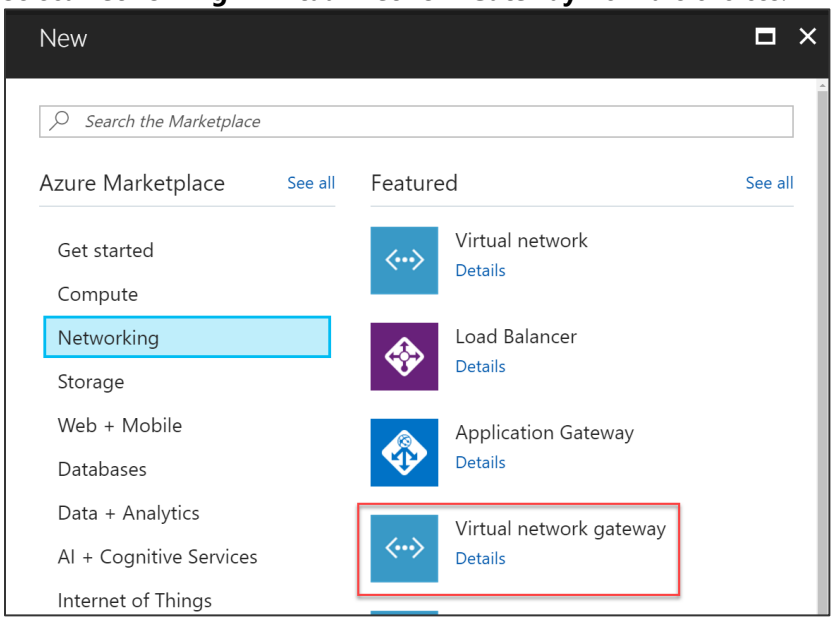


7. Once complete, you will see four subnets defined for **LitwareVNET**.

NAME	ADDRESS RANGE	AVAILABLE ADDR...
Apps	10.0.0.0/24	249
Data	10.0.1.0/24	250
Identity	10.0.2.0/24	250
GatewaySubnet	10.0.3.0/29	3

Task 2: Deploy VPN Gateway (Region 1)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.
3. Select **Networking > Virtual Network Gateway** from the choices.



4. In the settings for **Create virtual network gateway**, enter the following:

   a. Name: **LitwareGW1**

b. Gateway type: **VPN**

c. VPN type: **Route-based**

d. SKU: **Basic**

e. Virtual network: **LitwareVNET**

Note: If you do not see LitwareVNET as an option to choose, make sure you modify the Location to South Central US and come back to find the VNET.

a. Public IP address: **Choose a Public IP address, + Create new,** name it **LitwareGW1pubip**

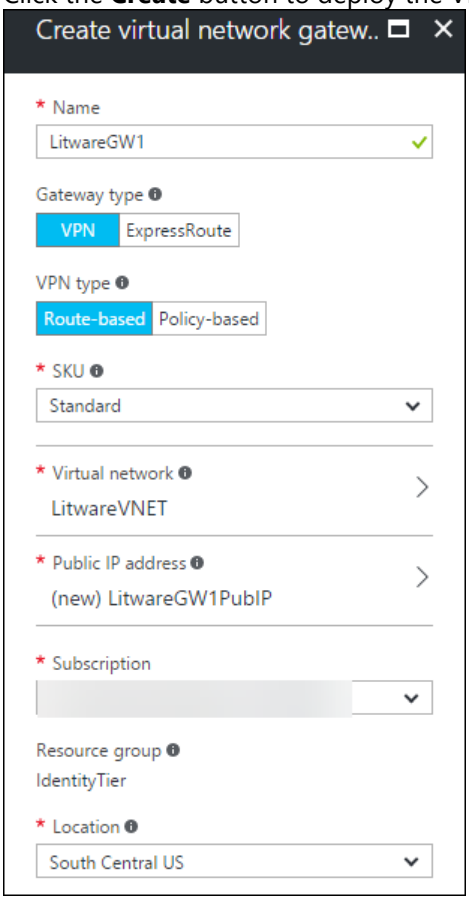
b. Subscription: **Select your subscription**

c. Resource group: **IdentityTier (Default)**

d. Location: **South Central US**

e. Pin to dashboard: **Check the checkbox**

f. Click the **Create** button to deploy the VPN Gateway.



Note: This will take up to 45 minutes to deploy so continue with the following steps while waiting on the deployment to complete.

Task 3: Create a Backup Vault (Region 1)

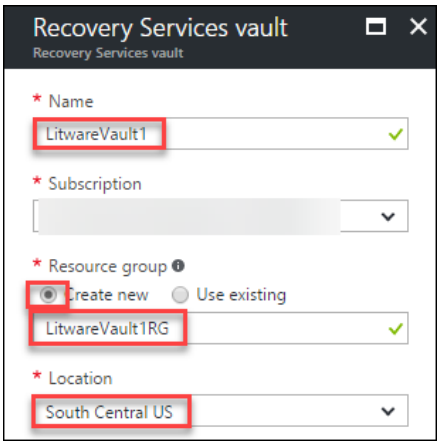
1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.

3. In the **Search the marketplace** window, type **Backup and Site Recovery (OMS)** then hit enter.
4. In the resulting **Everything** blade, choose **Backup and Site Recovery (OMS)**, and then click the **Create** button to continue.

5. In the **Recovery Services vault** configuration blade, enter the following settings:
    a. Name: **LitwareVault1**
    b. Subscription: **Select your subscription**
    c. Resource group: **Create new – LitwareVault1RG**
    d. Location: **South Central US**

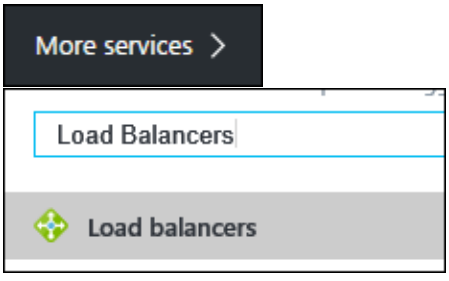
    Note: This Vault must be created in the same region to be able to see the VMs in the region for backup configuration.

    e. Pin to dashboard: **Check the checkbox**
    f. Click the **Create** button to continue and create the vault.



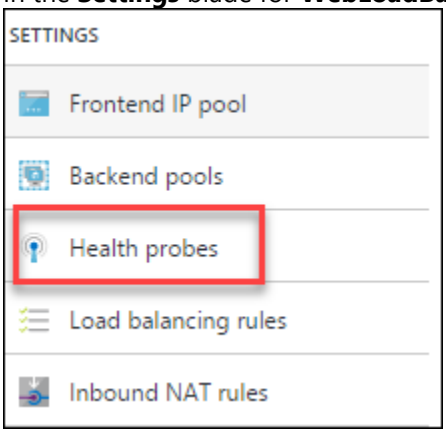
Task 4: Modify load balancer Settings (Region 1)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Browse for **Load balancers** by clicking the **More Services>** menu item in the left pane and typing **Load balancers** in the filter.

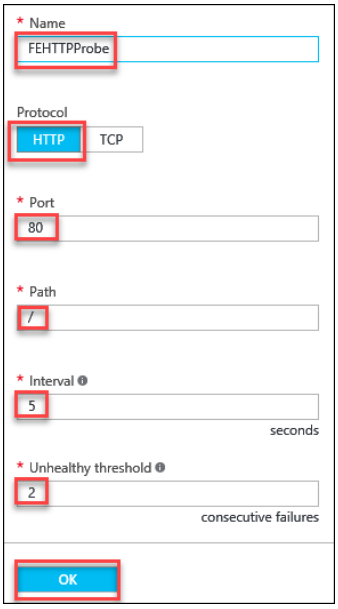


3. Find and click **WebLoadBalancer** to view its configuration.

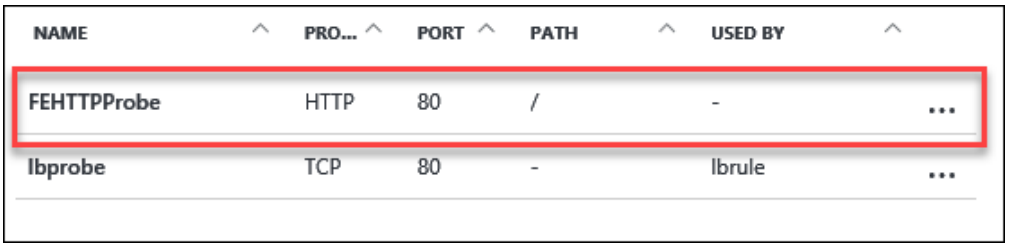
4. In the **Settings** blade for **WebLoadBalancer**, select **Health Probes.**



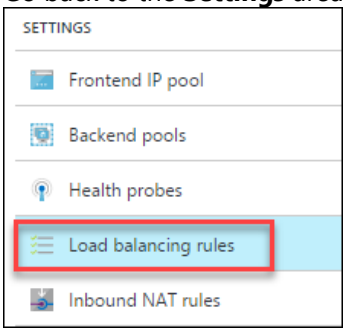
5. Click **+ Add** to add another probe.
6. For the **Add probe** settings, enter the following:
    a. Name: **FEHTTPProbe**
    b. Protocol: **HTTP**
    c. Port: **80**
    d. Path: **/**
    e. Interval: **5**
    f. Unhealthy threshold: **2**
    g. Click the **OK** button to continue.



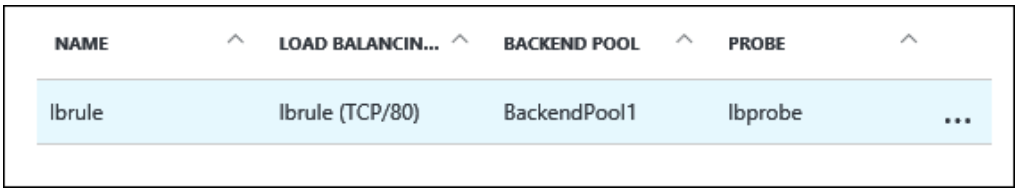
Note: Once the creating probe notification is complete in the portal, continue with the next steps.



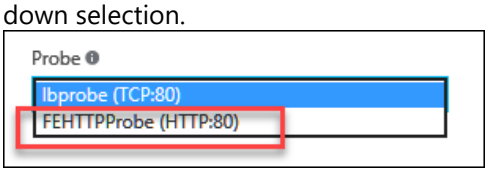
7. Go back to the **Settings** area for the load balancer, and select **Load balancing rules**.



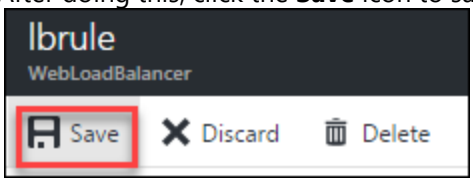
8. Select the **lbrule**.



9. In the settings, change the **Health Probe** from the **lbprobe** to the newly created **FEHTTPProbe** via the drop-down selection.

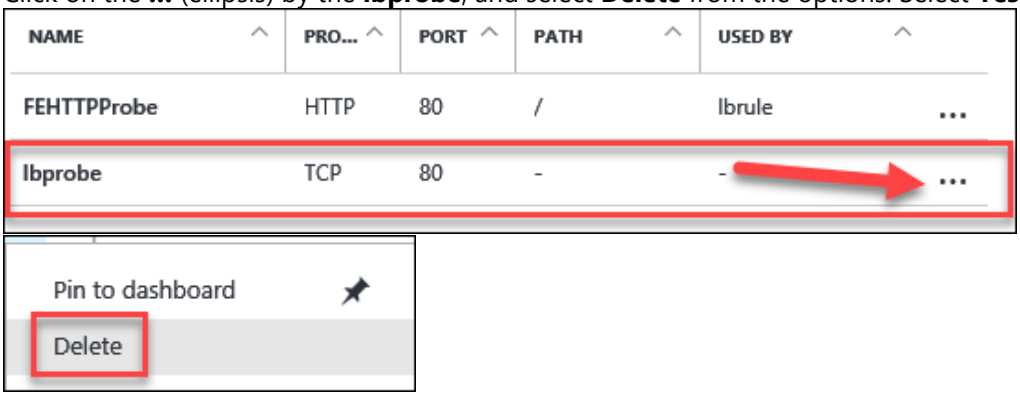


10. After doing this, click the **Save** icon to save the changes.

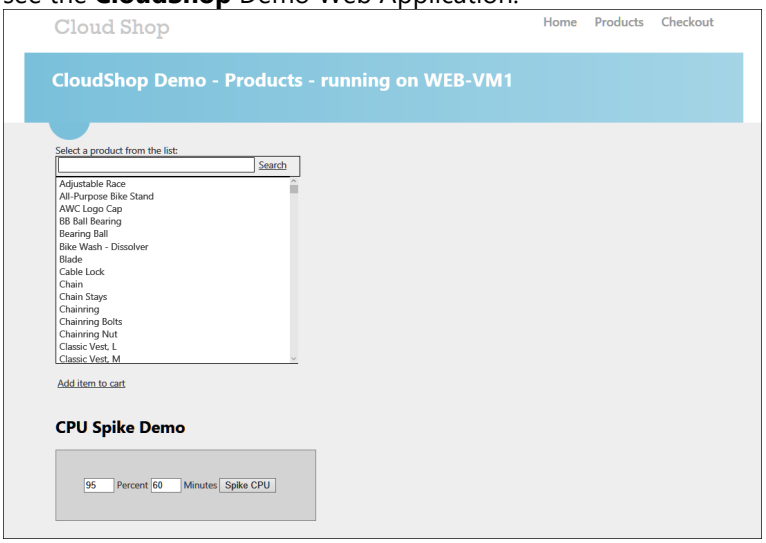


11. Once the Azure Notification for **Saved load balancer rule** appears, go back to the **Overview** blade for the load balancer, and select **Health Probes.**

12. Click on the **...** (ellipsis) by the **lbprobe**, and select **Delete** from the options. Select **Yes** to confirm the deletion.



13. Validate the load balancer is working by browsing to the load balancer Public IP address and make sure you can see the **CloudShop** Demo Web Application.



Summary

In this exercise, you designed and created IaaS resiliency options for the current Azure environment you deployed before the hands-on lab.

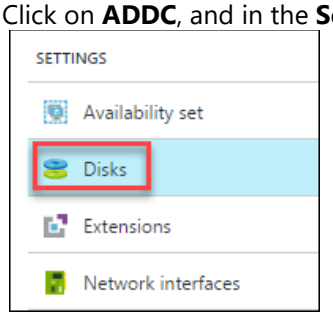
Exercise 3: Build the DCs in for resiliency

Duration: 30 minutes

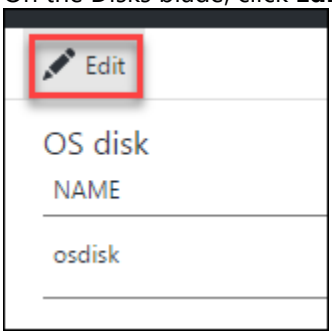
In this exercise, you will design and create IaaS resiliency options in the additional region. You will create multiple Active Directory Domain controllers using Managed Disks, add non-cached Managed data disks to house the Active Directory files, build a connection between VPN gateways, configure DNS settings across regions, and promote redundant domain controllers into the domain.

Task 1: Create Resilient Active Directory Deployment (Region 1)

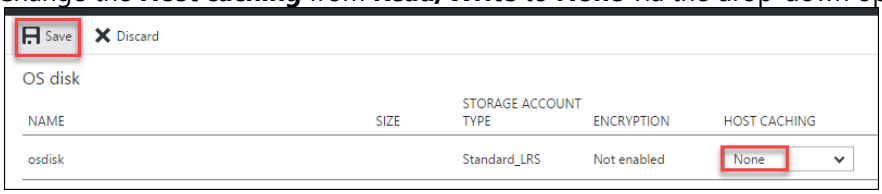
1. Convert the OS disk on ADDC to "Read Only" to avoid corruption of AD Data. To do this, perform the followings steps:
2. Select **Virtual machines** in the left menu pane of the Azure portal.
3. Click on **ADDC**, and in the **Settings** area, select **Disks**.



4. On the Disks blade, click **Edit**.

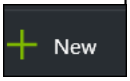


5. Change the **Host caching** from **Read/Write** to **None** via the drop-down option, and click the **Save** icon.

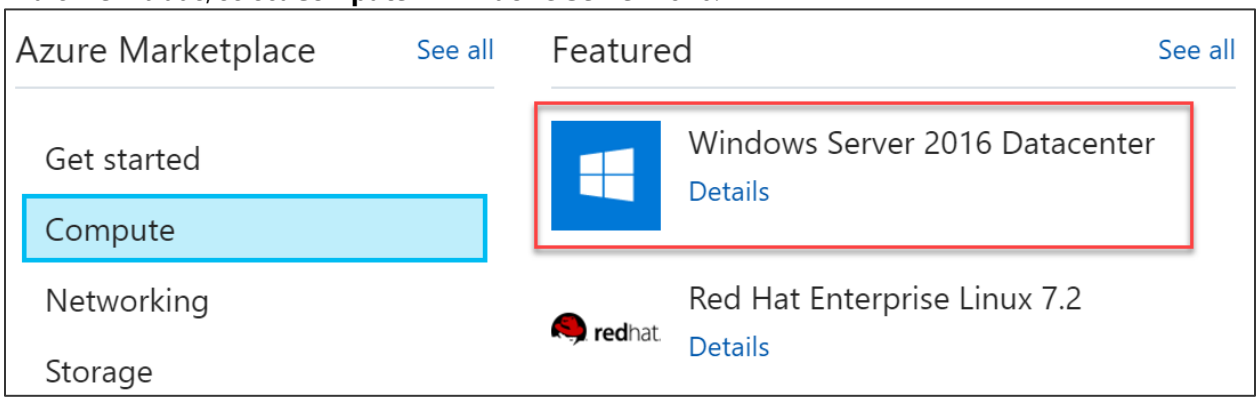


Note: In production, we would not want to have any OS drives that do not have read/write cache enabled. This machine will be decommissioned, but first, we want to make sure the AD Database and SYSVOL will not be corrupted during our updates.

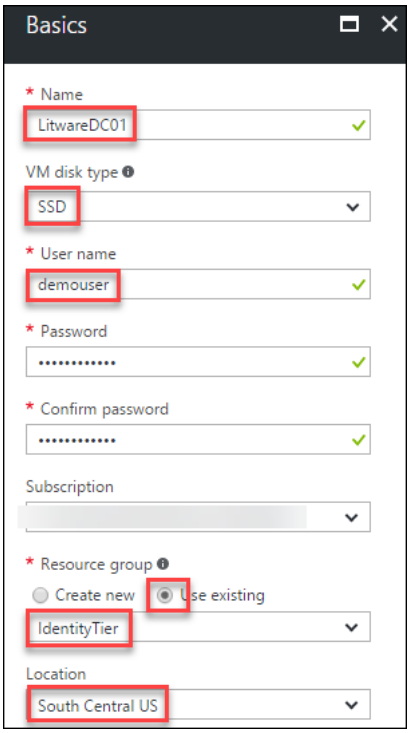
6. In the left pane, click **+ New**.



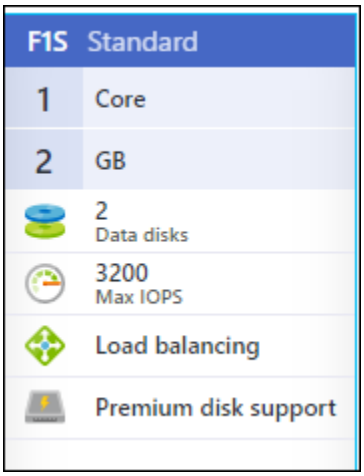
7. In the **New** blade, select **Compute > Windows Server 2016**.



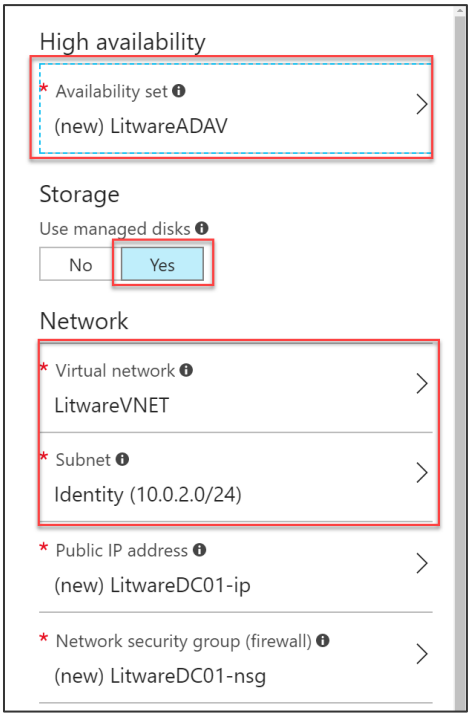
8. In the **Create virtual machine** blade, enter the **Basics** information:
   a. Name: **LitwareDC01**
   b. VM disk type**: SSD**
   c. Username: **demouser**
   d. Password: **demo@pass123**
   e. Confirm password: **demo@pass123**
   f. Subscription: **Select your subscription**
   g. Resource group: **Use existing – IdentityTier**
   h. Location: **South Central US**
   i. Click the **OK** button to continue.



9. For the **Size**, select **F1S Standard**. You may have to select the **View All** option if it is not one of the recommended sizes.



10. In the **Settings** options, choose the following configuration:
    a. Storage Use Managed Disks: **Yes**
    b. Virtual Network: **Click the name to choose LitwareVNET**
    c. Subnet: **Choose Identity as the subnet**
    d. Availability set: **Create new, LitwareADAV**
    e. Leave all other settings: **Default**
    f. Then, click the **OK** button to continue to the **Summary**.



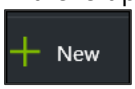
There will be a final validation and when this is passed, click the **Create** button to complete the deployment.

11. Give the deployment a few minutes to build the Availability Set resource. Then, repeat those steps to create LitwareDC02, as that will be another Domain Controller making sure to place it in the **LitwareADAV** availability set.

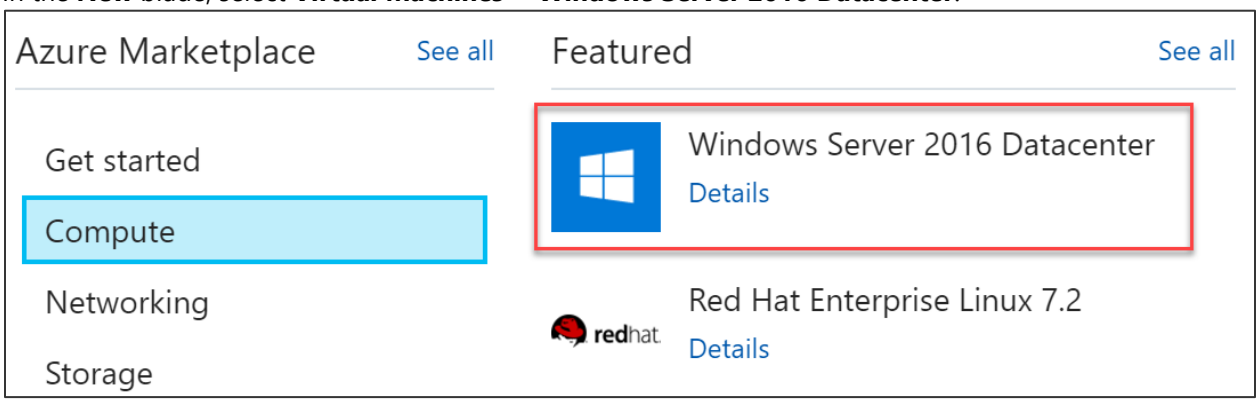
Task 2: Create the Active Directory Deployment (Region 2)

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.

