

M3

Open Visual Studio as an Administrator and select **File | Open | Project/Solution** and browse to **C:\AzurelaaSWS\M3 - Azure Storage\Labs\Exercise1\Begin\DeployStorage** and select the **DeployStorage.sln** file.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

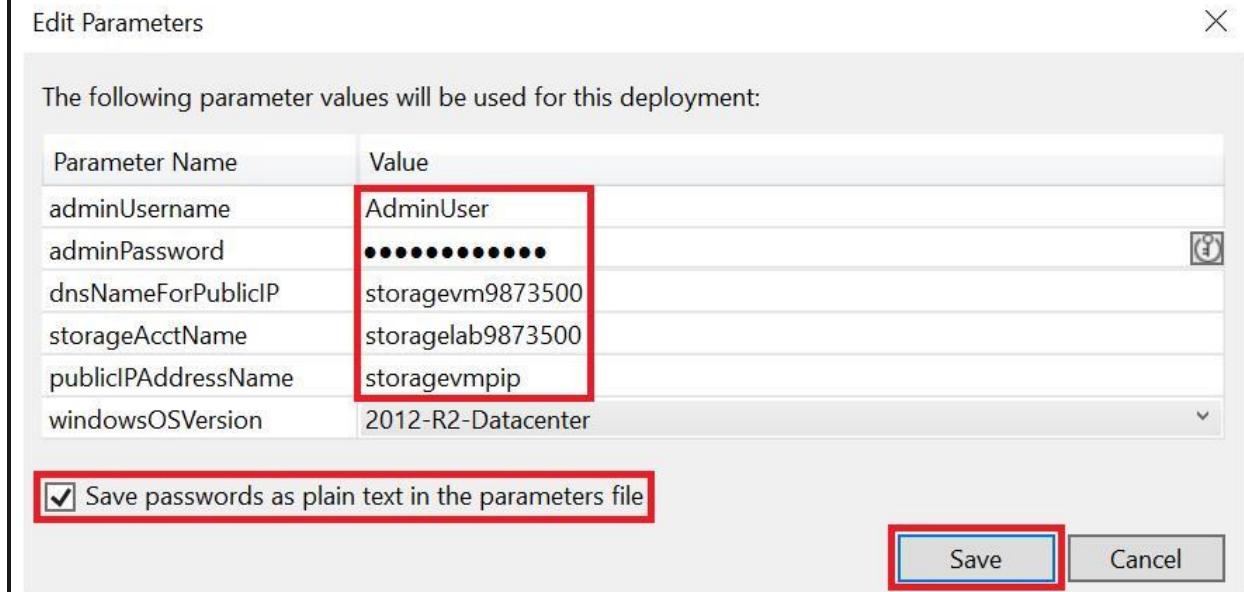
6 Hr 42 Min Remaining

Instructions Resources Help 100%

Task 2 - Deploy your Azure Resource Manager (ARM) template

1. Right-click on the **DeployStorage** project and select **Deploy | New...**
2. In the *Deploy to Resource Group* dialog box, click the **Add an account...** button and sign in using your **Azure Trial Pass** credentials.
3. Once you are signed in to Azure, click the Resource group dropdown menu and select the **storageLab-1odXXXXXX** resource group e.g. **storageLab-1od9873500**.
4. Click on the **Edit Parameters** button. Fill in the required parameters, ensuring that the **dnsNameForPublicIP** is unique in all of Azure. After filling in the parameters, make sure you check the **Save passwords as plain text in the parameters file** checkbox and then click the **Save** button. Note the password for later use.

Append your student number to naming values that require global uniqueness e.g. storagelab9873500 for a storage account name.



Parameter	Value
adminUsername	Enter the RDP login user name for the VM AdminUser
adminPassword	Enter the RDP login password for the VM P@55word1234
dnsNameForPublicIP	Although it is optional to provide a DNS name for your VM, in this lab you will need to provide a dns name unique in all of Azure.
storageAcctName	The name of your new storage account that will be created. Must be unique in all of Azure.
publicIPAddressName	This name will be used for the reserved public IP address used by the VM
windowsOSVersion	Leave the setting as is

5. Select the **Deploy** button on the Deploy to Resource Group dialog box. The deployment should take around 8 to 10 minutes.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

6 Hr 40 Min Remaining

Instructions Resources Help 100%

Task 3 - Confirm Deployment of your Azure Resource Manager (ARM) template

1. If the Visual Studio deployment succeeded, you will see something similar to the following in the Visual Studio output window, otherwise, correct any errors that appear within the Visual Studio output window and redeploy your template.

```
15:02:29 - Outputs          :
15:02:29 - OutputsString    :
15:02:29 - 
15:02:30 - 
15:02:30 - 
15:02:30 - Successfully deployed template 'windowsvirtualmachine.json' to resource group 'storageLab-1od9873500'.
```

2. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials. Then click Resource groups, then click **storageLab-lodXXXXXX** e.g. **storageLab-lod9873500**, and confirm that the resources have been successfully deployed. You can also click on the link for more details about your deployment.

storageLab-lod9873500 Resource group

Search (Ctrl+ /) Overview Add Edit columns Delete resource group Refresh Export to CSV Open query JSON View

Activity log Access control (IAM) Tags Events

Essentials

Subscription (change)
ASD Developer 1

Subscription ID
cd5624ee-c42c-4f43-9c6d-4aea23072cf3

Tags (change)
Click here to add tags

Deployments
1 Succeeded

Location
West US 2

3. Record the name of the new storage account, this will be required later on.

storageLab-lod9873500 Resource group

Search (Ctrl+ /) Overview Add Edit columns Delete resource group Refresh Export to CSV Open query JSON View

Activity log Access control (IAM) Tags Events

Settings

- Resource costs
- Deployments
- Security
- Policies
- Properties
- Locks

Monitoring

- Insights (preview)

Essentials

Subscription (change)
ASD Developer 1

Subscription ID
cd5624ee-c42c-4f43-9c6d-4aea23072cf3

Tags (change)
Click here to add tags

Filter for any field... Type == all Location == all Add filter

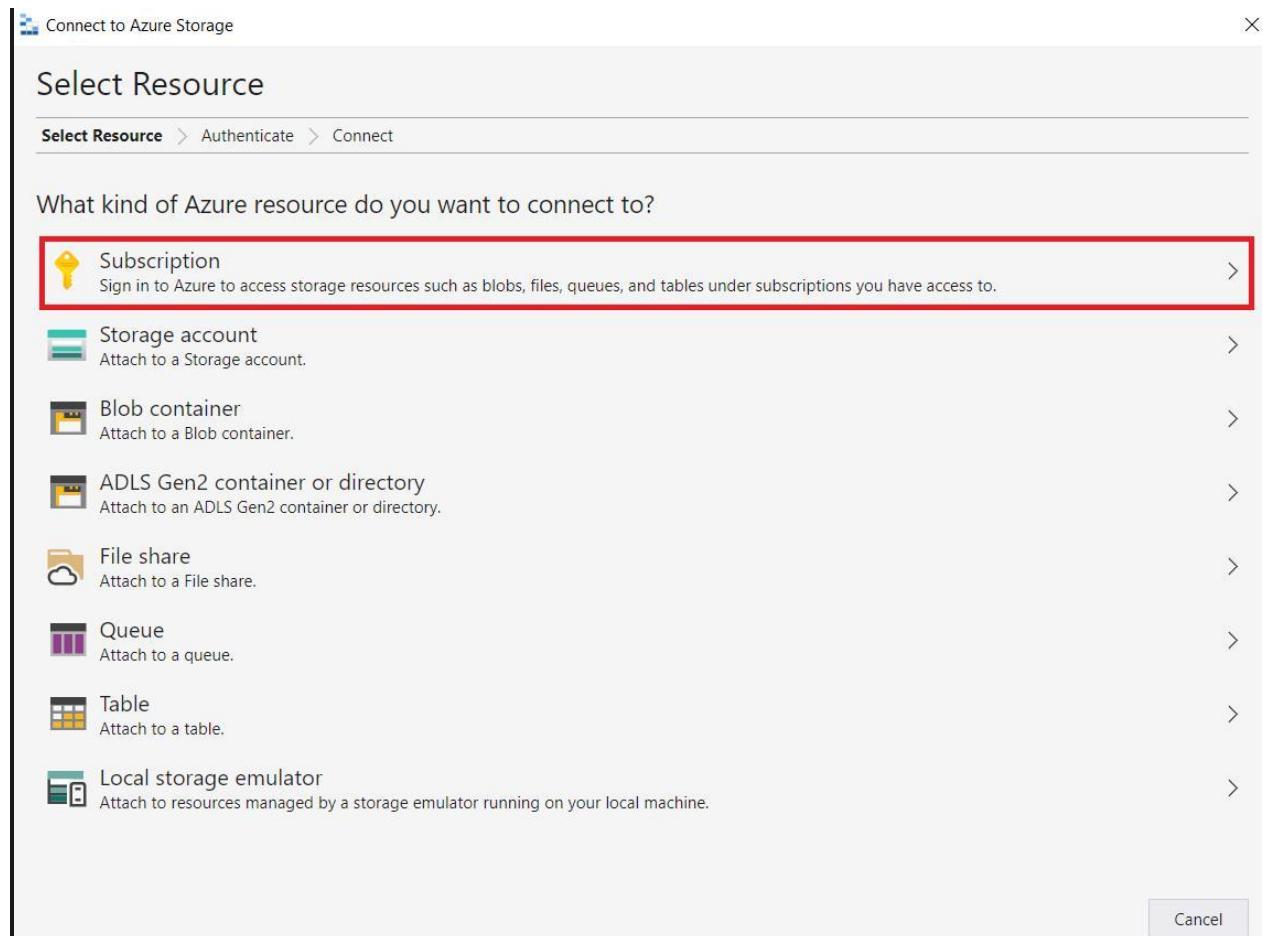
Showing 1 to 6 of 6 records. Show hidden types No grouping

Name	Type	Location
myVMNic	Network interface	West US
MyVNET	Virtual network	West US
MyWindowsVM	Virtual machine	West US
MyWindowsVM-nsg	Network security group	West US
storagelab9873500	Storage account	West US

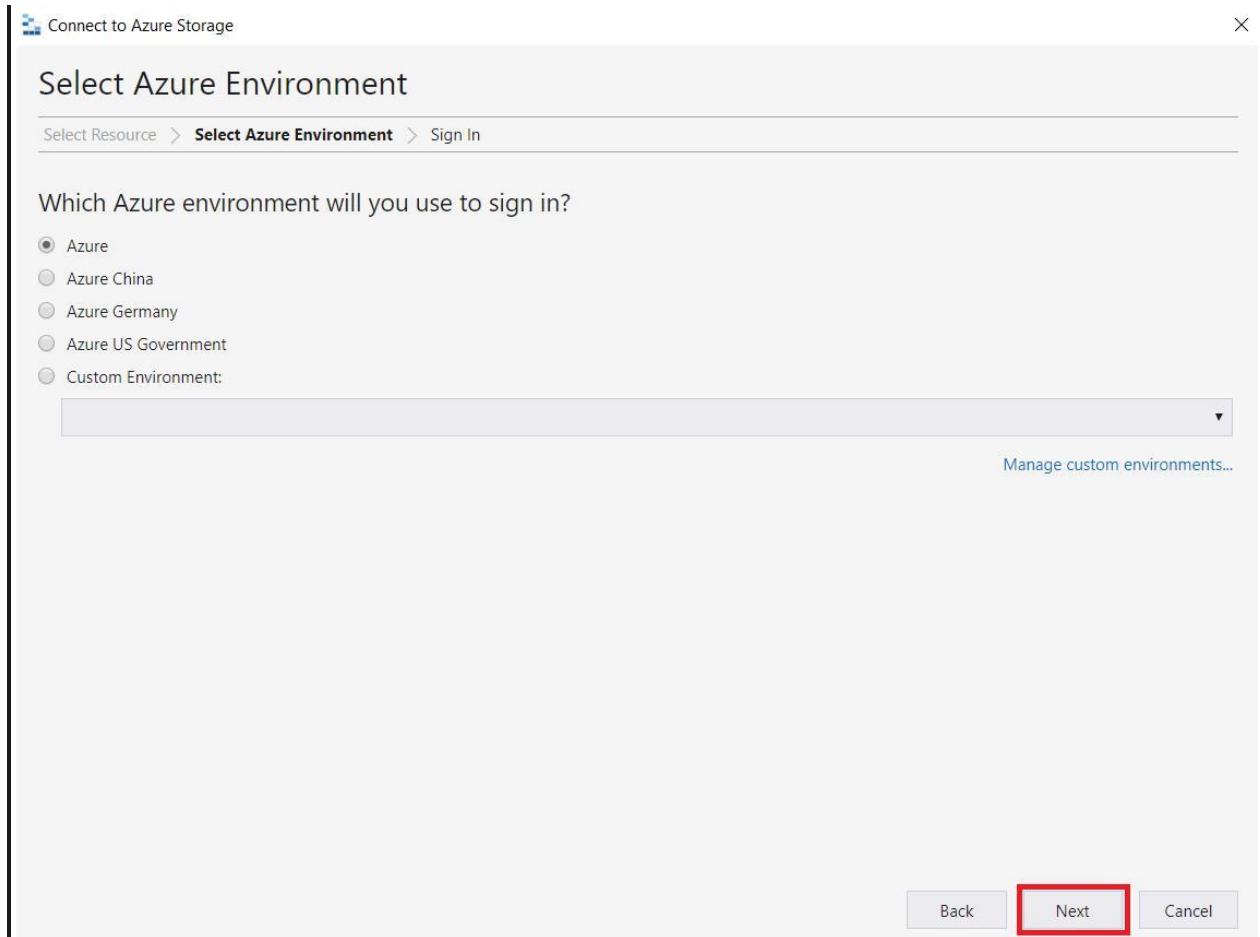
Task 4 - Install the Microsoft Azure Storage Explorer

There are many ways to analyze data that is sent to Azure storage. You can use Visual Studio, the Azure Portal, the Azure command line interface or the REST API. For this lab, you will use a free tool named Microsoft Azure Storage Explorer.

1. Use your web browser to browse to <http://storageexplorer.com>.
2. Select the Windows OS, then click on the **Download now** button and download the utility to your hard drive.
3. Install the Storage Explorer utility and select the option to **Launch Microsoft Azure Storage Explorer** at the end and click **Finish**.
4. When the Storage Explorer window opens, you will need to log in to your Azure account. At the top of the **Connect to Azure Storage** window, click on the **Subscription** tile. If you don't see the window then from the left-hand pane of Storage Explorer click on the icon that looks like a person and then click the **Add an account** link. This will present you with the window.



5. Ensure that the **Azure** environment has been selected and click Next.



6. Sign in to your Azure subscription using your Azure Trial Pass credentials.



Sign in to your account



Microsoft Azure



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Next



Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...

- Once Storage Explorer has logged in to Azure, click on the **Storage Explorer** button in the top left-hand corner, this will display your local and Azure storage. Using the

storage account name that you recorded earlier, you will be able to locate the new storage account that you created with the ARM template from here.

The screenshot shows the Azure Explorer interface. On the left is a vertical toolbar with icons for Home, User, Power, and Settings. The main area is titled 'EXPLORER' and contains a search bar with 'Search for resources' and a magnifying glass icon. Below the search bar are 'Collapse All' and 'Refresh All' buttons. A 'Quick Access' section is shown, followed by a tree view of resources. Under 'Local & Attached', there is a 'Storage Accounts' node, which has three children: 'storagegelab9873500' (highlighted with a red box), 'vhdstoragej3tvjmo7lxolm', and 'vhdstoragezn3vj6oupaxbk'. Under another node, there is a 'Disks' node with six child items: 'armPolicyLab-lod9873500', 'armPSLab-lod9873500', 'armVSLab-lod9873500', 'automationLab-lod9873500', 'backupLab-lod9873500', and 'identityLab-lod9873500'.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

6 Hr 39 Min Remaining

Instructions Resources Help 100%

Task 5 - Review metrics information being gathered

In a previous task, you added Microsoft Azure Diagnostics to your ARM template. The diagnostics settings have an abundance of performance counter configurations and settings which will be gathered and pushed out to an Azure storage table named **WADPerformanceCountersTable**. You will then view this table data.

1. From within Storage Explorer, locate your new storage account, then expand it, then expand **Tables** and then click on **WADPerformanceCountersTable**.

EXPLORER

Search for resources × 🔍

[Collapse All](#) [Refresh All](#)

- Quick Access
- Local & Attached
 - Storage Accounts
 - Cosmos DB Accounts (Deprecated)
 - Data Lake Storage Gen1 (Preview)
- ASD Developer 1 (Student-9873500@lodsasdoutlook.onmicrosoft.com)
 - Storage Accounts
 - storagelab9873500
 - Blob Containers
 - File Shares
 - Queues
 - Tables
 - \$MetricsCapacityBlob
 - \$MetricsHourPrimaryTransactionsBlob
 - \$MetricsHourPrimaryTransactionsFile
 - \$MetricsHourPrimaryTransactionsQueue
 - \$MetricsHourPrimaryTransactionsTable
 - SchemasTable
 - WADDiagnosticInfrastructureLogsTable
 - WADMetricsPT1HP10DV2S20210320
 - WADMetricsPT1MP10DV2S20210320
 - WADPerformanceCountersTable
 - Disks
 - armPolicyLab-lod9873500
 - armPSLab-lod9873500
 - armVSLab-lod9873500
 - automationLab-lod9873500

2. Within the table output window, you should be able to see the current metrics that have been gathered. From within this window, you can do sorting, querying, exporting of the data and many more activities.

WADPerformanceCountersTable			
PartitionKey	RowKey		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000042955581...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000085905254...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000171804600...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000214754273...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000257703946...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000300653619...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000343603292...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000386552965...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000429502638...		
06370277052000000000	3e1fcc3e-3172-4685-8063-d9be2dca7fa6__IaaS__MyWindowsVM__00000000472452311...		

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

6 Hr 38 Min Remaining

Instructions Resources Help 100%

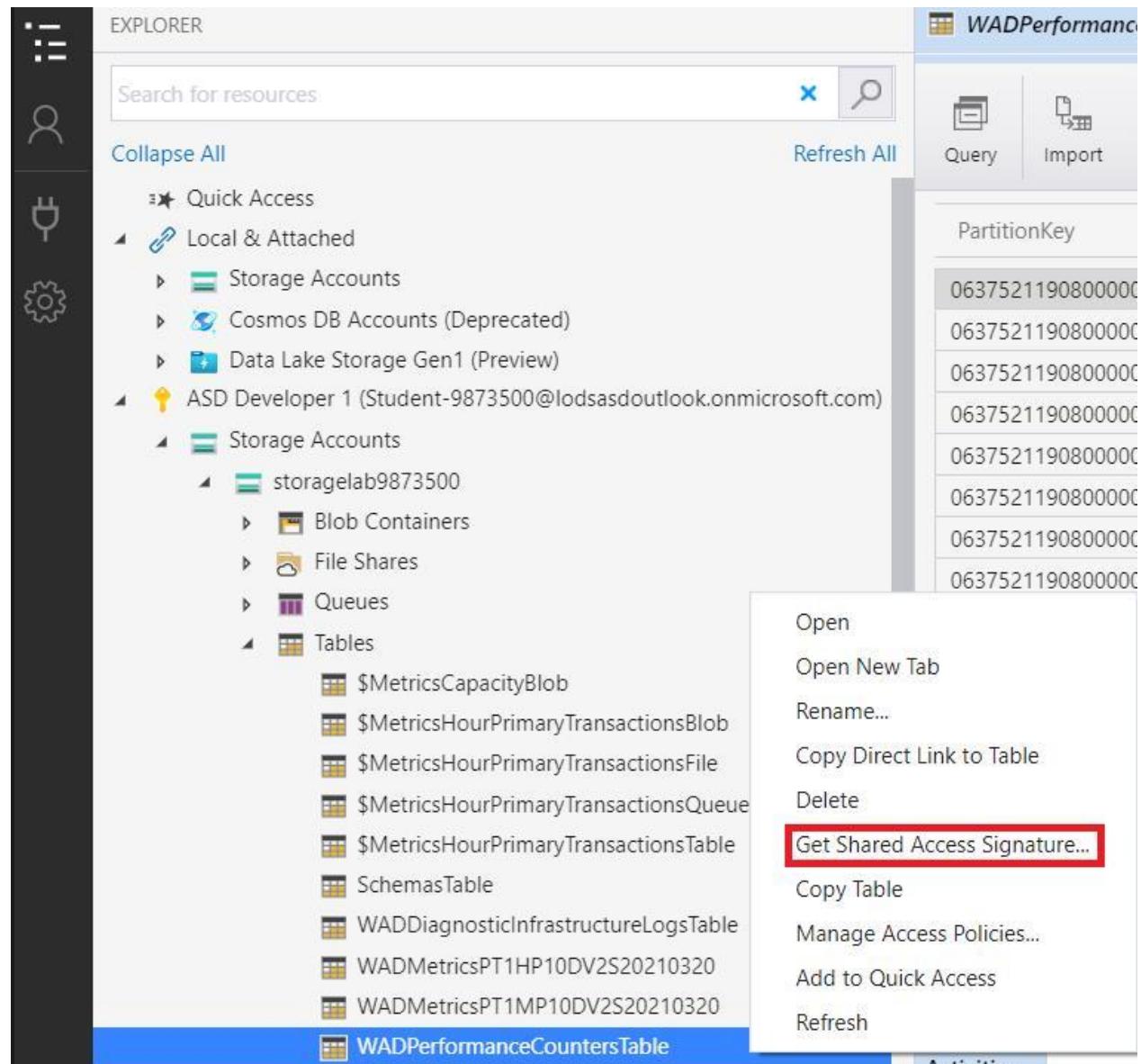
Exercise 2 - Allow access to Azure Storage table data

In this lab exercise, you will create a Shared Access Signature (SAS) key that will be used to allow another person access to the table storage data that has been generated in the previous exercise. This type of SAS key can be beneficial when needing to allow temporary access to your data without giving full access to the rest of your storage account.

Task 1 - Create the SAS Key

Your QA team would like access to the performance counter data you have gathered, therefore, you want to give them access to only the **WADPerformanceCountersTable**.

- From within Storage Explorer, right click on the **WADPerformanceCountersTable** table. Select the **Get Shared Access Signature...** menu item.



- In the Shared Access Signature dialog box, you can set a valid time limit that the key will be valid for, but in this case, leave the default value you see in your own windows as

it is. Make sure though that you only allow **Query** access and then select the **Create** button.

Shared Access Signature X

Shared Access Signature

Access policy: none ▾

Start time: 10/30/2020 01:22 AM

Expiry time: 10/31/2020 01:22 AM

Time zone:

Local
 UTC

Permissions:

Query
 Add
 Update
 Delete

Entity restrictions (optional):

Start: Starting partition key , Starting row key

End: Ending partition key , Ending row key

[Learn more about permissions](#)

Create Cancel

3. The SAS key will be generated. Copy the key to your clipboard, then click **Close**.



Shared Access Signature

X

Shared Access Signature

Table:

WADPerformanceCountersTable

URI:

<https://storagelab9873503.table.core.windows.net/WADPerformanceCountersTable>

Copy

Query string:

?st=2020-10-30T00%3A22%3A32Z&se=2020-10-31T00%3A22%3A30Z&srtoken=4f3a2a0a-1a2d-4e0c-a2a0-000000000000&sp=rw&sv=2019-02-02&sr=c

Copy

Back

Close

4. Paste the SAS key into Notepad within the hosted lab machine.



*Untitled - Notepad
File Edit Format View Help
<https://storagelab9873500.table.core.windows.net/WADPerformanceCountersTable?st=2021-03-24T13%3A10%3A32Z&se=2021-03-24T13%3A10%3A32Z&sp=r&sv=2018-03-28&tn=wadperformancecounterstable&sig=RRag0qjDHQs8cDUXUFaGULS911LnHzsQNhWzqeZ2YZ4%3D>

5. Your key should look something similar to this: <https://storagelab9873500.table.core.windows.net/WADPerformanceCountersTable?st=2021-03-24T13%3A10%3A32Z&se=2021-03-24T13%3A10%3A32Z&sp=r&sv=2018-03-28&tn=wadperformancecounterstable&sig=RRag0qjDHQs8cDUXUFaGULS911LnHzsQNhWzqeZ2YZ4%3D>

For ease of reading, the QA team should also be using Microsoft Azure Storage Explorer. In the next task, you will learn how to use the SAS key to retrieve the performance counter data.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

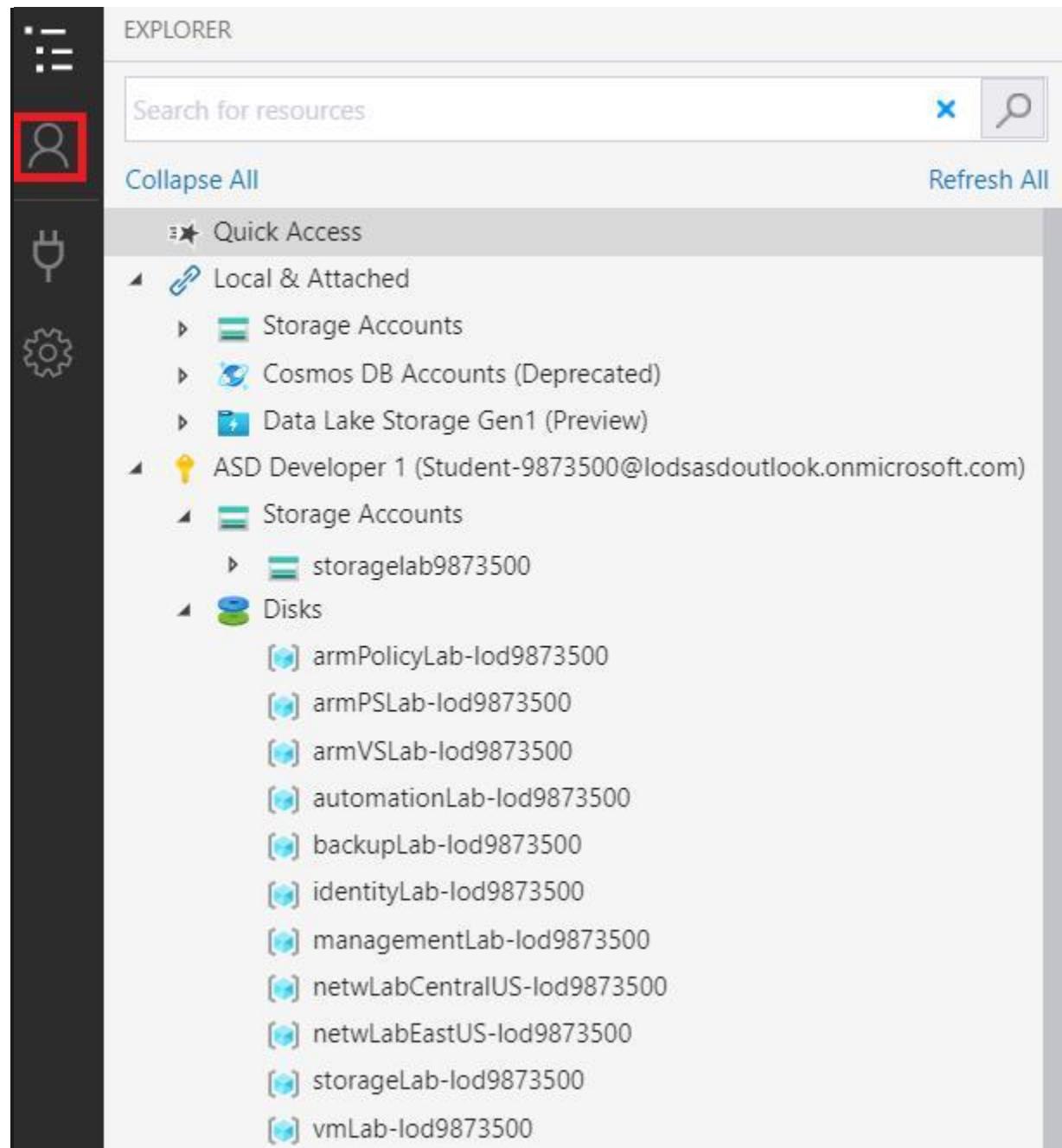
6 Hr 38 Min Remaining

Instructions Resources Help 100%

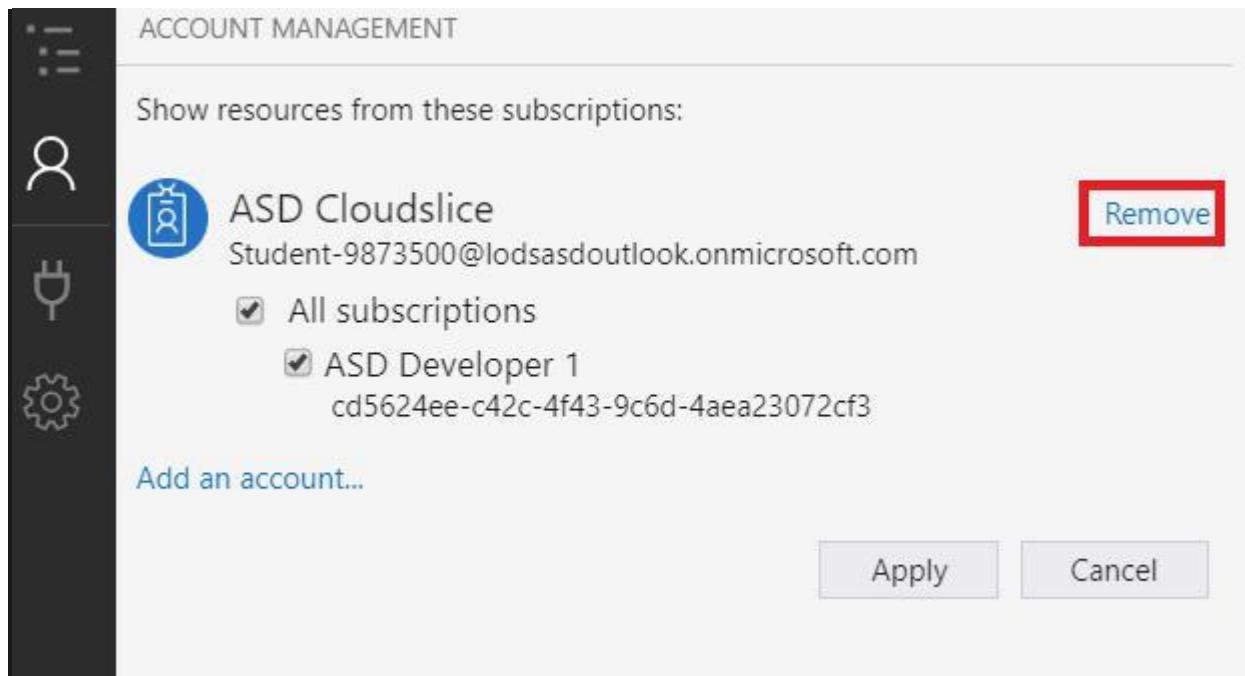
Task 2 - Using the SAS Key to query the table data

In the previous task, you created a SAS key and copied it to Notepad.

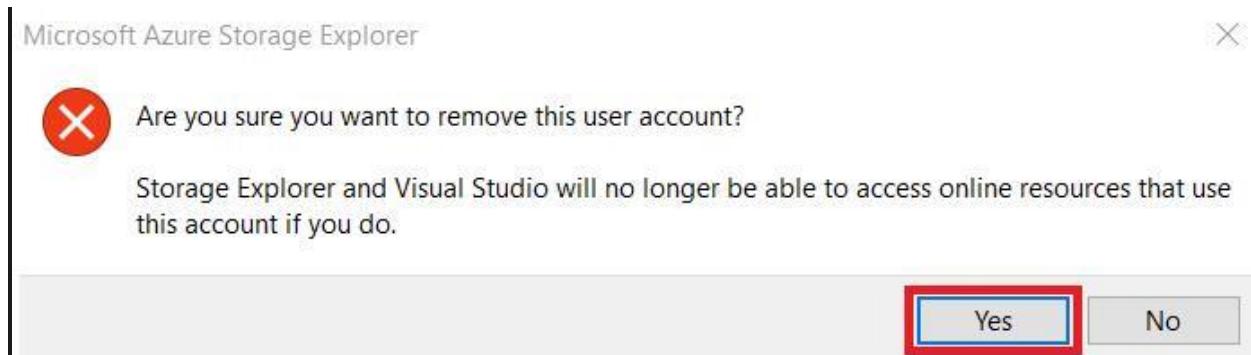
1. Open Microsoft Azure Storage Explorer and click on the **Manage Accounts** tile.



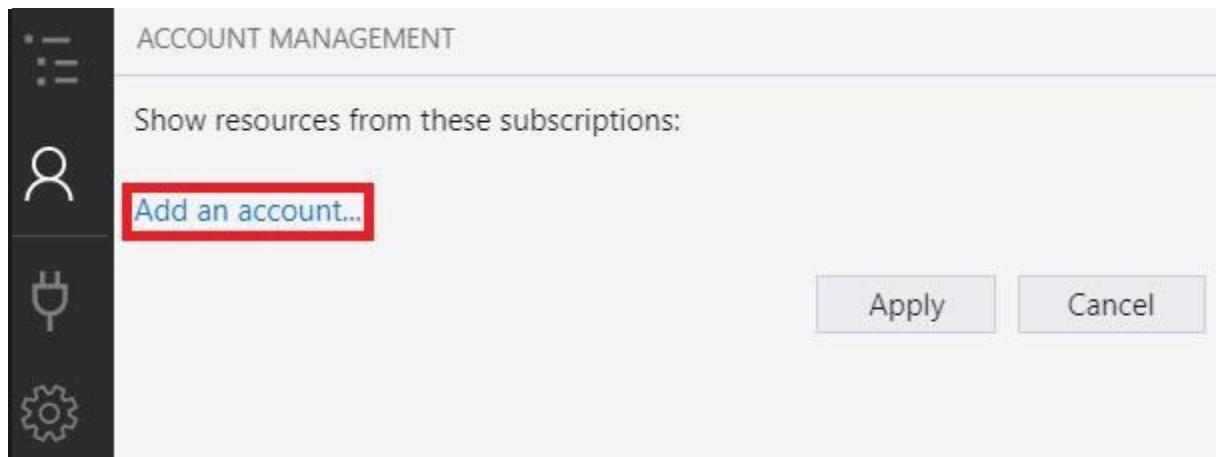
2. Then click the **Remove** link. This will remove your existing account so that you are able to test the SAS key.



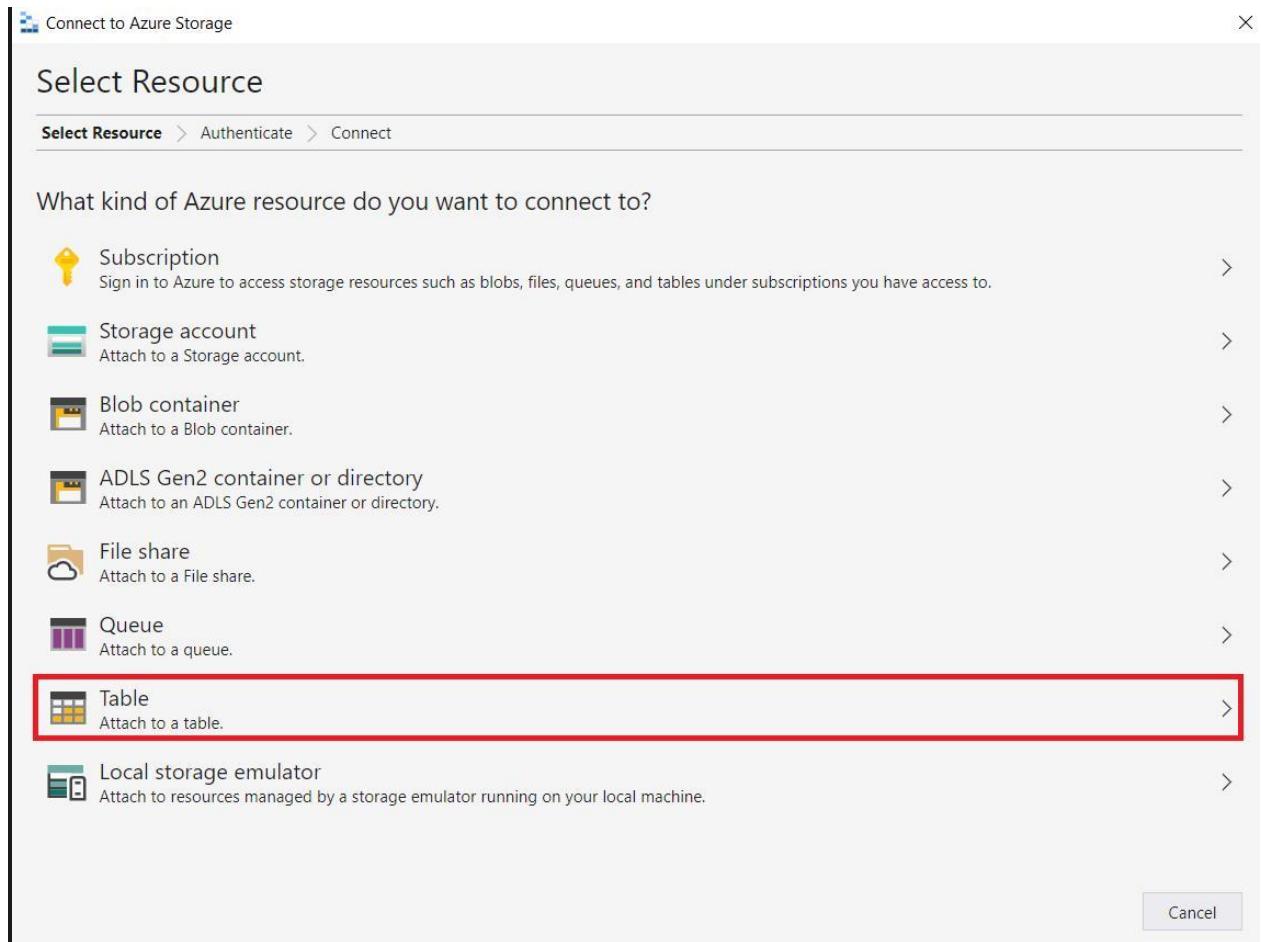
3. Click **Yes** to the Microsoft Azure Storage Explorer alert dialog box.



4. Click the **Add an account** link.



5. Click on the **Table** tile.



6. Copy the SAS Key from the Notepad file from the previous task and paste it into the **Table SAS URL:** text box. Then click the **Next** button.

Connect to Azure Storage

Enter Connection Info

Select Resource > **Enter Connection Info** > Summary

Display name:

Table SAS URL:

<https://storageblob9873502.table.core.windows.net/WADPerformanceCountersTable?st=2021-03-24T16%3A38%3A11Z&se=2021-03-25T16%3A38%3A11Z&sp=r&sv=2018-03-28&tn=wadperformancecounterstable&sig=SIlzwjRCZRj17e%2BqJ0l4q8E9Yd0hDQMpxOExGZ5CxXc%3D>

Back **Next** **Cancel**

7. Click **Connect** at the **Summary** page. You should then see the performance counter output data.

EXPLORER

Search for resources

WADPerformanceCountersTable

PartitionKey	RowKey	Timestamp	PreciseTimeStamp
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_000000004295558154	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_000000008590525450	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000012885492746	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000017180460042	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000021475427338	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000025770394634	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000030065361930	2020-10-29T23:10:40.233Z	2020-10-29T23:09:07.823Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_000000004360329226	2020-10-29T23:10:40.233Z	2020-10-29T23:09:22.825Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000038655296522	2020-10-29T23:10:40.233Z	2020-10-29T23:09:22.825Z
063739609740000000	2e453399-8d2f-4d9c-9b8f-f24ae656fc93_laaS__MyWindowsVM_0000000042950263818	2020-10-29T23:10:40.233Z	2020-10-29T23:09:22.825Z

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

Exercise 3 - Using Azure Files

In this lab exercise, you will be creating a file share and a directory within the file share using Azure Files and then you will RDP in to your VM to connect to the file share.

Task 1 - Create your file share and directory

1. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
2. Find and browse to the **storageLab-lodXXXXXX** e.g. **storageLab-lod9873500** resource group. Within the resource group, click on the storage account you created earlier.

The screenshot shows the Azure Portal interface for the resource group 'storageLab-lod9873500'. The left sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Events' under 'Essentials'. Below these are sections for 'Settings' (Resource costs, Deployments, Security, Policies, Properties, Locks) and 'Monitoring' (Insights (preview)). The main content area displays resource details for 'ASD Developer 1' (Subscription ID: cd5624ee-c42c-4f43-9c6d-4aea23072cf3). A table lists resources: myVMNic (Network interface, West US 2), MyVNET (Virtual network, West US 2), MyWindowsVM (Virtual machine, West US 2), storagelab9873500 (Storage account, West US 2), and storagevmpip (Public IP address, West US 2). The 'storagelab9873500' row is highlighted with a red box.

Name	Type	Location
myVMNic	Network interface	West US 2
MyVNET	Virtual network	West US 2
MyWindowsVM	Virtual machine	West US 2
storagelab9873500	Storage account	West US 2
storagevmpip	Public IP address	West US 2

3. In the storage account blade, select the **File shares** tile.

4. Click on the **+ File share** toolbar tile.

5. Enter a name for your file share, then set a quota of 1 GiB and then click the **Create** button.

New file share

X

Name *

xyzfileshare



Quota ⓘ

1



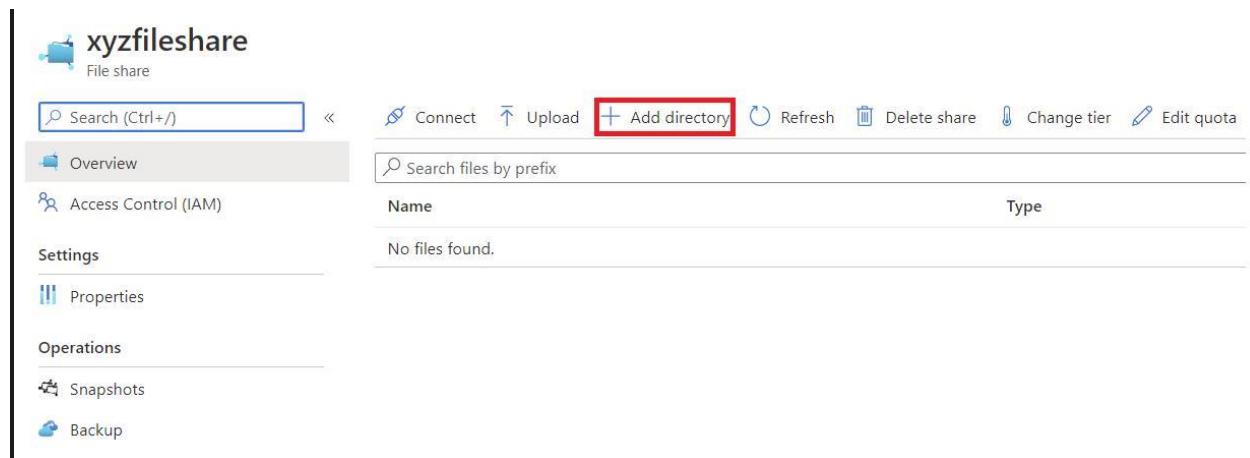
Set to maximum

GiB

Create

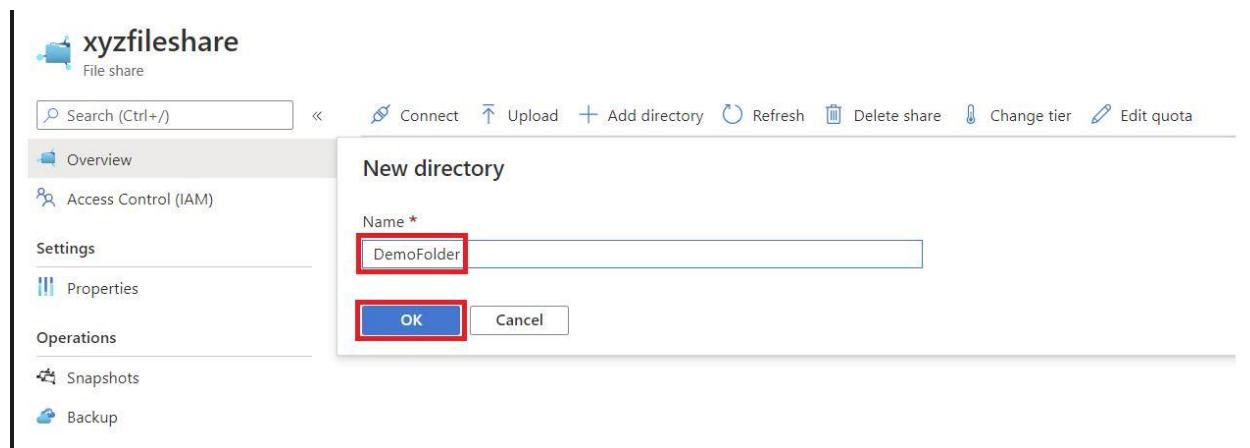
Discard

6. Click on the newly created file share name and then select the **Add directory** toolbar tile.



The screenshot shows the Azure portal interface for a file share named 'xyzfileshare'. On the left, there's a sidebar with options like Overview, Access Control (IAM), Settings, Properties, Operations, Snapshots, and Backup. The 'Overview' tab is selected. At the top, there's a toolbar with icons for Connect, Upload, Add directory (which is highlighted with a red box), Refresh, Delete share, Change tier, and Edit quota. Below the toolbar, there's a search bar labeled 'Search files by prefix' and a table with columns 'Name' and 'Type'. The table currently displays the message 'No files found.'

7. Add a new directory name and click the **OK** button.



The screenshot shows a 'New directory' dialog box overlaid on the file share overview page. The dialog has a title 'New directory' and a 'Name *' field containing 'DemoFolder'. There are 'OK' and 'Cancel' buttons at the bottom, with 'OK' also highlighted with a red box.

Prior to RDPing to the VM that you will be using to map this file share to, you can retrieve the connection command that should be used from within the VM to map to the share.

1. In the File share blade, click the **Connect** tile, then click the '**Click to copy**' button next to the command box.

The screenshot shows the Azure Storage File Share blade for a resource named 'xyzfileshare'. On the left, there's a sidebar with options like Overview, Access Control (IAM), Settings, Properties, Operations, Snapshots, and Backup. The main area has a search bar, a toolbar with 'Connect', 'Upload', 'Add directory', 'Refresh', and 'Delete' buttons, and a list of files. A file named 'DemoFolder' is visible. To the right, there's a detailed section for connecting from Windows, which includes a note about secure transfer requiring SMB 3.0 encryption, a 'Drive letter' dropdown set to 'Z', and a PowerShell command block:

```
$connectTestResult = Test-NetConnection -ComputerName storageblob9873502.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:storageblob9873502.file.core.windows.net" /user:"Azure\storageblob9873502"
    /pass:"YwqLaMKa2yrcU8tNnBicsBF846DozREZpBaLsqlv9/L52LUeHUo0gRvXktjPP1KjPh9pWaCqszbid82vIiAB0Q="""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root "\storageblob9873500.file.core.windows.net\xyzfileshare"
-Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
}
```

Below this, there's a note about port 445 and a link to learn how to circumvent the problem using a VPN.

- Paste the result into Notepad for use later on.

The screenshot shows a Notepad window with the title '*Untitled - Notepad'. The content of the window is the same PowerShell script shown in the previous screenshot, intended for copying and pasting into a local environment.

```
$connectTestResult = Test-NetConnection -ComputerName storageblob9873500.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:storageblob9873500.file.core.windows.net" /user:"Azure\storageblob9873500"
    /pass:"YwqLaMKa2yrcU8tNnBicsBF846DozREZpBaLsqlv9/L52LUeHUo0gRvXktjPP1KjPh9pWaCqszbid82vIiAB0Q="""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root "\storageblob9873500.file.core.windows.net\xyzfileshare"
-Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
}
```

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 42 Min Remaining

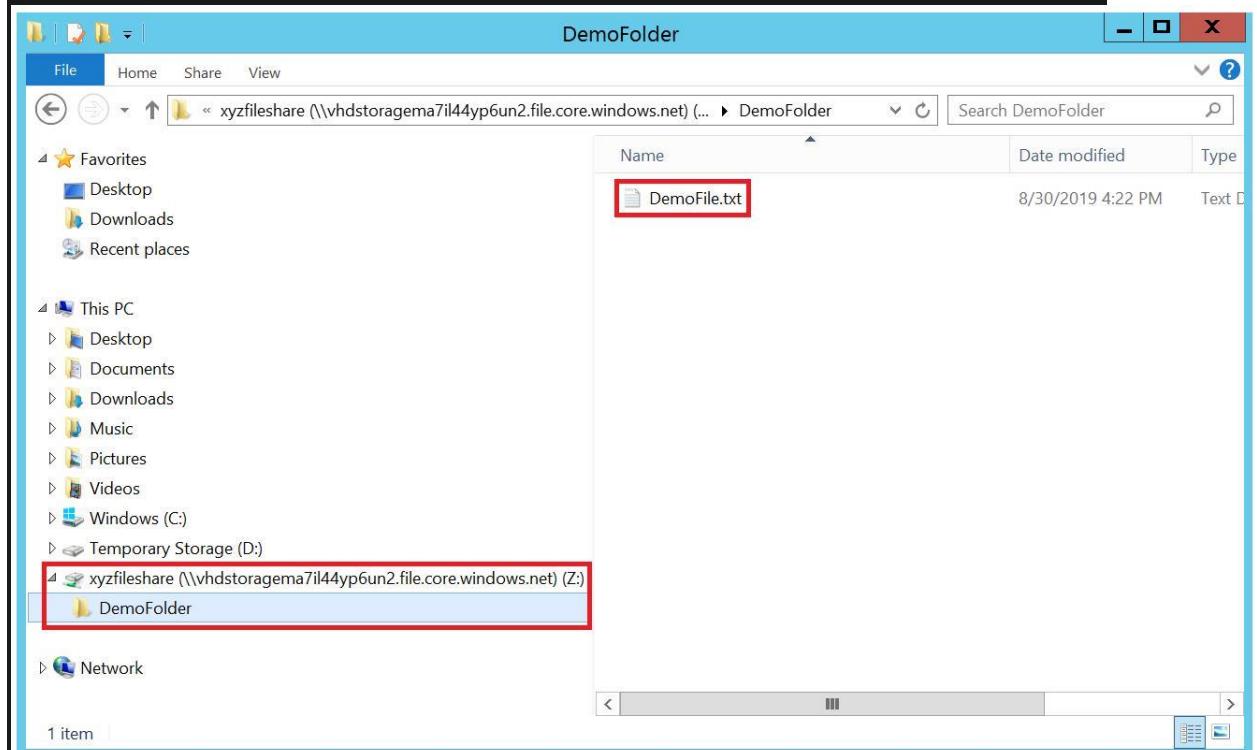
Instructions Resources Help 100%

Task 2 - RDP in to your VM and connect to the file share

- From within your resource group, click on the virtual machine icon. When the virtual machine blade opens, click the **Connect** toolbar icon at the top of the blade, download the RDP file and enter the credentials **AdminUser** and **P@55word1234** to log in to the server.

