**Azure Storage – Practical Exercises**

Overview

This course includes optional exercises where you can try out the techniques demonstrated in

the course for yourself. This guide lists the steps for the individual exercises.

Setup

If you already have a Microsoft Azure subscription, you can skip this section. Otherwise, follow

these steps to create a free trial subscription. You will need to provide a valid credit card

number for verification, but you will not be charged for Azure services

**CREATE FREE ACCOUNT (IGNORE IF ALREADY DONE)**

1. If you already have a Microsoft account that has not already been used to sign up for a

free Azure trial subscription, you’re ready to get started. If not, don’t worry, just create

a new Microsoft account.

2. After you’ve created a Microsoft account, create your free Microsoft Azure account.

You’ll need to sign-in with your Microsoft account if you’re not already signed in. Then

you’ll need to:

• Enter your cellphone number and have Microsoft send you a text message to

verify your identity.

• Enter the code you have been sent to verify it.

• Provide valid payment details. This is required for verification purposes only –

your credit card won’t be charged for any services you use during the trial

period, and the account is automatically deactivated at the end of the trial

period unless you explicitly decide to keep it active.

**Install Azure PowerShell (if needed)**

**In this exercise, you will install Azure PowerShell.**

If you have already installed Azure PowerShell you can skip this exercise.

1. From your computer, open an elevated PowerShell prompt.

Cmdlets for Resource Manager

2. Run the Install-Module AzureRM command. This will install the AzureRM module which

represents resource management.

3. If you get prompted to install and import the NuGet provider, Type Y and then press the

Enter key.

4. If you are notified that the repository is untrusted, confirm that you want to install the

modules by typing Y and then pressing the Enter key. The installation process will take

several minutes as packages are downloaded and installed.

5. After the download and installation is finished, run the Import-Module AzureRM command.

6. Note: If you receive a message about running scripts on your computer has been disabled,

temporarily change the execution policy:

Set-ExecutionPolicy Unrestricted

After the import command is complete, return the execution policy to restricted.

Set-ExecutionPolicy Restricted

**Module 1 – Planning Storage**

Create a Storage Account(Portal)

In this exercise, you will create a new storage account in the Azure portal. Once created you will

explore some of the basic file management capabilities, including the use of file shares.

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. Click Storage Accounts on the Hub menu.

• If you do not see Storage Accounts on the Hub menu, click More Services.

• Type storage accounts in the filter to reveal the available options for managing

storage accounts in the Azure Portal. Mark Storage Accounts as a favorite to pin it to

your Hub menu.

3. On the Storage accounts blade, if you have any existing storage accounts they will

appear in the list.

4. On the Storage accounts blade, click Add.

5. On the Create storage account blade, fill in the following values to create a new storage

account. Click Create when you are finished entering the information. As you enter the

information take a moment to use the Information icon to view details about the

required information.

• Name: <your choice>

• Deployment model: Resource Manager

• Account kind: General purpose

• Performance: Standard

• Replication: Read-access geo-redundant storage (RA-GRS)

• Storage service encryption: Disabled

• Subscription: <YourSubscription>

• Resource Group: <Create a new resource group>

• Location: <YourLocation>

6. On the menu bar, monitor the alerts for progress as the new storage account is created.

7. On the Hub menu, click Storage accounts. Confirm that the new storage account has

been created.

8. Double-click your storage account and review the options that are available. Review the

storage account Essentials area. Explore the Blobs, Files, Tables, and Queues areas.

**Create a Storage Account (PowerShell)**

**In this exercise, you will create a new storage account using PowerShell.**

1. Open an elevated Windows PowerShell ISE window.

2. Locate cmdlets dealing with the Azure login.

Get-Command \*login\*

3. Read the Help pages on the Login-AzureRmAccount cmdlet. If prompted to update the

help pages, do so.

Get-Help Login-AzureRmAccount -full

4. Login to Azure. When prompted enter your Azure credentials.

Login-AzureRmAccount

5. Locate cmdlets dealing with Azure subscriptions.

Get-Command \*azuresubscriptions\*

6. Use the Get-AzureRmSubscription cmdlet to retrieve your subscription name.

Get-AzureRmSubscription

7. Specify your subscription.

Select-AzureRmSubscription -SubscriptionName <your subscription name>

8. You will need resource group information. Make a note of the ResourceGroupName.

Get-AzureRmResourceGroup

9. You will need SkuName information. This is the replication scheme for the storage

account. Consult the help for applicable choices such as Standard\_RAGRS.