2. In the left pane, click **+ New**.

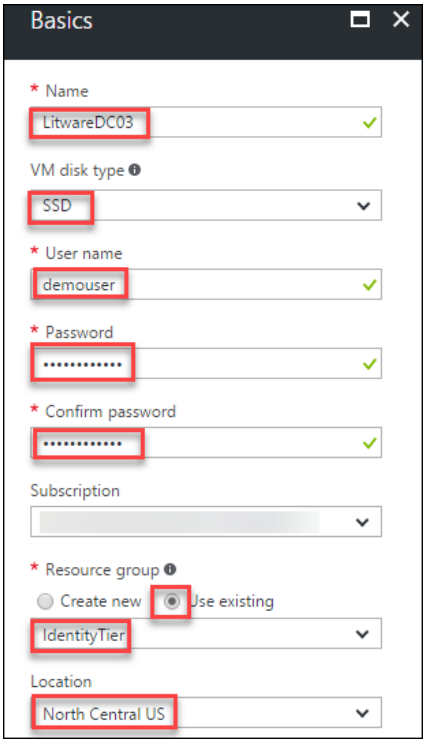


3. In the **New** blade, select **Virtual Machines > Windows Server 2016 Datacenter**.



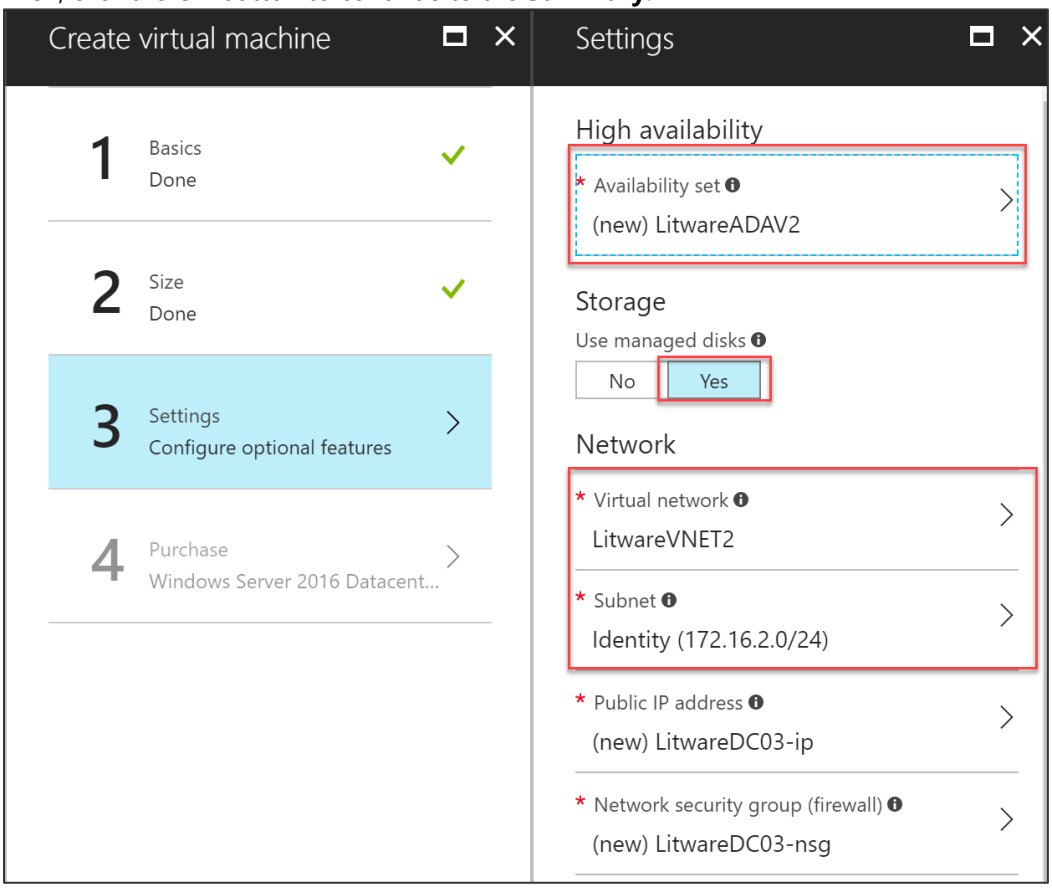
4. In the **Create virtual machine** blade, enter the **Basics** information:
    a. Name: **LitwareDC03**
    b. VM disk type**: SSD**
    c. Username: **demouser**
    d. Password: **demo@pass123**
    e. Confirm password: **demo@pass123**
    f. Subscription: **Select your subscription**
    g. Resource group: **Use existing – IdentityTier**
    h. Location: **North Central US**

i. Click the **OK** button to continue.



5. For the **Size**, select **F1S Standard**. You may have to select the **View All** option if it is not one of the recommended sizes.
6. Click the **Select** button to continue to **Settings**.
7. In the **Settings** options, choose the following configuration:
    a. Storage Use Managed Disks: **Yes**
    b. Virtual Network: **Click the name to choose LitwareVNET2**
    c. Subnet: **Choose Identity as the subnet**
    d. Availability set: **Create new, LitwareADAV2**
    e. Leave all other settings: **Default**

f. Then, click the **OK** button to continue to the **Summary**.

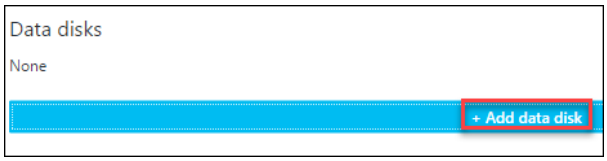


8. There will be a final validation. When this is passed, click the **Create** button to complete the deployment.

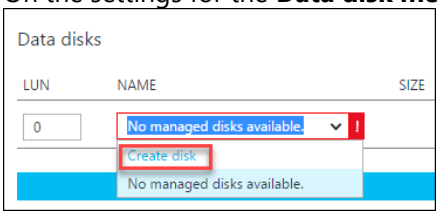
9. Give the deployment a few minutes to build the Availability Set resource. Repeat Steps 2-9 again to create **LitwareDC04** making sure to place it in the **LitwareADAV2** availability set.

Task 3: Add data disks to Active Directory domain controllers (both regions)

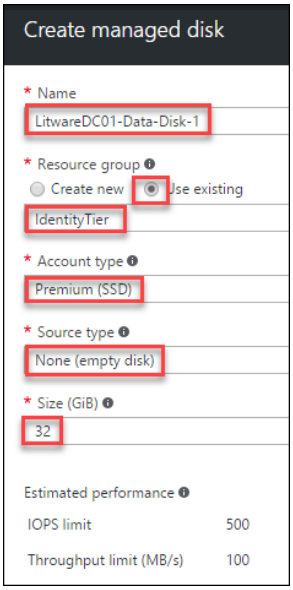
1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click on **LitwareDC01** on the Azure dashboard.
3. In the **Settings** blade, select **Disks.**
4. Click on **Add data disk** icon in the menu bar.



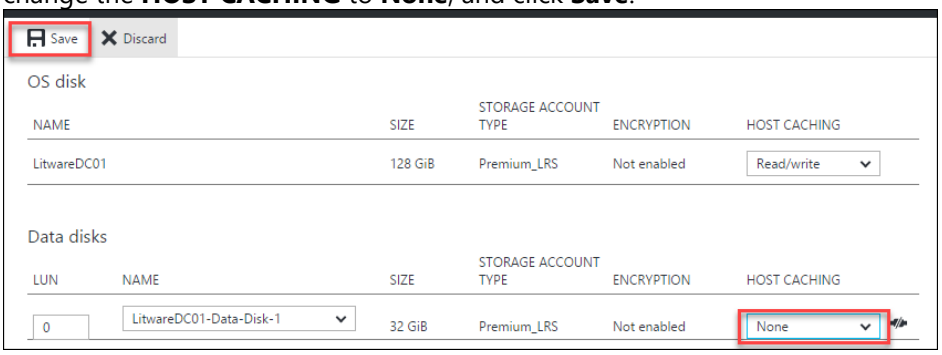
5. On the settings for the **Data disk menu**, click on the drop-down menu under **Name**, and click **Create Disk**.



6. On the Create managed disk blade, enter the following, and click **Create**.
   a. Name: **LitwareDC01-Data-Disk-1**
   b. Resource group: **Use existing / Identity Tier**
   c. Account Type: **Premium (SSD)**
   d. Source Type: **None (empty disk)**
   e. Size: **32**



7. Once the disk is created, the portal will move back to the **Disks** blade. Locate the new disk under **Data Disks**, change the **HOST CACHING** to **None**, and click **Save**.



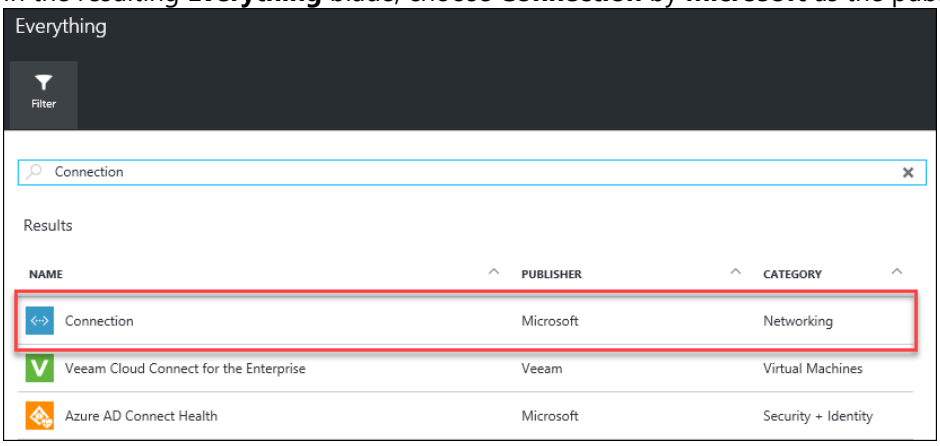
8. Perform these same steps for **LitwareDC02** naming the disk **LitwareDC02-Data-Disk-1**. Also, make sure the Host caching is set to **None**.

9. Perform Steps 1-4 for **LitwareDC03** and **LitwareDC04** naming the disks **LitwareDC03-Data-Disk-1** and **LitwareDC04-Data-Disk1** respectively. Make sure to set the Host caching to **None**.

Task 4: Build a connection between the VPN Gateways

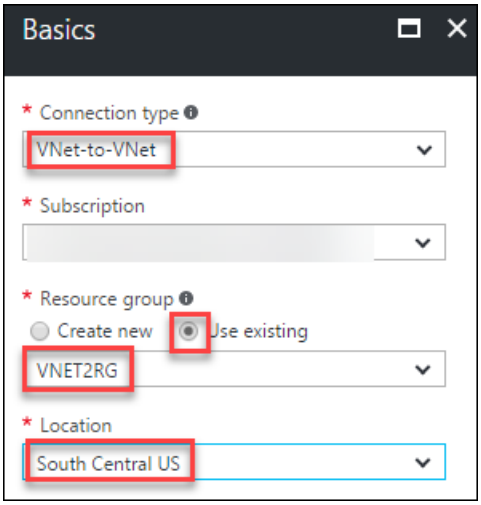
Note: Both VPN Gateways must have successfully deployed before completing this step. The hands-on lab was designed to provide ample time for them to complete while doing other deployments, but make sure to check before completing the following task.

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.
3. In the **Search the marketplace** window, type **Connection**, and hit Enter.
4. In the resulting **Everything** blade, choose **Connection** by **Microsoft** as the publisher.



5. Click the **Create** button to continue.
6. In the **Create connection** settings for **Basics**, enter the following:
    a. Connection type: **VNet-to-VNet**
    b. Subscription: **Choose your subscription**
    c. Resource Group: **Use existing – VNET2RG**
    d. Location: **South Central US**

e. Click the **OK** button to continue to **Settings**.



7. In the **Settings** blade, choose the following options:

   a. First virtual network gateway: **LitwareGW1**

   b. Second virtual network gateway: **LitwareGW2**

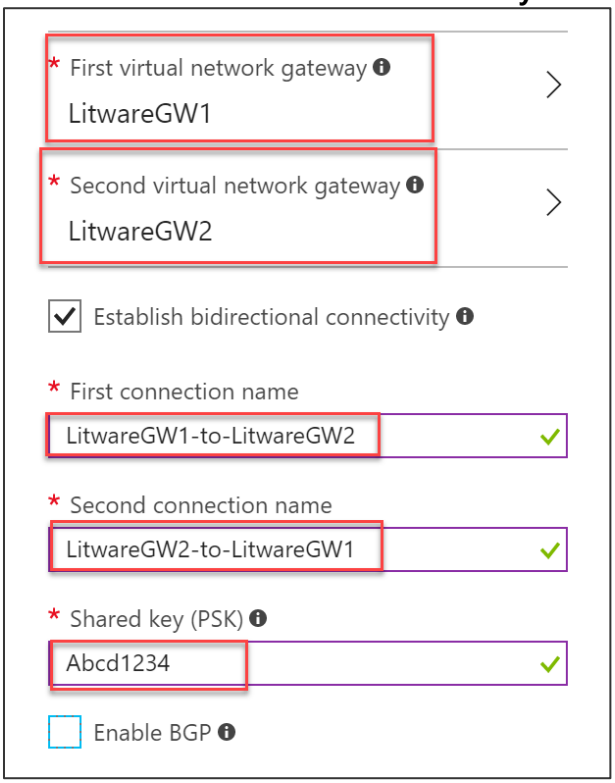
   c. Establish bidirectional connectivity: **Leave the checkbox selected**

   d. First connection name: **Default**

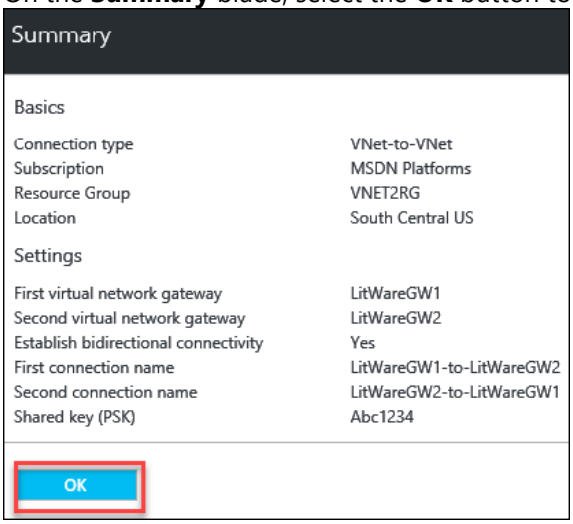
   e. Second connection name: **Default**

   f. Shared key: **Abcd1234**

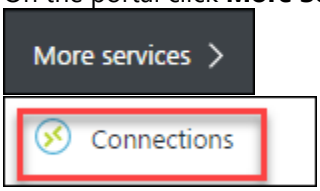
   g. Click the **OK** button to continue to **Summary**.



8. On the **Summary** blade, select the **OK** button to create the connection.



9. On the portal click **More Services >** and type **Connections**.

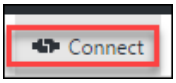


10. Wait until the **Connections** show the status of **Connected** before continuing to the next task. You might have to hit Refresh a few times until it comes completely online.

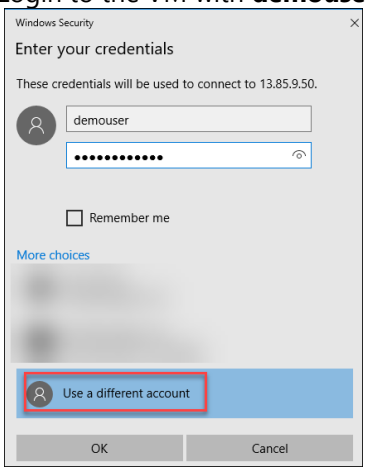
Note: This may take 10-15 minutes. If you want, you can format the data disks in the next task while waiting to help conserve time. Just be sure to not set the DNS settings until a connection is established between VPN Gateways.

Task 5: Format data disks on DCs and configure DNS settings across connection

1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click on **LitwareDC01** on the Azure dashboard.
3. Click the **Connect** icon on the menu bar to RDP into the server.

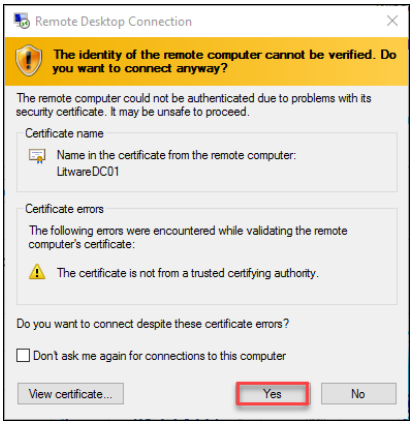


4. Login to the VM with **demouser** and password created during deployment.

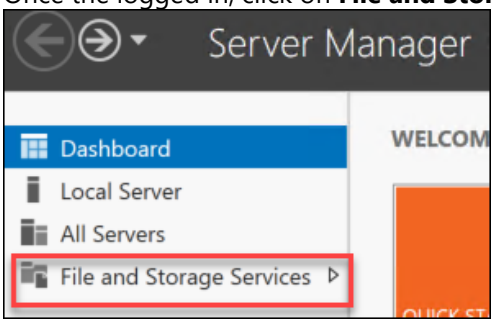


Note: You might have to click "Use a different account," depending on which OS you are connecting from to put in the demouser credentials.

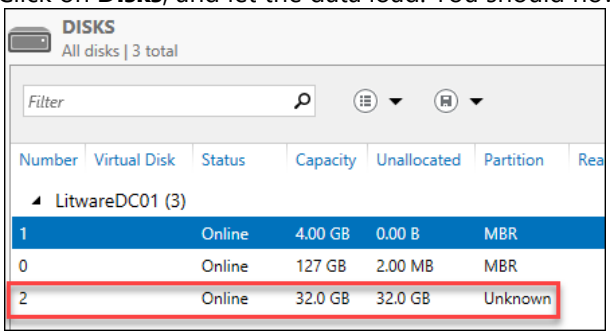
5. Click **Yes** to continue to connect to LitwareDC01.



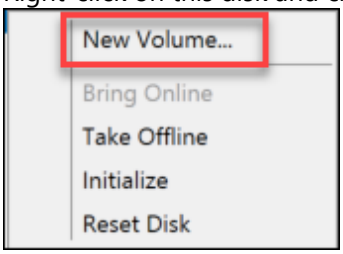
6. Once the logged in, click on **File and Storage Services** in **Server Manager**.



7. Click on **Disks**, and let the data load. You should now see an **Unknown** partition disk in the list.



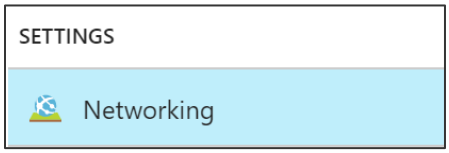
8. Right-click on this disk and choose **New Volume...** from the context menu options.



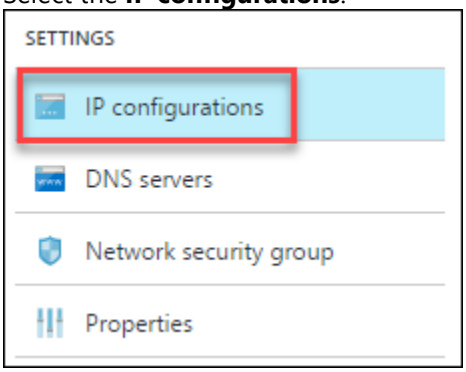
9. Follow the prompts in the **New Volume Wizard** to format this disk, as the **F:** drive for the domain controller.

10. Perform these same steps for the remaining 3 DCs (**LitwareDC02**, **LitwareDC03**, and **LitwareDC04**).

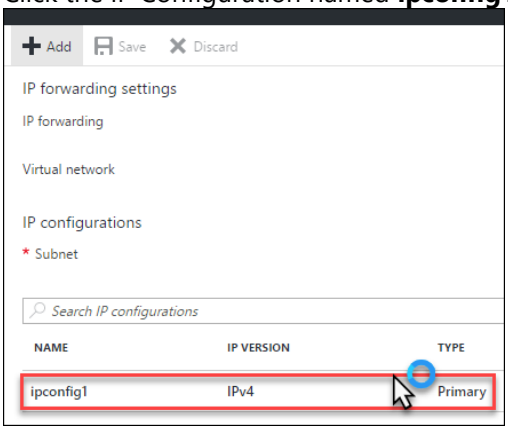
11. Go back to the Azure portal dashboard, and click on **LitwareDC01**. Next, click on **Networking** followed by the name of the NIC.



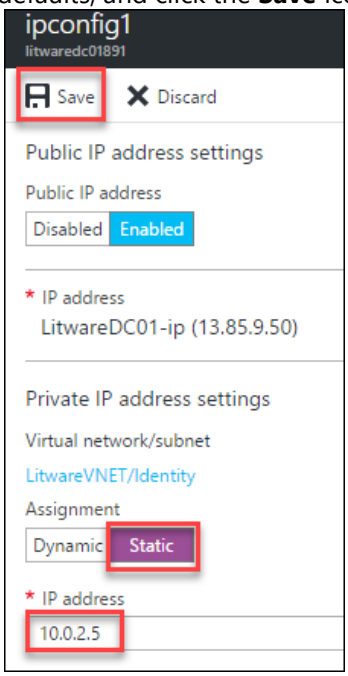
12. Select the **IP configurations**.



13. Click the IP Configuration named **ipconfig1**.



14. On the **ipconfig1** blade, change the **Private IP address settings** to **Static.** Leave all the other settings at their defaults, and click the **Save** icon.



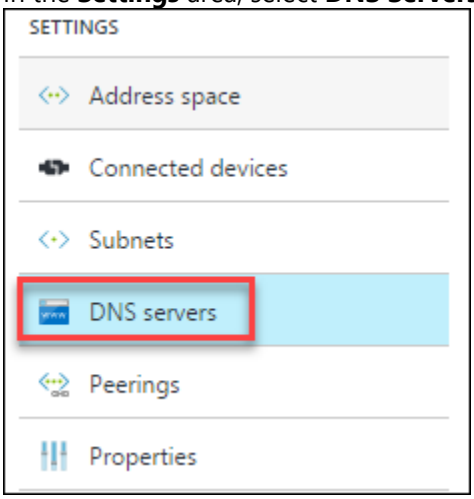
15. Once Azure notifies the network interface change is saved, repeat these steps on the remaining 3 DCs (**LitwareDC02**, **LitwareDC03**, and **LitwareDC04**).

    Note: Static IP for LitwareDC02 should be 10.0.2.6. LitwareDC03 should be 172.16.2.4 and LitwareDC04 should be 172.16.2.5.

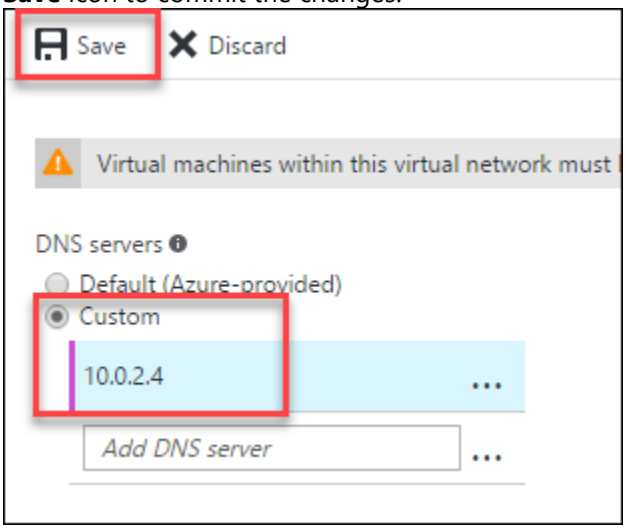
16. By this time, the Gateways should show **Connected**.

17. In the Azure portal, click **More Services >** and in the filter, type in **Virtual Networks**. Select **LitwareVNET2** from the list.

18. In the **Settings** area, select **DNS Servers**.



19. Change **DNS servers** to **Custom**, and provide the address of **10.0.2.4** in the **Primary DNS server** box. Click the **Save** icon to commit the changes.



