## Microsoft Cloud Workshops

Building a Resilient IaaS Architecture Hackathon

Lab Guide

February 2017

© 2017 Microsoft Corporation. All rights reserved. This document is confidential and proprietary to Microsoft. Internal use only. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

### Contents

[Exercise 0: Environment setup 2](#_Toc473900584)

[Building a Resilient Infrastructure as a Service (IaaS) Hackathon 17](#_Toc473900585)

[Building a Resilient Infrastructure as a Service (IaaS) Hackathon Answers 25](#_Toc473900586)

### Scenario

Contoso has asked you to deploy their infrastructure in a resilient manner to attain an SLA from Microsoft.

### Requirements

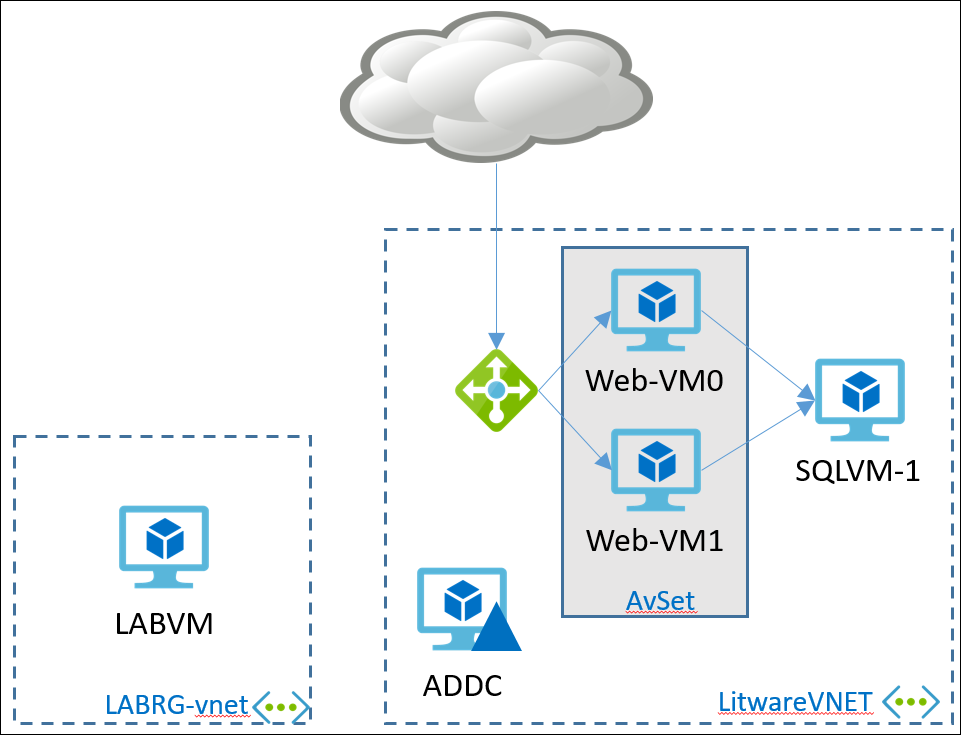
* Microsoft Azure subscription
* Local machine or a virtual machine configured with:
  + Visual Studio 2015 Community Edition Update 3
  + Azure SDK 2.9+ for Visual Studio
  + Azure PowerShell (installed as part of Azure SDK)
  + Reboot after installing the Azure SDK

### Lab overview and structure

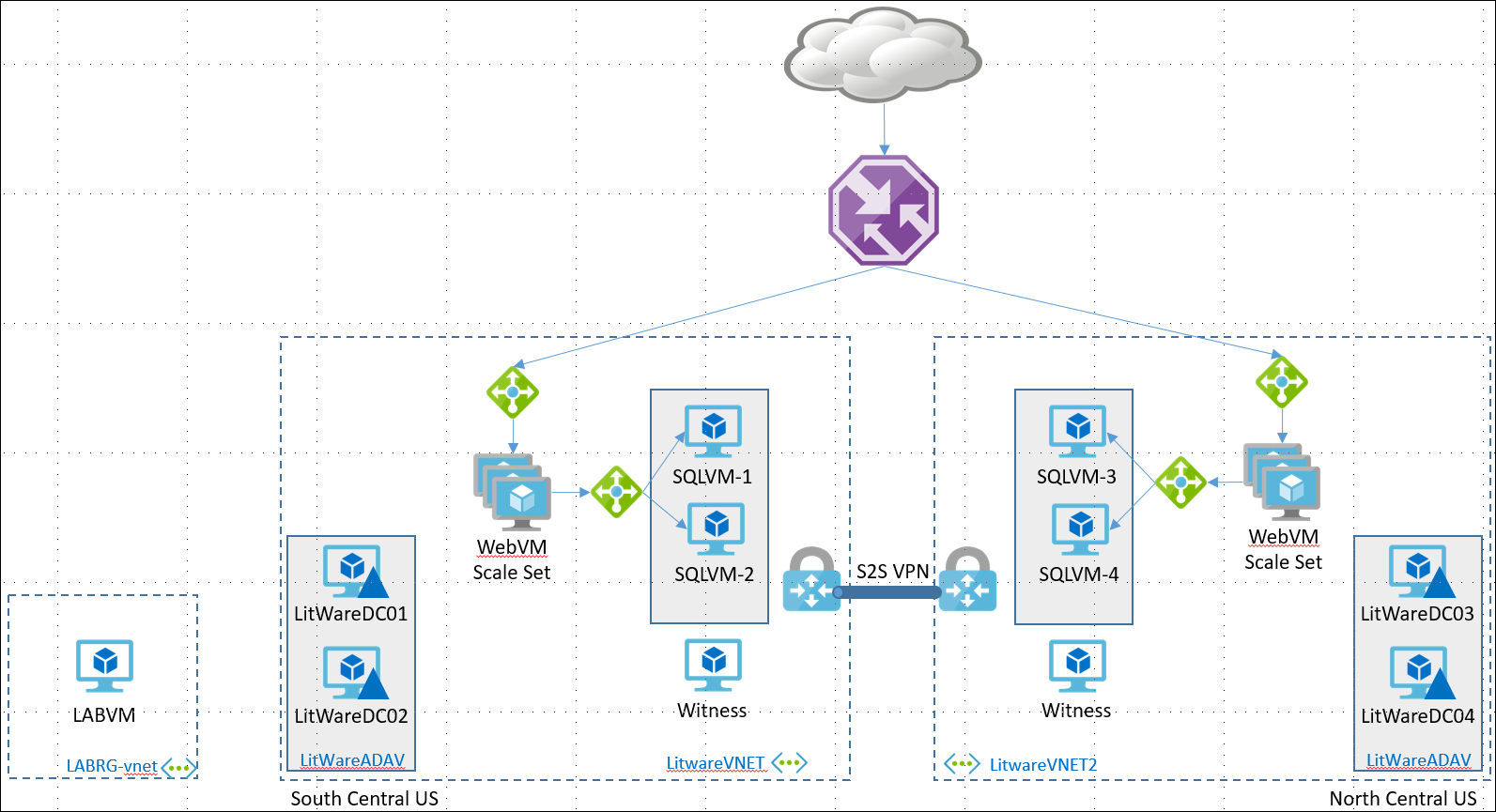
This lab simulates a customer environment which was poorly planned, and which lacks resilience. The goal of the lab is to expose you to the features in Azure that can help ensure a very resilient IaaS deployment.

We will begin by building the “sub-optimal” environment, which simulates what the customer deployed. We will use templates to make this part go a little faster. The remainder of the lab will be comprised of steps that will improve the resiliency of the initial ‘customer’ deployment.

After the template-based deployments, your environment will look like this diagram.



Once this entire lab is complete, the customer deployment will be highly available within a single region, and highly available across region. The design will look like the following diagram.



### Help references

|  |  |
| --- | --- |
| 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/> |

# Exercise 0: Environment setup

## Overview

In this lab, you will create an environment and download the required files for this course.

## Prerequisites

* Microsoft Azure subscription: <http://azure.microsoft.com/en-us/pricing/free-trial/>
* Client computer with Windows 7 or later with Visual Studio 2015 - SDK 2.9.+
  + Ensure you reboot after installing the SDK or Azure PowerShell will not work correctly

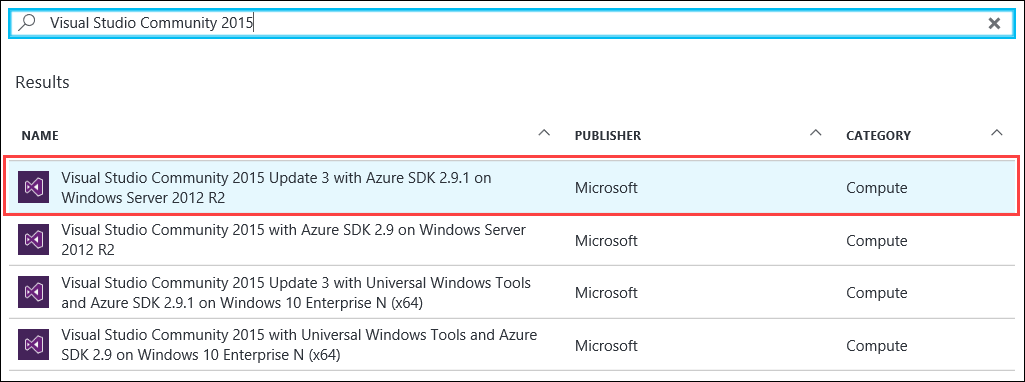
### Overview

In this exercise, you will prepare an Azure infrastructure that has a number of issues that need 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.

### Task 1: Configure a Development Environment

If you do not have a machine setup with Visual Studio 2015 Community and Azure SDK 2.9 complete this task.

1. Create a virtual machine in Azure using the Visual Studio Community 2015 Update 3 and SDK 2.9.+ on Windows Server 2012 R2 image.



It is *highly* recommended to use a DS2\_V2 or D2\_V2 instance size for this Virtual Machine (VM)

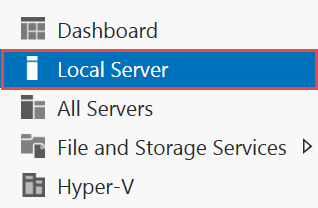
### Task 2: Disable IE Enhanced Security

Note: Sometimes this image has Internet Explorer (IE) Enhanced Security Configuration (ESC) disabled. Sometimes it does not.

1. On the new VM you just created, click the Server Manager icon.



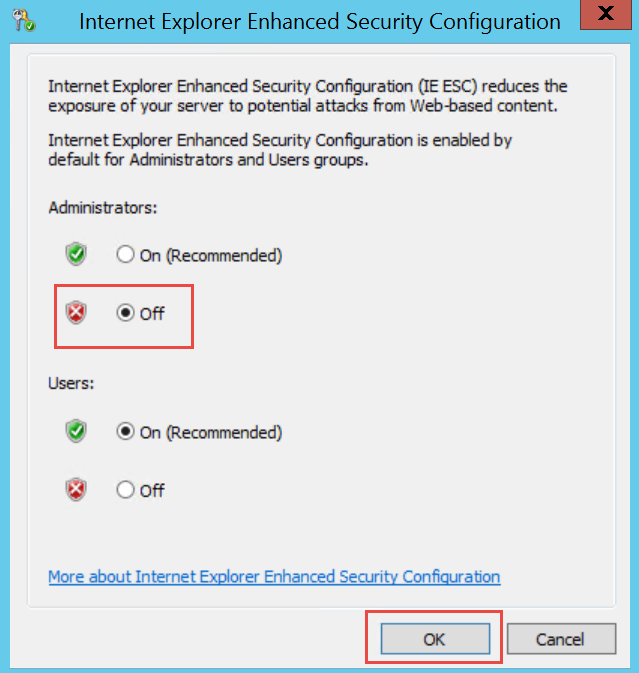
1. Click **Local Server**.



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

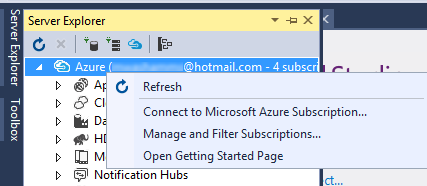


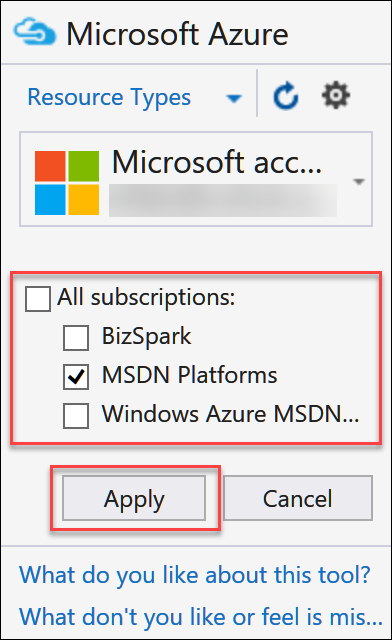
1. Change to **Off** for Administrators and click **OK**.



### Task 3: Validate Connectivity to Azure

1. From within the virtual machine, Launch Visual Studio 2015 and validate that 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 that you can connect to your Azure subscription.



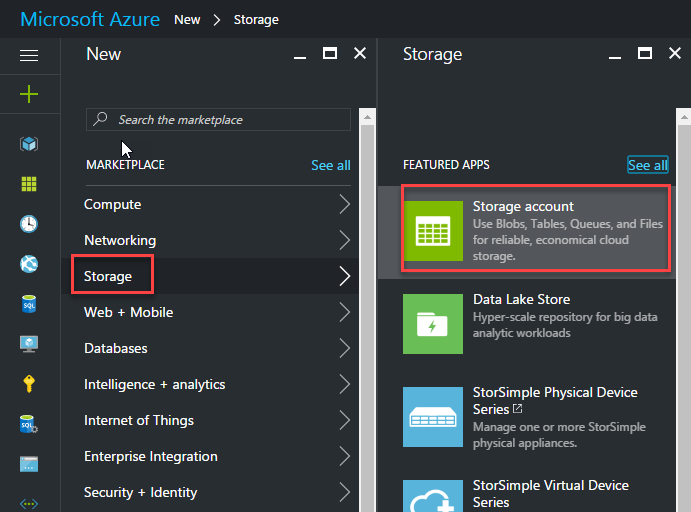
1. If you have multiple subscriptions or access to multiple subscriptions, be sure to select only the one where you want to deploy the hackathon environment.  
   

**Download the exercise files**

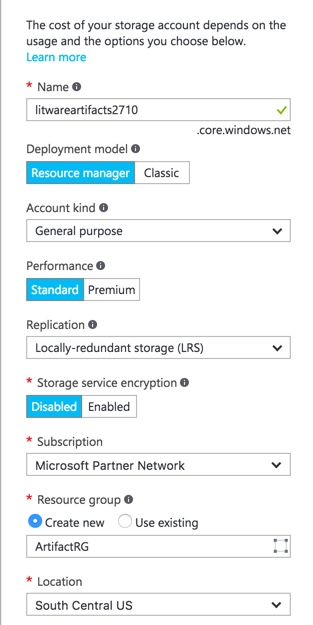
1. Download the exercise files for the training (from within the virtual machine).
   1. Create a new folder on your computer named **C:\Hackathon**
   2. Download the support files (.zip format), <https://opsgilityweb.blob.core.windows.net/cebootcamp-feb-2017/Building%20a%20Resilient%20IaaS%20Architecture%20-%20Hackathon%20-%20Student%20Files.zip> to the new folder.
   3. Extract the contents to the same folder.

### Task 4: 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**.



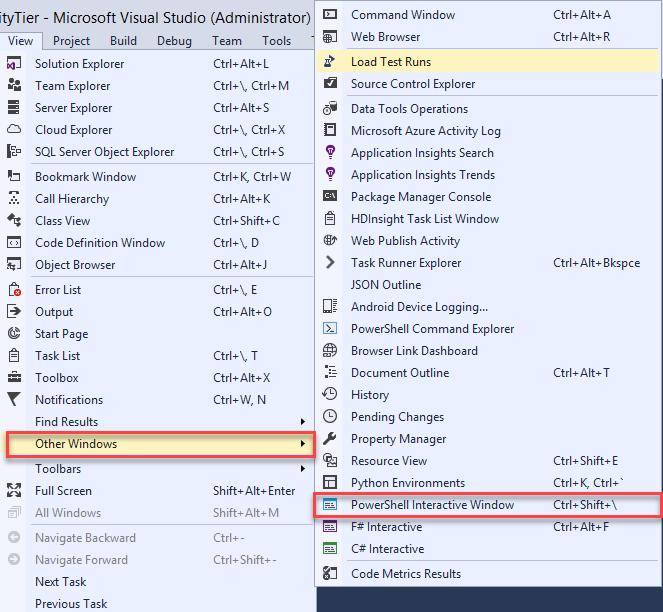
1. In the **Create storage account** blade, provide the following settings:
   1. Name: **litwareartifacts** (this name must be unique, so modify as appropriate)
   2. Replication: Change to **Locally-redundant storage (LRS)** via drop-down
   3. Resource Group: **Create new – ArtifactRG**
   4. Location: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

* 1. Click the **Create** button.  
     

1. This will allow for storing of the scripts that will be run in the following tasks.

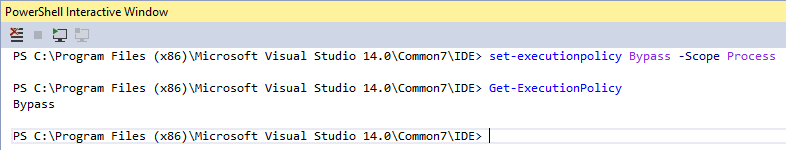
### Task 5: Run Script to create the Active Directory deployment

1. In Visual Studio, select **File | Open | Project/Solution** and then 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. Open **PowerShell Interactive Window** within Visual Studio.

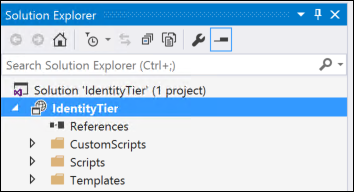


1. Run below commands to set PowerShell execution policy to bypass

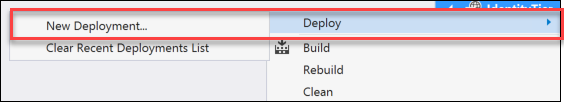
**set-executionpolicy Bypass -Scope Process**



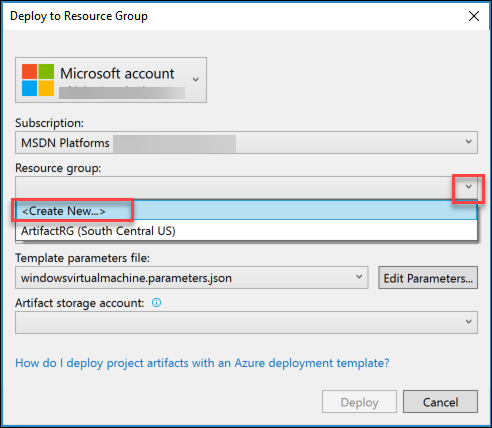
1. Once the Solution is open, right click on the name **IdentityTier** in Solution Explorer.



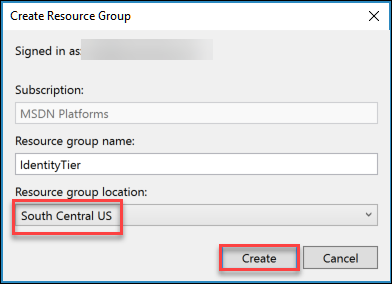
1. Now select **Deploy | New**.



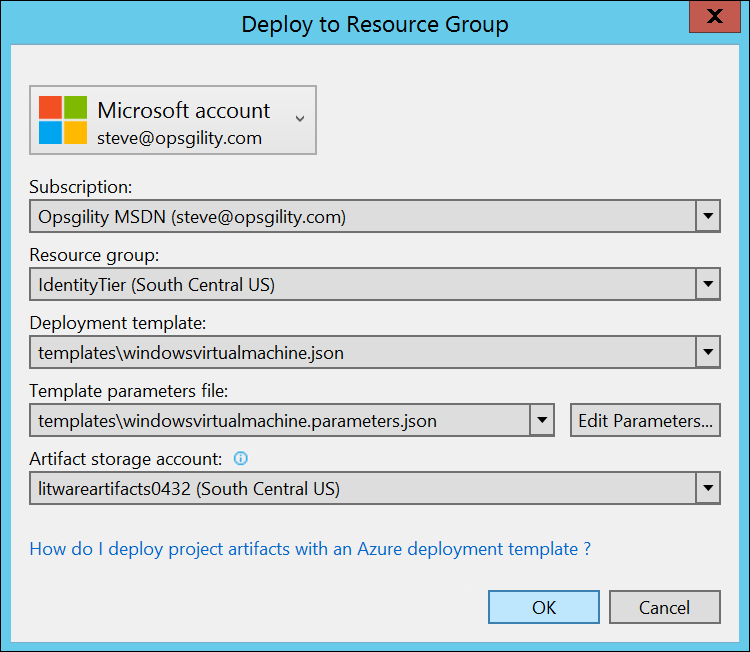
1. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New…>.** Name the new **Resource group “IdentityTier”.**



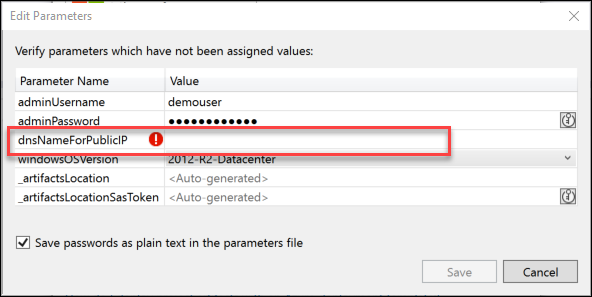
1. In the **Create Resource Group** window leave everything at the **Defaults** and choose a **Resource group location**. For our hackathon, let us choose **South Central US** then click the **Create** button to continue.



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



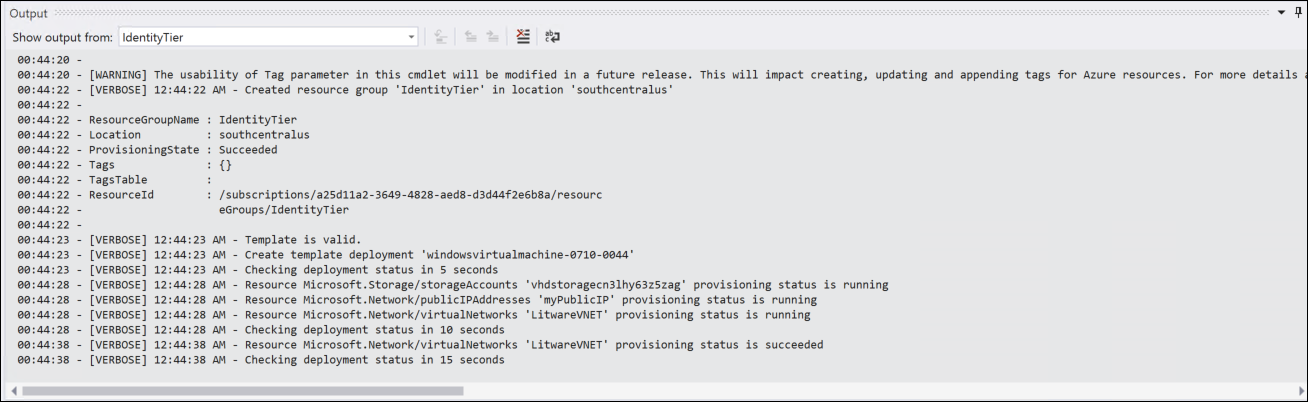
1. When prompted by the **Edit Parameters** window, enter a DNS name beside **dnsNameForPublicIP**, making sure it is comprised of letters (lower case) and/or numbers *only*. **If this name is not unique the deployment will fail**. An example name is: **addc0432**



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

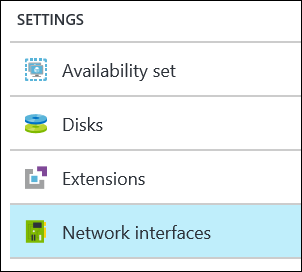


1. Monitor the output of the deployment in the **Output** window for success.

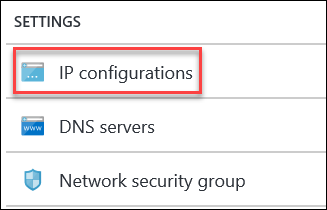


NOTE: This will take 20-25 minutes to deploy a Virtual Network, Storage Account, Subnets, other resources, and a domain controller Virtual Machine. It will also promote the DC as the primary DC for LitWare.com.

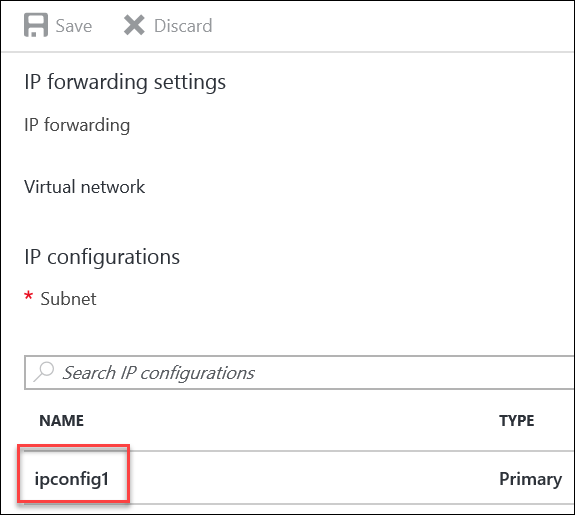
1. Before continuing to the next task, we need to change the DNS settings for the DC and the Virtual Network.
2. In the Azure portal, browse to **Virtual Machines** in the left-hand menu. Click the VM **ADDC** from the list of VMs.
3. In the **Settings** blade, click **Network Interfaces >** in the **SETTINGS** section.

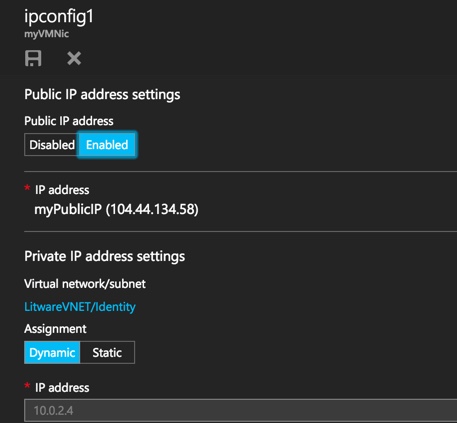


1. Click **myVMNic** to bring up the **Settings** for the **Network interface**. Then click on **IP configurations >** in the **SETTINGS** section.