2. From within the VM, right-click on the Windows icon (lower left corner of screen) and select **Windows PowerShell (Admin)** to open a console window.
3. Return to Notepad and copy and paste the entire command expression into the command prompt window and press Enter. This will add a key credential to the VM and map your Azure file share.
4. From within your VM, open up Windows Explorer and browse to the Z: drive.

You should be able to browse to your directory and if you have already placed a file into the directory, you should be able to see and manipulate it. You can add files or folders into the share from within the VM, programmatically or from within the Azure portal.



Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

Module 4 - Introduction to Microsoft Azure Virtual Machine Scale Sets

Introduction

In this lab, you will deploy a Virtual Machine Scale Set that consists of two load balanced virtual machines that will serve as a web frontend. You will also deploy a virtual machine running Windows Server 2016 with SQL Server 2017, that will serve as a database backend for the web frontend. These machines will be networked on an Azure virtual network.

You'll learn how to:

- Create an Azure Virtual Machine Scale Set
- Create an Azure Virtual Machine
- Configure a pair of IIS Web Servers and connect them to a SQL Server running on a virtual machine that is connected to a virtual network
- Configure a SQL Server virtual machine
- Deploy sample Web applications to the IIS Web Servers
- Configure an Azure Load Balancer for incoming traffic from the Internet
- Test an Azure Load Balancer

Prerequisites

The following are required to complete this hands-on lab:

- Microsoft Azure PowerShell v.5.1.1 or later
- SQL Server PowerShell Extensions (SQLPSX) v.2.3.2.1 or later on the database VM
- A Microsoft Azure subscription

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 41 Min Remaining

Instructions Resources Help 100%

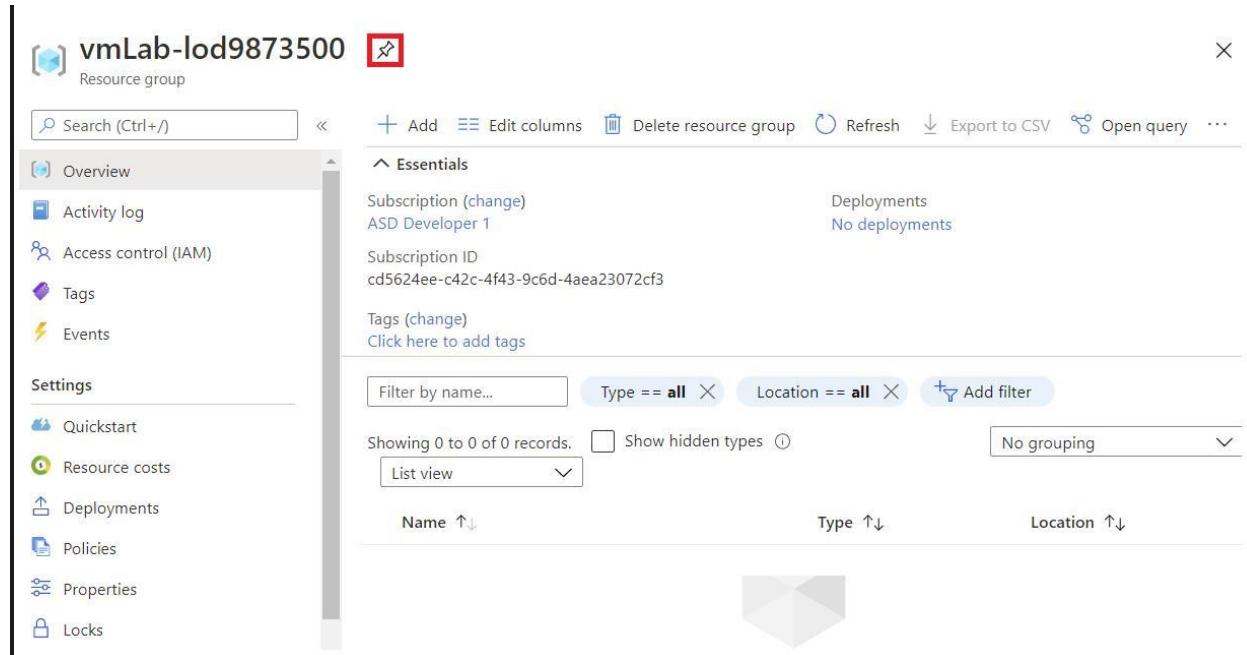
Task 1 - Create a Virtual Network

1. Our server infrastructure must be connected to a network in order to communicate. In this step, we will be deploying a virtual network to support this. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.

2. Click on the **Resource groups** menu item in the Azure portal and then select the **vmLab-lodXXXXXX** e.g. **vmLab-lod9873500** resource group. This will open up the resource group blade.

<input type="checkbox"/>	[Cloud icon] netwLabCentralUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	[Cloud icon] netwLabEastUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	[Cloud icon] storageLab-lod9873500	ASD Developer 1
<input checked="" type="checkbox"/>	[Cloud icon] vmLab-lod9873500	ASD Developer 1

3. For ease of finding your resource group again later, we will first pin the resource group to the Home page. Click the **Pin** tile at the top right-hand corner of the resource group. Now, the next time you click on the **Dashboard** menu item (left side of the portal window), you can find your resource group on a tile.



The screenshot shows the Azure Resource Group blade for the resource group 'vmLab-lod9873500'. The blade has a header with the resource group name and a red 'Pin' icon. Below the header is a search bar and a toolbar with 'Add', 'Edit columns', 'Delete resource group', 'Refresh', 'Export to CSV', 'Open query', and more. On the left is a sidebar with links to Overview, Activity log, Access control (IAM), Tags, Events, Settings, Quickstart, Resource costs, Deployments, Policies, Properties, and Locks. The main content area is titled 'Essentials' and displays subscription information (Subscription (change) to ASD Developer 1, Subscription ID cd5624ee-c42c-4f43-9c6d-4aea23072cf3), deployment status (No deployments), and tag information (Tags (change) with a link to add tags). There are filters for 'Type == all' and 'Location == all', and a 'List view' dropdown. At the bottom, there are columns for 'Name', 'Type', and 'Location'.

4. Click on the **Add** tile in the resource group blade.

The screenshot shows the Azure portal interface for a resource group named 'vmLab-lod9873500'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Events, Settings (Quickstart, Resource costs, Deployments, Policies, Properties, Locks), and a search bar. The main content area displays 'Essentials' information such as Subscription (change) to 'ASD Developer 1', Subscription ID 'cd5624ee-c42c-4f43-9c6d-4aea23072cf3', and Tags (change). A table lists 0 records with filters for Type (all) and Location (all). The table has columns for Name, Type, and Location.

5. Type in **Virtual Network** in the **Search the Marketplace** search box, then press Enter. This will list the Virtual Network resource, click **Create**.

The screenshot shows the 'Virtual Network' creation page. It features a large blue 'Create' button at the top right. Below it, there's a 'Save for later' link and a note about deploying with Resource Manager or Classic. The 'Overview' tab is selected. The main content area describes what a Virtual Network is and lists benefits like extending the datacenter, building distributed applications, and remote debugging. It also provides a link to 'Use Virtual Network to:'.

6. When setting up the virtual network, you will need to configure:

- Select your Azure subscription (Accept the default)
- Select the **vmLab-lodXXXXXXX** e.g. **vmLab-lod9873500** resource group if not already selected
- The name of the virtual network e.g. **vmssLabvNet**
- Select the Region to put the virtual network in
- The address space in CIDR notation (**Use 10.1.0.0/16**)

- The name of the subnet, for this lab exercise, name it **AppSubnet**
- Subnet address range (**Use 10.1.0.0/24**)
- BastionHost (leave disabled)
- DDoS Protection Standard (leave disabled)
- Firewall (leave disabled)
- Tags (leave empty)
- Click the **Next: Review + create** button
- Click the **Create** button

Create virtual network

Validation passed

Basics IP Addresses Security Tags **Review + create**

Basics

Subscription	ASD Developer 1
Resource group	vmLab-1od9873500
Name	vmsLabvNet
Region	South Central US

IP addresses

Address space	10.1.0.0/16
Subnet	AppSubnet (10.1.0.0/24)

Tags

None

Security

Create < Previous Next > Download a template for automation

7. Once the virtual network has been created, navigate back to the **vmLab-1odXXXXXX** e.g. **vmLab-1od9873500** resource group and click on the new virtual

network. This will open the virtual network blade. Click on the **Subnets** menu item and then click on the **+Subnet** tile.

The screenshot shows the 'vmssLabvNet | Subnets' blade in the Azure portal. The left sidebar has a 'Subnets' item highlighted with a red box. The top navigation bar includes a search bar, a '+ Subnet' button (also highlighted with a red box), a 'Gateway subnet' button, a 'Refresh' button, a 'Manage users' button, and a 'Delete' button. The main area displays a table with one row:

Name ↑	IPv4 ↑↓	IPv6 (many available) ↑↓	Delegated to ↑↓
AppSubnet	10.1.0.0/24 (251 available)	-	-

8. Enter the name **DBSubnet** for the new subnet name and accept the default subnet value. This is the subnet we will put the SQL Server machine on. Finally, select the **OK** button.

Add subnet

X

Name *

DBSubnet



Subnet address range * ⓘ

10.1.1.0/24

10.1.1.0 - 10.1.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None



Network security group

None



Route table

None



SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

OK

Cancel

9. Close all the blades and go all the way back to the Dashboard screen. From there, you can find the tile for your resource group and click on it. You should see your resource group blade appear with your virtual network in it.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 41 Min Remaining

Instructions Resources Help 100%

Task 2 - Create a Virtual Machine Scale Set for the IIS Frontend Servers

In this task, you will learn how to create a Virtual Machine Scale Set running **Windows Server 2019** using the Azure portal <https://portal.azure.com>. You will then configure the scale set instances with Internet Information Server, adding roles to use later on in this lab.

1. From within your **vmLab-1odXXXXXXX** e.g. **vmLab-1od9873500** resource group blade, click the **Add** tile.
2. In the **Search the Marketplace** search box, type in the search keywords **Virtual machine scale set** and press Enter. Click **Create** in the **Virtual machine scale set** pane.

Virtual machine scale set

Microsoft



Virtual machine scale set

Microsoft

Create

Save for later

Overview Plans Usage Information + Support

Azure virtual machine scale sets let you create and manage a group of identical, load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads. (Portal VMSS version 7.1.7)

- Easy to create and manage multiple VMs
- Provides high availability and application resiliency
- Allows your application to automatically scale as resource demand changes
- Works at large-scale

3. In the **Create virtual machine scale set** blade you will need to configure the following:

- Select your Azure subscription (Accept the default)
- Select the **vmLab-lodXXXXXXX** e.g. **vmLab-lod9873500** resource group if not already selected
- The name of the Virtual machine scale set e.g. **labVmss**
- Select the Region to put the Virtual machine scale set in
- Availability zone (leave as **none**)
- The operating system disk image (Click the **Image** drop down menu and select the **Windows Server 2019 Datacenter - Gen1** image.)

Instance details

Image * ⓘ

Windows Server 2019 Datacenter - Gen1

Browse all public and private images

- Azure Spot instance (leave as **No**)
- Instance size (here we specify the virtual machine size of each node, click the **Select size** link and click the **D2_v2** size, then click Select)

Select a VM size

Showing 221 VM sizes. Subscription: ASD Developer 1 Region: West Central US Current size: Standard_D2_v2 Image: Windows Server 2019 Datacenter Learn more about VM sizes							
VM Size ↑	Family ↑	vCPUs ↑	RAM (GiB) ↑	Data disks ↑	Max IOPS ↑	Temp storage (GiB) ↑	Premium disk ↑
Non-premium storage VM sizes Premium storage is recommended for most workloads							
D1_v2	General purpose	1	3.5	4	4x500	50	Not supported
D2_v2	General purpose	2	7	8	8x500	100	Not supported
D2_v3	General purpose	2	8	4	4x500	50	Not supported
D2_v4	General purpose	2	8	4	3200	0	Not supported
D2d_v4	General purpose	2	8	4	4x500	75	Not supported
D11_v2	Memory optimized	2	14	8	8x500	100	Not supported
D3_v2	General purpose	4	14	16	16x500	200	Not supported
D4_v3	General purpose	4	16	8	8x500	100	Not supported
D4_v4	General purpose	4	16	8	6400	0	Not supported
D4d_v4	General purpose	4	16	8	8x500	150	Not supported

Select Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. [View Azure pricing calculator](#).

- Username: **AdminUser**
- Password: **P@55word1234**
- Azure Hybrid Benefit (leave as **No**)
- OS disk type (leave as **Standard SSD**)

Basics **Disks** Networking Scaling Management Health Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * ⓘ

Standard SSD

Encryption type *

(Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility ⓘ

Yes No

Ultra Disk compatibility is not available for this VMSS size and location.

- Virtual network (select the Virtual network that you created in the earlier step of this lab from the Virtual network drop down menu)
- Click the **Pencil** icon to edit the Network interface configuration

+ Create new nic 



NAME

CREATE PUBLI...

SUBNET

NETWORK SECURI...

ACCELERATED N...



vmssLabvNet-nic01

No

AppSubnet (10.1.0.0/2...

Basic

Off



- Leave the Network interface name as the default
- Select the **AppSubnet** from the Subnet drop down menu if not already selected
- NIC network security group (leave as **Basic**)
- Public inbound ports (select **Allow selected ports**)
- Select **RDP** from the Select inbound ports drop down menu
- Public IP address (leave as **Disabled**)
- Accelerated networking (select **Enabled**)
- Click **OK**

Network interface

Name *

Virtual network

Subnet *

NIC network security group None Basic Advanced

Public inbound ports * None Allow selected ports

*Select inbound ports

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Public IP address Disabled Enabled

Accelerated networking Disabled Enabled

OK **Cancel**

- Click **Yes** to Use a load balancer
- Click the **Create new** link under the **Select a load balancer** drop down menu

- Type in a name for the Load balancer e.g. **labVmsslb**
- Type in a name for the Load balancers public IP address e.g. **labVmssLBpip**
- Type in a DNS name for the Load balancers public IP address, this must be a lower case, globally unique name. You can append your student number to the Load balancers name e.g. **labvmsslb9873500**
- Click **Create**

Create a load balancer

Azure Load Balancer enables you to scale your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications.

[Learn more about Azure Load Balancer.](#)

Your load balancer will be placed in the same subscription, resource group, and region as your virtual machine scale set. Azure will configure basic settings for the frontend IP, backend address pools, NAT rules, and NAT pools for this load balancer automatically. [Learn more](#)

Name *	labVmsslb	✓
Public IP address name *	labVmssLBpip	✓
Domain name label	labvmsslb9873500	✓

.westcentralus.cloudapp.azure.com

SKU	Public
Type	Standard
Availability zone	Zone-redundant

Create

Discard

- Click the **Review + create** button, followed by the **Create** button

Validation passed

Basics Disks Networking Scaling Management Health Advanced Tags **Review + create**

Basics

Subscription	ASD Developer 1
Resource group	vmLab-lod9873500
Virtual machine scale set name	labVmss
Region	West Central US
Availability zone	None
Image	Windows Server 2019 Datacenter - Gen1
Size	Standard D2 v2 (2 vcpus, 7 GiB memory)
Username	AdminUser
Azure Spot	No

Instance

Initial instance count	2
Would you like to use an existing Windows Server license?	No

Create < Previous Next > Download a template for automation

The Virtual machine scale set creation process will begin. This will take between 4 and 5 minutes, so proceed with the next task.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 41 Min Remaining

Instructions Resources Help 100%

Task 3 - Create a Virtual Machine with SQL Server

In this step, you will create a new virtual machine with SQL server using the Microsoft Azure Portal <https://portal.azure.com> which will be used to host your database.

1. For the SQL Server machine, we will be using a **SQL Server 2017 on Windows Server 2016** machine. Click on the **Add** button in your **vmLab-lodXXXXXX** e.g. **vmLab-lod9873500** resource group and then in the **Search the Marketplace** search box, type in the search words **SQL Server 2017 on Windows Server 2016** and press Enter. Select **SQL Server 2017 Enterprise Windows Server 2016** from the drop down menu and click **Create**.

SQL Server 2017 on Windows Server 2016

Microsoft



The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The top navigation bar includes the title "SQL Server 2017 on Windows Server 2016" and a "Save for later" button. Below the title, there's a "Select a plan" dropdown set to "SQL Server 2017 Web on Windows S...". A prominent red box highlights the "Create" button. To the right of the "Create" button are "Start with a pre-set configuration" and a "Filter" search bar. The main content area displays several SQL Server 2017 plan options, with "SQL Server 2017 Enterprise Windows Server 2016" highlighted by a red box. Below this, there are sections for "More offers from Microsoft" and a table comparing different server configurations.

Offer	Image	Region	OS	SKU	Version
{BYOL} SQL Server 2019 on Windows Server 2019		Microsoft	Windows Server 2019	Ubuntu1804	18.04
SQL Server 2019 BYOL Images on Windows Server 2019		Microsoft	SQL Server 2019 images on Windows Server 2019	SQL Server 2019 images on Ubuntu	16.04
SQL Server 2017 Enterprise Windows Server 2016		Microsoft	Windows Server 2016	Windows Server 2016	16.04
Free SQL Server License: SQL Server 2017 Developer on Windows Server 2016		Microsoft	Windows Server 2016	Windows Server 2016	16.04
Free SQL Server License: SQL Server 2017 Express on Windows Server 2016		Microsoft	Windows Server 2016	Windows Server 2016	16.04
SQL Server 2019 on Ubuntu1604		Microsoft	Ubuntu1604	Ubuntu1604	16.04

2. In the **Create a virtual machine** blade, do the following:
- o Leave the subscription and resource group settings as default
 - o Enter the virtual machine Name **dbvm**
 - o Select your region with No infrastructure redundancy required

Your image should be **SQL Server 2017 Enterprise Windows Server 2016 - Gen1**

Basics **Disks** **Networking** **Management** **Advanced** **SQL Server settings** **Tags** **Review + create**

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ ASD Developer 1 ▼

Resource group * ⓘ vmLab-lod9873500 ▼
[Create new](#)

Instance details

Virtual machine name * ⓘ dbvm ✓

Region * ⓘ (US) West Central US ▼

Availability options ⓘ No infrastructure redundancy required ▼

Image * ⓘ SQL Server 2017 Enterprise Windows Server 2016 - Gen1 ▼
[Browse all public and private images](#)

- If not selected by default, select VM size **Standard DS12 v2**
- Type in **AdminUser** as the Administrator Username and **P@55word1234** as the Password
- Click the **Allow selected ports** radio button and select **RDP (3389)** from the **Select inbound ports** drop down menu list and click the **Next : Disks >** button

Create a virtual machine

Basics Disks Networking Management Advanced SQL Server settings Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

ASD Developer 1

Resource group * ⓘ

vmLab-1od9873500

[Create new](#)

Instance details

Virtual machine name * ⓘ

dbvm

Region * ⓘ

(US) West Central US

Availability options ⓘ

No infrastructure redundancy required

Image * ⓘ

SQL Server 2017 Enterprise Windows Server 2016 - Gen1

[Browse all public and private images](#)

Azure Spot instance ⓘ

Yes No

Size * ⓘ

Standard_DS12_v2 - 4 vcpus, 28 GiB memory (US\$354.78/month)

[Select size](#)

Administrator account

Username * ⓘ

AdminUser

Password * ⓘ

.....

Confirm password * ⓘ

.....

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

None Allow selected ports

Select inbound ports *

RDP (3389)

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing Windows Server license? *

Yes No

[Review Azure hybrid benefit compliance](#)

[Review + create](#) [< Previous](#) [Next : Disks >](#)

- Accept the default Disks configuration and click the **Next : Networking >** button
- Ensure that your new **VNet** is selected, then select the **DBSubnet** from the Subnet drop down menu, then click the **Next : Management >** button

Create a virtual machine

Basics Disks **Networking** Management Advanced SQL Server settings Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	<input type="text" value="vmssLabvNet"/> <input type="button" value="Create new"/>
Subnet *	<input type="text" value="DBSubnet (10.1.1.0/24)"/> <input type="button" value="Manage subnet configuration"/>
Public IP	<input type="text" value="(new) dbvm-ip"/> <input type="button" value="Create new"/>
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	<input type="text" value="RDP (3389)"/>

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking On Off

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? Yes No

Review + create

< Previous

Next : Management >

- o Click the **Next : Advanced >** button
- o Click the **Next : SQL Server settings >** button

- On the SQL Server Settings tab, the only thing that needs to be changed is the toggle switch for **SQL Authentication**. Set this to **Enable** and leave all the other settings as default, then click the **Next : Tags >** button

You can see here that we are specifying for SQL connectivity, everything is within a virtual network and that we will need port 1433 inbound open on the virtual machine. Other settings are for automated patching, backups etc.

Regarding the port number setting, this setting tells the SQL Server instance that is installed on the virtual machine which port to listen on. You will still need to open a matching inbound firewall port to this port number.

Create a virtual machine

Basics Disks Networking Management Advanced **SQL Server settings** Tags Review + create

Security & Networking

SQL connectivity *

Port *

SQL Authentication

SQL Authentication

Login name *

Password *

Azure Key Vault integration

Storage configuration

Customize performance, size, and workload type to optimize storage for this virtual machine. For optimal performance, separate drives will be created for data and log storage by default. [Learn more about SQL Server best performance practices](#).

i The default storage configuration for SQL virtual machines has changed, now including OLTP optimization and separate drives for data and log storage.

Storage **Storage optimization: Transactional processing**
SQL Data: 1024 GiB, 5000 IOPS, 200 MB/s
SQL Log: 1024 GiB, 5000 IOPS, 200 MB/s
SQL TempDb: Use local SSD drive
[Change configuration](#)

SQL Server License
Save up to 43% with licenses you already own. Already have a SQL Server license? [Learn more](#)

SQL Server License No Yes

Automated patching
Set a patching window during which all Windows and SQL patches will be applied.

Automated patching **Enabled**
Sunday at 2:00
[Change configuration](#)

Automated backup
Automated backup [Disable](#) [Enable](#)

R Services(Advanced Analytics)
SQL Server Machine Learning Services (In-Database) [Disable](#) [Enable](#)

[Review + create](#) [< Previous](#) [Next : Tags >](#)

- o Click the **Next : Review + create >** button
- o Click the **Create** button

The machine creation process will begin. This will take between 8 and 9 minutes, so proceed with the next task.

Create a virtual machine

 Validation passed

Basics Disks Networking Management Advanced SQL Server settings Tags **Review + create**

 **You have set RDP port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	ASD Developer 1
Resource group	vmLab-lod9873500
Virtual machine name	dbvm
Region	West Central US
Availability options	No infrastructure redundancy required
Image	SQL Server 2017 Enterprise Windows Server 2016 - Gen1
Size	Standard DS12 v2 (4 vcpus, 28 GiB memory)
Username	AdminUser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Create

< Previous

Next >

Download a template for automation

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 40 Min Remaining

Instructions Resources Help 100%

Task 4 - Configuring the Virtual Machine Scale Set instances with IIS

Next, you will configure the Virtual machine scale set instances with IIS by adding the necessary roles to deploy the MVC application.

1.  From within your **vmLab-lodXXXXXXX** e.g. **vmLab-lod9873500** resource group blade, select the **Virtual machine scale set** that was created earlier.

Showing 1 to 14 of 14 records. Show hidden types ⓘ

No grouping List view

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/> dbvm_DataDisk_1	Disk	West Central US <input type="button" value="..."/>
<input type="checkbox"/> dbvm_OsDisk_1_93960e708c8d41e8a49567bc3de88b05	Disk	West Central US <input type="button" value="..."/>
<input type="checkbox"/> labVmss	Virtual machine scale set	West Central US <input type="button" value="..."/>

2. On the virtual machine scale set blade, select the **Instances** tile, this will list the instances in this virtual machine scale set. Click on the **first** instance in the list.

labVmss | Instances

Virtual machine scale set

Search (Ctrl+ /)

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Instances

Name	Computer name	Status	Health state	Provisioning state
labVmss_0	labvmsse700000	Running	Green	Succeeded
labVmss_2	labvmsse700002	Running	Green	Succeeded

3. Click the **Connect** button, then select RDP.

labVmss_0

Scale set instance

Search (Ctrl+ /)

Connect RDP SSH Bastion

Overview Settings Networking Connect Disks Properties Monitoring

Public IP address	-
Private IP address	10.1.0.4
Public IP address (IPv6)	-
Private IP address (IPv6)	-
Virtual network/subnet	vmsslabvNet/AppSubnet

4. Click the **IP address** dropdown menu and select the **Load balancer public IP address**, then click the **Download RDP File** button, this will save the remote desktop settings file to your local machine.

The screenshot shows the Azure portal interface for a virtual machine named 'labVmss_0'. The left sidebar has a 'Connect' section selected. The main area is titled 'Connect with RDP' with a note to enable just-in-time access. It shows the IP address and port number, both highlighted with a red border, and a 'Download RDP File' button which is also highlighted with a red border.

5. Once the file has downloaded, click **Open** and log on using the credentials you defined when creating the virtual machine scale set. You will also be prompted to accept the certificate. Select **Yes**.

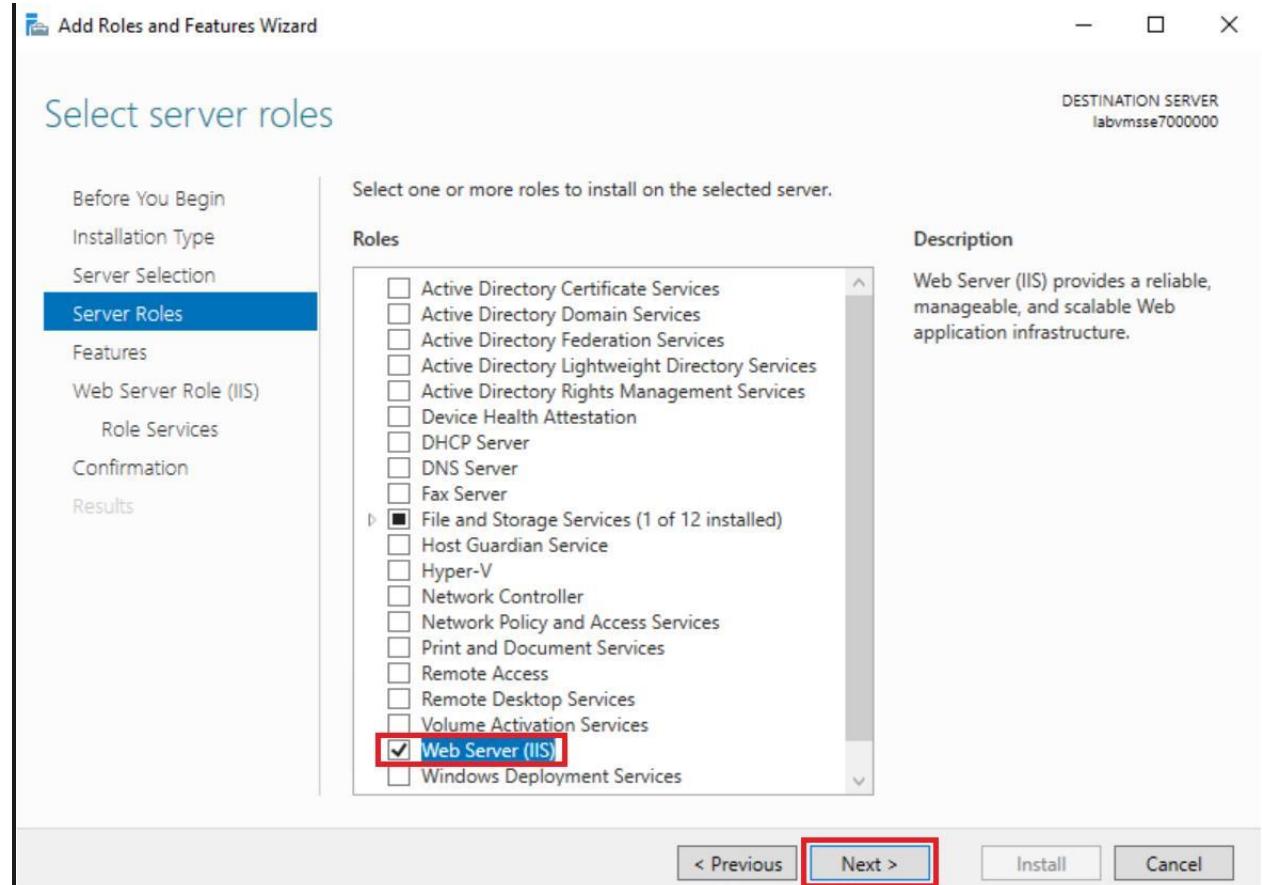
If you cannot RDP to the virtual machine, check with your Network Administrator to ensure that the necessary ports are open on your network to allow RDP.

6. Wait until the Server Manager appears and then select the **Add Roles and Features** link in the dashboard.

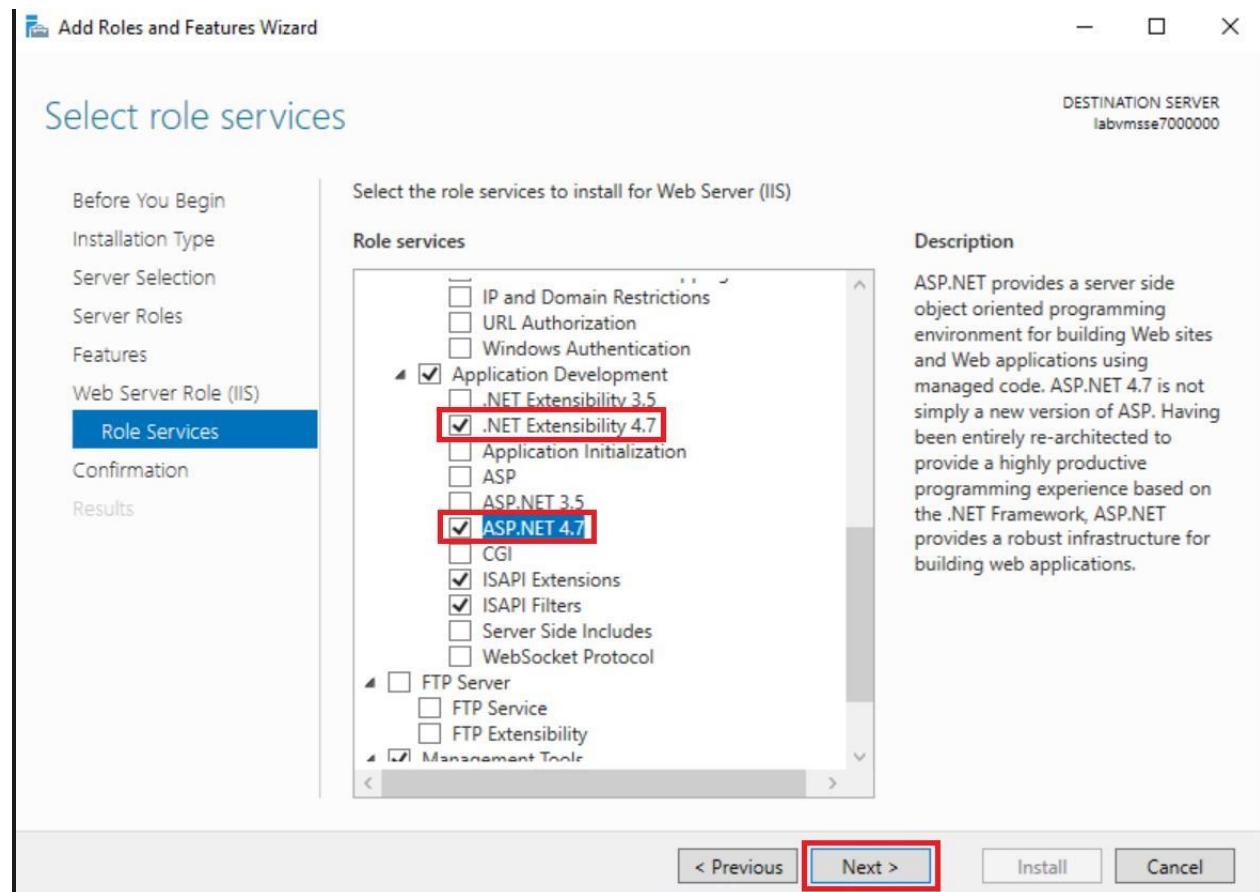
The screenshot shows the Windows Server Manager dashboard. The left navigation bar has 'Dashboard' selected. The main area is titled 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing 'WHAT'S NEW' and 'LEARN MORE'. To the right, a numbered list of steps is shown, with the second step, 'Add roles and features', highlighted with a red box.

- 1 Configure this local server
- 2 **Add roles and features**
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

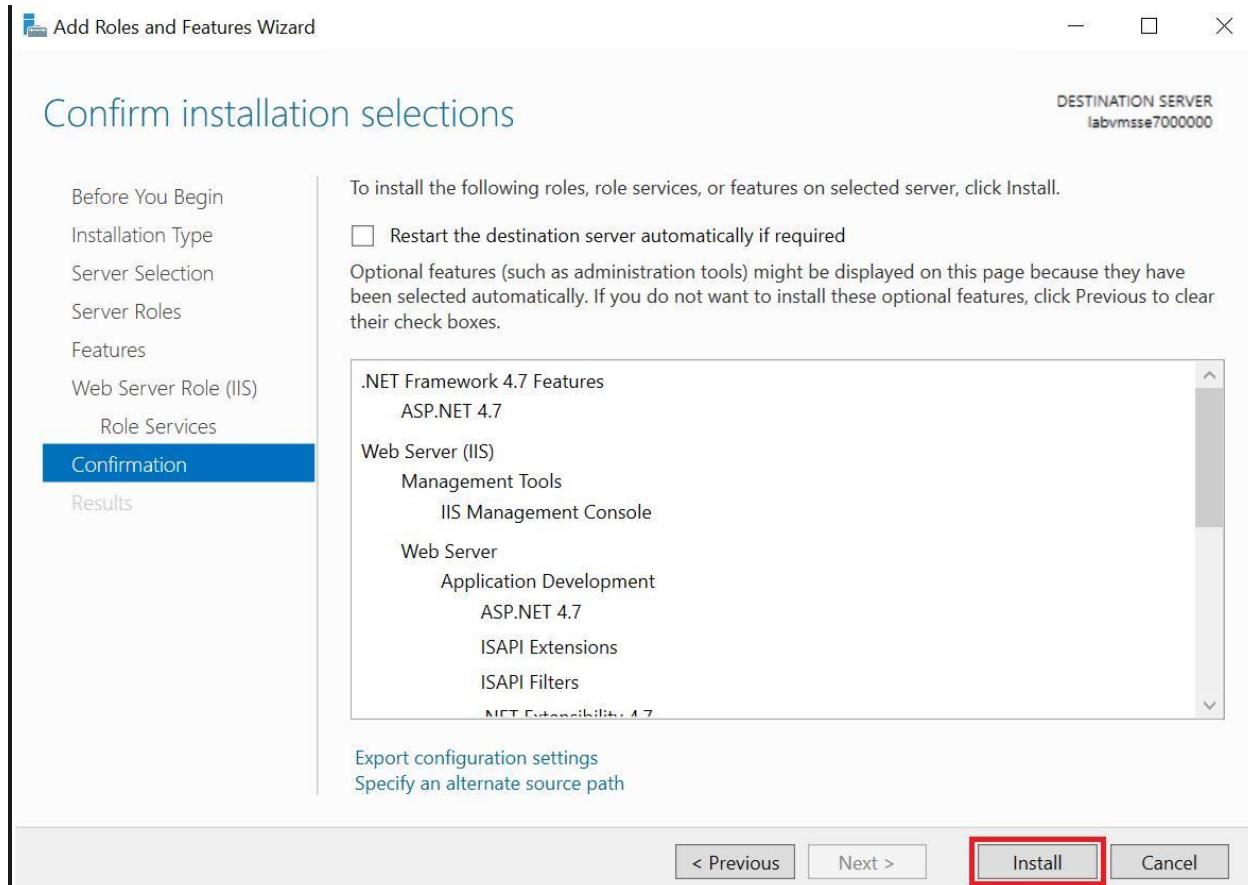
7. In the **Add Roles and Features Wizard** window, click the **Next** button until you reach the **Select server roles** page. In this window, select the **Web Server (IIS)** role and click the **Add Features** button in the **Add features that are required for Web Server (IIS)?** pop up, then click the **Next** button.



8. Click the **Next** button.
9. Click the **Next** button.
10. In the **Select role services** page, expand **Application Development**, tick the **.NET Extensibility 4.7** tick box, click the **Add Features** button in the **Add features that are required for .NET Extensibility 4.7?** pop up, then tick the **ASP.NET 4.7** tick box, click the **Add Features** button in the **Add features that are required for ASP.NET 4.7?** pop up and click the **Next** button.



11. Click the **Install** button.



12. Once the installation has completed, you can click the **Close** button.
13. Leave the remote desktop session open since you will need to copy the web application to this machine later.
14. Repeat steps 1 - 11 in this task on the **second** instance in the Virtual machine scale set.

Do not exit the virtual machine scale set RDP sessions as they will be used later on in the lab.

labVmss | Instances

Virtual machine scale set

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Instances

Search (Ctrl+ /)

Start Restart Stop Reimage Delete Upgrade Refresh Protection Policy

Name	Computer name	Status	Health state	Provisioning state
labVmss_0	labvmss700000	Running	Green	Succeeded
labVmss_2	labvmss700002	Running	Green	Succeeded

Task 5 - Setting Inbound Security rules for the Virtual Machine Scale Set instances

The Virtual machine scale set has been deployed with two instances behind a Load balancer but they (the instances) have not been configured to allow inbound **HTTP** traffic from the **Load balancer**. During this task, you will enable an inbound firewall rule at a **Network level** (not to be confused with the Windows Firewall which is at an **OS level**) that allows incoming traffic from the Load balancer destined for port 80 on either scale set instance. To configure this, we need to enable **port 80** inbound on the scale set instances network adaptor or subnet (network adaptor in our case). In Azure, this is configured using an **Inbound Security Rule** in a Network Security group.

1. From within your **vmLab-1odXXXXXX** e.g. **vmLab-1od9873500** resource group, select the **network security group** that was created during your Virtual machine scale set deployment.

Showing 1 to 14 of 14 records. <input type="checkbox"/> Show hidden types ⓘ			No grouping	List view
<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓		
<input type="checkbox"/> basicNsgvmssLabvNet-nic01	Network security group	West Central US	...	
<input type="checkbox"/> dbvm	Virtual machine	West Central US	...	
<input type="checkbox"/> dbvm	SQL virtual machine	West Central US	...	

2. Select **Inbound security rules**

Settings



Inbound security rules



Outbound security rules



Network interfaces



Subnets



Properties



Locks

3. In the **Inbound security rules** blade, select the **Add** button which will advance you to the **Add inbound security rule** blade. Set the field settings as shown below, and then click **Add**:

Setting	Value
Source	Any (since we do not know where the request will come from)
Source port ranges	Any

Setting	Value
Destination	Any
Destination port ranges	80 (since this is a web application)
Protocol	TCP
Action	Allow
Priority	100 (You could specify a priority if you wish, the lower the number, the higher the priority)
Name	A name of your choice, the lab uses webport



Add inbound security rule

X

basicNsgvmssLabvNet-nic01



Basic

Source * ⓘ

Any



Source port ranges * ⓘ

*

Destination * ⓘ

Any



Destination port ranges * ⓘ

80



Protocol *

Any

TCP

UDP

ICMP

Action *

Allow

Deny

4.

Priority * ⓘ

 ✓

Name *

 ✓

Description

Add

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 39 Min Remaining

Instructions Resources Help 100%

Task 6 - Configuring the SQL Server 2017 Instance

In this step, you will set up the SQL Server instance and database to be used by the web application.

When you create an IaaS SQL machine, Azure will automatically add a 1TB data disk to the machine for you, but it will not automatically configure it. You will use this data disk to store the SQL Server logs and data files.

1. To do this, go back to your resource group blade and select the **dbvm** virtual machine (Not the SQL virtual machine resource type).

Showing 1 to 14 of 14 records. Show hidden types ⓘ

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓	<input type="checkbox"/> No grouping	<input type="checkbox"/> List view
<input type="checkbox"/> basicNsgvmssLabvNet-nic01	Network security group	West Central US	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> dbvm	Virtual machine	West Central US	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> sql dbvm	SQL virtual machine	West Central US	<input type="checkbox"/>	<input type="checkbox"/>

2. From the SQL Server blade, click the **Connect** tile, **Public IP address** should be automatically selected, if it is not then select it, then click the **Download RDP**

- File** button. This will save the remote desktop settings file to your local machine. Click **Open** and log on using the credentials you defined when creating the virtual machine. You will also be prompted to accept the certificate. Select **Yes**.
3. Using Windows Explorer, go to your new F:\ drive and make sure you have a **Backup**, **Data** and **Log** directory. Create these directories if necessary.



All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 39 Min Remaining

Instructions Resources Help 100%

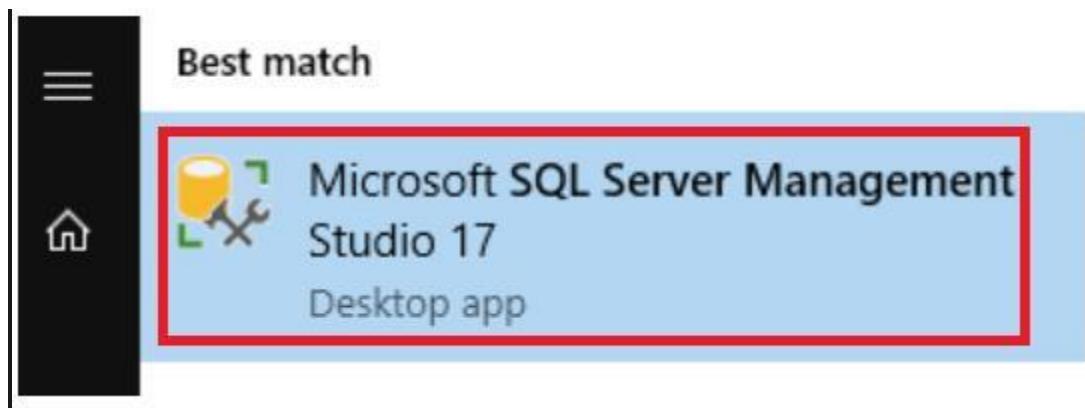
Task 7 - Installing the AdventureWorks Database

In this step, you will add the AdventureWorks database that will be used by the web application.

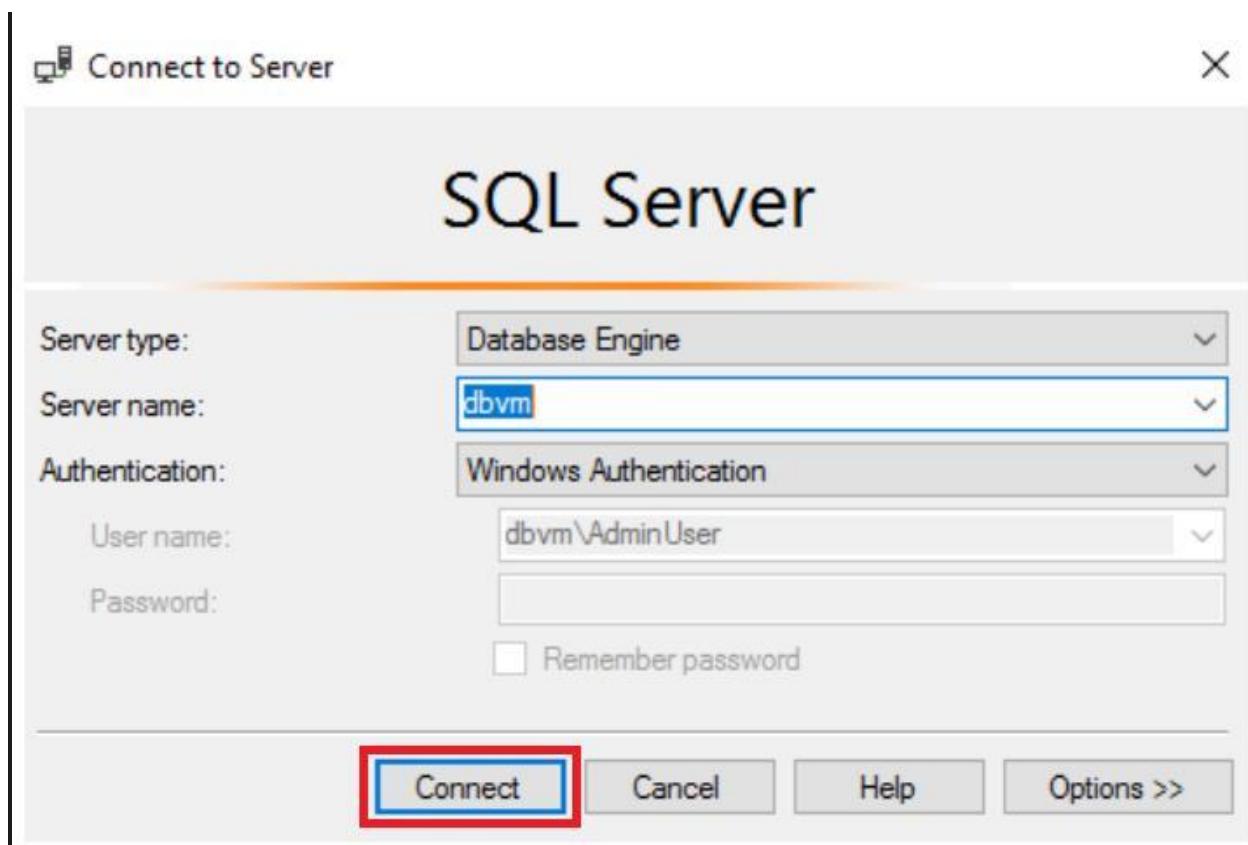
1. Browse to the **C:\AzureIaaS\WS\VM4 - Azure Virtual Machines\Labs\IntroToAzureVMs\Source\Assets** directory in the hosted lab machine.
2. Copy the entire **Database** directory over to the SQL Server IaaS virtual machine and drop it on the C:\ drive.

You can do this by selecting the Database directory on the source drive, select CTRL+C and then selecting CTRL+V onto the C:\ Drive of the database VM.

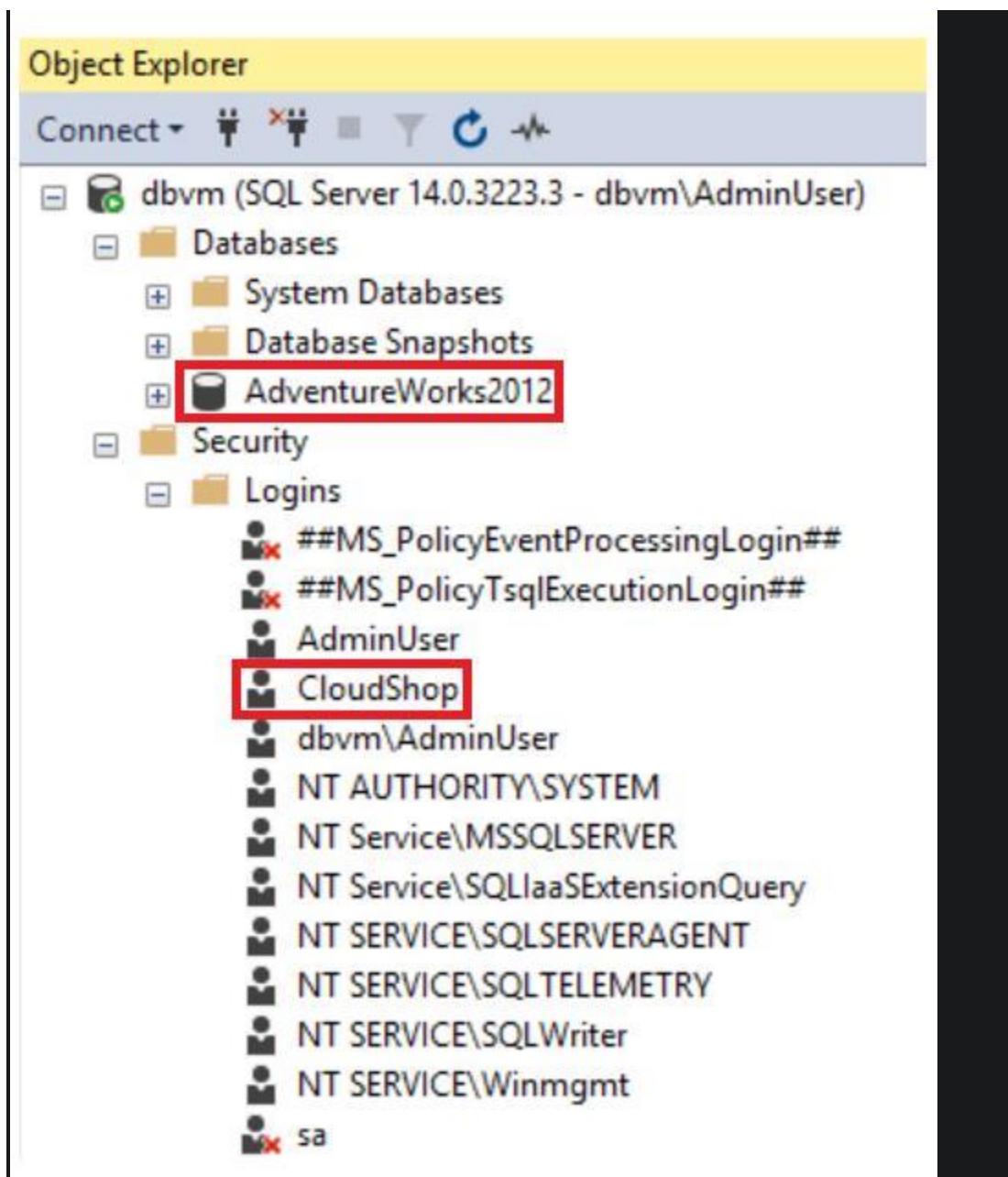
3. On the SQL IaaS machine, browse to **C:\Database**.
4. Right-click the **AdventureWorks2012_Database.zip** file and extract the contents to **F:\Data**.
5. Browse to the **C:\Database\Scripts** directory.
6. Right-click on the **InstallDB.cmd** file and select **Run as Administrator**. The DBSetup.ps1 PowerShell script will be executed and will:
 - a. Attach the AdventureWorks2012 database.
 - b. Set the database server instances to mixed mode.
 - c. Add a user login, CloudShop, and set user mappings.
7. Open **SQL Server Management Studio** by clicking the Start button, then typing **SQL Server Management Studio**. Click on the **Microsoft SQL Server Management Studio 17** app that is returned by the search.