20. At this point, restart **LitwareDC03** and **LitwareDC04**, so they can get their new DNS Settings.

    Note: LitwareDC01 and LitwareDC02 received the correct DNS settings from the VNET DNS configured prior to their deployment, as the Customer DNS was set before the hands-on lab for that VNET. LitwareDC03 and LitwareDC04 must be rebooted to receive the updated DNS settings from their virtual network.

21. While these two DCs are rebooting, RDP into **ADDC**, and run the following PowerShell command:

```
Set-DnsServerPrimaryZone -Name Litware.com -DynamicUpdate NonsecureAndSecure
```

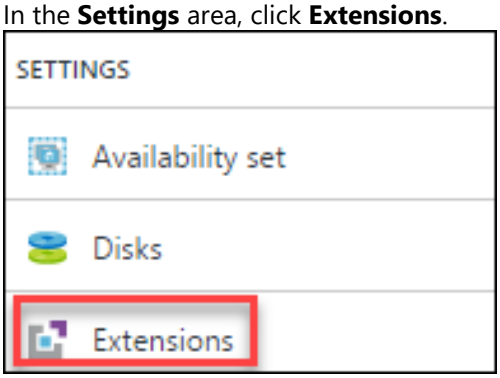
    Note: This would not be done in a production environment, but for purposes of our hands-on lab, we need to perform this step for the SQL Cluster in the coming tasks.

22. After the PowerShell command runs, Sign Out of **ADDC**.

Task 6: Promote DCs as additional domain controllers (both regions)

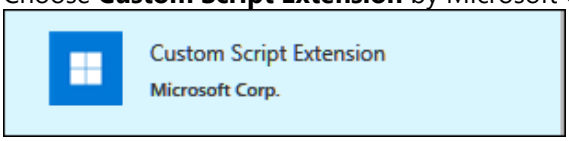
1. Login to **LABVM** created before the hands-on lab or the machine where you have downloaded the exercise files.

2. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
3. Click on **LitwareDC01** on the Azure dashboard.
4. In the **Settings** area, click **Extensions**.

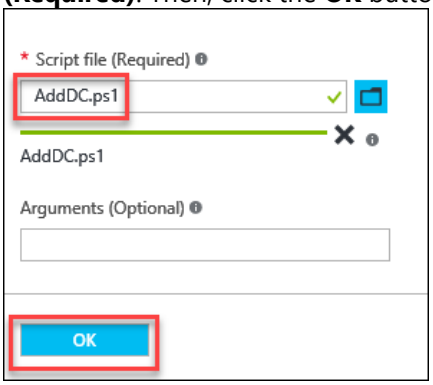


5. Click the **+ Add** icon.

6. Choose **Custom Script Extension** by Microsoft Corp., and click the **Create** button to continue.

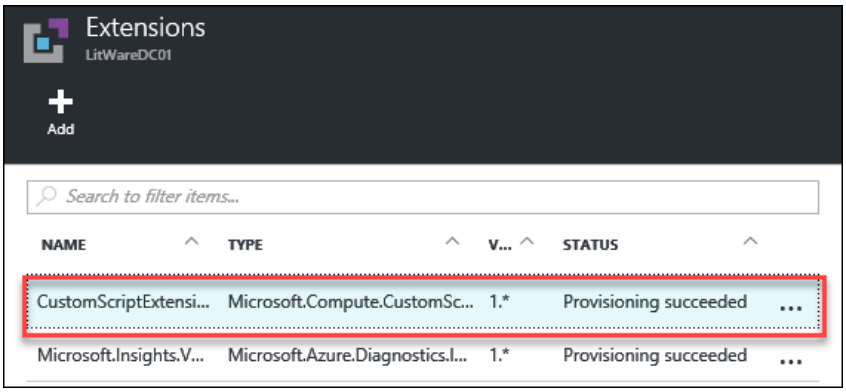


7. Browse to the **C:\Hackathon** folder, and select the **AddDC.ps1** script by clicking the folder icon for **Script file (Required)**. Then, click the **OK** button to continue.



8. This script will run the commands to add this DC to the domain as an additional DC in the Litware.com domain. Repeat these steps for **LitwareDC02**, **LitwareDC03**, and **LitwareDC04**.

9. Once this succeeds, you will see a **Provisioning succeeded** message under **Extensions** for all four domain controllers.



Note: While this a live production environment, there would need to be some additional steps to clean up Region 1 and to configure DNS, Sites and Services, Subnets, etc. Please refer to documentation on running Active Directory Virtualized or in Azure for details. ADDC should be demoted gracefully, and if required, a new DC can be added to the ADAVSet and data disk attached for F:\.

Summary

In this exercise, you designed and created IaaS resiliency options in the additional region. You created multiple Active Directory Domain controllers, added non-cached data disks to house the Active Directory files, built a connection between VPN gateways, configured DNS settings across regions, and promoted redundant domain controllers into the domain.

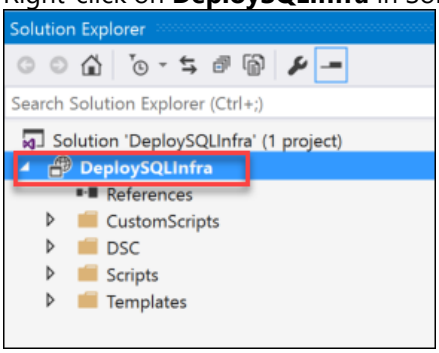
Exercise 4: Build web tier and SQL for resiliency

Duration: 60 minutes

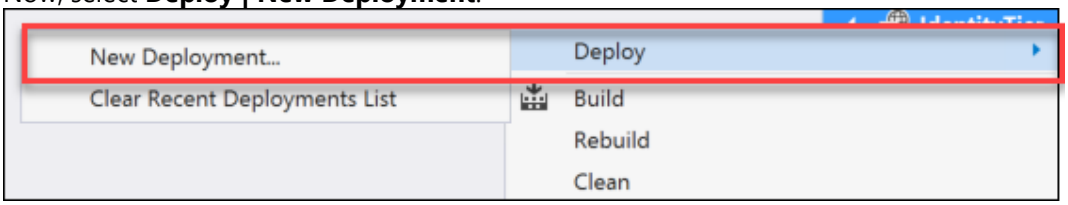
In this exercise, you will design and create IaaS resiliency options in the additional region. You will deploy resilient Web Servers, an additional load balancer, and a SQL Always-On Cluster for Database resiliency.

Task 1: Deploy SQL Always-On Cluster (Region 1)

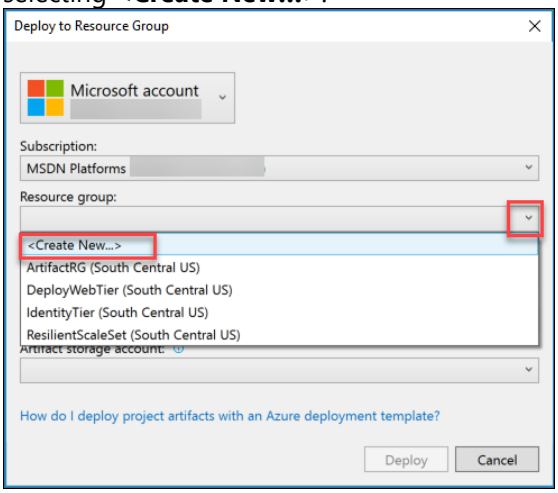
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution**, and browse to the files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SQL** folder, and select the Visual Studio Solution file: **DeploySQLInfra.sln**.
4. Right-click on **DeploySQLInfra** in Solution Explorer.



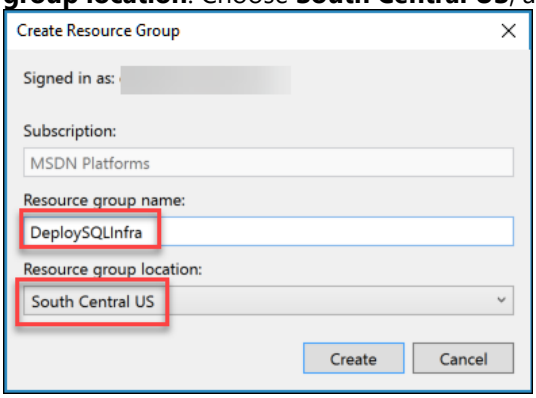
5. Now, select **Deploy | New Deployment**.



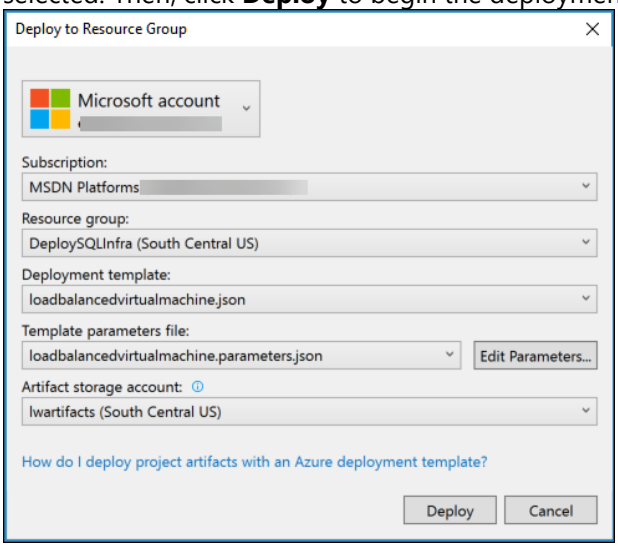
6. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New...>**.



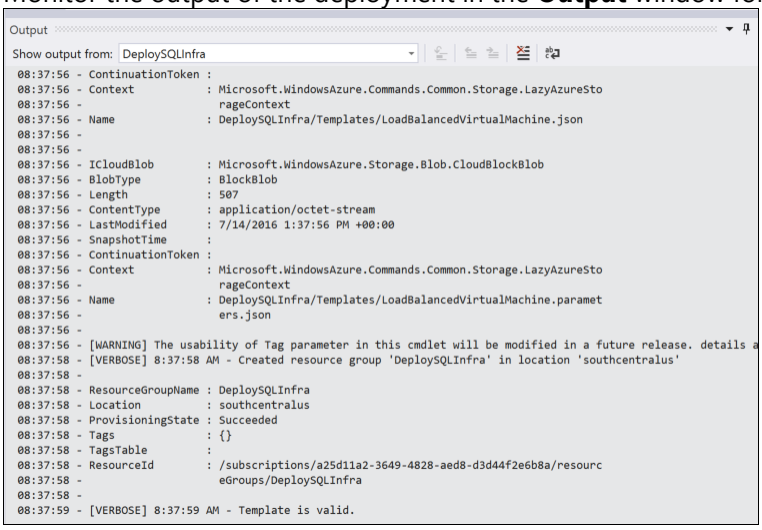
7. In the **Create Resource Group**, enter the **Resource group name** as **DeploySQLInfra**, and choose a **Resource group location**. Choose **South Central US**, and click the **Create** button to continue.



8. Back in the **Deploy to Resource Group** dialog, check to make sure an **Artifact storage account** has been selected. Then, click **Deploy** to begin the deployment.

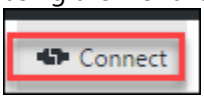


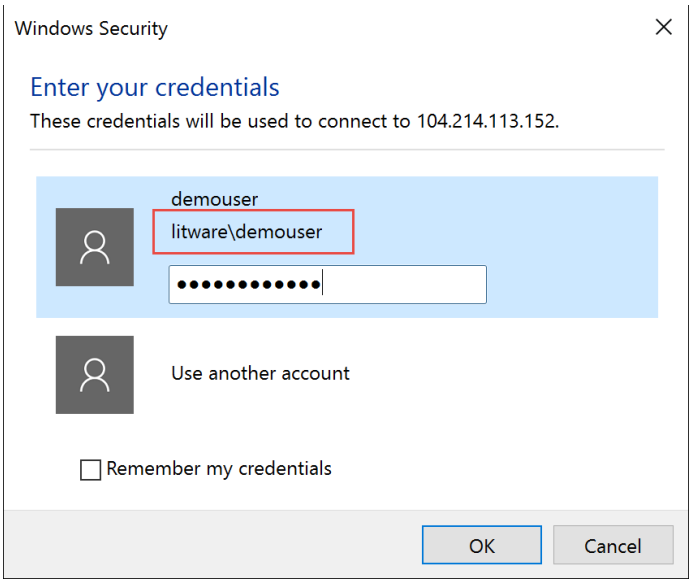
9. Monitor the output of the deployment in the **Output** window for success.



Note: This will take 20-25 minutes to deploy a SQL Always-On Cluster in Region 1. After this is complete, it will be manually configured.

10. Open a remote desktop connection to the **SQLVM-1** virtual machine you created in the previous task, and login using the **Litware\demouser** account.



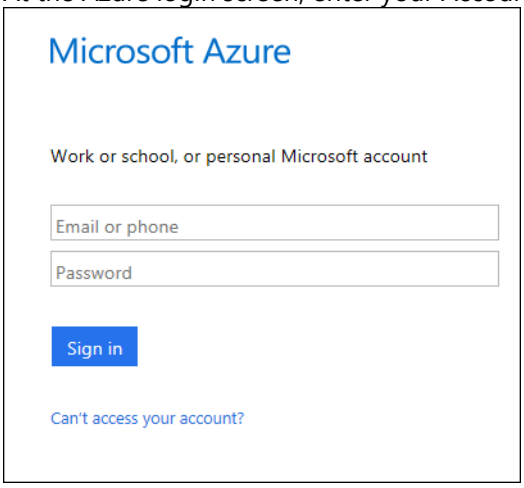


11. Once connected, open the Windows Explorer, check to make sure the F:\ Drive is present, and the Database was restored to the F:\Data directory.
12. Sign out of SQLVM-1.
13. On LABVM open the PowerShell ISE Tool.

    Note: In the next few steps, you will use PowerShell to migrate the disks for the SQL Unfractured to Managed Disks.
14. In the execution pane, login to Azure using the Login-AzureRmAccount, and press Enter.

```
Login-AzureRmAccount
```

15. At the Azure login screen, enter your Account and Password.

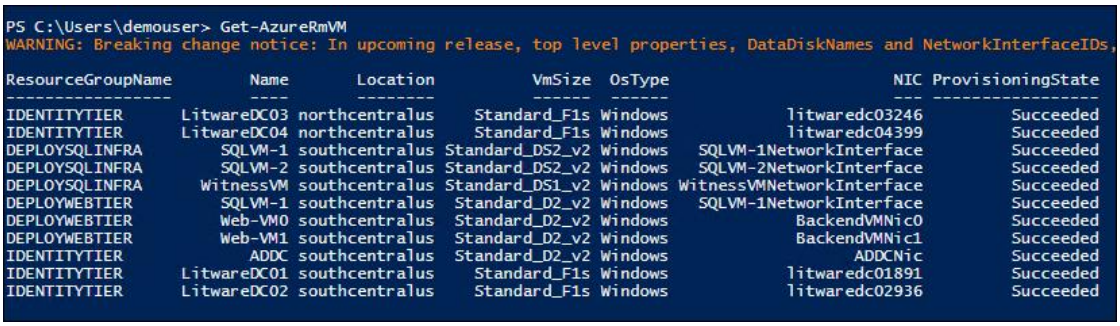


16. Once logged in, make sure to set your subscription that is the default for this hands-on lab.

```
Get-AzureRMSubscription
Select-AzureRmSubscription -SubscriptionName “your subscription name”
```

17. Once this is completed, run the following command to verify your VMs for the hands-on lab are present.

```
Get-AzureRMVm
```



```
PS C:\Users\demouser> Get-AzureRmVM
WARNING: Breaking change notice: In upcoming release, top level properties, DataDiskNames and NetworkInterfaceIDs,

ResourceGroupName        Name       Location          VmSize  OsType                      NIC ProvisioningState
-----------------        ----       --------          ------  ------                      --- -----------------
IDENTITYTIER      LitwareDC03 northcentralus    Standard_F1s Windows           litwaredc03246         Succeeded
IDENTITYTIER      LitwareDC04 northcentralus    Standard_F1s Windows           litwaredc04399         Succeeded
DEPLOYSQLINFRA        SQLVM-1 southcentralus Standard_DS2_v2 Windows   SQLVM-1NetworkInterface         Succeeded
DEPLOYSQLINFRA        SQLVM-2 southcentralus Standard_DS2_v2 Windows   SQLVM-2NetworkInterface         Succeeded
DEPLOYSQLINFRA      WitnessVM southcentralus Standard_DS1_v2 Windows WitnessVMNetworkInterface         Succeeded
DEPLOYWEBTIER         SQLVM-1 southcentralus  Standard_D2_v2 Windows   SQLVM-1NetworkInterface         Succeeded
DEPLOYWEBTIER         Web-VM0 southcentralus  Standard_D2_v2 Windows            BackendVMNic0         Succeeded
DEPLOYWEBTIER         Web-VM1 southcentralus  Standard_D2_v2 Windows            BackendVMNic1         Succeeded
IDENTITYTIER             ADDC southcentralus  Standard_D2_v2 Windows                  ADDCNic         Succeeded
IDENTITYTIER      LitwareDC01 southcentralus    Standard_F1s Windows           litwaredc01891         Succeeded
IDENTITYTIER      LitwareDC02 southcentralus    Standard_F1s Windows           litwaredc02936         Succeeded
```

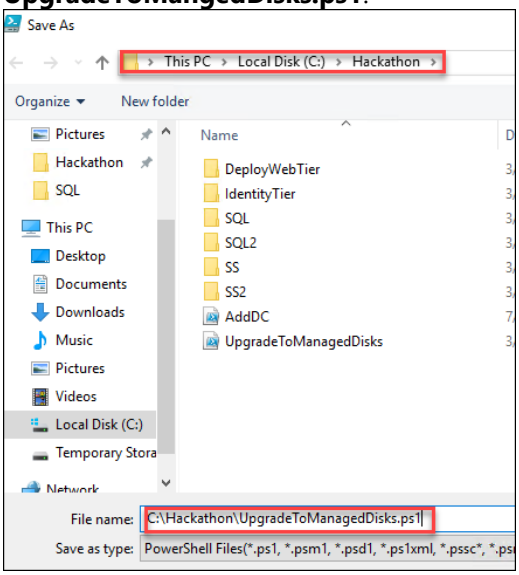
18. Now, move to the scripting pane of the PowerShell ISE tool. Paste this code into the window.

```
$rgName = 'myResourceGroup'

$avSetName = 'myAvailabilitySet'


$avSet =  Get-AzureRmAvailabilitySet -ResourceGroupName $rgName -Name $avSetName


Update-AzureRmAvailabilitySet -AvailabilitySet $avSet -Managed


foreach($vmInfo in $avSet.VirtualMachinesReferences)

    {

   $vm =  Get-AzureRmVM -ResourceGroupName $rgName | Where-Object {$_.Id -eq $vmInfo.id}


   Stop-AzureRmVM -ResourceGroupName $rgName -Name  $vm.Name -Force


   ConvertTo-AzureRmVMManagedDisk -ResourceGroupName $rgName -VMName $vm.Name


    }
```

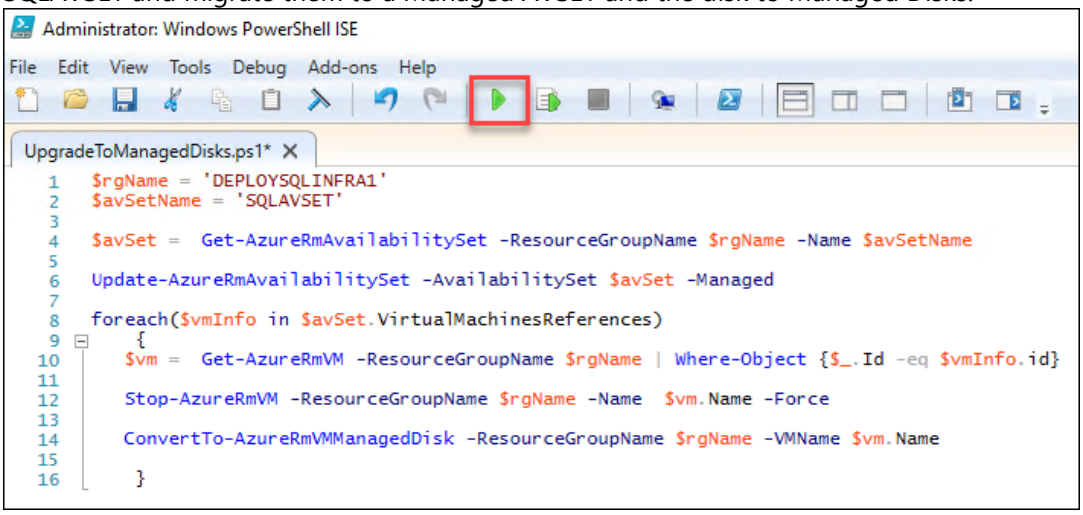
19. Update the variables at the top of the script with the names of the Resource Group and the Availability Set used for the **SQLVM-1**, **SQLVM-2** and **WitnessVM**.

```
$rgName = 'DEPLOYSQLINFRA'

$avSetName = 'SQLAVSET'
```

20. In PowerShell_ISE, click **File > Save**, and in the **C:\Hackathon** directory, name the file **UpgradeToMangedDisks.ps1**.

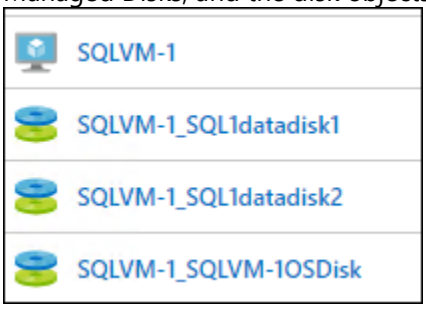


21. Next, click the Play button in PowerShell_ISE. This will deallocate all of the machines in the Availability Set SQLAVSET and migrate them to a Managed AVSET and the disk to Managed Disks.



Note: This process will take about 10-15 minutes to complete and be careful not to stop the process.

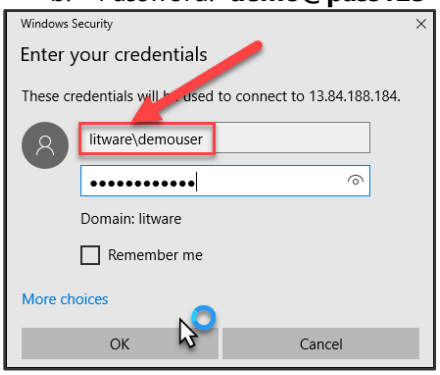
22. Open the Azure portal, and browse to the **DeploySQLInfra** Resource Group. Notice now, the machines are using Managed Disks, and the disk objects now appear.