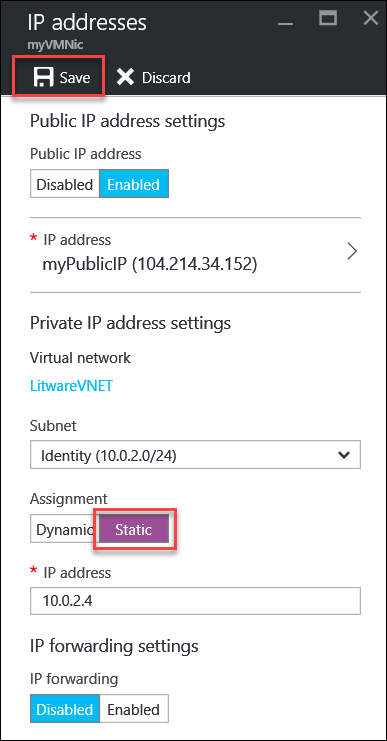


1. Click on **ipconfig1**

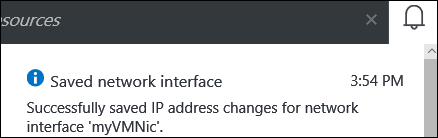




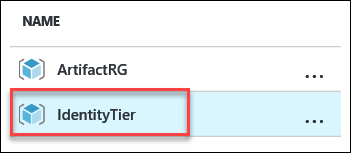
1. Change the **Assignment** to **Static** under the **Private IP address settings** and then click the **Save** icon to save the changes.



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

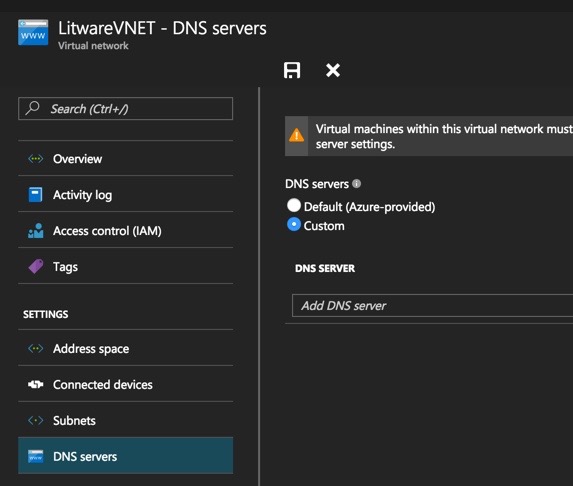


1. In the Azure portal, click on **Resource Groups** in the left hand menu. Click on the resource group named **IdentityTier** from the list of Resource Groups.

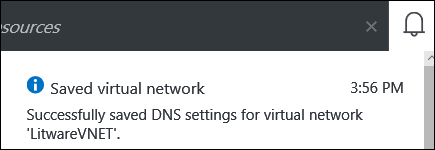


1. Click on **LitwareVNET** in the list of resources to open the VNET Resource.
2. In the **Settings** blade, click **DNS servers >** in the **SETTINGS** section.

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

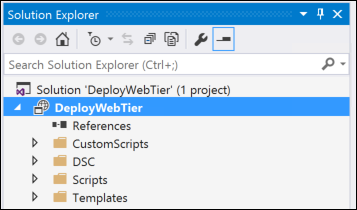


1. Once the Azure notification occurs for **Saved virtual network**, continue to the next task.

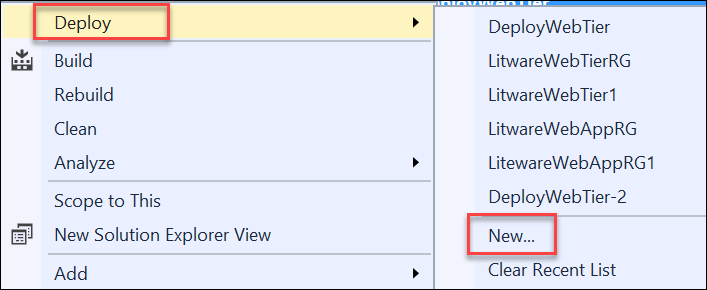


### Task 6: Run Script to create the SQL Database tier

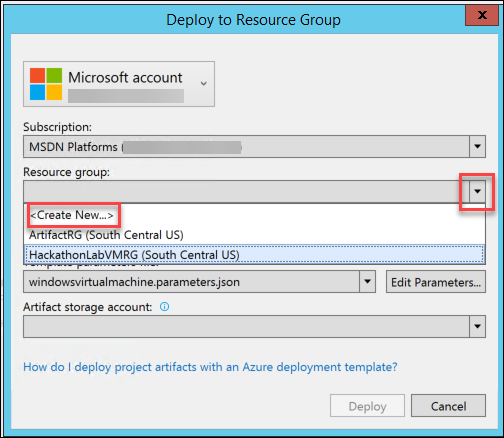
1. Go back to the remote desktop session (RDP session for your Development Environment VM.
2. In Visual Studio, select **File | Open | Project/Solution** and then browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **DeployWebTier** 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.



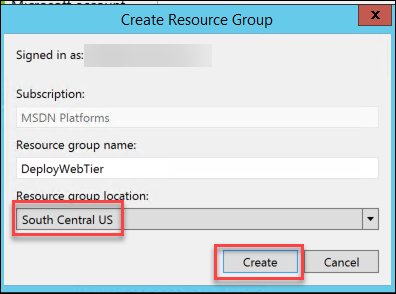
1. Now select **Deploy | New**.



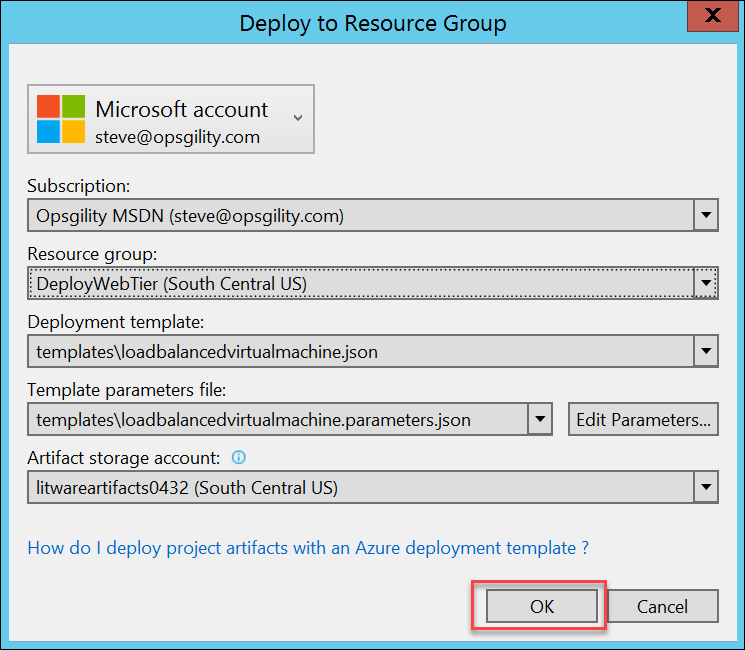
1. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New…>**.Name the new **Resource group “DeployWebTier”.**



1. In the **Create Resource Group** window leave everything at the **Defaults** and choose a **Resource group location**. For our hackathon, let us choose **South Central US** then click the **Create** button to continue.



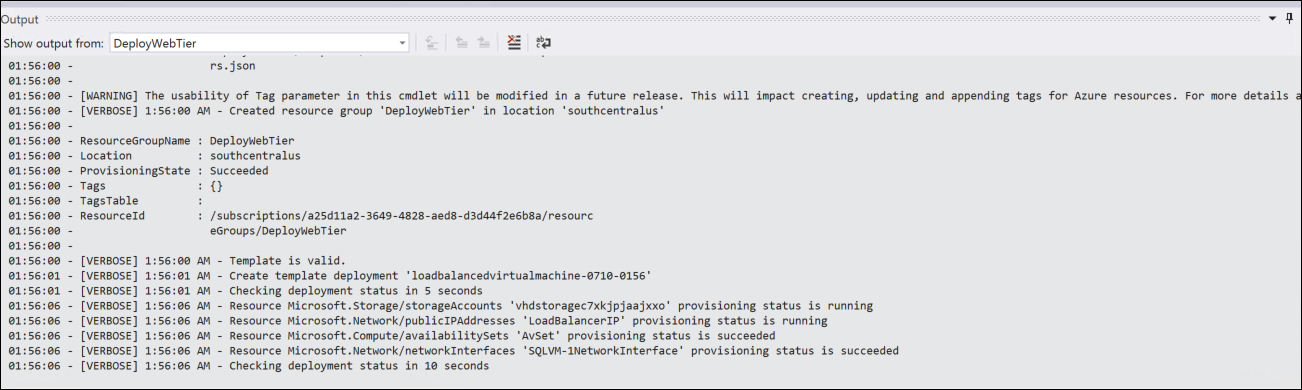
1. Back in the **Deploy to Resource Group** dialog, now choose the **Artifact storage account** that was created in the previous task. Then click **OK** to begin the deployment.



1. When prompted by the **Edit Parameters** window, enter a **LoadBlancerIPDnsName** making sure it is all lower-case and/or numbers. **The name must be unique or the deployment will fail**. An example name is **weblb0432**.

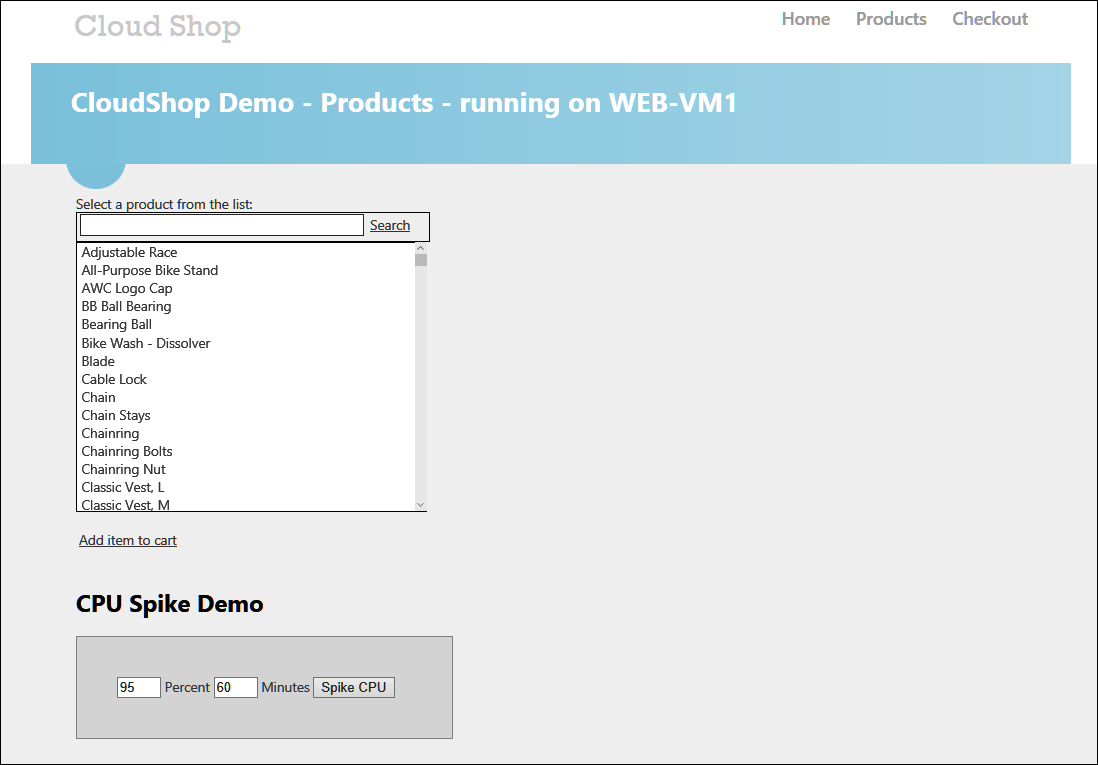


1. Monitor the output of the deployment in the **Output** window for success.



NOTE: This deployment provisions VMs for SQL Server, Web Servers, a Load Balancer, and configures IIS and SQL. 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 Hackathon.

1. Once deployment is successful, validate the deployment by browsing to the load balancer public IP address that was 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 Hackathon.

### Summary

In this exercise, you prepared an Azure infrastructure that has a number of issues that need 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.

# Building a Resilient Infrastructure as a Service (IaaS) Hackathon

## Exercise 1: Prepare the Infrastructure Region 2

In this exercise, you will design and create Infrastructure as a Service (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)

*Tasks to complete*

* Create a Virtual Network in a 2nd Region with subnets that mirror the original deployment in Region 1. Address Space: 172.16.0.0/16 with subnets for Apps, Data, and Identity.

*Exit criteria*

* Verify creation of the VNET with the correct address space. Verify the existence of the Apps, Data, and Identity subnets with correct address ranges.

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

*Tasks to complete*

* Create a Gateway subnet in the Virtual Network that was created in Task 1. This subnet should have the address range of 172.16.3.0/16.

*Exit criteria*

* Verify the creation of the fourth subnet in the VNET with an available number of IP addresses listed as 3.

### Task 3: Deploy VPN Gateway (Region 2)

*Tasks to complete*

* Create a VPN Gateway deployment in Region 2 to allow for Site-to-Site region connectivity between the virtual network in the original Region 1 and the newly created Virtual Network in Region 2.

*Exit criteria*

* You sign in to the portal and verify the creation and the successful deployment of a Virtual Network Gateway device. NOTE: This does take up to 45 minutes for deployment.

### Task 4: Create a Backup Vault (Region 2)

*Tasks to complete*

* Create a new Backup and Site Recovery (OMS) Recovery Services Vault in the new Region 2 to allow IaaS virtual machines to be configured for backup into the vault.

*Exit criteria*

* You sign in to the portal and verify creation of the recovery services vault in Region 2. Additional verification will occur in a later task when IaaS VMs are configured for backup within this region.

## Exercise 2: Resilient Infrastructure Options Region 1

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: Add Gateway subnet to existing VNET (Region 1)

*Tasks to complete*

* Create a Gateway subnet in the Virtual Network that was created in Prerequisite Task 5. This subnet should have the address range of 10.10.3.0/16.

*Exit criteria*

* You sign in to the portal and verify creation of the fourth subnet in the VNET with an available number of IP addresses listed as 3.

### Task 2: Deploy VPN Gateway (Region 1)

*Tasks to complete*

* Create a VPN Gateway deployment in Region 1 to allow for Site-to-Site region connectivity between the virtual network in the original Region 1 and the newly created Virtual Network in Region 2.

*Exit criteria*

* You sign in to the portal and verify creation and the successful deployment of a Virtual Network Gateway device. NOTE: This does take up to 45 minutes for deployment.

### Task 3: Create a Backup Vault (Region 1)

*Tasks to complete*

* Create a new Backup and Site Recovery (OMS) Recovery Services Vault in Region 1 to allow IaaS virtual machines to be configured for backup into the vault.

*Exit criteria*

* You sign in to the portal and verify creation of the recovery services vault in Region 1. Additional verification will occur in a later task when IaaS VMs are configured for backup within this region.

### Task 4: Modify Load Balancer Settings (Region 1)

*Tasks to complete*

* Create a new HTTP Health Probe for the Load Balancer. Once it is created, change the existing Health Probe for TCP to a Health Probe for HTTP, and delete the TCP Probe.

*Exit criteria*

* You sign in to the portal and verify creation of the HTTP Health Probe and that it is now the Probe in use for the Load Balancer.

## Exercise 3: Build the DCs in for resiliency

In this exercise, you will design and create IaaS resiliency options in the additional region. You will create multiple Active Directory Domain controllers, add non-cached 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.

SLA’s for IAAS VM’s have been changed, with the ability to get a 99.9% SLA on single instance VM’s where they meet the following <https://azure.microsoft.com/en-us/blog/announcing-4-tb-for-sap-hana-single-instance-sla-and-hybrid-use-benefit-images/>, VM’s using premium storage will not be provided with a 99.9% SLA

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

*Tasks to complete*

* Deploy two Windows Server 2012 R2 virtual machines as two additional DCs in Region 1. These need to be deployed into an Availability Set that is created so there is resiliency for the DCs.

*Exit criteria*

* Verify two VMs deployed into an Availability Set in Region 1 that will be used for resilient servers once configured in the following tasks.

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

*Tasks to complete*

* Deploy two Windows Server 2012 R2 virtual machines as two additional DCs in Region 2. These need to be deployed into an Availability Set that is created so there is resiliency for the DCs.

*Exit criteria*

* Verify two VMs deployed into an Availability Set in Region 2 that will be used for resilient servers once configured in the following tasks.

### Task 3: Add Data Disks to Active Directory domain controllers (Both Regions)

*Tasks to complete*

* A Data Disk needs to be added to each of the four DCs that were deployed (2 for South Central US and 2 for North Central US) with their Host Caching set to None to avoid Active Directory

*Exit criteria*

* Validate the creation of the Data Disks by checking in storage accounts under VHDs and looking for the Data Disks via name or checking under Disks in each VM to see that each of them contain a Data Disk with Disk Caching set to None.

### Task 4: Build a connection between the VPN Gateways

*Tasks to complete*

* Create a Connection between the two VPN Gateways (one in each region) with a Pre-Shared Key.
* Change the DNS Settings for the VNET in Region 2 to point to Custom DNS.

*Exit criteria*

* Under Connections in the Portal, verify the bi-directional connections (Region 1 to Region 2 and Region 2 to Region 1) are up and the status is Connected.
* Have DNS connectivity between VNETs.

### Task 5: Format Data Disks on DCs and configure DNS settings across connection

*Tasks to complete*

* RDP into each of the four domain controllers and launch Storage Spaces to initialize and format the Data Disk as Drive F:\ for storage of the SYSVOL and NTDS folders.

*Exit criteria*

* In the RDP session of each domain controller, make sure in Explorer that the F:\ drive is formatted and visible.

### Task 6: Promote DCs as Additional domain controllers (Both Regions)

*Tasks to complete*

* Run a Custom Script Extension (script provided) to promote the four VMs to domain controllers in the LitWare.com forest.

*Exit criteria*

* In the portal under Extensions for each of the VMs, see that the CustomScriptExtension provisioned successfully.
* Additionally, RDP into any DC and see in Active Directory Users and Computers that there are now 5 DCs under the domain controller OU.

## Exercise 4: Build Web Tier and SQL for resiliency

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

Task 1: Deploy SQL Always On cluster (Region 1)  
*Tasks to complete*

* Run a template in Visual Studio (template provided) to deploy the SQL Always-On infrastructure.
* Configure the SQL Always-On cluster manually.

*Exit criteria*

* Verify the template deployed successfully by checking the VMs and the resource group in the portal.
* Verify that you have configured the Always-On cluster per the configuration steps.

### Task 2: Deploy Web Tier Scale Set (Region 1)

*Tasks to complete*

* Run a template (template provided) to create a Web Scale Set.
* Configure the database for use by the scale set.

*Exit criteria*

* Verify the template succeeded in running via the portal and view the scale set resources.
* Verify CloudShop works with the scale set.
* Spike the CPU for 15 minutes to watch the scale set deploy additional web servers.

### Task 3: Deploy SQL Always On cluster (Region 2)

*Tasks to complete*

* Run a template in Visual Studio (template provided) to deploy the SQL Always-On infrastructure.
* Configure the SQL Always-On cluster manually to be a secondary for Region 1.

*Exit criteria*

* Verify the template deployed successfully by checking the VMs and the resource group in the portal.
* Verify that you have configured the Always-On cluster per the configuration steps.

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

*Tasks to complete*

* Run a template (template provided) to create a Web Scale Set.
* Configure the database for use by the scale set in Region 2.

*Exit criteria*

* Verify the template succeeded in running via the portal and view the scale set resources.
* Verify CloudShop works with the scale set.
* Spike the CPU for 15 minutes to watch the scale set deploy additional web servers.

## Exercise 5: Prepare other resources for resiliency

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

### Task 1: Create Traffic Manager in Priority Mode

*Tasks to complete*

* Create a new Traffic Manager and set the Algorithm for the Routing method as Priority. Create Endpoints connected to Public IP addresses to the load balancers in each region for the Web Servers.

*Exit criteria*

* You sign in to the portal and verify creation of the Traffic Manager node. Then browse to the Traffic Manager DNS name making sure that the Web Site can still be accessed and viewed.

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

*Tasks to complete*

* Create a new Log Analytics OMS Portal from within Azure. Add AD Assessment, SQL Assessment, and System Update Assessment Solutions from the Gallery.

*Exit criteria*

* You sign in to the portal and verify creation OMS Portal creation. In addition, you sign in to the OMS Portal and check the results of the Assessments added for information.

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

*Tasks to complete*

* Using the Recovery Services Vaults created in a previous task, configure a few IaaS VMs for Default Backup options in each region.

*Exit criteria*

* You sign in to the portal and verify that there are servers configured to be backed up by the DefaultPolicy in each Vault by seeing the number of Backup items/Azure VM Backup set to the number of servers that were configured.

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

*Tasks to complete*

* Configure six Network Security Groups, one for each of the three subnets in both regions.
* Assign the appropriate NSG to the Identity subnet, the Apps subnet, and the Data subnet.

*Exit criteria*

* You validate the NSGs are assigned to the subnets via the portal and all traffic is continuing to flow per the rules.

# Building a Resilient Infrastructure as a Service (IaaS) Hackathon Answers

## Overview

This portion of the lab is designed to help you if you are blocked or have limited experience with Azure Resource Manager.

**Note:** **This section assumes you have carried out the steps under Exercise 0: Environment Setup on page 2 of this lab guide.** **The following exercises will not work properly until all of Exercise 0 has been completed.**

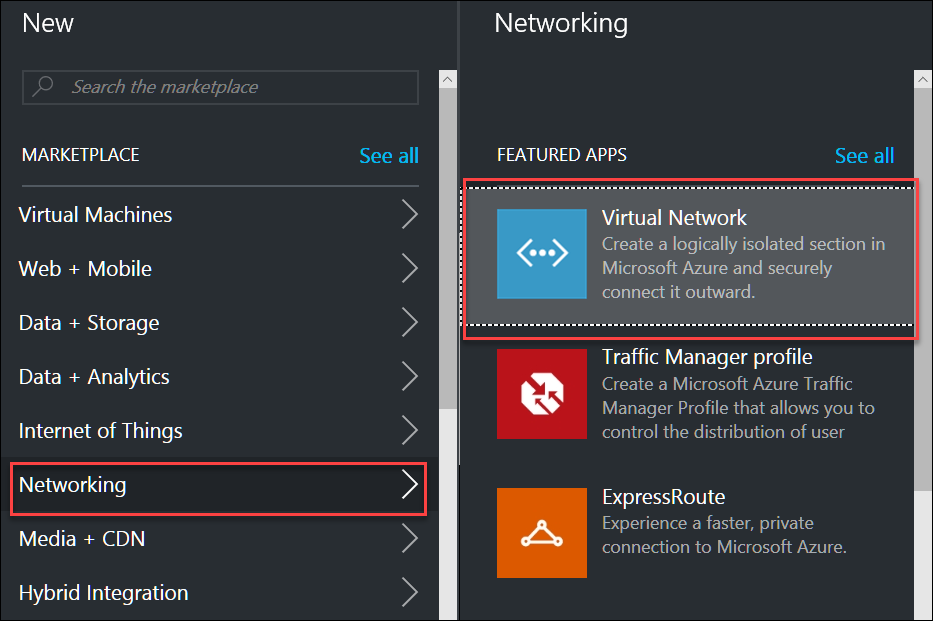
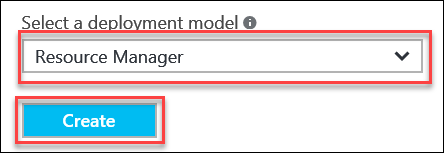
The goal of this lab is to improve on the resiliency of the “sub-optimal” initial customer deployment. You will design and create IaaS resiliency options by provisioning the web application and AD DCs in an additional Azure region. This will help provide protection from a regional outage.

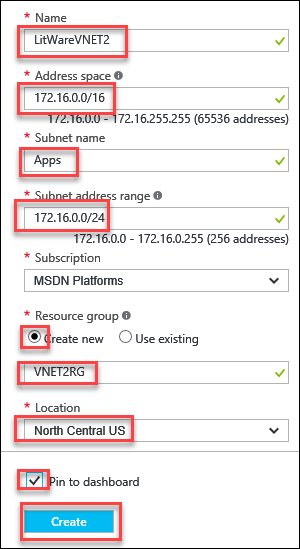
## Exercise 1: Prepare the Infrastructure Region 2

### Overview

In this exercise, you will create a Virtual Network with subnets, a Gateway subnet, a VPN Gateway, and a Backup Vault, all within a new Azure region.

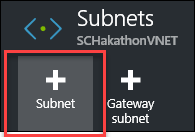
### Task 1: Create a Virtual Network for the Azure Infrastructure (Region 2)

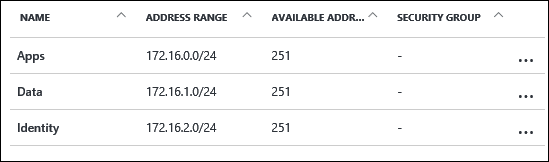
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. In the left pane, click **+ New**.  
   
3. In the **New** blade, select **Networking >** and then **Virtual Network**.  
     
   
4. In, the **Select a deployment model** drop-down, leave the choice as **Resource Manager** and then click **Create**.  
     
   
5. For the **Create virtual network** settings, enter the following information:
   1. Name: **LitWareVNET2**
   2. Address space: **172.16.0.0/16**
   3. Subnet name: **Apps**
   4. Subnet address range: **172.16.0.0/24**
   5. Subscription: **Choose your subscription**
   6. Resource group: **Create new – VNET2RG**
   7. Location: **North Central US**
   8. Pin to dashboard: **Check the checkbox**
   9. Click the **Create** button to continue.



1. Once the deployment is complete, add two more subnets to the VNET. To do this, select the **Subnets** icon in the **Settings** blade under the **SETTINGS** heading.



1. Click the **+ Subnet** option and enter the following settings:   
   
   1. Name: **Data**
   2. Address range (CIDR block): **172.16.1.0/24**
   3. Click the **OK** button to add this subnet.
2. Once the subnet is created successfully, repeat the above step for an **Identity** subnet with the following settings:
   1. Name: **Identity**
   2. Address range (CIDR block): **172.16.2.0/24**
   3. Click the **OK** button to add this subnet.
3. The subnets will look like this once complete:

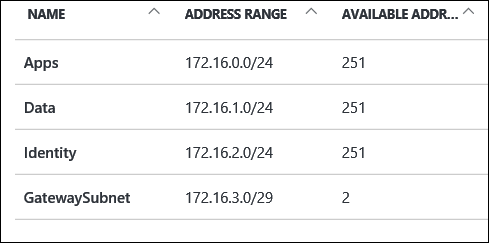


### Task 2: Add Gateway subnet to the VNET (Region 2)

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

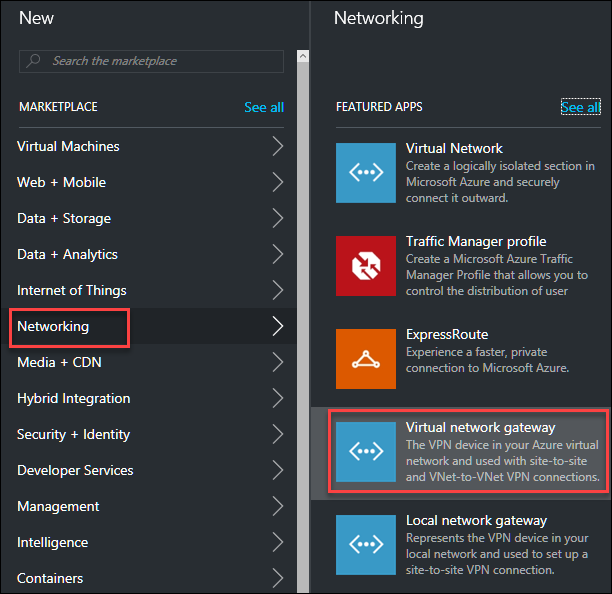


1. In the **Add subnet** blade, configure the following:
   1. Name: **GatewaySubnet (Default)**
   2. Address range (CIDR block): **172.16.3.0/29**
   3. Route table: **None**
   4. Click the **OK** button to add this subnet.
2. Once complete, you will see four subnets defined for **LitWareVNET2**.