8. Click the **Connect** button in the **Connect to Server** dialog box.



9. Expand the **Databases** node and verify that the **AdventureWorks2012** database has been attached, then expand the **Security** node, then **Logins** and verify that the **CloudShop** account has been created.



10. Close SQL Server Management Studio and minimize the RDP session.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 38 Min Remaining

Instructions Resources Help 100%

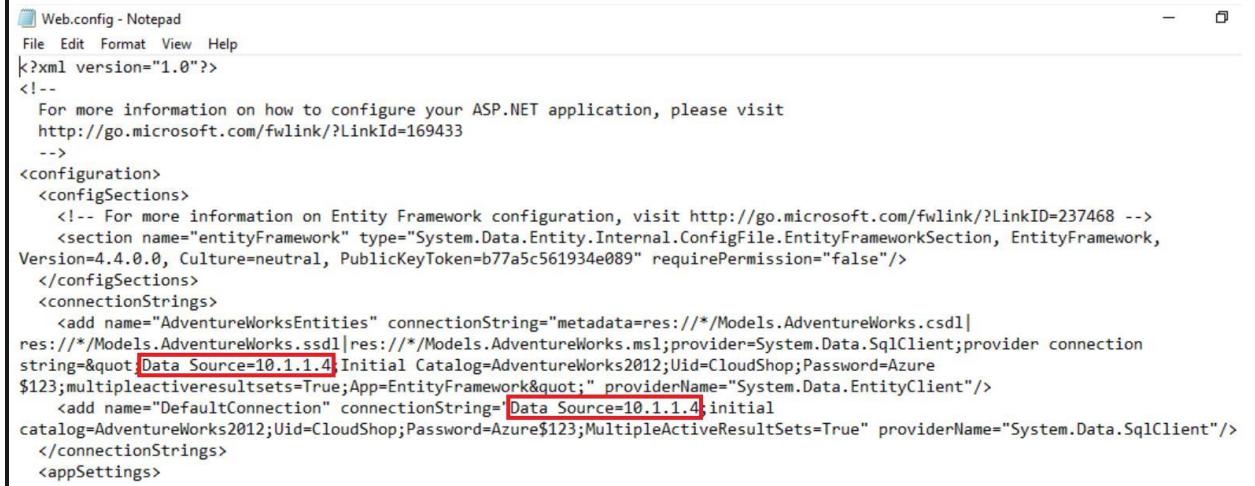
Task 8 - Deploying the MVC4 Application

1. Navigate to the C:\AzureIaaS\M4 - Azure Virtual Machines\Labs\IntroToAzureVMs-

V2\Source\Assets\CloudShop\VMSSInstance1 folder on the hosted lab machine and copy the **CloudShop.zip** file. Return to the RDP session of the first virtual machine scale set instance from earlier and paste the copied file in the **C:\inetpub\wwwroot** folder. To do this, copy **CloudShop.zip** (Ctrl + C) and paste it (Ctrl + V) in the virtual machine's wwwroot folder. Extract all files to the **C:\inetpub\wwwroot\CloudShop** folder.

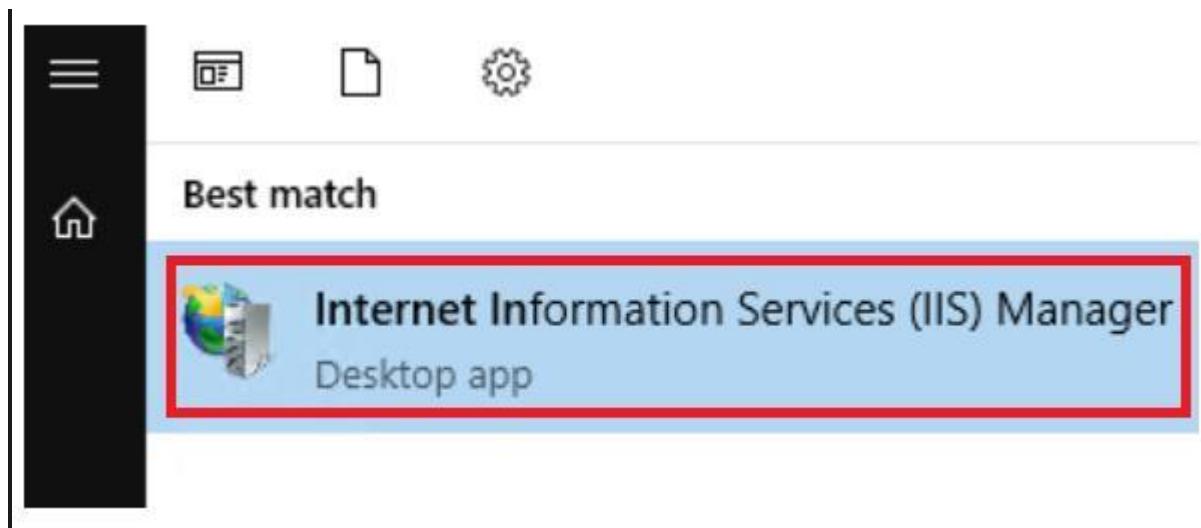
2. Using Notepad, open the **Web.config** file located in the **C:\inetpub\wwwroot\CloudShop** folder, select **Format** from the file menu, then select **Word Wrap**. Replace the "Data Source=[ENTER YOUR SQL MACHINE PRIVATE IP ADDRESS]" placeholder with the internal IP address of your SQL Server (by default, it is the virtual machine's IP address, which you can obtain by looking at the **Overview** section of the SQL server virtual machine in the Azure portal).

Do not include the brackets at the beginning and end of the data Source Setting.



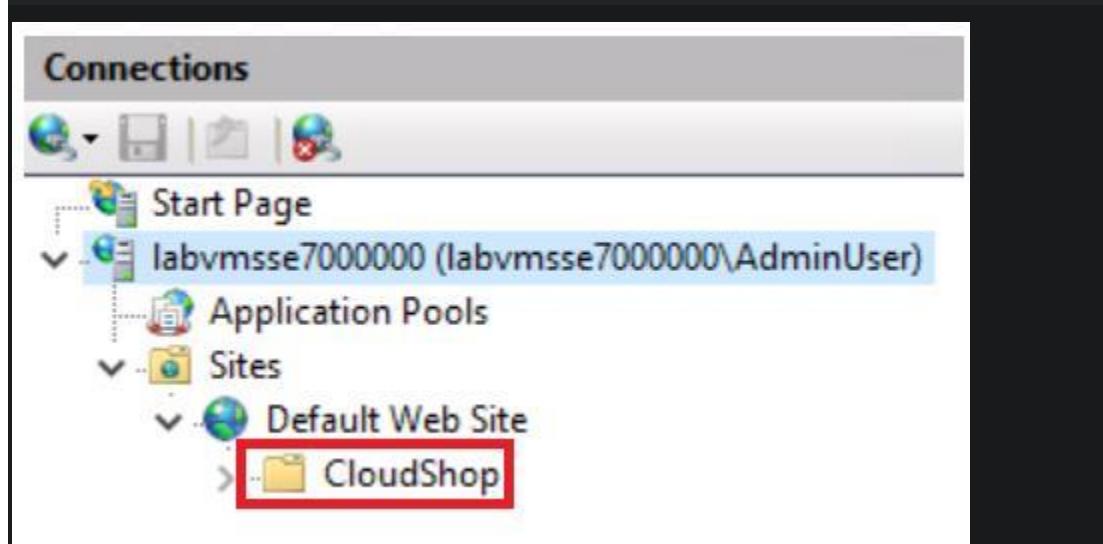
```
Web.config - Notepad
File Edit Format View Help
<?xml version="1.0"?>
<!--
  For more information on how to configure your ASP.NET application, please visit
  http://go.microsoft.com/fwlink/?LinkId=169433
-->
<configuration>
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework,
Version=4.4.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false"/>
  </configSections>
  <connectionStrings>
    <add name="AdventureWorksEntities" connectionString="metadata=res://*/Models.AdventureWorks.csdl|
res://*/Models.AdventureWorks.ssdl|res://*/Models.AdventureWorks.msl;provider=System.Data.SqlClient;provider connection
string="Data Source=10.1.1.4;Initial Catalog=AdventureWorks2012;Uid=CloudShop;Password=Azure
$123;multipleactiveresultsets=True;App=EntityFramework"" providerName="System.Data.EntityClient"/>
    <add name="DefaultConnection" connectionString="Data Source=10.1.1.4;initial
catalog=AdventureWorks2012;Uid=CloudShop;Password=Azure$123;MultipleActiveResultSets=True" providerName="System.Data.SqlClient"/>
  </connectionStrings>
  <appSettings>
```

3. Save the file.
4. Open the **Internet Information Services (IIS) Manager** by clicking on the Start button then typing **Internet Information Services**. Click on the **Internet Information Services (IIS) Manager** app that is returned by the search.

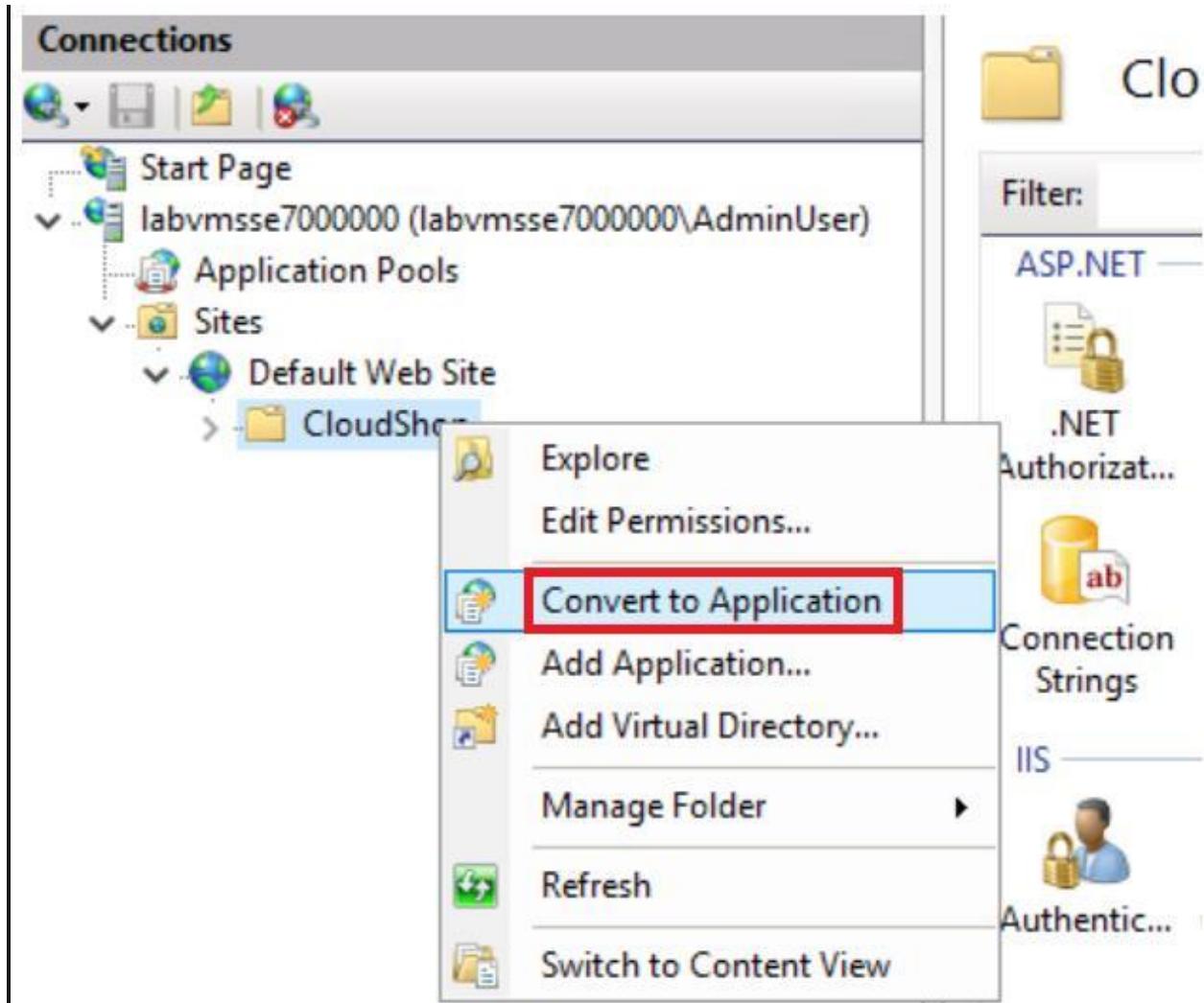


5. In the **Connections** pane, expand the Server node, then the Sites node, then the Default Web Site.

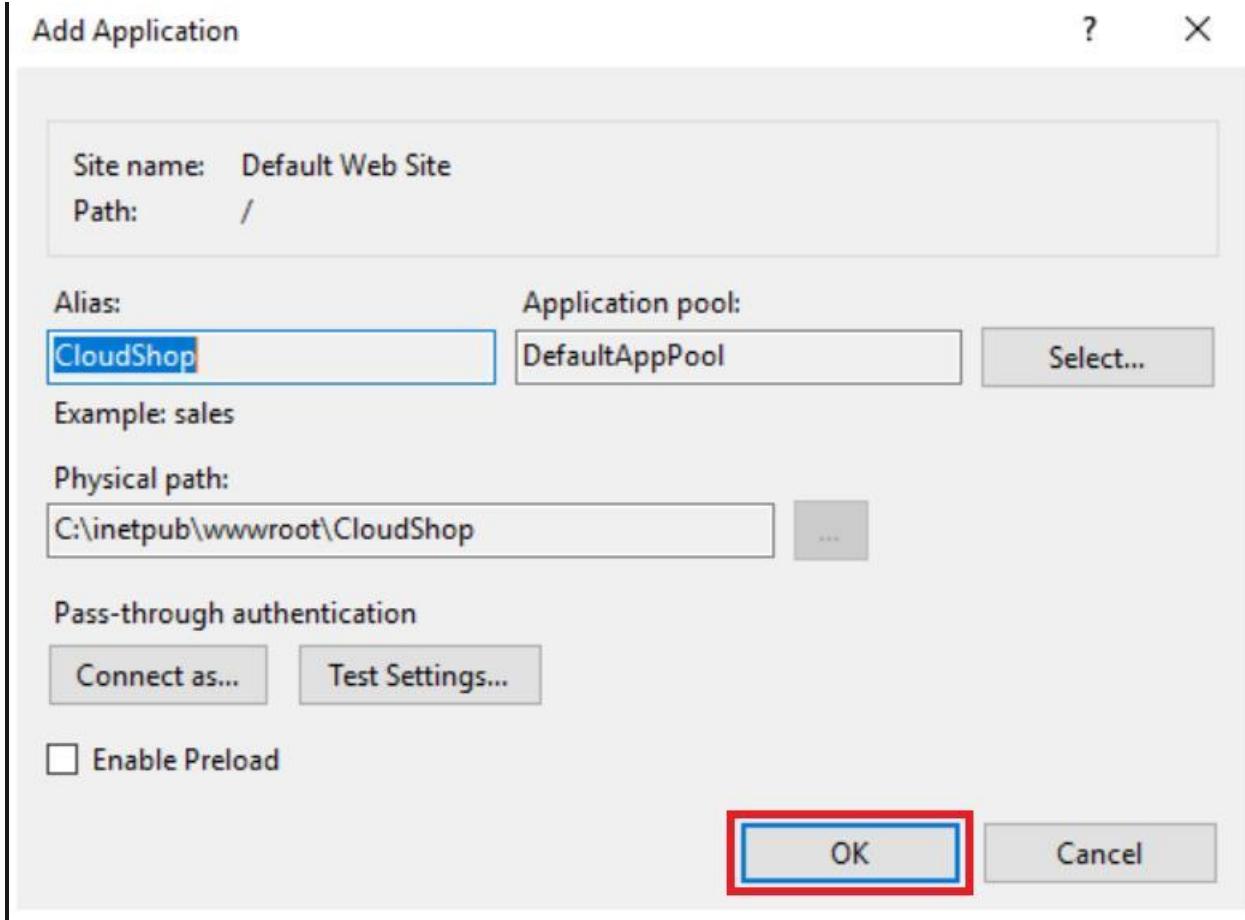
You will see the CloudShop folder you copied in the wwwroot folder.



6. Right-click the **CloudShop** folder and select **Convert to Application**.



7. In the **Add Application** dialog, click **OK**.



8. Close the Internet Information Server (IIS) Manager window.
9. Repeat steps 1 - 8 in this task for the second instance in the Virtual machine scale set, this time navigating to the **C:\AzureIaaS\M4 - Azure Virtual Machines\Labs\IntroToAzureVMs-V2\Source\Assets\CloudShop\VMSSInstance2** folder on the hosted lab machine and copying the **CloudShop.zip** file to the **C:\inetpub\wwwroot** folder on the second instance and so on.
10. Close the Remote Desktop Connection.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 38 Min Remaining

Instructions Resources Help 100%

Task 9 - Verification

In this task, you will test the Cloud Shop MVC4 application that you deployed using a Virtual machine scale set and an SQL server in the previous task.

- From within your **vmLab-lodXXXXXXX** e.g. **vmLab-lod9873500** resource group, select the **Public IP Address** resource that was created during your Virtual machine scale set deployment.

Showing 1 to 14 of 14 records. Show hidden types

No grouping List view

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/> labVmsslb	Load balancer	West Central US
<input checked="" type="checkbox"/> labVmssLBPip	Public IP address	West Central US
<input type="checkbox"/> vmlablod9873500diag	Storage account	West Central US

- Click on the **Copy to clipboard** button for the **DNS Name** value.

The screenshot shows the Azure portal interface for managing a Public IP Address named 'labVmssLBPip'. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, Settings, Configuration, and Properties. The main pane displays essential details such as Resource group (change) to 'vmLab-lod9873500', Location as West Central US, and SKU as Standard. The 'DNS name' field is explicitly highlighted with a red box, containing the value 'labvmsslb9873500.westcentralus.cloudapp.azure.com'. A 'Copy to clipboard' button is positioned next to this field, also highlighted with a red box.

- Open an Internet Explorer browser and paste in the clipboard value that you have just copied into the address bar and add **/cloudshop** path to the end of the URL e.g. **labvmsslb9873500.centralus.cloudapp.azure.com/cloudshop**, then press enter. This will render the Cloud Shop MVC4 application using one of the Virtual machine scale set instances.

The screenshot captures an Internet Explorer browser displaying a web page titled 'Cloud Shop on VMSS Node 1'. The address bar shows the URL 'http://labvmsslb9873500.centralus.cloudapp.azure.com/cloudshop'. The page header includes 'Home', 'Products', and 'Checkout' links. Below the header, a search bar is followed by a list of products: 'Adjustable Race', 'All-Purpose Bike Stand', 'AWC Logo Cap', 'BB Ball Bearing', and 'Bearing Ball'. The entire screenshot is framed by a thick black border.

4. From within Internet Explorer, open a new tab and paste in the URL from the previous step followed by the **/cloudshop** path, this session will generate a new source port, resulting in a new **5-tuple hash** value for the Load balancer and finally redirecting your request to another Load balanced endpoint.

The screenshot shows a Microsoft Internet Explorer window with the following details:

- Address Bar:** http://labvmsslb9873500.centralus.cloudapp.azure.com/cloudshop
- Title Bar:** Cloud Shop Products - Cloud S... (repeated twice)
- Menu Bar:** File Edit View Favourites Tools Help
- Page Content:**
 - Header:** Cloud Shop on VMSS Node 2
 - Navigation:** Home Products Checkout
 - Text:** Select a product from the list:
 - Search Bar:** A search input field with the placeholder "Search" and a "Search" button.
 - Product List:** A scrollable list of products:
 - Adjustable Race
 - All-Purpose Bike Stand
 - AWC Logo Cap
 - BB Ball Bearing
 - Bearing Ball

5. In the Search box, type **Classic** and click **Search**. It will show all the products that have a product name that match the search criteria.

If you experience the "500 - Internal server error" when you try to access the CloudShop web application, check if you have completed Task 4, step 10 of this lab.

Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 38 Min Remaining

Instructions Resources Help 100%

Module 5 - VNet-to-VNet Connectivity with BGP

Introduction

In this lab, you will create two Azure virtual networks and connect them together. You will then enable BGP on both networks and confirm that it has been successfully implemented.

You'll learn:

- How to create Azure virtual networks
- How to define Azure virtual gateways
- How to connect virtual networks using Azure Connections
- How to confirm connectivity between two virtual networks
- How to enable BGP and confirm its implementation
- How to enable virtual network Service Endpoints
- How to enable the storage account firewall

Prerequisites

The following are required to complete this hands-on lab:

- Microsoft Azure PowerShell v5.1.1 or later
- Microsoft Azure PowerShell Az module v2.5.0 or later
 - A Microsoft Azure subscription

Although this lab demonstrates setting up a VNet-to-VNet connection from within the Azure Portal, you can also achieve this through PowerShell. See <https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-vnet-vnet-rm-ps/> for more information on using PowerShell.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 16 Min Remaining

Instructions Resources Help 100%

Exercise 1 - VNet-to-VNet Connectivity

Task 1 - Create the first virtual Network and Virtual Network gateway

In this task, we will choose to create our virtual networks in two different regions, East US and Central US. You can choose whatever regions you wish to use, just remember to change your settings in the appropriate places while stepping through the exercise.

1. Connect to **Win10 Lab VM** as **Student** using **pass@word1** as the password.
2. Log in to the Azure portal at **https://portal.azure.com** using your Azure Trial Pass credentials.
3. Select the **Resource Groups** menu item (which will open the Resource Groups blade) and then select the **netwLabEastUS-1odXXXXXXX** e.g. **netwLabEastUS-1od9873500** resource group.

Showing 1 to 11 of 11 records.		Subscription ↑↓
	Name ↑↓	
<input type="checkbox"/>	armVSLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	automationLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	backupLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	identityLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	managementLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	netwLabCentralUS-lod9873500	ASD Developer 1
<input checked="" type="checkbox"/>	netwLabEastUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	storageLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	vmLab-lod9873500	ASD Developer 1

4. From within the resource group, click the **Add** button, then type in **Virtual Network** in the **Search the Marketplace** search box, then press Enter. This will list the Virtual Network resource, click **Create**.

Virtual Network ↗
Microsoft

Virtual Network ↗ Save for later
Microsoft **Create**

Deploy with Resource Manager (change to Classic)

[Overview](#) [Plans](#) [Usage Information + Support](#)

Create a logically isolated section in Microsoft Azure with this networking service. You can securely connect it to your on-premises datacenter or a single client machine using an IPsec connection. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX.

Use Virtual Network to:

- Extend your datacenter
- Build distributed applications
- Remotely debug your applications

5. When setting up the virtual network, you will need to configure:

- Select your Azure subscription (Accept the default)
- Select the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group if not already selected
- The name of the virtual network e.g. **vnetEast**
- Select the Region to put the virtual network in, this should be **East US**
- The address space in CIDR notation (**Use 10.2.0.0/16**)
- The name of the subnet, for this lab exercise, name it **AppSubnet**
- Subnet address range (**Use 10.2.0.0/24**)

- BastionHost (leave disabled)
- DDoS Protection Standard (leave disabled)
- Firewall (leave disabled)
- Tags (leave empty)
- Click the **Next: Review + create** button
- Click the **Create** button

Create virtual network

✓ Validation passed

Basics IP Addresses Security Tags **Review + create**

Basics

Subscription ASD Developer 1
Resource group netwLabEastUS-1od9873500
Name vnetEast
Region East US

IP addresses

Address space 10.2.0.0/16
Subnet AppSubnet (10.2.0.0/24)

Tags

Create

< Previous

Next >

Download a template for automation

6. Go back to the **netwLabEastUS-1odXXXXXX** e.g. **netwLabEastUS-1od9873500** resource group and click on the **vnetEast** virtual network. This will bring up the vnetEast blade.
7. In the **vnetEast** blade, click on the **Subnets** tile. Then click the **+ Gateway subnet** button in the Subnets blade to add a new gateway subnet.

vnetEast | Subnets

Virtual network

Search (Ctrl+ /)

+ Subnet + Gateway subnet Refresh Manage users Delete

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

Address space Connected devices Subnets (highlighted with a red box)

DDoS protection Firewall Security

Subnets

Name ↑↓	IPv4 ↑↓	IPv6 (many available) ↑↓	Delegated to ↑↓
AppSubnet	10.2.0.0/24 (251 available)	-	-

8. Accept the default address range and click OK. Once the gateway subnet has been created, go back to the **netwLabEastUS-1odXXXXXX** e.g. **netwLabEastUS-1od9873500** resource group blade.

Add subnet

X

Name

GatewaySubnet

Subnet address range * ⓘ

10.2.1.0/24

10.2.1.0 - 10.2.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None



Network security group

None



Route table

None



SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

OK Cancel

9. In order for our virtual network to connect to another network via an IPsec VPN, it needs to have a virtual network gateway or router implemented.

Click the **Add** button in your resource group blade and then type **Virtual network gateway** in the **Search the Marketplace** search box, then press Enter. This will list the Virtual Network Gateway resource, click **Create**.

Virtual network gateway ✎

Microsoft

 Virtual network gateway Microsoft Save for later

Create

Overview Plans Usage Information + Support

A virtual network gateway is the software VPN device for your Azure virtual network. Use this with a connection to set up a site-to-site VPN connection between an Azure virtual network and your local network, or a VNet-to-VNet VPN connection between two Azure virtual networks. It can also be used to connect a virtual network to an ExpressRoute circuit.

Microsoft Azure provides a 99.9% uptime SLA for virtual network gateways.

10. When setting up the virtual network gateway, you will need to configure:
- Select your Azure subscription (Accept the default)
 - The name of your virtual network gateway e.g. **vnetEastGw**
 - Select the Region to put the virtual network gateway in, this should be **East US**
 - Gateway type, select **VPN**
 - VPN type, select **Route-based**
 - SKU, select **VpnGw1**

- Generation, select **Generation1**
- Virtual network, select the virtual network that you recently created in this resource group e.g. **vnetEast** (this specifies which virtual network your gateway will be attached to)
- Public IP address, select **Create new**
- The name of your gateways Public IP address, e.g. **vnetEastGw-Pip**
- Enable active-active mode, select **Disabled** (this configures both gateways in an active-active configuration as opposed to an active-standby configuration)
- Configure BGP ASN, select **Disabled** (this will be configured later on using another method)

11.  Click the **Review + create** button.

Create virtual network gateway

[Basics](#) [Tags](#) [Review + create](#)

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#).

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

ASD Developer 1

Resource group 

netwLabEastUS-1od9873500 (derived from virtual network's resource group)

Instance details

Name *

vnetEastGw

Region *

East US

Gateway type * 

VPN ExpressRoute

VPN type * Route-based Policy-based

SKU * VpnGw1

Generation Generation1

Virtual network * vnetEast Create virtual network

Subnet GatewaySubnet (10.2.1.0/24)

Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address * Create new Use existing

Public IP address name * vnetEastGw-Pip

Public IP address SKU Basic

Assignment Dynamic Static

Enable active-active mode * Enabled Disabled

Configure BGP * Enabled Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

Review + create Previous [Next : Tags >](#) Download a template for automation

12.  Click the **Create** button.

Create virtual network gateway

Validation passed

Basics Tags Review + create

Basics

Subscription	ASD Developer 1
Resource group	netwLabEastUS-lod9873500
Name	vnetEastGw
Region	East US
SKU	VpnGw1
Generation	Generation1
Virtual network	vnetEast
Subnet	GatewaySubnet (10.2.1.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled

Create

Previous

Next

Download a template for automation

Please note that it can take up to 40 minutes for the gateway creation process to complete, you are however able to move forward with the lab whilst waiting for it to complete.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

5 Hr 15 Min Remaining

Instructions Resources Help 100%

Task 2 - Create the second Virtual Network and Virtual Network gateway

1. Go back to the **Resource Groups** blade and select the **netwLabCentralUS-
lodXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource group. You are going to
go through the same steps of creating a virtual network with a virtual network gateway
that you carried out in the previous task, except that this will be for
the **netwLabCentralUS-
lodXXXXXX** e.g. **netwLabCentralUS-lod9873500** resource
group with all resources located in the **Central US** region.

All resources	Showing 1 to 11 of 11 records.	Subscription
<input type="checkbox"/> Resource groups		ASD Developer 1
<input type="checkbox"/> App Services		ASD Developer 1
<input type="checkbox"/> Function App		ASD Developer 1
<input type="checkbox"/> SQL databases		ASD Developer 1
<input type="checkbox"/> Azure Cosmos DB		ASD Developer 1
<input type="checkbox"/> Virtual machines		ASD Developer 1
<input type="checkbox"/> Load balancers		ASD Developer 1
<input type="checkbox"/> Storage accounts		ASD Developer 1
<input type="checkbox"/> Virtual networks		ASD Developer 1
<input type="checkbox"/> Azure Active Directory		ASD Developer 1
<input checked="" type="checkbox"/> netwLabCentralUS-lod9873500		
<input type="checkbox"/> netwLabEastUS-lod9873500		
<input type="checkbox"/> storageLab-lod9873500		
<input type="checkbox"/> vmLab-lod9873500		

2. From within the **netwLabCentralUS-
lodXXXXXX** e.g. **netwLabCentralUS-
lod9873500** resource group, click the **Add** button and add a new virtual network
named **vnetCentral**. Pay close attention to the IP addresses that are being used
i.e. **10.3.0.0/16** for the address space and **10.3.0.0/24** for the AppSubnet. Click
the **Create** button.

Create virtual network

Validation passed

Basics IP Addresses Security Tags **Review + create**

Basics

Subscription	ASD Developer 1
Resource group	netwLabCentralUS-1od9873500
Name	vnetCentral
Region	Central US

IP addresses

Address space	10.3.0.0/16
Subnet	AppSubnet (10.3.0.0/24)

Tags

Create

< Previous

Next >

Download a template for automation

- Once the virtual network has been created, create a new gateway subnet.

Add subnet

X

Name

GatewaySubnet

Subnet address range * ⓘ

10.3.1.0/24

10.3.1.0 - 10.3.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None



Network security group

None



Route table

None



SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

OK Cancel

4. Create a virtual network gateway named **vnetCentralGw** and associate it with your **vnetCentral** virtual network. You also need to have a different public IP address name than **vnetEastGw** and make sure you choose the Route-based VPN type. Click the **Review + create** button.

Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#).

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group ⓘ

Instance details

Name * ✓

Region *

Gateway type * ⓘ VPN ExpressRoute

VPN type * Route-based Policy-based

SKU *

Generation

Virtual network *
[Create virtual network](#)

Subnet

Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address * Create new Use existing

Public IP address name *

Public IP address SKU Basic

Assignment Dynamic Static

Enable active-active mode * Enabled Disabled

Configure BGP * Enabled Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

Review + create Previous Download a template for automation

5. On successful validation, click the **Create** button. Remember that it can take up to 40 minutes to deploy the gateway.

Create virtual network gateway

 Validation passed

Basics Tags **Review + create**

Basics

Subscription	ASD Developer 1
Resource group	netwLabCentralUS-lod9873500
Name	vnetCentralGw
Region	Central US
SKU	VpnGw1
Generation	Generation1
Virtual network	vnetCentral
Subnet	GatewaySubnet (10.3.1.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled

Create

Previous

Next

Download a template for automation

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 55 Min Remaining

Instructions Resources Help 100%

Task 3 - Confirm Virtual Network Gateway creation

You will know that your virtual network gateways have been successfully created, when Azure provides a new public IP address to the gateway. Check both gateways.

1. Navigate to the **netwLabEastUS-lodXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group and click on your **virtual network gateway**.

2. You will notice your new public IP address in the virtual network gateway blade.

The screenshot shows the 'Essentials' section of a Virtual Network Gateway blade. It includes fields for Resource group, Location, Subscription, Subscription ID, SKU, Gateway type, VPN type, Virtual network, and Public IP address. The Public IP address field is highlighted with a red border and contains the value '52.152.139.75 (vnetEastGw-Pip)'.

Resource group (change)	SKU
netwLabEastUS-1od9873500	VpnGw1
Location	Gateway type
East US	VPN
Subscription (change)	VPN type
ASD Developer 1	Route-based
Subscription ID	Virtual network
cd5624ee-c42c-4f43-9c6d-4aea23072cf3	vnetEast
Public IP address	
52.152.139.75 (vnetEastGw-Pip)	

3. Repeat the process for the **netwLabCentralUS-1odXXXXXX** e.g. **netwLabCentralUS-1od9873500** resource group and confirm that the virtual network gateway has been assigned a public IP address.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 55 Min Remaining

Instructions Resources Help 100%

Task 4 - Create the virtual network connections

Now that you have the virtual network gateways created, you need to create a Connection to enable connectivity between the gateways.

1. From within the **netwLabEastUS-1odXXXXXX** e.g. **netwLabEastUS-1od9873500** resource group blade, select **Add**, then type in **Connection** in the **Search the Marketplace** search box, then press Enter. This will list the Connection resource, click **Create**.
2. On the **Basics** blade, select the **VNet-to-VNet** Connection type, the default Azure subscription, the existing resource group **netwLabEastUS-1odXXXXXX** e.g. **netwLabEastUS-1od9873500** if it has not been selected by default, also select the same location as the resource group, in this case **East US**. Click the **OK** button.

Basics

Connection type * ⓘ

VNet-to-VNet



Subscription *

ASD Developer 1



Resource group * ⓘ

netwLabEastUS-1od9873500



[Create new](#)

Location *

East US



OK

3. On the **Settings** blade, review the properties below.

- Since we are already in the **netwLabEastUS-1odXXXXXX** e.g. **netwLabEastUS-1od9873500** resource group, we will choose the first virtual network gateway as **vnetEastGw**
- Our second gateway created in an earlier task is **vnetCentralGw**
- Select **Establish bidirectional connectivity** (to create connections in both directions, not selecting this will result in a single connection being created with traffic flow in one direction only)
- Type in connection names for the first and second connections or accept the default names
- Enter a Shared key e.g. **abc123** (this is used for the gateways to authenticate to each other, in a production environment, a more complex key should be used)
- Leave **Enable BGP** unselected, we will enable BGP at a later stage
- Click the **OK** button

Settings

*First virtual network gateway ⓘ >

vnetEastGw

*Second virtual network gateway ⓘ >

vnetCentralGw

Establish bidirectional connectivity ⓘ

First connection name *

vnetEastGw-to-vnetCentralGw



Second connection name *

vnetCentralGw-to-vnetEastGw



Shared key (PSK) * ⓘ

abc123



IKE Protocol ⓘ

IKEv1 IKEv2

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

OK

4. Click the **OK** button on the summary page.

Summary

Basics

Connection type	VNet-to-VNet
Subscription	ASD Developer 1
Resource Group	netwLabEastUS-1od9873500
Location	East US

Settings

First virtual network gateway	vnetEastGw
Second virtual network gateway	vnetCentralGw
Establish bidirectional connectivity	Yes
First connection name	vnetEastGw-to-vnetCentralGw
Second connection name	vnetCentralGw-to-vnetEastGw
Shared key (PSK)	abc123
Enable BGP	No
IKE Protocol	

OK

Because you selected the **Establish bidirectional connectivity** option in the Settings blade (above), you do not need to create a connection from the **vnetCentral** virtual network gateway to the **vnetEast** virtual network gateway, since this will be included during the creation of this connection.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 55 Min Remaining

Instructions Resources Help 100%

Task 5 - Confirm the connection between the virtual networks

There are a few ways in which to verify the connectivity status between virtual networks. One of the fastest ways is to use PowerShell to do this.

1. Open PowerShell as an Administrator.
2. In the PowerShell command prompt, type in **Connect-AzAccount** and press Enter, then login using your Azure Trial Pass credentials.
3. To confirm the **vnetEastGw** connection to **vnetCentralGw** and vice versa, type in the following and press Enter (if you are prompted to confirm the action, select Yes to All):

```
Windows_PowerShell
Get-AzVirtualNetworkGatewayConnection -name vnetEastGw-to-vnetCentralGw -ResourceGroupName netwLabEastUS-1od18918877 | fl Name, ConnectionStatus, IngressBytesTransferred, EgressBytesTransferred
```

```
PS C:\> Get-AzVirtualNetworkGatewayConnection -name vnetEastGw-to-vnetCentralGw -ResourceGroupName netwLabEastUS-1od9873500

Name          : vnetEastGw-to-vnetCentralGw
ConnectionStatus : Connected
IngressBytesTransferred : 0
EgressBytesTransferred : 0
```

You should be able to see the **ConnectionStatus** with a status of **Connected**. The number of ingress and egress bytes transferred will be zero since there is no traffic flowing between the two gateways yet. If the status shows as "Unknown", "Connecting" or "Not connected" wait a few minutes and try again.

4. Run the same PowerShell command but this time for the vnetCentralGw-to-vnetEastGw connection in the same resource group.
5. Leave your PowerShell session open.

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 54 Min Remaining

Instructions Resources Help 100%

Exercise 2 - Enable BGP on virtual network gateways and connections

BGP is a routing protocol that enables routers to exchange routing table information between them. This is useful because it reduces the administrative overhead for a network administrator. Without BGP, the network administrator would have to manually configure routing paths.

During the previous steps of this lab, you configured a VNet-to-VNet VPN connection whereby the routing paths were configured between the two gateways during the creation of your VPN connections. These routing paths were derived from each of the VNets address spaces (this is the reason why a local network gateway is not required for a VNet-to-VNet connection). The routing paths were not configured by means of the gateways exchanging their routing tables.

During this exercise, we will be enabling both gateways and their respective connections to use BGP.

Task 1 - Check the BGP status on the existing virtual network gateway

1. From the previously opened PowerShell session, run the following script to confirm that BGP is not enabled on the gateways:

```
Windows_PowerShell
Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEastGw -ResourceGroupName netwLabEastUS-1od18918877

PS C:\> Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEastGw -ResourceGroupName netwLabEastUS-1od9873500
PS C:\>
```

2. Repeat the above step for the vnetCentralGw gateway in the **netwLabCentralUS-1odXXXXXXX** e.g. **netwLabCentralUS-1od9873500** resource group.
3. Leave your PowerShell session open.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 54 Min Remaining

Instructions Resources Help 100%

Task 2: - Enable BGP on the virtual network gateway and connections

1. Browse to <https://resources.azure.com/> and login using your Azure Trial Pass credentials.
2. In the top right-hand corner, click the Read/Write toggle button if it has not been selected by default.



3. In the left-hand pane, expand **subscriptions|YourSubscriptionName|resourceGroups|netwLabEastUS-lodXXXXXXX|providers|Microsoft.Network|virtualNetworkGateways** and click the **vnetEastGw** then click **Edit** in the right-hand pane.

The screenshot shows the Azure Resource Explorer (Preview) interface. On the left, the navigation tree is expanded to show resources under 'netwLabEastUS-lod9873500', specifically focusing on the 'Microsoft.Network/virtualNetworkGateways' node, which contains the 'vnetEastGw' resource. On the right, the details for 'vnetEastGw' are displayed. The 'Actions' tab is selected, showing 'Data (GET, PUT)' and 'Actions (POST, DELETE)'. Below these are 'GET' and 'Edit' buttons, with the 'Edit' button highlighted by a red box. The URL 'https://management.azure.com...' is shown next to it. The JSON representation of the resource is partially visible on the right:

```
1: {
2:   "name": "vnetEastGw",
3:   "id": "/subscriptions/cd5624ee-c421-4100-8f3e-10d9873500/providers/Microsoft.Network/virtualNetworkGateways/vnetEastGw",
4:   "etag": "W/"c21f1b14-b9e1-4d2c-b811-4a2c7253-7e28-4",
5:   "type": "Microsoft.Network/virtualNetworkGateways",
6:   "location": "eastus",
7:   "tags": {},
8:   "properties": {
9:     "provisioningState": "Succeeded",
10:    "resourceGuid": "b42c7253-7e28-4",
11:    "ipConfigurations": [
12:      {
13:        "name": "default",
14:        "ipAddress": "192.168.1.100",
15:        "subnet": {
16:          "id": "/subscriptions/cd5624ee-c421-4100-8f3e-10d9873500/resourceGroups/netwLabEastUS-lod9873500/providers/Microsoft.Network/virtualNetworks/vnetEastGw/subnets/default"
17:        }
18:      }
19:    ],
20:    "connectionEstablished": true,
21:    "connectionEstablishedTime": "2018-09-10T10:45:00Z",
22:    "connectionEstablishedBy": "Virtual Machine"
23:  }
24:}
```

4. In the right-hand pane, scroll down to the "**enableBgp**" tag and configure it to **true** and configure its "**asn**" tag value to **65010**.

```

44 },
45 "gatewayType": "Vpn",
46 "vpnType": "RouteBased",
47 "enableBgp": true,
48 "activeActive": false,
49 "bgpSettings": {
50   "asn": 65010,
51   "bgpPeeringAddress": "10.2.1.254",
52   "peerWeight": 0
53 },
54 "gatewayDefaultSite": {
55   "id": "(String)"

```

5. Scroll to the top and click the **Put** button.



6. Repeat this process for the **vnetCentralGw** gateway and using an **asn** tag value of **65020**. This will enable both gateways for BGP. The next step is to enable BGP on the gateway connections.
7. Navigate to **subscriptions|YourSubscriptionName|resourceGroups|netwLabEastUS-1odXXXXXXX|providers|Microsoft.Network|connections** and click the **vnetCentralGw-to-vnetEastGw** connection, then click **Edit** in the right-hand pane.

8. In the right-hand pane, scroll down to the "enableBgp" tag (under "connectionType": "Vnet2Vnet") and configure it to **true** and click the **Put** button.

```
},  
  "connectionType": "Vnet2Vnet",  
  "connectionProtocol": "IKEv2",  
  "routingWeight": 0,  
  "sharedKey": "abc123",  
  "enableBgp": true,  
  "usePolicyBasedTrafficSelectors": false,  
  "ipsecPolicies": [
```

9. Repeat this process for the **vnetEastGw-to-vnetCentralGw** gateway connection.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 54 Min Remaining

Instructions Resources Help 100%

Task 3 - Confirm that BGP has been enabled

1. From the previously opened PowerShell session, run the following script to confirm that BGP has been enabled:

```
Windows_PowerShell  
Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEastGw -ResourceGroupName netwLabEastUS-1od18918877  
  
PS C:\> Get-AzVirtualNetworkGatewayBGPPeerStatus -VirtualNetworkGatewayName vnetEastGw -ResourceGroupName netwLabEastUS-1od9873500  
  
LocalAddress      : 10.2.1.254  
Neighbor         : 10.3.1.254  
Asn              : 65020  
State             : Connected  
ConnectedDuration : 00:00:17.4870197  
RoutesReceived    : 1  
MessagesSent      : 3  
MessagesReceived  : 5
```

2. Confirm that there is a successful connection with your BGP peer (which is the other VNet gateway in this case) and that at least 1 route has been received or learnt.

3. Repeat this process for the **vnetCentralGw** gateway.
4. The exchange of routing information between the two gateways has now generated network traffic. You can confirm this by running the PowerShell command that you ran earlier.

```
Windows_PowerShell  
Get-AzVirtualNetworkGatewayConnection -name vnetEastGw-to-vnetCentralGw -  
ResourceGroupName netwLabEastUS-1od18918877 | fl Name,  
ConnectionStatus, IngressBytesTransferred, EgressBytesTransferred
```

```
PS C:\> Get-AzVirtualNetworkGatewayConnection -name vnetEastGw-to-vnetCentralGw -ResourceGroupName netwLabEastUS-1od9873500  
  
Name : vnetEastGw-to-vnetCentralGw  
ConnectionStatus : Connected  
IngressBytesTransferred : 2058  
EgressBytesTransferred : 1080
```

5. Repeat this process for the **vnetCentralGw-to-vnetEastGw** gateway connection.

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 54 Min Remaining

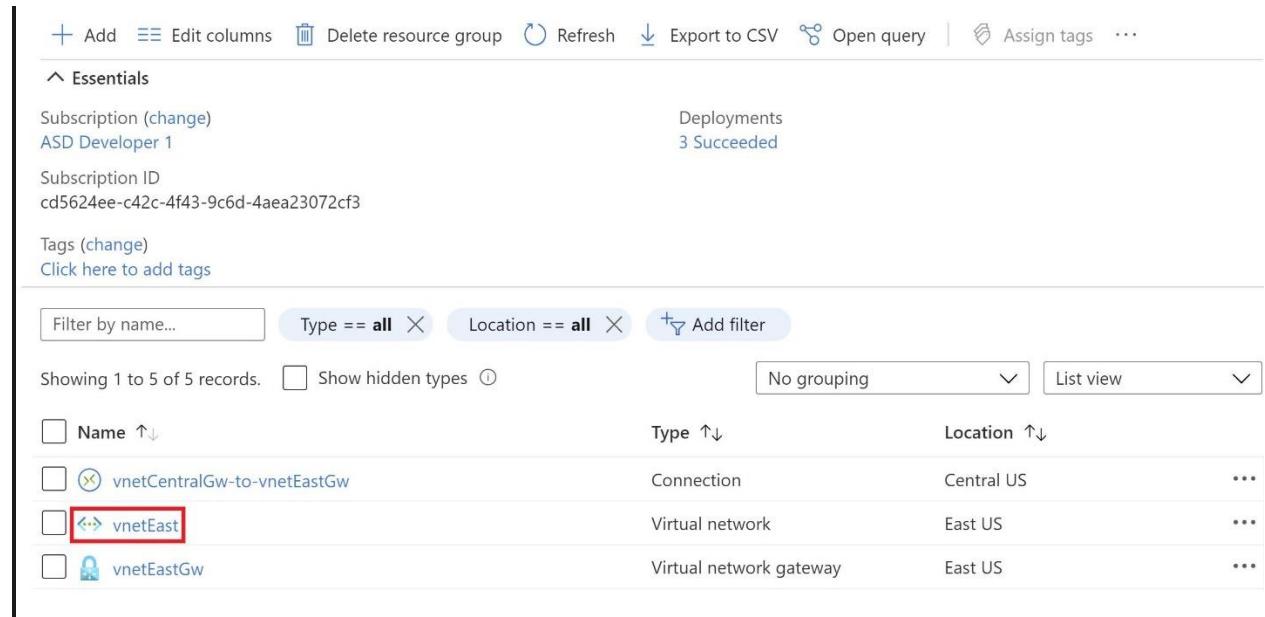
Instructions Resources Help 100%

Exercise 3 - Configure Virtual Network Service Endpoints and Storage Account Firewall

Now that we've deployed our virtual network, it's a good idea to secure communication to and from it when accessing Azure public facing services. One example of this is Azure Storage. When we access an Azure Storage account from a virtual network, we do this over the Internet albeit inside a Microsoft Azure datacenter. This does raise security concerns in most organizations. Using Virtual Network Service Endpoints, we create a connection between a virtual network and an Azure Storage account over the Microsoft Azure backbone network so traffic between a virtual network and a storage account does not go over the Internet giving you a more secure connection.

Task 1 - Configure Virtual Network Service Endpoints

- From within the Azure portal, navigate to the **netwLabEastUS-
IodXXXXXX** e.g. **netwLabEastUS-Iod9873500** resource group and click on the
vnetEast virtual network.



The screenshot shows the Azure portal interface for managing service endpoints. At the top, there are navigation links: Add, Edit columns, Delete resource group, Refresh, Export to CSV, Open query, Assign tags, and more. Below this is a section titled 'Essentials' with information about the subscription (ASD Developer 1) and deployments (3 Succeeded). The main area displays a list of service endpoints:

Name	Type	Location	Actions
vnetCentralGw-to-vnetEastGw	Connection	Central US	...
vnetEast (highlighted with a red box)	Virtual network	East US	...
vnetEastGw	Virtual network gateway	East US	...

Below the table, there are filters for Name, Type, and Location, along with buttons for Show hidden types, No grouping, List view, and grouping dropdowns.

- In the left-hand pane, click **Service endpoints**.

 **vnetEast** 

Virtual network

Search (Ctrl+ /)

 Overview

 Activity log

 Access control (IAM)

 Tags

 Diagnose and solve problems

Settings

 Address space

 Connected devices

 Subnets

 DDoS protection

 Firewall

 Security

 DNS servers

 Peerings

 Service endpoints

 Private endpoints

3. In the right-hand pane, click **Add**, then select Microsoft.Storage from the Service drop down menu, then **AppSubnet** from the Subnets drop down menu and click **Add**. This process can take up to 15 minutes.