10. Use New-AzureRMStorageAccount to create a new storage account.

New-AzureStorageAccount -Name <your choice> -ResourceGroupName <your

resource group> -Location <your location> -SkuName <replication scheme>

11. Use Get-AzureRmStorageAccount to verify the account was created. Alternatively, you

could return to the portal and refresh the storage account page.

Get-AzureRmStorageAccount

Note: Throughout the course make an effort to try to use this tool. You will find it easy to

use.

**Install Azure Storage Explorer**

**In this exercise, you will install the Microsoft Azure Storage Explorer desktop application,**

**connect to your Azure account, and explore the various options for managing your data in the**

**Azure cloud.**

1. Navigate to the Storage Explorer download site.

2. Download and install the appropriate version (Windows, Mac, or Linux).

3. Launch the tool.

4. In the Connect to Azure Storage window, ensure that the option to sign in using your

Azure account is selected and then click Connect.

5. In the Sign in to your account window, enter your Azure administrative credentials and

then click Sign in. Complete your authentication as needed (for example, if you have

two-factor authentication enabled, you might be prompted for the second factor).

6. On the menu bar, click the person icon for Azure account settings.

7. Your Azure subscriptions for your account will be displayed. Click the checkbox for your

Azure subscription (or click All subscriptions) and then click Apply.

8. Notice that you are able to view Local and Attached storage as well as your subscription

storage.

9. If you followed the previous exercises you should see two storage accounts under your

subscription.

10. Take a moment to browse the storage accounts. You may see diagnostic tables

capturing metric data.

Note: Throughout the course make an effort to try to use this tool. You will find it easy to

use.

**Install AZCopy**

**In this exercise you will install the AzCopy tool and explore the syntax.**

1. Download and install the latest version of AzCopy - http://aka.ms/downloadazcopy.

2. Locate the executable which is typically installed in either

%ProgramFiles(x86)%\Microsoft SDKs\Azure\AzCopy or %ProgramFiles%\Microsoft

SDKs\Azure\AzCopy.

3. Open an elevated Command Prompt and navigate to the AZCopy installation directory.

4. View the Help pages for the utility.

AzCopy /?

5. Read through the examples at the end of the Help page.

Note: Throughout the course make an effort to try to use this tool. You will find it easy to

use.

(SKIP IT FOR TIME BEING)

Module 2 – Virtual Machine Storage

Create a New Windows Virtual Machine (Portal -Optional)

In this exercise, you will create a new virtual machine with the Resource Manager deployment

model. Note: If you already have virtual machine to use for attaching disks you can skip this

exercise.

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click New.

3. On the New blade, search for Server 2012 R2.

4. In the search results, click Windows Server 2012 R2 Datacenter.

5. In the Everything blade, click Windows Server 2012 R2 Datacenter.

6. On the Windows Server 2012 R2 Datacenter blade, notice the default deployment

model is set to Resource Manager. Click Create.

7. On the Create Virtual Machine blade, fill in the following values for basic settings

(substituting your information for the user name, subscription, and location) and click

OK.

• Name: WServer-01

• VM disk type: HDD

• User name: wsadmin

• Password: <your choice

• Subscription: <your subscription>

• Resource group: Create a new one <your choice>

• Location: <Your location>

8. On the Choose a size blade, click View all. Click the A0 Basic size and then click Select.

9. On the Settings blade, review the default options for storage, network, extensions, high

availability, and monitoring. Notice your virtual machine will use a new storage account.

Click OK.

10. On the Summary blade, review the configuration and then click OK.

11. When the VM creation finishes, click Virtual machines in the left pane.

12. In the Virtual machines blade, click the server name for the VM that you deployed.

13. In the WServer-01 blade, click Stop at the top of the blade to stop the VM. This ensures

that you don’t consume resources unnecessarily.

(SKIP IT FOR TIME BEING)

Attach a New Disk (Portal)

In this exercise, you will attach a new disk to an Azure virtual machine. Optionally, you can

upload an existing disk with data from your on-premises data center to Azure and then add that

disk as a data disk to a VM.

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click Virtual machines.

3. Click a virtual machine that you created earlier in this module or previously had created.

4. On the blade, under Settings, click Disks.

5. Notice your choices for Attach new and Attach existing.

6. Notice the OS disk that was created for you. Notice there are no data disks.

7. On the Disks blade, click Attach new.

8. On the Attach new blade, review the list of available settings. Use the information icon

to obtain help about the settings.