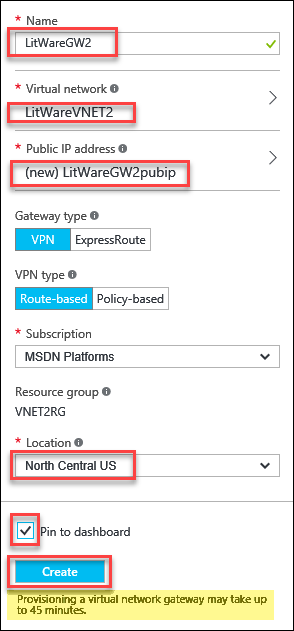


### Task 3: Deploy VPN Gateway (Region 2)

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.



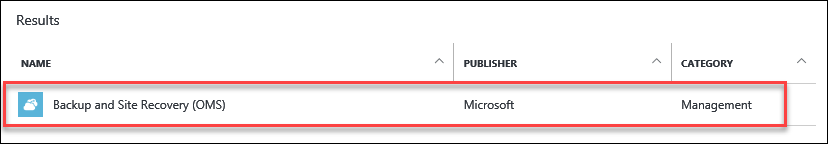
1. In the settings for **Create virtual network gateway**, enter the following:
   1. Name: **LitWareGW2**
   2. Gateway type: **VPN**
   3. VPN type: **Route-based**
   4. SKU: **Standard**
   5. Virtual network: **LitWareVNET2**
   6. Public IP address: **Choose a public IP address, + Create new, LitWareGW2pubip**
   7. Subscription: **Select your subscription**
   8. Resource group: **VNET2RG (Default)**
   9. Location: **North Central US**
   10. Pin to dashboard: **Check the checkbox**
   11. Click the **Create** button to deploy the VPN Gateway.



NOTE: This will take up to 45 minutes to deploy. Continue with the following steps while waiting on the deployment to complete.

### Task 4: Create a Backup Vault (Region 2)

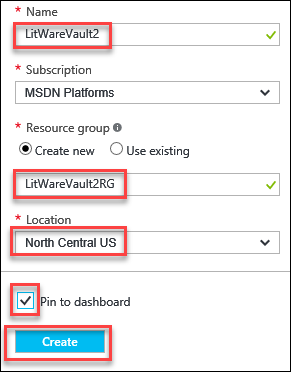
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click **+ New**.
3. In the **Search the marketplace** window, type **Backup and Site Recovery (OMS)** then hit enter.
4. In the resulting **Everything** blade, choose **Backup and Site Recovery (OMS)**, and then click the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



1. In the **Recovery Services vault** configuration blade, enter the following settings:
   1. Name: **LitWareVault2**
   2. Subscription: **Select your subscription**
   3. Resource group: **Create new – LitWareVault2RG**
   4. Location: **North Central US**

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

* 1. Pin to dashboard: **Check the checkbox**
  2. 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

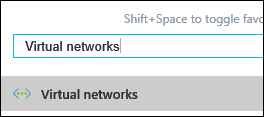
### Overview

In this exercise, you design and create IaaS resiliency options for the sub-optimal customer deployment in the first region (deployed via template).

### 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 **Browse >** menu item in the left pane and typing **virtual networks** in the filter.





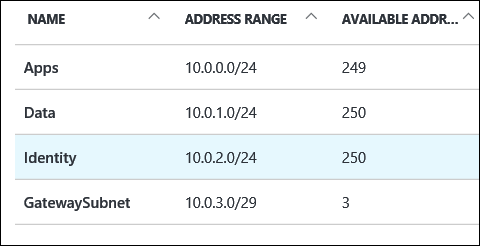
1. Select **LitwareVNET** from the list of networks.



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

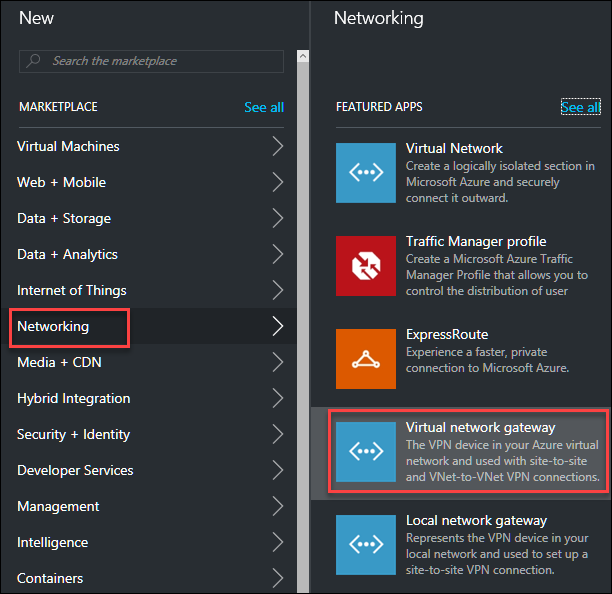


1. In the **Add subnet** blade, configure the following:
   1. Name: **GatewaySubnet (Default)**
   2. Address range (CIDR block): **10.0.3.0/29**
   3. Route table: **None**
   4. Click the **OK** button to add this subnet.
2. Once complete, you will see four subnets defined for **LitwareVNET**.



### Task 2: Deploy VPN Gateway (Region 1)

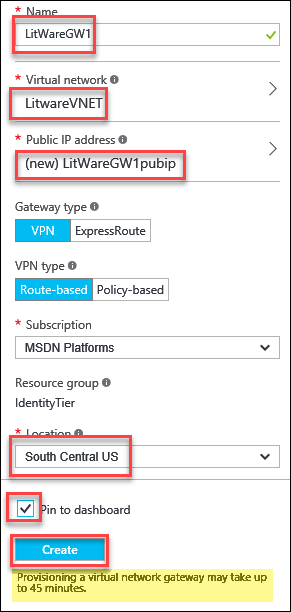
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click **+ New**.
3. Select **Networking > Virtual Network Gateway** from the choices.



1. In the settings for **Create virtual network gateway**, enter the following:
   1. Name: **LitWareGW1**
   2. Gateway type: **VPN**
   3. VPN type: **Route-based**
   4. SKU: **Standard**
   5. 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.

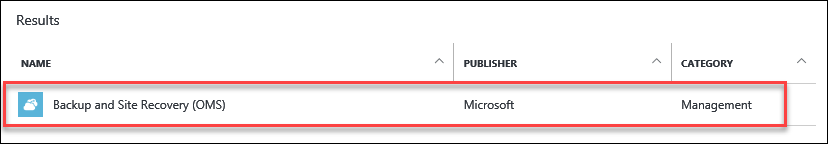
* 1. Public IP address: **Choose a public IP address, + Create new, LitWareGW1pubip**
  2. Subscription: **Select your subscription**
  3. Resource group: **IdentityTier (Default)**
  4. Location: **South Central US**
  5. Pin to dashboard: **Check the checkbox**
  6. Click the **Create** button to deploy the VPN Gateway.



NOTE: This will take up to 45 minutes to deploy. Continue with the following steps while waiting on the deployment to complete.

### Task 3: Create a Backup Vault (Region 1)

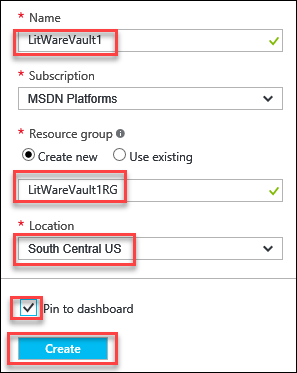
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click **+ New**.
3. In the **Search the marketplace** window, type **Backup and Site Recovery (OMS)** then hit enter.
4. In the resulting **Everything** blade, choose **Backup and Site Recovery (OMS)**, and then click the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



1. In the **Recovery Services vault** configuration blade, enter the following settings:
   1. Name: **LitWareVault1**
   2. Subscription: **Select your subscription**
   3. Resource group: **Create new – LitWareVault1RG**
   4. Location: **South Central US**

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

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

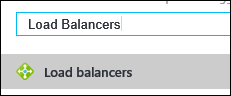


### Task 4: Modify Load Balancer Settings (Region 1)

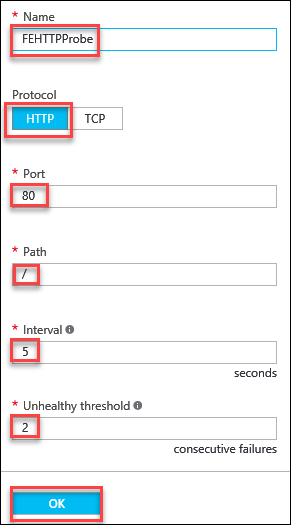
The customer had already deployed a load balancer in front of their web server, but we will make changes to optimize the configuration. The currently configured health probe uses TCP, but the Azure load balancer has an HTTP probe which will perform an application level health check. After we create the new health probe, we will assign it to the load balancer.

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.

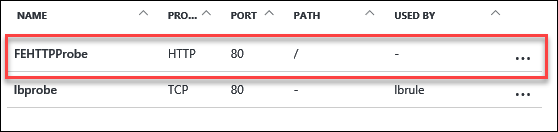




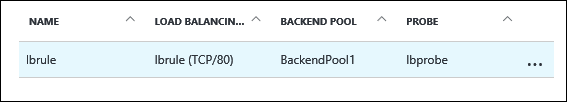
1. Find **WebLoadBalancer** on the list and click it to open the settings.
2. In the **Settings** blade for **WebLoadBalancer**, select **Health** **Probes >** under the **Settings** heading.
3. Click **+ Add** to add another probe.
4. For the **Add probe** settings, enter the following:
   1. Name: **FEHTTPProbe**
   2. Protocol: **HTTP**
   3. Port: **80**
   4. Path: **/**
   5. Interval: **5**
   6. Unhealthy threshold: **2**
   7. Click the **OK** button to continue.



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



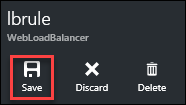
1. Go back to the **Settings** blade for the load balancer and select **Load balancing rules >** under the **Settings** heading.
2. Select the **lbrule**.



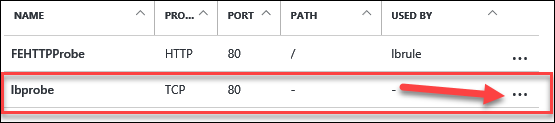
1. In the settings, change the **Probe** from the **lbprobe** to the newly created **FEHTTPProbe** via the drop-down selection.

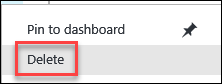


1. After doing this, click the **Save** icon to save the changes.

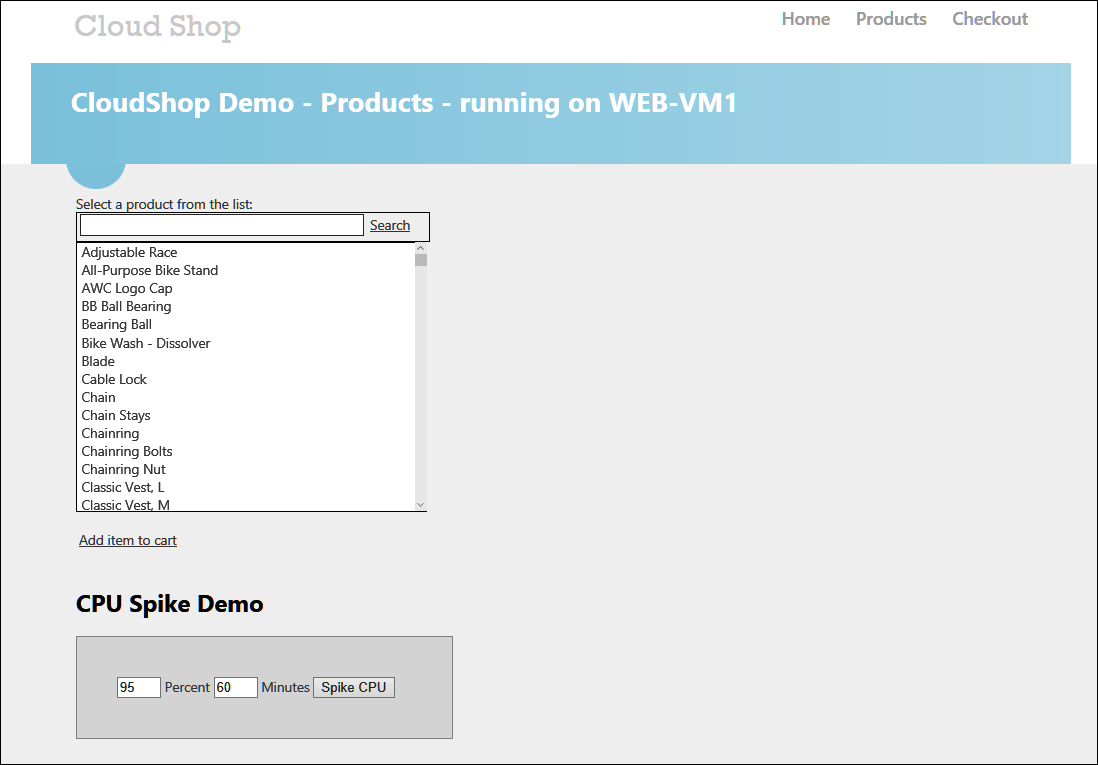


1. Once the Azure Notification for **Saved load balancer rule** appears, go back to the **Settings** blade for the load balancer and select **Health** **Probes >** under the **SETTINGS** heading.
2. Right click on the **…** (ellipsis) by the **lbprobe** and select **Delete** from the options. Select **Yes** to confirm the deletion.





* 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 improved the resiliency of the web site deployed in Azure by using a health probe that will validate the application’s health, rather than just that the TCP port is responding.

## Exercise 3: Build the DCs in for resiliency

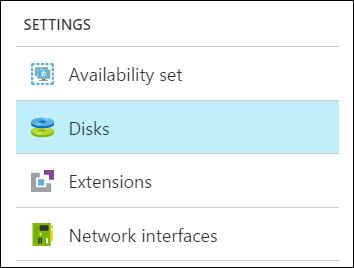
### Overview

In this exercise, you will improve the resiliency of the AD domain components deployed into Azure. You will create multiple Active Directory Domain controllers, add non-cached 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.

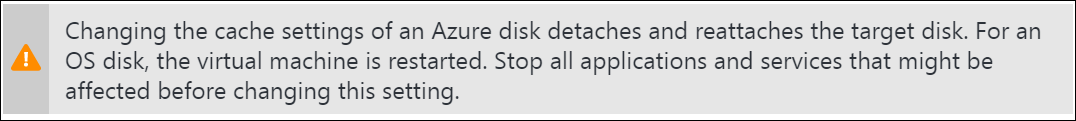
### Task 1: Create Resilient Active Directory Deployment (Region 1)

Read/Write caching is enabled on VM disks by default. Caching options like this can cause corruption of the ADDS database files.

1. Turn of disk caching on the OS disk for ADDC to avoid corruption of AD Data. To do this, perform the followings steps:
   1. Select **Virtual machines** in the left menu pane of the Azure portal.
   2. Click on **ADDC** and in the **Settings** blade, select **Disks >** under the **SETTINGS** heading.



* 1. Click on **osdisk** to view the properties.
  2. Then change the **Host caching** from **Read/Write** to **None** via the drop-down option.
  3. Notice the warning message. This action will impact the availability of the VM because the disk is detached and reattached with the new cache settings. In the case of an OS disk, the VM is also restarted. Be certain to perform this action during a maintenance window.



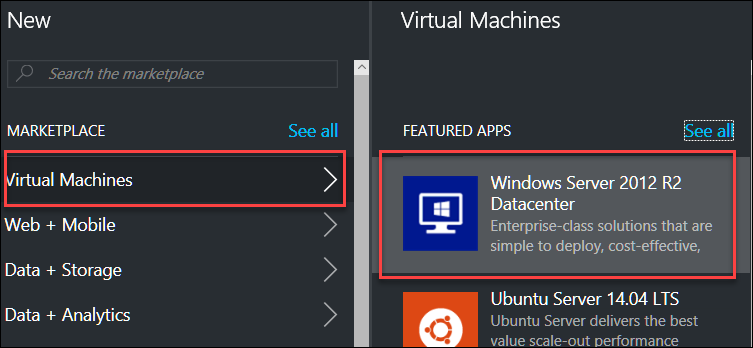
* 1. Click the **Save** icon to save the change.



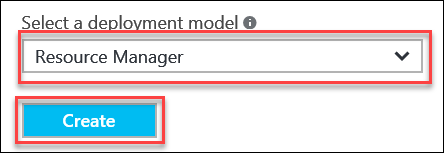
1. We will now create a new VM to function as a domain controller. In the left pane, click **+ New**.



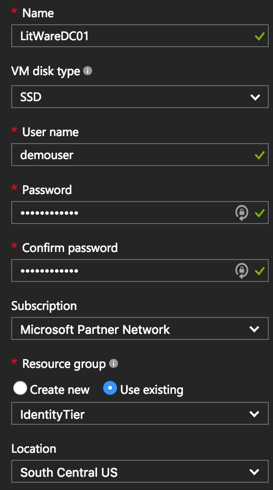
1. In the **New** blade, select **Compute** and then **Windows Server 2012 R2 Datacenter**.



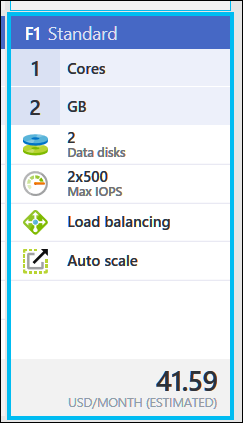
1. In, the **Select a deployment model** drop-down, leave the choice as **Resource Manager** and then click **Create**.



1. In the **Create virtual machine** blade, enter the **Basics** information:
   1. Name: **LitWareDC01**
   2. VM Disk type: **HDD**
   3. Username: **demouser**
   4. Password: **demo@pass123**
   5. Confirm password: **demo@pass123**
   6. Subscription: **Select your subscription**
   7. Resource group: **Use existing – IdentityTier**
   8. Location: **South Central US**
   9. Click the **OK** button to continue to **Size**.



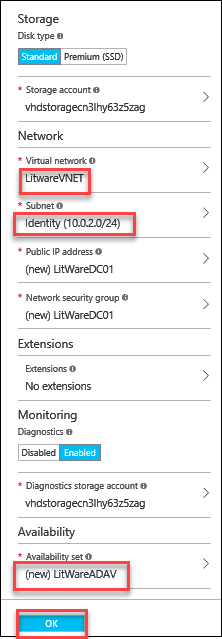
1. For the **Size**, select **F1 Standard**. You may have to select the **View All** option if it is not one of the recommended sizes.



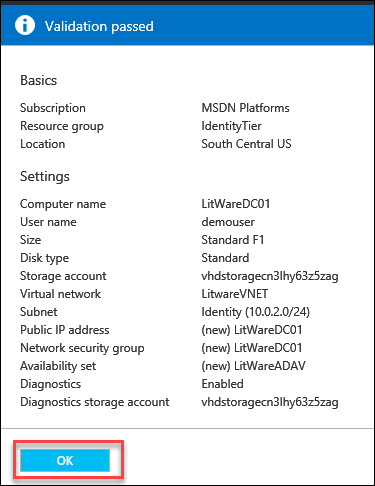
1. Click the **Select** button to continue to **Settings**.



1. In the **Settings** options, choose the following configuration:
2. Storage account: **Default to allow Azure to create an account**
3. Virtual Network: Click the name to choose **LitwareVNET**
4. Subnet: Choose **Identity** as the subnet
5. Availability set: **Create new, LitWareADAV**
6. Leave all other settings: **Default**
7. Then click the **OK** button to continue to the **Summary**.



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



Give the deployment a few minutes to build the Availability Set resource, then repeat Steps 2-9 again to create **LitWareDC02** making sure to place it in the **LitWareADAV** availability set.

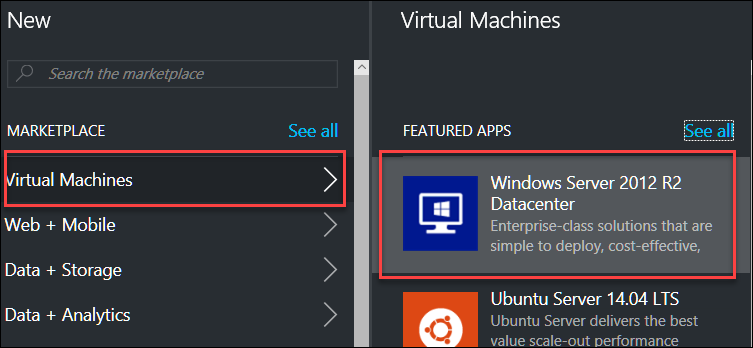
### Task 2: Create the Active Directory Deployment (Region 2)

We will now deploy additional domain controllers in the new region.

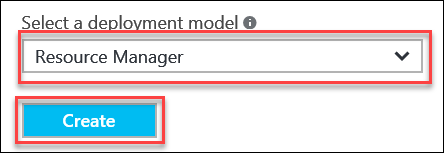
1. In the left pane, click **+ New**.



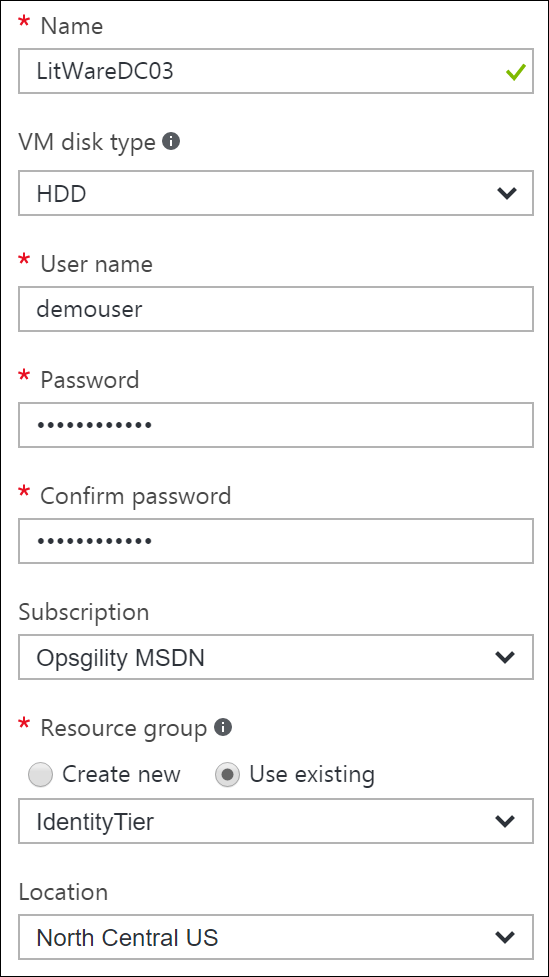
1. In the **New** blade, select **Virtual Machines >** and then **Virtual Windows Server 2012 R2 Datacenter**.



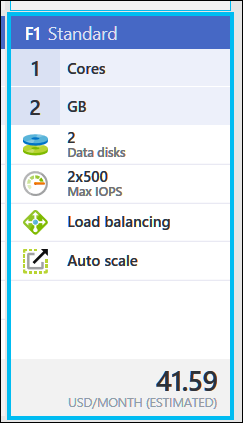
1. In, the **Select a deployment model** drop-down, leave the choice as **Resource Manager** and then click **Create**.



1. In the **Create virtual machine** blade, enter the **Basics** information:
2. Name: **LitWareDC03**
3. VM disk type: **HDD**
4. Username: **demouser**
5. Password: **demo@pass123**
6. Confirm password: **demo@pass123**
7. Subscription: **Select your subscription**
8. Resource group: **Use existing – IdentityTier**
9. Location: **North Central US**
10. Click the **OK** button to continue to **Size**.



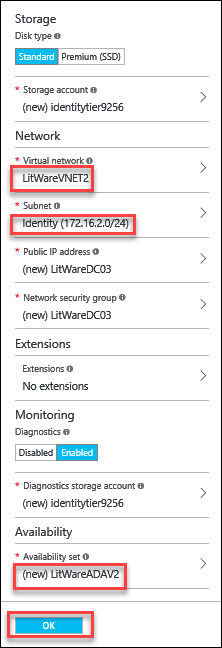
1. For the **Size**, select **F1 Standard**. You may have to select the **View All** option if it is not one of the recommended sizes.



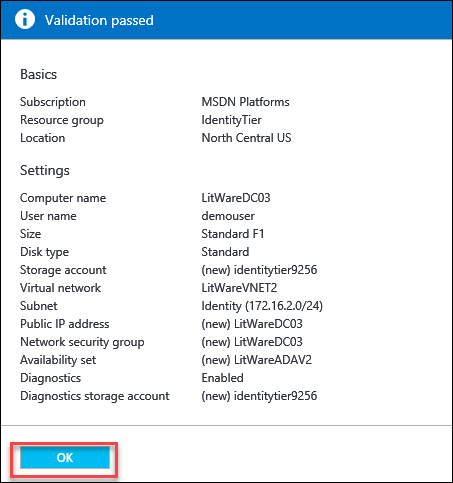
1. Click the **Select** button to continue on to **Settings**.



1. In the **Settings** options, choose the following configuration:
2. Storage account: **Default to allow Azure to create an account**
3. Virtual Network: Click the name to choose **LitWareVNET2**
4. Subnet: Choose **Identity** as the subnet
5. Availability set: **Create new, LitWareADAV2**
6. Leave all other settings: **Default**
7. Then click the **OK** button to continue to the **Summary**.



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



1. Give the deployment a few minutes to build the Availability Set resource, then repeat Steps 2-9 again to create **LitWareDC04** making sure to place it in the **LitWareADAV2** availability set.