23. Click on **SQLVM-1**, and press **Connect** to RDP to the Server. Make sure to use the Domain Credentials from now on.

    a. User: **LITWARE\demouser**

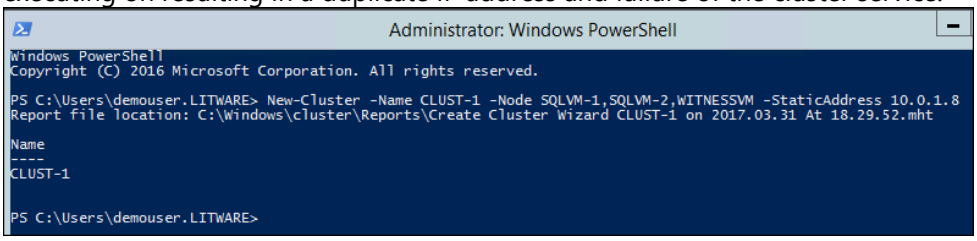
    b. Password: **demo@pass123**



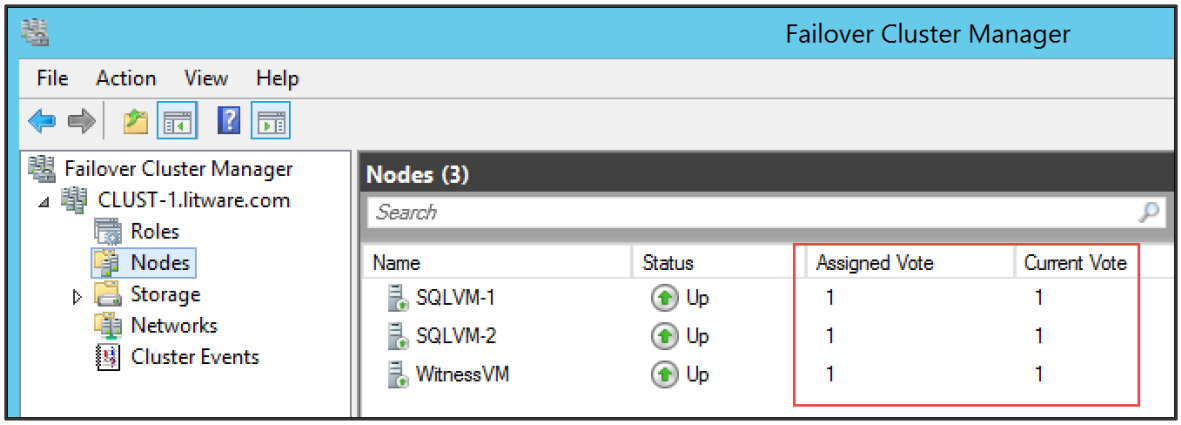
24. Next, run this command from **SQLVM-1** to create a Cluster for the SQL Always-On Group. **Start > PowerShell > Enter**, and execute the following commands:

```
New-Cluster -Name CLUST-1 -Node SQLVM-1,SQLVM-2,WITNESSVM -StaticAddress 10.0.1.8
```

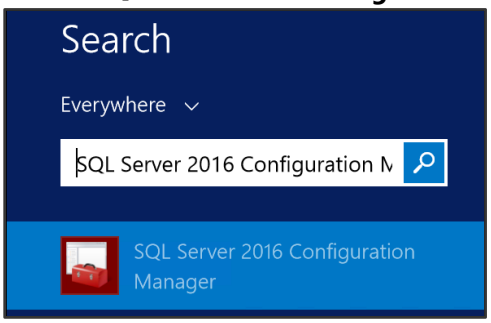
25. This will create a three-node cluster with a static IP address. It is also possible to use a wizard for this task, but the resulting cluster will require additional configuration to set the static IP address to be viable in Azure. This is due to the way Azure DHCP distributes IP addresses causing the cluster to receive the same IP address as the node it is executing on resulting in a duplicate IP address and failure of the cluster service.



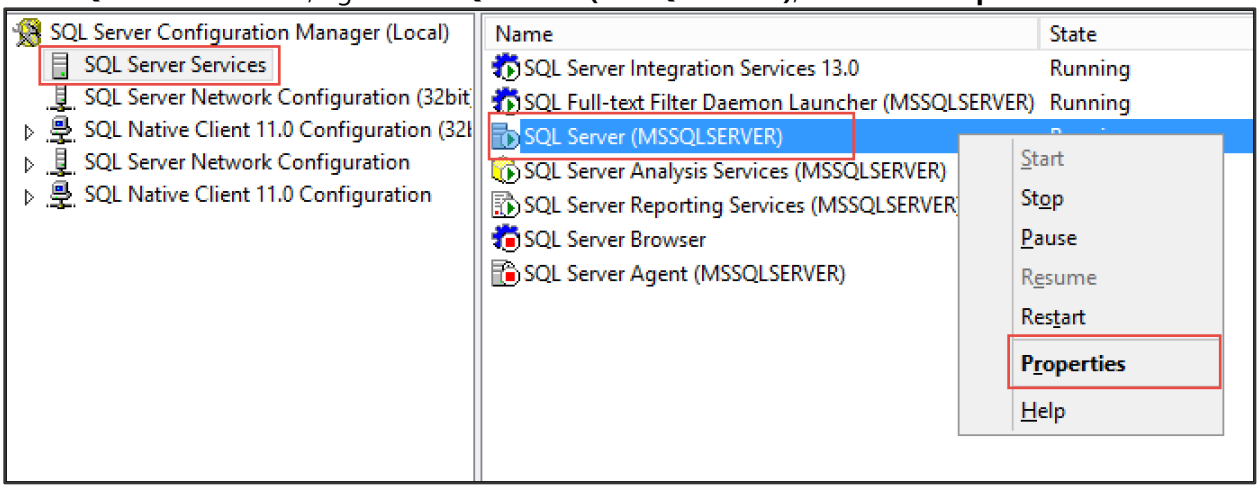
26. Once the PowerShell command has completed, open the **Failover Cluster Manager**, expand the **CLUS-1** cluster, select Nodes, validate all nodes are online and Assigned Vote and Current Vote are listed as "1" for all nodes of the cluster.



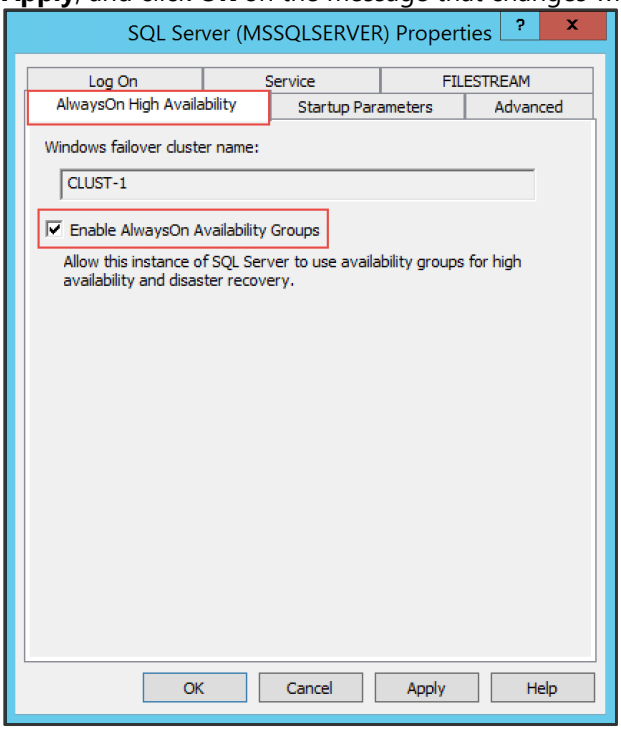
27. Launch **SQL Server 2016 Configuration Manager** on **SQLVM-1**.



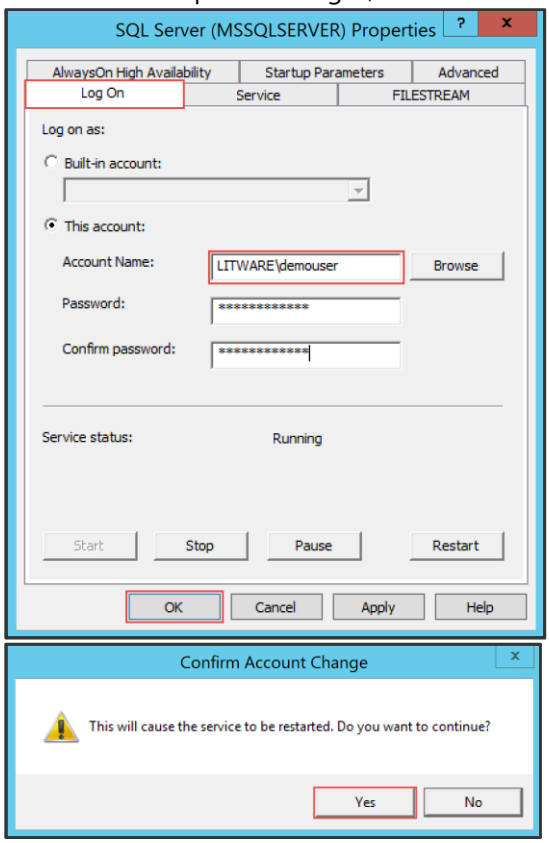
28. Click **SQL Server Services**, right-click **SQL Server (MSSQLSERVER)**, and select **Properties**.



29. Select the **AlwaysOn High Availability** tab, check the box for **Enable AlwaysOn Availability Groups**, click **Apply**, and click **OK** on the message that changes will not take effect until after the server is restarted.

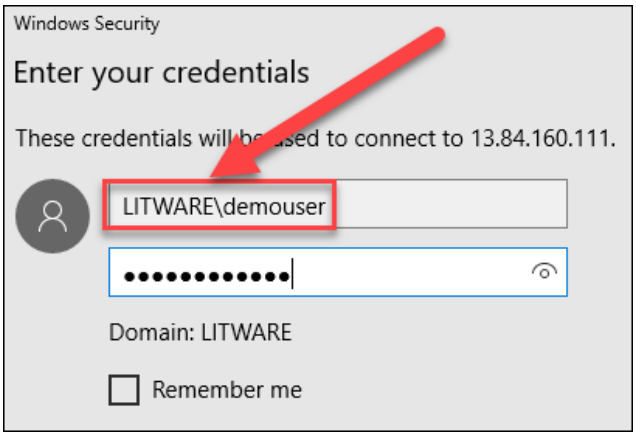


30. On the **Log On** tab, change the service account to **Litware\demouser** using **demo@pass123** for the password. Click **OK** to accept the changes, and click **Yes** to confirm the restart of the server.



31. Minimize the RDP Window for **SQLVM-1.**

32. From the Azure portal, locate **SQLVM-2**, and click **Connect.** Make sure to Sign On using the LITWARE\demouser domain account.

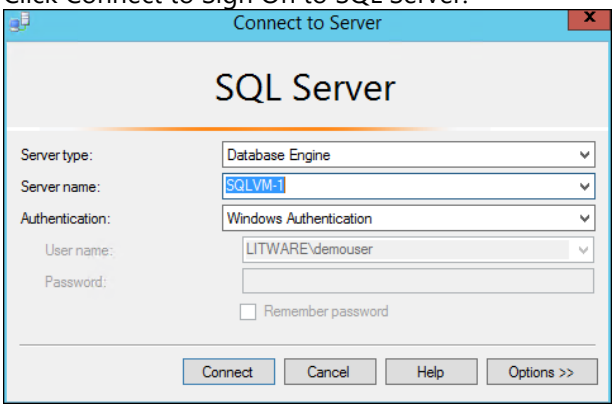


33. From the RPD Session on **SQLVM-2**, repeat steps to configure the **Always On Groups** and **Log On** using SQL 2016 Configuration Manager.

34. Move back to RDP session with **SQLVM-1.**

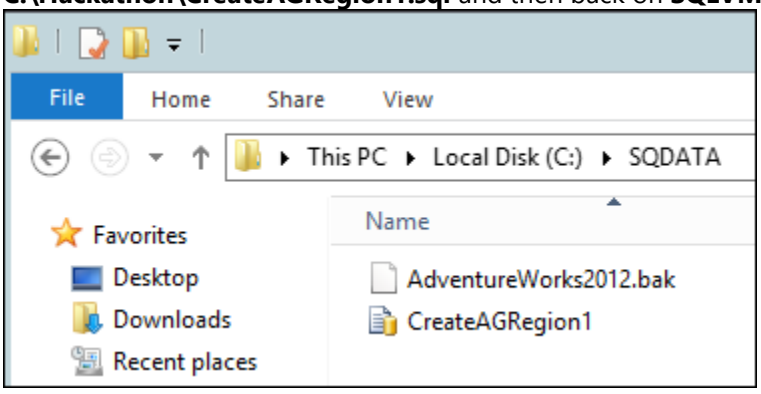
35. Launch **SQL Server 2016 Management Studio**, and connect to the local instance of SQL Server.

36. Click Connect to Sign On to SQL Server.

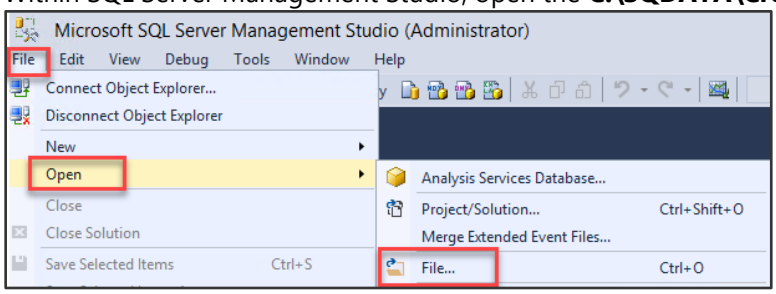


Note: Availability Groups require that the databases be in full recovery mode and that an initial backup has been taken. If you deployed via the ARM template this will be done for you.

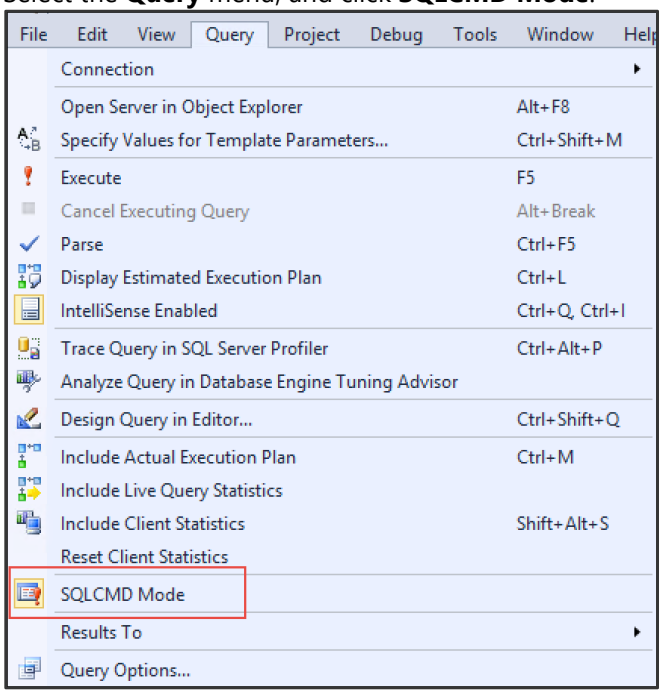
37. Minimize your **SQLVM-1** RDP Session and then Copy from your **LABVM** the file **C:\Hackathon\CreateAGRegion1.sql** and then back on **SQLVM-1** paste it into the **C:\SQDATA** directory**.**



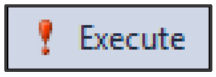
38. Within SQL Server Management Studio, open the **C:\SQDATA\CreateAGRegion1.sql** file.



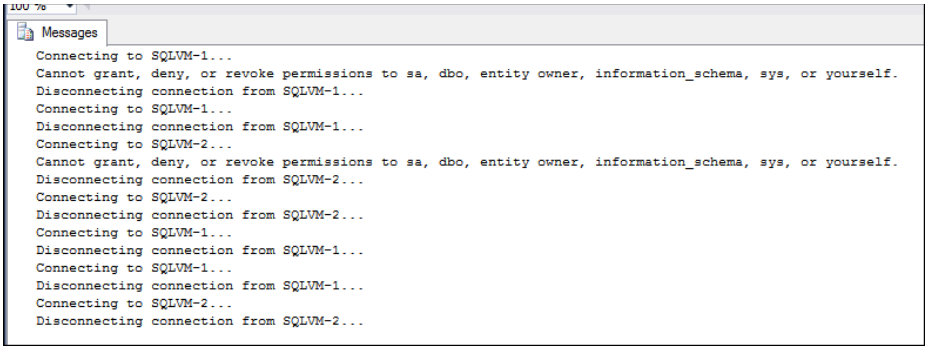
39. Select the **Query** menu, and click **SQLCMD Mode**.



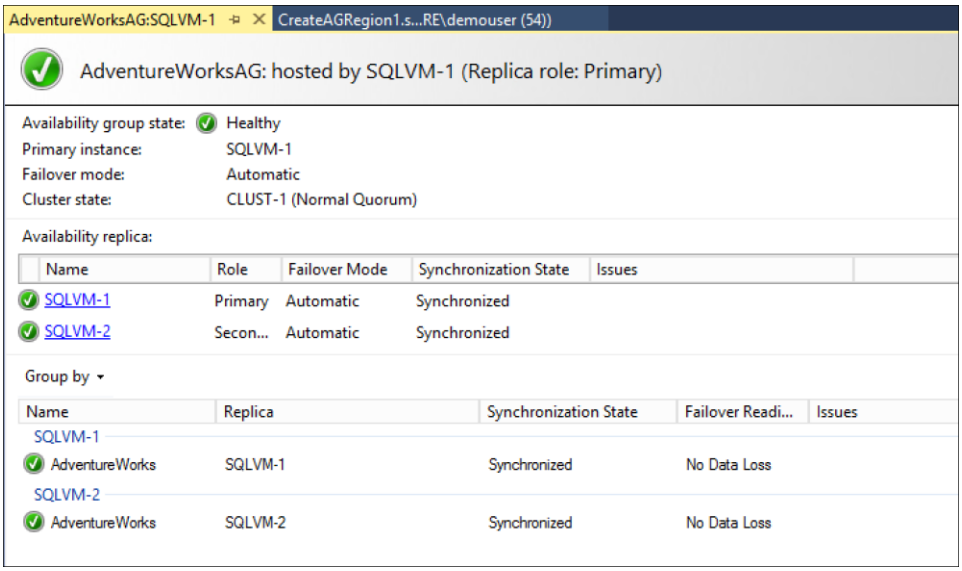
40. Click the **Execute** button to configure the Availability Group.



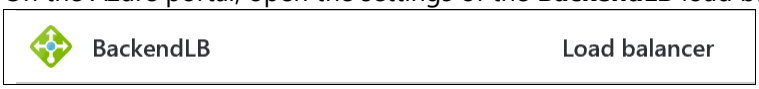
Note: Some security messages are expected. This script was generated by the SQL Server New Availability Group Wizard and modified to support AUTOMATIC_SEEDING. Automatic seeding makes initializing replicas much easier, and the speed of the process is increased significantly. For more details on automatic seeding and performance improvements please refer to SQLCAT's blog: https://blogs.msdn.microsoft.com/sqlcat/2016/06/28/sqlsweet16-episode-2-availability-groups-automatic-seeding-2/.



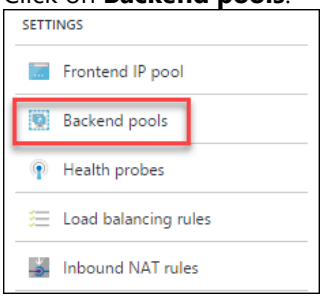
41. Expand **AlwaysOn High Availability -> Availability Groups**, right-click **AdventureWorksAG** (Primary), and choose **Show Dashboard**. Your dashboard should look similar to this:



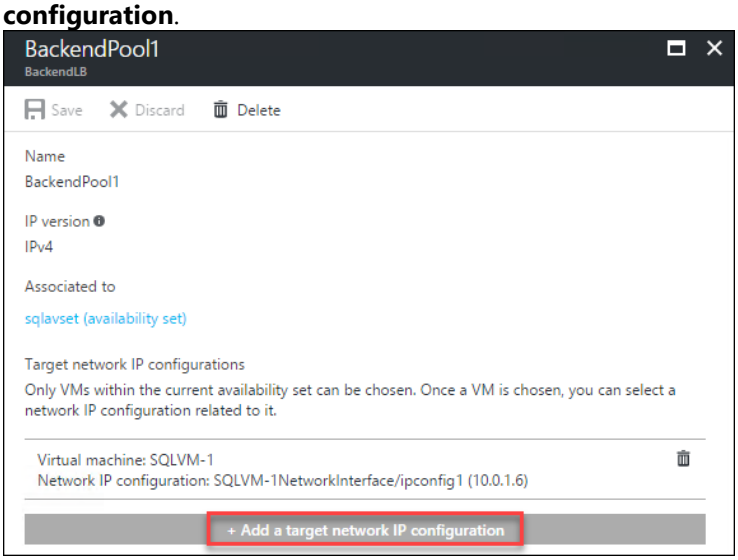
42. On the Azure portal, open the settings of the **BackendLB** load balancer in the **DeploySQLInfra1** resource group.



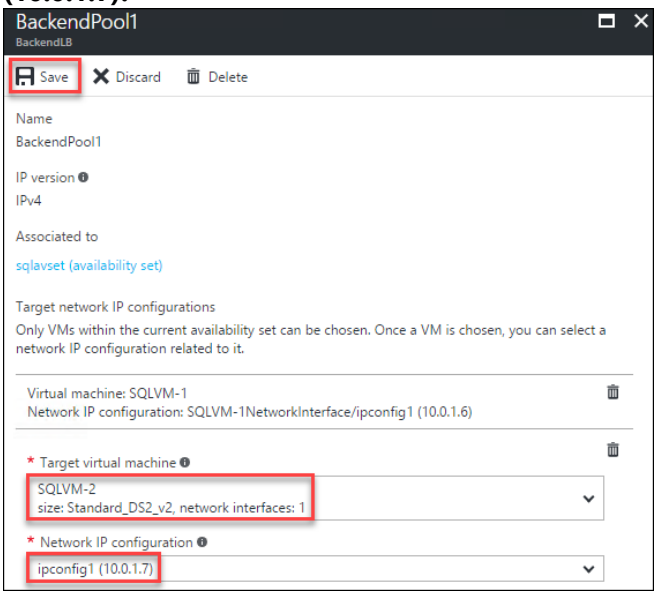
43. Click on **Backend pools**.



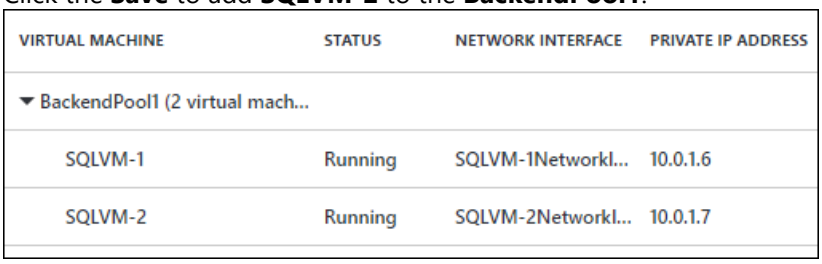
44. Click **BackendPool1** which will open a window showing SQLVM-1. Click the **Add a target network IP configuration**.



45. From the List for Target Virtual Machine select the **SQLVM-2** and the Network IP Configuration **ipconfig1 (10.0.1.7).**



46. Click the **Save** to add **SQLVM-2** to the **BackendPool1**.



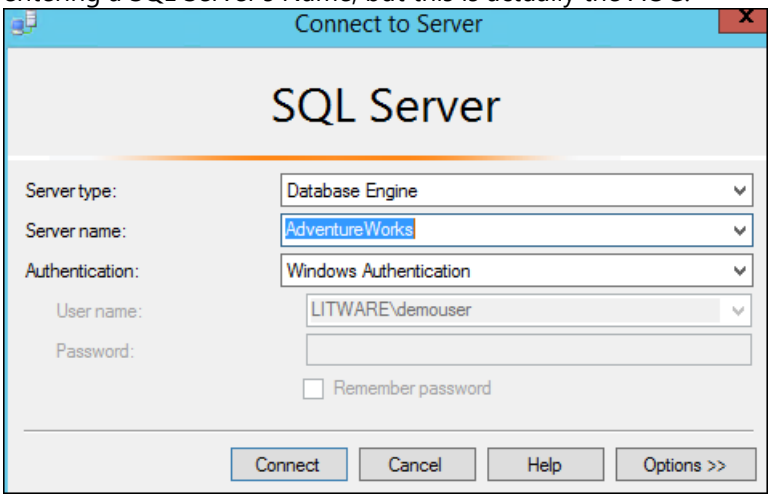
47. Go back to **SQLVM-1**, and open an **Administrative PowerShell_ISE** session. Execute the following PowerShell to configure your cluster for the probe port.