9. Fill in the following values and click OK.

• Name: <Your choice>

• Type: HDD

• Size (GiB): 10

• Location: <Select the storage account>

• Host caching: None

10. On the menu bar, monitor the alerts for progress as the new virtual disk is created and

attached to the virtual machine.

11. Verify you have a new data disk attached to your virtual machine.

12. If you have existing disks, experiment with adding those disks to your virtual machine.

(SKIP IT FOR TIME BEING)

Add a New Disk (PowerShell)

In this exercise, you will use PowerShell to add a new (empty) data disk to your VM.

1. Note: This exercise assumes you have logged in and selected your subscritptionas you did in

the first eight steps of the Create a Storage Account (PowerShell) exercise.

2. Open an elevated PowerShell prompt. Consider using the ISE.

3. Retrieve information about your virtual machine.

Get-AzureRmVM -Name <your vm> -ResourceGroupName <your resource group>

This assumes you have logged into Azure and selected your subscription. If you need to

remember how to do this, see Create a Storage Account (PowerShell)

4. Review the information, specifically the disk information. For your existing data disk make a

note of the Uri you will need this in the next step.

5. To add a new 10GB data disk pipe the previous command to Add-AzureDataDisk. (add this

to the previous command).

| Add-AzureRmVmDataDisk -Name <your choice> -DiskSizeInGB 10 -CreateOption empty

-VhdUri <use the Uri with a different disk name>

6. Use Get-AzureRmVm again to review your disk information. Your new disk should display.

7. Use Update-AzureRmVM to deploy your changes. This may take a minute.

Get-AzureRmVM | Update-AzureRmVM

8. Return to the Azure Portal, make sure your virtual machine is started, and then select

Connect.

9. Save the RDP connection file to your Desktop.

10. Double-click the connection file on your Desktop and provide your virtual machine Windows

administrator credentials.

11. Open the Disk Management console.

12. Verify your new disk is shown.

**Work with Files (Portal and Storage Manager)**

**In this exercise, you will explore some of the basic file management capabilities, including the**

**use of file shares.**

Manage files in the portal

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click Storage accounts.

3. Select the storage account you created in Module 1.

4. On the storage account blade, review the list of available management options. Under

File Services, click Files.

5. On the File service blade, click + File Share.

6. On the New file share blade, fill in the following values to create a new file share. Use

the information icon to learn about the quota. Click Create when you are finished

entering the information.

• Name: <your choice>

• Quota: 5

7. On the menu bar, monitor the alerts for progress as the new file share is created.

8. On the File service blade, click your new file share.

9. Notice the ability to Connect, Upload, Add Directory, and Delete share.

10. Select More and then Properties.

11. Copy the file share URL to Notepad. You will need this information to use Azcopy.

12. On the share blade, click Upload.

13. Create a new text file on your desktop. browse to and click the text file. Click Upload.

14. On the menu bar, monitor the alerts for progress as the text file is uploaded.

15. On the file share blade, confirm that the new file appears in the list.

16. Return to the storage account blade, and select your storage account,

17. Under Settings, click Access Keys.

18. Copy the primary key to the Notepad. You will need this information to use Azcopy.

Manage files in Storage Manager

1. When you are finished exploring the new storage account and file share, close the web

page.

2. Switch to Storage Explorer.

3. Navigate to your storage account.

4. Click File Shares. Review the list of available files shares. Ensure your uploaded file is

listed.

5. Notice that you can also right-click on File Shares and Create File Share.

6. As you have time experiment with creating other files shares, download, open, rename,

and delete.

**Manage file with Azcopy**

1. Open a command prompt and navigate to the Azcopy directory.

2. To copy files to your file share use this format:

AzCopy Source:<location of files to copy> /Dest:<file share URL> /Destkey:<access

key>

3. As you have time experiment with other Azcopy functionality such as creating a

directory in your file share and downloading files.

**Work with Files (PowerShell)**

**In this exercise, you will use PowerShell to connect to your Azure storage account, create a new**

**file share, and manage your files in the Azure cloud.**

1. Login in to your account. When prompted enter your Azure administrator credentials.

Login-AzureRmAccount

2. Retrieve the storage account keys and copy them to Notepad. You will need this

information when creating the file share.

Get-AzureRmStorageAccountKey -Name <storage account name> -

ResourceGroupName <resource group name>

3. Create a variable to hold the account context. This will make it easier for the next

commands.