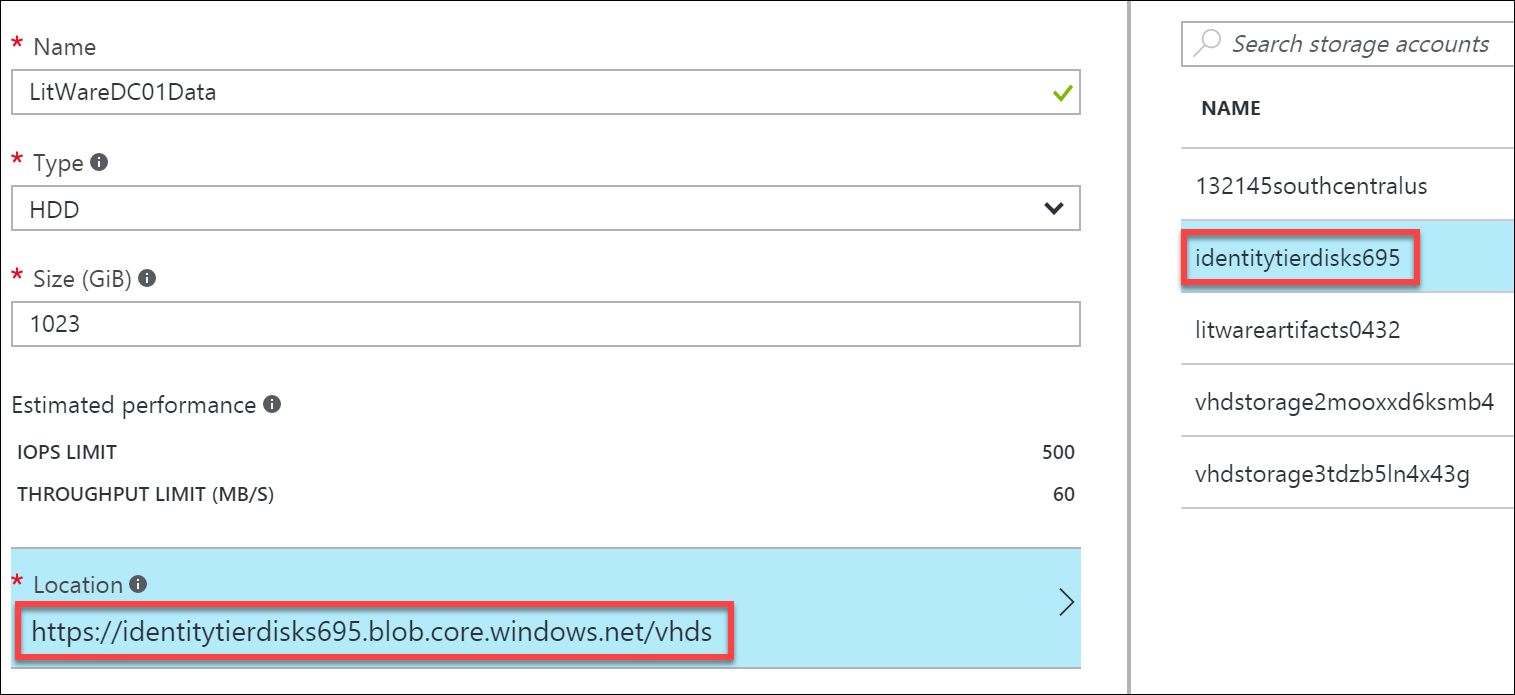
### Task 3: Add Data Disks to Active Directory domain controllers (Both Regions)

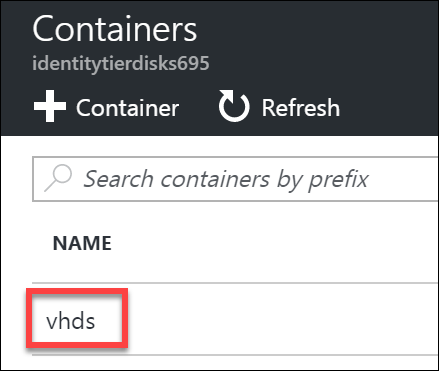
We will now add data disks to our VMs that will function as domain controllers. It is a best practice to separate the ADDC database and log files from the OS disk.

1. Click on **Virtual Machines** on the left-hand Azure Menu, then click on **LitWareDC01**.
2. In the **Settings** blade, select **Disks >** under the **SETTINGS** heading.
3. Click on **Attach new** icon in the menu bar.

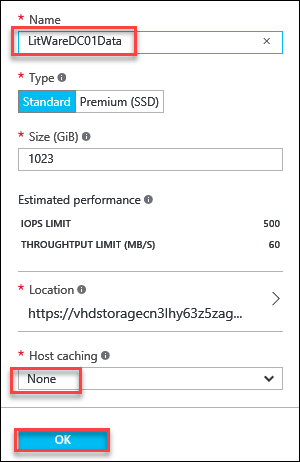


1. In the settings for **Attach new disk**, enter the following:
   1. Name: **LitWareDC01Data**
   2. Type: **HDD**
   3. Size: **1023**
   4. Location: If not pre-selected, click the value under **Location** and choose the **identitytierdisksxxxx** storage account. Then choose the **vhds** container.





* 1. Host caching: **None**
  2. Click the **OK** button to attach the disk.

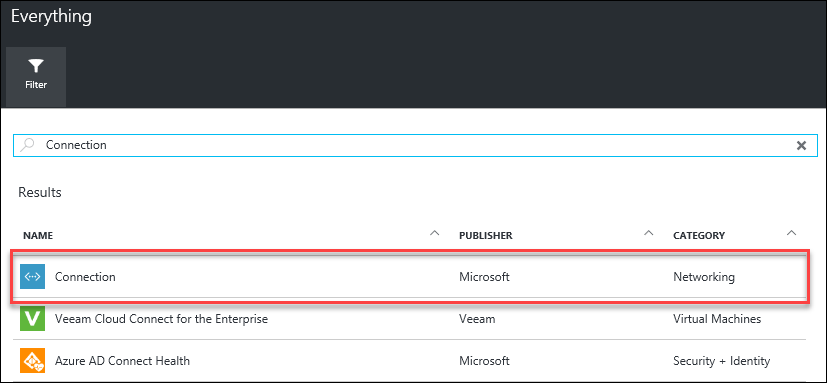


1. Perform Steps 1-4 for **LitWareDC02** naming the disk **LitWareDC02Data** and making sure the Host caching is set to **None.**
2. Perform Steps 1-4 for **LitWareDC03** and **LitWareDC04** and naming the disks **LitWareDC03Data** and **LitWareDC04Data** respectively. Make sure to set the Host caching to **None**.

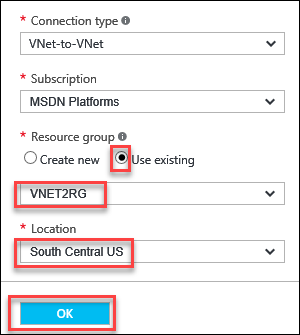
### Task 4: Build a connection between the VPN Gateways

NOTE: Both VPN Gateways need to have successfully deployed before completing this step. The Hackathon was designed to provide ample time for them to complete while doing other deployments, but make sure to check before completing the following task.

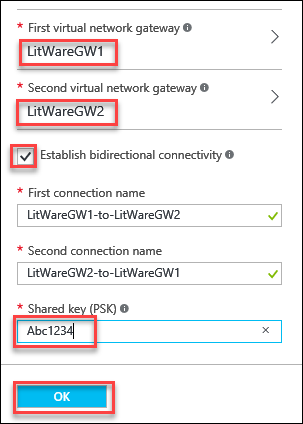
1. Click **+ New**.
2. In the **Search the marketplace** window, type **Connection** then hit enter.
3. In the resulting **Everything** blade choose **Connection** by **Microsoft** as the publisher.



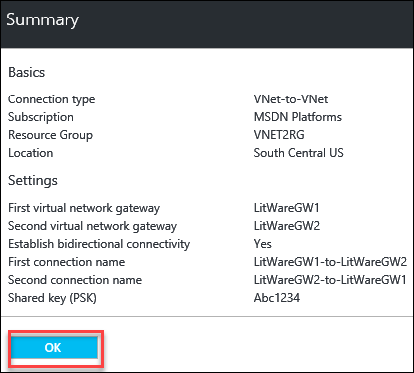
1. Click the **Create** button to continue.
2. In the **Create connection** settings for **Basics** enter the following:
   1. Connection type: **VNet-to-VNet**
   2. Subscription: **Choose your subscription**
   3. Resource Group: **Use existing – VNET2RG**
   4. Location: **South Central US**
   5. Click the **OK** button to continue to **Settings**



1. In the **Settings** blade, choose the following options:
   1. First virtual network gateway: **LitWareGW1**
   2. Second virtual network gateway: **LitWareGW2**
   3. Establish bidirectional connectivity: **Leave the checkbox selected**
   4. First connection name: **Default**
   5. Second connection name: **Default**
   6. Shared key: **Abcd1234**
   7. Click the **OK** button to continue to **Summary**



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



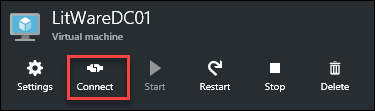
1. Click on **More services** > **Connections**. Wait until the **Connections** show status of **Connected** before continuing to the next task.



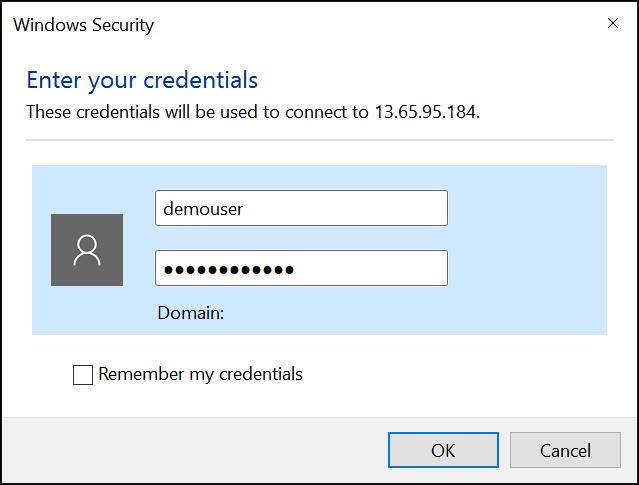
NOTE: This may take 10-15 minutes. If you want, you can format the data disks in the next task while waiting to help conserve time. Just be sure to not set the DNS settings until a connection is established between VPN Gateways.

### Task 5: Format Data Disks on DCs and configure DNS settings across connection

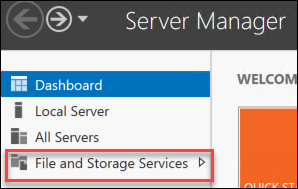
1. From the **Virtual Machines** menu on the left of the portal, click on **LitWareDC01** on the Azure dashboard.
2. Click the **Connect** icon on the menu bar to RDP into the server.



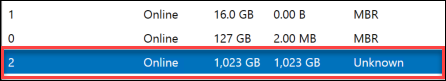
1. Save the RDP file and open it to begin the RDP session.
2. Login to the VM with **demouser** and password created during deployment.



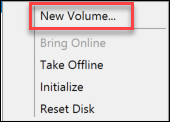
1. Once the logged in, click on **File and Storage Services** in **Server Manager**.



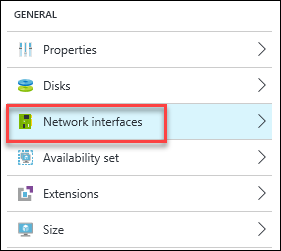
1. Click on **Disks** and let the data load. You should now see an **Unknown** partition disk in the list.



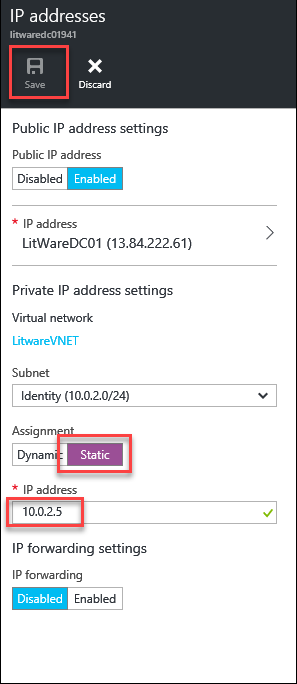
1. Right click on this disk and choose **New Volume…** from the context menu options.



1. Follow the prompts in the **New Volume Wizard** to format this disk as the **F:\** drive for the domain controller.
2. Perform Steps 2-9 for the remaining 3 DCs (**LitWareDC02**, **LitWareDC03**, and **LitWareDC04**).
3. Go back to the Azure Portal Dashboard and click on **LitWareDC01**. Click on **Network interfaces >** in the **Settings** blade.



1. Select the **IP** addresses to open the **Settings** for the network interface.
2. Under **Settings** for the **Network interface**, select **IP addresses** and change the **Private IP address settings** to **Static.** Leave all the other settings at their defaults and click the **Save** icon.



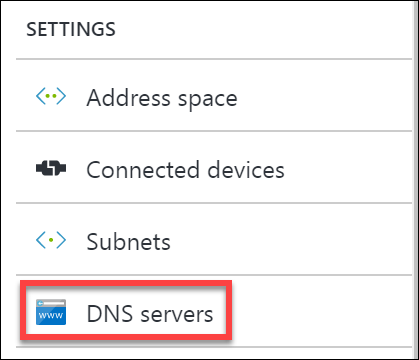
1. Once Azure notifies that the network interface change is saved, repeat Steps 11-14 the remaining 3 DCs (**LitWareDC02**, **LitWareDC03**, and **LitWareDC04**).

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.

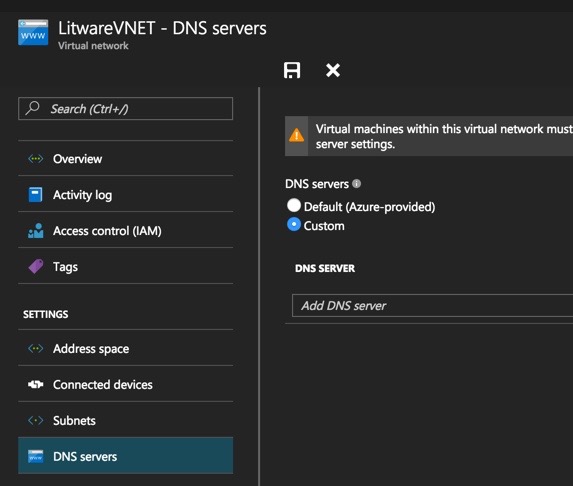
1. By this time, the Gateways should show **Connected**.



1. In the Azure Portal, click **More Services** > and in the filter type in **Virtual Networks**. Select **LitWareVNET2** from the list.
2. In the resulting **Settings** blade, select **DNS Servers >** under the **SETTINGS** heading.



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



1. 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.

1. While these two DCs are rebooting, RDP into **ADDC** and run the following PowerShell command:  
     
   Set-DnsServerPrimaryZone -Name litware.com -DynamicUpdate NonsecureAndSecure

NOTE: This change allows both non-secure and secure updates of DNS records, and would not be appropriate in a production environment. This change is being accomplished for lab purposes.

1. After the PowerShell command runs, log off of **ADDC**.

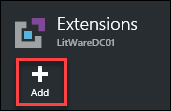
### Task 6: Promote DCs as Additional domain controllers (Both Regions)

In this step, we will promote the new VMs we created to be domain controllers. We will use a PowerShell script and the custom script extension to accomplish this.

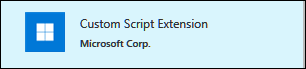
1. Login to Lab VM created in exercise 0 or the machine where you have downloaded the exercise files.
2. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
3. Click on **LitWareDC01** on the Azure dashboard.
4. In the **Settings** blade, click **Extensions >** under the **SETTINGS** heading.



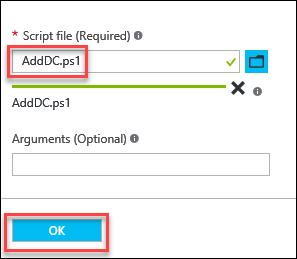
1. Click the **+ Add** icon.



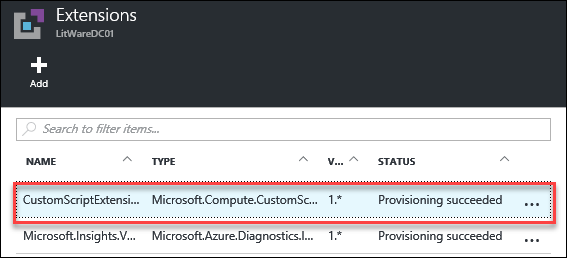
1. Choose **Custom Script Extension** by Microsoft Corp. then click the **Create** button to continue.



1. 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.



1. This script will run the commands to add this DC to the domain as an additional DC in the Litware.com domain. Repeat Steps 2-6 for **LitWareDC02**, **LitWareDC03**, and **LitWareDC04**.
2. Once this succeeds, you will see a **Provisioning succeeded** message under **Extensions** for all four domain controllers.



NOTE: Were 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. Because there are now 2 properly configured domain controllers in both regions, we could gracefully demote ADDC and update both VNets to use the new DCs as DNS servers.

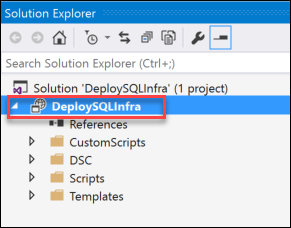
## Exercise 4: Build Web Tier and SQL for resiliency

### Overview

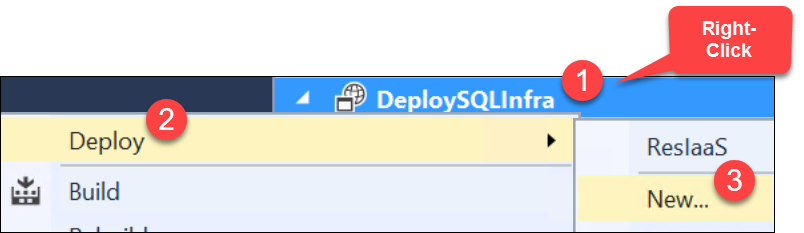
In this exercise, you will design and create IaaS resiliency options in the additional region. You will use a template-based deployment to deploy 2 SQL servers and another load balancer. These will comprise an Always On Availability Group, ensuring resiliency of the data tier in the first region. You will also accomplish a template-based deployment to …eploy 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)

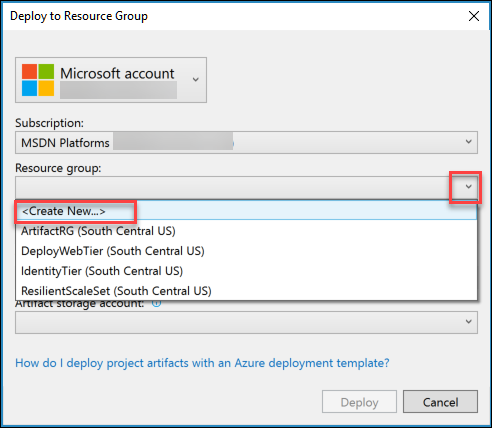
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution** and then browse to the files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SQL** folder and select the Visual Studio Solution file: **DeploySQLInfra.sln**.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



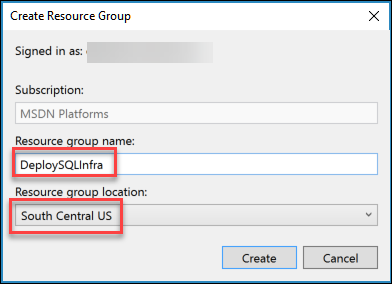
1. Now select **Deploy | New**.



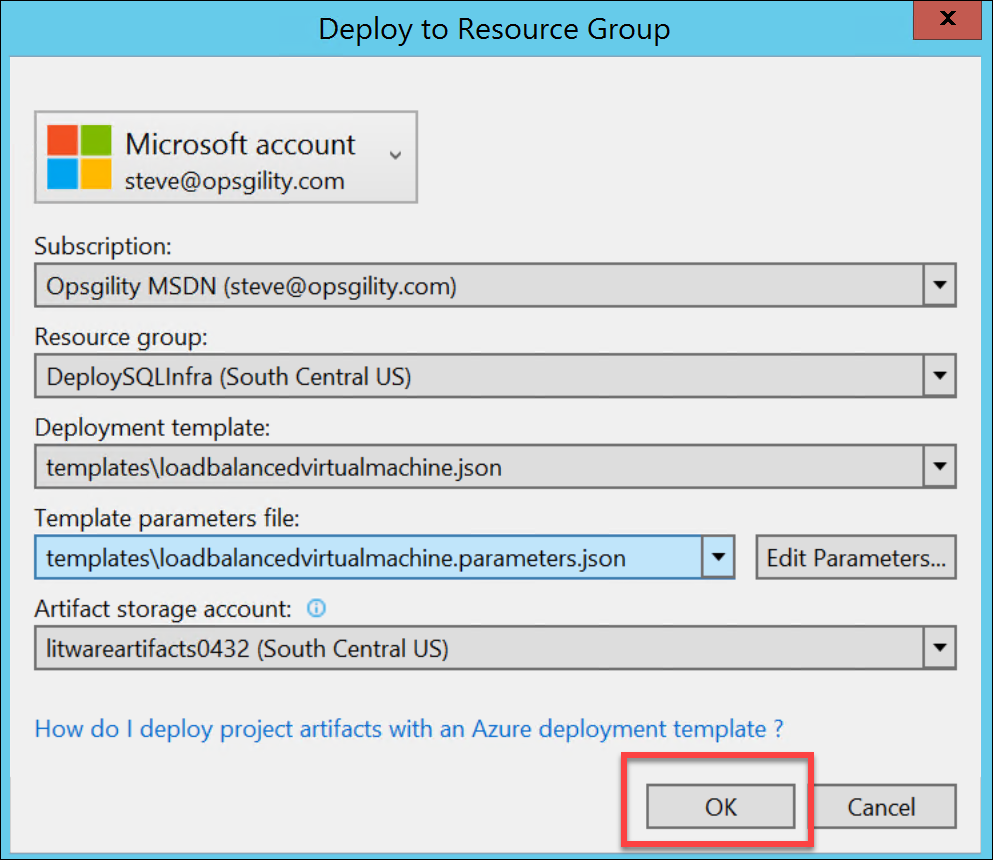
1. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New…>**



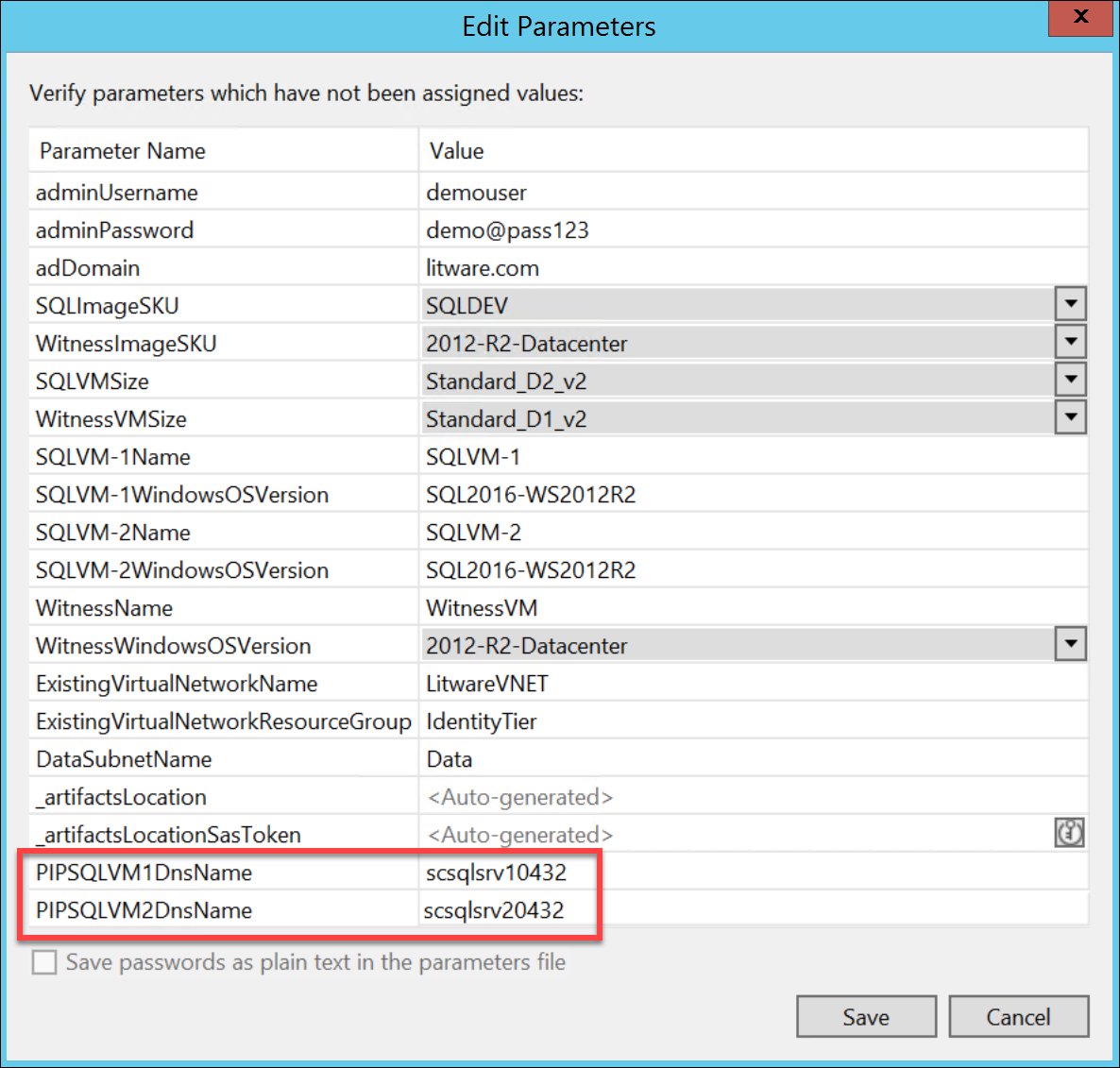
1. In the **Create Resource Group** enter the **Resource group name** as **DeploySQLInfra** and choose a **Resource group location**. Choose **South Central US** then click the **Create** button to continue.



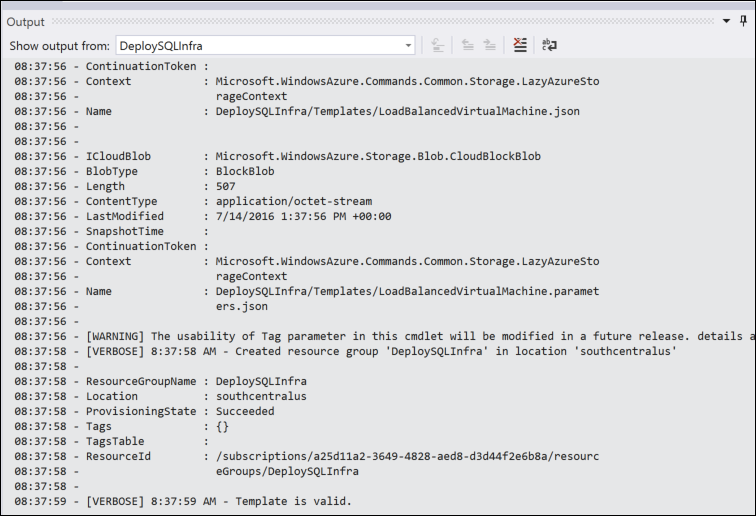
1. Back in the **Deploy to Resource Group** dialog, now choose the **Artifact storage account** that was created earlier. Then click **Deploy** to begin the deployment.