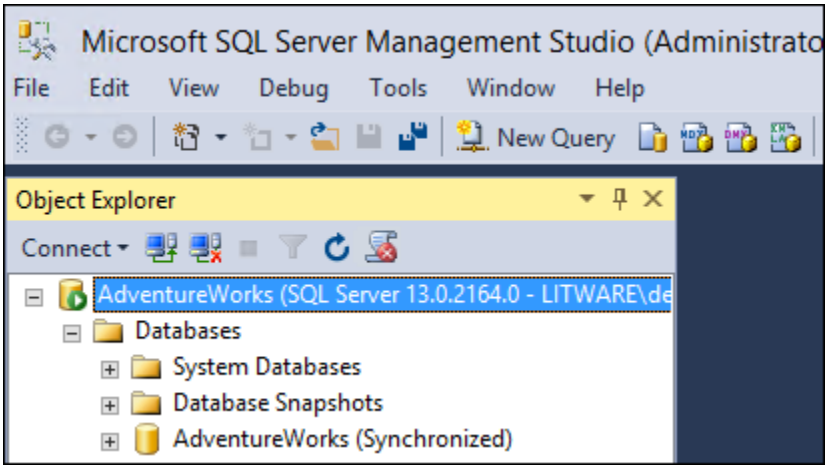
```
$ClusterNetworkName = "Cluster Network 1"
$IPResourceName = "AdventureWorksAG_10.0.1.9"
$ILBIP = "10.0.1.50"
Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
@{"Address"="$ILBIP";"ProbePort"="59999";"SubnetMask"="255.255.255.255";"Net
work"="$ClusterNetworkName";"EnableDhcp"=0}
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "AdventureWorksAG"
```

```
PS C:\Users\demouser> $ClusterNetworkName = "Cluster Network 1"
$IPResourceName = "AdventureWorksAG_10.0.1.9"
$ILBIP = "10.0.1.50"
Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{"Address"="$ILBIP"
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "AdventureWorksAG"
WARNING: The properties were stored, but not all changes will take effect until Adventure

Name                      State   OwnerGroup       ResourceType
----                      -----   ----------       ------------
AdventureWorksAG_10.0.1.9 Offline AdventureWorksAG IP Address
AdventureWorksAG          Online  AdventureWorksAG SQL Server Availability Group
```

48. Connect to **SQLVM-02**, and launch **SQL Server Management Studio**.

49. Open a Server connection to the **AdventureWorks** listener endpoint to verify connectivity. The listener is like entering a SQL Server's Name, but this is actually the AOG.



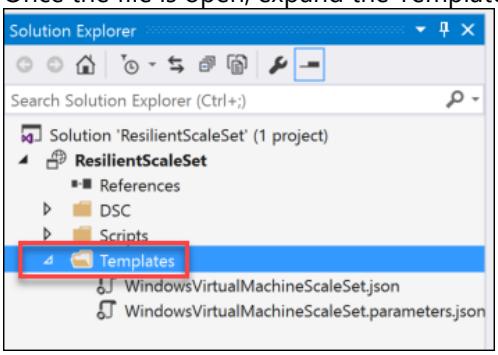


50. After successfully connecting to the AOG listener, disconnect from both SQLVM-1 and SQLVM-2 by using Sign Out from the RDP windows.

Task 2: Run Script to Deploy Web Tier Scale Set (Region 1)

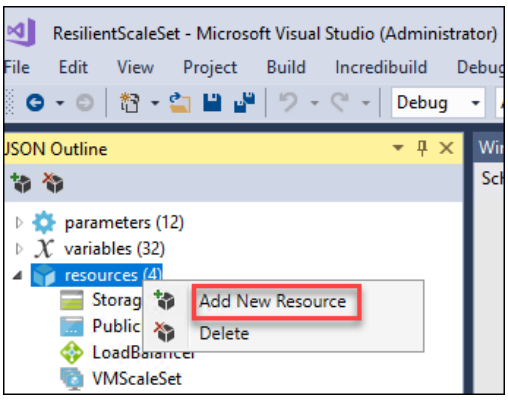
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution**, and browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SS** folder, and select the Visual Studio Solution file: **ResilientScaleSet.sln**.

4. Once the file is open, expand the Templates folder under the name **ResilientScaleSet** in Solution Explorer.

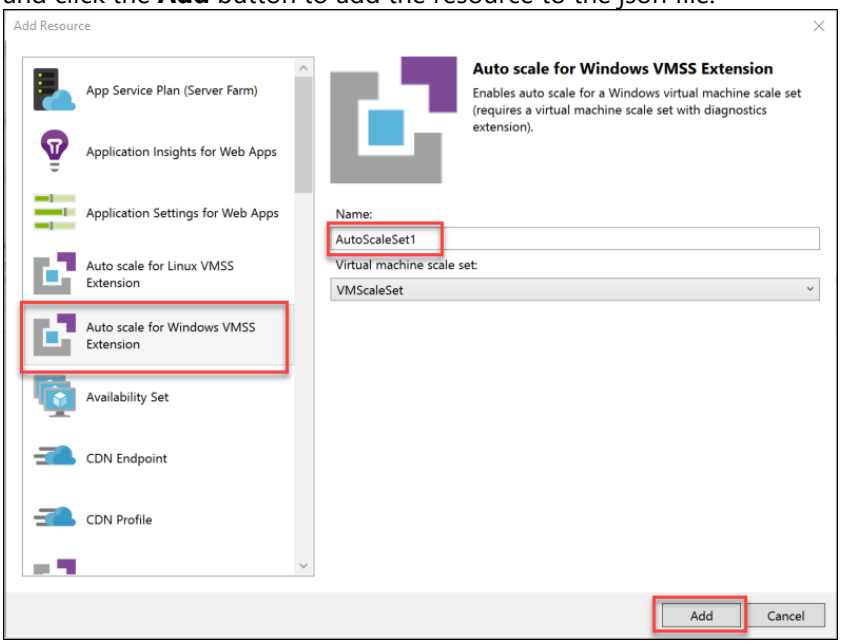


5. Click on the **WindowsVirtualMachineScaleSet.json** file to open it.

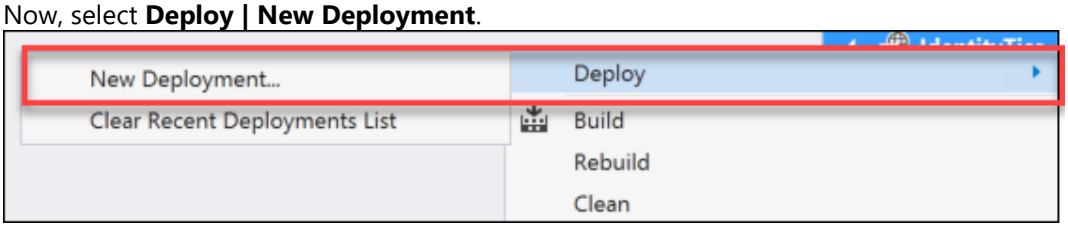
6. Once it is open, in the **JSON Outline** box, right-click on **Resources** and select **Add New Resource** from the context menu.



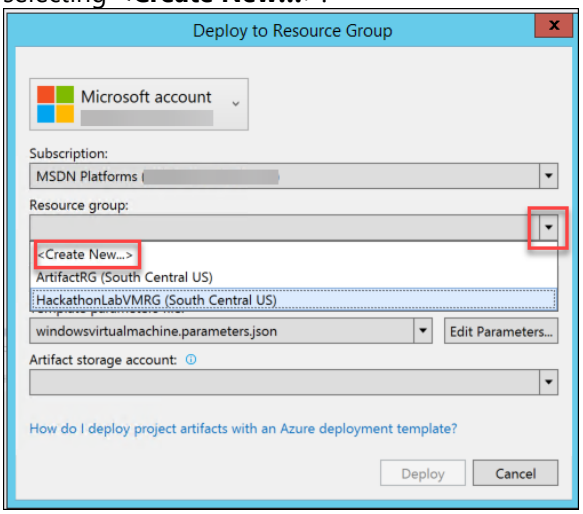
7. From the resource list, choose **Auto scale for Windows VMSS Extension**. In the **Name** box enter **AutoScaleSet1**, and click the **Add** button to add the resource to the json file.



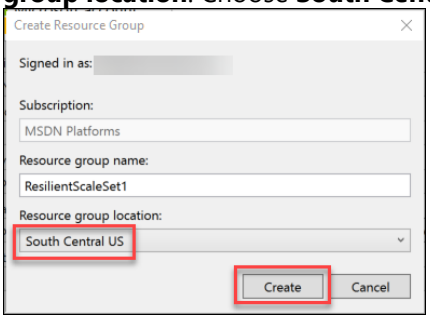
8. Click the **Save** icon to save the changes.
9. Right-click on **ResilientScaleSet** in Solution Explorer.
10. Now, select **Deploy | New Deployment**.



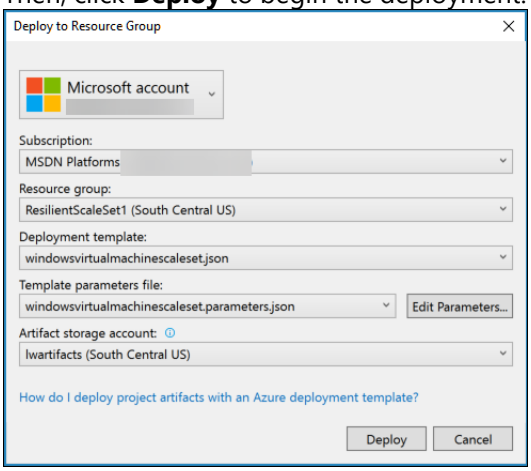
11. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New...>**.



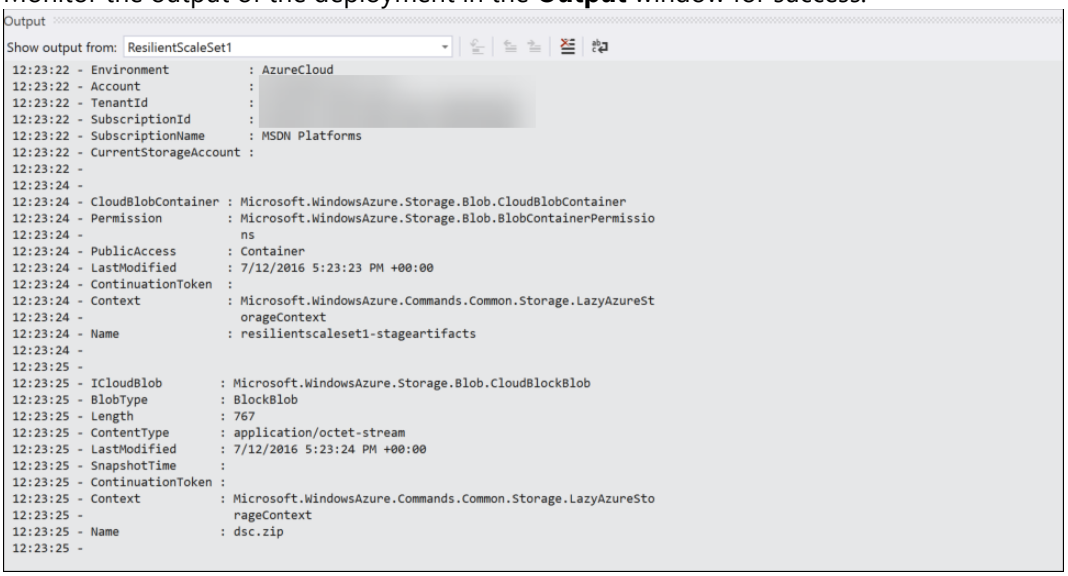
12. In the **Create Resource Group**, enter the **Resource group name** as **ResilientScaleSet1**, and choose a **Resource group location**. Choose **South Central US**, and click the **Create** button to continue.



13. Back in the **Deploy to Resource Group** dialog, choose the **Artifact storage account** created in the previous task. Then, click **Deploy** to begin the deployment.



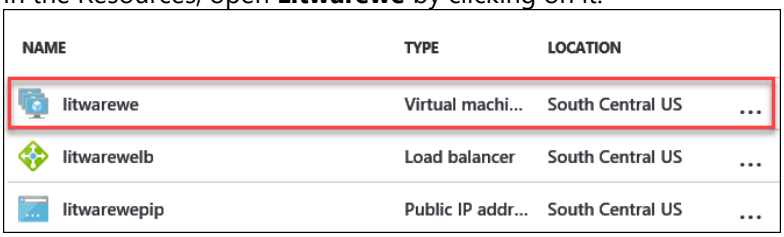
14. Monitor the output of the deployment in the **Output** window for success.



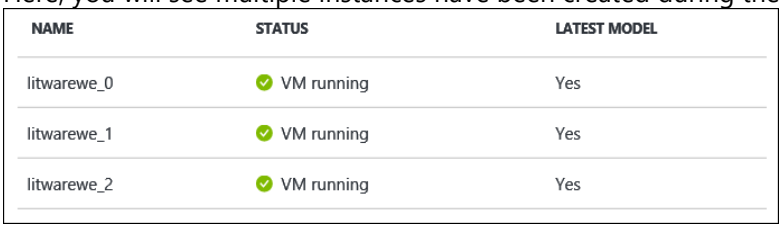
Note: This will take 10-15 minutes to deploy a Scale Set for the Web Tier in Region 1. After this is complete, we can perform some actions to show the Scale capabilities of the Web Tier. While this a real production network, the IaaS VMs (Web-0 and Web-1) could be decommissioned or reused for other purposes.

15. Browse to **Resource Groups** in the left pane menu in the Azure portal. Select the **ResilientScaleSet1** from the list of **Resource Groups**.

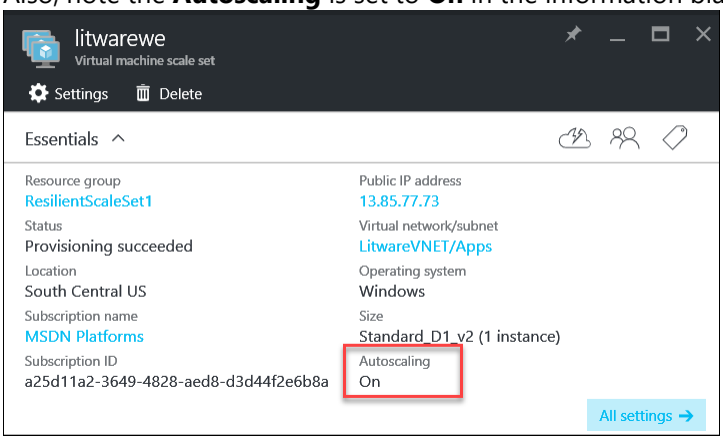
16. In the Resources, open **Litwarewe** by clicking on it.



17. Here, you will see multiple instances have been created during the deployment.

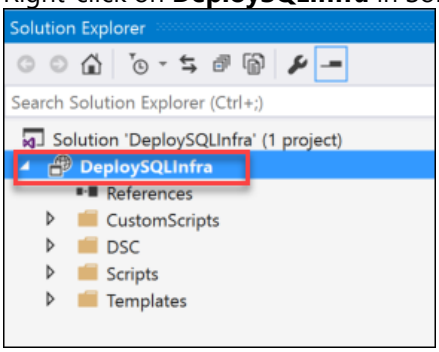


18. Also, note the **Autoscaling** is set to **On** in the information blade.

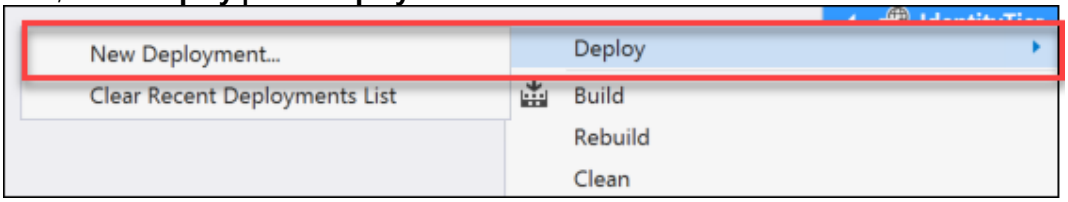


Task 3: Deploy SQL Always-On Cluster (Region 2)

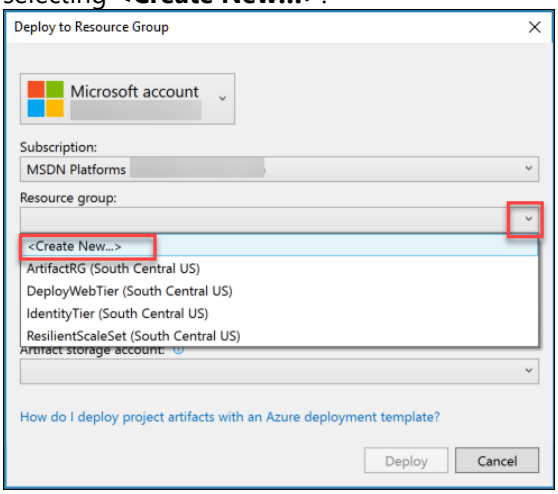
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution**, and browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SQL2** folder, and select the Visual Studio Solution file: **DeploySQLInfra.sln**.
4. Right-click on **DeploySQLInfra** in Solution Explorer.



5. Now, select **Deploy | New Deployment**.



6. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New...>**.



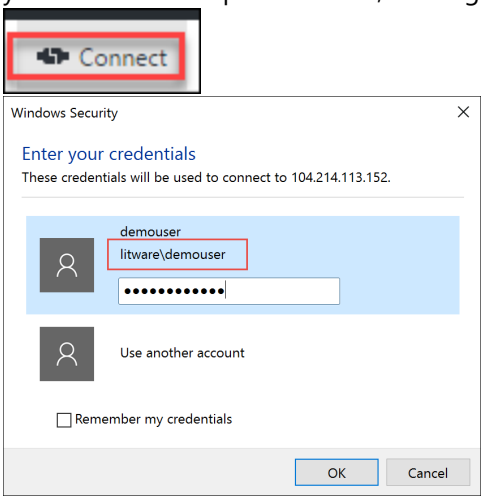
7. In the **Create Resource Group**, enter the **Resource group name** as **DeploySQLInfra2**, and choose a **Resource group location**. Choose **North Central US**, and click the **Create** button to continue.

8. Back in the **Deploy to Resource Group** dialog, make sure an **Artifact storage account** is selected. Then, click **Deploy** to begin the deployment.

9. Monitor the output of the deployment in the **Output** window for success.

   Note: This will take 20-25 minutes to deploy a SQL Always-On Cluster in Region 1. After this is complete, it will be manually configured.

10. Open a remote desktop connection to the **SQLVM-1 (in the DeploySQLInfra Resource Group)** virtual machine you created in the previous task, and login using the **Litware\demouser** account.



11. Once connected, open the Windows Explorer, and check to make sure the **F:** Drive is present.

12. Sign out of **SQLVM-3**.

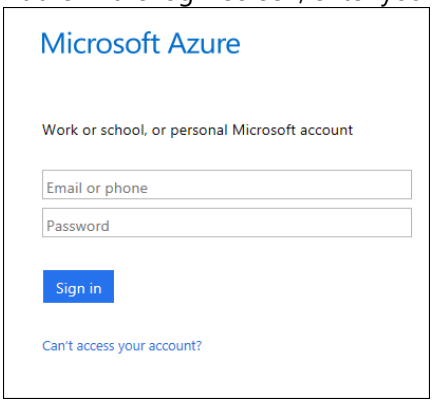
13. From your **LABVM** open the PowerShell ISE Tool.

    Note: In the next few steps, you will use PowerShell to migrate the disks for the SQL Unfractured to Managed Disks.

14. In the execution pane, login to Azure using the **Login-AzureRM** account, and press Enter.

```
Login-AzureRAccount
```

15. At the Azure login screen, enter your Account and Password.



16. Once logged in, make sure to set your subscription to the default for this hands-on lab.

```
Get-AzureRMSubscription
Select-AzureRmSubscription -SubscriptionName
“<YOURSUBSCRIPTIONLEAVETHEQUOTES>”
```

17. Once this is completed, run the following command to verify your VMs for the hands-on lab are present.

```
Get-AzureRMVm
```

```
PS C:\Users\demouser> Get-AzureRmVM
WARNING: Breaking change notice: In upcoming release, top level properties, DataDiskNames and NetworkInterfaceIDs,

ResourceGroupName       Name       Location          VmSize  OsType                     NIC ProvisioningState
-----------------       ----       --------          ------  ------                     --- -----------------
IDENTITYTIER      LitwareDC03 northcentralus    Standard_F1s Windows           litwaredc03246         Succeeded
IDENTITYTIER      LitwareDC04 northcentralus    Standard_F1s Windows           litwaredc04399         Succeeded
DEPLOYSQLINFRA        SQLVM-1 southcentralus Standard_DS2_v2 Windows   SQLVM-1NetworkInterface        Succeeded
DEPLOYSQLINFRA        SQLVM-2 southcentralus Standard_DS2_v2 Windows   SQLVM-2NetworkInterface        Succeeded
DEPLOYSQLINFRA      WitnessVM southcentralus Standard_DS1_v2 Windows WitnessVMNetworkInterface        Succeeded
DEPLOYWEBTIER         SQLVM-1 southcentralus  Standard_D2_v2 Windows   SQLVM-1NetworkInterface        Succeeded
DEPLOYWEBTIER         Web-VM0 southcentralus  Standard_D2_v2 Windows            BackendVMNic0         Succeeded
DEPLOYWEBTIER         Web-VM1 southcentralus  Standard_D2_v2 Windows            BackendVMNic1         Succeeded
IDENTITYTIER             ADDC southcentralus  Standard_D2_v2 Windows                  ADDCNic         Succeeded
IDENTITYTIER      LitwareDC01 southcentralus    Standard_F1s Windows           litwaredc01891         Succeeded
IDENTITYTIER      LitwareDC02 southcentralus    Standard_F1s Windows           litwaredc02936         Succeeded
```

18. Now, move to the scripting pane of the PowerShell ISE tool. Paste this code into the window.

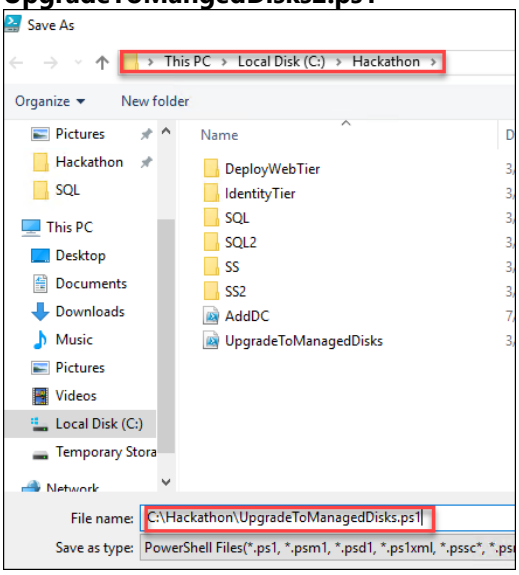
```
$rgName = 'myResourceGroup'

$avSetName = 'myAvailabilitySet'


$avSet =  Get-AzureRmAvailabilitySet -ResourceGroupName $rgName -Name $avSetName


Update-AzureRmAvailabilitySet -AvailabilitySet $avSet -Managed


foreach($vmInfo in $avSet.VirtualMachinesReferences)
```

```
 {
$vm =  Get-AzureRmVM -ResourceGroupName $rgName | Where-Object {$_.Id -eq $vmInfo.id}

Stop-AzureRmVM -ResourceGroupName $rgName -Name  $vm.Name -Force

ConvertTo-AzureRmVMManagedDisk -ResourceGroupName $rgName -VMName $vm.Name

 }
```

19. Update the variables at the top of the script with the names of the Resource Group and the Availability Set used for the **SQLVM-3**, **SQLVM-4** and **WitnessVM2**.