4. Confirm that the Azure Storage Service endpoints have been added while you are still in the Service endpoints pane. You have now configured all inbound and outbound traffic from your virtual network to your Azure storage account to go over the Microsoft Azure backbone network.

Service	Subnet	Status	Locations
Microsoft.Storage	AppSubnet	Succeeded	East US, West US

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 54 Min Remaining

Instructions Resources Help 100%

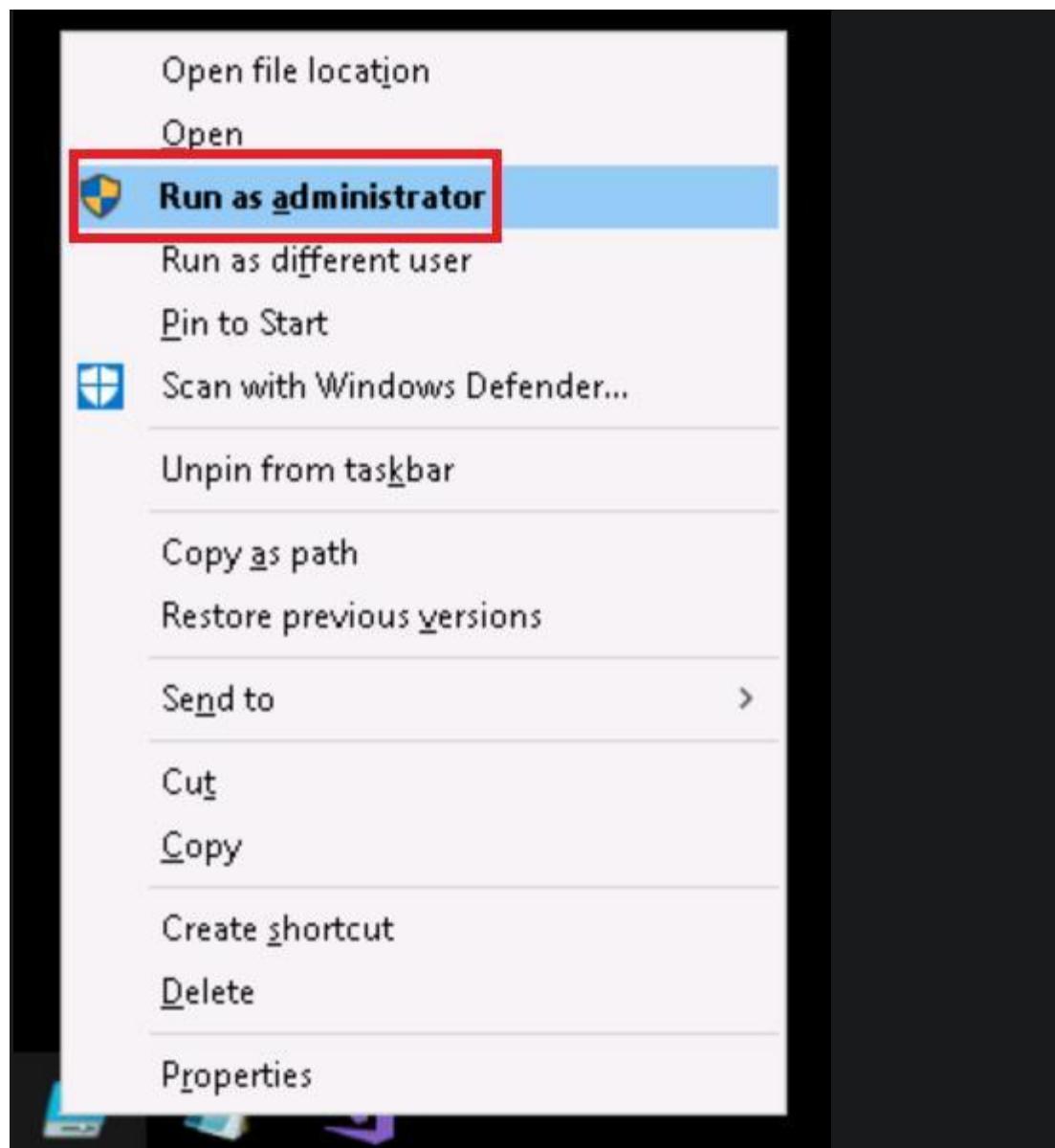
Task 2 - Configure Storage Account Firewall

Prior to configuring a storage account firewall, we need to create a storage account.

1. Login to the [**Win10 Lab VM**](#) hosted lab machine in the left hand pane with a Username of **Student** and a Password of **pass@word1** Once logged in, if you do not already have a US keyboard layout select your keyboard layout from the task bar.



2. Shift and right-click the PowerShell shortcut on the taskbar and select **Run as administrator**



3. Click **Yes** to the User Account Control pop-up.

4. In the PowerShell command prompt window, type in **Connect-AzAccount** and press **Enter**.
5. Enter the email address that was used to redeem your **Azure Trial Pass** into the Sign in dialog box and click **Next** or press **Enter**.
6. Enter your password and click **Sign in** or press **Enter**. This will log you in to your Azure Trial Pass subscription.

```
PS C:\> Connect-AzAccount
```

Account	SubscriptionName	TenantId	Environment
iaaswslab@hotmail.com	Azure Pass - Sponsorship	f30ae15e-afec-42d9-aefc-3709be909663	AzureCloud

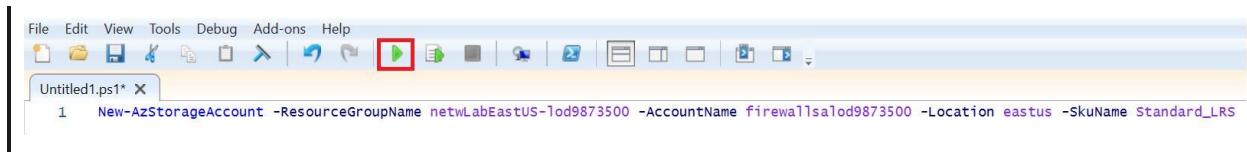
7. Copy the below PowerShell commands to your PowerShell script pane.

Click the **Type Text** icon to automatically type the associated text to the active window in your hosted lab machine on the left.

Windows_PowerShell

```
New-AzStorageAccount -ResourceGroupName netwLabEastUS-lod18918877 -  
AccountName firewallsalod18918877 -Location eastus -SkuName Standard_LRS
```

8. Click the **Run** button or press **F5**. This will create the storage account that will be used in this lab.



9. The storage account has been successfully created.

StorageAccountName	ResourceGroupName	PrimaryLocation	SkuName	Kind	AccessTier	CreationTime	ProvisioningState	EnableHttpsTrafficOnly	LargeFileShares
firewallsalod9873500	netwLabEastUS-lod9873500	eastus	Standard_LRS	StorageV2	Hot	30-04-2020 19:54:46	Succeeded	True	

10. From within the Azure portal, navigate to the **netwLabEastUS-lodXXXXXXX** e.g. **netwLabEastUS-lod9873500** resource group and click on the **firewallsalodXXXXXXX** e.g. **firewallsalod9873500** storage account.

[+](#) Add [Edit columns](#) [Delete resource group](#) [Refresh](#) [Export to CSV](#) [Open query](#) | [Assign tags](#) ...

[^ Essentials](#)

Subscription (change)
ASD Developer 1

Deployments
4 Succeeded

Subscription ID
cd5624ee-c42c-4f43-9c6d-4aea23072cf3

Tags (change)
Click here to add tags

Filter by name... Type == all Location == all [+ Add filter](#)

Showing 1 to 6 of 6 records. Show hidden types ⓘ

No grouping [List view](#)

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓	...
<input type="checkbox"/> firewallsalod9873500	Storage account	East US	...
<input type="checkbox"/> vnetCentralGw-to-vnetEastGw	Connection	Central US	...
<input type="checkbox"/> vnetEast	Virtual network	East US	...

11. In the left-hand pane, click **Firewalls and virtual networks**.



firewallsalod9873

Storage account

Search (Ctrl+ /)



Tags



Diagnose and solve problems



Access Control (IAM)



Data transfer



Events



Storage Explorer (preview)

Settings



Access keys



Geo-replication



CORS



Configuration



Encryption



Shared access signature



Firewalls and virtual networks

12. In the right-hand pane, click the **Selected networks** radio button, then click **+ Add existing virtual network** this will automatically select your subscription, then select **vnetEast** from the Virtual networks drop down menu, and finally select **AppSubnet** from the Subnets drop down menu. Click **Add** and then click **Save**.

Subscription * ASD Developer 1

Virtual networks * vnetEast

Subnets * AppSubnet

AppSubnet is selected.

13. While you are still in the Firewalls and virtual networks pane, click the expand arrow under Virtual Network and confirm that the Azure Storage Account Firewall has been configured to allow network traffic from the **AppSubnet** in the **vnetEast** virtual network.

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
vnetEast	1			netwLabEastUS-lod9...	ASD Developer 1
	AppSubnet	10.2.0.0/24	✓ Enabled	netwLabEastUS-lod9...	ASD Developer 1

You have now successfully configured your Azure Storage Account to accept inbound and outbound network traffic from your specified virtual network only. This means that this storage account will no longer be accessible from the Internet unless additional rules are configured to allow this.

Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 53 Min Remaining

Instructions Resources Help 100%

Module 6 - Introduction to Azure Role Based Access Control (RBAC)

Introduction

In this lab, you will deploy a simple Web Application that is hosted on an Azure App Service instance. This will provide you with an environment that will allow you to test RBAC for users in an Azure Active Directory (AAD) tenant. **Note** that there is a difference between **Azure RBAC** and **Azure AD RBAC** in that Azure RBAC relates to Azure roles such as **Virtual Machine Contributor** whilst Azure AD RBAC relates to Azure AD roles such as **Global Administrator**. You will be configuring **Azure RBAC** during this lab.

You'll learn:

- How to deploy a pre-configured MVC web application to an Azure Resource Group using a Visual Studio template deployment
- How to configure RBAC for users in your Azure AD tenant

Prerequisites

The following are required to complete this hands-on lab:

- Microsoft Visual Studio 2015 Professional with Update 3 or later
- Microsoft Azure SDK for .NET (VS 2015) v2.9.5 or later
- A Microsoft Azure subscription

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 53 Min Remaining

Instructions Resources Help 100%

Exercise 1 - Deploy a Web Application using Visual Studio

During this exercise you will be building, deploying and testing a simple Web Application that is hosted on an Azure App service instance.

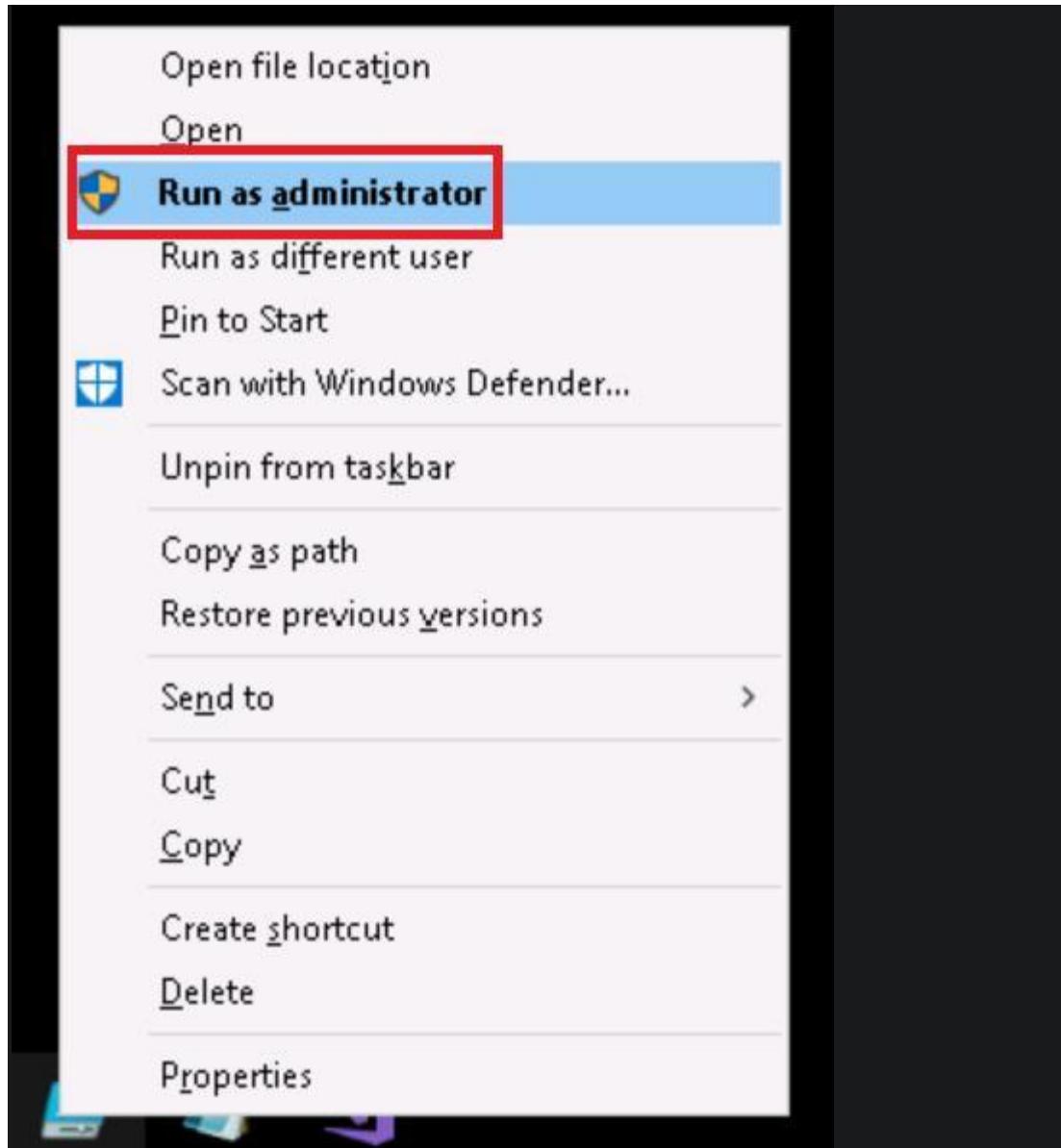
Task 1 - Create a storage account and build the Visual Studio solution

For this exercise you will use a pre-configured Visual Studio project that contains an Azure Resource Group deployment and a Web Application. (This is the source code for the ARM lab that was carried out earlier). A storage account will also be created to store the Web Application package.

1. Login to the **Win10 Lab VM** hosted lab machine in the left hand pane with a Username of **Student** and a Password of **pass@word1**. Once logged in, if you do not already have a US keyboard layout select your keyboard layout from the task bar.



2. Shift and right-click the PowerShell shortcut on the taskbar and select **Run as administrator**



3. Click **Yes** to the User Account Control pop-up.
4. In the PowerShell command prompt window, type in **Connect-AzAccount** and press **Enter**.
5. Enter the email address that was used to redeem your **Azure Trial Pass** into the Sign in dialog box and click **Next** or press **Enter**.
6. Enter your password and click **Sign in** or press **Enter**. This will log you in to your Azure Trial Pass subscription.

```
PS C:\> Connect-AzAccount
```

Account	SubscriptionName	TenantId	Environment
iaaswslab@hotmail.com	Azure Pass - Sponsorship	f30ae15e-afec-42d9-aefc-3709be909663	AzureCloud

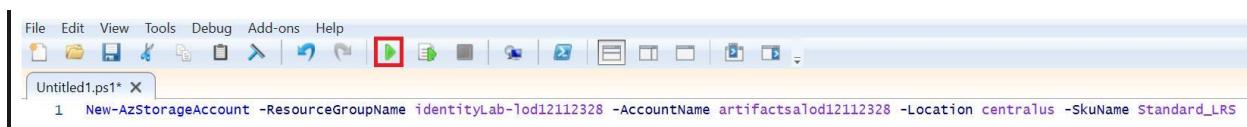
7. Copy the below PowerShell commands to your PowerShell script pane.

Click the **Type Text** icon to automatically type the associated text to the active window in your hosted lab machine on the left.

Windows_PowerShell

```
New-AzStorageAccount -ResourceGroupName identityLab-lod18918877 -AccountName artifactsalod18918877 -Location centralus -SkuName Standard_LRS
```

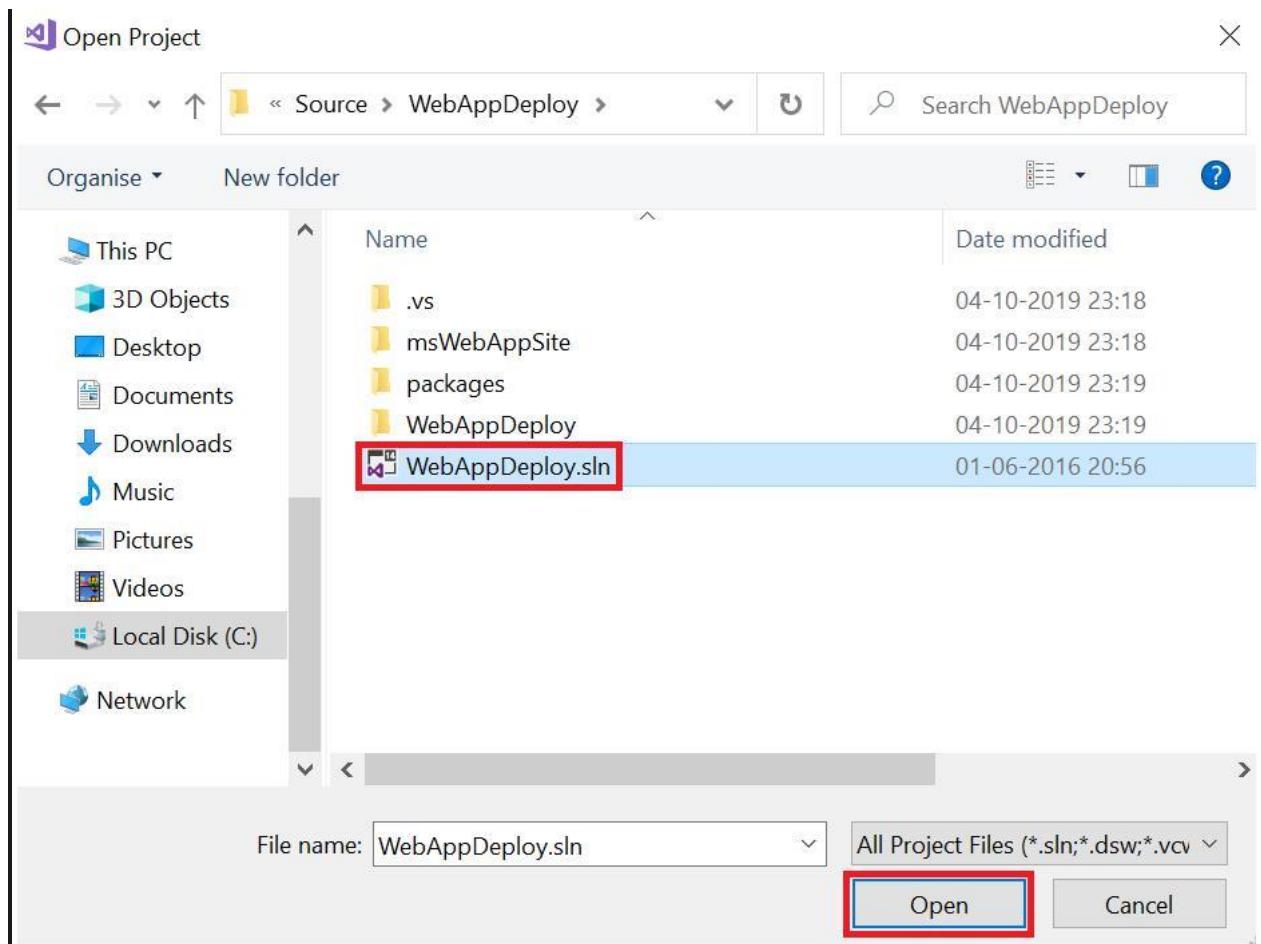
8. Click the **Run** button or press **F5**. This will create the storage account that will be used in this lab.



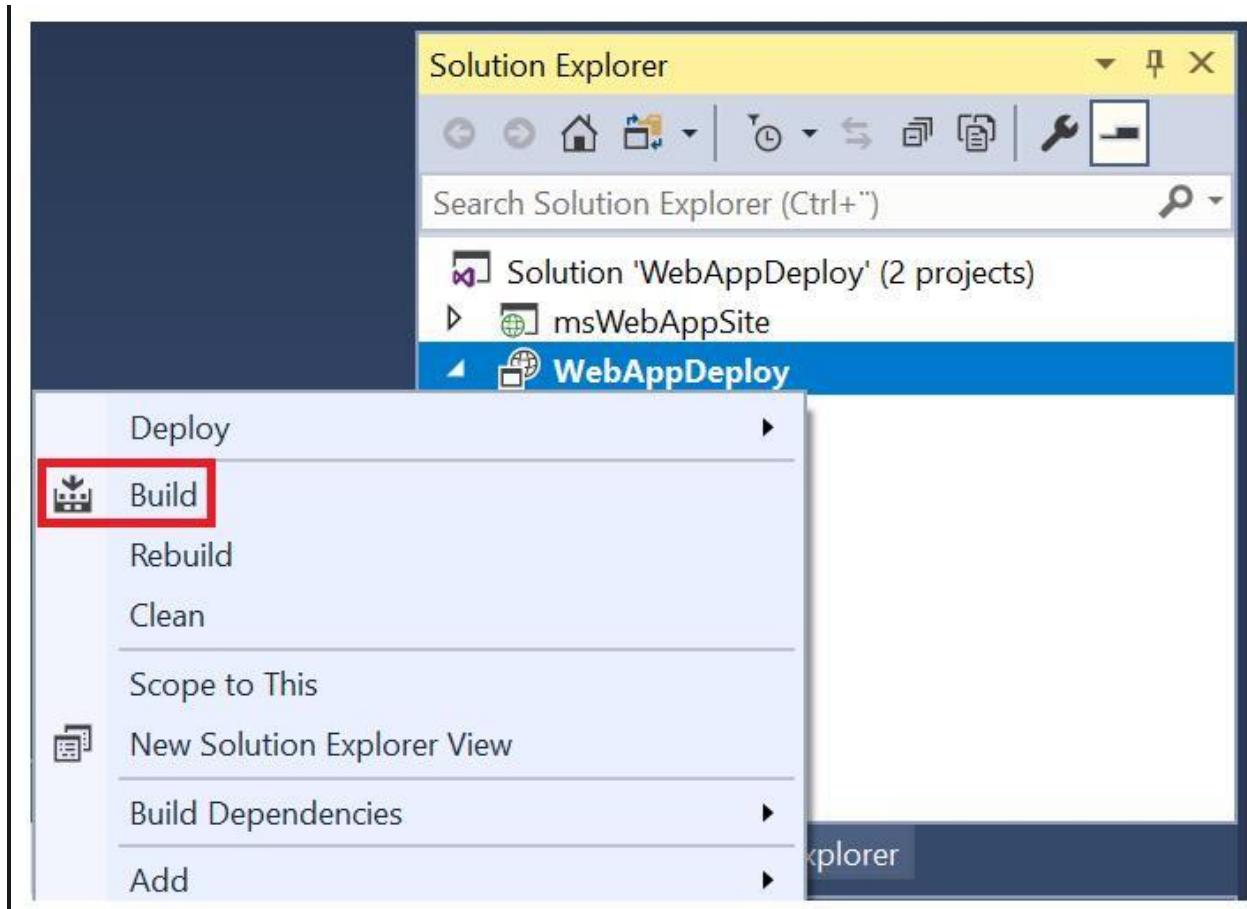
9. The storage account has been successfully created.

StorageAccountName	ResourceGroupName	PrimaryLocation	SkuName	Kind	AccessTier	CreationTime	ProvisioningState	EnableHttpsTrafficOnly	LargeFileShares
artifactsalod9873500	identityLab-lod9873500	centralus	Standard_LRS	StorageV2	Hot	01-05-2020 12:56:20	Succeeded	True	

10. Whilst still in the hosted lab machine, from the Taskbar, open **Visual Studio** as an **Administrator**.
11. Click **File | Open | Project/Solution** and then browse to **C:\AzureIaaS\WS\M6 - Azure Identity\Labs\IntroToRBAC\Source\WebAppDeploy** then select the **WebAppDeploy.sln** file and click **Open**.



12. Right-click the **WebAppDeploy** solution in Solution Explorer, and select **Build**.



13. This will take around thirty to forty seconds to complete.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 53 Min Remaining

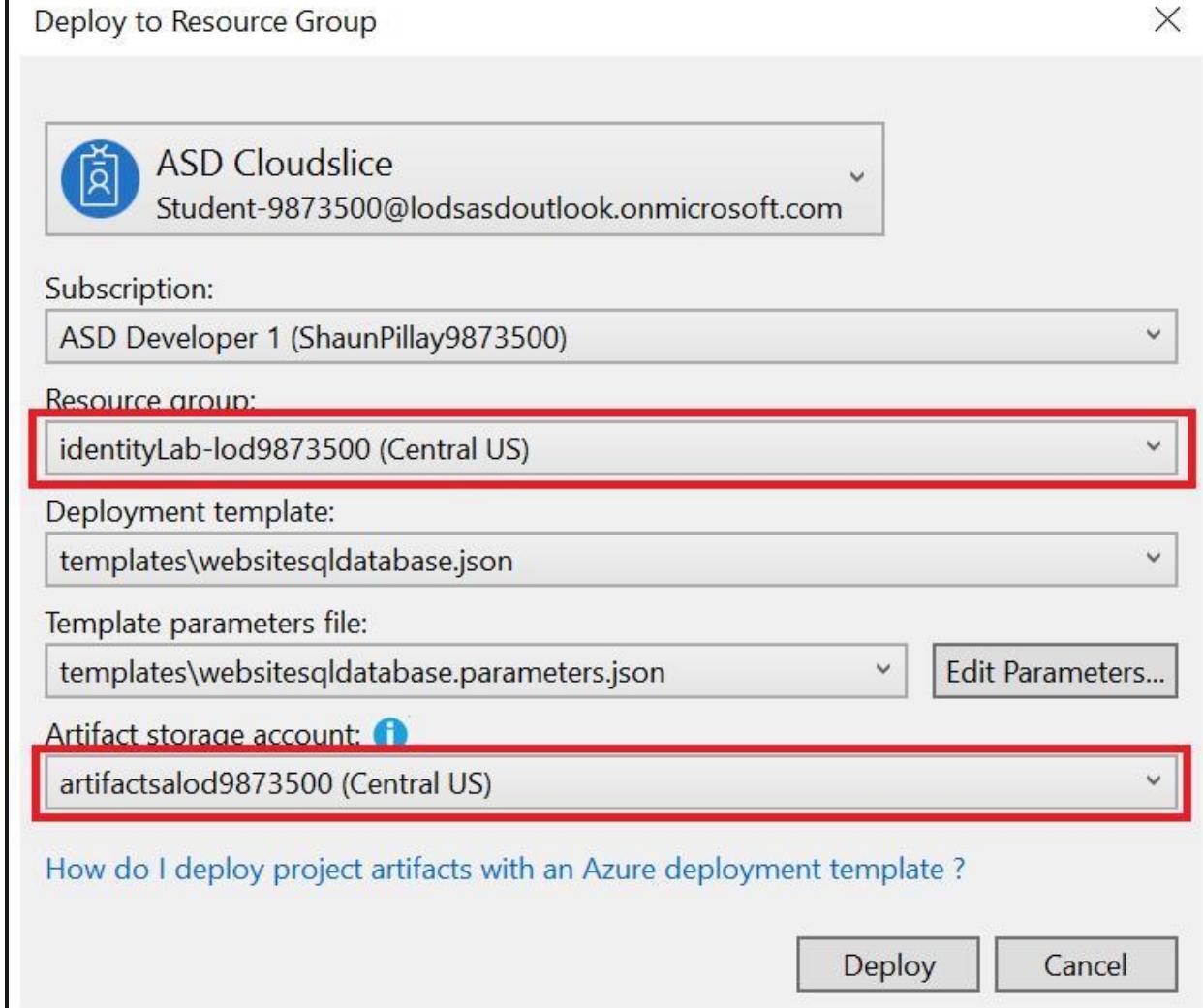
Instructions Resources Help 100%

Task 2 - Deploy the Web Application

During this exercise you will be deploying the simple Web Application that was built in the previous task to an **Azure App Service** instance.

1. Whilst still in **Visual Studio**, right-click on the **WebAppDeploy** project in the Solution Explorer and select **Deploy | New**.
2. In the Deploy to Resource Group dialog box, if you have not already signed in to Azure, select **Add an Account** from the top left-hand corner dropdown menu and sign in using your Azure Trial Pass credentials.

3. Once you are signed in to Azure, click the **Resource group** dropdown menu and select the **identityLab-lodXXXXXX** e.g. **identityLab-lod9873500** resource group, then click the **Artifact storage account** dropdown menu and select the **artifactsalodXXXXXX** e.g. **artifactsalod9873500** storage account that was created earlier. This storage account will be used to store your resource deployment, in this case a Web Application.



4. Click the **Edit Parameters** button to explore the parameters that are required for this deployment.

Edit Parameters

X

The following parameter values will be used for this deployment:

Parameter Name	Value
hostingPlanName	identityAppPlan
skuName	S1
skuCapacity	1
administratorLogin	AdminUser
administratorLoginPassword	*****
databaseName	memberdb
collation	SQL_Latin1_General_CI_AS
edition	Basic
maxSizeBytes	1073741824
requestedServiceObjectiveName	Basic
_artifactsLocation	<Auto-generated>
_artifactsLocationSasToken	<Auto-generated>
msdeployPackageFolder	msWebAppSite
msdeployPackageFileName	package.zip

Save passwords as plain text in the parameters file

Save

Cancel

The mandatory parameters that must be configured are highlighted above.

Parameter	Value
hostingPlanName	the hosting plan name for the Azure App service
skuName	Azure App service tier
skuCapacity	size of the web server machines
administratorLogin/Password	username and password for the db server
databaseName	must be memberdb for this exercise

Parameter	Value
msdeployPackageFolder	the project name of the web application being deployed. Pay no attention to the fact that it says 'folder'.
msdeployPackageName	the name of the package file to be deployed. In our case, the name will be package.zip

- 5. Make sure you check the '**Save Passwords as plain text...**' checkbox and click **Save**.
- 6. Click the **Deploy** button. If the Edit Parameters box pops up again, just make sure you select the **Save Passwords as plain text...** checkbox again and click **Save**.

The deployment should take on average around 4 - 6 minutes to complete.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 53 Min Remaining

Instructions Resources Help 100%

Task 3 - Confirm Deployment of Web App in Azure

- 1. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
- 2. On the left-hand side, click the **Resource groups** tile, then click the **identityLab-
IodXXXXXX** e.g. **identityLab-Iod9873500** resource group.

Showing 1 to 11 of 11 records.		Subscription ↑↓
<input type="checkbox"/> Name ↑↓		
<input type="checkbox"/>	armPolicyLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	armPSLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	armVSLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	automationLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	backupLab-lod9873500	ASD Developer 1
<input checked="" type="checkbox"/>	identityLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	managementLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	netwLabCentralUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	netwLabEastUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	storageLab-lod9873500	ASD Developer 1

3. Your resource group blade will open. It will display all resources that belong to this resource group. Click on the **web app**.

Showing 1 to 6 of 6 records. <input type="checkbox"/> Show hidden types ⓘ		Type ↑↓
<input type="checkbox"/> Name ↑↓		Type ↑↓
<input type="checkbox"/>	artifactsalod9873500	Storage account
<input type="checkbox"/>	identityAppPlan	App Service plan
<input type="checkbox"/>	memberdb (sqlserverwqfpnjguw2hcq/memberdb)	SQL database
<input type="checkbox"/>	sqlserverwqfpnjguw2hcq	SQL server
<input type="checkbox"/>	webSitewqfpnjguw2hcq	Application Insights
<input checked="" type="checkbox"/>	webSitewqfpnjguw2hcq	App Service

4. In the web app blade, scroll down and click on the **Configuration** tile.

The screenshot shows the Azure portal interface for managing an App Service. The top navigation bar displays the site name "webSitewqfpnjguw2hcq" and the "App Service" category. A search bar is present at the top left. Below the header, there are several navigation links: "Quickstart", "Deployment slots", "Deployment Center", and a "Settings" section which includes "Configuration", "Authentication / Authorization", "Application Insights", "Identity", "Backups", "Custom domains", and "TLS/SSL settings". The "Configuration" link is specifically highlighted with a red rectangular box.

5. In the Configuration blade, scroll down to the **Connection strings** setting and click the **Advanced edit** button.

Connection strings

Connection strings are encrypted at rest and transmitted over an encrypted channel.

		New connection string	Show values	Advanced edit	Filter
Name	Value	Type			
DefaultConnection	Hidden value. Click show values button above to view				SQLServer

6. In the **Advanced edit** pane, scroll along to the right and confirm that the Admin username and password matches that of which was specified during your template deployment in Visual Studio, then click **OK**.

```
2
3
4  :1433;Initial Catalog=memberdb;User Id=AdminUser@sqlserverwqfpnjguw2hcq;Password=P@55word1234 ";
5
6
```

7. To test the application, in the left-hand pane, scroll up to the top and click the **Overview** tile, then in the right hand pane, click the **Browse** tile.

Browse	Stop	Swap	Restart	Delete	Get publish profile	Reset publish profile
Resource group (change) identityLab-lod9873500					URL https://websitewqfpnjguw2hcq.azurewebsites.net	
Status Running					App Service Plan identityAppPlan (\$1: 1)	
Location Central US					FTP/deployment username No FTP/deployment user set	
Subscription (change) ASD Developer 1					FTP hostname ftp://waws-prod-dm1-063.ftp.azurewebsites.windows.net	
Subscription ID cd5624ee-c42c-4f43-9c6d-4aea23072cf3					FTPS hostname ftps://waws-prod-dm1-063.ftp.azurewebsites.windows.net	

8. If your web application was successfully deployed, the returned website will look like the screenshot below. You will also be able to register new users and log in.

ASP.NET

ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS and JavaScript.

[Learn more »](#)

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 52 Min Remaining

Instructions Resources Help 100%

Exercise 2 - Delegate roles using Azure RBAC

During this exercise you will be delegating administration using Azure RBAC to the environment that was built in the previous step. A set of user accounts and groups must be created prior to carrying out this task. These user accounts and groups must be added to their respective groups, the details of which can be seen in the table below. User and group names can be suffixed with your unique student ID e.g. **Kyle-9873500** and **Admins-9873500**.

Group	Description	Membership
Admins-XXXXXXX	Resource Group administrators - full control	Kyle
Web Dev-XXXXXXX	Web Developers - access web as a contributor but cannot access SQL	George, Admins-XXXXXXX
Web Reader-XXXXXXX	Web readers can only read web app information	Fred

Group	Description	Membership
SQL Dev-XXXXXXX	SQL Dev can access databases, make changes, add tables etc	Angie, Admins-XXXXXXX

In line with best practices, roles will be delegated using groups. These groups along with their respective RBAC roles and scope have been defined in the table below. This is the delegation of administration model that we will be following.

RBAC Role	Scope	AAD Group
Owner	Resource Group	Admins
Website Contributor	Web App	Web Dev
Reader	Web App	Web Reader
SQL DB Contributor	SQL Server	SQL Dev

As a reference, the selected RBAC roles above have the following capabilities:

Owner - By default lets you manage everything, including access to resources.

Website Contributor - Lets you manage websites (not web plans), but not access to them.

Reader - By default lets you view everything, but not make any changes.

SQL DB Contributor - Lets you manage SQL databases, but not access to them. Also, you can't manage their security-related policies or their parent SQL servers.

Create Azure Active Directory Users and Groups

1. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
2. Click the **Azure Active Directory** tile.

Microsoft Azure Search

«

-  Create a resource
-  Home
-  Dashboard
-  All services
- FAVORITES**
-  Virtual machines
-  Load balancers
-  Storage accounts
-  Virtual networks
-  Azure Active Directory
-  Monitor
-  Advisor
-  Security Center
-  Cost Management + Bill...
-  Help + support

3. Click the **Users** tile.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the "Microsoft Azure" logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the breadcrumb navigation shows "Home > Default Directory | Overview". The main content area has a sidebar on the left with various service tiles: "Create a resource", "Home", "Dashboard", "All services", and a "FAVORITES" section containing "Virtual machines", "Load balancers", "Storage accounts", "Virtual networks", "Azure Active Directory", "Monitor", "Advisor", "Security Center", and "Cost Management + Bill...". To the right of the sidebar, the "Default Directory | Overview" page is displayed. It features an "i" icon and the text "Default Directory | Overview" under "Azure Active Directory". There's a search bar at the top right labeled "Search (Ctrl+/)". Below the search bar are three quick links: "Overview", "Getting started", and "Diagnose and solve problems". Under the "Manage" heading, there's a list of items: "Users" (which is highlighted with a red box), "Groups", "Organizational relationships", "Roles and administrators (Pr...)", "Administrative units (Preview)", "Enterprise applications", and "Devices".

4. Click the **+ New user** tile.

The screenshot shows the 'Users | All users (Preview)' page in Azure Active Directory. At the top, there's a navigation bar with 'Default Directory - Azure Active Directory'. Below it, a toolbar has several buttons: '+ New user' (highlighted with a red box), '+ New guest user', 'Bulk create', 'Bulk invite', and 'Bulk delete'. On the left, there are two dropdown menus: 'All users (Preview)' and 'Deleted users'. A search bar with 'Search users' and a 'Add filters' button are also present.

5. Ensure the **Create user** radio button is selected.

The screenshot shows the 'New user' creation page. The URL in the browser is 'Home > Default Directory > Users | All users (Preview) > New user'. The page title is 'New user' with 'Default Directory' below it. There's a 'Got feedback?' link with a heart icon. Two options are shown: 'Create user' (selected and highlighted with a red box) and 'Invite user'. Both options have descriptive text and a 'I want to...' link. At the bottom, there's a 'Help me decide' link.

6. Type in a **User name** of **kyle** and a **Name** of **Kyle**. Tick the **Show Password** tickbox and copy the **Initial password** and save it to notepad for use later on. Leave the other settings as default and click **create**

New user

Default Directory

Got feedback?

Identity

User name * ⓘ

kyle @ iaaswslab@hotmail.onmicrosoft.com The domain name I need isn't shown here

Name * ⓘ

Kyle

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password

Bala3963

Show Password

Create

7. Repeat this process to create user accounts for the other three users, George, Fred and Angie.
8. The next step is to create the Azure Active Directory groups. From within the Azure Active Directory blade, click the **Groups** tile.

 Create a resource

 Home

 Dashboard

 All services

 **FAVORITES**

 SQL databases

 Azure Cosmos DB

 Virtual machines

 Load balancers

 Storage accounts

 Virtual networks

 Azure Active Directory

 Monitor

 Advisor



Default Directory | Overview

Azure Active Directory

Search (Ctrl+ /) «

 Overview

 Getting started

 Diagnose and solve problems

Manage

 Users

 Groups

 Organizational relationships

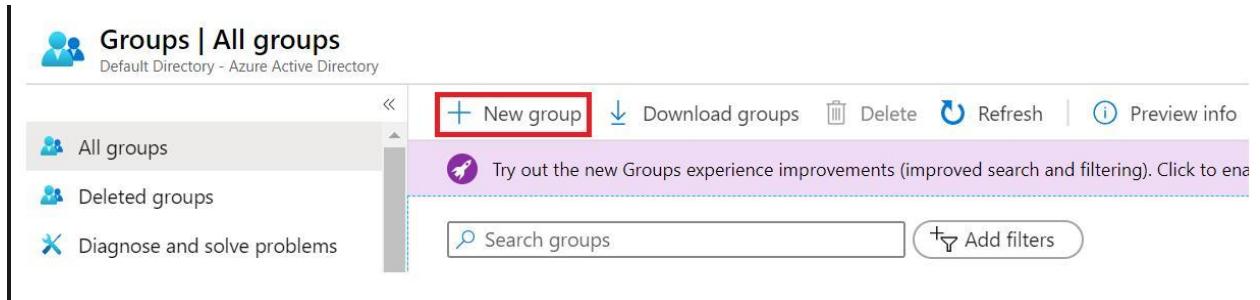
 Roles and administrators (Pr...)

 Administrative units (Preview)

 Enterprise applications

 Devices

9. Click the + New group tile.



10. Accept the default group type of **Security**, then type in a **Group name** of **Admins-XXXXXX** where **XXXXXX** is your unique student ID number e.g. **Admins-9873500**. Type in the group description from the table above, e.g. for the **Admins-XXXXXX** group, the description is **Resource Group administrators - full control**.

Home > Default Directory > Groups | All groups > New Group

New Group

Group type *

Security

Group name * ⓘ

Admins-9873500

Group description ⓘ

Resource Group administrators - full control

Membership type ⓘ

Assigned

A screenshot of the 'New Group' form. The 'Group name' field contains 'Admins-9873500' and the 'Group description' field contains 'Resource Group administrators - full control'. Both fields are highlighted with a red border and a green checkmark in the bottom right corner. The other fields ('Group type' and 'Membership type') are not highlighted.

11. Click the **No members selected** link.

Group description ⓘ

Resource Group administrators - full control ✓

Membership type ⓘ

Assigned ▾

Owners

No owners selected

Members

No members selected

12. Type in **Kyle** into the search box, then click on **Kyles** account from the results.

Home > Default Directory > Groups | All groups > New Group

New Group

Security

Group name * ⓘ

Admins-9873500

Group description ⓘ

Resource Group administrators - full control

Membership type ⓘ

Assigned

Owners

No owners selected

Members

No members selected

Add members

Search ⓘ

KY Kyle kyle@iaaswslabhotmail.onmicrosoft.com

Selected items

No items selected

Create Select

13. Click the **Select** button.

New Group

Security

Group name * ⓘ
Admins-9873500

Group description ⓘ
Resource Group administrators - full control

Membership type ⓘ
Assigned

Owners
No owners selected

Members
No members selected

Create Select

14. You should now have one group member selected, click the **Create** button.

Home > Default Directory > Groups | All groups > New Group

New Group

Group type *
Security

Group name * ⓘ
Admins-9873500

Group description ⓘ
Resource Group administrators - full control

Membership type ⓘ
Assigned

Owners
No owners selected

Members
1 member selected

Create

15. Repeat this process to create the other three groups and configure their group memberships during group creation time. Refer to the table above for the respective group names, descriptions and memberships.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 52 Min Remaining

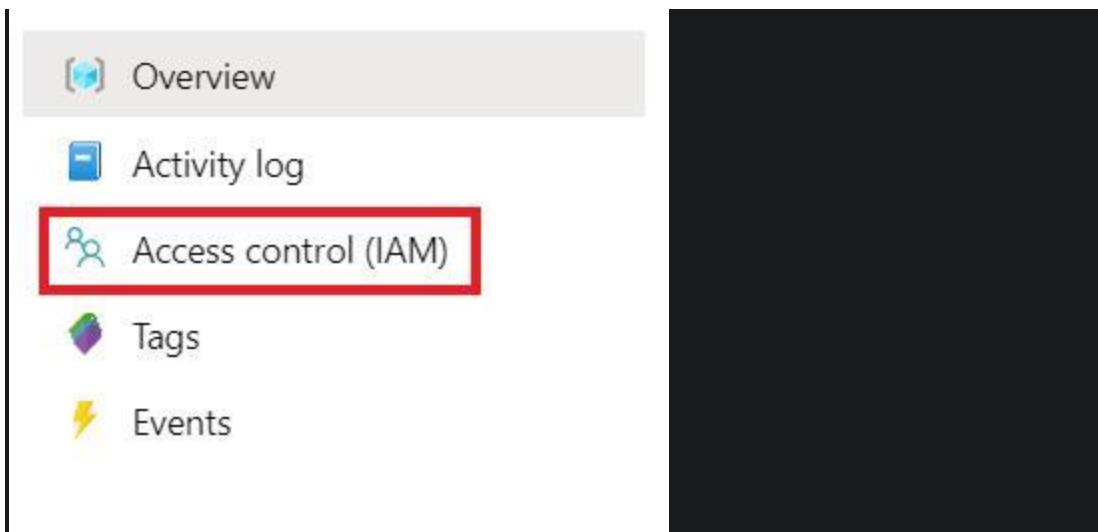
Instructions Resources Help 100%

Task 1 - Assigning roles using the Azure portal

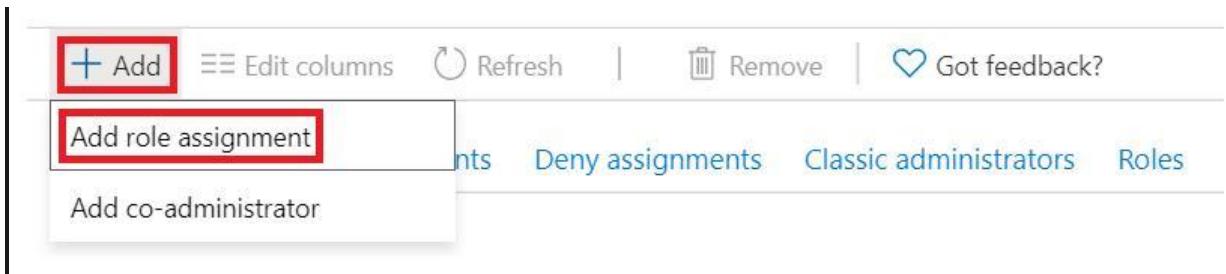
1. If not already logged in, log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
2. Click **Resource Groups** in the left-hand pane, then click on the **identityLab-lodXXXXXX** e.g. **identityLab-lod9873500** resource group. This will open up your resource group blade.

Name	Subscription
armPolicyLab-lod9873500	ASD Developer 1
armPSLab-lod9873500	ASD Developer 1
armVSLab-lod9873500	ASD Developer 1
automationLab-lod9873500	ASD Developer 1
backupLab-lod9873500	ASD Developer 1
identityLab-lod9873500	ASD Developer 1
managementLab-lod9873500	ASD Developer 1
netwLabCentralUS-lod9873500	ASD Developer 1
netwLabEastUS-lod9873500	ASD Developer 1
storageLab-lod9873500	ASD Developer 1

3. The first thing you need to do is set permissions at the **resource group** level. Recall from the table earlier that **Kyle** is an administrator and should be set to **Owner** for all items in this resource group. From within the resource group blade, click on the **Access control (IAM)** tile to access RBAC settings.



4. Click the **+ Add** tile, then click **Add role assignment**.



5. In the Add role assignment blade, click **Role** and then select **Owner**.



6. In the **Select** search box, type in **Admins-** followed by your unique student ID e.g. **Admins-9873500**. This will list your Admin group. It is very important that you select the Admins group that is suffixed with your student ID in order to avoid a misconfiguration. Click the **Admins-XXXXXXX** e.g. **Admins-9873500** group.

Role ⓘ

Owner

Assign access to ⓘ

Azure AD user, group, or service principal

Select ⓘ

Admins-9873500

 Admins-9873500

7. Click **Save**.

Selected members:



Admins-9873500

[Remove](#)

Save

Discard

Recall that you want Angie to have SQL database developer/modification permissions. In order to provide this, you will need to configure this permission at the resource group level.

8. Click the **+ Add** tile, then click **Add role assignment**. Click **Role** then select **SQL DB Contributor**, type in **SQLDev-** followed by your unique student ID e.g. **SQLDev-**

9873500 into the **Select** search box. This will list your SQL Dev group. Click the **SQLDev-XXXXXX** e.g. **SQLDev-9873500** group.

The screenshot shows the 'Assign access to' blade. At the top, the 'Role' dropdown is set to 'SQL DB Contributor'. Below it, the 'Assign access to' dropdown is set to 'Azure AD user, group, or service principal'. A search bar contains the text 'SQLDev-9873500'. A list item 'SQLDev-9873500' is shown, featuring a purple square icon with 'SQ' and the text 'SQLDev-9873500'. The entire search bar and the list item are highlighted with a red box.

9. Click **Save**.

The screenshot shows the 'Selected members' list. It contains one item: 'SQLDev-9873500', which is preceded by a purple square icon with 'SQ'. To the right of the item is a 'Remove' link. At the bottom of the list are two buttons: a blue 'Save' button with a red border and a blue 'Discard' button.

10. Close the Access Control (IAM) blade.
11. From within the resource groups blade, click on the **identityLab-
lodXXXXXX** e.g. **identityLab-lod9873500** resource group, then click on the web application tile. This will open the web app blade.

Showing 1 to 6 of 6 records. Show hidden types

<input type="checkbox"/> Name ↑↓	Type ↑↓
<input type="checkbox"/> artifactsalod9873500	Storage account
<input type="checkbox"/> identityAppPlan	App Service plan
<input type="checkbox"/> memberdb (sqlserverwqfpnjguw2hcq/memberdb)	SQL database
<input type="checkbox"/> sqlserverwqfpnjguw2hcq	SQL server
<input type="checkbox"/> webSitewqfpnjguw2hcq	Application Insights
<input type="checkbox"/> webSitewqfpnjguw2hcq	App Service

12. Click the **Access Control (IAM)** tile like you did earlier in order to configure RBAC.
13. On the Access Control (IAM) blade, click **+ Add** then click **Add role assignment**.
14. Click on **Role**, select **Website Contributor**, search for your **WebDev-XXXXXXX** e.g. **WebDev-9873500** group and select it.

Role

Website Contributor

Assign access to

Azure AD user, group, or service principal

Select

WebDev-9873500

WebDev-9873500

15. Click **Save**.

Selected members:

The screenshot shows a list of selected members under the 'Access Control (IAM)' blade of a web application. One member, 'WebDev-9873500', is listed with a 'WE' icon. To the right of the member name is a 'Remove' link. At the bottom of the list are two buttons: 'Save' (highlighted with a red border) and 'Discard'.

16. While still in the **Access Control (IAM)** blade of the web application, click **+ Add** then click **Add role assignment**. Click **Role**, select the **Reader** role, then search for your **WebReader-XXXXXXX** e.g. **WebReader-9873500** group, select it and click **Save**.