1. The **Edit Parameters** dialog opens. Enter DNS names for both SQL servers that will be deployed. Remember that DNS names must only contain lowercase letters and/or numbers, and must be unique. Click **Save**.



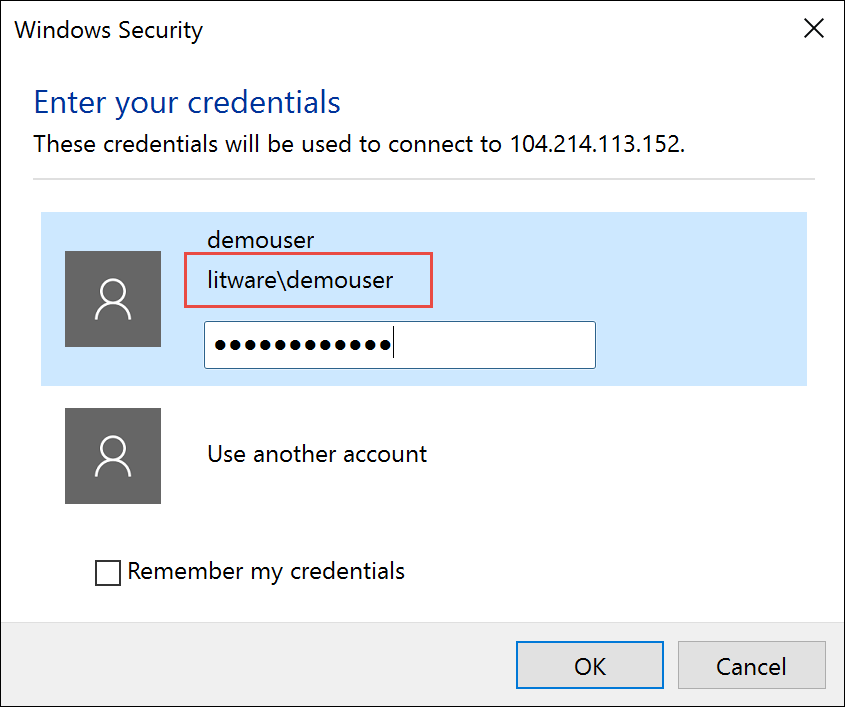
1. Monitor the output of the deployment in the **Output** window for success.



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.

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

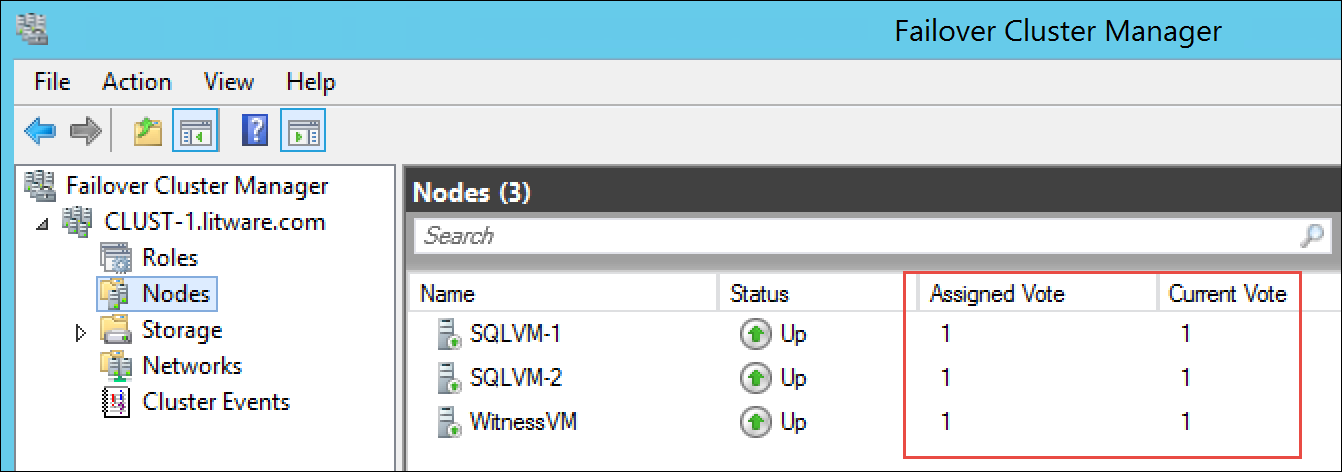




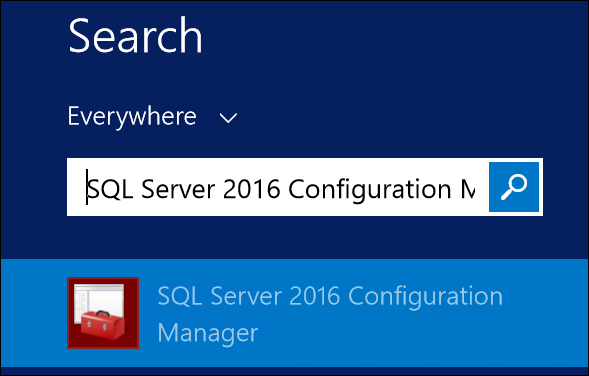
1. Open PowerShell and execute the following code:

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

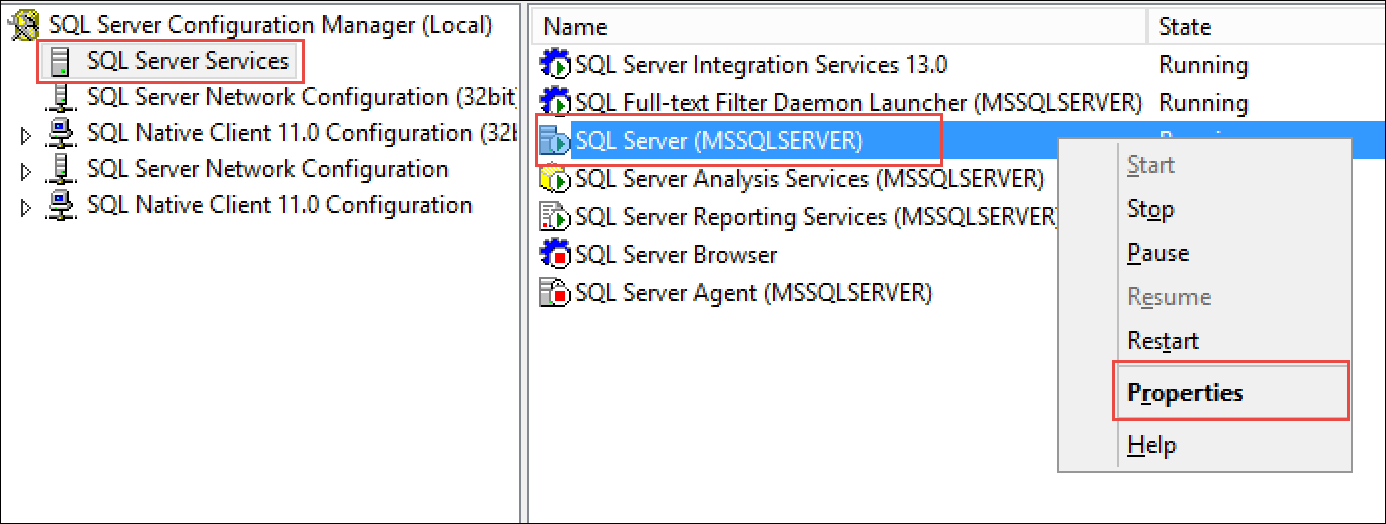
1. This will create a three-node cluster with a static IP address. It is also possible to use a wizard for this task but the resulting cluster will require additional configuration to set the static IP address to be viable in Azure. This is due to the way Azure DHCP distributes IP addresses, causing 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.
2. Open the Failover Cluster Manager, expand the CLUS-01 cluster, select Nodes, validate that all nodes are online and that Assigned Vote and Current Vote are 1 for all nodes of the cluster.



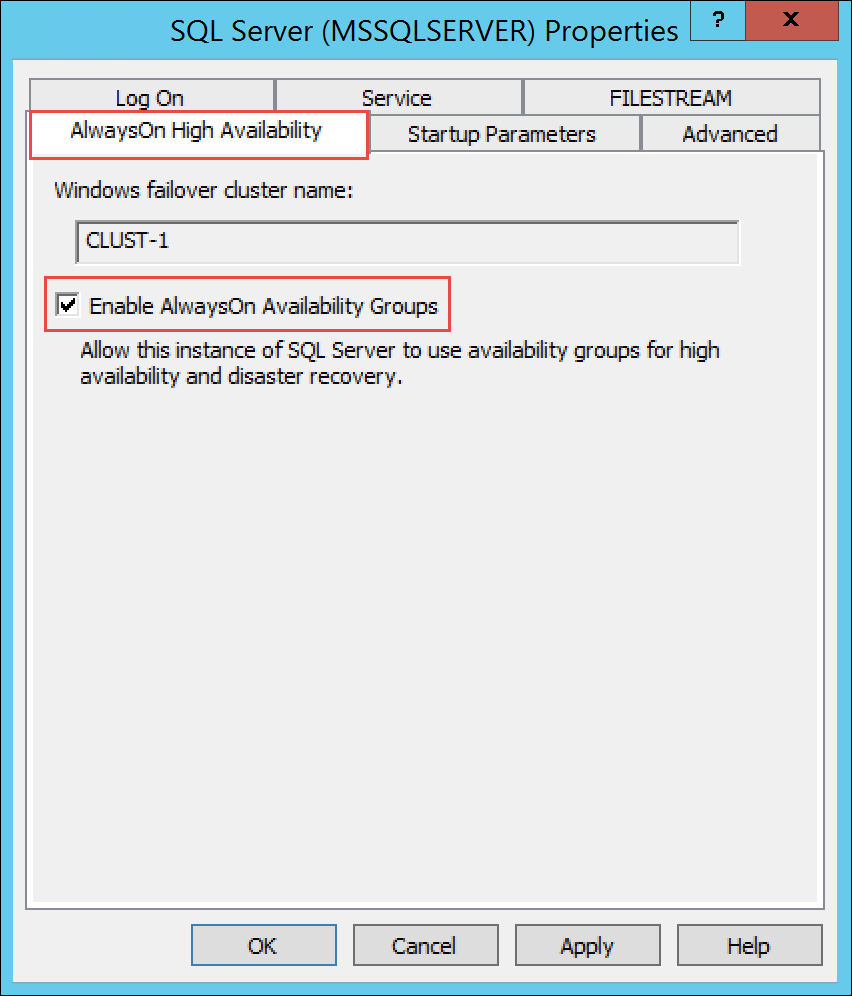
1. Launch **SQL Server 2016 Configuration Manager** on **SQLVM-1**.



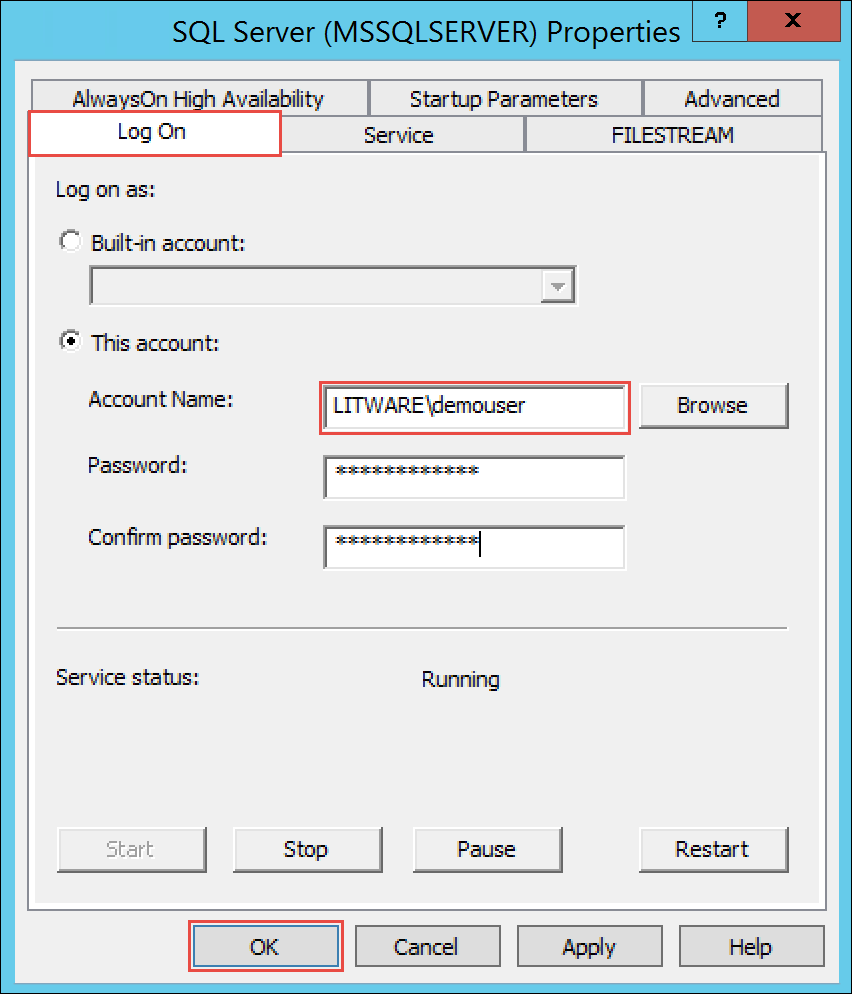
1. Click **SQL Server Services**, then right-click **SQL Server (MSSQLSERVER)** and select **Properties**.

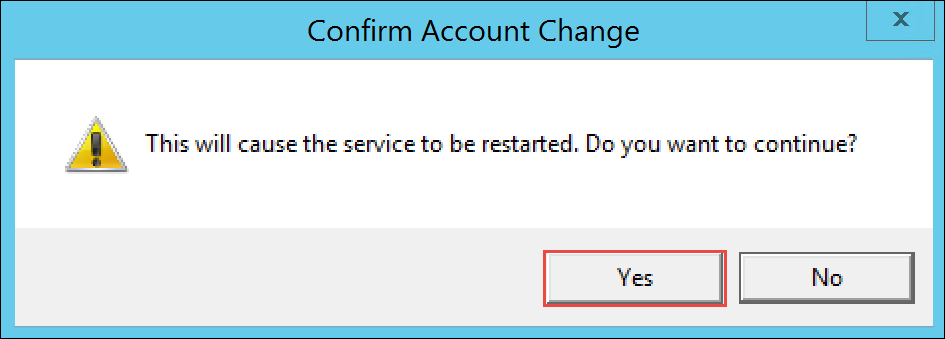


1. Select the **AlwaysOn High Availability** tab and check the box for **Enable AlwaysOn Availability Groups**, then click **OK**, then click **OK** again.



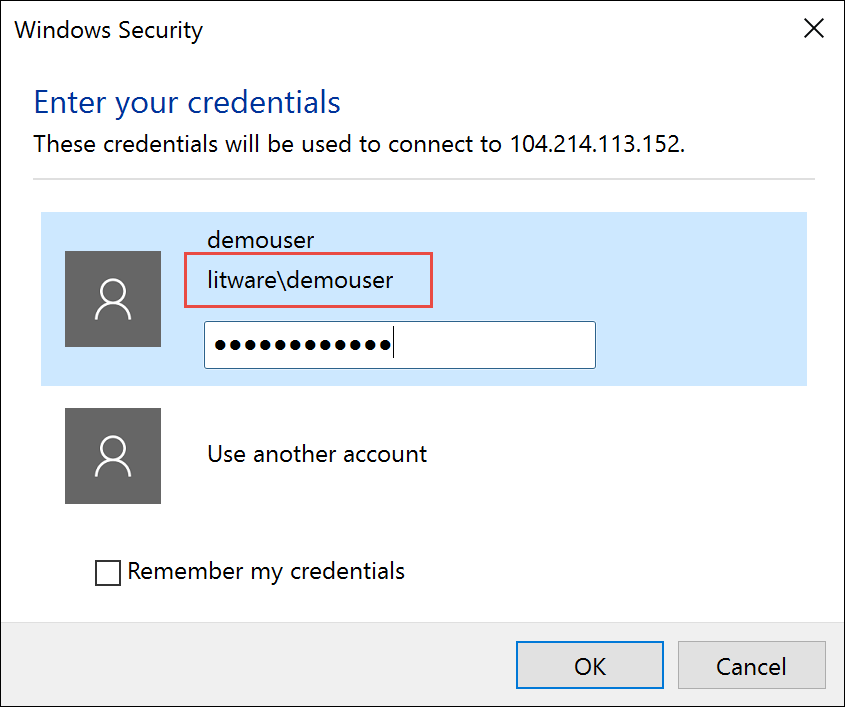
1. Click on the **Log On** tab. Change the service account to **litware\demouser**, using **demo@pass123** for the password. Click **OK** to accept the changes, and then click **Yes** to confirm the restart of the server.





1. Repeat steps 14-17 on **SQLVM-2**.
2. Open a remote desktop connection to the **SQLVM-1** virtual machine you created in the previous task and login using the **litware\demouser** account.

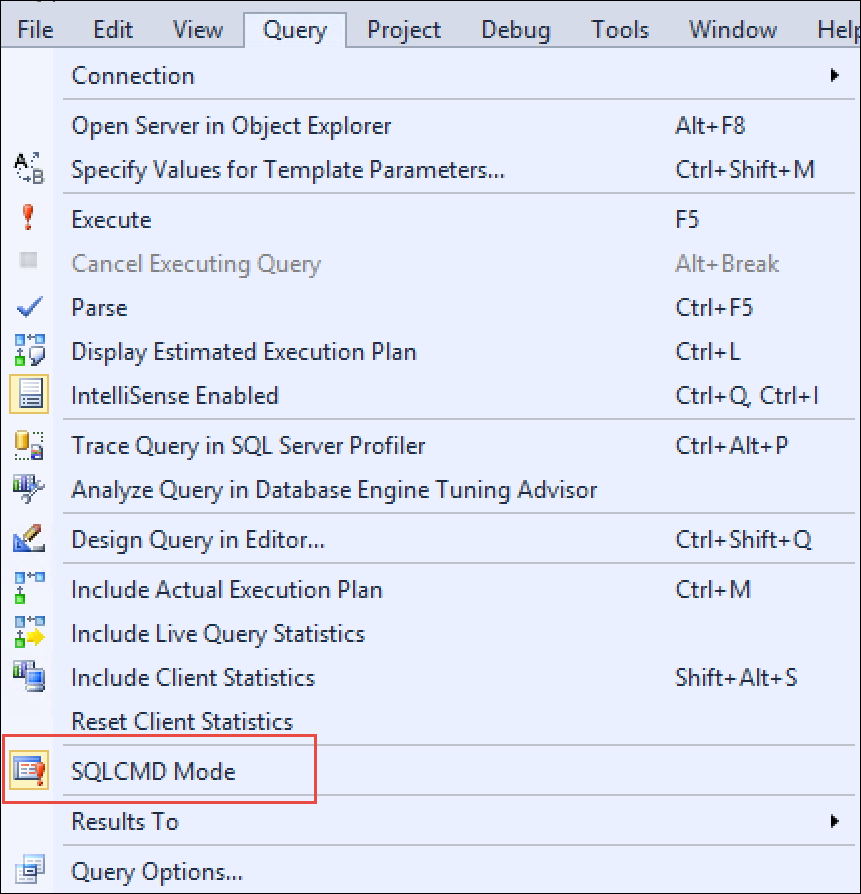




1. Launch **SQL Server 2016 Management Studio** and connect to the local instance of SQL Server.



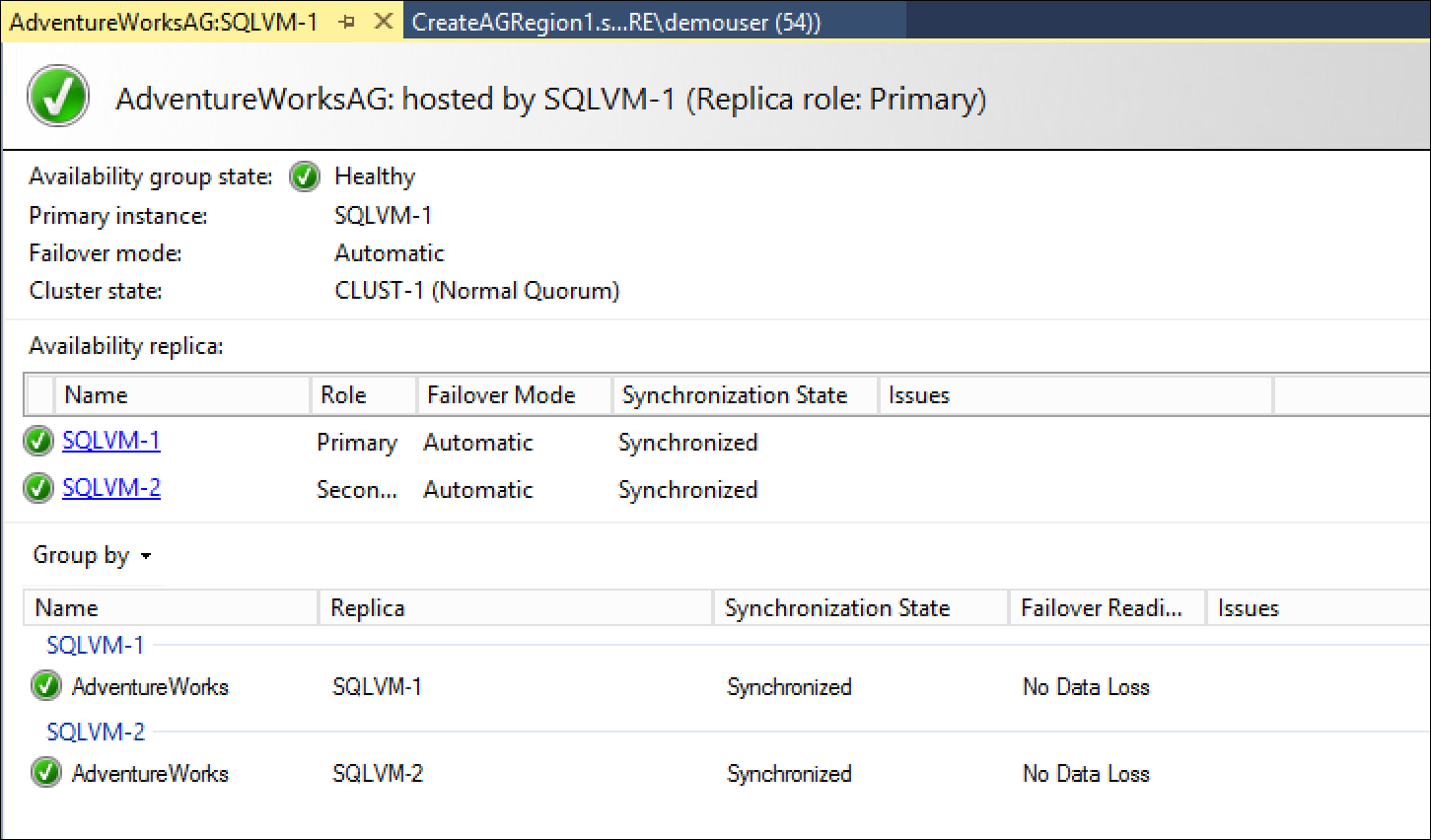
1. Availability Groups require that the databases be in full recovery mode and that an initial backup has been taken. If you deployed via the ARM template this will be done for you.
2. Copy file **C:\Hackathon\CreateAGRegion1.sql** from your development environment machine to **SQLVM-1: C:\SQLDATA**
3. Within SQL Server Management Studio, open the **C:\SQLDATA\CreateAGRegion1.sql** file.
4. Click the **Query** menu and then click **SQLCMD Mode**.



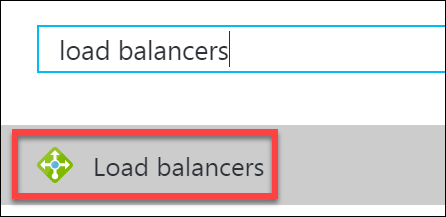
1. Click the **Execute** button to configure the Availability Group.



1. 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 speed the process 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/>
2. Expand **AlwaysOn High Availability -> Availability Groups**, then right-click **AdventureWorksAG** (Primary) and choose **Show Dashboard**. Your dashboard should look similar to this:



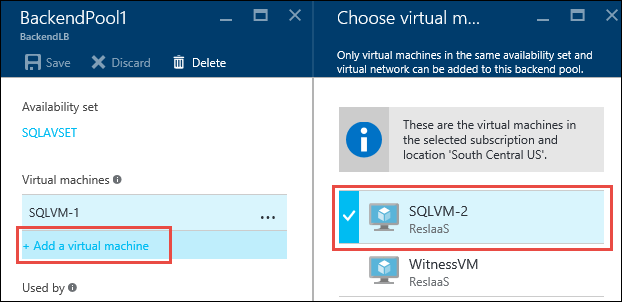
1. Within the Azure portal, click on **More services** > enter **Load Balancer**,Click on **Load Balancers**.



1. Click on **BackendLB** to open the settings of the load balancer that was created by the template.



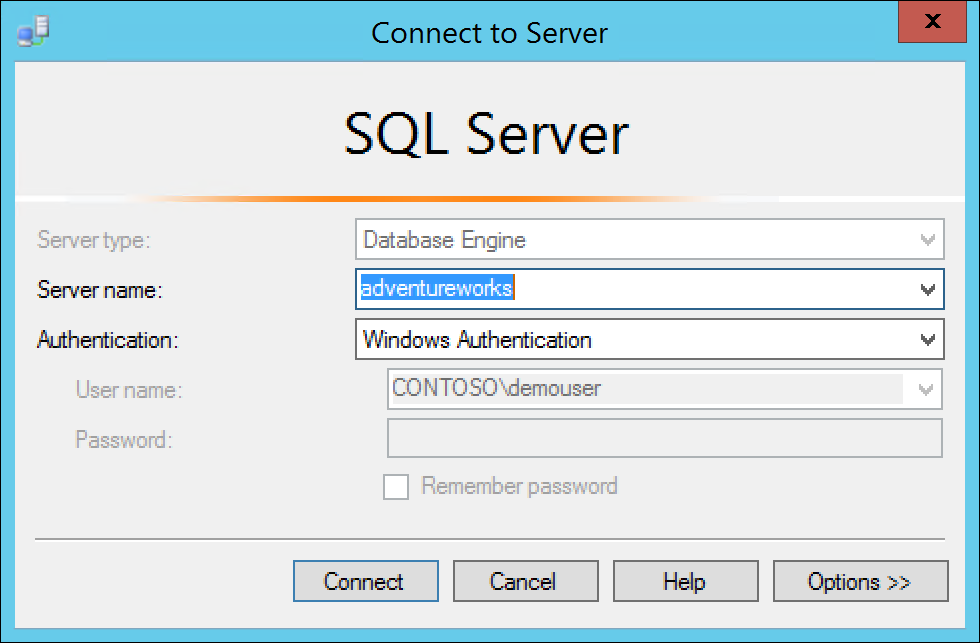
1. Click on **Backend pools**, select **BackendPool1** and click **+Add a virtual machine**: then select **SQLVM-2** and click the **Select** button.