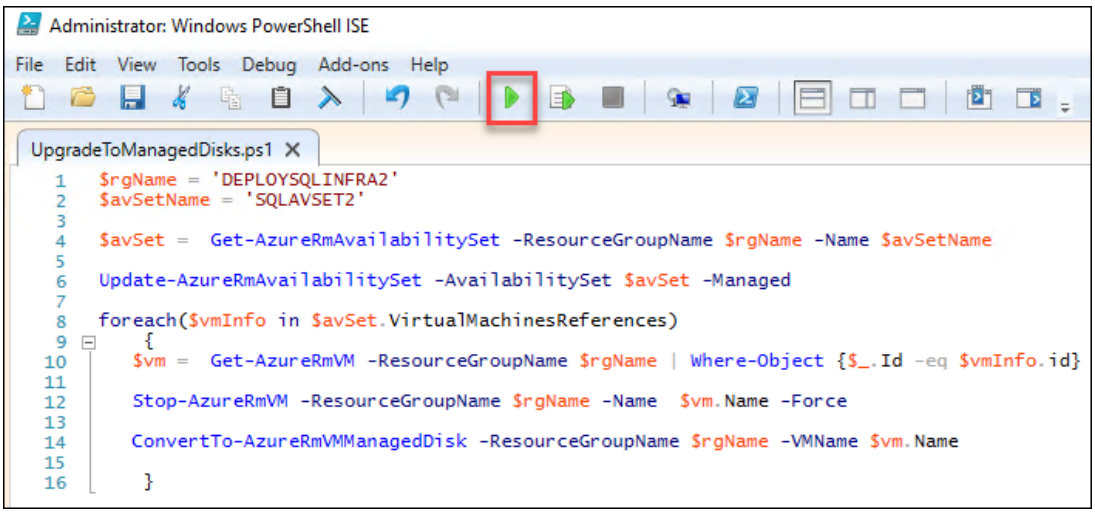
```
$rgName = 'DEPLOYSQLINFRA2'
$avSetName = 'SQLAVSET2'
```

20. In PowerShell_ISE, click **File > Save**, and in the **C:\Hackathon** directory, name the file **UpgradeToMangedDisks2.ps1**



21. Next, click the Play button in PowerShell_ISE.

    Note: This will deallocate all of the machines in the Availability Set SQLAVSET2 and migrate them to a Managed Availability Set and the Unmanaged Disks to Managed Disks.



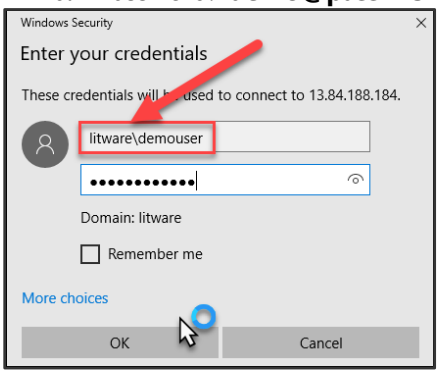
    Note: This process will take about 10-15 minutes to complete. Be careful not to stop the process.

22. Open the Azure portal, and browse to the **DeploySQLInfra2** Resource Group. Notice the machines are now using Managed Disks, and the disk objects now appear.

23. Click on SQLVM-3, and press Connect to RDP to the Server. Make sure to use the Domain Credentials from now on.

    a. User: **LITWARE\demouser**

    b. Password: **demo@pass123**

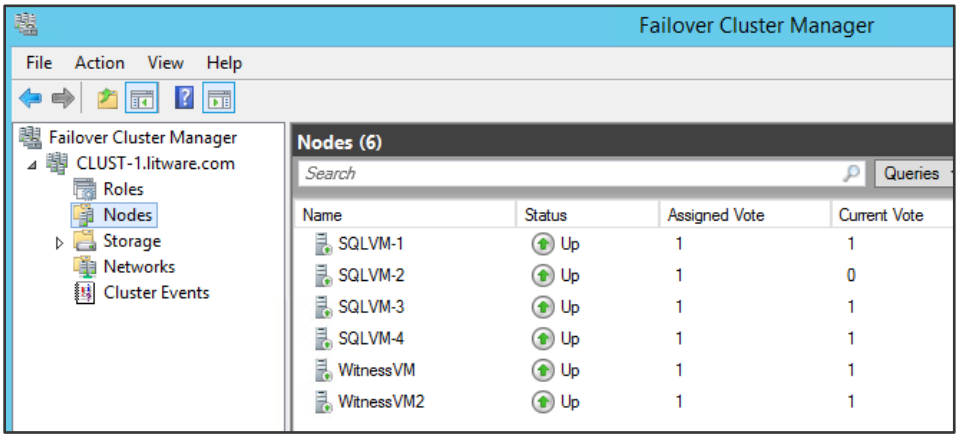


24. Next, run this command from **SQLVM-1** to create a Cluster for the SQL Always-On Group. **Start > PowerShell > Enter**, and execute the following code:

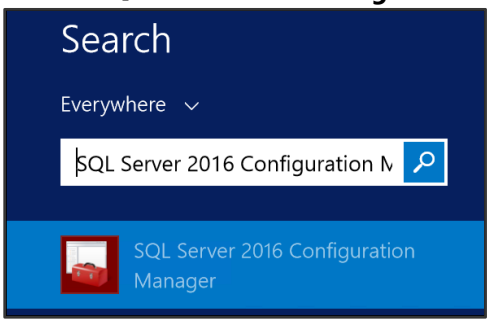
```
Add-ClusterNode -Name SQLVM-3,SQLVM-4,WITNESSVM2
```

25. This will add three nodes to your existing cluster.

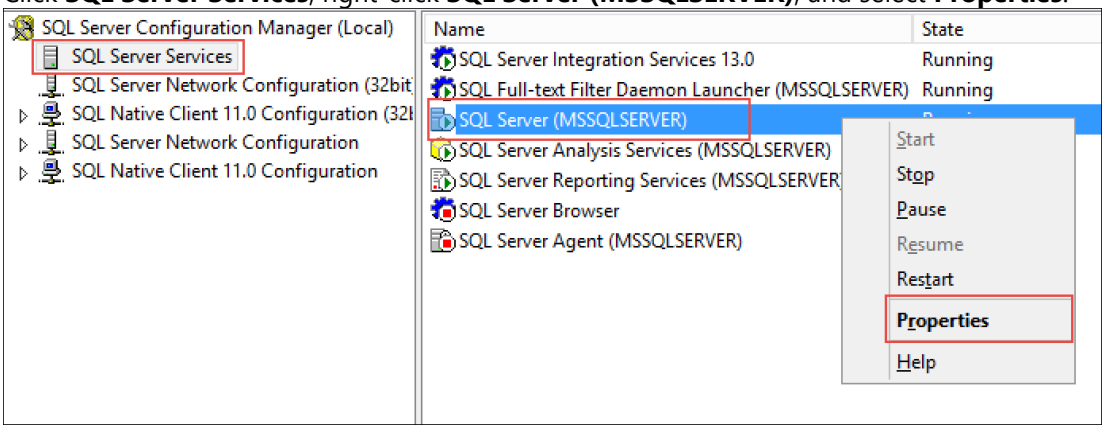
26. Open the Failover Cluster Manager, expand the **CLUST-1** cluster, select Nodes, and validate that all nodes are online.



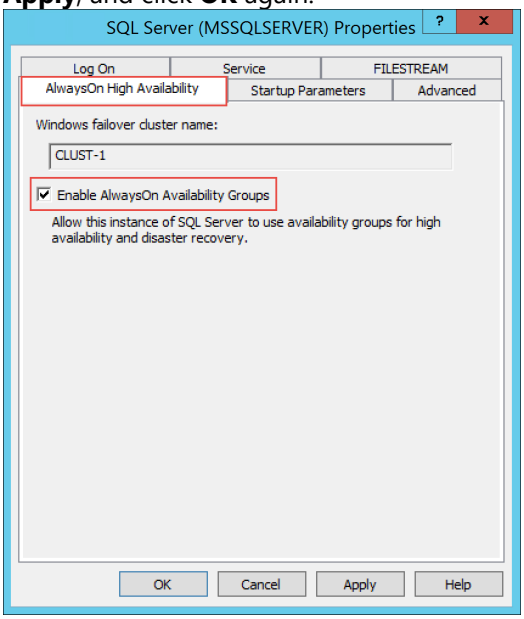
27. Launch **SQL Server 2016 Configuration Manager** on **SQLVM-3**.



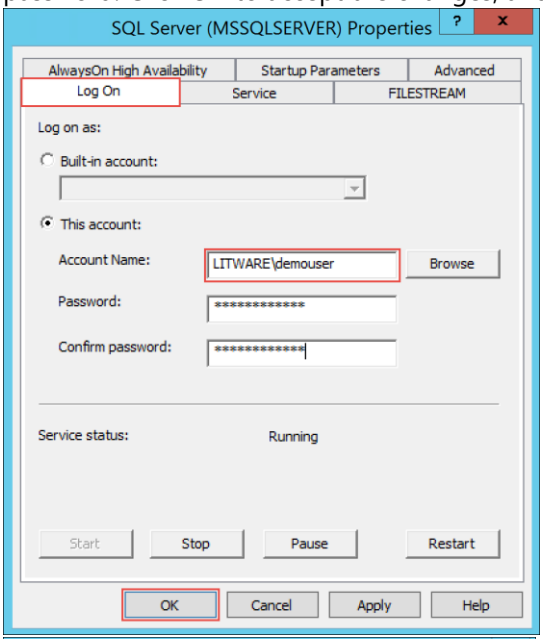
28. Click **SQL Server Services**, right-click **SQL Server (MSSQLSERVER)**, and select **Properties**.



29. Select the **AlwaysOn High Availability** tab, and check the box for **Enable AlwaysOn Availability Groups**, click **Apply**, and click **OK** again.

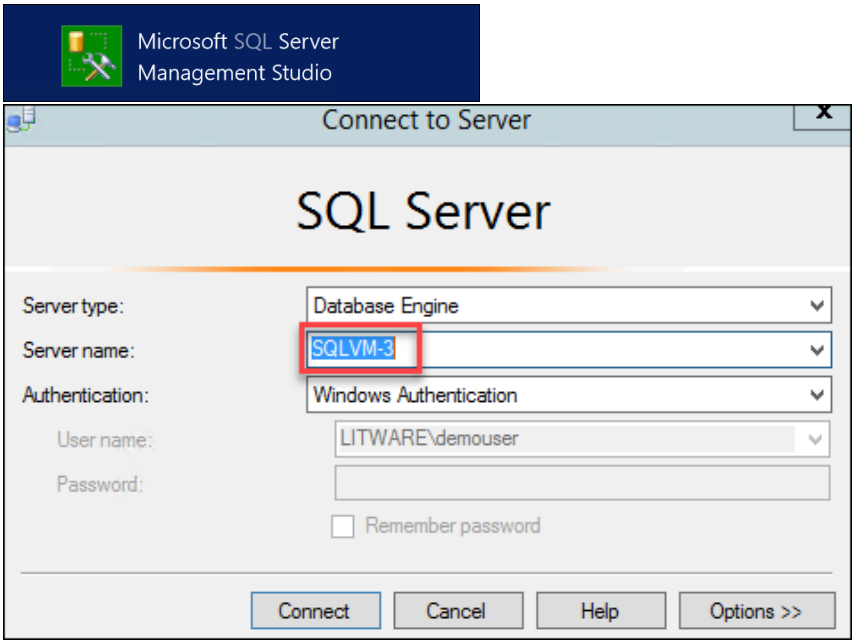


30. Click on the **Log On** tab, and change the service account to **Litware\demouser** using **demo@pass123** for the password. Click **OK** to accept the changes, and click **Yes** to confirm the restart of the server.



31. Minimize your RDP window for **SQLVM-3.** Using the Azure portal, connect to **SQLVM-4** and then repeat these same steps.

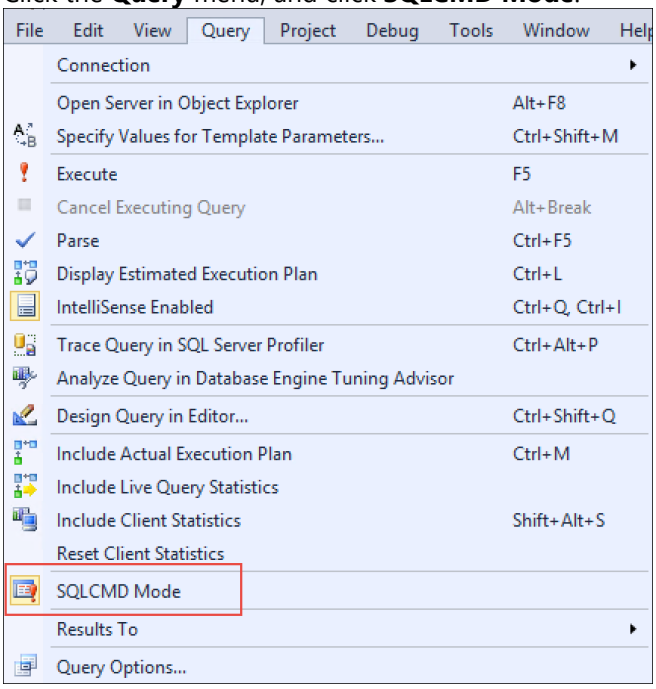
32. Move back to your open a remote desktop connection to the **SQLVM-3**, launch **SQL Server 2016 Management Studio**, and **connect to the local instance of SQL Server**.



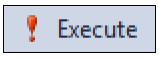
33. Copy file **C:\Hackathon\CreateAGRegion2.sql** from your **LABVM** machine to **SQLVM-3** in the **C:\SQDATA.**

34. Within SQL Server Management Studio, open the **C:\SQLDATA\CreateAGRegion2.sql** file.

35. Click the **Query** menu, and click **SQLCMD Mode**.



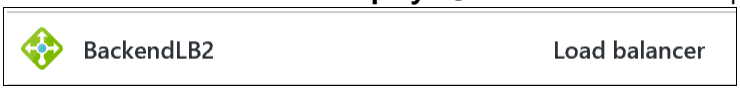
36. Click the **Execute** button to configure the Availability Group.



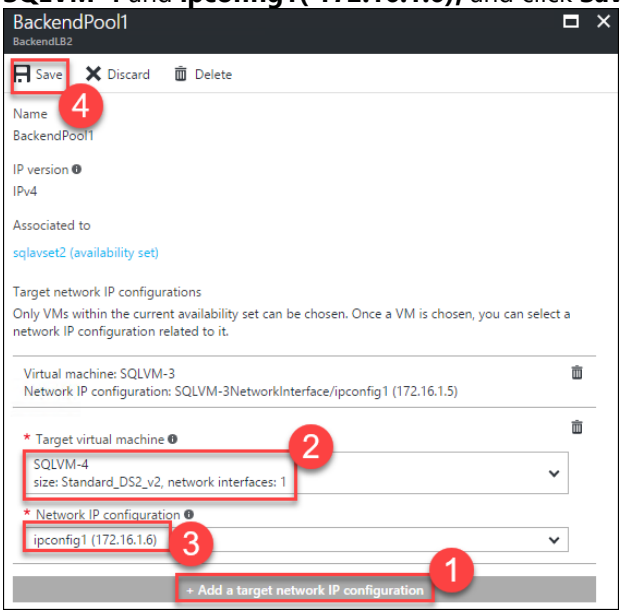
37. Some security messages are expected. This is a successful run of the script.

```
Messages
Connecting to SQLVM-3...
Cannot grant, deny, or revoke permissions to sa, dbo, entity owner, information_schema, sys, or yourself
Disconnecting connection from SQLVM-3...
Connecting to SQLVM-3...
Disconnecting connection from SQLVM-3...
Connecting to SQLVM-1...
Disconnecting connection from SQLVM-1...
Connecting to SQLVM-4...
Cannot grant, deny, or revoke permissions to sa, dbo, entity owner, information_schema, sys, or yourself
Disconnecting connection from SQLVM-4...
Connecting to SQLVM-4...
Disconnecting connection from SQLVM-4...
Connecting to SQLVM-1...
Disconnecting connection from SQLVM-1...
Connecting to SQLVM-1...
Disconnecting connection from SQLVM-1...
Connecting to SQLVM-3...
Disconnecting connection from SQLVM-3...
Connecting to SQLVM-4...
Disconnecting connection from SQLVM-4...
```

38. Minimize the **SQLVM-3** RDP session, and using the Azure portal on LABVM, open the settings of the **BackendLB2** load balancer located in the **DeploySQLInfra2** Resource Group.



39. Click on **Backend pools**, select **BackendPool1**, and click **+Add a target network IP Configuration**. Select **SQLVM-4** and **ipconfig1(172.16.1.6),** and click **Save**.



40. Go back to **SQLVM-3**, and open an **Administrative PowerShell_ISE** session. Execute the following PowerShell to configure your cluster for the probe port.

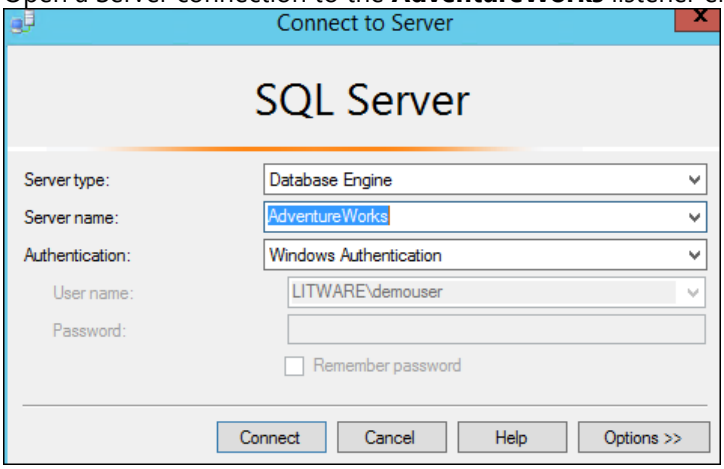
```
$ClusterNetworkName = "Cluster Network 1"
$IPResourceName = "AdventureWorksAG_172.16.1.9"
$ILBIP = "172.16.1.50"
Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
@{"Address"="$ILBIP";"ProbePort"="59999";"SubnetMask"="255.255.255.255";"Net
work"="$ClusterNetworkName";"EnableDhcp"=0}
```

```
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "AdventureWorksAG"
```

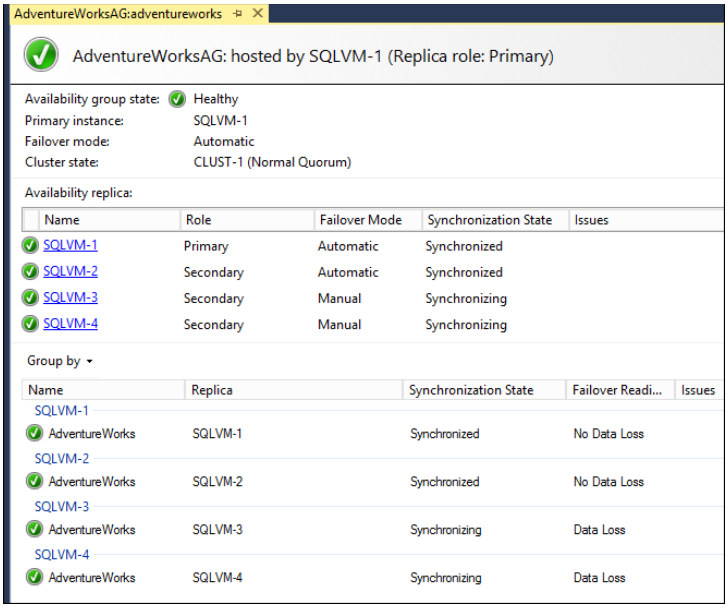
```
PS C:\Users\demouser> $ClusterNetworkName = "Cluster Network 1"
$IPResourceName = "AdventureWorksAG_172.16.1.9"
$ILBIP = "172.16.1.50"
Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{"Address"="$
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "AdventureWorksAG"

Name                           State   OwnerGroup       ResourceType
----                           -----   ----------       ------------
AdventureWorksAG_172.16.1.9 Offline AdventureWorksAG IP Address
AdventureWorksAG            Online  AdventureWorksAG SQL Server Availability Group
```

41. Connect to **SQLVM-04**, and launch **SQL Server Management Studio**.

42. Open a Server connection to the **AdventureWorks** listener endpoint to verify connectivity to the AOG.



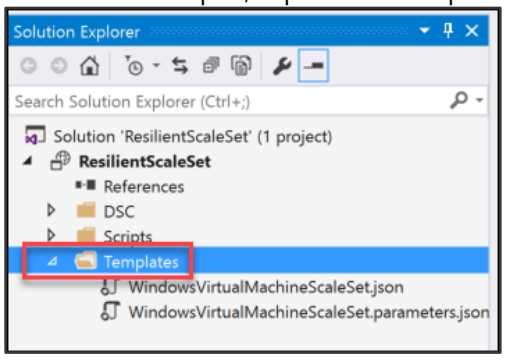
43. Click the **Always On High Availability**, and expand the **Availability Groups**. Right-click **AdventrueWorksAG**, and click **Show Dashboard**.



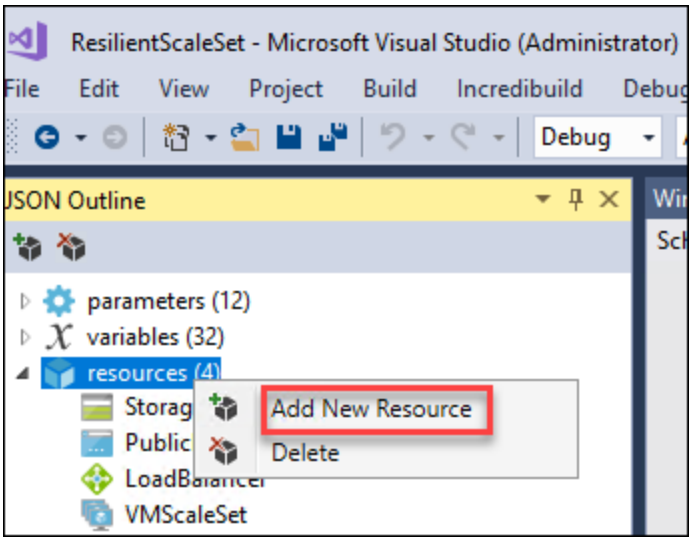
44. Close your RDP Windows.

Task 4: Deploy Web Tier Scale Set (Region 2)

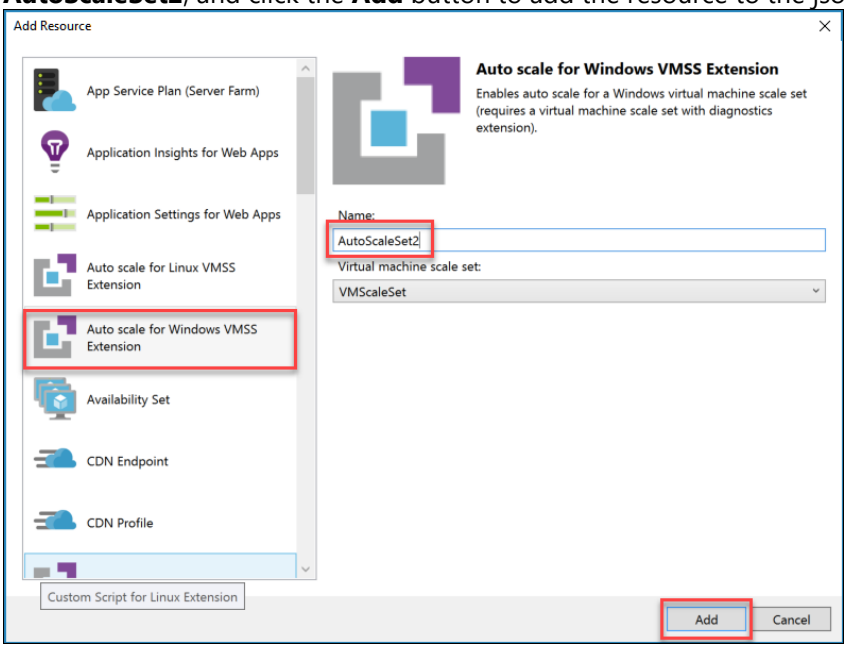
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution**, and browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SS2** folder, and select the Visual Studio Solution file: **ResilientScaleSet.sln**.
4. Once the file is open, expand the Templates folder under the name **ResilientScaleSet** in Solution Explorer.