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 52 Min Remaining

Instructions Resources Help 100%

Exercise 3 - Test Azure RBAC roles

Now that you have configured Azure RBAC, you will test access control for your users.

Task 1 - Confirm Admin group permissions

- Right-click on your Internet Explorer icon and click **Start InPrivate Browsing**.
- Log in to the Azure portal at <https://portal.azure.com> using **Kyles** credentials.

3. Click the **Resource groups** tile, then click on the **identityLab-
lodXXXXXX** e.g. **identityLab-lod9873500** resource group. Note that the only resources shown in the list are the ones that Kyle has permission to access.
4. Within the resource group blade, you can perform tasks like grant other users permission to resources within the resource group, modify the web app etc. you will also notice that Kyle has full permission to do this.
5. Select the **+ Create a resource** button in the top left-hand corner of the portal and try to create a new resource. You will be allowed to create this new resource, but you can only put the resource in the resource group that *Kyle* has permission to access.
6. Sign out of the Azure portal with Kyle's account.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 51 Min Remaining

Instructions Resources Help 100%

Task 2 - Confirm SQL Dev group permissions

1. Right-click on your Internet Explorer icon and select Start InPrivate Browsing.
2. Log in to the Azure portal at <https://portal.azure.com> using **Angies** credentials.
3. Click the **Resource groups** tile, then click on the **identityLab-
lodXXXXXX** e.g. **identityLab-lod9873500** resource group. Note that Angie can only see the database server and the **memberdb** database.
4. Click on the **memberdb** database, then click on the **Configure** button in the database blade. Here you can test to see if Angie has permission to make changes to the database.

Try increasing the DTU's Max data size from 1GB to 2GB and click **Apply**.

5. However, since Angie is only a SQL DB Contributor, she cannot make changes such as turning on Auditing. Click the Auditing button and verify that she has no access here.
6. Sign out of the Azure portal with Angie's account.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 51 Min Remaining

Instructions Resources Help 100%

Task 3 - Confirm Web Dev permissions

1. Right-click on your Internet Explorer icon and select **Start InPrivate Browsing**.
2. Log in to the Azure portal at <https://portal.azure.com> using **Georges** credentials.

Recall that George is in the Web Dev group that has been given the Website Contributor permission directly on the web app. This means that George can not access other resources in the resource group.

Because the Web Dev group only has access to the web app, if *George* tries to browse for resource groups, he will not see any listed. Instead, click **All services** in the top left hand pane then type in **App Services** into the All services search box and hit Enter. This will list the web application that you have deployed.

[more...](#)

3. Click your web app from the list, this will open the web app blade.
4. Scroll through the list of settings. You will notice that there are some settings grayed out, which means that George cannot make changes to them. The reason for this is because George has been granted the Website Contributor permission. In order to change the grayed-out settings, George would need to have the Contributor permission or higher.
5. Sign out of the Azure portal with George's account.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 51 Min Remaining

Instructions Resources Help 100%

Task 4 - Confirm Web Reader permissions

1. Right-click on your Internet Explorer icon and select **Start InPrivate Browsing**.
2. Log in to the Azure portal at <https://portal.azure.com> using **Freds** credentials.

Recall that Fred is in the Web Reader group that has been given the Reader permission directly on the web app. This means that Fred can not access other resources in the resource group, he can only read settings for the web app.

Because the Web Reader group only has access to the web app, if Fred tries to browse for resource groups, he will not see any listed. Instead, click **All services** in the top left-hand pane then type in **App Services** into the All services search box and hit Enter. This will list the web application that you have deployed.

[...less](#)

3. Click your web app from the list, this will open the web app blade.
4. Click the Application settings tile, notice that Fred can read most settings but some settings such as connection strings he has no access to.
5. Sign out of the Azure portal with Fred's account.

Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 50 Min Remaining

Instructions Resources Help 100%

Module 7 - Automating Virtual Machine Deployment with Microsoft Azure PowerShell

Introduction

In this hands-on lab you will understand the advantages of automating the deployment and management of virtual machines in Microsoft Azure.

Objectives

In this hands-on lab, you will learn how to:

- Create a Storage Account
- Create an Availability Set
- Create an Azure Load Balancer with NAT rules defined
- Configure virtual machines as backends for the Azure Load Balancer

Prerequisites

The following are required to complete this hands-on lab:

- Microsoft Azure PowerShell v5.1.1 or later
- Microsoft Azure PowerShell Az module v2.5.0 or later
- A Microsoft Azure subscription

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 50 Min Remaining

Instructions Resources Help 100%

Exercise 1 - Create Load Balancer dependent resources

Task 1 - Obtain and set your Azure subscription

1. Connect to **Win10 Lab VM** as **Student** using **pass@word1** as the password.
2. Open PowerShell as an Administrator.
3. In the PowerShell command prompt, run the following command and press Enter.

```
Windows_PowerShell  
Connect-AzAccount
```

4. At the Sign in prompt, log in to your Azure subscription using your Azure Trial Pass credentials.
5. Get the available subscriptions by using the following command.

```
Windows_PowerShell  
Get-AzSubscription | Sort Name | Select Name
```

6. Set your Azure subscription for the current session. Replace the **[Your-subscription-name]** placeholder below with the value returned from the previous command.

```
Windows_PowerShell  
$subscr="[Your-subscription-name]"  
Get-AzSubscription -SubscriptionName $subscr | Select-AzSubscription
```

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 50 Min Remaining

Instructions Resources Help 100%

Task 2 - Create a Storage Account

The best practice when deploying virtual machines is to use **Managed Disks**, this exercise uses **Unmanaged Disks** so that you are familiar with the concept should you be required to deploy virtual machines with unmanaged disks.

1. Create a storage account for your new virtual machine with these commands.

```
Windows_PowerShell
$rgName="managementLab-lod18918877"
$locName="centralus"
$saName="student18918877sa"
$saType="Standard_LRS"

New-AzStorageAccount -Name $saName -ResourceGroupName $rgName -Type
$saType -Location $locName
```

2. You must pick a globally unique name for your storage account that contains only lowercase letters and numbers. You can use this command to check the availability of a different storage account name should the storage account name above be in use.

```
Windows_PowerShell
Get-AzStorageAccountNameAvailability -Name "accountname"
```

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 50 Min Remaining

Instructions Resources Help 100%

Task 3 - Check availability of a DNS hostname

Prior to creating a Load Balancer and assigning it a hostname, you need to check if the hostname that you would like to assign is available. The name can only contain letters, numbers and hyphens. The first and last character must be a letter or number.

1. To check the availability of your hostname, use the following command:

```
Windows_PowerShell
$hostName="student18918877ilb"
$locName="centralus"

Test-AzDnsAvailability -DomainQualifiedName $hostName -Location $locName
If DNSAvailability is "True", your proposed name is globally unique.
```

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 50 Min Remaining

Instructions Resources Help 100%

Task 4 - Create an Availability Set

1. **Availability Sets** are recommended when there are two or more VMs deployed. This is so that they can be placed in separate physical racks in an Azure datacenter. In this lab we are deploying a single VM so an Availability Set will add little value, however, we create an Availability Set using PowerShell so that you are familiar with the concept when deploying multiple VMs.

```
Windows_PowerShell
$avName="manageLabAvSet"
$rgName="managementLab-lod18918877"
$locName="centralus"

New-AzAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location
$locName
```

2. Use this command to list existing Availability Sets, in doing so, we are also verifying the creation of our Availability Set.

```
Windows_PowerShell
Get-AzAvailabilitySet -ResourceGroupName $rgName | Sort Name | Select Name
```

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 49 Min Remaining

Instructions Resources Help 100%

Task 5 - Create a Virtual Network

Virtual Machines created with the Resource Manager deployment model require a Resource Manager virtual network. Create a new Resource Manager virtual network with at least one subnet for the new virtual machine.

1. Use the following commands to create a new virtual network named **manageLabVNet** with two subnets named **frontendSubnet** and **backendSubnet**.

```
Windows_PowerShell
$rgName="managementLab-lod18918877"
$locName="centralus"
$vnetName="manageLabVNet"

$frontendSubnet=New-AzVirtualNetworkSubnetConfig -Name frontendSubnet -
AddressPrefix 10.4.0.0/24
```

```
$backendSubnet=New-AzVirtualNetworkSubnetConfig -Name backendSubnet -  
AddressPrefix 10.4.4.0/24  
  
New-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName -Location  
$locName -AddressPrefix 10.4.0.0/16 -Subnet $frontendSubnet,$backendSubnet
```

2. Use this command to list existing virtual networks, in doing so, we are also verifying the creation of our virtual network.

```
Windows_PowerShell  
$rgName="managementLab-lod18918877"  
$locName="centralus"  
  
Get-AzVirtualNetwork -ResourceGroupName $rgName | Sort Name | Select Name
```

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 49 Min Remaining

Instructions Resources Help 100%

Exercise 2 - Create a Public Load Balancer

1. Create a public IP address to be used by the frontend IP pool:

```
Windows_PowerShell  
$rgName="managementLab-lod18918877"  
$hostName="student18918877ilb" #The name that you checked availability  
on earlier  
$publicipname ="manageLabPublicIp"  
$locName="centralus"  
  
$publicIP = New-AzPublicIpAddress -Name $publicipname -  
ResourceGroupName $rgName -Location $locName -AllocationMethod Dynamic  
-DomainNameLabel $hostName  
  
Get-AzPublicIPAddress -Name $publicipname -ResourceGroupName $rgName
```

2. Using the public IP variable (\$publicIP) from the previous step, create the front end IP pool.

```
Windows_PowerShell
```

```
$frontendIP = New-AzLoadBalancerFrontendIpConfig -Name LB-Frontend -  
PublicIpAddress $publicIP
```

3. Set up a back end address pool used to receive incoming traffic from the front end IP pool:

```
Windows_PowerShell  
$beaddresspool= New-AzLoadBalancerBackendAddressPoolConfig -Name "LB-  
backend"
```

4. Create two inbound NAT rules (One for each VM).

```
Windows_PowerShell  
$inboundNATRule1= New-AzLoadBalancerInboundNatRuleConfig -Name "RDP1" -  
FrontendIpConfiguration $frontendIP -Protocol TCP -FrontendPort 3441 -  
BackendPort 3389  
Windows_PowerShell  
$inboundNATRule2= New-AzLoadBalancerInboundNatRuleConfig -Name "RDP2" -  
FrontendIpConfiguration $frontendIP -Protocol TCP -FrontendPort 3442 -  
BackendPort 3389
```

5. Create a new health probe.

```
Windows_PowerShell  
$healthProbe = New-AzLoadBalancerProbeConfig -Name "HealthProbe" -  
RequestPath "/" -Protocol http -Port 80 -IntervalInSeconds 15 -ProbeCount  
2
```

6. Create a new load balancer rule.

```
Windows_PowerShell  
$lbrule = New-AzLoadBalancerRuleConfig -Name "HTTP" -  
FrontendIpConfiguration $frontendIP -BackendAddressPool $beAddressPool -  
Probe $healthProbe -Protocol Tcp -FrontendPort 80 -BackendPort 80
```

7. Create the load balancer adding all objects (NAT rules, Load balancer rules, probe configurations) together:

```
Windows_PowerShell  
$manageLabLB = New-AzLoadBalancer -ResourceGroupName $rgName -Name  
"manageLab-LB" -Location $locName -FrontendIpConfiguration $frontendIP -  
InboundNatRule $inboundNATRule1,$inboundNATRule2 -LoadBalancingRule  
$lbrule -BackendAddressPool $beAddressPool -Probe $healthProbe
```

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

Exercise 3 - Create Virtual Machines for the Public Load Balancer backend pool

1. From within the PowerShell session that you have open, click **File|Open** and navigate to the **C:\AzureIaaS\WS\7 - Azure Management\Labs\PSManagement-ARM** folder, where you will find a PowerShell script called **CommandSet.ps1**. Open this file and enter in your appropriate parameter values for the **\$rgName**, **\$locName** and **\$saName** variables only.

The CommandSet.ps1 file has commands to create the NIC, select the VM size, create the VM, add an additional data disk and also set other configuration parameters for the VM.

2. Once you have entered in your appropriate parameter values, save the file. Then press **F5** to run the script. You will be prompted to enter a Username and Password. These will be used to login to the VMs. Type in **AdminUser** in the Username box and **P@55word1234** in the Password box and press enter.

The script will take around 8 - 9 minutes to complete.

3. To verify the deployment, locate the public IP address of the load balancer.

```
Windows_PowerShell  
Get-AzPublicIPAddress -Name manageLabPublicIp -ResourceGroupName  
managementLab-1od18918877 | flIpAddress
```

4. RDP to the virtual machine via the Public Load Balancer by using **mstsc /v:<IP>:3441**. Replace the <IP> field with the IP address that was returned from the previous command and login with Username: **AdminUser** and Password: **P@55word1234**

Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

4 Hr 48 Min Remaining

Instructions Resources Help 100%

Module 8.1 - Calling a Microsoft Azure Automation Runbook with a Webhook

Introduction

In this lab, you will import a pre-existing Azure Automation runbook which will be used to start and stop Azure VMs. You will then create a **Webhook** and use PowerShell as a client application to call the webhook which will then call the automation runbook.

You'll learn:

- How to create an Automation Account
- How to import, edit and publish an Automation Runbook
- How to create a Webhook
- How to call the Webhook using PowerShell

Prerequisites

The following are required to complete this hands-on lab:

- One or more virtual machines running in this subscription that can be shutdown (you will be creating a virtual machine to be used in this lab in the next task)
- Microsoft Azure subscription

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 47 Min Remaining

Instructions Resources Help 100%

Task 1 - Create a Virtual Machine and an Azure Automation Account

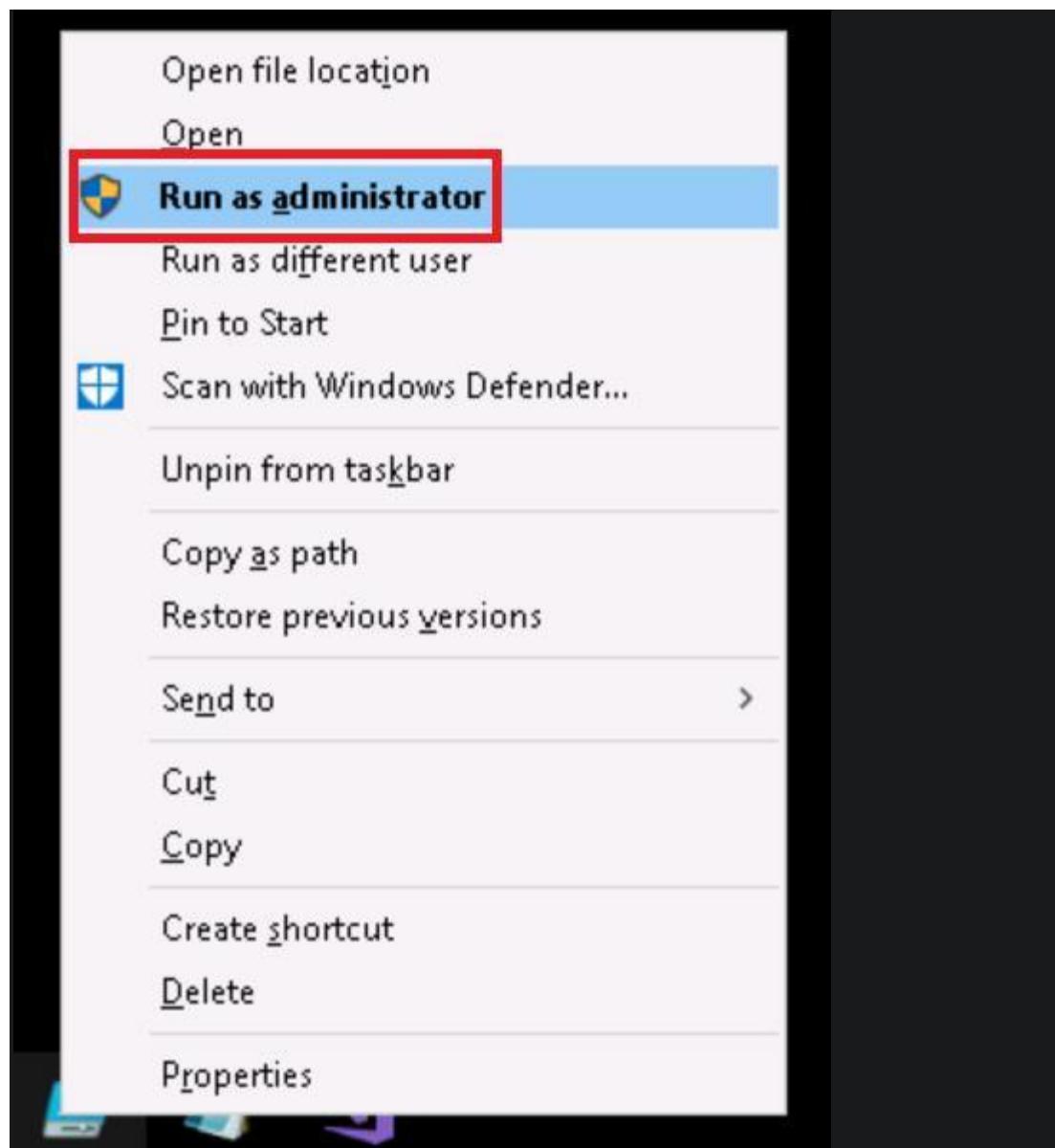
To begin using Azure Automation you need an Automation Account. Automation accounts securely contain the resources that configure and run your runbook jobs. An Automation Account is a logical container and security boundary for all automation resources (runbooks, connections, etc.). Assets within an Automation account are visible only to other assets within the account. An Automation

Account also provides affinity to a region, which helps with data sovereignty concerns (your runbook IP or data is located in a single region only).

1. Login to the [Win10 Lab VM](#) hosted lab machine in the left hand pane with a Username of **Student** and a Password of **pass@word1** Once logged in, if you do not already have a US keyboard layout select your keyboard layout from the task bar.



2. Shift and right-click the PowerShell shortcut on the taskbar and select **Run as administrator**



3. Click **Yes** to the User Account Control pop-up.
4. In the PowerShell command prompt window, type in **Connect-AzAccount** and press **Enter**.
5. Enter the email address that was used to redeem your **Azure Trial Pass** into the Sign in dialog box and click **Next** or press **Enter**.
6. Enter your password and click **Sign in** or press **Enter**. This will log you in to your Azure Trial Pass subscription.

```
PS C:\> Connect-AzAccount

  Account          SubscriptionName      TenantId      Environment
  -----          -----              -----          -----
iaasws1lab@hotmail.com Azure Pass - Sponsorship f30ae15e-afec-42d9-aefc-3709be909663 AzureCloud
```

7. Copy the below PowerShell commands to your PowerShell script pane.

Click the **Type Text** icon to automatically type the associated text to the active window in your hosted lab machine on the left.

Windows_PowerShell

```
Set-Item Env:\SuppressAzurePowerShellBreakingChangeWarnings "true"
$resourceGroup = "automationLab-lod18918877"
.setLocation = "centralus"
$vmName = "VM1"
$userName='AdminUser'
$password='P@55word1234'| ConvertTo-SecureString -Force -AsPlainText
$cred=New-Object PSCredential($UserName,$Password)
$subnetConfig = New-AzVirtualNetworkSubnetConfig -Name frontEnd -
AddressPrefix 10.5.0.0/28
$vnet = New-AzVirtualNetwork -ResourceGroupName $resourceGroup -
Location $location `-
-Name AutomvNET1 -AddressPrefix 10.5.0.0/24 -Subnet $subnetConfig -Force
$pip = New-AzPublicIpAddress -ResourceGroupName $resourceGroup -
Location $location `-
-Name "autoVm1pip$(Get-Random)" -AllocationMethod Static -
IdleTimeoutInMinutes 4
$nsgRuleRDP = New-AzNetworkSecurityRuleConfig -Name
myNetworkSecurityGroupRuleRDP -Protocol Tcp `-
-Direction Inbound -Priority 1000 -SourceAddressPrefix * `-
SourcePortRange * -DestinationAddressPrefix * `-
-DestinationPortRange 3389 -Access Allow
$nsg = New-AzNetworkSecurityGroup -ResourceGroupName $resourceGroup -
Location $location `-
-Name autoVm1NetworkSecurityGroup -SecurityRules $nsgRuleRDP -Force
$nic = New-AzNetworkInterface -Name AutomVM1Nic -ResourceGroupName
$resourceGroup -Location $location `-
-SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -
NetworkSecurityGroupId $nsg.Id -Force
$vmConfig = New-AzVMConfig -VMName $vmName -VMSize Standard_D2_v2 | `-
Set-AzVMOperatingSystem -Windows -ComputerName $vmName -Credential
$cred | `
```

```

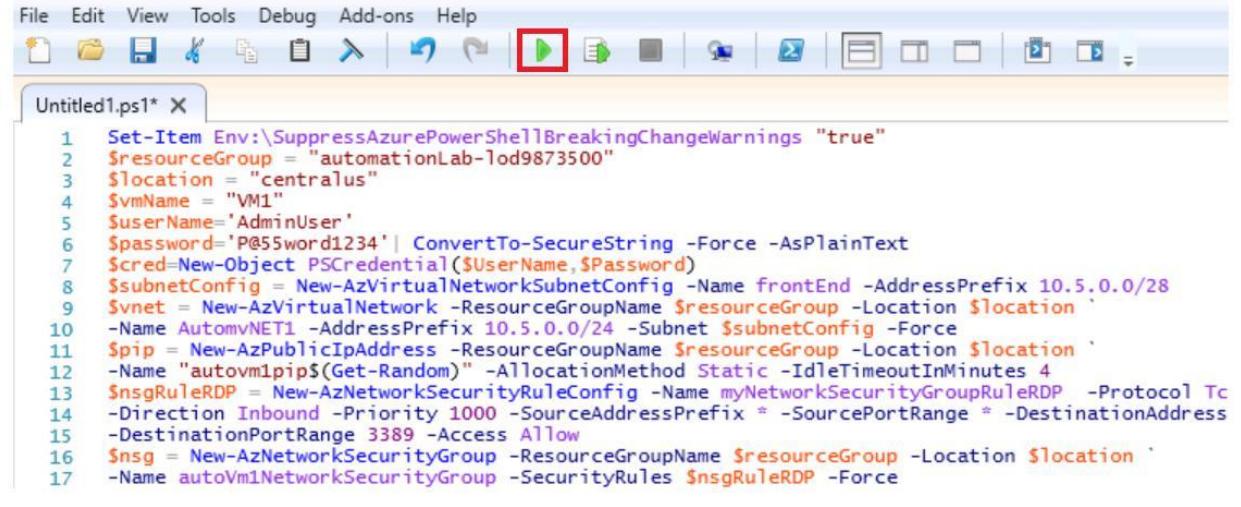
Set-AzVMSourceImage -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2019-Datacenter -Version latest | `

Add-AzVMNetworkInterface -Id $nic.Id

New-AzVM -ResourceGroupName $resourceGroup -Location $location -VM $vmConfig

```

8. Click the **Run** button or press **F5**. This will create the virtual machine that will be used in this lab.



```

File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
1 Set-Item Env:\SuppressAzurePowerShellBreakingChangeWarnings "true"
2 $resourceGroup = "automationLab-1od9873500"
3 $location = "centralus"
4 $vmName = "VM1"
5 $userName='AdminUser'
6 $password='P@55word1234' | ConvertTo-SecureString -Force -AsPlainText
7 $cred=New-Object PSCredential($UserName,$Password)
8 $subnetConfig = New-AzVirtualNetworkSubnetConfig -Name frontEnd -AddressPrefix 10.5.0.0/28
9 $vnet = New-AzVirtualNetwork -ResourceGroupName $resourceGroup -Location $location
10 -Name AutoVmNET1 -AddressPrefix 10.5.0.0/24 -Subnet $subnetConfig -Force
11 $pip = New-AzPublicIpAddress -ResourceGroupName $resourceGroup -Location $location
12 -Name "autoVm1pip$((Get-Random))" -AllocationMethod Static -IdleTimeoutInMinutes 4
13 $nsgRuleRDP = New-AzNetworkSecurityRuleConfig -Name myNetworkSecurityGroupRuleRDP -Protocol Tc
14 -Direction Inbound -Priority 1000 -SourceAddressPrefix * -SourcePortRange * -DestinationAddress
15 -DestinationPortRange 3389 -Access Allow
16 $nsg = New-AzNetworkSecurityGroup -ResourceGroupName $resourceGroup -Location $location
17 -Name autoVm1NetworkSecurityGroup -SecurityRules $nsgRuleRDP -Force

```

9. The virtual machine has been successfully created.

RequestId	IsSuccess	Status	StatusCode	ReasonPhrase
	True		OK	OK

10. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
11. Click **+ Create a resource**, type in **Automation** in the **Search the Marketplace** search box, then press Enter. This will list the Automation resource, click **Create**.

Automation
Microsoft



Automation Microsoft

Create

Create an Automation Account

An Automation Account is a container for your Azure Automation resources. It provides a way to separate your environments or further organize your Automation workflows and resources.

Process automation that simplifies cloud management

Azure Automation allows you to automate the creation, deployment, monitoring, and maintenance of resources in your Azure environment and across external systems. Azure uses a highly scalable and reliable workflow execution engine to simplify cloud management. Orchestrate time-consuming and frequently repeated tasks across Azure and third-party systems.

Integrate into the systems you depend on

With Automation, you can connect into any system that exposes an API over typical Internet protocols. Azure Automation includes integration into many Azure services, including:

- Web Sites (management)
- Cloud Services (management)
- Virtual Machines (management and WinRM support)
- Storage (management)
- SQL Server (management and SQL support)

12.  When setting up an Automation Account, you will need to configure:

- The name of the Automation Account e.g. **labAutomAcc**
- Select your Azure subscription (Accept the default)
- Select the **automationLab-1odXXXXXXX** e.g. **automationLab-1od9873500** resource group if not already selected
- Select a Location to put the Automation Account in, this should be **Central US**
- Select **Yes** to create an Azure Run As account
- Click **Create**.

Add Automation Account



Name * ⓘ

labAutomAcc



Subscription *

ASD Developer 1



Resource group *

automationLab-lod9873500



[Create new](#)

Location *

Central US



Create Azure Run As account * ⓘ

Yes

No



This will create Azure Run As account in the Automation account which are useful for authenticating with Azure to manage Azure resources from Automation runbooks. Note that the creation of Azure Run As account may affect the security of the subscription.[Learn more](#)



Learn more about Automation pricing.

Create

13. Once the Automation Account has been created, navigate to the **automationLab-
lodXXXXXXX** e.g. **automationLab-lod9873500** resource group and click on your Automation Account.

automationLab-1od9873500

Resource group

Overview

Subscription (change)
ASD Developer 1

Deployments
1 Succeeded

Subscription ID
cd5624ee-c42c-4f43-9c6d-4aea23072cf3

Tags (change)
Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 10 of 10 records. Show hidden types

Name	Type
AzureAutomationTutorialPython2 (labAutomAcc/AzureAutomationTutorialPython2)	Runbook
AzureAutomationTutorialScript (labAutomAcc/AzureAutomationTutorialScript)	Runbook
labAutomAcc	Automation Account
VM1	Virtual machine
VM1 OsDisk 1 3644195408ea4dde993079f4d3e4958d	Disk

14. The Overview of your Automation Account should look similar to this:

labAutomAcc

Automation Account

Overview

Resource group... : automationLab-1od9873500

Location : Central US

Subscription (change) : ASD Developer 1

Tags (change) : Click here to add tags

Subscription I... : cd5624ee-c42c-4f43-9c6d-4aea23072cf3

Status : Active

Last modified : 11/8/2019, 3:32 PM

Job Statistics
Last 24 Hours

0

Status	Count
Failed	0
Suspended	0
Completed	0
Running	0
Queued	0
Stopped	0

Task 2 - Import an Automation Runbook

A Runbook is the central concept in Azure Automation. Runbooks are PowerShell Workflow scripts that contain the steps you want to automate. When you execute a Runbook, it is queued for execution as a job. The Automation service picks up the job, runs it, and records the status. You do not have control over the Automation services, they are part of the Automation infrastructure and managed by Azure.

1.  Click on the **Runbooks** tile within the Automation Account blade.

The screenshot shows the Azure portal interface for an Automation Account named 'labAutomAcc'. The left sidebar contains a navigation menu with the following items:

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Below this is a section titled 'Configuration Management' containing:

- Inventory
- Change tracking
- State configuration (DSC)

Under 'Update management':

- Update management

Under 'Process Automation':

- Runbooks

The 'Runbooks' item is highlighted with a red rectangular border.

2. Click on the **Import a runbook** button.

The screenshot shows the Azure portal interface for an Automation Account named 'labAutomAcc'. On the left, there's a navigation sidebar with links like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. The main area is titled 'Runbooks' and contains a search bar ('Search (Ctrl+/)') and a list of three runbooks. The first runbook is 'AzureAutomationTutorial' (Published, Graphical Runbook, 11/8/2019, 3:09 PM). The second is 'AzureAutomationTutorialP...' (Published, Python 2 Runbook, 11/8/2019, 3:09 PM). The third is 'AzureAutomationTutorialS...' (Published, PowerShell Runbook, 11/8/2019, 3:09 PM). At the top right, there are buttons for 'Create a runbook', 'Import a runbook' (which is highlighted with a red box), 'Browse gallery', 'Learn more', and 'Refresh'.

Name	Authoring status	Runbook type	Last modified
AzureAutomationTutorial	✓ Published	Graphical Runbook	11/8/2019, 3:09 PM
AzureAutomationTutorialP...	✓ Published	Python 2 Runbook	11/8/2019, 3:09 PM
AzureAutomationTutorialS...	✓ Published	PowerShell Runbook	11/8/2019, 3:09 PM

3. Select the **Import** menu item in the Add Runbook blade then browse to the **C:\AzurelaaSWS\M8 - Azure Automation\Labs\AutomationUsingWebhooks\Assets** folder and find the **Shutdown-Start-VMs-By-Resource-Group.ps1** file. Leave the other settings within the import blade as they are and click the **Create** button.

 Import a runbook X

Runbook file * ⓘ
"Shutdown-Start-VMs-By-Resource-Gro..." 

Name * ⓘ
Shutdown-Start-VMs-By-Resource-Group

Runbook type * ⓘ
PowerShell Workflow ▼

Description

Create

4.  Review the commented code in the runbook. Once you are finished reviewing, select the **Publish** button on the toolbar.

If we were not using a Webhook, you could click on **Test pane** to test the runbook, but in our case, we have specifically coded the runbook to only allow a Webhook to be used. Select **Yes** at the prompt to publish the runbook.



```
1 workflow Shutdown-Start-VMs-By-Resource-Group
2 {
3     Param
4     (
5         # Using WebhookData allows us to pass in multiple parameters
6         [object]$WebhookData
7     )
8 }
```

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

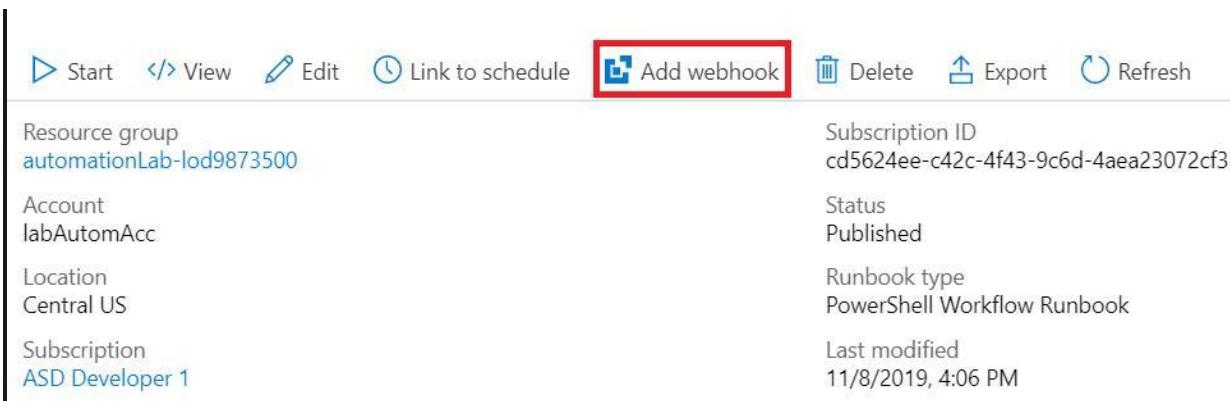
4 Hr 46 Min Remaining

Instructions Resources Help 100%

Task 3 - Add the Webhook

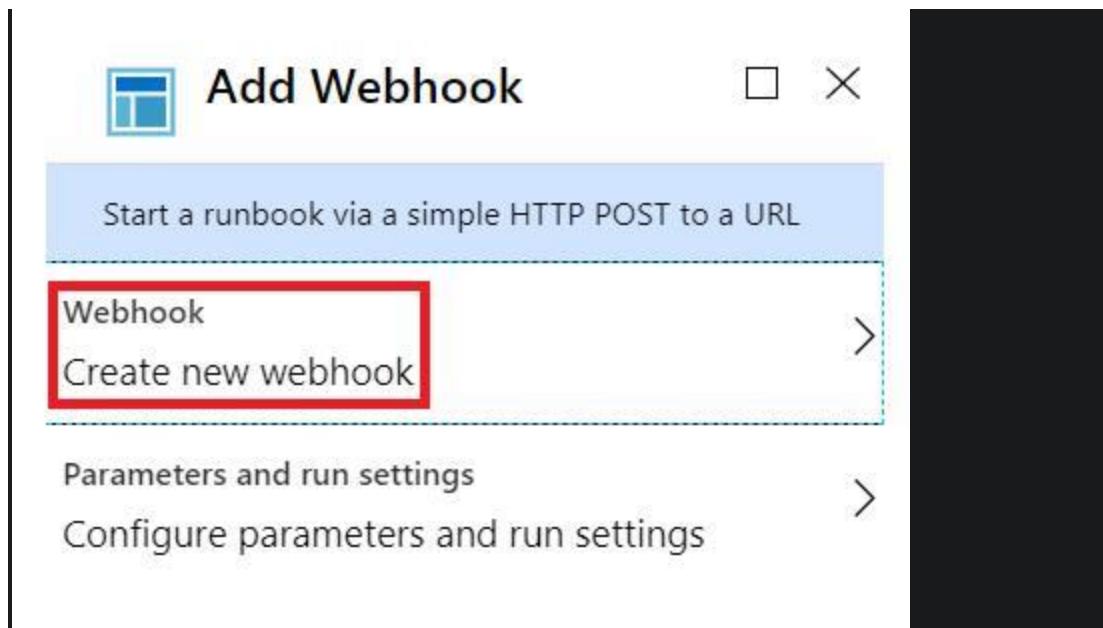
A webhook allows you to start a runbook in Azure Automation through a single HTTP POST request. This allows external services such as Visual Studio Team Services, GitHub, or customer applications to start runbooks without implementing a full solution using the Azure Automation API.

1.  Within the runbook blade, select the **Add Webhook** icon.



Start	View	Edit	Link to schedule	 Add webhook	Delete	Export	Refresh
Resource group automationLab-lod9873500				Subscription ID cd5624ee-c42c-4f43-9c6d-4aea23072cf3			
Account labAutomAcc				Status Published			
Location Central US				Runbook type PowerShell Workflow Runbook			
Subscription ASD Developer 1				Last modified 11/8/2019, 4:06 PM			

2.  Click the **Create new Webhook** button on the Add Webhook blade.



3. Type in a name for your webhook e.g. **start-stop-vms**, an expiration date and copy the URL to the clipboard, then paste it into the **Webhook URL** text box below. Click the **OK** button.

If you do not copy the Webhook URL before closing the blade, you will not be able to retrieve the URL again and will have to create a new webhook!

Create a new webhook

For security, after creating a webhook its URL can't be viewed. Make sure to copy it before pressing "OK", and to store it securely. [Learn more](#)

Name * ✓

Enabled * Yes No

Expires * 4:10:52 PM

URL ⓘ 

OK

Webhook URL

4. Click on the **Configure parameters and run settings** tile, then click the **OK** button.

For our purpose, we do not need to put in any data into the WEBHOOKDATA field, this will be passed in via PowerShell.

The screenshot shows the 'Add Webhook' blade in the Azure portal. The left pane lists the webhook details: 'Start a runbook via a simple HTTP POST to a URL', 'Webhook' named 'start-stop-vms', and 'Parameters and run settings'. The right pane shows the 'Parameters' section for the 'start-stop-vms' webhook, which includes a 'WEBHOOKDATA' parameter set to 'No value' (with a note 'Optional, Object') and 'Run Settings' and 'Run on Azure' options.

5. Click the **Create** button in the Add Webhook blade.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 46 Min Remaining

Instructions Resources Help 100%

Task 4 - Call the Webhook from PowerShell

There are multiple ways to call a webhook. Any language or API that can implement a HTTP POST call, can call a webhook. For the purposes of this lab, the client application will be a PowerShell script.

1. Open PowerShell as an Administrator.
2. Click **File|Open** and navigate to **C:\AzureelaaSWS\M8 - Azure Automation\AutomationUsingWebhooks\Assets** and open the **Client.ps1** file.
3. Replace the **[YOUR-PRIVATE-URL]** placeholder with the URL **<WebhookURL>** that you copied in the previous task. Make sure that you remove the [] brackets.
4. Replace the **[RESOURCE-GROUP-WITH-VM]** placeholder with the name of the resource group that contains the virtual machine to be shutdown, in your case resource group **automationLab-1d18918877**.

The \$headers variable contains *From* and *Date* fields, but these fields are not used in this script so you can leave these values as they are.

5. Save the changes.
6. Your final edited script should look similar to this:

```
Windows_PowerShell
$uri = "https://s25events.azure-
automation.net/webhooks?token=0cQok8psTj%2bu3EDVUpSjCKf%2bdZXXXXXXXXXXXX
XXXXQQHw%3d"
$headers = @{"From"="user@contoso.com";"Date"="02/23/2016 15:47:00"}

$myvars = @( 
    @{AzureResourceGroup="automationLab-lod9873500";Shutdown="true"
}
)

$body = ConvertTo-Json -InputObject $myvars

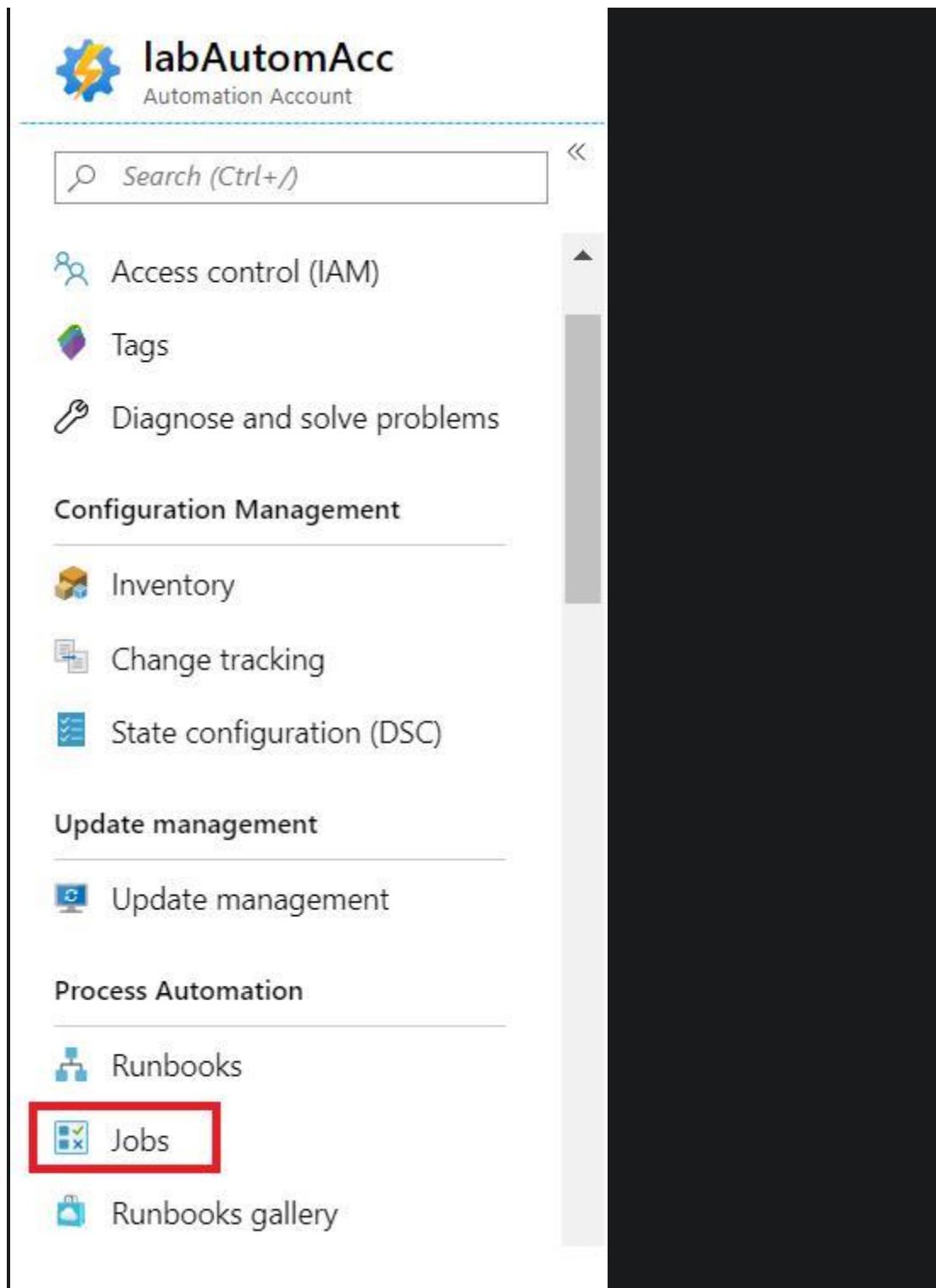
$response = Invoke-RestMethod -Method Post -Uri $uri -Headers $headers
-Body $body

Write-Output $response.Jobs
```

7. At the PowerShell command prompt, type **Connect-AzAccount** and press Enter.
8. Login to the Azure subscription using your Azure Trial Pass credentials.
9. Press **F5** to execute the script.
10. Your PowerShell output should look similar to the following on successful completion of the script.

```
PS C:\> C:\Users\StudentPC\Desktop\Webhook.ps1
cd2a686a-f85d-422a-b76a-8021f7d36d0a
```

11. Go back to the Azure portal and navigate to the **Automation Account**, then click on the **Jobs** tile.



12. The job status will either be Queued, Starting, Suspended, Running or Completed.

Runbook	Job created	Status	Ran on	Last status update
Shutdown-Start-VMs-By-Resource-Group	11/12/2019, 2:15:25 PM	Running	Azure	11/12/2019, 2:16:01 PM

13. Click on the job entry after it has completed. If it has been suspended or stopped, you can also click on it to see what has happened.
14. In the job status blade, click on the **All Logs** tab. This will open up an **All Logs** pane where you can click on each individual output that occurred while the script was executing.

 Shutdown-Start-VMs-By-Resource-Group 11/12/2019, 2:15 PM

► Resume Stop || Suspend  Refresh

Id : 7fb510da-ffb9-45fb-8f0f-c86fa42b0fe8	Created : 11/12/2019, 2:15:25 PM
Status : Completed	Last Update : 11/12/2019, 2:17:27 PM
Ran ... : Azure	Runbook : Shutdown-Start-VMs-By-Resource-Group
Ran ... : User	Source snapshot... : View source snapshot

Input Output Errors Warnings **All Logs** Exception

Errors Warnings
0 ! 0 !

Type : Any

Search logs...

Time	Type	Details
11/12/2019, 2:16:01 PM	Output	Logging in to Azure...
11/12/2019, 2:16:06 PM	Output	
11/12/2019, 2:16:06 PM	Output	Stopping VMs in 'automationLab-lod9873500' resource group
11/12/2019, 2:16:06 PM	Output	ARM VMs:
11/12/2019, 2:16:07 PM	Output	Stopping 'VM1' ...
11/12/2019, 2:17:24 PM	Output	
11/12/2019, 2:17:24 PM	Output	ASM VMs:

Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 46 Min Remaining

Instructions Resources Help 100%

Module 8.2 - Microsoft Azure Automation Desired State Configuration (DSC)

Introduction

In this lab, you will use Azure Automation Desired State Configuration (DSC) to configure an existing VM with IIS and its components.

You'll learn:

- How to configure and compile a DSC configuration in Azure Automation
- How to deploy the DSC configuration to a VM (node)
- How to confirm the node configuration

Prerequisites

The following are required to complete this hands-on lab:

- One or more virtual machines running in this subscription that can be shutdown (a virtual machine has been deployed to the **automationLab-lodXXXXXX** e.g. **automationLab-lod9873500** resource group in advance)
- Microsoft Azure subscription

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 45 Min Remaining

Instructions Resources Help 100%

Task 1 - Prepare the lab environment

During this lab, we will be using the Automation Account that was created during the previous exercise. We will also be using the virtual machine that was pre-created during the provisioning of your subscription. If you have deleted the Automation Account and/or the virtual machine from the

previous exercise, they will need to be created again. It is important that these resources exist prior to working with this lab.

1. If not already logged into the Azure portal, login using your Azure Trial Pass credentials.
2. Navigate to the **automationLab-1odXXXXXX** e.g. **automationLab-1od9873500** resource group and click on the virtual machine resource (**VM1**)

Showing 1 to 11 of 11 records. <input type="checkbox"/> Show hidden types <small>①</small>	
<input type="checkbox"/> Name ↑↓	Type ↑↓
<input type="checkbox"/>  autoVm1NetworkSecurityGroup	Network security group
<input type="checkbox"/>  autovm1pip2131270906	Public IP address
<input type="checkbox"/>  AzureAutomationTutorial (labAutomAcc/AzureAutomationTuto...)	Runbook
<input type="checkbox"/>  AzureAutomationTutorialPython2 (labAutomAcc/AzureAutoma...)	Runbook
<input type="checkbox"/>  AzureAutomationTutorialScript (labAutomAcc/AzureAutomatio...)	Runbook
<input type="checkbox"/>  labAutomAcc	Automation Account
<input type="checkbox"/>  Shutdown-Start-VMs-By-Resource-Group (labAutomAcc/Shutd...)	Runbook
<input type="checkbox"/>  VM1	Virtual machine
<input type="checkbox"/>  VM1_OsDisk_1_3644195408ea4dde993079f4d3e4958d	Disk

3. Notice that the virtual machine is in a **Stopped (deallocated)** status. This is because we used a Runbook that was triggered by a Webhook in the previous exercise to shut it down. Click the **Start** tile in the top menu bar to start the virtual machine.

Resource group (change)
automationLab-lod9873500

Status
Stopped (deallocated)

Location
Central US

Subscription (change)
ASD Developer 1

Subscription ID
cd5624ee-c42c-4f43-9c6d-4aea23072cf3

Computer name
(start VM to view)

Operating system
Windows

Size
Standard D2 v2 (2 vcpus, 7 GiB memory)

Ephemeral OS disk
N/A

Public IP address
40.122.161.41

Private IP address
10.5.0.4

Virtual network/subnet
AutomvNET1/frontEnd

DNS name
Configure

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 45 Min Remaining

Instructions Resources Help 100%

Task 2 - Review the DSC script

In this task, you will review a pre-created script that will be used to apply a configuration to your virtual machine.

1. Open PowerShell as an administrator.
2. Navigate to **C:\AzurelaaSWS\M8 - Azure Automation\Labs\AutomationDSC\DSCWebRoleConfig.ps1** and click Open.

At the top of the file you will see:
`Configuration DSCWebRoleConfig {`

DSCWebRoleConfig is the "name" of the configuration and you will use this name later to import the configuration into Azure Automation DSC.