1. Click the **Save** button on the **BackendPool1** blade.
2. Go back to **SQLVM-1** and open an **Administrative PowerShell\_ISE** session. Execute the following PowerShell to configure your cluster for the probe port.

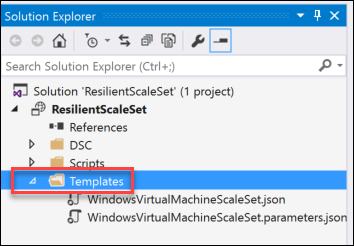
$ClusterNetworkName = "Cluster Network 1"  
$IPResourceName = "AdventureWorksAG\_10.0.1.9"  
$ILBIP = "10.0.1.50"  
Import-Module FailoverClusters  
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{"Address"="$ILBIP";"ProbePort"="59999";"SubnetMask"="255.255.255.255";"Network"="$ClusterNetworkName";"EnableDhcp"=0}  
Stop-ClusterResource -Name $IPResourceName  
Start-ClusterResource -Name "AdventureWorksAG"

1. Connect to **SQLVM-02** and launch **SQL Server Management Studio**.
2. Open a Server connection to the AdventureWorks listener endpoint to verify connectivity.

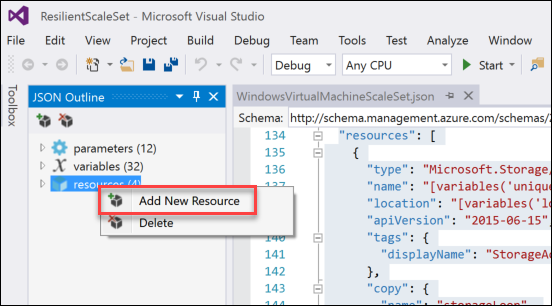


### Task 2: Run Script to Deploy Web Tier Scale Set (Region 1)

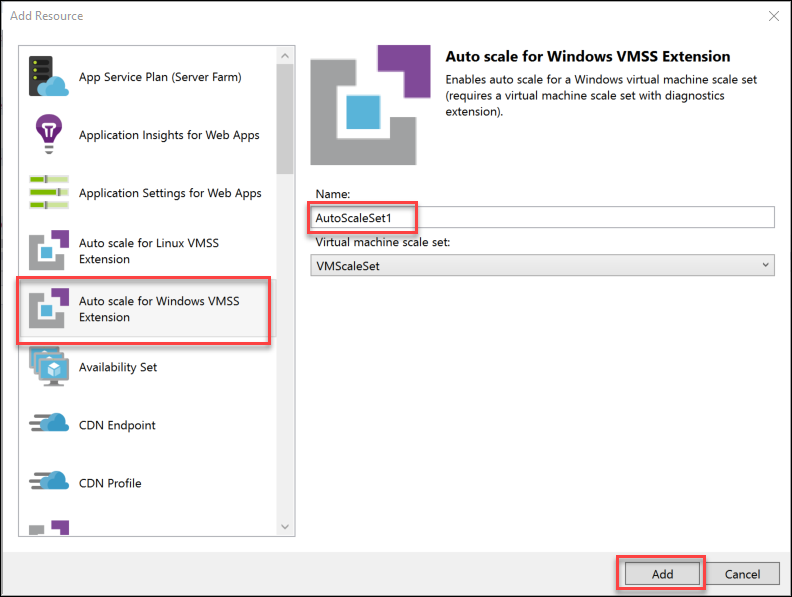
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution** and then browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SS** folder and select the Visual Studio Solution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



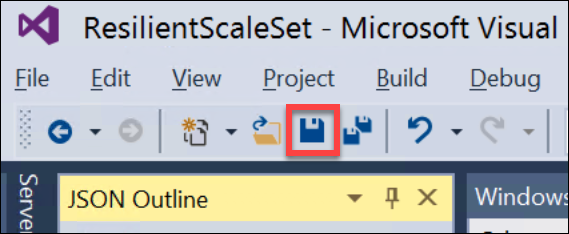
1. Click on the **WindowsVirtualMachineScaleSet.json** file to open it.
2. Once it is open, in the **JSON Outline** box, right click on **Resources** and then select **Add New Resource** from the context menu.



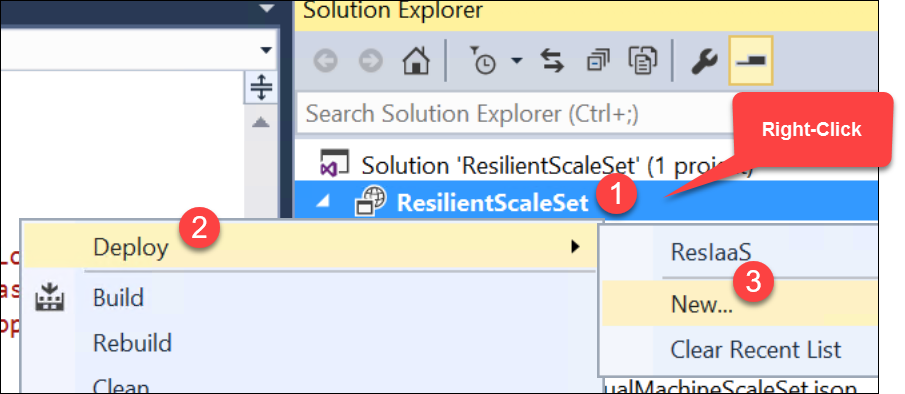
1. From the resource list, choose **Auto scale for Windows VMSS Extension**. In the **Name** box enter **AutoScaleSet1** and click the **Add** button to add the resource to the json file.



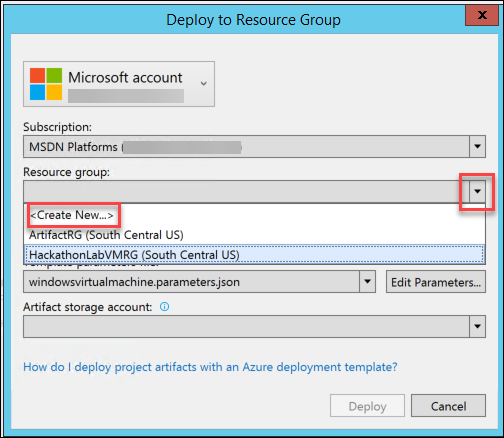
1. Click the **Save** icon to save the changes.



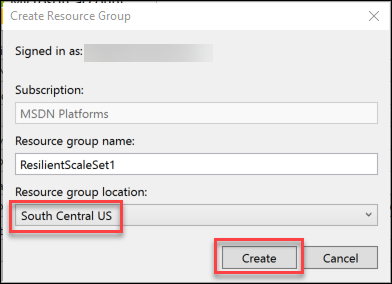
1. Right click on **ResilientScaleSet** in Solution Explorer.
2. Now select **Deploy | New**



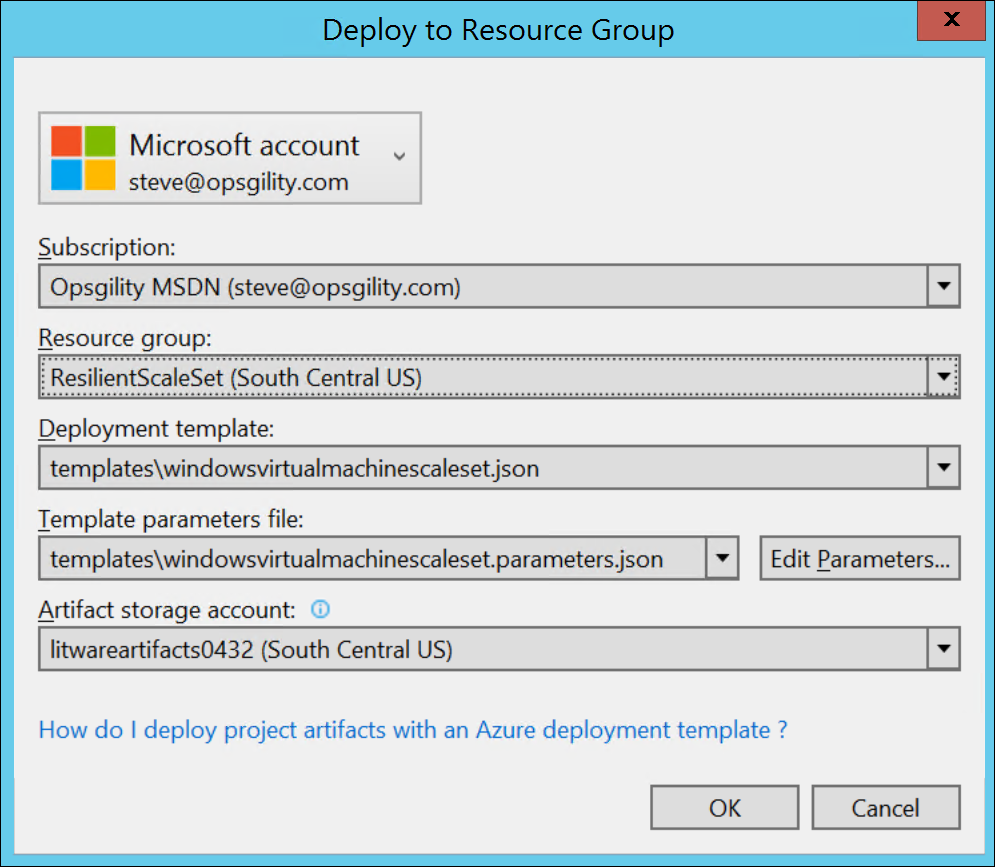
1. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New…>**



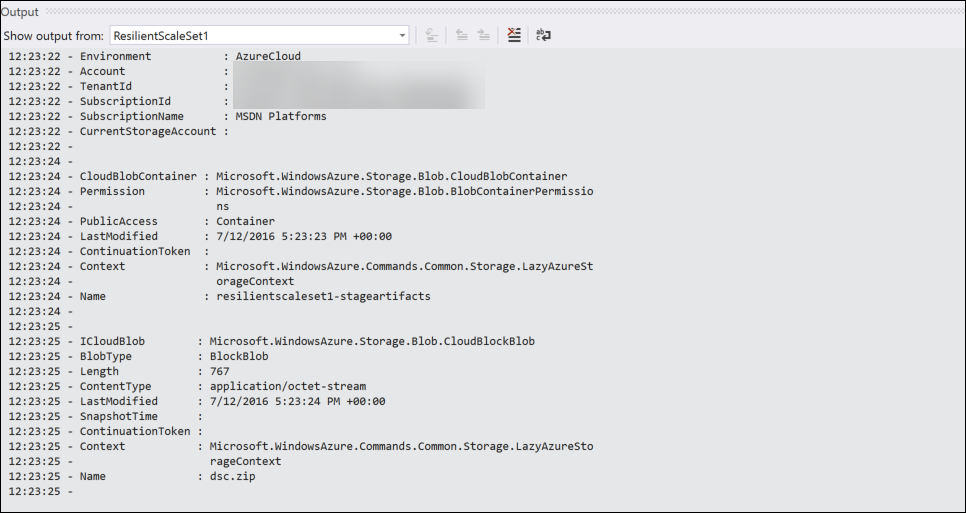
1. In the **Create Resource Group** enter the **Resource group name** as **ResilientScaleSet1** and choose a **Resource group location**. Choose **South Central US** then click the **Create** button to continue.



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

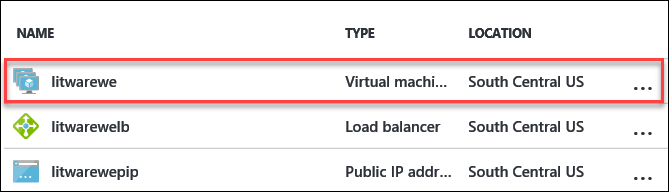


1. Monitor the output of the deployment in the **Output** window for success.

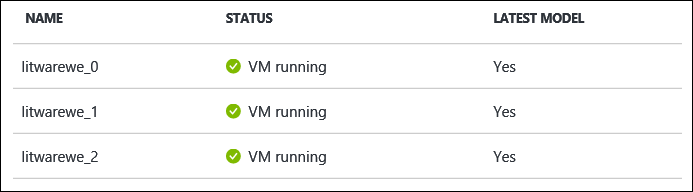


NOTE: This will take 10-15 minutes to deploy a Scale Set for the Web Tier in Region 1. After this is complete, we can perform some actions to show the Scale capabilities of the Web Tier. Were this a real production network, the IaaS VMs (Web-0 and Web-1) could be decommissioned or reused for other purposes.

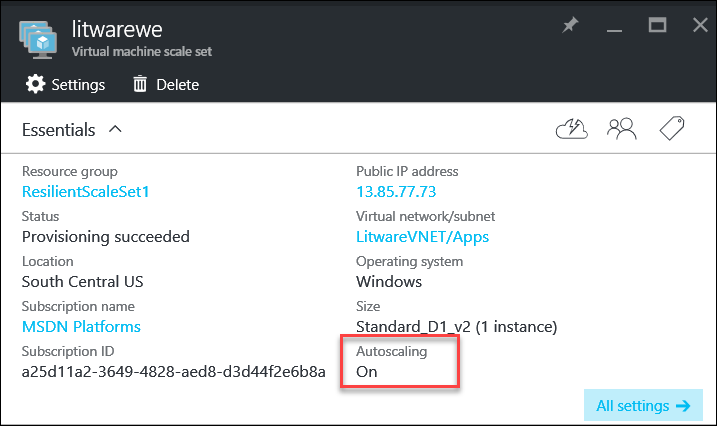
1. Browse to **Resource Groups** in the left pane menu in the Azure Portal. Select the **ResilientScaleSet** from the list of **Resource Groups**.
2. In the Resources, select **litwarewe** and click on it to open it.



1. Here you will see that multiple instances have been created during the deployment.

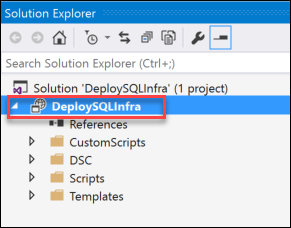


1. Also, note the **Autoscaling** is set to **On** in the information blade.

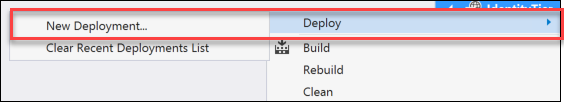


### Task 3: Deploy SQL Always On cluster (Region 2)

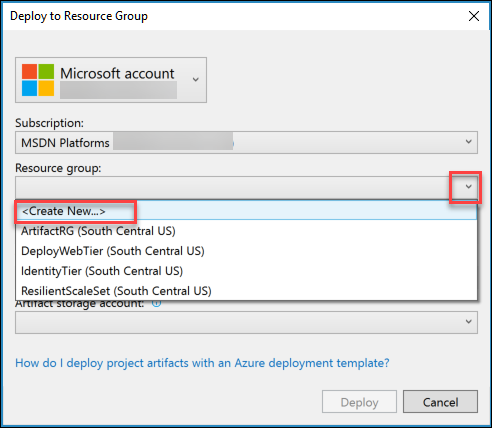
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution** and then browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SQL2** folder and select the Visual Studio Solution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



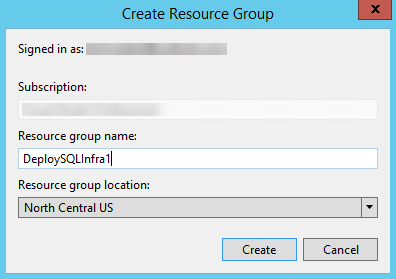
1. Now select **Deploy | New Deployment**.



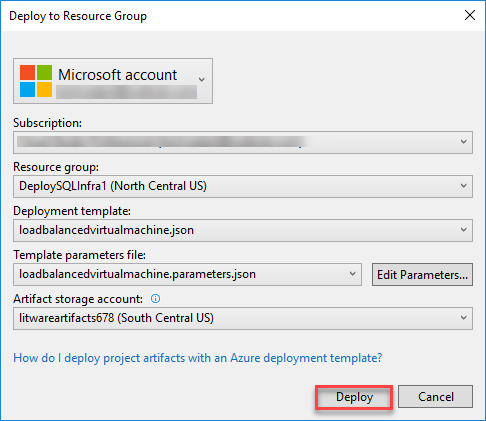
1. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New…>**



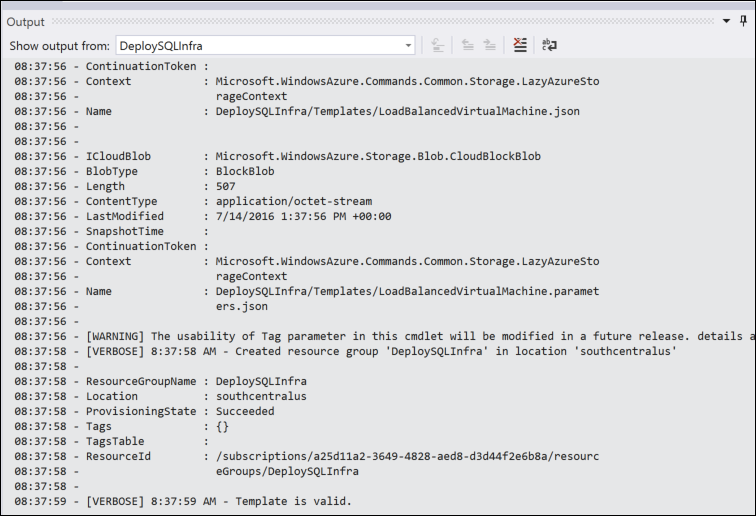
1. In the **Create Resource Group** enter the **Resource group name** as **DeploySQLInfra1** and choose a **Resource group location**. Choose **North Central US** then click the **Create** button to continue.



1. Back in the **Deploy to Resource Group** dialog, now choose the **Artifact storage account** that was created earlier. Then click **Deploy** to begin the deployment.



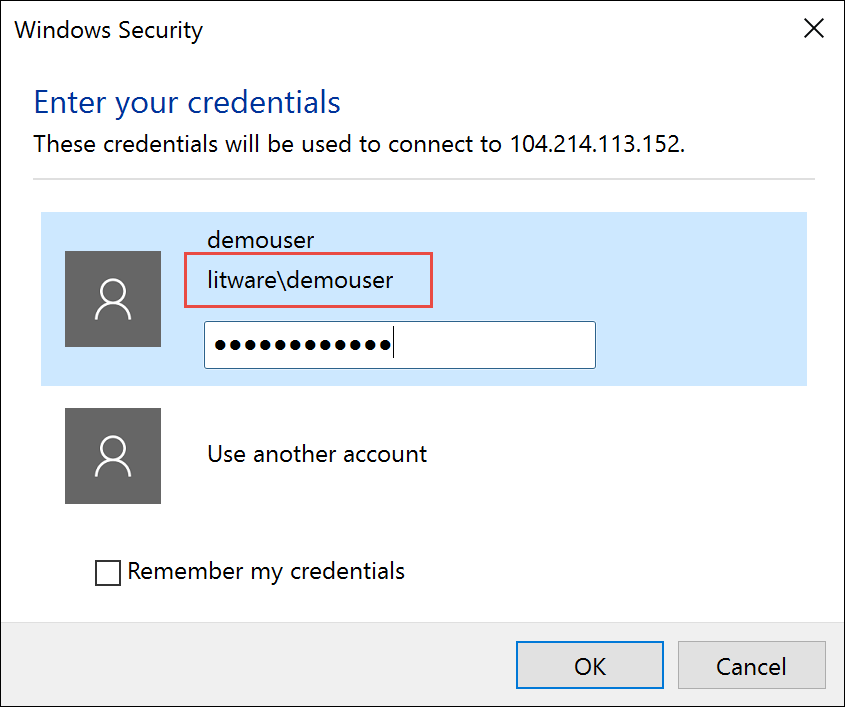
1. Monitor the output of the deployment in the **Output** window for success.



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.

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

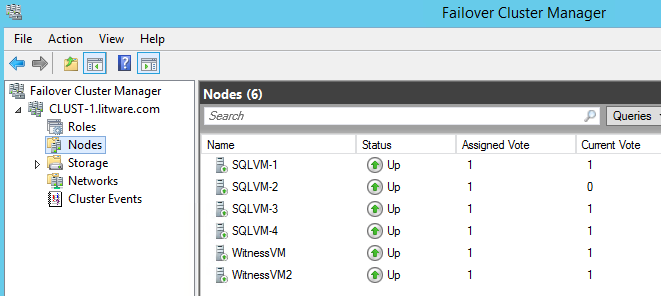




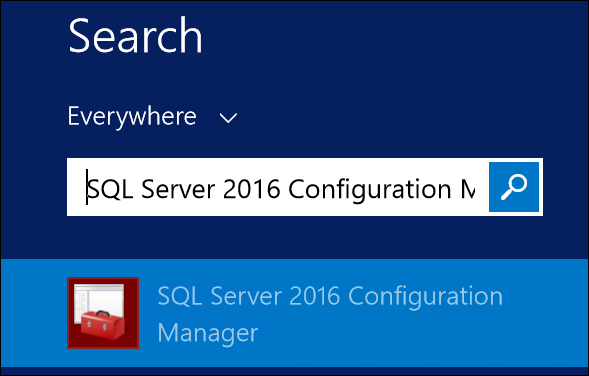
1. Open PowerShell and execute the following code:

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

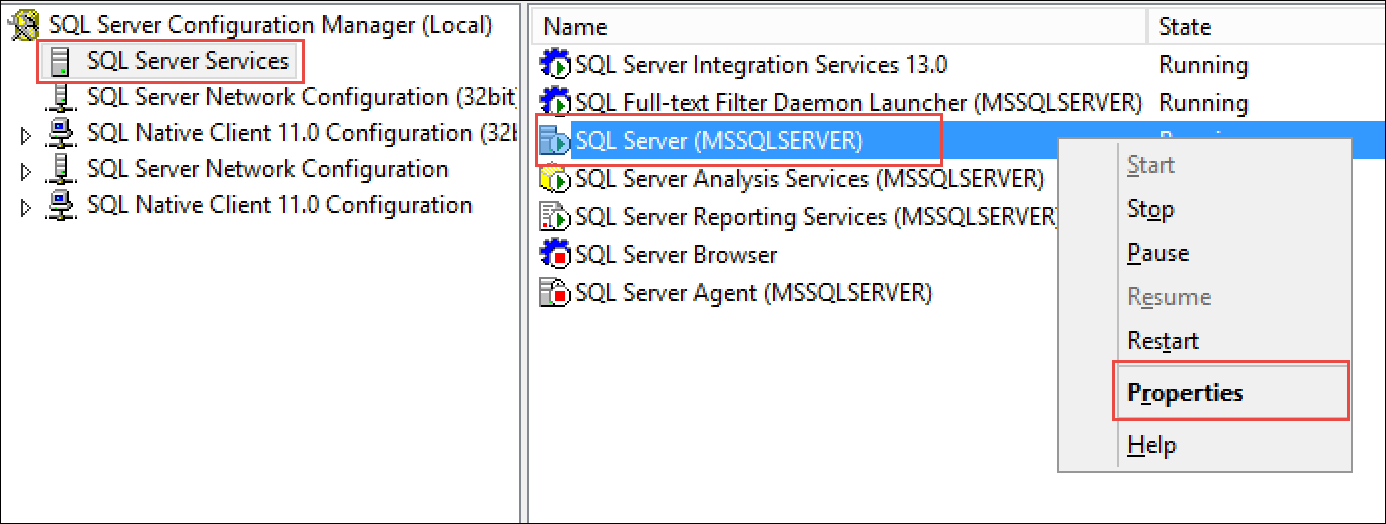
1. This will add three nodes to your existing cluster.
2. Open the Failover Cluster Manager, expand the CLUST-1 cluster, select Nodes, validate that all nodes are online.



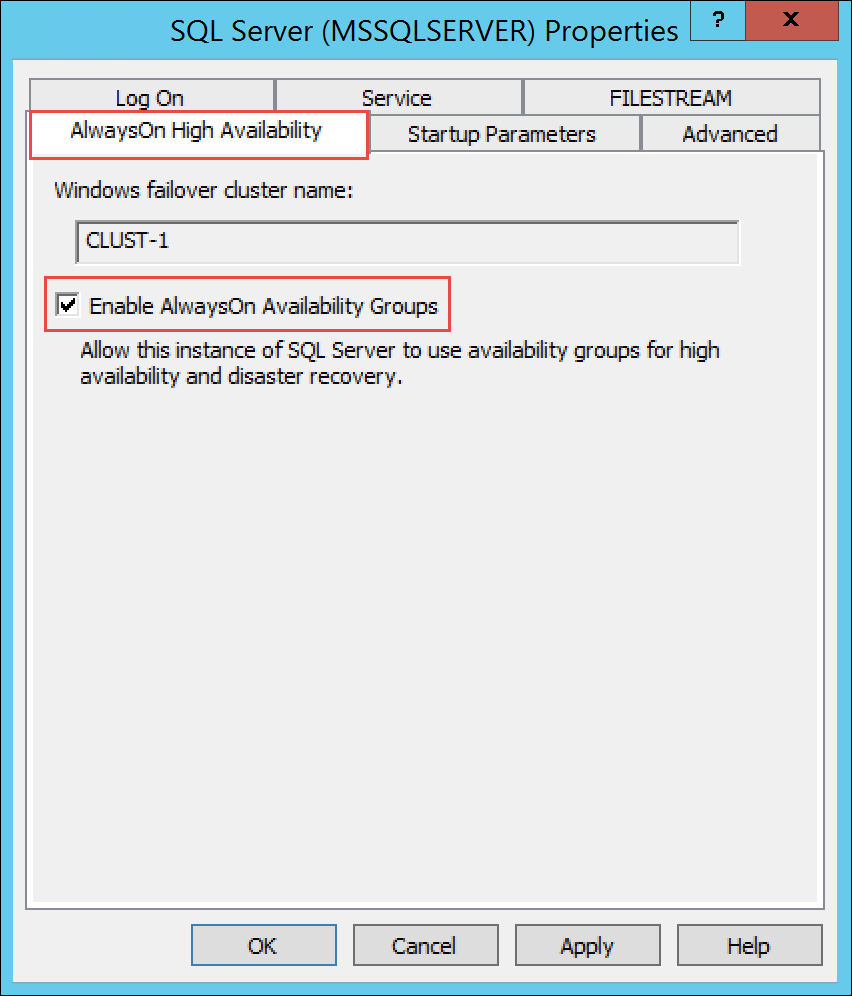
1. Launch **SQL Server 2016 Configuration Manager** on SQLVM-3.