$Context = New-AzureStorageContext -StorageAccountName <storage account name>

-StorageAccountKey <access key 1>

4. Verify the contents of your variable

$Context

5. Create a new file share called Documents.

New-AzureStorageShare –Name Documents –Context $Context

6. Confirm that your file share has been created.

Get-AzureStorageShare –Context $Context

7. In your file share, create a new directory called WorkOrders

New-AzureStorageDirectory -ShareName Documents -Context $Context –Path

WorkOrders

8. Confirm that your new WorkOrders directory has been created.

Get-AzureStorageFile -ShareName Documents -Context $Context

9. Identify a file, and upload it to your new directory.

Set-AzureStorageFileContent -ShareName Documents -Context $Context -Source

<path to upload file> -Path WorkOrders

10. Confirm your file was uploaded to the Workorders directory.

Get-AzureStorageFile -ShareName Documents -Context $Context -Path WorkOrders |

Get-AzureStorageFile

11. As you have time experiment with downloading a file.

(SKIP IT FOR TIME BEING)

Map a File Share - Windows

In this exercise, you will map a file share from the Windows machine. Click here if you need

instructions to create a Windows virtual machine.

1. In the Azure Portal, access to your storage account, choose Settings and then Access

Keys.

2. Read how access keys are used to authenticate your application requests when making

requests to the Azure storage account.

3. Copy the Storage account name and key1 to Notepad. You will need this information

when you map the drive.

4. Navigate to your file share, click ..More, and then click Properties.

5. Copy the file share URL to Notepad.

6. From your client Desktop, open File Explorer, right-click This PC, and then select Map a

Network Drive.

7. In the Map a Network Drive wizard, enter the following then click Finish. The file share

URL must take the form \\<storage URL>\<file share>\. For example,

\\storageaccount.file.core.windows.net\fshare1.

• Drive: z:

• Folder: <the file share URL>

• Connect using different credentials

8. When prompted for credentials:

User: <storage account>

Password: <access key>

9. You should now be connected to your file share and able to access files.

**Module 3 – Unstructured Data**

**Create New Blob Storage (Azure Portal and Storage Explorer)**

**In this exercise, you will create a Blob storage container in the Azure portal. Once created you**

**will connect to your Azure storage account and manage the contents of the Blob storage**

**container by using Microsoft Azure Storage Explorer.**

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click Storage accounts, and then select your storage account.

3. Under BLOB SERVICES, click Containers and click + Container.

4. On the New container blade, type a lowercase name for the new container. In the

dropdown menu for the access type, click Private. Click Create to create the container.

5. On the menu bar, monitor the alerts for progress as the new Blob container is created.

6. On the Blob service blade, confirm your new blob container appears in the list.

7. On the blade, review the available options in the menu bar for managing this container,

such as delete container, properties, and access policy. Notice you do not have the

ability to add blobs to the container.

8. Open the Microsoft Azure Storage Explorer application. If needed, connect to your

Azure account.

9. Under you Azure subscription, navigate to Blob Containers and confirm that your blob

container is available. Note that if you do not see the container you can refresh the view

by hovering your mouse over Blob Containers and clicking on the magnifying glass icon.

10. Select the blob container which should be empty at this time.

11. On the ribbon, click Upload and then click Upload Folder.

12. On the Upload Folder dialog window, click the ellipsis (…), click a folder that contains a

small amount of data, and then click Upload. Monitor the activity log at the bottom of

your screen as the files are uploaded to the container.

13. Once uploaded, navigate through the folder structure. Locate a file and click Download

in the ribbon. Save the file to your desktop.

14. As you have time experiment with other options in Blob storage.

15. As you have time experiment with Azcopy.

**Module 4 – Structured Data**

**Manage Tables (Azure Portal, Storage Explorer, and PowerShell)**

**In this exercise, you will view table information in the portal, use PowerShell to create a table**

**and add entities, and view/edit the table in Storage Explorer.**

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click Storage accounts, and then select your storage account.

3. Click the Azure Table service node. Notice you can only view existing tables. There are

no additional tasks such as create a table, or add items to a table.

4. Before leaving the portal, copy your subscription name, resource group, storage account

name, and storage access key to Notepad. You will need this information in PowerShell.

5. Open an elevated PowerShell ISE window.

6. Login to Azure. When prompted enter your Azure credentials.

Login-AzureRmAccount

7. Specify your subscription.

Select-AzureRmSubscription -SubscriptionName $SubscriptionName

Steps 8 – 14 are demonstrated in the course video for this section. To shorten your

typing, you can retrieve pieces of the sample code from How to add entities. The codes

is spread out in the How to Manage Table Entries section. Be sure to walk through the

code so you know what is happening. Lastly, execute the code to create the Employee

table with four entries.