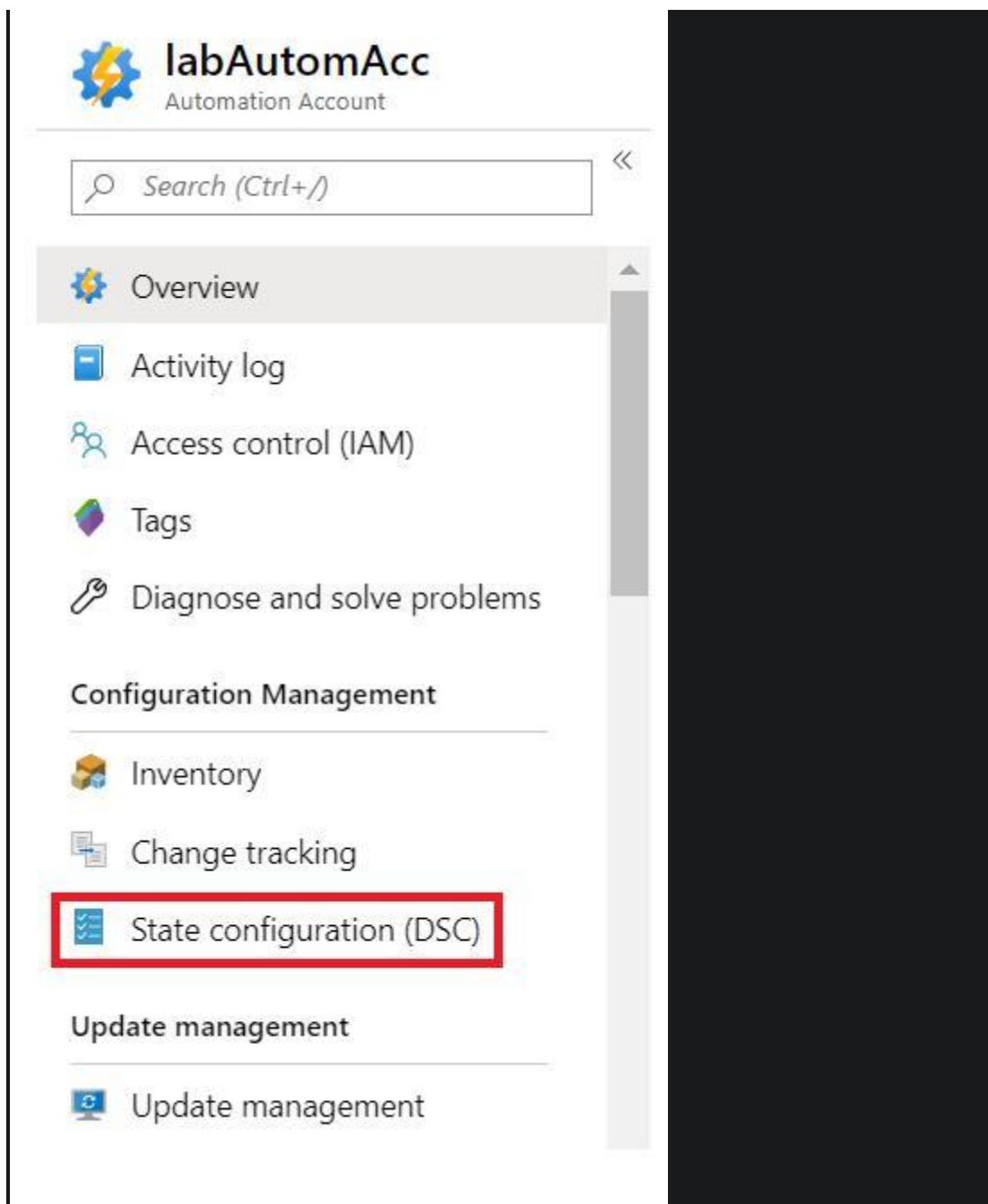
Next, you will see the features that will be applied to your VM (or node in DSC terms). The Name parameters are standard Windows features that can be installed. The Ensure parameter setting of Present means that DSC should install the feature.

```
$features = @(
    @{Name = "Web-Server"; Ensure = "Present"},
    @{Name = "Web-WebServer"; Ensure = "Present"},
    @{Name = "Web-Common-Http"; Ensure = "Present"},
    @{Name = "Web-Default-Doc"; Ensure = "Present"}
```

Next, you will see the node name, localhost. This name is also important when we import the configuration in to Automation DSC. This script has a for loop that will loop through and install all the features on the node

```
node localhost {
    foreach ($feature in $features){
        WindowsFeature ($feature.Name) {
            Name = $feature.Name
            Ensure = $feature.Ensure
        }
    }
}
```

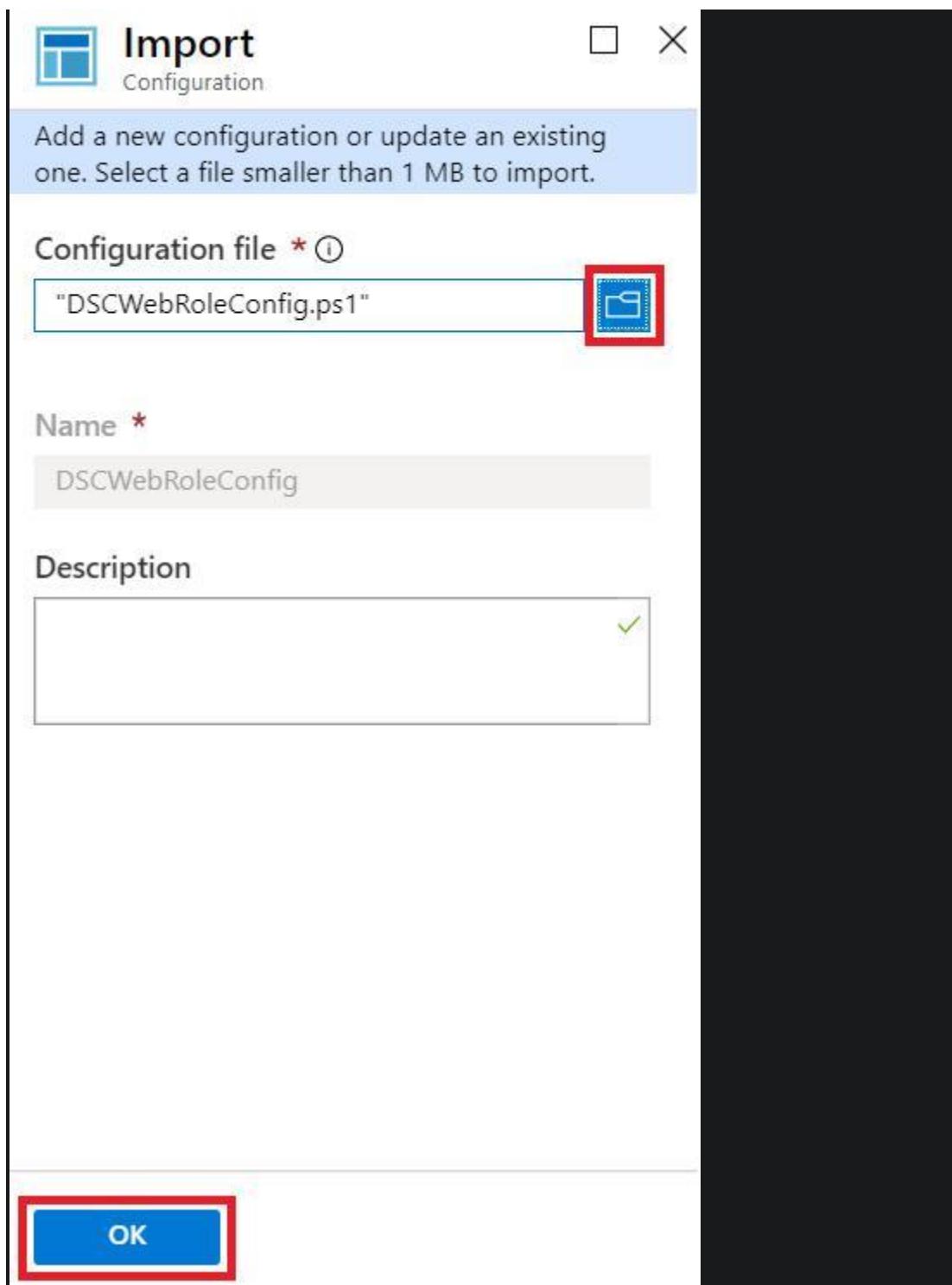
3. Navigate to your Automation Account in the Azure portal and from within it, click the **State configuration (DSC)** tile.



4. Click on the **Configurations** tab, then click the **Add** tile.

The screenshot shows the Azure Automation DSC configuration management interface. At the top, there are several buttons: '+ Add' (highlighted with a red box), 'Compose configuration', 'Refresh', and 'Reset filters'. Below these are tabs: 'Nodes' (blue), 'Configurations' (highlighted with a red box), 'Compiled configurations', and 'Gallery'. A search bar labeled 'Search configurations...' is present. The main area displays a table with columns: 'Configuration' (with a help icon), 'Compiled Configuration Count', and 'Last Modified'. A single row shows 'No data'. The entire interface has a light blue background.

5. Click the Browse button and navigate to **C:\Azure\laaSWS\M8 - Azure Automation\Labs\AutomationDSC** and select the **DSCWebRoleConfig.ps1** file. Click the **OK** button to import the script into Azure Automation DSC.



6. Refresh the State configuration (DSC) blade and notice that the name **DSCWebRoleConfig** is the name of the configuration.

Nodes Configurations Compiled configurations Gallery

Configuration	Compiled Configuration Count	Last Modified
DSCWebRoleConfig	0	11/12/2019, 3:31 PM

7. Click on the **DSCWebRoleConfig** DSC configuration and a new blade will appear. In this blade, select the **Compile** button. Click **Yes** to the informational message. A configuration has to be compiled (into a MOF file) in order for you to apply the configuration to a node.

DSCWebRoleConfig

Configuration

Compile Export Delete

Resource group...	: automationLab-10d9873500	Account	: labAutomAcc
Location	: Central US	Subscription...	: ASD Developer 1
Subscription ID	: cd5624ee-c42c-4f43-9c6d-4aea23072cf3	Status	: Published
Last published	: 11/12/2019, 3:31 PM	Configuration source	: View configuration source

Compilation jobs Node configurations

Created	Status	Last updated
---------	--------	--------------

The compile request will be queued, started and then completed.

8. Once the compile job has successfully completed, go back to the main **State configuration (DSC)** blade and select the **Compiled configurations** tab, notice that there is a **Node Configuration** item.

This appears after you do a compile of your DSC Configuration. If you do not have a DSC Node Configuration item present, you will not be able to apply a configuration to a node. (You may need to refresh the browser at this point).

The screenshot shows the 'Compiled configurations' tab selected in the top navigation bar. Below it, a search bar labeled 'Search node configurations...' is present. A table lists a single configuration entry:

Node Configuration	Configuration	Node Count	Created	Last Modified
DSCWebRoleConfig.localhost	DSCWebRoleConfig	0	11/12/2019, 3:40 PM	11/12/2019, 3:40 PM

9. Click on the **Nodes** tab. This is where you will configure which VM (node) to apply this configuration to. Click the **Add** button.

The screenshot shows the 'Nodes' tab selected in the top navigation bar. It features a summary section with a large circle showing '0' nodes and status counts for Failed, Pending, Not compliant, In progress, Unresponsive, and Compliant. Below this are search and filter fields for 'Nodes', 'Status', and 'Node configuration'. A table at the bottom shows no data.

Node	Status	Node configuration	Last seen
No data			

10. Clicking the **Add** button will bring up a list of Virtual Machines. Click on the virtual machine that you want to apply the node configuration to (in your case VM1 that you started at the beginning of this lab) and then click + **Connect**. Note that the VM must be running to do this.

The screenshot shows the Azure portal's Virtual Machines blade. The left pane lists several virtual machines, and the right pane provides detailed information for the selected VM1. The 'VM1' row is highlighted with a red box.

Virtual Machines	Subscription	Resource group	Location
dbvm	ASD Developer 1	vmLab-lod9873500	Central US
DiagVM0	ASD Developer 1	storageLab-lod9873500	Central US
LBVMO	ASD Developer 1	armVSLab-lod9873500	Central US
LBVM1	ASD Developer 1	armVSLab-lod9873500	Central US
LBVMPSO	ASD Developer 1	armPSLab-lod9873500	Central US
LBVMPS1	ASD Developer 1	armPSLab-lod9873500	Central US
VM1	ASD Developer 1	automationLab-lod9873500	Central US
VM2	ASD Developer 1	backupLab-lod9873500	Central US
VM3	ASD Developer 1	backupLab-lod9873500	Central US

VM1
Virtual machine

+ Connect Refresh Learn more

Not connected

Power State
VM running

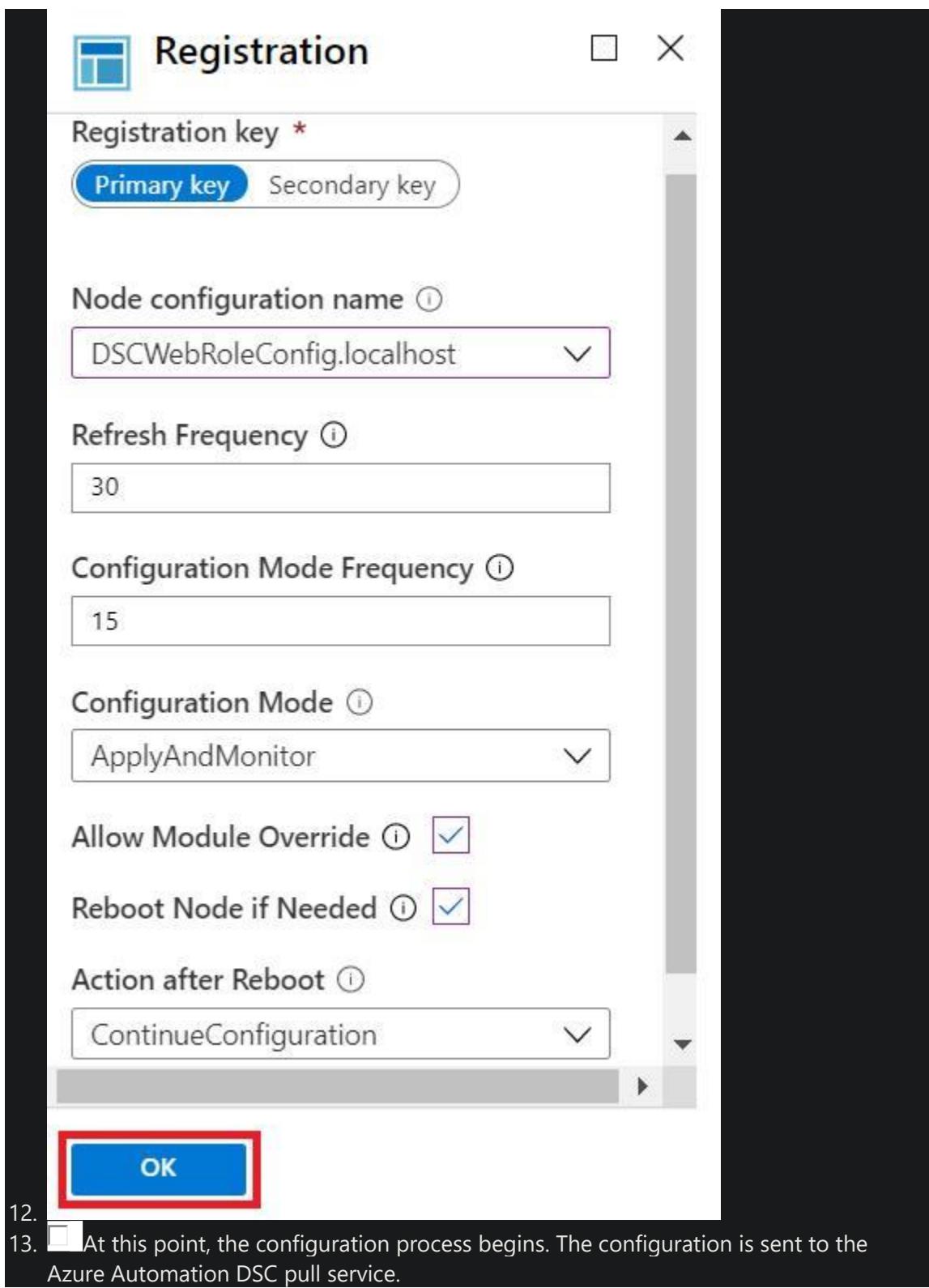
OS
Windows

Status
Not connected

11. You are now presented with the Registration blade. The information entered here is very important. Click **OK** once you have completed your configuration.

Setting	Value
RegistrationKey	The automation account has a primary and secondary key for security. Leave this as the default setting (Primary key)
Node Configuration Name	Select DSCWebRoleConfig.localhost from the dropdown menu
Refresh Frequency	Represents the frequency (in minutes) at which the PS DSC Local Configuration Manager contacts the Azure Automation DSC pull server to download the latest node configuration. Minimum 30 minutes
Configuration Mode Frequency	Represents the frequency (in minutes) at which the background application of DSC attempts to implement the current node configuration on the target node. Leave this set to 15 minutes.
Configuration Mode	This is how you would like DSC to apply the configuration Apply and monitor – Apply the configuration initially and monitor for changes after. Apply Only – Apply the configuration initially and no more. Apply and Auto Correct – Apply configuration and

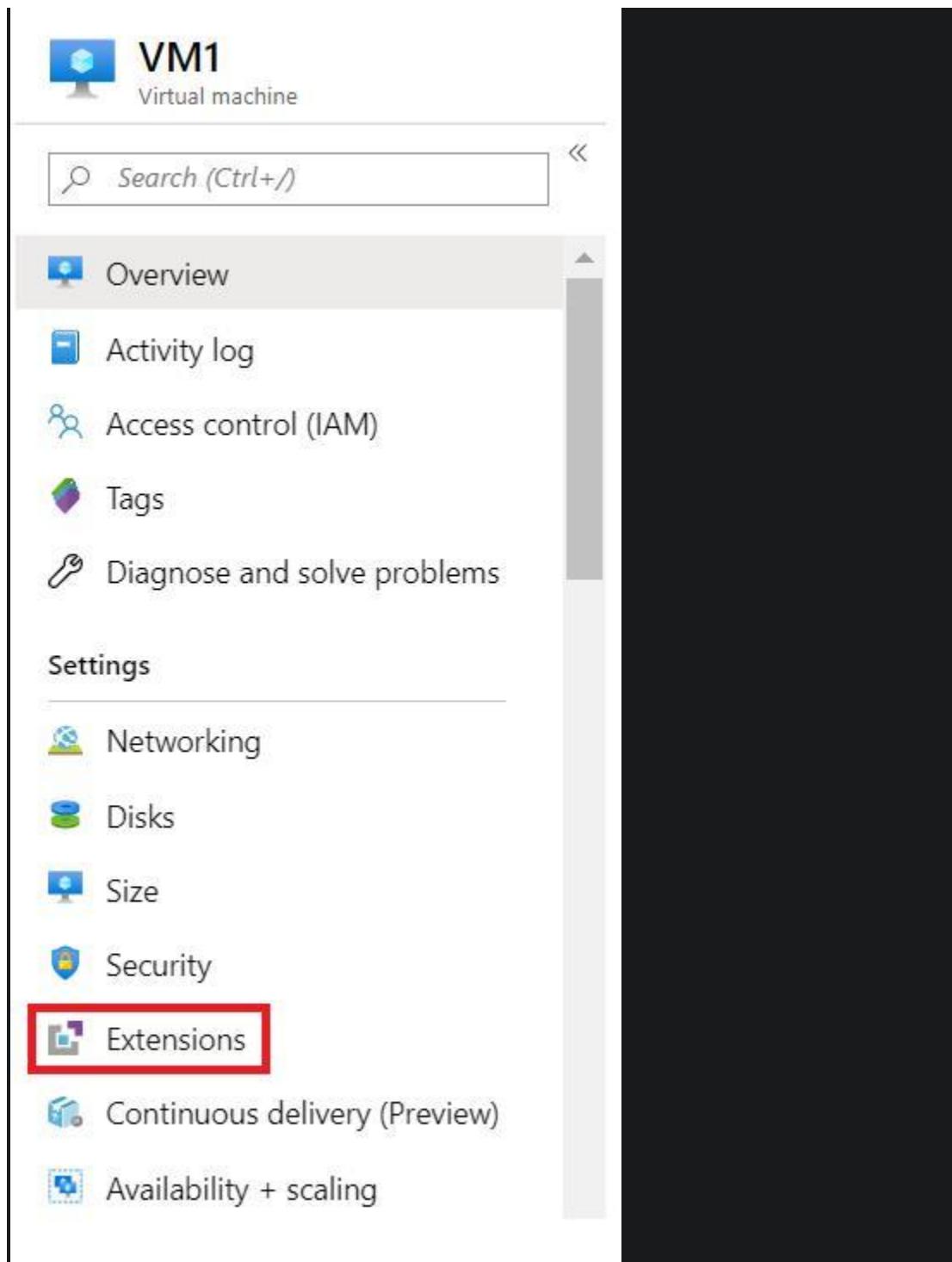
Setting	Value
	continue to apply should the VM sway from the desired state. Leave this as ApplyAndMonitor.
Allow Module Override	Controls whether new configurations downloaded from the Azure Automation DSC pull server are allowed to overwrite the old modules already on the target node. Check this box
Reboot Node if Needed	If anything applied to the machine requires a machine reboot, allow it. Check this box
Action after Reboot	You can choose to continue with any missing configuration or stop any further configuration



It can take approximately **10 minutes** for the initial application of DSC to the node.

Task 3 - Confirm node configuration

1. From within the Azure portal, navigate to the resource group that contains the VM that you applied the DSC configuration to (**VM1** in the **automationLab-lodXXXXXX** e.g. **automationLab-lod9873500** resource group). Go to the VM blade and click the **Extensions** button.



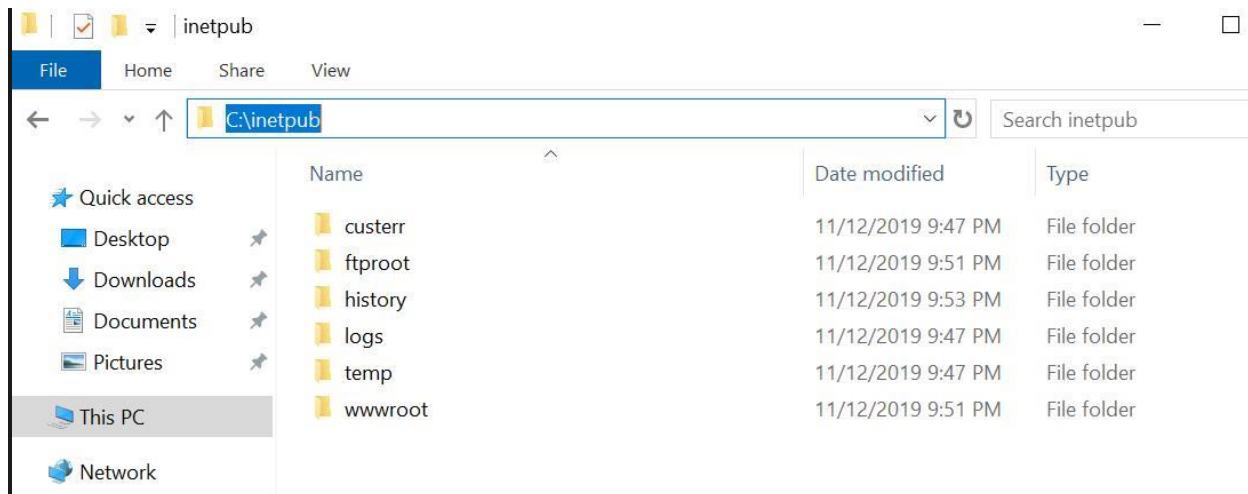
2. Confirm that the **Microsoft.Powershell.DSC** extension has a status of "Provisioning succeeded". This takes around 5 - 10 minutes to complete.

Add						
Search to filter items...						
Name	Type	Version	Status			
BGInfo	Microsoft.Compute.BGInfo	2.*	Provisioning succeeded	...		
Microsoft.Powershell.DSC	Microsoft.Powershell.DSC	2.*	Provisioning succeeded	...		
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitoring.Microso...	1.*	Provisioning succeeded	...		

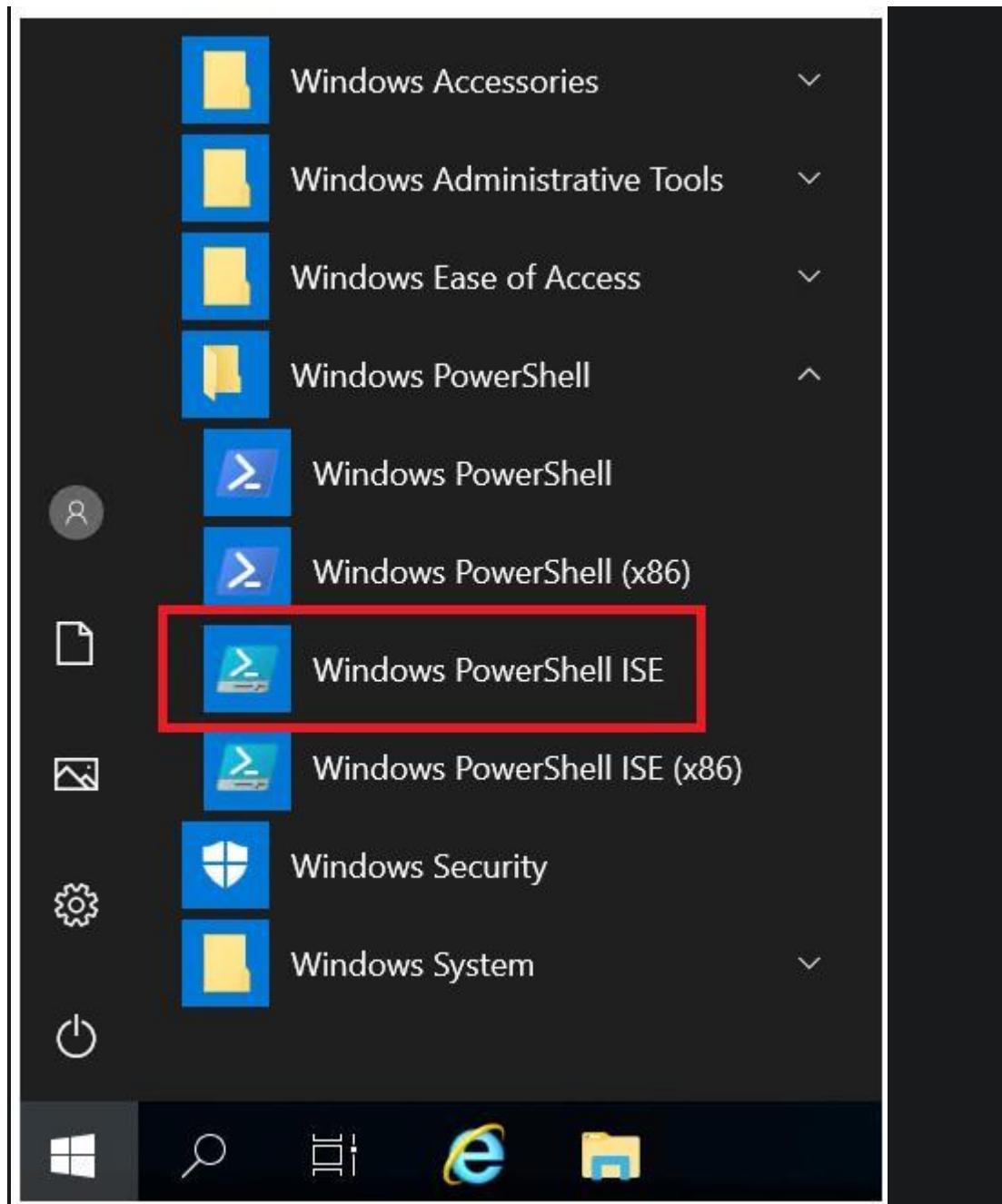
3. Go back to the VM blade and click the **Connect** toolbar icon at the top of the blade, download the RDP file and log in to the server using the credentials **AdminUser** and **P@55word1234**.

Resource group (change)	Computer name
automationLab-lod9873500	VM1
Status	Operating system
Running	Windows (Windows Server 2019 Datacenter)
Location	Size
Central US	Standard D2 v2 (2 vcpus, 7 GiB memory)
Subscription (change)	Ephemeral OS disk
ASD Developer 1	N/A

4. Once you have RDP'd in to the VM, verify that the **C:\inetpub** folder exists. This means that IIS has been installed. If you do not see **C:\inetpub**, this means that the configuration has not taken place yet.



5. On the VM, open **PowerShell** by clicking on the **Start** button, then **Windows PowerShell** then **PowerShell**.



6. Once **PowerShell** is open, type **Test-DscConfiguration -Verbose** into the command window and press **Enter**. Your output should look similar to the below.

Should you receive path errors or an error that tells you that the DSC configuration is currently being applied, remember the minimum amount of time it will take to apply the

configuration is approximately **10 minutes**. Wait until the DSC configuration has finished applying and then run the command again.

```
PS C:\Users\AdminUser> Test-DscConfiguration -Verbose
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, ''methodName' = TestConfiguration,'className' = MSFT_DSCLocalConfigurationManager,'namespaceName' = root\Microsoft\Windows\DesiredStateConfiguration'.
VERBOSE: An LCM method call arrived from computer VM1 with user sid S-1-5-21-566815699-491834584-1416231068-500.
VERBOSE: [VM1]: LCM: [ Start Test ] [[WindowsFeature]Web-Server]
VERBOSE: [VM1]: LCM: [ Start Resource ] [[WindowsFeature]Web-Server]
VERBOSE: [VM1]: LCM: [ Start Test ] [[WindowsFeature]Web-Server]
VERBOSE: [VM1]: [[WindowsFeature]Web-Server] The operation 'Get-WindowsFeature' started: Web-Server
VERBOSE: [VM1]: [[WindowsFeature]Web-Server] The operation 'Get-WindowsFeature' succeeded: Web-Server
VERBOSE: [VM1]: LCM: [ End Test ] [[WindowsFeature]Web-Server] True in 0.5940 seconds.
VERBOSE: [VM1]: LCM: [ End Resource ] [[WindowsFeature]Web-Server]
VERBOSE: [VM1]: LCM: [ Start Resource ] [[WindowsFeature]Web-WebServer]
VERBOSE: [VM1]: LCM: [ Start Test ] [[WindowsFeature]Web-WebServer]
VERBOSE: [VM1]: [[WindowsFeature]Web-WebServer] The operation 'Get-WindowsFeature' started: Web-WebServer
VERBOSE: [VM1]: [[WindowsFeature]Web-WebServer] The operation 'Get-WindowsFeature' succeeded: Web-WebServer
VERBOSE: [VM1]: LCM: [ End Test ] [[WindowsFeature]Web-WebServer] True in 0.3430 seconds.
VERBOSE: [VM1]: LCM: [ End Resource ] [[WindowsFeature]Web-WebServer]
VERBOSE: [VM1]: LCM: [ Start Resource ] [[WindowsFeature]Web-Common-Http]
VERBOSE: [VM1]: LCM: [ Start Test ] [[WindowsFeature]Web-Common-Http]
VERBOSE: [VM1]: [[WindowsFeature]Web-Common-Http] The operation 'Get-WindowsFeature' started: Web-Common-Http
VERBOSE: [VM1]: [[WindowsFeature]Web-Common-Http] The operation 'Get-WindowsFeature' succeeded: Web-Common-Http
VERBOSE: [VM1]: LCM: [ End Test ] [[WindowsFeature]Web-Common-Http] True in 0.3600 seconds.
VERBOSE: [VM1]: LCM: [ End Resource ] [[WindowsFeature]Web-Common-Http]
VERBOSE: [VM1]: LCM: [ Start Resource ] [[WindowsFeature]Web-Default-Doc]
```

Congratulations!

You have successfully completed this module. Click **Next** to advance to the next module.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 44 Min Remaining

Instructions Resources Help 100%

Module 9 - Introduction to Microsoft Recovery Services

Introduction

In this lab, you will create an Azure Recovery Services vault and configure a full server backup for an Azure IaaS VM. You will also configure a folder level backup and restore of an Azure IaaS VM. The Azure Recovery Services vault will be used to store backup information that will include configuration and backup data.

You'll learn:

- How to create an Azure Recovery Services vault

- How to configure an Azure VM for a full server backup using the Azure portal
- How to backup and restore a folder using the Microsoft Azure Recovery Services Agent (MARS Agent)

Prerequisites

The following are required to complete this hands-on lab:

- Microsoft Azure subscription
- Two virtual machines running in this subscription (you will be creating two virtual machines that will be used in this lab in the next task)

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 44 Min Remaining

Instructions Resources Help 100%

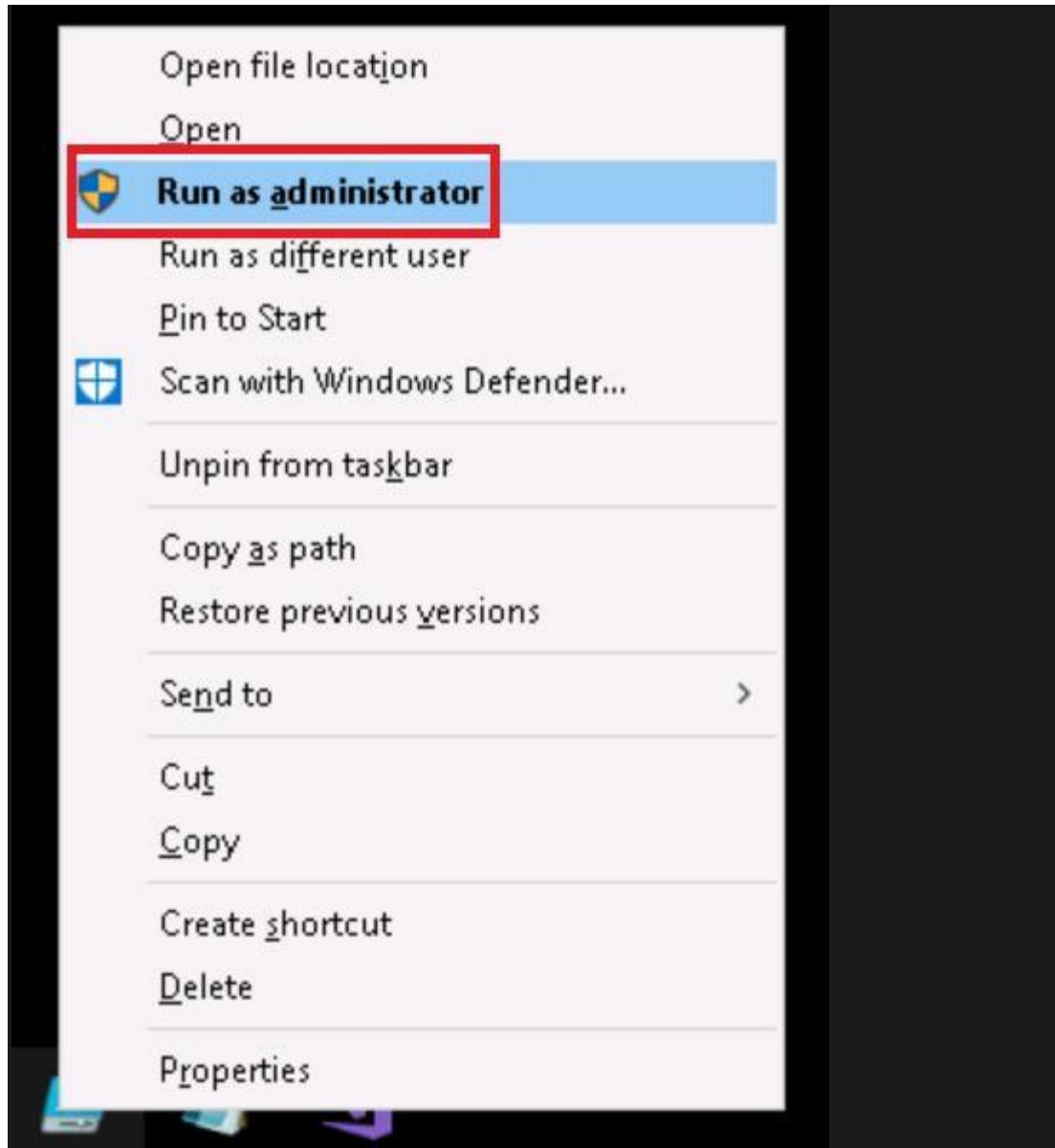
Exercise 1 - Azure Recovery Services (ARM)

Task 1: - Creating Virtual Machines and a Recovery Services vault

1. Login to the **Win10 Lab VM** hosted lab machine in the left hand pane with a Username of **Student** and a Password of **pass@word1** Once logged in, if you do not already have a US keyboard layout select your keyboard layout from the task bar.



2. Shift and right-click the PowerShell shortcut on the taskbar and select **Run as administrator**



3. Click Yes to the User Account Control pop-up.
4. In the PowerShell command prompt window, type in **Connect-AzAccount** and press **Enter**.
5. Enter the email address that was used to redeem your **Azure Trial Pass** into the Sign in dialog box and click **Next** or press **Enter**.
6. Enter your password and click **Sign in** or press **Enter**. This will log you in to your Azure Trial Pass subscription.

```
PS C:\> Connect-AzAccount
```

Account	SubscriptionName	TenantId	Environment
iaaswslab@hotmail.com	Azure Pass - Sponsorship	f30ae15e-afec-42d9-aefc-3709be909663	AzureCloud

7. Copy the below PowerShell commands to your PowerShell script pane.

Click the **Type Text** icon to automatically type the associated text to the active window in your hosted lab machine on the left.

Windows_PowerShell

```
Set-Item Env:\SuppressAzurePowerShellBreakingChangeWarnings "true"
$resourceGroup2 = "backupLab-lod18918877"
$location2 = "centralus"
$vmName2 = "VM2"
$userName2='AdminUser'
$password2='P@55word1234' | ConvertTo-SecureString -Force -AsPlainText
$cred2=New-Object PSCredential($UserName2,$Password2)
$subnetConfig2 = New-AzVirtualNetworkSubnetConfig -Name frontEnd -
AddressPrefix 10.6.0.0/28
$vnet2 = New-AzVirtualNetwork -ResourceGroupName $resourceGroup2 -
Location $location2 `-
-Name BackupvNET2 -AddressPrefix 10.6.0.0/24 -Subnet $subnetConfig2 -`-
Force
$pip2 = New-AzPublicIpAddress -ResourceGroupName $resourceGroup2 -`-
Location $location2 `-
-Name "backupvm2pip$(Get-Random)" -AllocationMethod Static -`-
IdleTimeoutInMinutes 4
$nsgRuleRDP2 = New-AzNetworkSecurityRuleConfig -Name
myNetworkSecurityGroupRuleRDP -Protocol Tcp `-
-Direction Inbound -Priority 1000 -SourceAddressPrefix * `-
SourcePortRange * -DestinationAddressPrefix * `-
-DestinationPortRange 3389 -Access Allow
$nsg2 = New-AzNetworkSecurityGroup -ResourceGroupName $resourceGroup2 -`-
Location $location2 `-
-Name backupVm2NetworkSecurityGroup -SecurityRules $nsgRuleRDP2 -Force
$nic2 = New-AzNetworkInterface -Name BackupVM2Nic -ResourceGroupName
$resourceGroup2 -Location $location2 `-
-SubnetId $vnet2.Subnets[0].Id -PublicIpAddressId $pip2.Id -`-
NetworkSecurityGroupId $nsg2.Id -Force
$vmConfig2 = New-AzVMConfig -VMName $vmName2 -VMSize Standard_D2_v2 | `-
Set-AzVMOperatingSystem -Windows -ComputerName $vmName2 -Credential
$cred2 | `-
Set-AzVMSourceImage -PublisherName MicrosoftWindowsServer -Offer
WindowsServer -Skus 2019-Datacenter -Version latest | `-
Add-AzVMNetworkInterface -Id $nic2.Id
New-AzVM -ResourceGroupName $resourceGroup2 -Location $location2 -VM
$vmConfig2


$resourceGroup3 = "backupLab-lod18918877"
$location3 = "centralus"
$vmName3 = "VM3"
$userName3='AdminUser'
$password3='P@55word1234' | ConvertTo-SecureString -Force -AsPlainText
$cred3=New-Object PSCredential($UserName3,$Password3)
$subnetConfig3 = New-AzVirtualNetworkSubnetConfig -Name frontEnd -`-
AddressPrefix 10.7.0.0/28
$vnet3 = New-AzVirtualNetwork -ResourceGroupName $resourceGroup3 -`-
Location $location3 `-
```

```

>Name BackupvNET3 -AddressPrefix 10.7.0.0/24 -Subnet $subnetConfig3 -
Force
$pip3 = New-AzPublicIpAddress -ResourceGroupName $resourceGroup3 -
Location $location3 `-
-Name "backupvm3pip$(Get-Random)" -AllocationMethod Static -
IdleTimeoutInMinutes 4
$nsgRuleRDP3 = New-AzNetworkSecurityRuleConfig -Name
myNetworkSecurityGroupRuleRDP -Protocol Tcp `-
-Direction Inbound -Priority 1000 -SourceAddressPrefix * `-
SourcePortRange * -DestinationAddressPrefix * `-
-DestinationPortRange 3389 -Access Allow
$nsg3 = New-AzNetworkSecurityGroup -ResourceGroupName $resourceGroup3 -
Location $location3 `-
-Name backupVm3NetworkSecurityGroup -SecurityRules $nsgRuleRDP3 -Force
$nic3 = New-AzNetworkInterface -Name BackupVM3Nic -ResourceGroupName
$resourceGroup3 -Location $location3 `-
-SubnetId $vnet3.Subnets[0].Id -PublicIpAddressId $pip3.Id -
NetworkSecurityGroupId $nsg3.Id -Force
$vmConfig3 = New-AzVMConfig -VMName $vmName3 -VMSize Standard_D2_v2 | `-
Set-AzVMOperatingSystem -Windows -ComputerName $vmName3 -Credential
$cred3 | `-
Set-AzVMSourceImage -PublisherName MicrosoftWindowsServer -Offer
WindowsServer -Skus 2019-Datacenter -Version latest | `-
Add-AzVMNetworkInterface -Id $nic3.Id
New-AzVM -ResourceGroupName $resourceGroup3 -Location $location3 -VM
$vmConfig3

```

8. Click the **Run** button or press **F5**. This will create the virtual machines that will be used in this lab.

The screenshot shows the PowerShell ISE interface with a script editor window titled "Untitled1.ps1*". The script contains 17 numbered lines of PowerShell code for creating a second virtual machine. The code includes variables for resource groups, locations, VM names, user credentials, network configurations, and security rules. A red box highlights the green play button icon in the toolbar, indicating where to click to run the script.

```

1 Set-Item Env:\SuppressAzurePowerShellBreakingChangeWarnings "true"
2 $resourceGroup2 = "backupLab-10d9873500"
3 $location2 = "centralus"
4 $vmName2 = "VM2"
5 $userName2='AdminUser'
6 $password2='P@ssword1234' | ConvertTo-SecureString -Force -AsPlainText
7 $cred2=New-Object PSCredential($userName2,$password2)
8 $subnetConfig2 = New-AzVirtualNetworkSubnetConfig -Name frontEnd -AddressPrefix 10.6.0.0/28
9 $vnet2 = New-AzVirtualNetwork -ResourceGroupName $resourceGroup2 -Location $location2 `-
-Name BackupvNET2 -AddressPrefix 10.6.0.0/24 -Subnet $subnetConfig2 -Force
10 $pip2 = New-AzPublicIpAddress -ResourceGroupName $resourceGroup2 -Location $location2 `-
-Name "backupvm2pip$(Get-Random)" -AllocationMethod Static -IdleTimeoutInMinutes 4
11 $nsgRuleRDP2 = New-AzNetworkSecurityRuleConfig -Name myNetworkSecurityGroupRuleRDP -Protocol
12 -Direction Inbound -Priority 1000 -SourceAddressPrefix * -SourcePortRange * -DestinationAddress
13 -DestinationPortRange 3389 -Access Allow
14 $nsg2 = New-AzNetworkSecurityGroup -ResourceGroupName $resourceGroup2 -Location $location2 `-
-Name backupVm2NetworkSecurityGroup -SecurityRules $nsgRuleRDP2 -Force
15
16
17

```

9. The virtual machines have been successfully created.

RequestId	IsSuccess	Status	StatusCode	ReasonPhrase
	True		OK	OK
	True		OK	OK

10. Log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
11. Click + Create a resource, type in **Backup and Site Recovery** in the Search the Marketplace search box, then press Enter. This will list the Backup and Site Recovery resource, click **Create**.

Backup and Site Recovery

Microsoft

Backup and Site Recovery Microsoft

Create

A disaster recovery and data protection strategy keeps your business running when unexpected events occur.

The Backup service is Microsoft's born in the cloud backup solution to backup data that's located on-premises and in Azure. It replaces your existing on-premises or offsite backup solution with a reliable, secure and cost competitive cloud backup solution. It also provides the flexibility of protecting your assets running in the cloud. You can backup Windows Servers, Windows Clients, Hyper-V VMs, Microsoft workloads, Azure Virtual Machines (Windows and Linux) with its in-built resilience and high SLAs. [Learn more](#).

The Site Recovery service ensures your servers, virtual machines, and apps are resilient by replicating them so that when disasters and outages occur you can easily fail over to your replicated environment and continue working. When services are resumed you simply failback to your primary location with uninterrupted access. Site Recovery helps protect a wide range of Microsoft and third-party workloads. [Learn more](#).

Useful Links

[Backup Pricing details](#)

[Site Recovery Pricing details](#)

12. When setting up the Backup and Site Recovery vault, you will need to configure:
- Select your Azure subscription (Accept the default)
 - Select the **backupLab-1odXXXXXX** e.g. **backupLab-1od9873500** resource group if not already selected
 - The name of the vault e.g. **labVault**
 - Select the Location to put the vault in, this should be **Central US**
 - Click **Review + create**.

Create Recovery Services vault

Preview

Basics * Tags Review + create

Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription * ⓘ

ASD Developer 1

Resource group * ⓘ

backupLab-lod9873500

[Create new](#)

Instance Details

Vault name * ⓘ

labVault

Region * ⓘ

Central US

[Review + create](#)

[Next: Tags](#)

13. Once the configuration has been successfully validated, click **Create**.

Create Recovery Services vault

Preview

Basics * Tags Review + create

Summary

Basics

Subscription	ASD Developer 1
Resource group	backupLab-lod9873500
Vault name	labVault
Region	Central US



After creating vault, it is highly recommended that you review default vault properties before protecting items. [Learn more](#).

Create

Previous: Tags

[Download a template for automation](#)

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 44 Min Remaining

Instructions Resources Help 100%

Task 2 - Configure an Azure VM Backup

1. From within the Azure portal, click the **Resource Groups** menu item in the left hand pane (which will open the Resource Groups blade), then select the **backupLab-lodXXXXXXX** e.g. **backupLab-lod9873500** resource group.

	Name ↑↓	Subscription ↑↓
<input type="checkbox"/>	armPolicyLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	armPSLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	armVSLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	automationLab-lod9873500	ASD Developer 1
<input checked="" type="checkbox"/>	backupLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	identityLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	managementLab-lod9873500	ASD Developer 1
<input type="checkbox"/>	netwLabCentralUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	netwLabEastUS-lod9873500	ASD Developer 1
<input type="checkbox"/>	storageLab-lod9873500	ASD Developer 1

2. Click the newly created **Backup and Site Recovery** vault

	Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/>	backupVmNetworkSecurityGroup	Network security group	Central US
<input type="checkbox"/>	BackupVMNic	Network interface	Central US
<input type="checkbox"/>	backupvmpip1109741097	Public IP address	Central US
<input type="checkbox"/>	BackupvNET	Virtual network	Central US
<input checked="" type="checkbox"/>	labVault	Recovery Services vault	Central US
<input type="checkbox"/>	VM2	Virtual machine	Central US
<input type="checkbox"/>	VM2_OsDisk_1_0852d3b9de7e45e7b765f459aa78a786	Disk	Central US

3. Click **Backup**.

The screenshot shows the Azure Recovery Services vault interface for a vault named 'labVault'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, and Export template. Under 'Getting started', the 'Backup' link is highlighted with a red box. The main content area has tabs for Overview, Backup, and Site Recovery, with 'Backup' selected. A 'What's new' section lists several updates. Below the news are two blue cloud icons with circular arrows, representing backup and replication.

4. Select **Azure** under the **Where is your workload running?** drop down menu then select **Virtual machine** under the **What do you want to backup?** drop down menu and click **Backup**.

The screenshot shows the 'labVault - Backup' configuration screen. The left sidebar is identical to the previous screenshot. The right side features two dropdown menus: 'Where is your workload running?' set to 'Azure' and 'What do you want to backup?' set to 'Virtual machine', both highlighted with red boxes. Below these is a section titled 'Step: Configure Backup' with a large blue 'Backup' button, also highlighted with a red box.

5. Leave the **Backup policy** setting as is (DefaultPolicy), then click the **Add** button and select **VM2** from the list of virtual machines and click **OK**. Then click the **Enable backup** button.

Configure Backup

labVault

Backup policy * ⓘ

DefaultPolicy

Create a new policy

Policy Details

Full Backup

Backup Frequency

Daily at 4:30 AM UTC

Instant Restore

Retain instant recovery snapshot(s) for 2 day(s)

Retention of daily backup point

Retain backup taken every day at 4:30 AM for 30 Day(s)

Virtual machines

Name

Resource Group

OS Disk only

No Virtual machines selected.

Add

i **OS Disk only backup** option allows you to backup Azure Virtual Machine with only OS disk and exclude all the data disks. You can use Selective Disk Backup feature through Powershell or CLI to include or exclude specific data disks. Know more about Selective Disk Backup feature, its limitation and pricing - [Learn more](#).