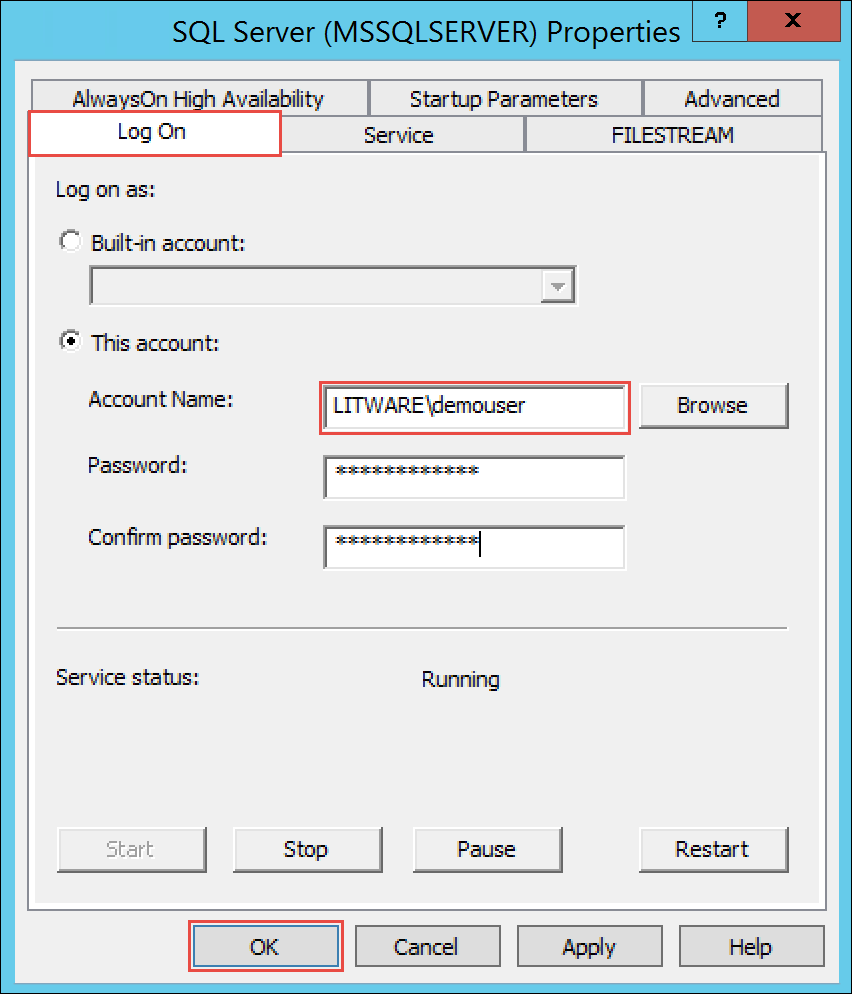
1. Click **SQL Server Services**, then right-click **SQL Server (MSSQLSERVER)** and select **Properties**.

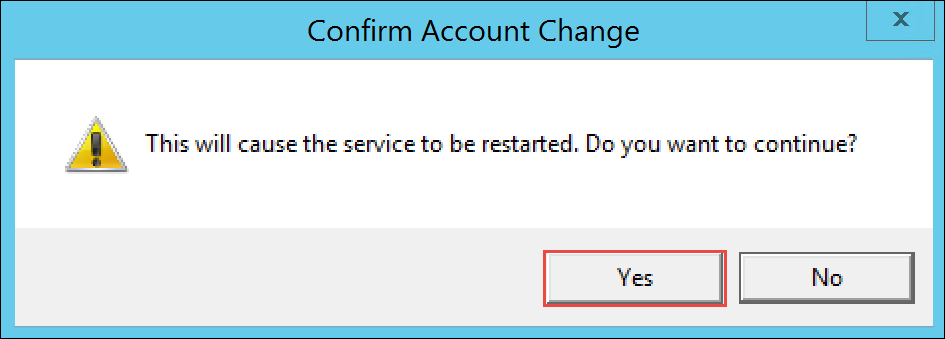


1. Select the **AlwaysOn High Availability** tab and check the box for **Enable AlwaysOn Availability Groups**, then click **OK**, then click **OK** again.



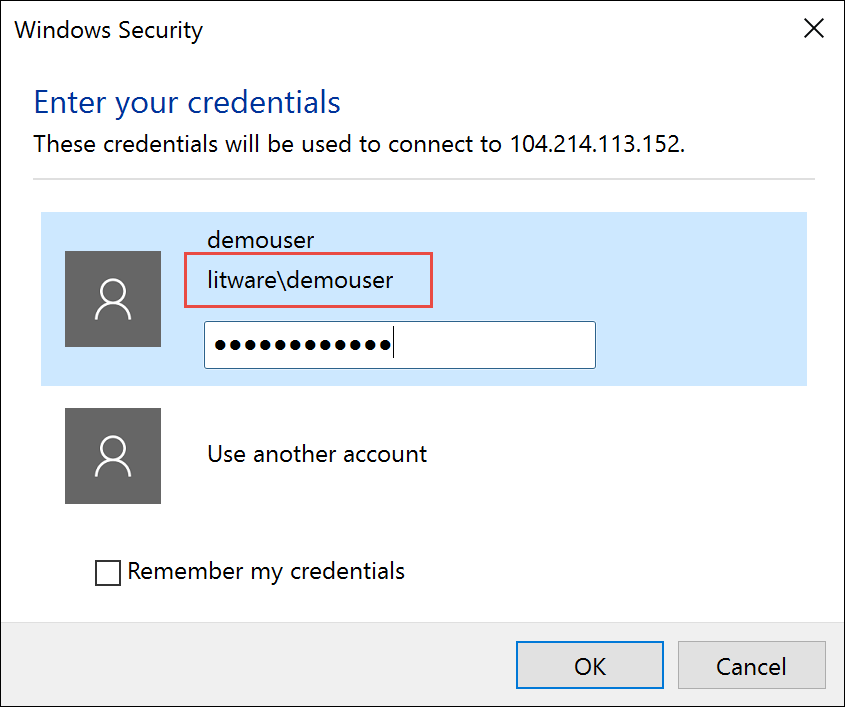
1. Click on the **Log On** tab. Change the service account to **litware\demouser**, using **demo@pass123** for the password. Click **OK** to accept the changes, and then click **Yes** to confirm the restart of the server.





1. Repeat steps 14-17 on **SQLVM-4**.
2. Open a remote desktop connection to the **SQLVM-3** virtual machine you created in the previous task and login using the **litware\demouser** account.

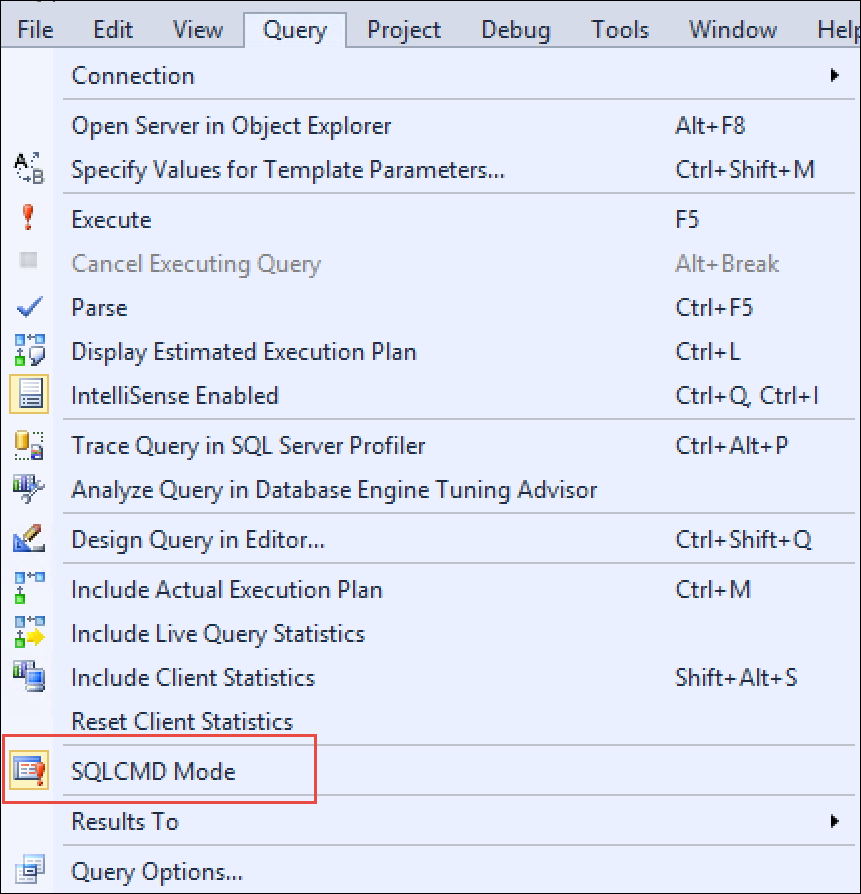




1. Launch **SQL Server 2016 Management Studio** and connect to the local instance of SQL Server.



1. 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.
2. Copy file **C:\Hackathon\CreateAGRegion2.sql** from your development environment machine to **SQLVM-1: C:\SQLDATA**
3. Within SQL Server Management Studio, open the **C:\SQLDATA\CreateAGRegion2.sql** file.
4. Click the **Query** menu and then click **SQLCMD Mode**.



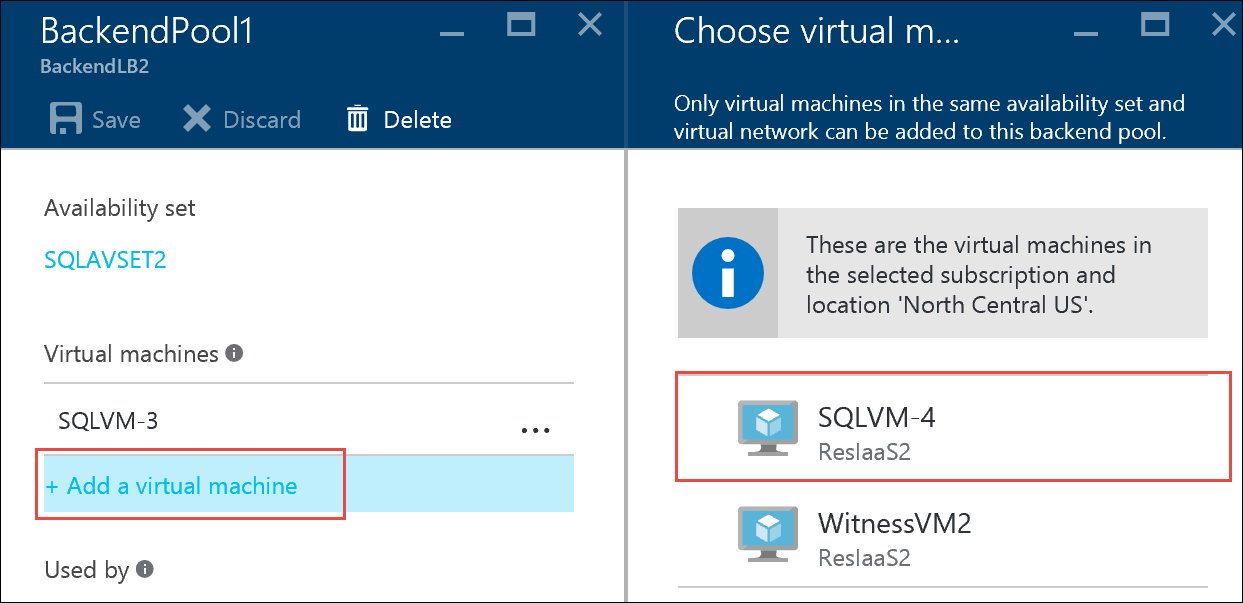
1. Click the **Execute** button to configure the Availability Group.



1. Some security messages are expected.
2. Open the settings of the **BackendLB2** load balancer that was created by the template.



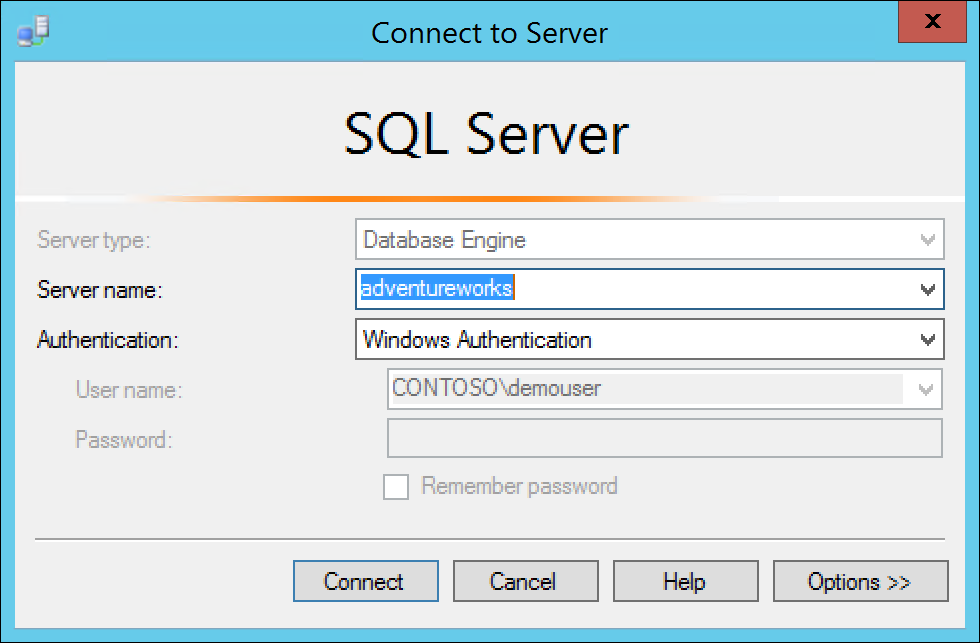
1. Click on **Backend pools**, select **BackendPool1** and click **+Add a virtual machine**: then select **SQLVM-4** and click the **Select** button.



1. Click the **Save** button on the **BackendPool1** blade.
2. Go back to **SQLVM-3** and open an **Administrative PowerShell\_ISE** session. Execute the following PowerShell to configure your cluster for the probe port.

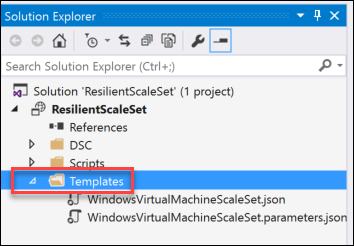
$ClusterNetworkName = "Cluster Network 1"  
$IPResourceName = "AdventureWorksAG\_172.16.1.9"  
$ILBIP = "172.16.1.50"  
Import-Module FailoverClusters  
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{"Address"="$ILBIP";"ProbePort"="59999";"SubnetMask"="255.255.255.255";"Network"="$ClusterNetworkName";"EnableDhcp"=0}  
Stop-ClusterResource -Name $IPResourceName  
Start-ClusterResource -Name "AdventureWorksAG"

1. Connect to **SQLVM-04** and launch **SQL Server Management Studio**.
2. Open a Server connection to the AdventureWorksAG listener endpoint to verify connectivity.

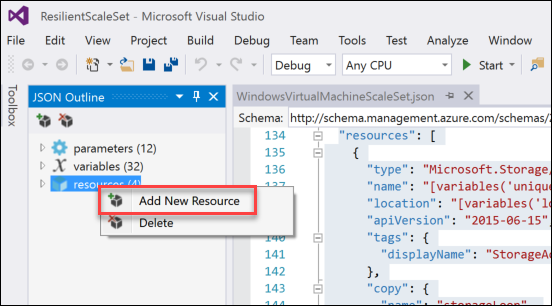


### Task 4: Deploy Web Tier Scale Set (Region 2)

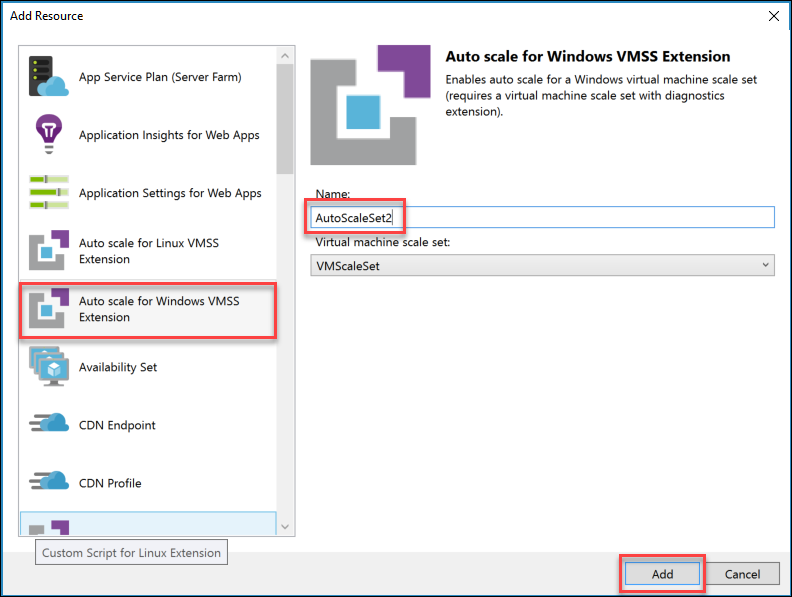
1. From your Development Environment VM, launch Visual Studio.
2. In Visual Studio, select **File | Open | Project/Solution** and then browse to the **Templates** directory in files you previously downloaded and extracted to **C:\Hackathon**.
3. Open the **SS2** folder and select the Visual Studio Solution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



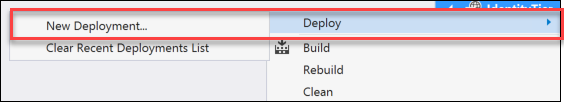
1. Click on the **WindowsVirtualMachineScaleSet.json** file to open it.
2. Once it is open, in the **JSON Outline** box, right click on **Resources** and then select **Add New Resource** from the context menu.



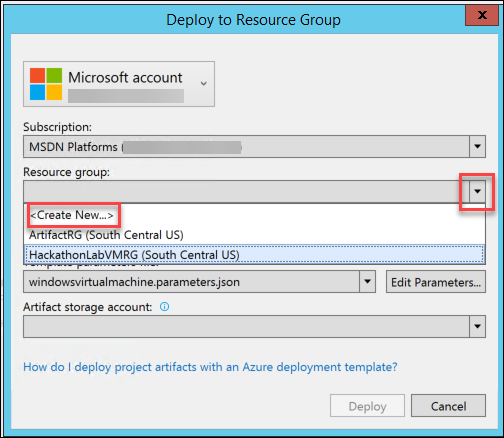
1. From the resource list, choose **Auto scale for Windows VMSS Extension**. In the **Name** box enter **AutoScaleSet2** and click the **Add** button to add the resource to the json file.



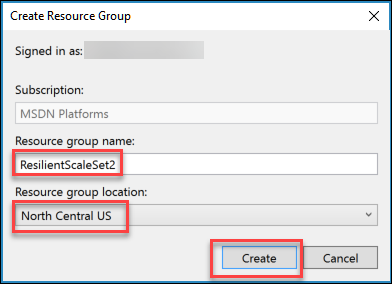
1. Once the resource is added, click the **Save** icon to save the changes.
2. Right click on **ResilientScaleSet** in Solution Explorer.
3. Now select **Deploy | New Deployment**.



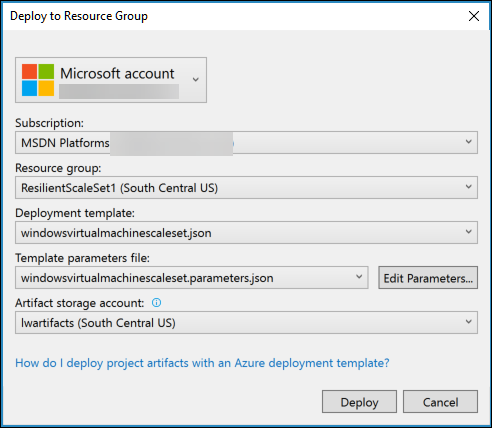
1. Once the **Deploy to Resource Group** window appears, select a **Resource group** by choosing the drop-down and selecting **<Create New…>**



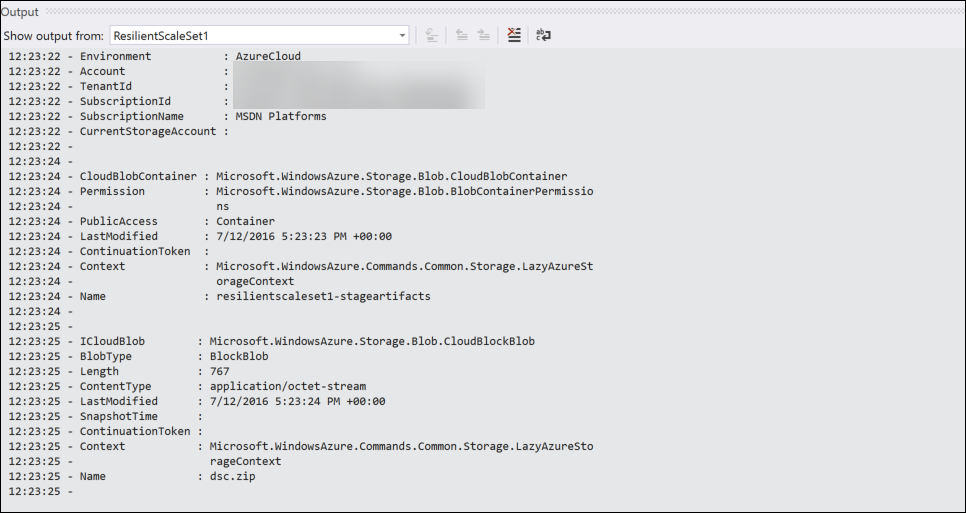
1. In the **Create Resource Group** enter the **Resource group name** as **ResilientScaleSet2** and choose a **Resource group location**. Choose **North Central US** then click the **Create** button to continue.



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



1. 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.

1. Browse to **Resource Groups** in the left pane menu in the Azure Portal. Select the **ResilientScaleSet** from the list of **Resource Groups**.
2. 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.



1. On the **CPU Spike Demo** section, change the minutes to 15 and click the **Spike CPU** button.
2. Monitor the **litwarewe** Scale Set and you should see additional instances being deployed by auto scaling.

### 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

### Overview

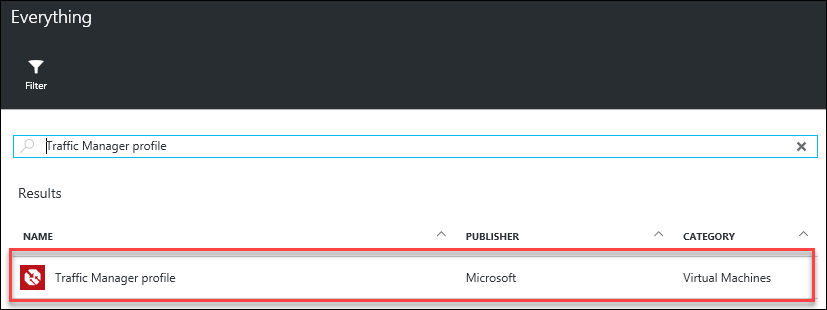
In this exercise, you will design and additional resiliency options in Azure. You will deploy a Traffic Manager in Priority Mode; you will configure Operations Management Suite and check for missing patches. You will configure IaaS backups in both regions and finally, configure Network Security Groups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

### Task 1: Create Traffic Manager in Priority Mode

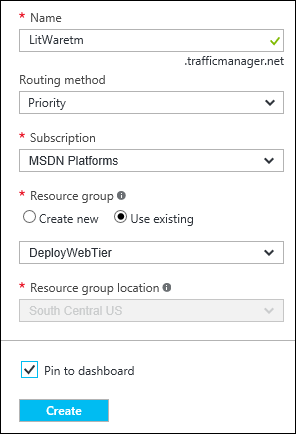
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click **+ New**.



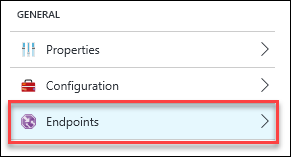
1. In the **Search the marketplace** window, type **Traffic Manager Profile** and hit enter.
2. In the resulting **Everything** blade choose **Traffic Manager profile** by **Microsoft** as the publisher.



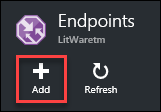
1. Click the **Create** button to continue.
2. In the **Create Traffic Manager profile** settings, enter the following:
   1. Name: **LitWaretm**
   2. Routing method: **Priority**
   3. Subscription: **Select your subscription**
   4. Resource group: **Use existing** **–** **DeployWebTier**
   5. Resource group location: **South Central US (Default)**
   6. Pin to dashboard: **Check the checkbox**
   7. Click the **Create** button to deploy the traffic manager.



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



1. Click the **+ Add** icon.



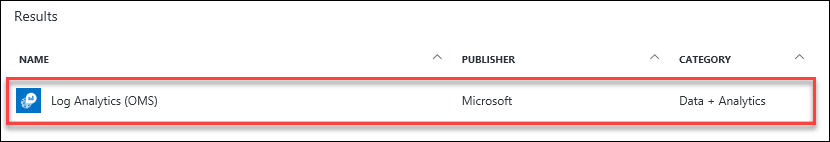
1. Enter the following settings on the **Add endpoint** blade:
   1. Type: **Azure endpoint**
   2. Name: **Region1**
   3. Target resource type: **Public IP address**
   4. Target resource: **Choose a public IP address – LoadBalancerIP1**
   5. Priority: **1**
   6. Click the **OK** button to save the endpoint.
2. Click the **+ Add** icon again.
3. Enter the following settings on the **Add endpoint** blade:
   1. Type: **Azure endpoint**
   2. Name: **Region2**
   3. Target resource type: **Public IP address**
   4. Target resource: **Choose a public IP address – LoadBalancerIP2**
   5. Priority: **2**
   6. Click the **OK** button to save the endpoint.

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

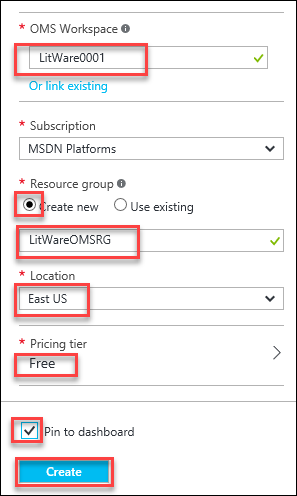
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click **+ New**.



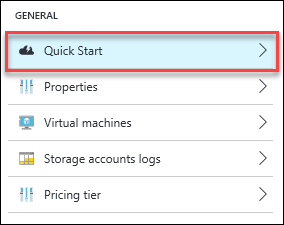
1. In the **Search the marketplace** window, type **Log Analytics (OMS)** and hit enter.
2. In the resulting **Everything** blade choose **Log Analytics (OMS)** by **Microsoft** as the publisher.



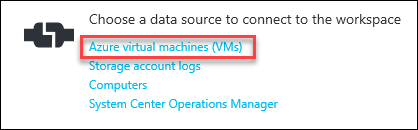
1. Click the **Create** button to continue.
2. In the **OMS Workspace** settings blade, enter the following settings:
   1. OMS Workspace: **LitWare0xxx** (where 0xxx is a unique number)
   2. Subscription: **Choose your subscription**
   3. Resource Group: **Create new – LitWareOMSRG**
   4. Location: **East US** (there are only a few regions where this can be deployed)
   5. Pricing tier: **Free**
   6. Pin to dashboard: **Click the checkbox**
   7. Click the **Create** button to deploy the workspace.