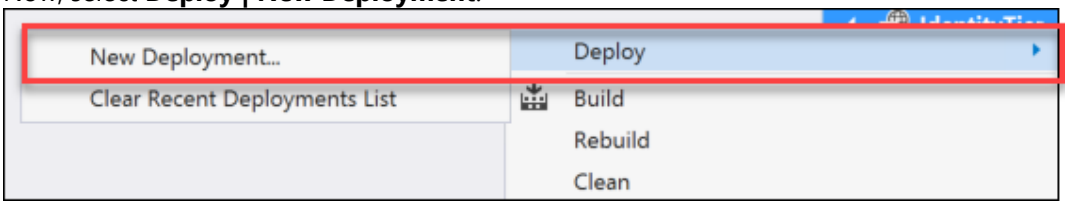
5. Click on the **WindowsVirtualMachineScaleSet.json** file to open it.
6. Once it is open, in the **JSON Outline** box, right-click on **Resources**, and select **Add New Resource** from the context menu.



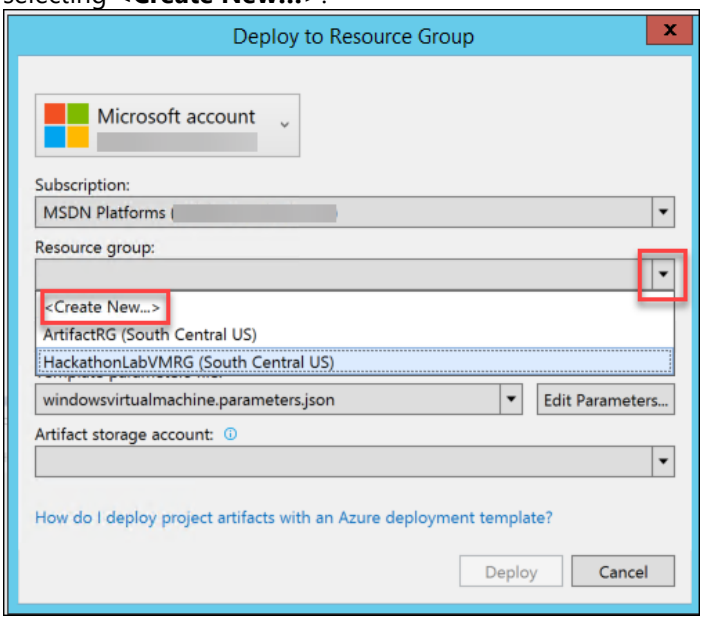
7. From the resource list, choose **Auto scale for Windows VMSS Extension**. In the **Name** box, enter **AutoScaleSet2**, and click the **Add** button to add the resource to the json file.



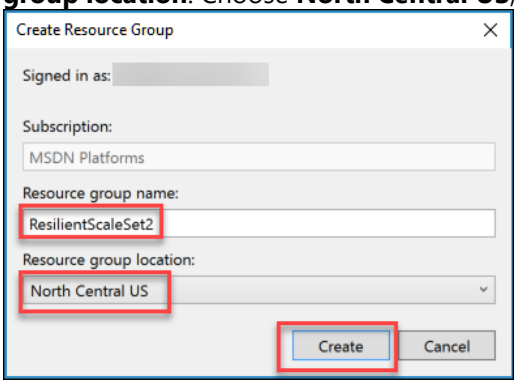
8. Once the resource is added, click the **Save** icon to save the changes.
9. Right-click on **ResilientScaleSet** in Solution Explorer.
10. Now, select **Deploy | New Deployment**.



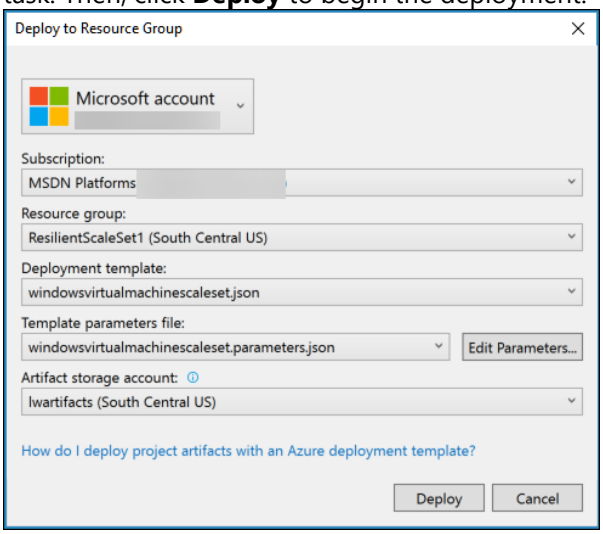
11. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New...>**.



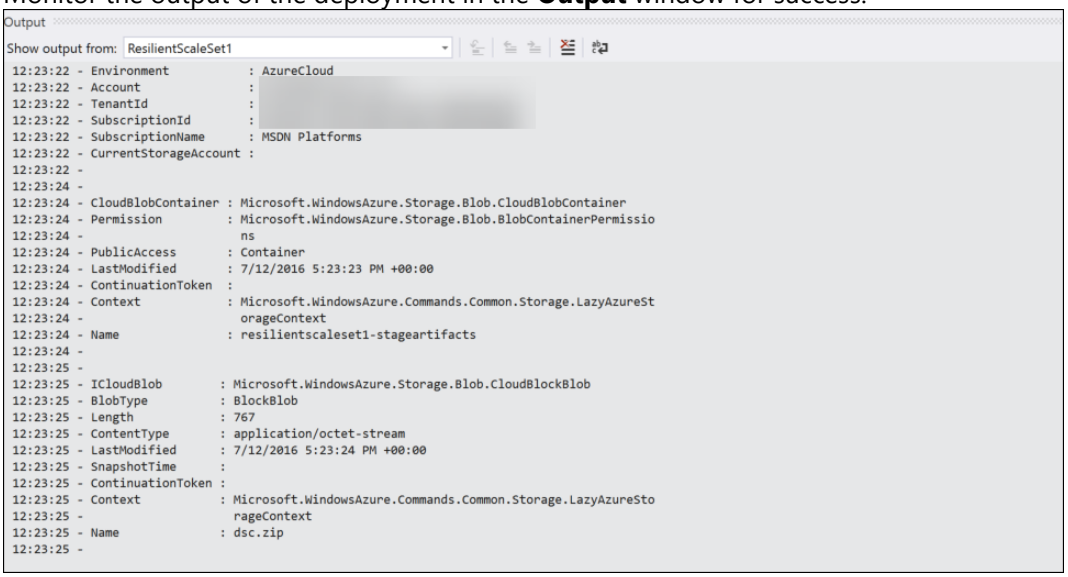
12. In the **Create Resource Group**, enter the **Resource group name** as **ResilientScaleSet2**, and choose a **Resource group location**. Choose **North Central US**, and click the **Create** button to continue.



13. Back in the **Deploy to Resource Group** dialog, now choose the **Artifact storage account** created in the previous task. Then, click **Deploy** to begin the deployment.



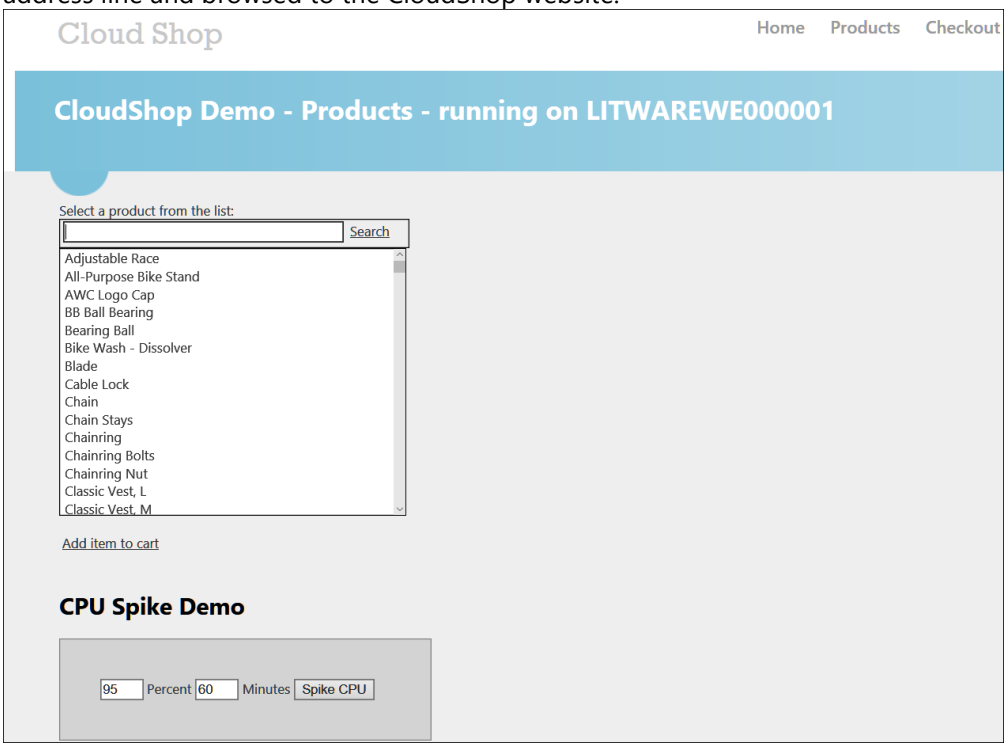
14. Monitor the output of the deployment in the **Output** window for success.



Note: This will take 10-15 minutes to deploy a Scale Set for the Web Tier in Region 2. After this is complete, we can perform some actions to show the Scale capabilities of the Web Tier.

15. Browse to **Resource Groups** in the left pane menu in the Azure portal. Select the **ResilientScaleSet2** from the list of **Resource Groups**.

16. In the Resources, select **Litwarepip**, and click on it to open it. Copy the **DNS name**, and paste it in a browser address line and browsed to the CloudShop website.



17. On the **CPU Spike Demo** section, change the minutes to 15, and click the **Spike CPU** button.
18. Monitor the **Litwarewe** Scale Set, and you should see additional instances being deployed by autoscaling.

Summary

In this exercise, you designed and created IaaS resiliency options in the additional region. You deployed resilient Web Servers, an additional Load Balancer, and a SQL Always-On Cluster for Database resiliency.

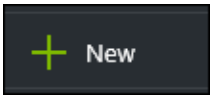
Exercise 5: Prepare other resources for resiliency

Duration: 45 minutes

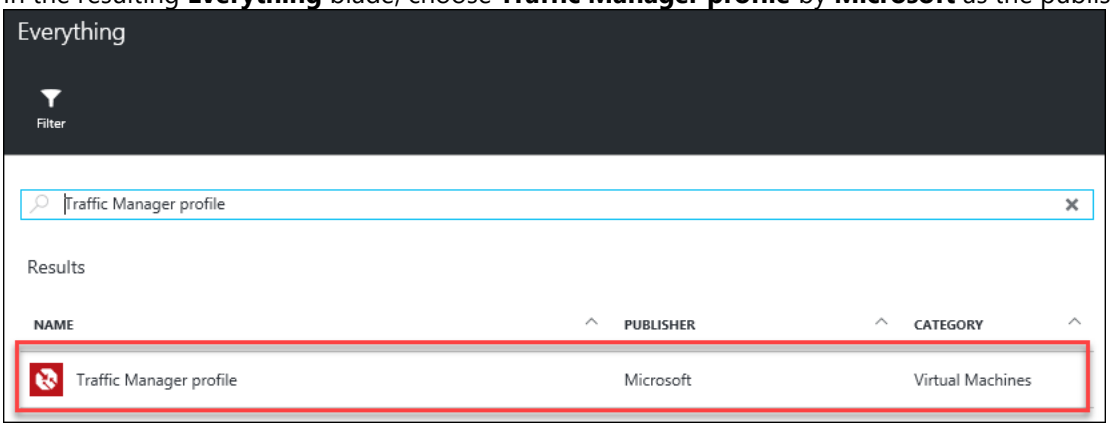
In this exercise, you will design additional resiliency options in Azure, deploy a Traffic Manager in Priority Mode, configure Operations Management Suite and check for missing patches. You will also configure IaaS backups in both regions as well as configure Network Security Groups as needed.

Task 1: Create Traffic Manager in Priority Mode

1. Browse to the Azure Portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.

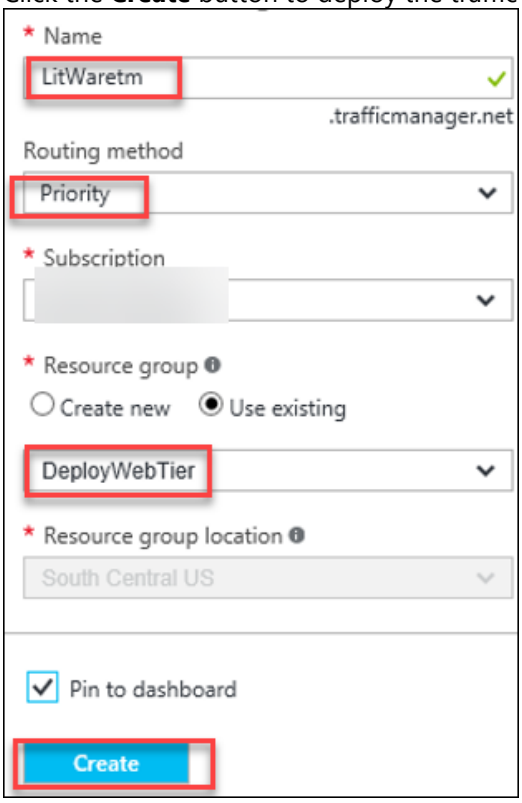


3. In the **Search the marketplace** window, type **Traffic Manager Profile** and hit Enter.
4. In the resulting **Everything** blade, choose **Traffic Manager profile** by **Microsoft** as the publisher.

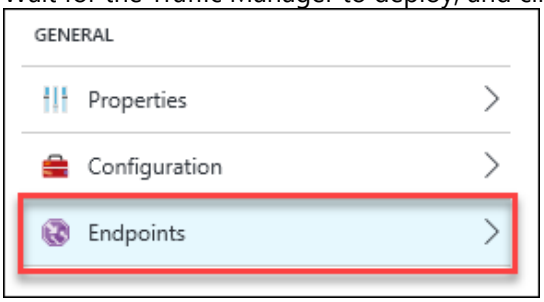


5. Click the **Create** button to continue.
6. In the **Create Traffic Manager profile** settings, enter the following:
    a. Name: **litwaretm(add uniqueness)**
    b. Routing method: **Priority**
    c. Subscription: **Select your subscription**
    d. Resource group: **Use existing – DeployWebTier**
    e. Resource group location: **South Central US (Default)**
    f. Pin to dashboard: **Check the checkbox**

g. Click the **Create** button to deploy the traffic manager.



7. Wait for the Traffic Manager to deploy, and click **Endpoints >** in the **Settings** blade.



8. Click the **+ Add** icon.

9. Enter the following settings on the **Add endpoint** blade:

   a. Type: **Azure endpoint**

   b. Name: **South Central**

   c. Target resource type: **Public IP address**

   d. Target resource: **Choose a Public IP address – that is attached to your Load Balancer in the South Central Region**

   e. Priority: **1**

   f. Click the **OK** button to save the endpoint.

10. Click the **+ Add** icon again.

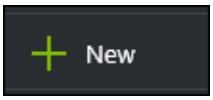
11. Enter the following settings on the **Add endpoint** blade:
    a. Type: **Azure endpoint**
    b. Name: **North Central**
    c. Target resource type: **Public IP address**
    d. Target resource: **Choose a Public IP address – LoadBalancerIP2**
    e. Priority: **2**
    f. Click the **OK** button to save the endpoint.

NAME	STATUS	MONITOR STATUS	TYPE	PRIORITY
South Central	Enabled	Checking endpoint	Azure endpoint	1
North Central	Enabled	Checking endpoint	Azure endpoint	2

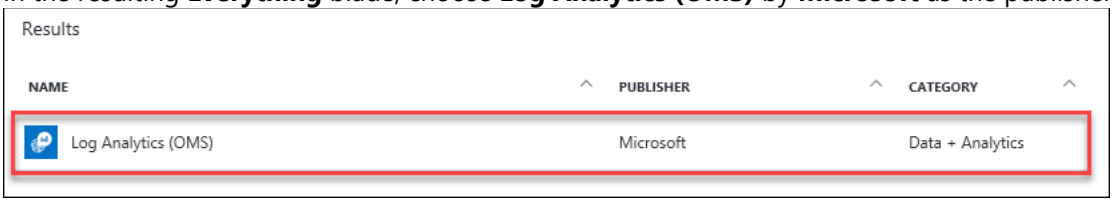
12. Once the South Central Site comes online, you can point your browser to the DNS name of the traffic manager. You can simulate an outage as well by deallocating your Scale set in this South Central region and see it failover to North Central.

Task 2: Configure Operations Management Suite for Monitoring (Region 1 and 2)

1. Browse to the Azure Portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.

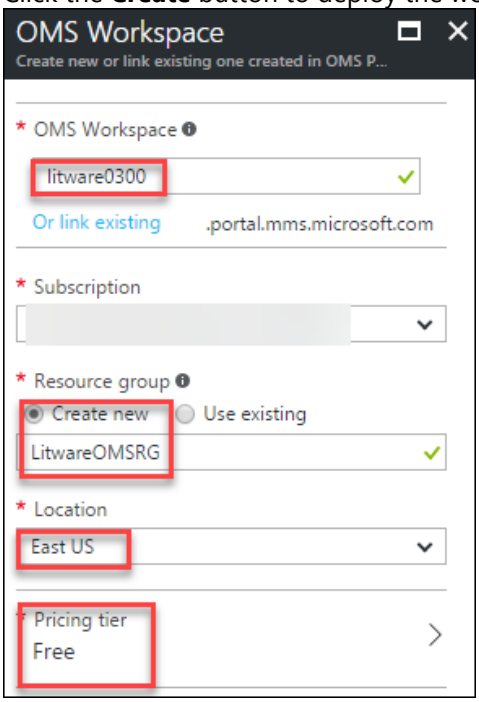


3. In the **Search the marketplace** window, type **Log Analytics (OMS)** and hit Enter.
4. In the resulting **Everything** blade, choose **Log Analytics (OMS)** by **Microsoft** as the publisher.

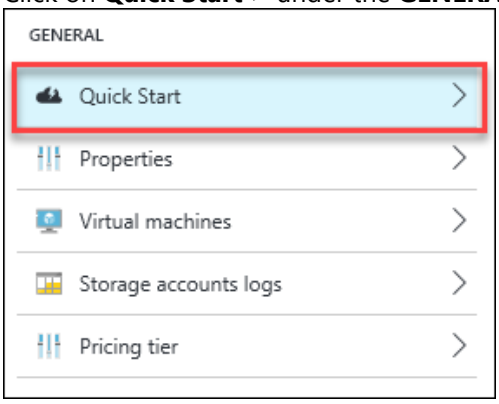


5. Click the **Create** button to continue.
6. In the **OMS Workspace** settings blade, enter the following settings:
    a. OMS Workspace: **Litware0xxx** (where 0xxx is a unique number)
    b. Subscription: **Choose your subscription**
    c. Resource Group: **Create new – LitwareOMSRG**
    d. Location: **East US** (there are only a few regions where this can be deployed)
    e. Pricing tier: **Free**
    f. Pin to dashboard: **Click the checkbox**

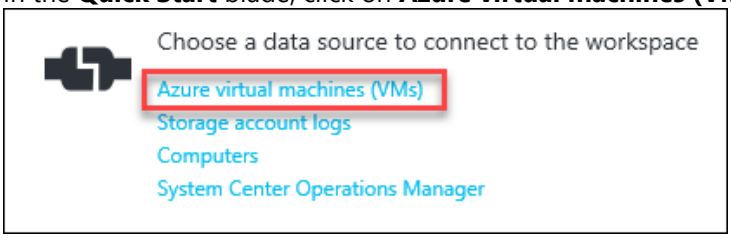
g. Click the **Create** button to deploy the workspace.



7. Click on **Quick Start >** under the **GENERAL** heading.



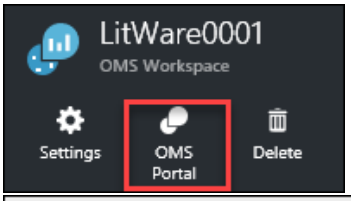
8. In the **Quick Start** blade, click on **Azure virtual machines (VMs)**.

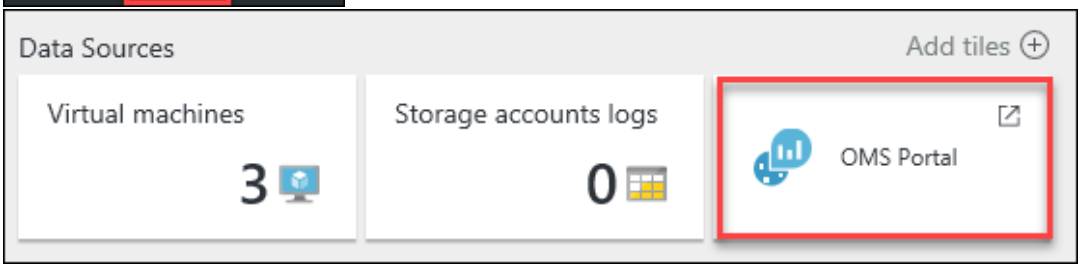


9. In the list of **Virtual Machines**, select the domain controllers, and click the **Connect** icon for each individual machine.

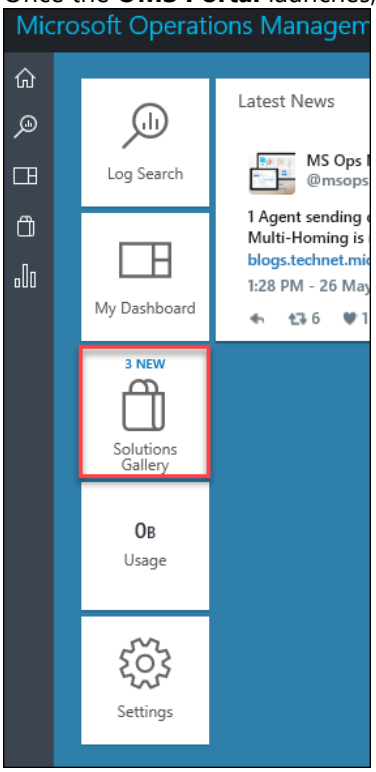
NAME	OMS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP
ADDC	Connecting	Windows	MSDN Platforms	IdentityTier
LitWareDC01	Connecting	Windows	MSDN Platforms	IdentityTier
LitWareDC02	Connecting	Windows	MSDN Platforms	IdentityTier
LitWareDC03	Connecting	Windows	MSDN Platforms	IdentityTier
LitWareDC04	Connecting	Windows	MSDN Platforms	IdentityTier

10. Repeat these steps to connect the SQL Servers.
11. Once the servers are connected, click on the **OMS Portal** icon or tile to launch the OMS Portal.