Enable backup

At this stage, the VM has been configured for backup. It has not been backed up yet. You can either wait until the configured backup schedule runs (daily at 04:30 AM UTC) or, you can manually initiate a backup.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

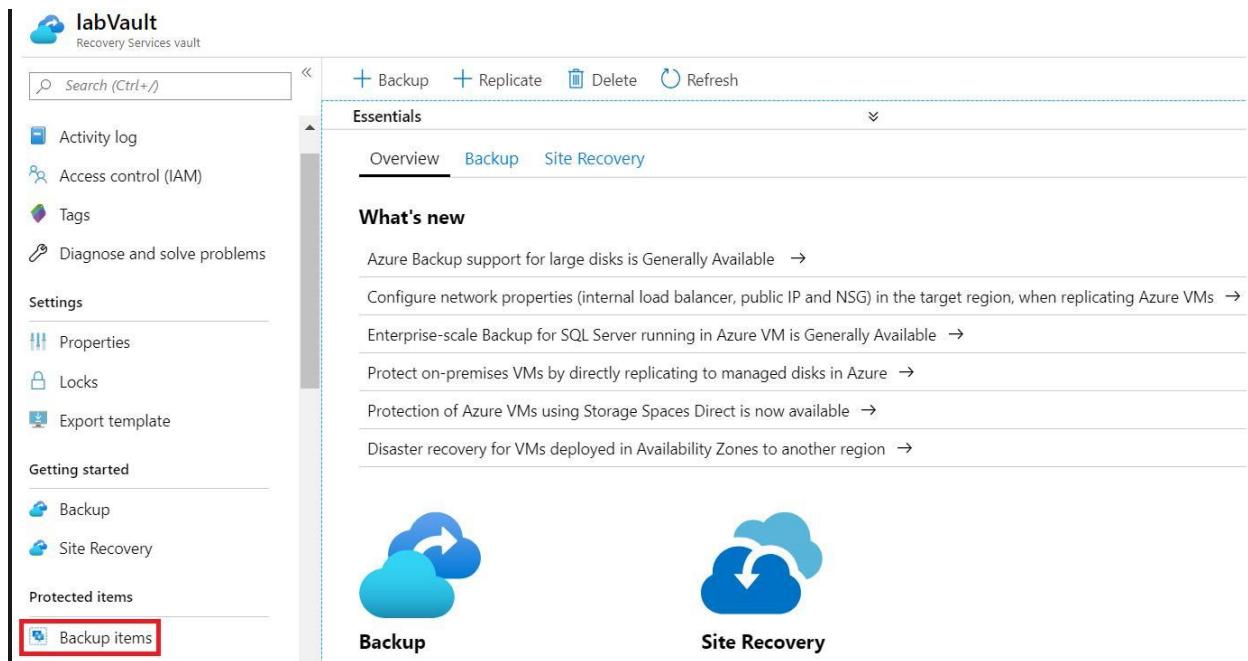
4 Hr 43 Min Remaining

Instructions Resources Help 100%

Task 3 - Performing an Initial Backup

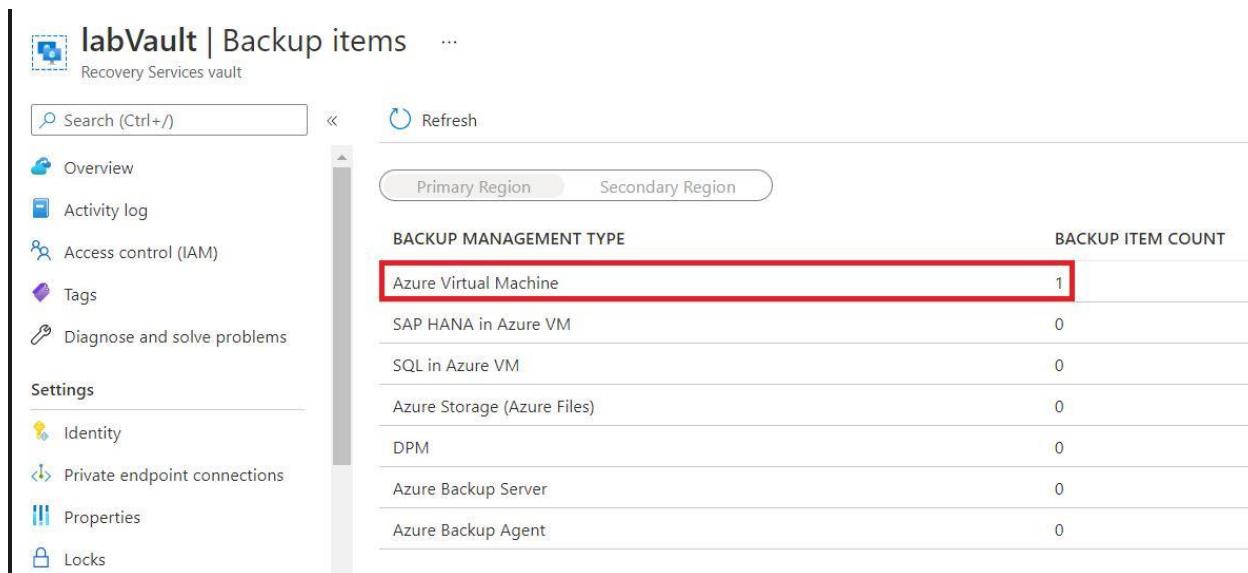
Once a backup policy has been configured for a virtual machine, it does not mean that the machine has been backed up. By default, the first scheduled backup (as defined in the backup policy) is the initial backup. Until the initial backup occurs, the **Last Backup Status** in the Backup Items blade will show as "**Warning (initial backup pending)**".

1.  In the vault blade, click on the **Backup Items** tile.



The screenshot shows the Azure Recovery Services vault interface for 'labVault'. The left sidebar contains navigation links: Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Properties, Locks, Export template), Getting started (Backup, Site Recovery), Protected items, and Backup items (which is highlighted with a red box). The main area has tabs: Overview, Backup (which is selected and highlighted in blue), and Site Recovery. A 'What's new' section lists several features with arrows pointing to their descriptions. Below the news are two icons: 'Backup' (two clouds with a circular arrow) and 'Site Recovery' (two clouds with a downward arrow).

2. Click on **Azure Virtual Machine** from within the Backup items blade.



The screenshot shows the 'Backup items' blade for 'labVault'. The left sidebar includes: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Identity, Private endpoint connections, Properties, Locks), and Backup items. The main area displays a table titled 'BACKUP MANAGEMENT TYPE' with columns: BACKUP MANAGEMENT TYPE and BACKUP ITEM COUNT. The table rows are: Azure Virtual Machine (1), SAP HANA in Azure VM (0), SQL in Azure VM (0), Azure Storage (Azure Files) (0), DPM (0), Azure Backup Server (0), and Azure Backup Agent (0). The 'Azure Virtual Machine' row is highlighted with a red box.

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	1
SAP HANA in Azure VM	0
SQL in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0
Azure Backup Agent	0

3. Click the '...' ellipse at the end of the backup item line and then select **Backup now**. Click **OK** in the **Backup now** pane. This will start the initial backup.

Backup Items (Azure Virtual Machine)

labVault

Refresh Add Filter

Fetching data from service completed.

Filter items ...

Name	Resource Group	Backup Pre-Check	Last Backup Status	Latest restore point
VM2	backupLab-lod9873500	Passed	Warning(Initial backup)	

Pin to dashboard

Backup now (highlighted)

Restore VM

File Recovery

Stop backup

Delete backup data

4. Go back to the Vault blade and click on the **Backup Jobs** tile then click on **In progress**.

labVault - Backup Jobs

Recovery Services vault

Search (Ctrl+ /)

Choose columns Filter Export jobs Refresh

Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 11/4/2019, 3:06:24 PM, End Time - 11/5/2019, 3:06:24 PM

Completed fetching data from the service.

Filter items...

Workload n...	Operation	Status	Type	Start time	Duration	...
vm2	Backup	In progress	Azure virtual ma...	11/5/2019, 3:05:...	00:01:10	...
vm2	Configure backup	Completed	Azure virtual ma...	11/5/2019, 3:00:...	00:00:31	...

Alerts

Diagnostic settings

Backup Jobs (highlighted)

Site Recovery jobs

Backup Alerts

Site Recovery events

5. Confirm that your backup is successfully running.

Backup

vm2

Cancel Deploy Template

Job Details

VM Name	vm2
Recovery Point Expiry Time in UTC	12/5/2019 10:59:59 PM
Activity ID	f5bca5d5-72c6-4393-aa61-472969dc5022-2019-11-05T14:05:04Z-lbz

Sub Tasks

Name	Status
Take Snapshot	In progress
Transfer data to vault	Not started

Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next exercise.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 43 Min Remaining

Instructions Resources Help 100%

Exercise 2 - Configure a File or Folder Backup

Task 1 - Installing a Backup Agent on an Azure VM

If you have not already created a **Recovery Services Vault**, go back to Exercise 1 and perform that task. Although we could target an on-premises machine to take a backup of files, folders or a System State, for the purposes of this lab, we will be targeting an Azure virtual machine.

1. From within the **backupLab-10dXXXXXX** e.g. **backupLab-10d9873500** resource group click on **VM3**, then click the **Connect** tile at the top of the blade.

The screenshot shows the Azure portal interface for a virtual machine named 'VM3'. The left sidebar lists navigation options: Overview (selected), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (selected), Networking, Disks, Size, and Security. The main content area displays the following details:

Setting	Value
Resource group (change)	backupLab-lod9873500
Status	Running
Location	Central US
Subscription (change)	ASD Developer 1
Subscription ID	cd5624ee-c42c-4f43-9c6d-4aea23072cf3
Computer name	VM3
Operating system	Windows (Windows Server 2019 Datacenter)
Size	Standard D2 v2 (2 vcpus, 7 GiB memory)
Ephemeral OS disk	N/A
Public IP address	40.86.101.114
Private IP address	10.3.0.4
Virtual network/subnet	BackupvNET2/frontEnd
DNS name	Configure

2. Download and open the RDP file, then enter the credentials **AdminUser** and **P@55word1234** and log in to the server.
3. Turn off security for Internet Explorer by going in to the **Server Manager**, selecting **Local Server | IE Enhanced Security Configuration** then configure the **Administrators** and **Users** Enhanced Security to **Off**.



Internet Explorer Enhanced Security Configuration



Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:



On (Recommended)



off

Users:



On (Recommended)



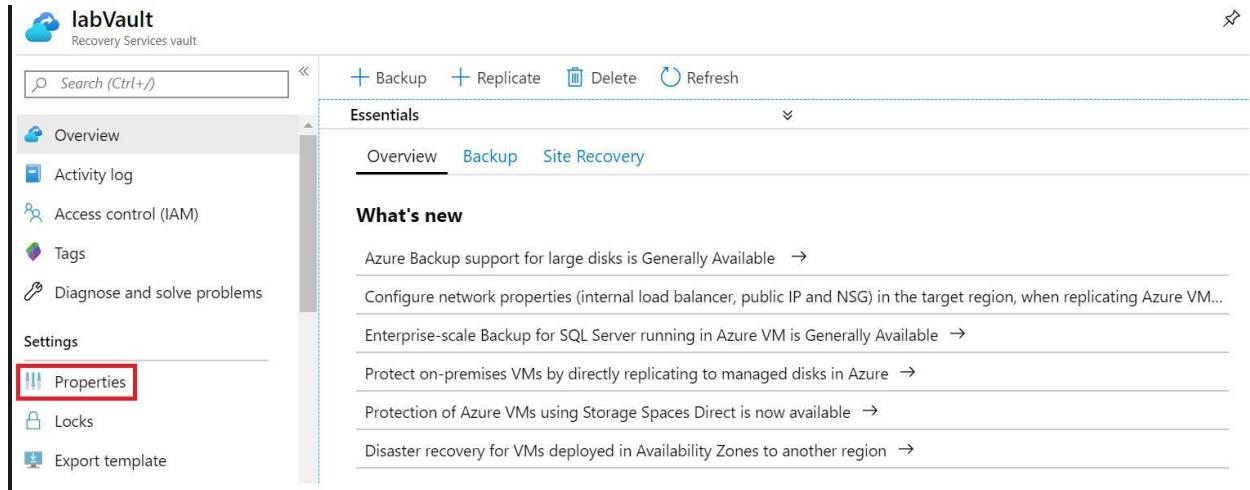
off

[More about Internet Explorer Enhanced Security Configuration](#)

OK

Cancel

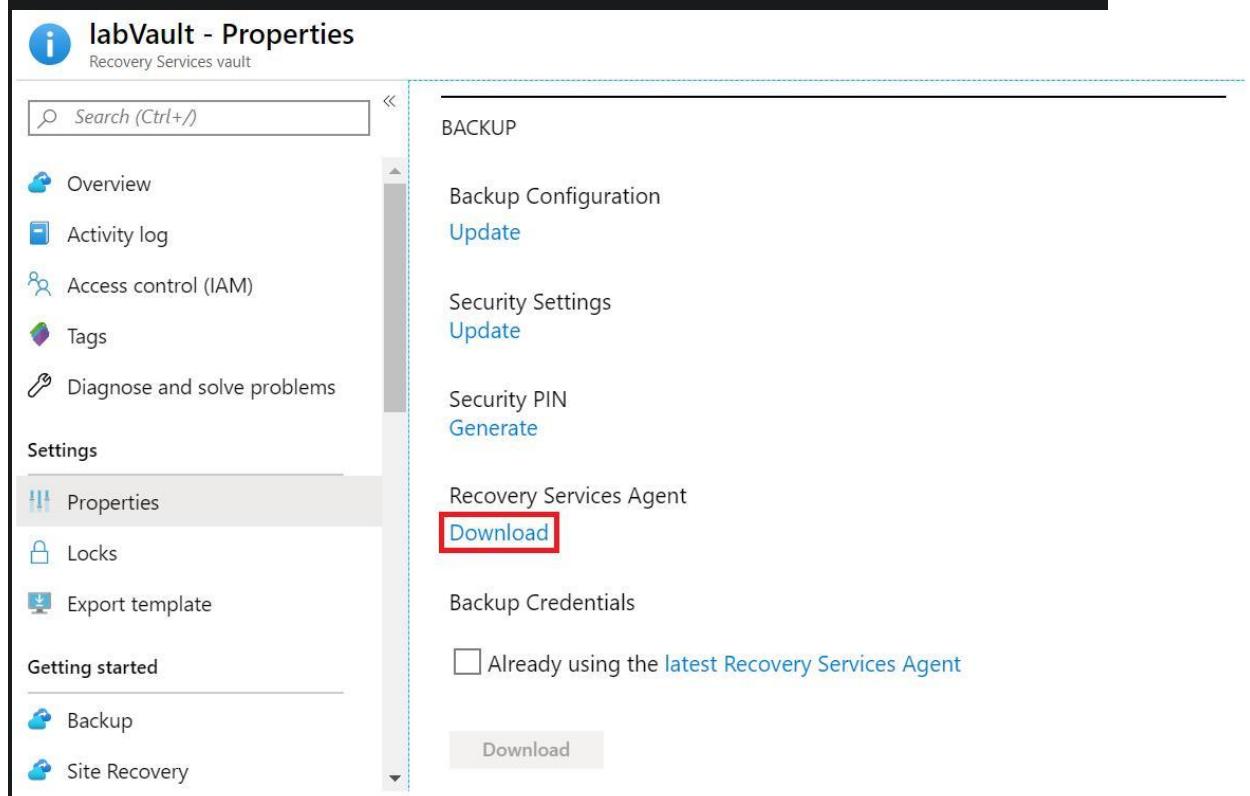
4. From within the virtual machine that you logged into, log in to the Azure portal at <https://portal.azure.com> using your Azure Trial Pass credentials.
5. Navigate to the **backupLab-1dXXXXXXXX** e.g. **backupLab-1d9873500** resource group that contains your Recovery Services vault and then click on the Recovery Services vault that was created earlier. Click on the **Properties** tile.



The screenshot shows the Azure portal interface for a Recovery Services vault named 'labVault'. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Properties (which is selected and highlighted with a red box), Locks, and Export template. The main content area is titled 'Essentials' and contains tabs for Overview, Backup, and Site Recovery. Under 'Overview', there's a 'What's new' section listing several Azure Backup features. At the top of the main area are buttons for Backup, Replicate, Delete, and Refresh.

6. Click on the **Download** link under **Recovery Services Agent** and save the **MARSAgentInstaller.exe** file to the desktop.

Do NOT initiate the installation process yet and leave the Azure portal open.



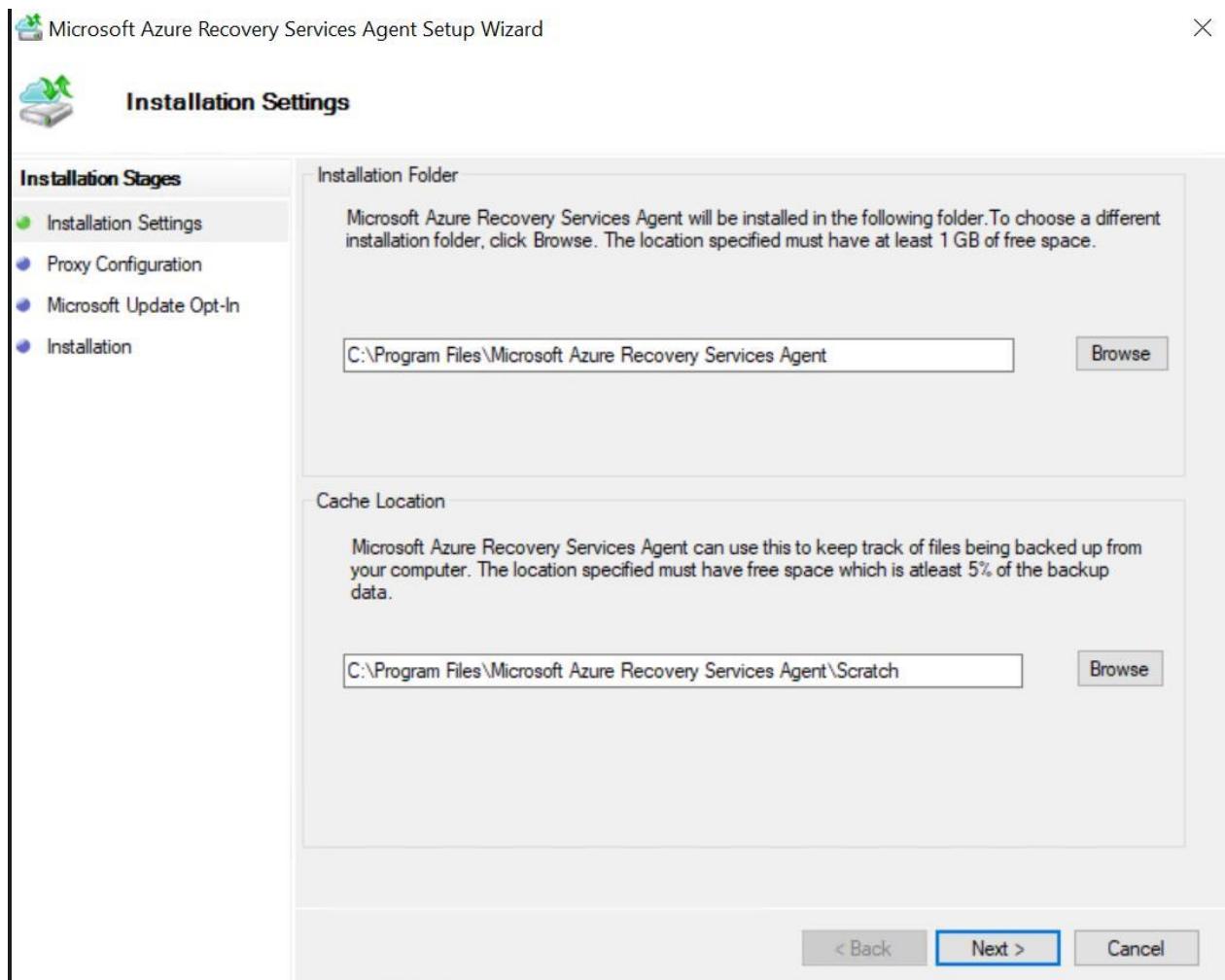
This screenshot shows the 'Properties' page for the 'labVault' Recovery Services vault. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (with 'Properties' selected and highlighted with a red box), 'Locks', and 'Export template'. In the main pane, under the 'RECOVERY SERVICES AGENT' heading, there are sections for 'Backup Configuration' (with a 'Update' link), 'Security Settings' (with a 'Update' link), 'Security PIN' (with a 'Generate' link), and 'Recovery Services Agent' (with a 'Download' link highlighted with a red box). Below these, there's a checkbox for 'Already using the latest Recovery Services Agent' and a 'Download' button.

7. From within the same pane, under **Backup Credentials**, tick the **Already using the latest Recovery Services Agent** checkbox, then click the **Download** button below it and save the file to the desktop. These credentials are required when you install a Microsoft

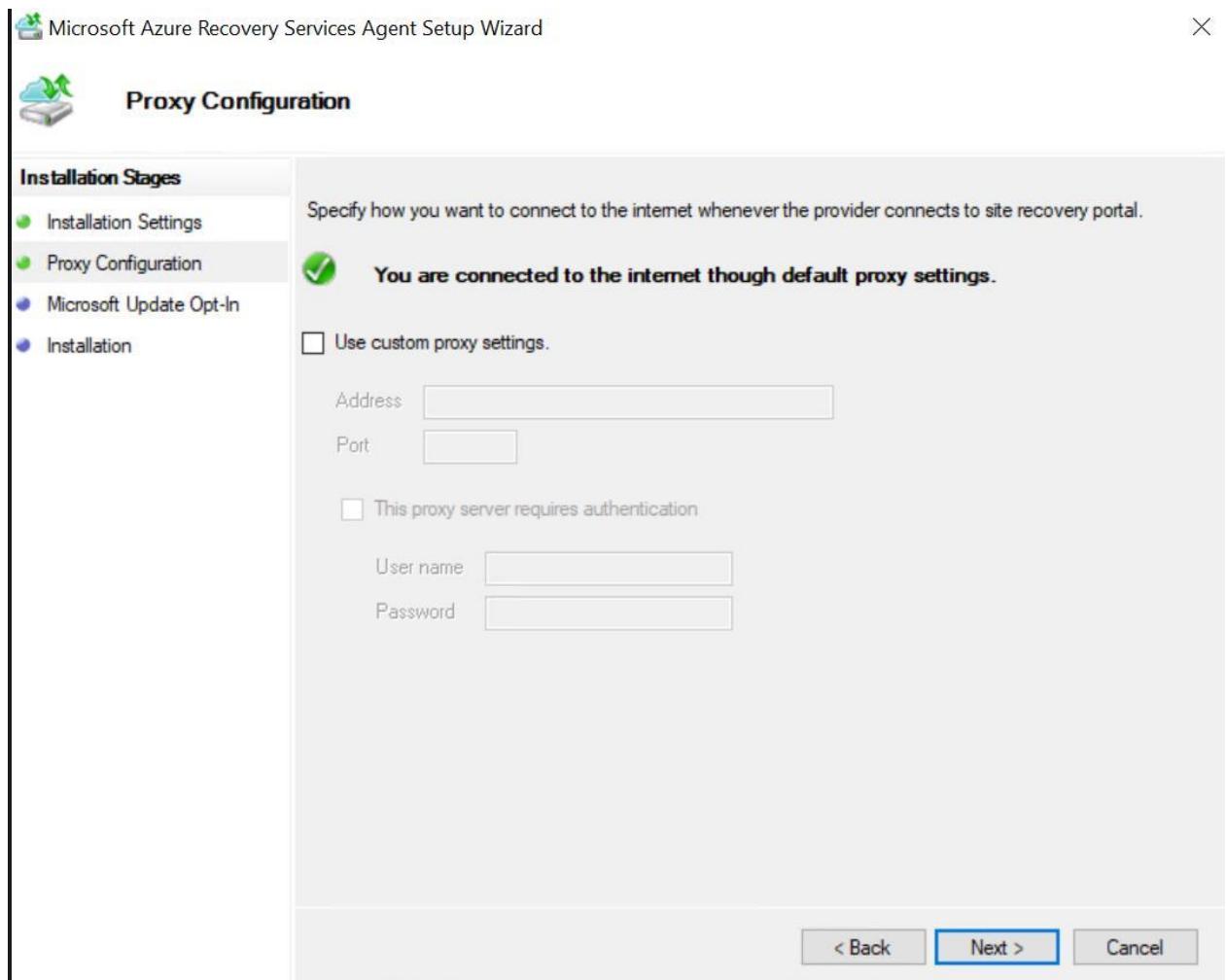
Azure Recovery Services backup agent on a machine that you would like to backup files, folders or a System State on.

The screenshot shows the 'Properties' page for a Recovery Services vault named 'labVault'. The left sidebar has a search bar and links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties (which is selected and highlighted), Locks, and Export template. The main area is titled 'BACKUP' and contains several options: 'Backup Configuration' with a 'Update' link, 'Security Settings' with a 'Update' link, 'Security PIN' with a 'Generate' link, 'Recovery Services Agent' with a 'Download' link, and 'Backup Credentials'. At the bottom of the main area, there is a checkbox labeled 'Already using the latest Recovery Services Agent' with a checked box, and a large blue 'Download' button.

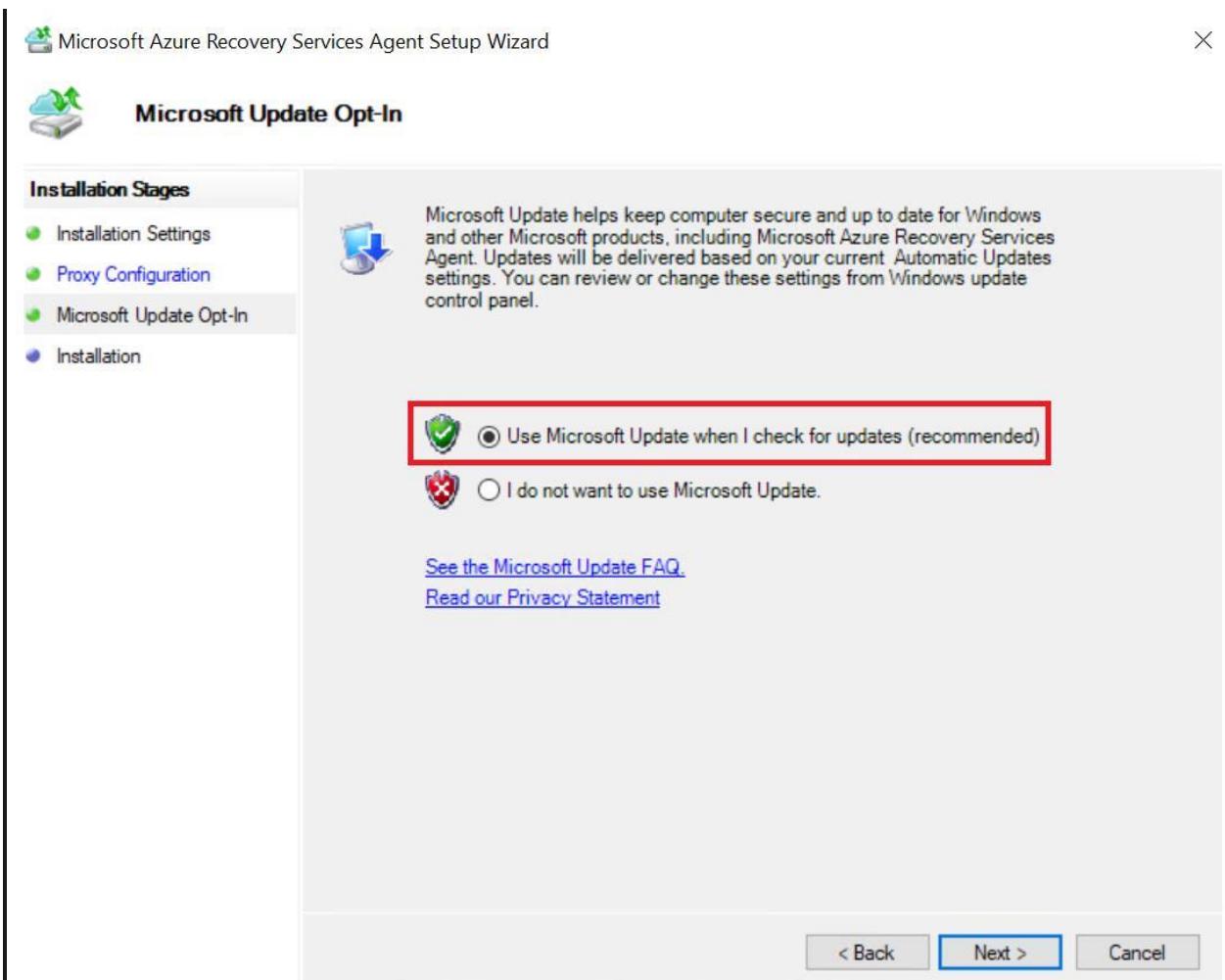
8. Run the **MARSAgentInstaller.exe** file from the desktop. Accept UAC prompts for the software if prompted. For the lab exercise, you can accept the default settings for the installation and cache locations. Click **Next**.



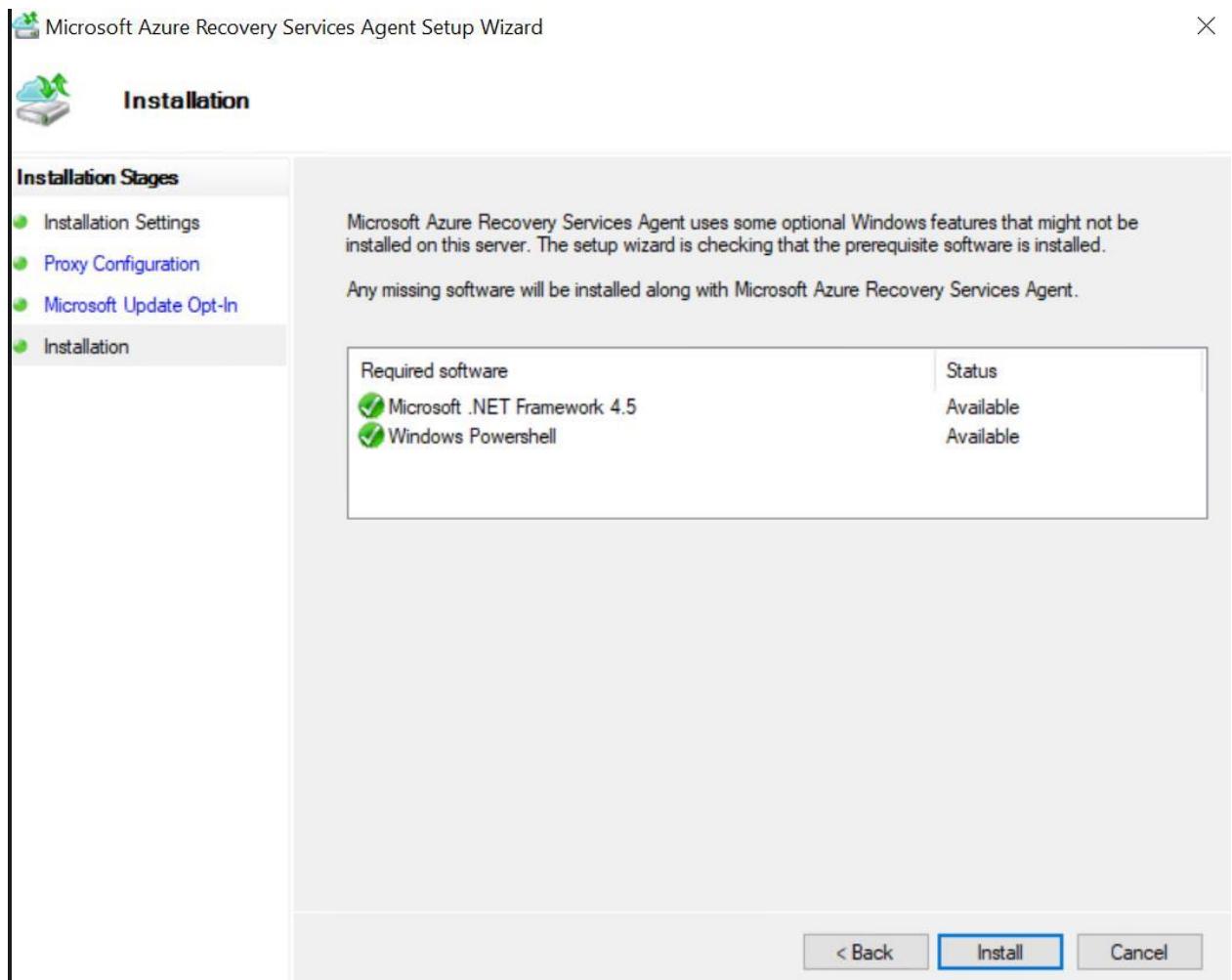
9. Click **Next** at the **Proxy Configuration** stage.



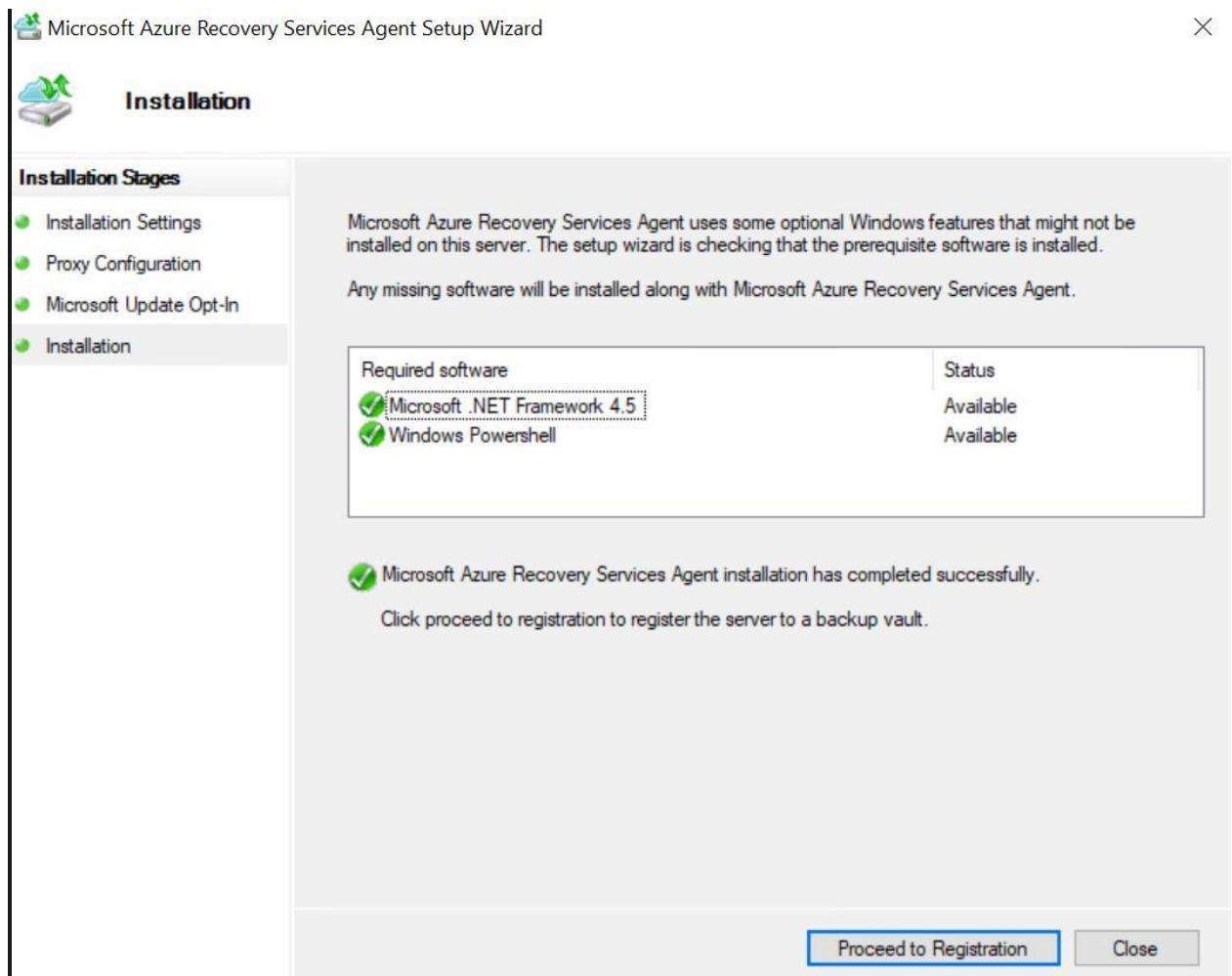
10. Select the **Use Microsoft Update when I check for updates (recommended)** radio button at the **Microsoft Update Opt-In** stage and click **Next**.



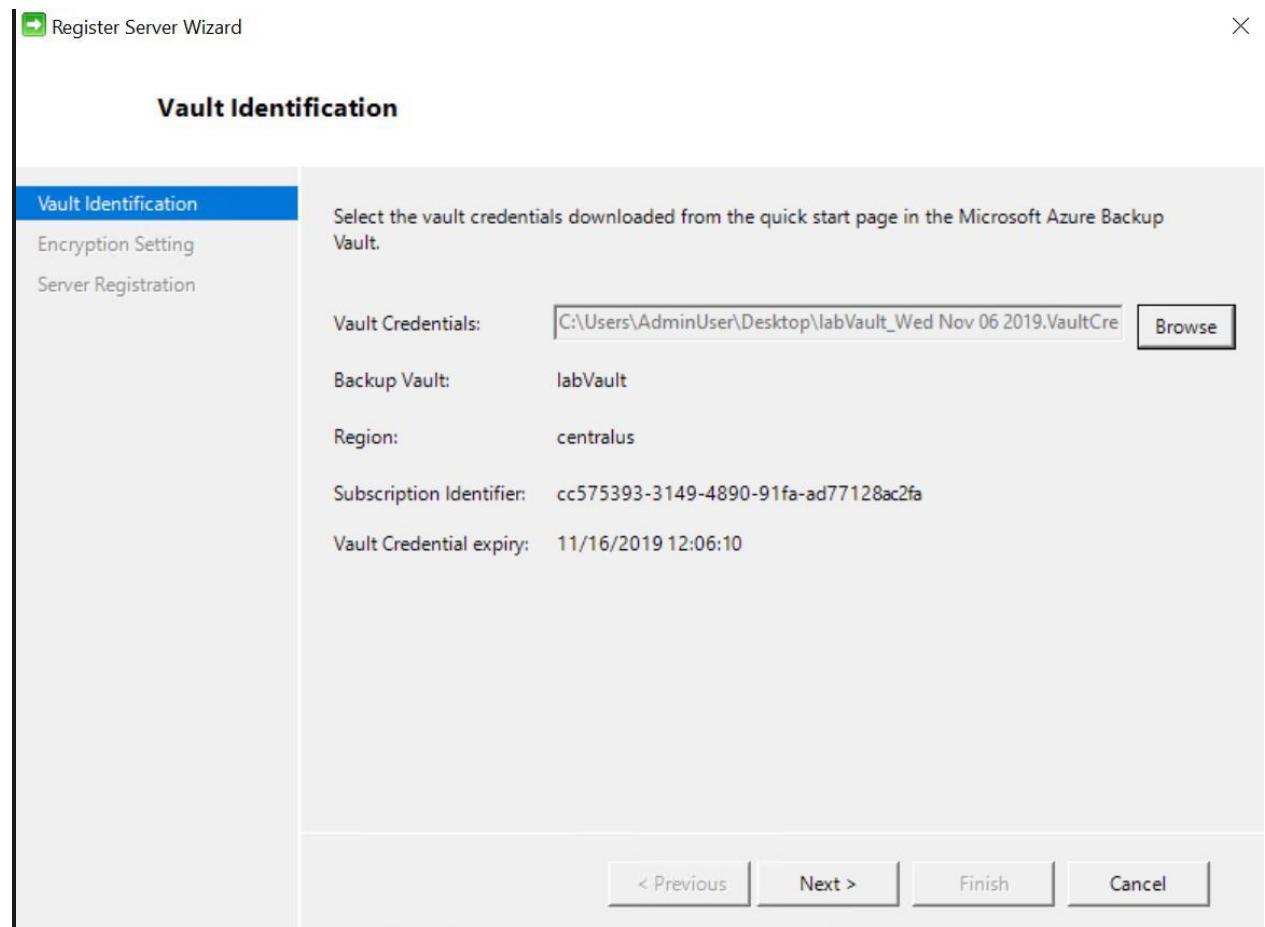
11. Click **Install** at the **Installation** stage.



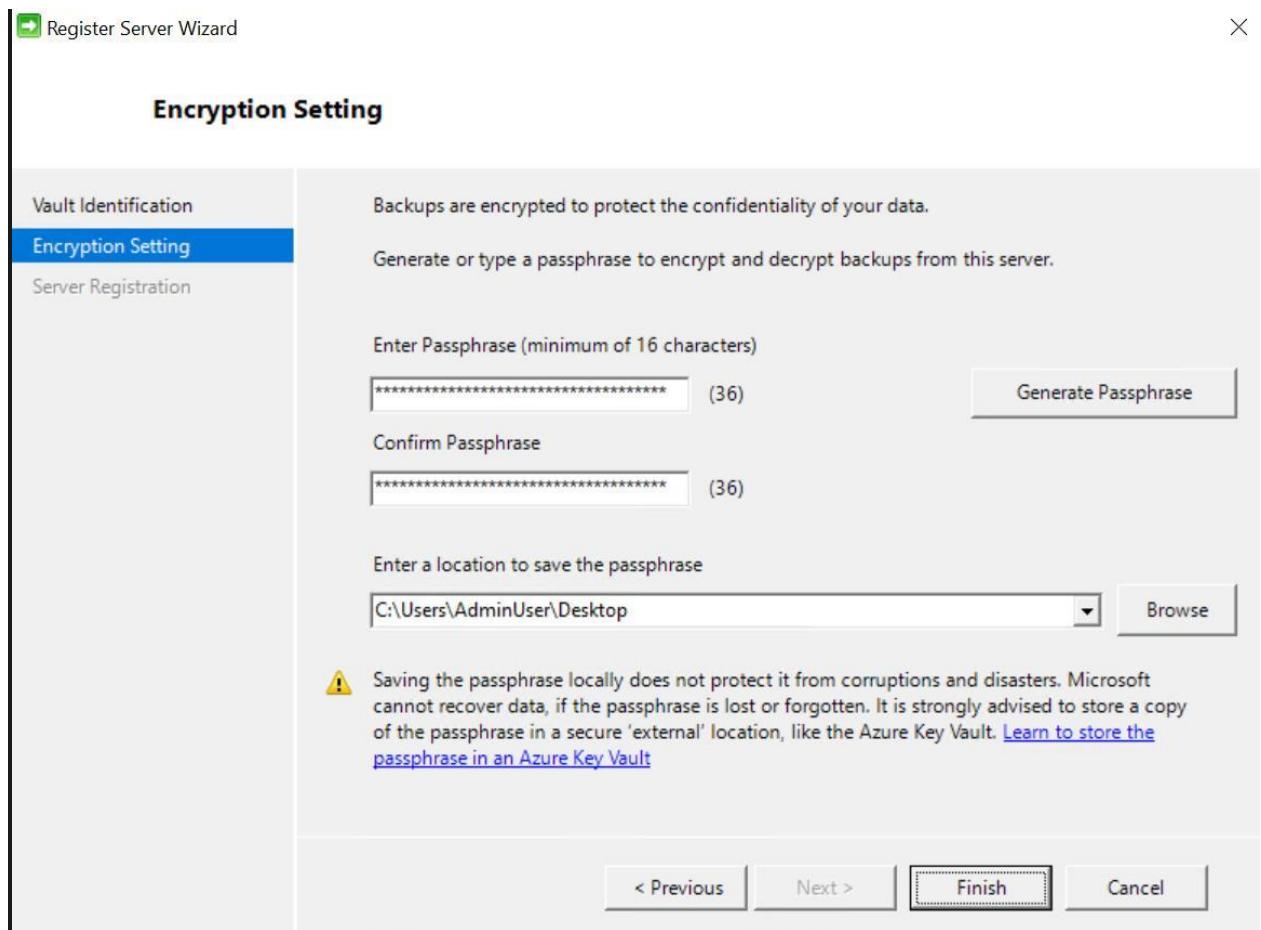
12. On completion of the installation, click the "**Proceed to Registration**" button.



13. At the **Vault Identification** stage, click "**Browse**", then navigate to the **Vault Credentials file** downloaded from the portal earlier, select it, then click **Open**, then click **Next**.

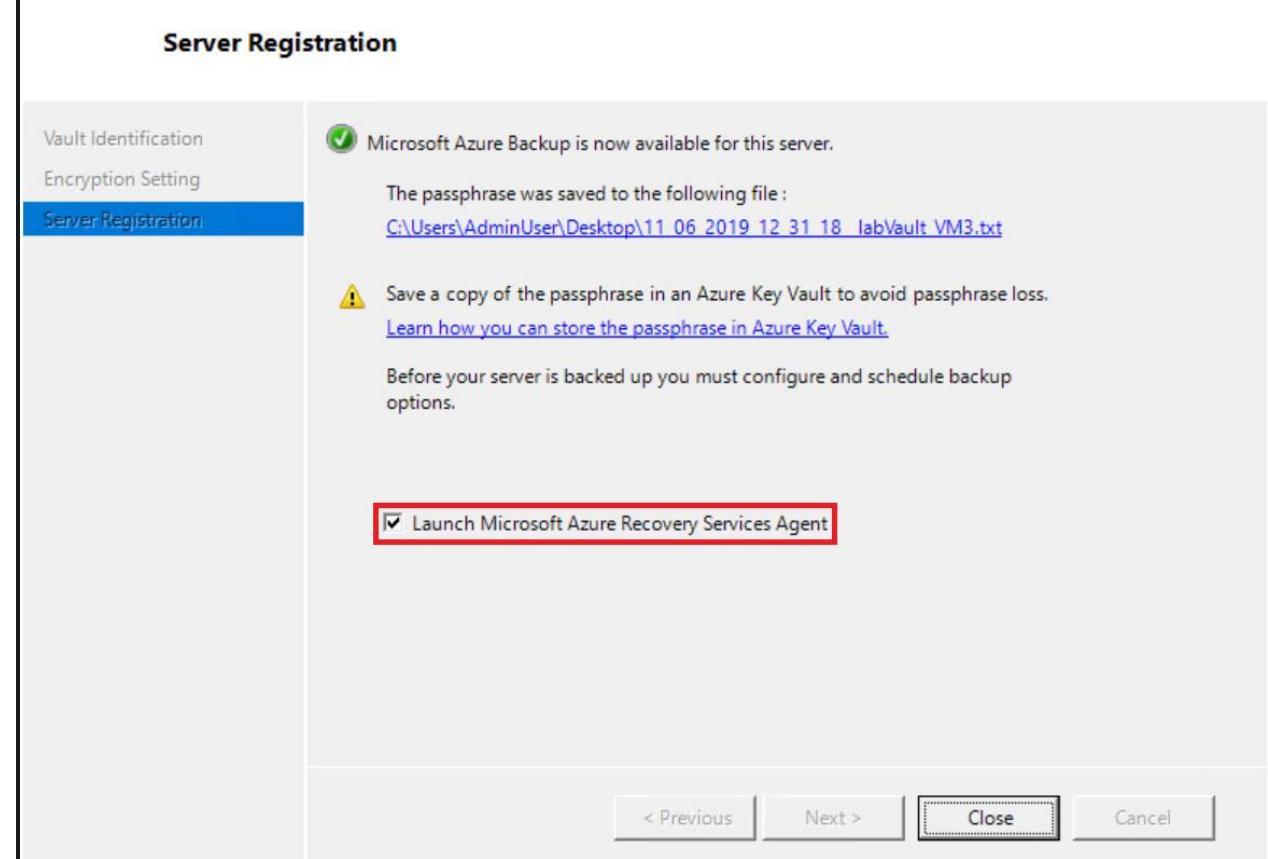


14. Click the **Generate Passphrase** button. This passphrase will be used to encrypt and decrypt backups for the backed up machine (**it is machine specific**) and needs to be very strong (at least 16 characters). Click **Browse** and enter a location to save the passphrase file. Keep this file in a safe place e.g. Azure Key Vault. For this lab, you can use the Desktop. Click **Finish**.



15. Confirm that the **Launch Microsoft Azure Recovery Service Agent** tickbox is ticked, then click **Close**.

Register Server Wizard



16. The Microsoft Azure Backup Admin console is then launched.
17. Click the **Schedule Backup** link on the right side.

Microsoft Azure Backup

Microsoft Azure Backup supports scheduled backups of files and folders, and Windows System State.

⚠ Backups have not been configured for this server. Click "Schedule Backup" in the Actions pane to configure backup options and protect your File Servers, Domain Controllers and IIS Web-Servers from corruptions, attacks and ransomware. You can also Configure Notifications from Alerts blade to receive email alerts for backup failures. [Learn More](#).

Jobs (Activity in the past 7 days, double click on the message to see details)

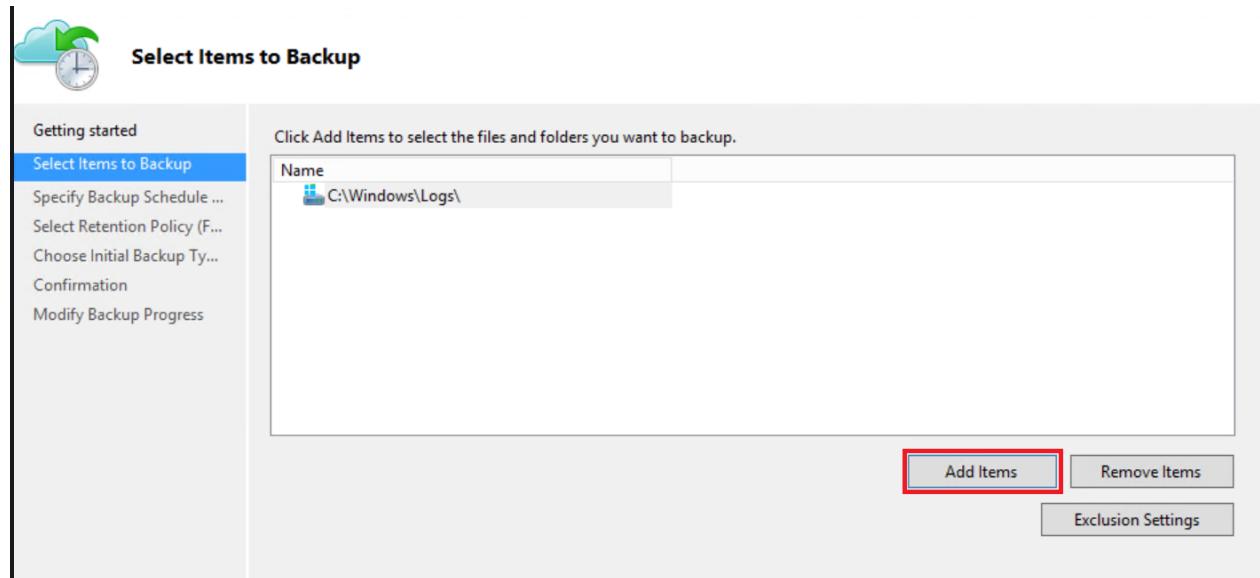
Status	Time	Message	Description

Actions

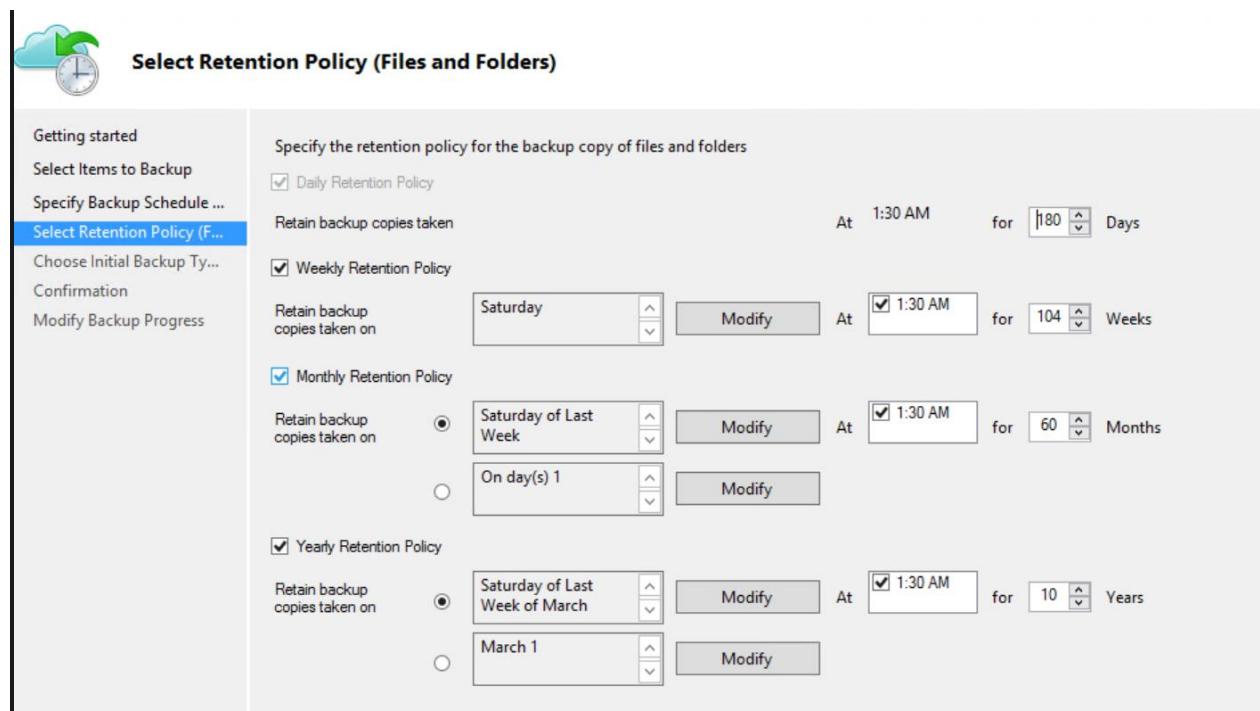
- Backup
- Schedule Backup**
- Recover Data
- Change Properties
- Open Portal
- About Microsoft Azure Recovery Services
- Privacy & Cookies
- View
- Help

18. Click **Next** at the **Getting started** stage.

19. You can add items e.g. files, folders or System State to backup. You can also set exclusion settings to exclude certain files or folders. Click **Add Items**, add C:\Windows\Logs\, and click **OK**.