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

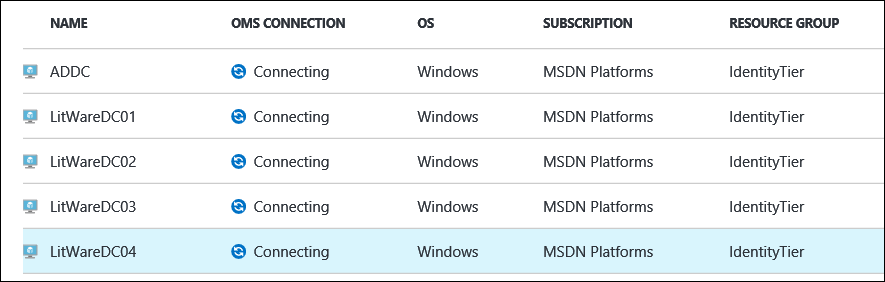


1. In the **Quick Start** blade, click on **Azure virtual machines (VMs)**.



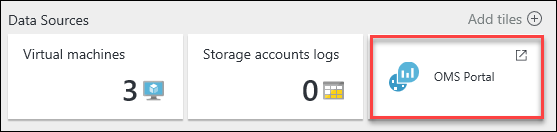
1. In the list of **Virtual Machines**, select the domain controllers and then click the **Connect** icon for each individual machine.



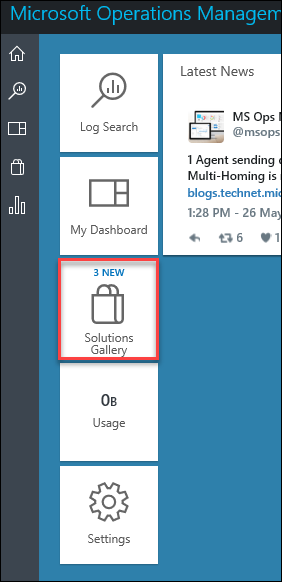


1. Repeat these steps to connect the SQL Servers.
2. Once the servers are connected, click on the **OMS Portal** icon or tile to launch the OMS Portal.

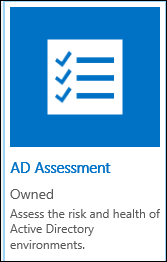




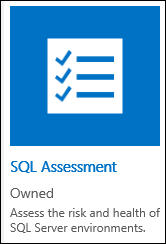
1. Once the **OMS Portal** launches, select the **Solutions Gallery** from the dashboard.



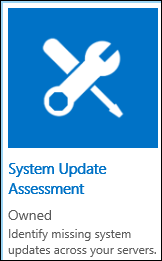
1. Add the following solutions from the **Solutions Gallery** by clicking the solution and then the **Add** button for each:
   1. AD Assessment



* 1. SQL Assessment



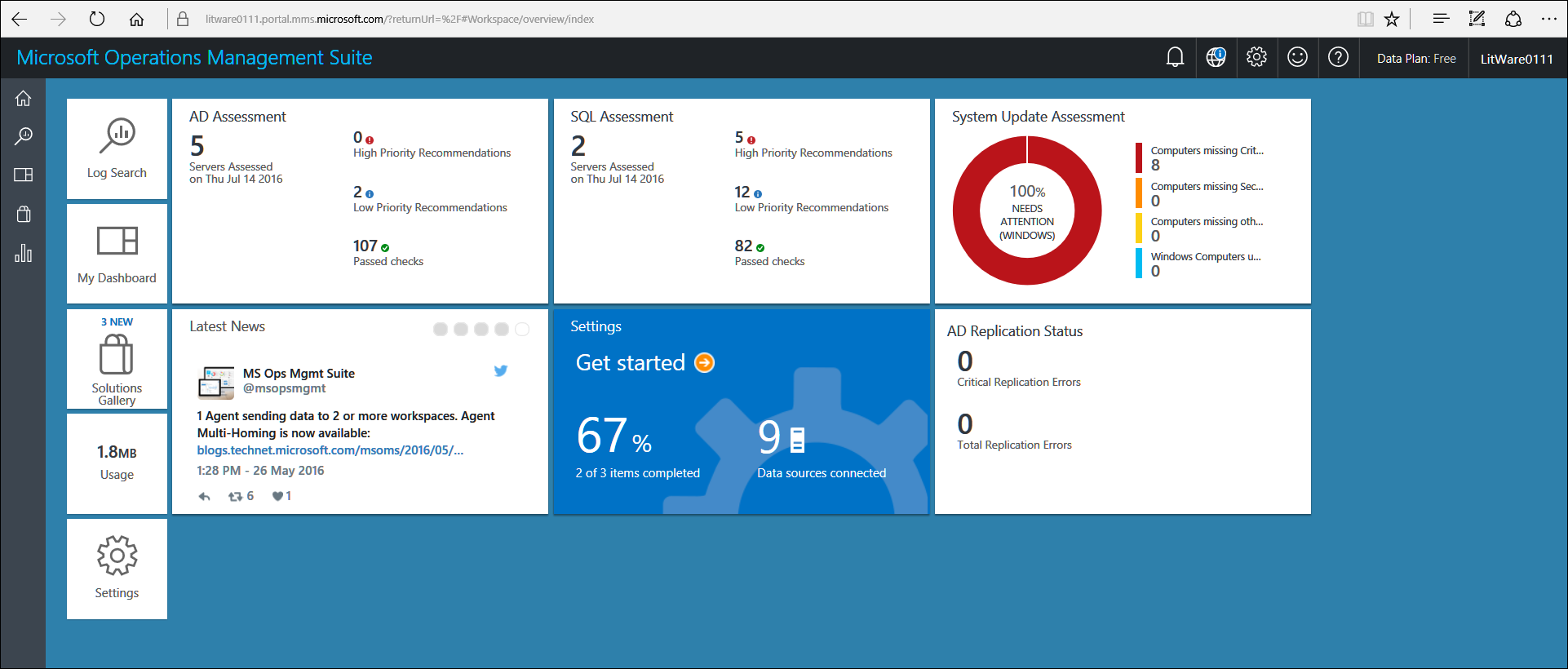
* 1. System Update Assessment

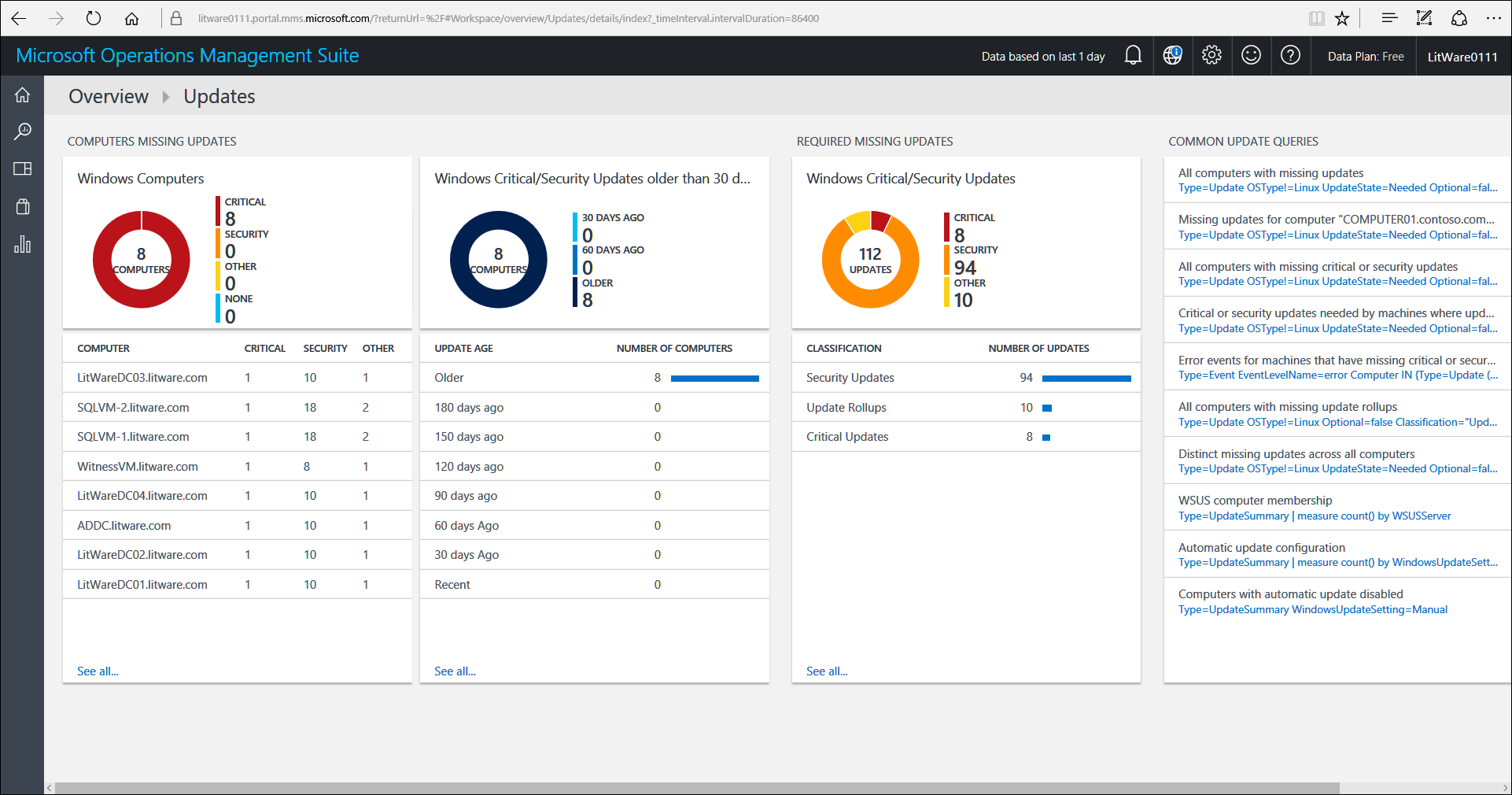


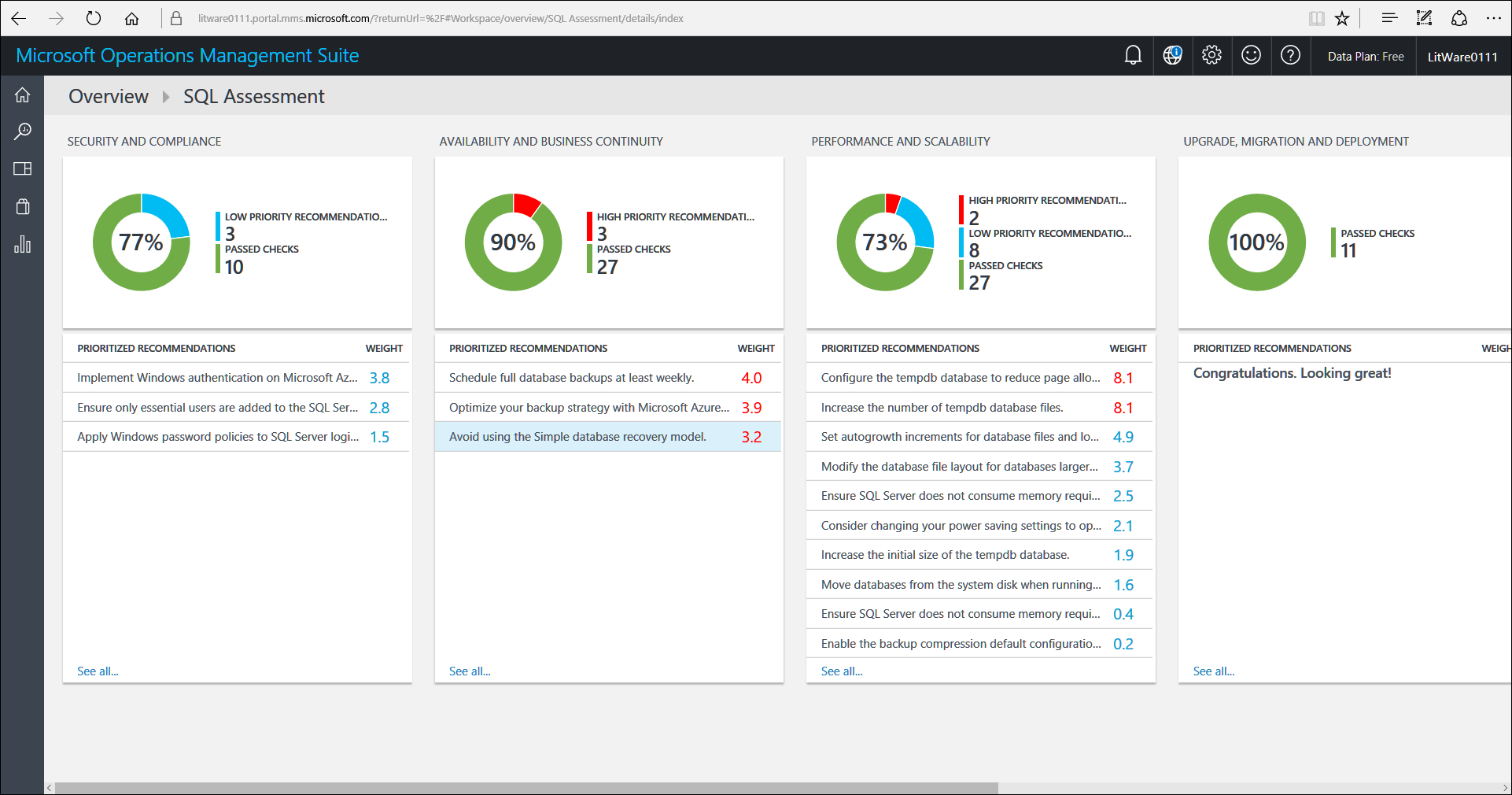
1. Make note of the other options that are available from the Gallery.

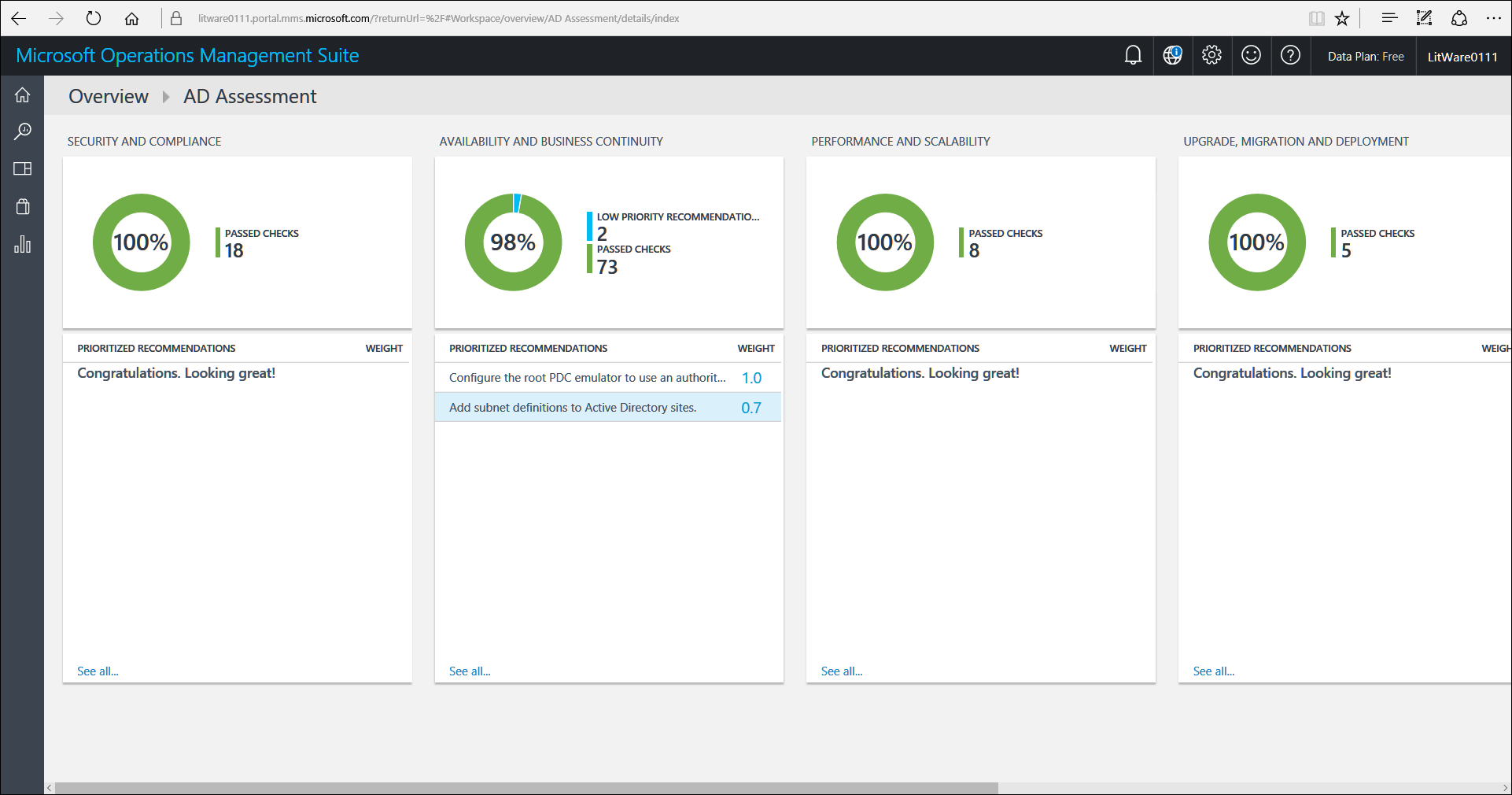
NOTE: These assessments will begin and will inform you that it will take some time for these to be complete. Give these some time to complete as you perform other tasks. You may need to check them even after the Hackathon is complete for data.

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







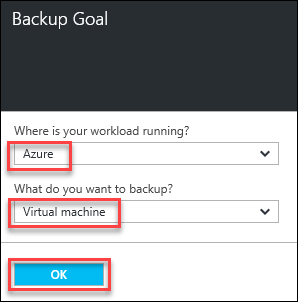


### Task 3: Configure Backups of IaaS Servers in Vaults (Region 1 and 2)

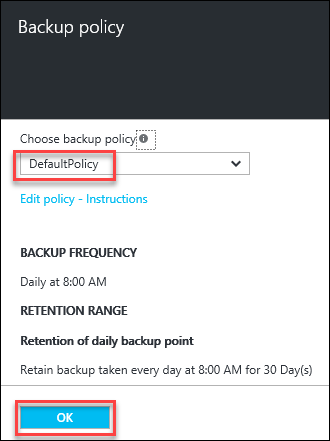
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click on **LitWareVault1** on the Azure Portal Dashboard.
3. Click **Backup >** in the **GETTING STARTED** section.



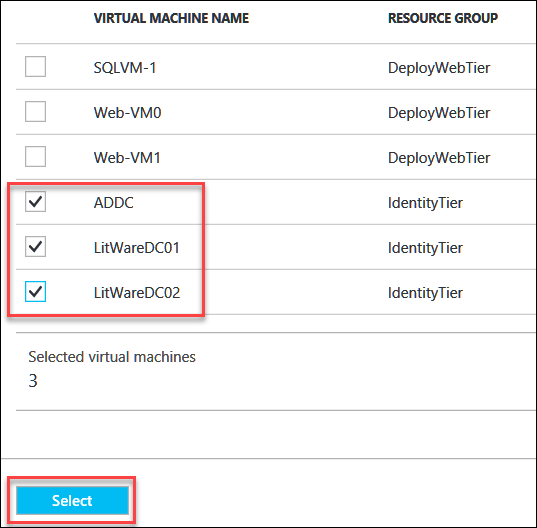
1. In the **Getting started with backup**, choose the **Backup Goal** of Azure and Virtual machine then click **OK** to continue.



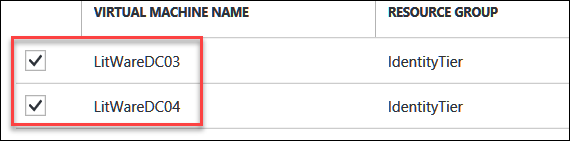
1. In the **Backup policy** blade, leave the settings at the DefaultPolicy and click the **OK** button to continue.



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



1. This will configure the machines to be backed up via Azure Backup in the **South Central US** region.
2. Repeat Steps 2-6 for **LitWareVault2** to be able to backup IaaS VMs in the **North Central US** region.

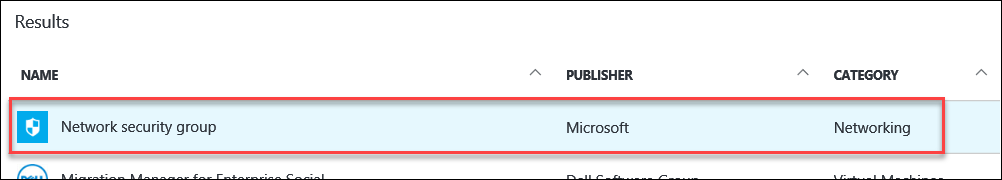


### Task 4: Configure Network Security Groups as Needed (Region 1 and 2)

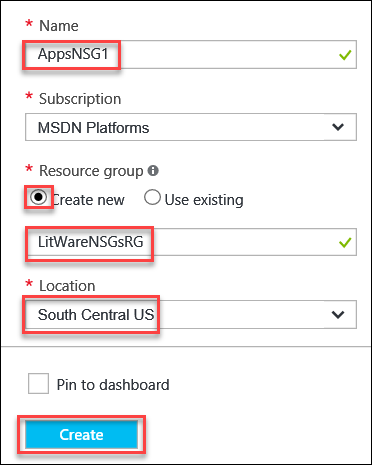
1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. Click **+ New**.



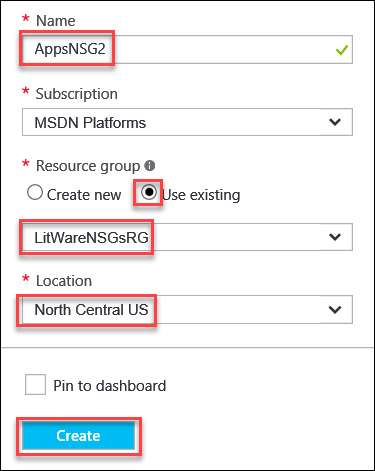
1. In the **Search the marketplace** window, type **Network Security Group** and hit enter.
2. In the resulting **Everything** blade choose **Network security group** by **Microsoft** as the publisher.



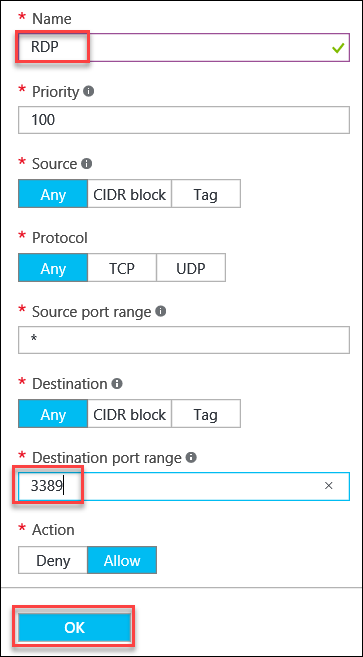
1. Leave the deployment model as **Resource Manager** and click the **Create** button to continue.
2. In the **Settings** blade, enter the following:
   1. Name: **AppsNSG1**
   2. Subscription: **Select your subscription**
   3. Resource Group: **Create new – LitWareNSGsRG**
   4. Location: **South Central US**
   5. Click the **Create** button to complete the creation of the NSG.



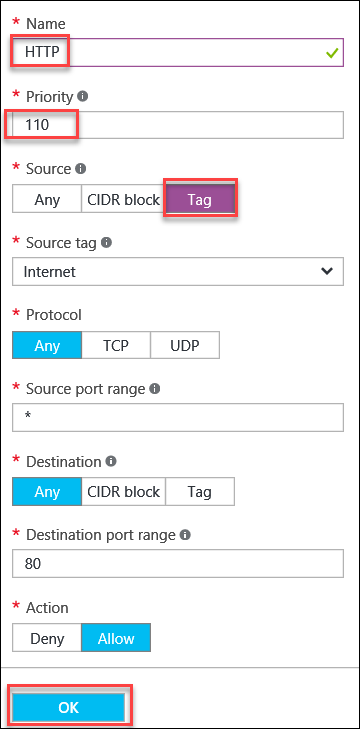
1. Repeat Steps 2-6 for **DataNSG1**, and **IdentityNSG1** both in **South Central US**. Be sure for Resource Group to **Use existing – LitWareNSGsRG**.
2. Now use the **Browse >** menu item in the left pane on the Azure Portal and type **Network security groups** in the filter bar and select it from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



1. Repeat using the **+ Add** icon for **DataNSG2**, and **IdentityNSG2** both in **North Central US**. Be sure for Resource Group to **Use existing – LitWareNSGsRG**.
2. 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.



1. For both of the **AppsNSGs** be sure and add another Rule to allow Internet traffic with the following settings or your CloudShop app will no longer work:
   1. Name: **HTTP**
   2. Priority: **110**
   3. Source: **Tag**
   4. Source Tag: **Internet**
   5. Leave all the others at the defaults and click the **OK** button.

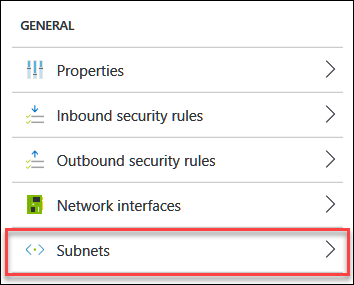


NOTE: Were this live production, there would be more explicit rules created and assigned. This is just an example how to create them for this Hackathon.

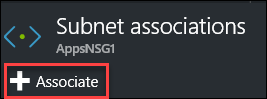
1. Now assign the appropriate NSGs to the correct **Subnet** in each region.
2. Click on **AppsNSG1** in the list of **Network security groups**.



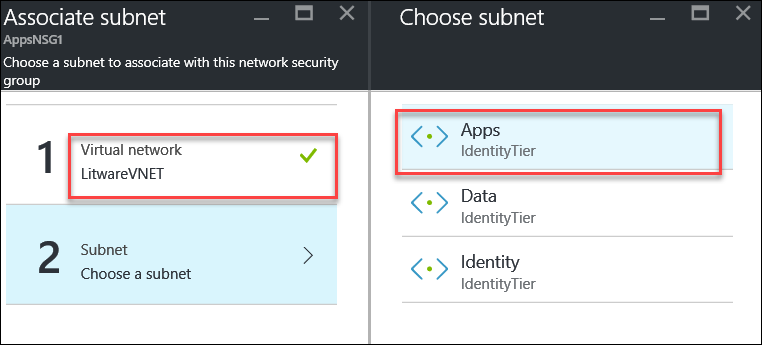
1. Select **Subnets >** from the **Settings** blade under the **GENERAL** heading.



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



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



1. Click the **OK** button to complete the association.
2. Repeat Steps 13-17 for **DataNSG1** and **IdentityNSG1** selecting the appropriate Subnet to associate them with in **LitwareVNET**.
3. Repeat Steps 13-17 for **AppsNSG2**, **DataNSG2**, and **IdentityNSG2** selecting 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 configured IaaS backups in both regions and finally, configured Network Security Groups as needed.