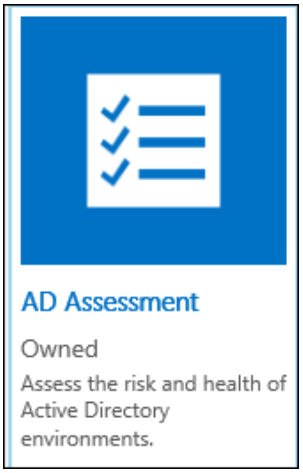


12. Once the **OMS Portal** launches, select the **Solutions Gallery** from the dashboard.

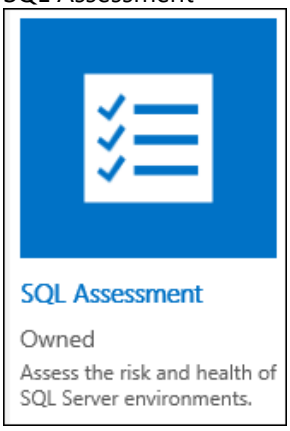


13. Add the following solutions from the **Solutions Gallery** by clicking the solution followed by the **Add** button for each:

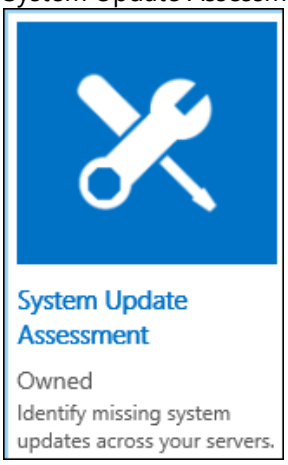
    a. AD Assessment



b. SQL Assessment



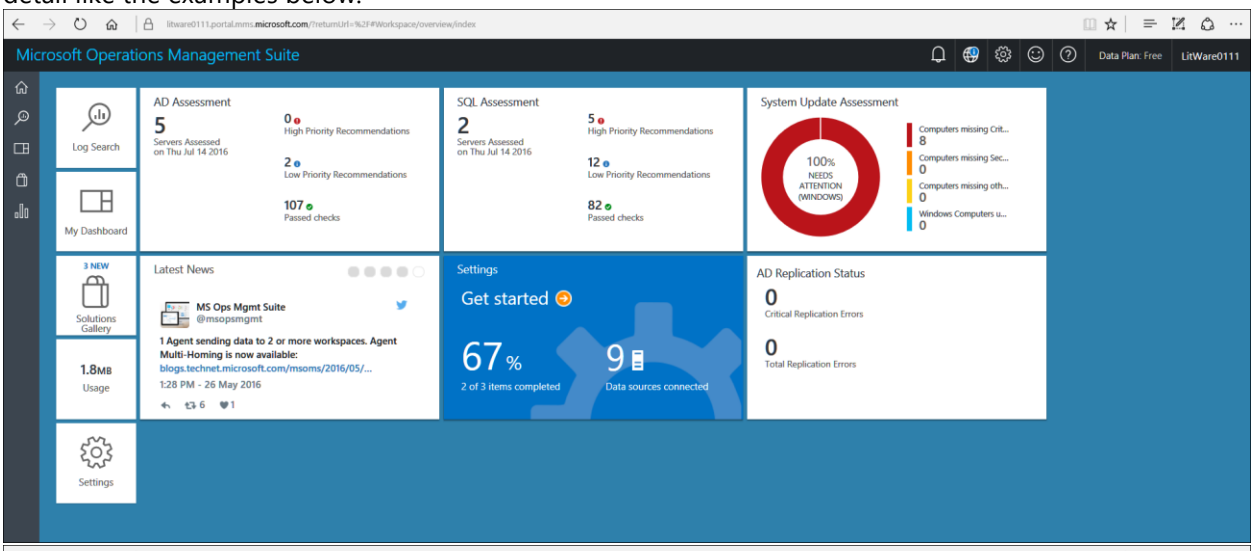
c. System Update Assessment

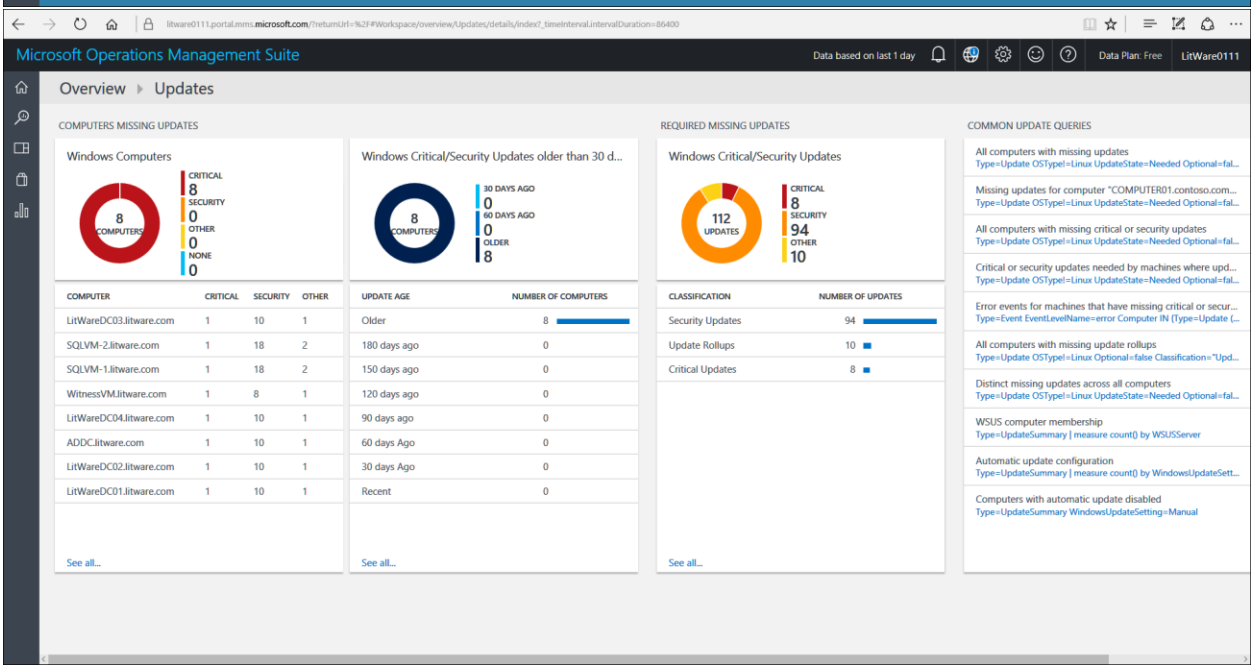


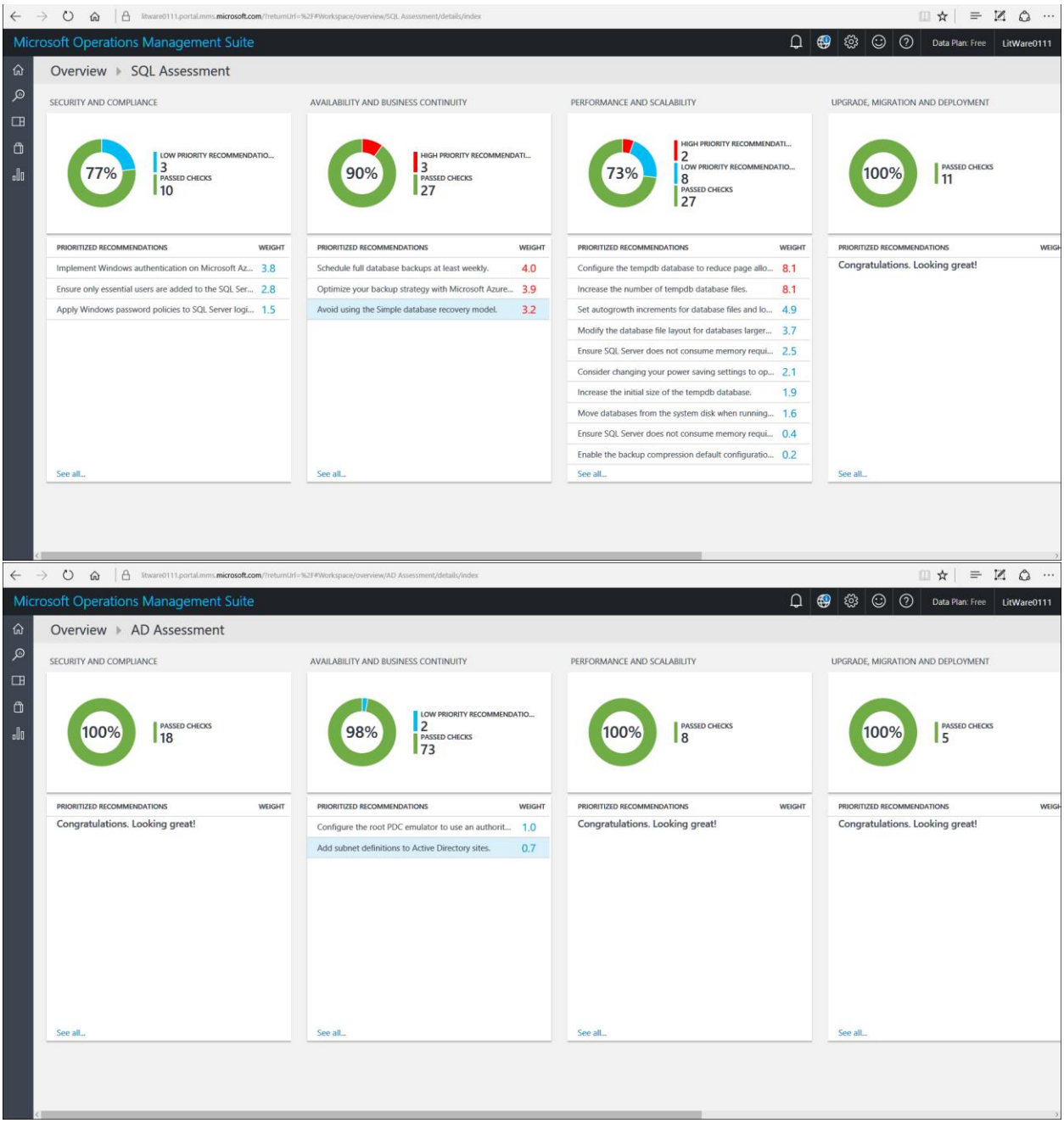
14. Make note of the other options that are available from the Gallery.

    Note: These assessments will begin. They will inform you it will take some time for these to be complete. Give these some time to complete as you perform other tasks. You may need to check them even after the hands-on lab is complete for data.

15. When the data has imported, the dashboard will look like the example below, and the assessments will provide detail like the examples below:

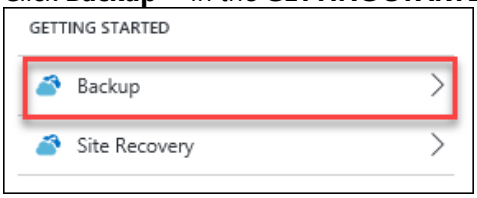




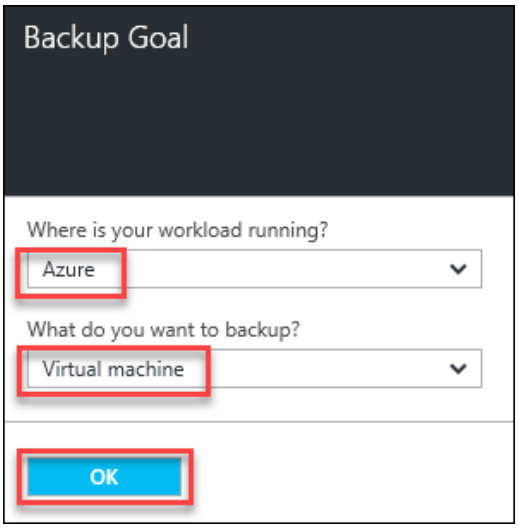


Task 3: Configure Backups of IaaS Servers in Vaults (Region 1 and 2)

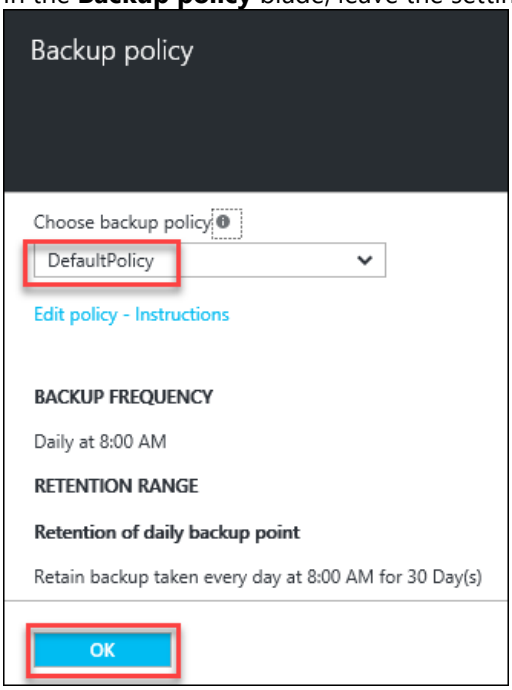
1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click on **LitwareVault1** on the Azure Portal Dashboard.
3. Click **Backup >** in the **GETTING STARTED** section.



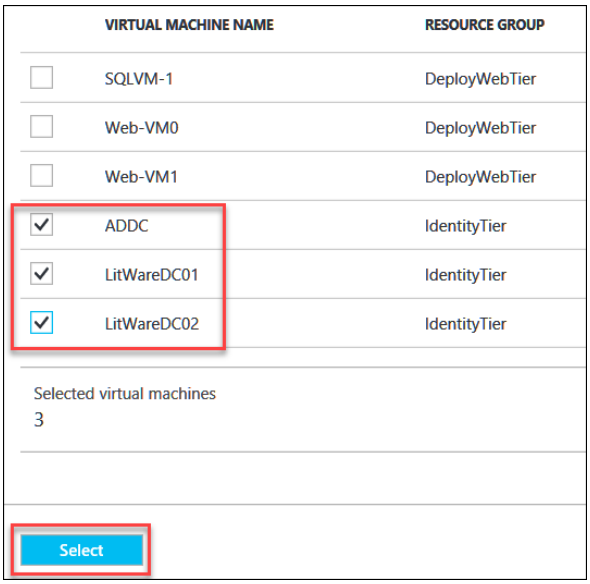
4. In the **Getting started with backup**, choose the **Backup Goal** of Azure and Virtual machine, and click **OK** to continue.



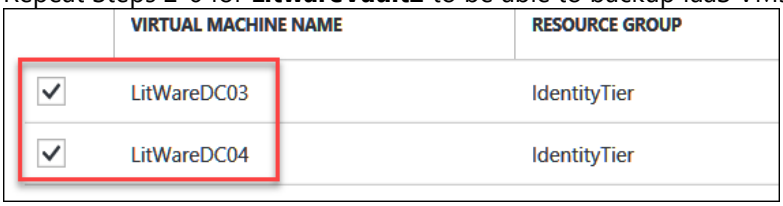
5. In the **Backup policy** blade, leave the settings at the DefaultPolicy, and click the **OK** button to continue.



6. In the **Select virtual machines**, select a few VMs to configure for backup with checkboxes, and click the **Select** button.

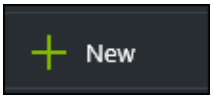


7. This will configure the machines to be backed up via Azure Backup in the **South Central US** region.
8. Repeat Steps 2-6 for **LitwareVault2** to be able to backup IaaS VMs in the **North Central US** region.



Task 4: Configure Network Security Groups as Needed (Region 1 and 2)

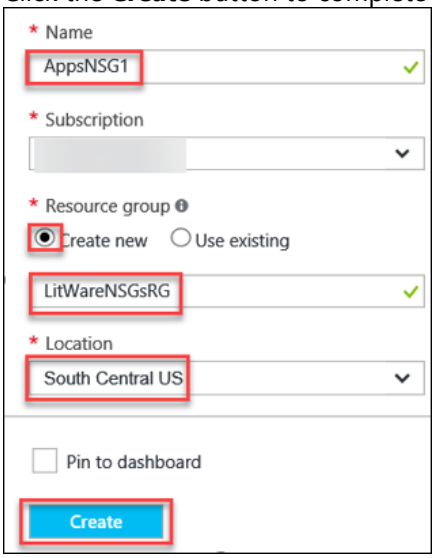
1. Browse to the Azure portal, and authenticate at https://portal.azure.com/.
2. Click **+ New**.



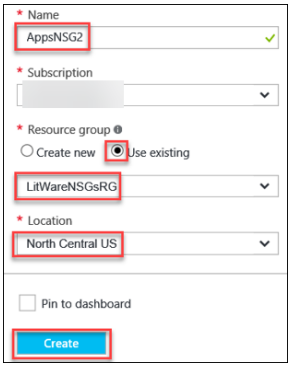
3. In the **Search the marketplace** window, type **Network Security Group** and hit Enter.
4. In the resulting **Everything** blade, choose **Network security group** by **Microsoft** as the publisher.

5. Leave the deployment model as **Resource Manager**, and click the **Create** button to continue.

6. In the **Settings** blade, enter the following:
    a. Name: **AppsNSG1**
    b. Subscription: **Select your subscription**
    c. Resource Group: **Create new – LitwareNSGsRG**
    d. Location: **South Central US**
    e. Click the **Create** button to complete the creation of the NSG.

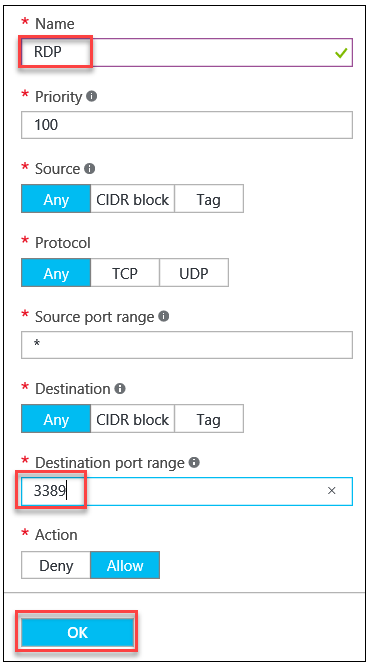


7. Repeat Steps 2-6 for **DataNSG1**, and **IdentityNSG1** both in **South Central US**. Be sure for Resource Group to **Use existing – LitwareNSGsRG**.
8. Now use the **Browse >** menu item in the left pane on the Azure Portal, type **Network security groups** in the filter bar, and select it from the results.
9. In the resulting blade, you will see all the NSGs for **Litware**. Click the **+ Add** icon to add the following:
    a. Name: **AppsNSG2**
    b. Subscription: **Select your subscription**
    c. Resource Group: **Use existing – LitwareNSGsRG**
    d. Location: **North Central US**
    e. Click the **Create** button to complete the creation of the NSG.



10. Repeat using the **+ Add** icon for **DataNSG2**, and **IdentityNSG2** both in **North Central US**. Be sure for Resource Group to **Use existing – LitwareNSGsRG**.

11. Click on each newly created NSG, and create an **Inbound security rule** for RDP. Below is an example rule for you to create for all six.



12. For both **AppsNSGs**, be sure to add another Rule to allow Internet traffic with the following settings or your CloudShop app will no longer work:

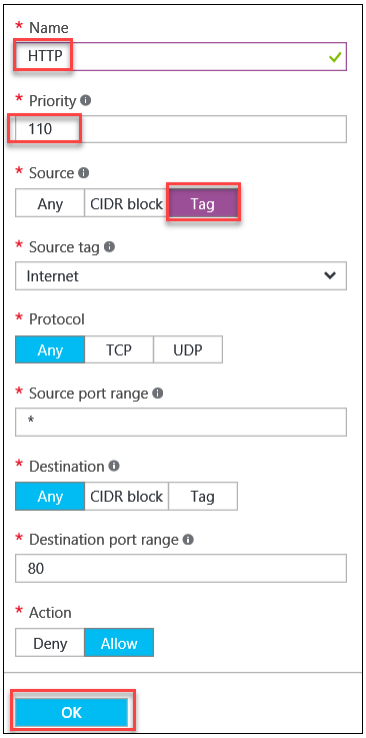
    a. Name: **HTTP**

    b. Priority: **110**

    c. Source: **Tag**

    d. Source Tag: **Internet**

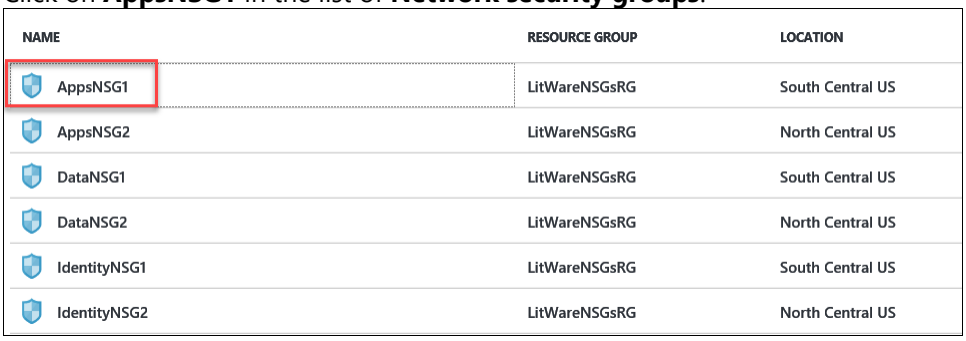
e. Leave all the others at the defaults, and click the **OK** button.



Note: While this is a live production, there would be more explicit rules created and assigned. This is just an example how to create them for this hands-on lab.

13. Now, assign the appropriate NSGs to the correct **Subnet** in each region.

14. Click on **AppsNSG1** in the list of **Network security groups**.

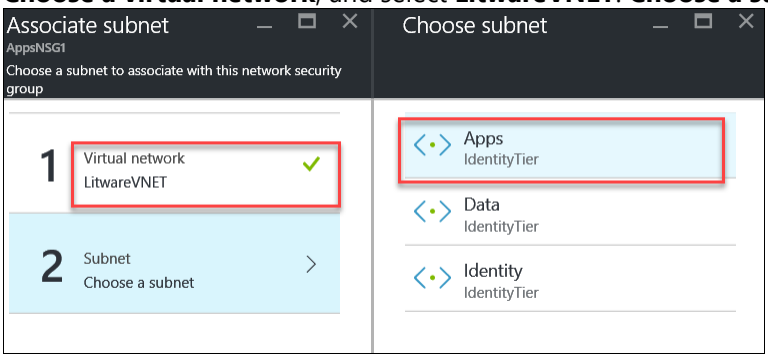


NAME	RESOURCE GROUP	LOCATION
AppsNSG1	LitWareNSGsRG	South Central US
AppsNSG2	LitWareNSGsRG	North Central US
DataNSG1	LitWareNSGsRG	South Central US
DataNSG2	LitWareNSGsRG	North Central US
IdentityNSG1	LitWareNSGsRG	South Central US
IdentityNSG2	LitWareNSGsRG	North Central US

15. Select **Subnets** from **Settings**.

16. Click on the **+ Associate** icon in the resulting **Subnet associations** blade.

17. **Choose a virtual network**, and select **LitwareVNET**. **Choose a subnet**, in this case, **Apps**.



18. Click the **OK** button to complete the association.
19. Repeat Steps 13-17 for **DataNSG1** and **IdentityNSG1.** Select the appropriate Subnet to associate them within **LitwareVNET**.
20. Repeat Steps 13-17 for **AppsNSG2**, **DataNSG2**, and **IdentityNSG2**. Select the appropriate Subnet to associate them with in **LitwareVNET2.**

Summary

In this exercise, you designed and created additional resiliency options in Azure. You deployed a Traffic Manager in Priority Mode, you configured Operations Management Suite and checked for missing patches. You also configured IaaS backups in both regions as well as configured Network Security Groups as needed.

After the hands-on lab

Duration: 10 minutes

Task 1: Delete the resource groups created

1. Within the Azure portal, click Resource Groups on the left navigation.
2. Delete each of the resource groups created in this lab by clicking them followed by clicking the Delete Resource Group button. You will need to confirm the name of the resource group to delete.

You should follow all steps provided *after* attending the hands-on lab.