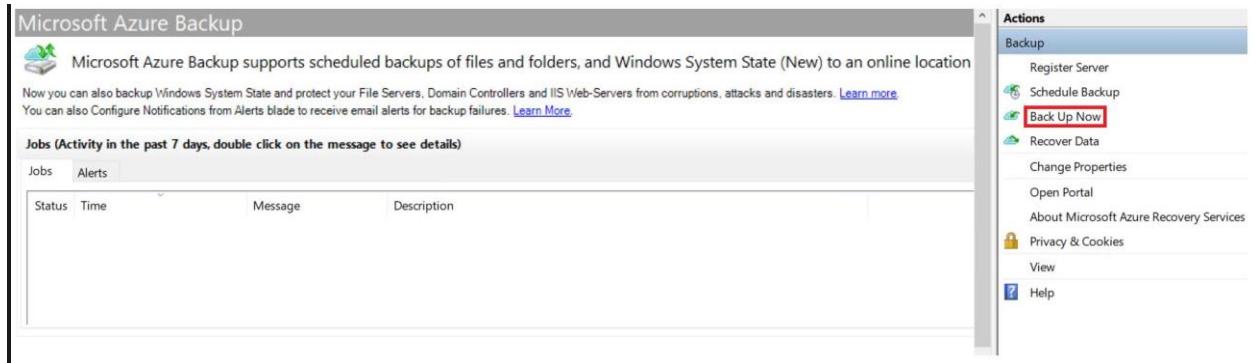
20. Click **Next**.
21. You can create a schedule for backing up the data. Either daily or weekly, up to 3 times per day. Accept the default configuration and click **Next**. Backed up data can be retained **daily, weekly, monthly** and **yearly**. Accept the default configuration and click **Next**.



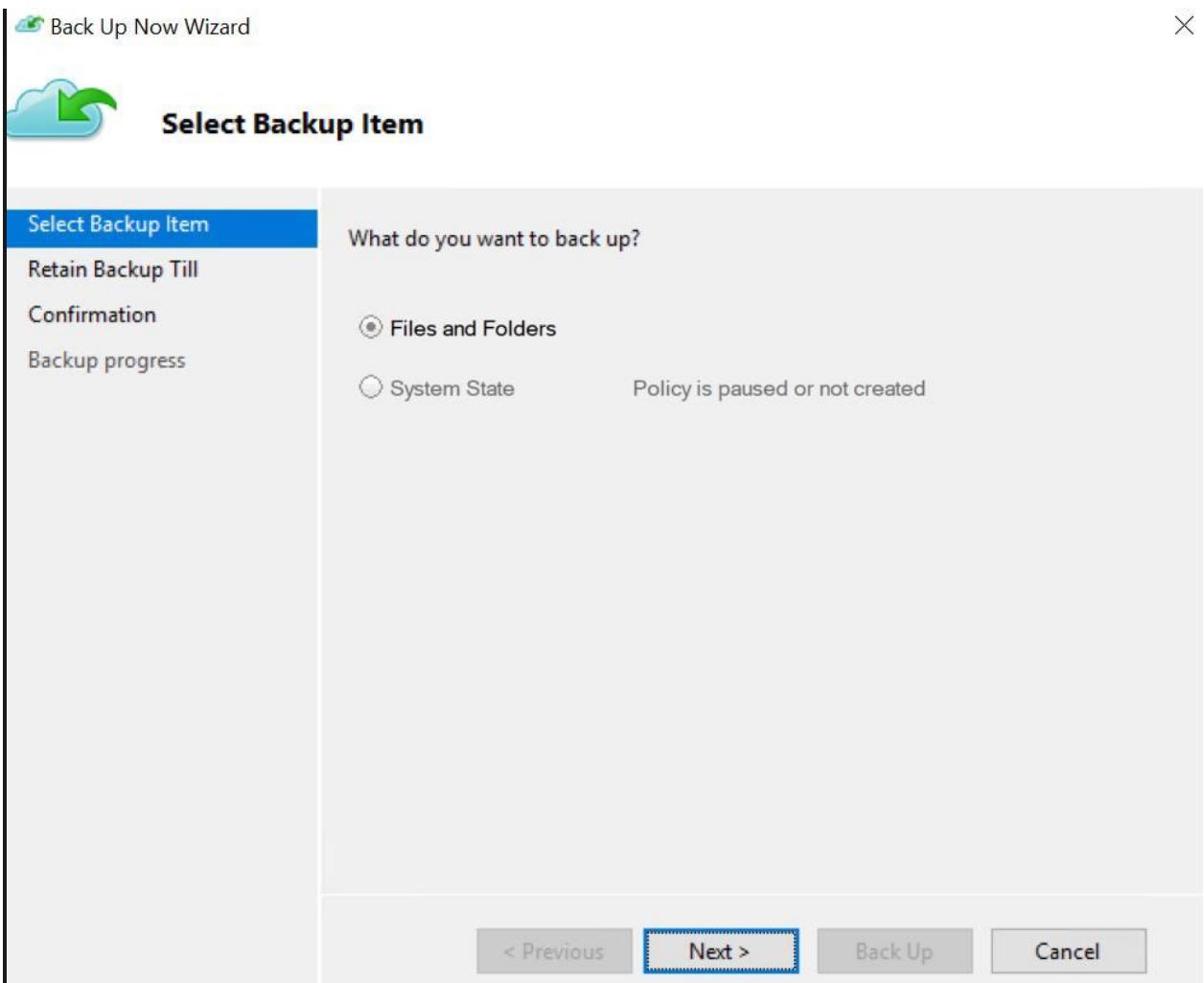
22. Accept the default configuration (**Automatically over the network**) at the **Choose Initial Backup Type (Files and Folders)** stage and click **Next**.

This will back up the files over the Internet to Azure. If you want to backup locally and send the data to a drive, you would select Offline backup and enter the settings. Click the **here** link for more information on how to create the offline backup and shipping instructions.

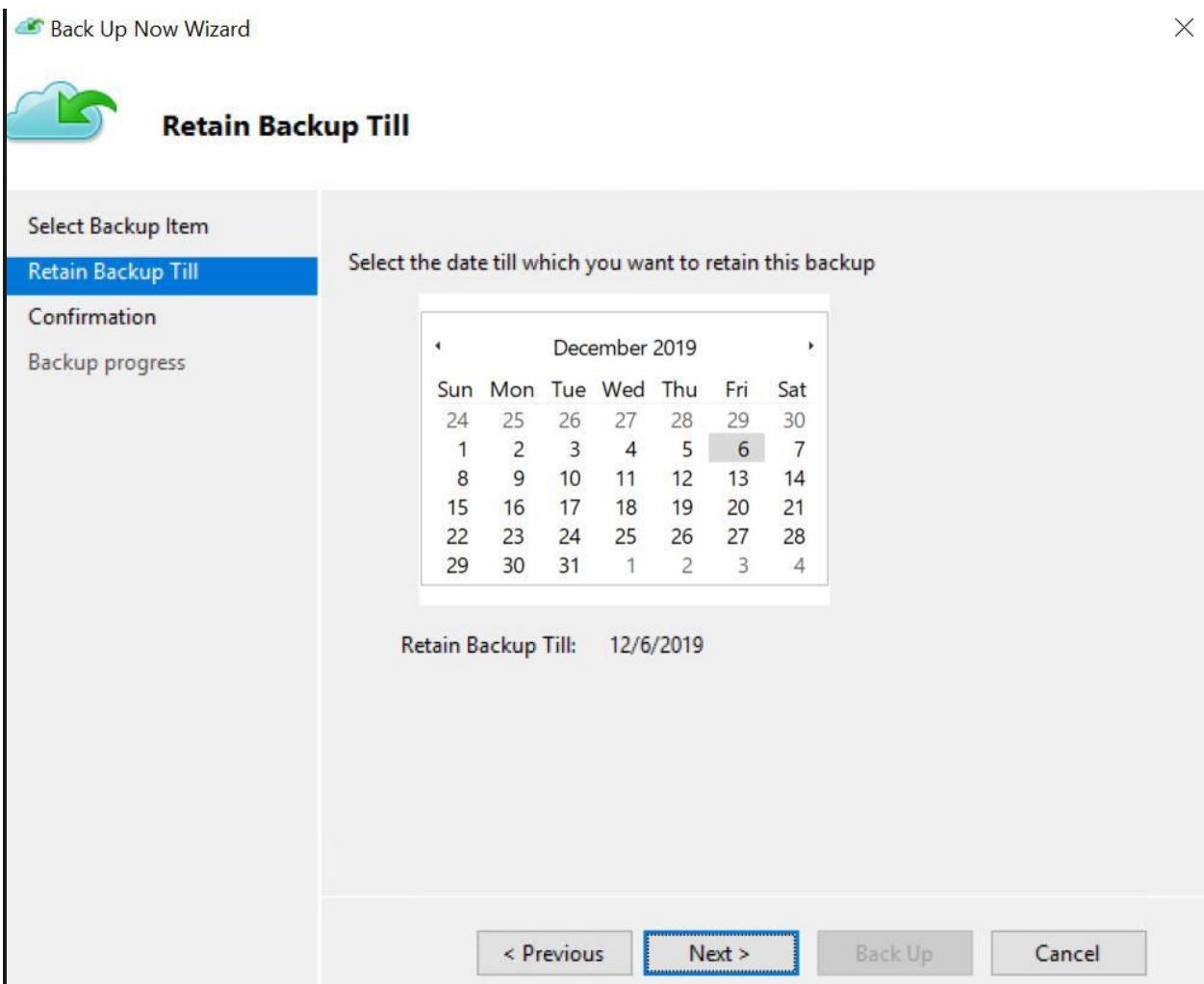
23. Click **Finish**.
24. Click **Close** on successful creation of a backup schedule.
25. Click the **Back Up Now** button on the right side.



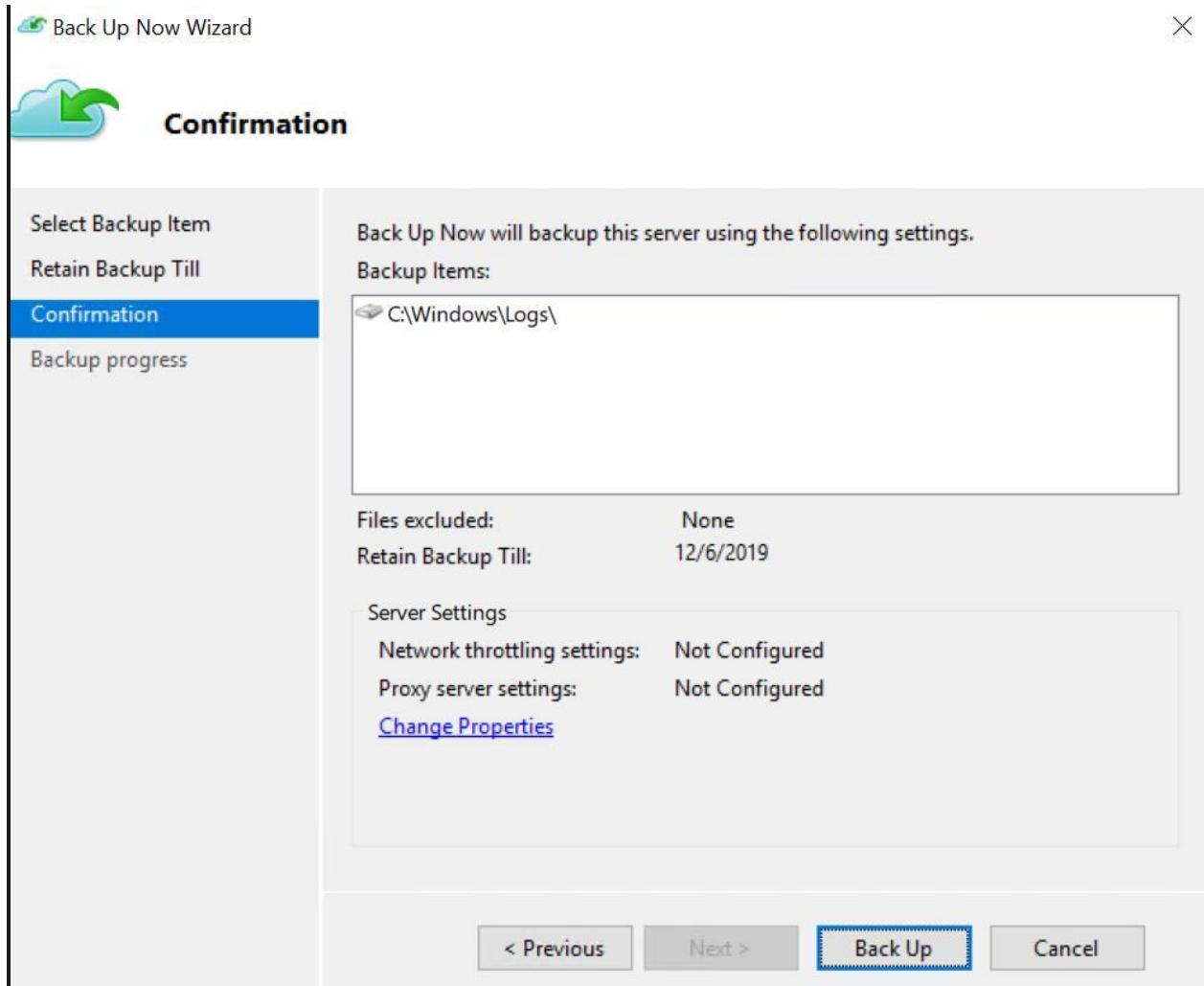
26. Accept the default configuration at the **Select Backup Item** stage and click **Next**.



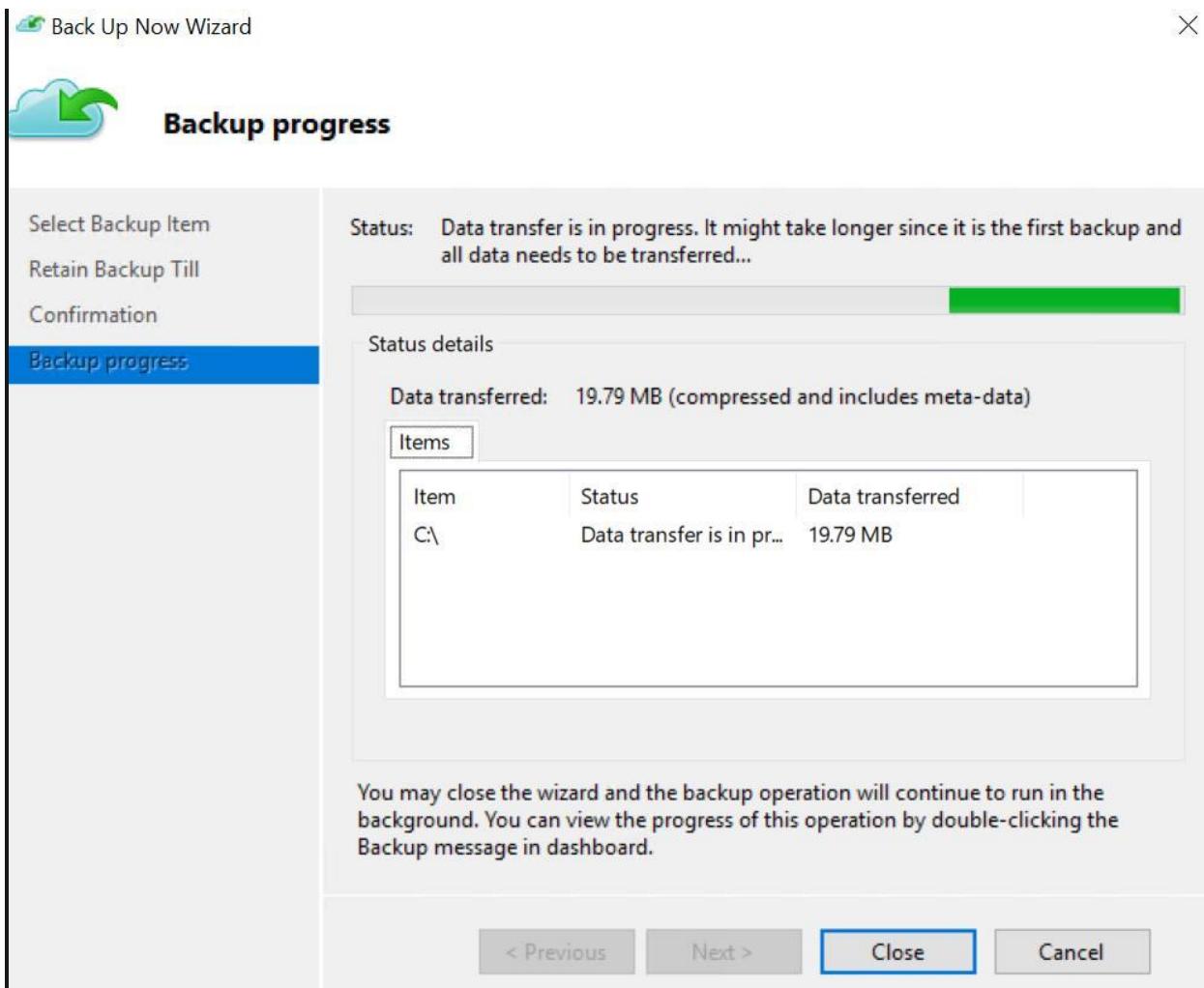
27. Accept the default configuration at the **Retain Backup Till** stage and click **Next**



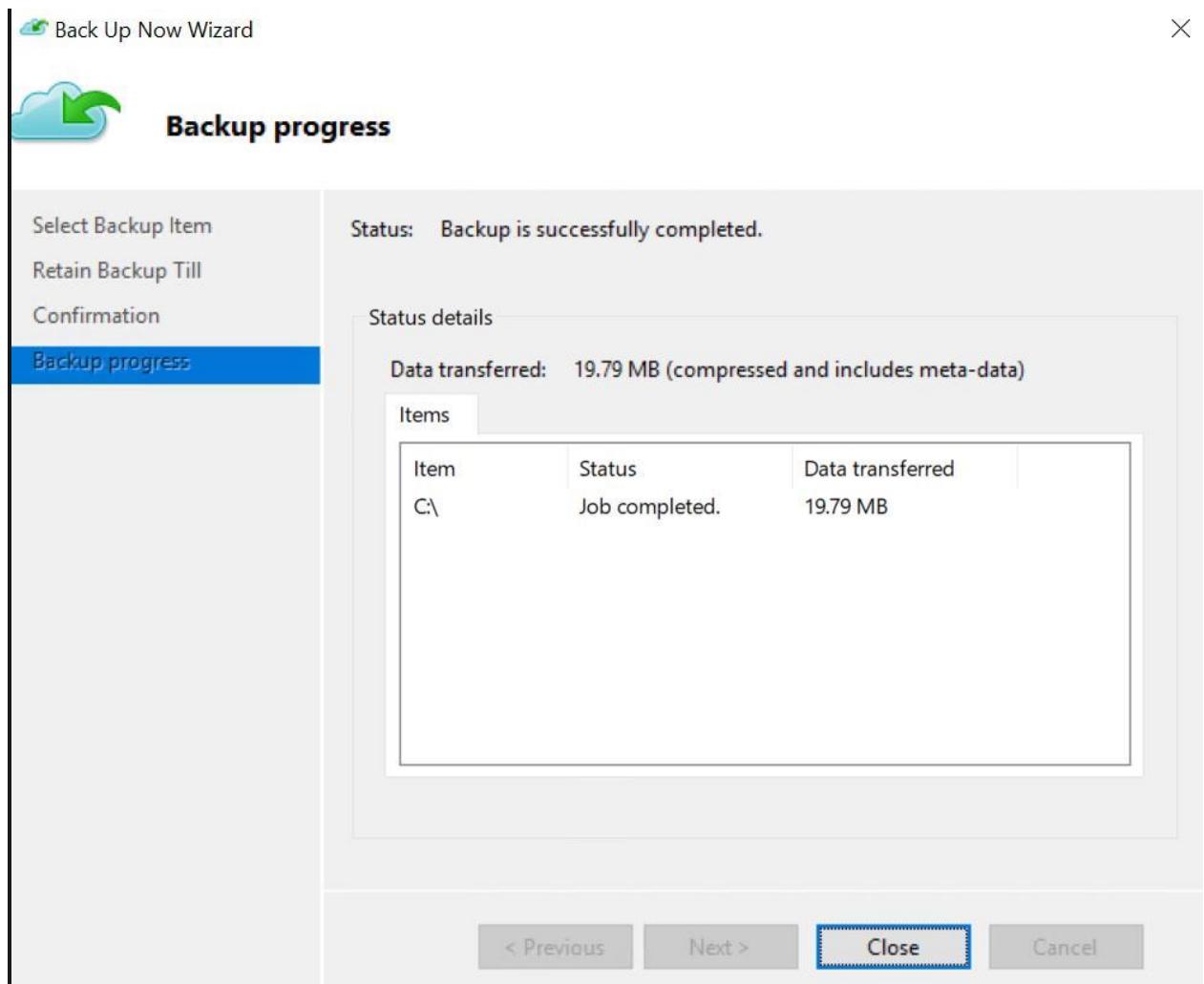
28. Click **Back Up** at the **Confirmation** stage. This will back up the location that you have selected earlier.



29. Confirm that the backup is in progress.



30. Click **Close** on successful completion of the backup.



All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 42 Min Remaining

Instructions Resources Help 100%

Task 2 - Performing a File or Folder restore

1. On the desktop of the virtual machine that you have taken a file or folder backup of (in this case **VM3**), open the **Microsoft Azure Backup** application if it is not already running.



2. You should have a previously successful backup listed in the **Status** section and at least 1 **Total backups** listed.

Status		Next Backup	Available Recovery Points	Last Recovery
Last Backup				
Status: ✓ Successful		Status: Scheduled	Total backups: 1	Status: -
Time: 11/6/2019 1:14 PM		Time: 11/7/2019 8:30 AM	Latest copy: 11/6/2019 1:14 PM	Time: -
View details			Oldest copy: 11/6/2019 1:14 PM	View details

3. Click the **Recover Data** link on the right side.

Jobs (Activity in the past 7 days, double click on the message to see details)			
Jobs		Alerts	
Status	Time	Message	Description
✓	11/6/2019 1:14 PM	Backup	Job completed.

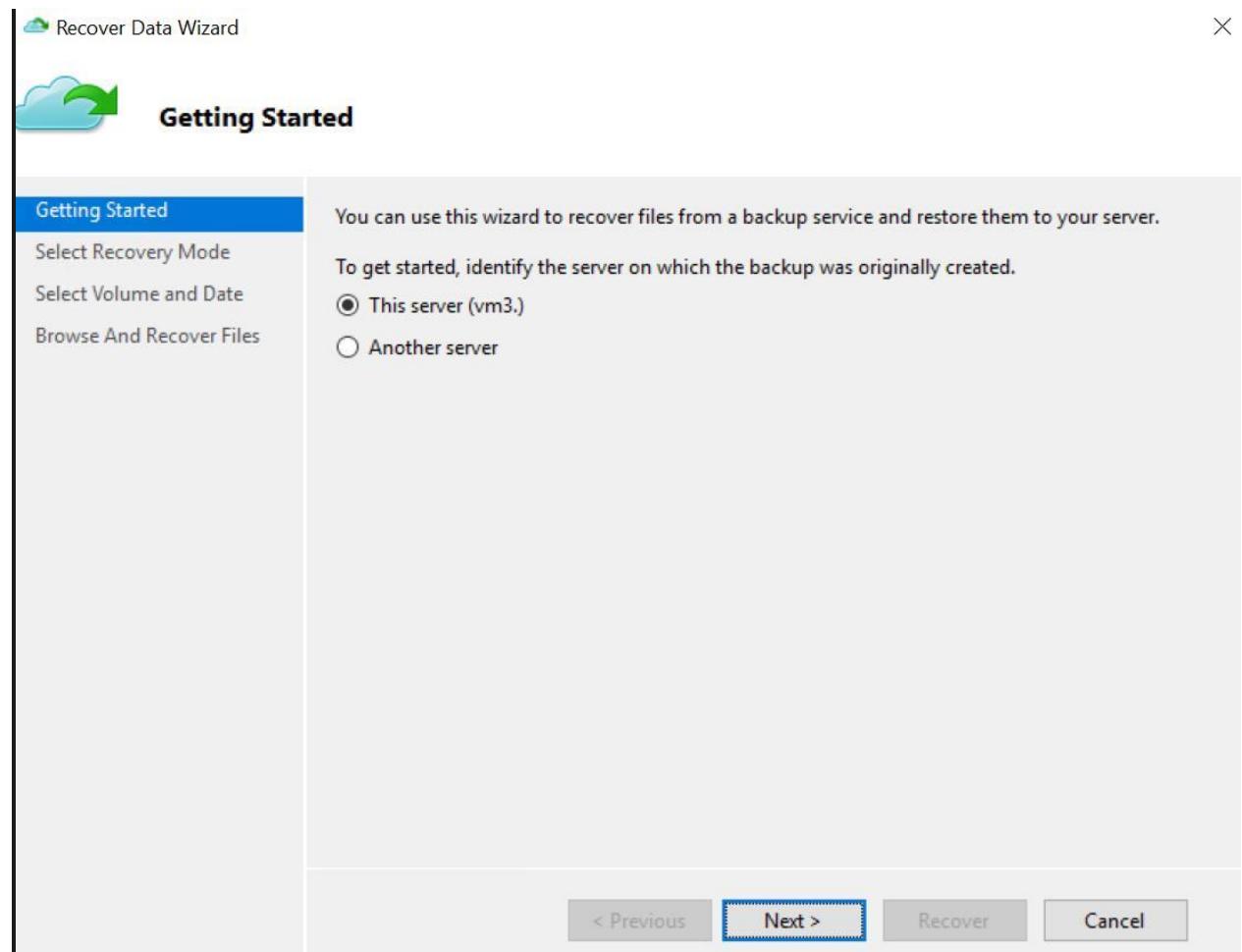
Status

Last Backup	Next Backup	Available Recovery Points

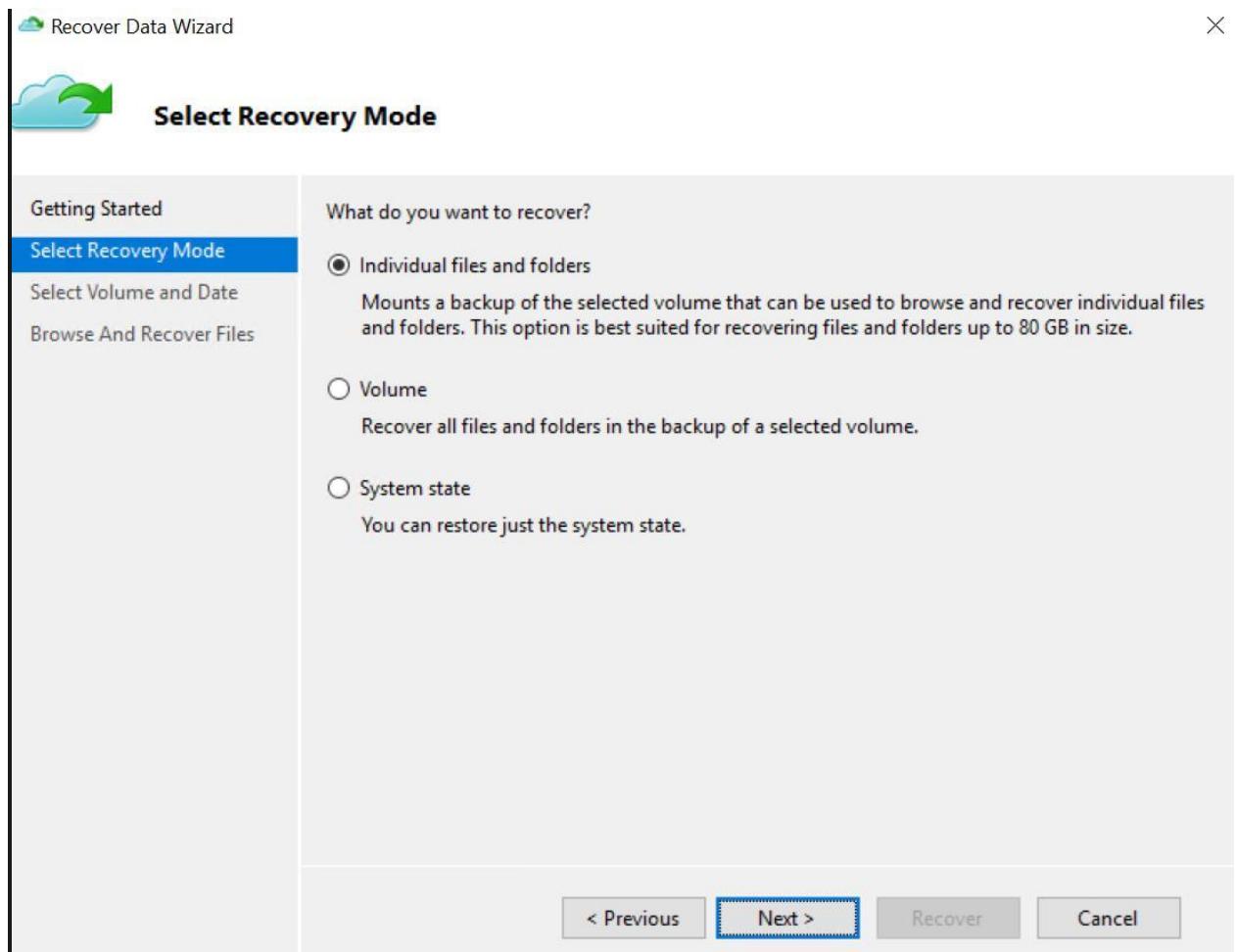
Actions

- Backup
- ✓ Schedule Backup
- ✓ Back Up Now
- Recover Data
- Change Properties
- Open Portal
- About Microsoft Azure Recovery ...
- 🔒 Privacy & Cookies
- ? Help

4. Accept the default configuration at the **Getting Started** stage (**VM3** since the backup was taken on **VM3**) and click **Next**.



5. Accept the default configuration at the **Select Recovery Mode** stage (since a backup of **files and folders** was taken) and click **Next**.



6. Select the **C:** volume from the **Select the volume** drop down menu at the **Select Volume and Date** stage, this will list available backups that can be used for a restore operation. Select the latest backup (there should only be one) and click **Mount**. This will mount the backup as an additional volume in the Windows file system.

Recover Data Wizard

 **Select Volume and Date**

Getting Started
Select Recovery Mode
Select Volume and Date
Browse And Recover Files

Select the volume: C:\

Available backups
Oldest available backup: 11/6/2019 1:14 PM
Newest available backup: 11/6/2019 1:14 PM

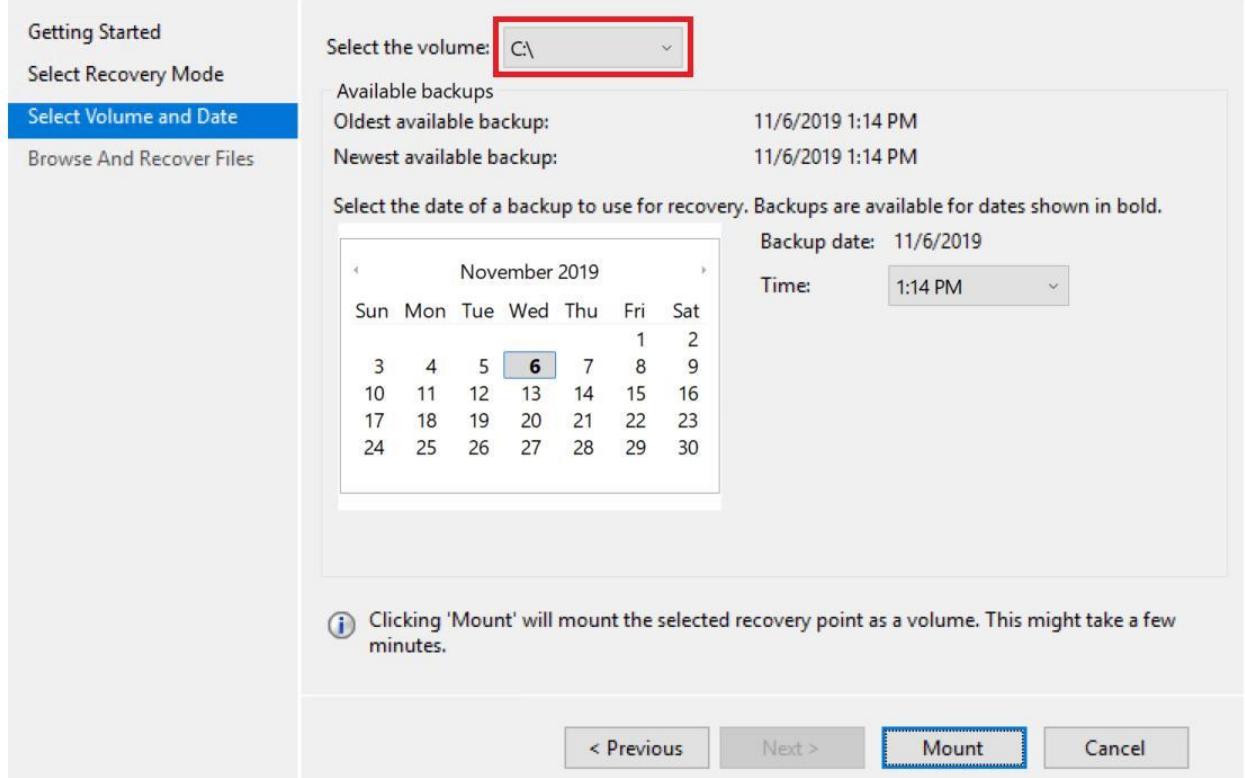
Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

November 2019						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

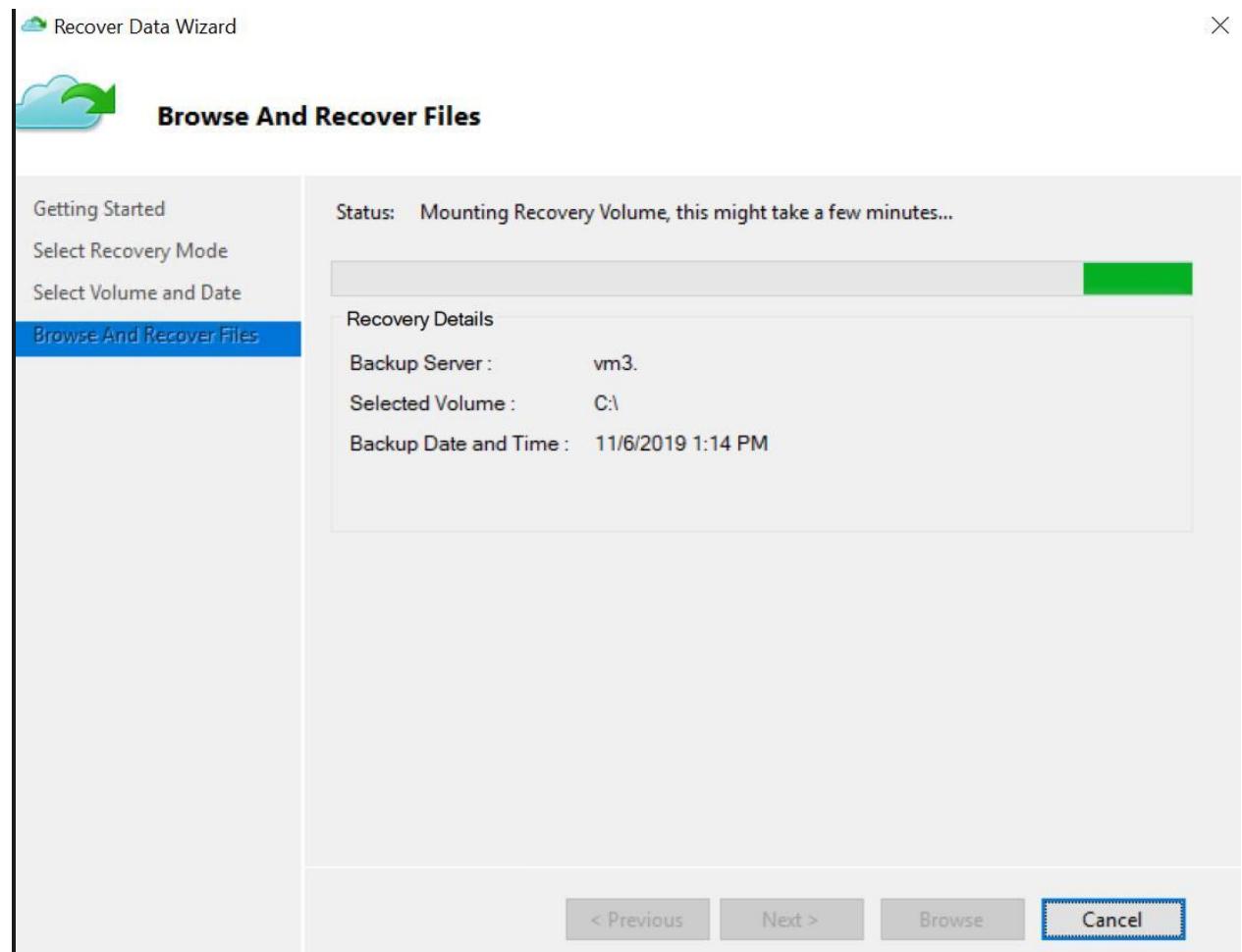
Backup date: 11/6/2019
Time: 1:14 PM

 Clicking 'Mount' will mount the selected recovery point as a volume. This might take a few minutes.

< Previous Next > Mount Cancel



7. Confirm that the backup volume mount is in progress.



8. Once the backup volume has been mounted, click **Browse** and click **OK** to the Robocopy tip.

Recover Data Wizard

Browse And Recover Files

Getting Started
Select Recovery Mode
Select Volume and Date
Browse And Recover Files

Status: Recovery volume mounted as disk. Browse volume from file explorer to recover items.

Recovery Details

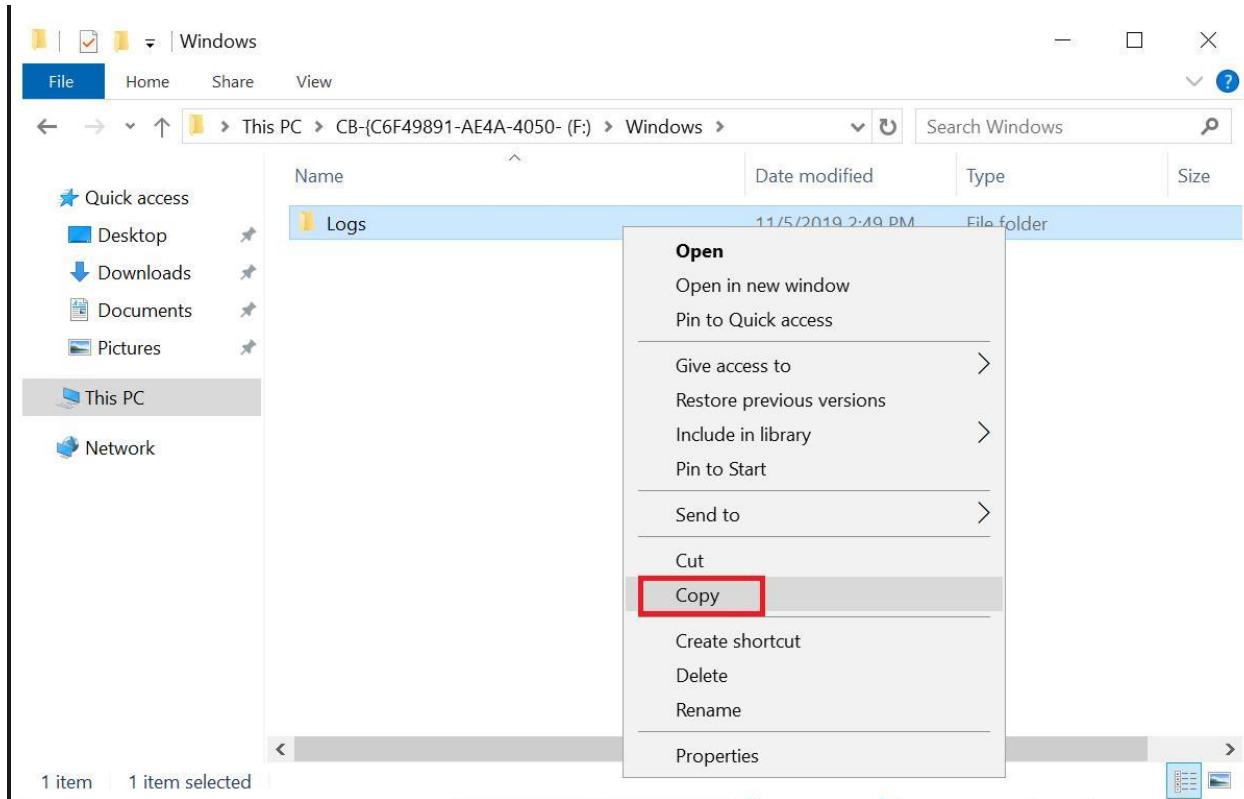
Recovery Volume :	F:\
Backup Server :	vm3.
Selected Volume :	C:\
Backup Date and Time :	11/6/2019 1:14 PM

Click 'Browse' or open the recovery volume from explorer to browse and copy items, to recover them. Click 'Unmount' to unmount the volume and finish recovering.

! Recovery volume is available till 11/6/2019 7:52:58 PM. Mount time is extended to a maximum of 7 days in case of an ongoing file-copy. Any backups scheduled during this time, will run after the volume is unmounted.

< Previous Next > **Browse** Unmount

9. Navigate to the file or folder that you would like to restore and manually copy the data that you need to recover.



All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 42 Min Remaining

Instructions Resources Help 100%

Lab review exercises

It is expected that all course labs have been complete. This lab will assume the same Office 365 tenant used in the course is still being used and certain settings, users, groups, policies, and other configured items are still present. Exercises will be presented primarily as scenarios rather than step-by-step instructions. If appropriate, exercises may be combined in a single scenario.

Prerequisites

This lab will leverage the knowledge gained in previous labs you've already completed.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 41 Min Remaining

Instructions Resources Help 100%

Exercise 1: Deploy a virtual machine using a Visual Studio template

You are required to deploy Azure resources using the Visual Studio 2017 built-in templates. In this exercise, you will create a load-balanced Azure Resource Group in Visual Studio 2017 and deploy it to Microsoft Azure. Confirm the deployment of the load-balanced virtual machines in the Microsoft Azure web portal.

Use the below tables for the required parameters of the Azure Resource Group configurations. Be sure to add commas at the end of lines when additional values are needed.

LoadBalancedVirtualMachine.json Configuration Parameters:

"imageSKU"

Parameter	Value
defaultValue	"2019-Datacenter"
allowedValues	"2019-Datacenter"

Make sure you add a comma after the last value prior to adding a new value.

"variables"

Parameter	Value
vmNamePrefix	"LBVMCAP"

Deploy to Resource Group parameters:

Parameter	Value
Subscription	ASD Developer 1
Resource group	armVSLab-lodxxxxxx
Deployment template	loadBalancedVirtualMachine.parameters.json

Template parameters file:

Parameter	Value
adminUsername	AdminUser
adminPassword	P@55word1234
imageSKU	2019-Datacenter
vmSize	Leave the default value.
numberOfInstances	Leave the default value.

Make sure you select the box to save the passwords as plain text in the parameters file.

PreviousNext: Exercise 2: Working with...

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 41 Min Remaining

Instructions Resources Help 100%

Exercise 2: Working with Azure Storage

Create Azure storage accounts

Create Azure Storage accounts using the Microsoft Azure portal and Azure PowerShell. The account names should be unique to Microsoft Azure and contain your student number for reference. After the two accounts are created, view them using either the Microsoft Azure Storage explorer preview or the Microsoft Storage Explorer application. Ensure that both accounts are configured to utilize the secure transfer feature that forces requests to the storage account to only accept secure connections.

Azure Storage Explorer was installed in an earlier exercise. If you need to reinstall Azure Storage Explorer, you can browse to <https://storageexplorer.com>.

Create Azure storage account using the Microsoft Azure portal

The below parameters should be left at their default values during the storage account creation process.

Parameter	Value
Performance	Standard
Account kind	StorageV2 (general-purpose v2)
Replication	Read-access geo-redundant storage (RA-GRS)
Access tier	Hot

Create Azure storage account using the Azure PowerShell

When creating a storage account using Azure PowerShell, append the characters **PS** to the storage account name to denote that it was created using PowerShell rather than the Microsoft Azure portal.

Creating a storage account using PowerShell was completed in a previous module and can be used for reference.

Configure a storage account to use a customer-managed storage service encryption key

The storage account can be configured to use either Microsoft-managed or customer-managed keys to protect the data. In this exercise, you are required to encrypt the data using a customer-managed key. Browse to <https://portal.azure.com> and navigate to the encryption settings of the storage account to create a new key vault.

Encryption

Parameter	Value
Encryption type	Customer Managed Keys
Encryption key	Select from Key vault
Key vault and key	Select a key vault and key

Select key from Azure Key Vault

Create key vault

Project details

Parameter	Value
-----------	-------

Subscription Select your subscription from the drop-down list

Resource group Select your resource group from the drop-down list

Instance details

Parameter	Value
-----------	-------

Key vault name Vault name must only contain alphanumeric characters and dashes and cannot start with a number

Pricing tier Standard

Soft delete Enable

Retention period (days) 90

Purge protection Disable

After all values have been selected or entered, Select **Review + create** then **Create**.

Select key from Azure Key Vault

- Select **Create new** to create a new key.

Create a key

- Select **Generate** from the drop-down list.
- Enter a name for the key that only contains alphanumeric characters and dashes.
- Accept the default values for the remaining attributes and select **Create**.

Select key from Azure Key Vault

- Select **Select**.

Encryption

- Select **Save**.

The customer-managed key is now assigned to the storage account.

For more information about managing keys with the Azure Key Vault in the Microsoft Azure portal, browse to <https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal>.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 40 Min Remaining

Instructions Resources Help 100%

Exercise 3: Calling a Microsoft Azure Automation Runbook with a Webhook

In this exercise, you will create an Automation Account for your resource group using the Microsoft Azure portal. This account will be used to run a webhook that will stop virtual machines in the resource group. After the runbook called **Shutdown-Start-VMs-By-Resource-Group.ps1** has been imported using the Microsoft Azure portal, the webhook will be created and called by the **Client.ps1** file using the administrative PowerShell.

Using the Microsoft Azure portal, navigate to the Automation Account to examine the status of the processed job.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 40 Min Remaining

Instructions Resources Help 100%

Exercise 4: Using Microsoft Azure Recovery Services vault

In this exercise, you will create a recovery services vault using the backupLab-1odXXXXXX resource group and complete the initial backup of VM2 using the Microsoft Azure portal. Once the backup job has been started, monitor the status of the job using the appropriate tool.

All Labs: Microsoft Azure: Infrastructure as a Service - Remote

4 Hr 40 Min Remaining

Instructions Resources Help 100%

Exercise 5: Azure Recovery Services - Files/Folders

Installing backup agent on Azure VM

In this exercise, you will configure VM3 for Microsoft Azure backups and restores. Perform the below tasks in order to configure the Microsoft Azure Recovery Services Agent on VM3.

- Connect to VM3 and download, install and configure the Microsoft Azure Recovery Services Agent using the credentials file for the vault.
- Generate a secure passphrase that will be used to encrypt and decrypt the backups for VM3.
- Back up the VM3 C:\Windows\Help folder using the default settings of the Microsoft Azure Backup application.

Restore data from Azure

In this exercise, you will restore the C:\Windows\Help folder to VM3 from the VM3 backup that you previously completed. Perform the below tasks in order to access and restore the required data.

- Browse the initial backup of VM3.
- Copy the contents of the backup to a folder on the VM3 server.
- Unmount the backup file from VM3.

Congratulations!

You have successfully completed this module. To mark the lab as complete click **End**.