Note: These steps require PowerShell and some coding knowledge. If this coding is

outside you skill level, simply use Storage Explorer to practice creating a table with

entities.

8. Create a function to add an entity to your table. This table will have a partition key, row

key, employee name, and employee id.

function Add-Entity() {

[CmdletBinding()]

param(

$table,

[String]$partitionKey,

[String]$rowKey,

[String]$name,

[Int]$id

)

$entity = New-Object -TypeName

Microsoft.WindowsAzure.Storage.Table.DynamicTableEntity -ArgumentList

$partitionKey, $rowKey

$entity.Properties.Add("Name", $name)

$entity.Properties.Add("ID", $id)

$result =

$table.CloudTable.Execute([Microsoft.WindowsAzure.Storage.Table.TableOperati

on]::Insert($entity))

}

9. Create variables for each of the following. These are string values.

$StorageAccountName = <your storage account name>

$StorageAccountKey = <your storage account key>

$Ctx = New-AzureStorageContext $StorageAccountName -StorageAccountKey

$StorageAccountKey

$TableName = “Employees”

10. Retrieve the table if it already exists.

$table = Get-AzureStorageTable –Name $TableName -Context $Ctx -ErrorAction Ignore

11. Create a new table if it doesn’t exist.

if ($table -eq $null)

{

$table = New-AzureStorageTable –Name $TableName -Context $Ctx

}

12. Confirm the table exists.

Get-AzureStorageTable -Context $Ctx

13. Use your Add-Entity function to add an employee to the table. Notice you are defining

where the entity is added (partition1, row1).

Add-Entity -Table $table -PartitionKey Partition1 -RowKey Row1 -Name Chris -Id 1

Add-Entity -Table $table -PartitionKey Partition1 -RowKey Row2 -Name Jessie -Id 2

Add-Entity -Table $table -PartitionKey Partition2 -RowKey Row1 -Name Christine -Id 3

Add-Entity -Table $table -PartitionKey Partition2 -RowKey Row2 -Name Steven -Id 4

14. Return to the portal and confirm your table was created.

15. Open Azure Storage Explorer, and locate your table.

16. Notice table features such as copy, new, and delete the table.

17. Open the table and ensure rows are returned.

18. Notice record features such as create a new record and delete a record.

19. As you have time experiment with tables and entities.

Manage Queues (Azure Portal, Storage Explorer, and PowerShell)

**In this exercise, you will view queue information in the portal and in Storage Explorer, and use**

**PowerShell to add a message to your queue.**

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click Storage accounts, and then select your storage account.

3. Click the Azure Queue service node. Notice you can only view existing queues. There are

no additional tasks such as create a queue, or add items to a queue.

4. Open Storage Explorer.

5. Locate your storage account and the queues node.

6. Create a new queue called messages.

7. Insert a new message in the queue

Call customer

8. Notice the message has an Id, Insertion time, and Expiration time.

9. Double-click the message and change the Expiration time.

10. Return to the portal and confirm your message queue was created.

11. Open an elevated PowerShell ISE window.

12. Login to Azure. When prompted enter your Azure credentials.

Login-AzureRmAccount

13. Specify your subscription.

Select-AzureRmSubscription -SubscriptionName $SubscriptionName

Steps 8 – 14 are demonstrated in the course video for this section. To shorten your

typing, retrieve the sample code from How to manage Azure queues and queue

messages. After pasting in the code, walk through each section to ensure you know

what is happening. Lastly, execute the code to retrieve your existing queue and add a

new message.

14. Retrieve your messages queue. This assumes you have established your context in the

previous Tables exercise.

$QueueName = "messages"

$Queue = Get-AzureStorageQueue –Name $QueueName –Context $Ctx

15. View the queue and verify you have at least one message. Notice the class,

Microsoft.WindowsAzure.Storage.Queue.CloudQueue.

$queue

16. Check to ensure the queue exists, and then add another message.

if ($Queue -ne $null) {

$QueueMessage = New-Object -TypeName

Microsoft.WindowsAzure.Storage.Queue.CloudQueueMessage -ArgumentList “my

second message”

$Queue.CloudQueue.AddMessage($QueueMessage)

}

17. After your code executes successfully, return to Storage Explorer.

18. Refresh your message queue and confirm you new message was added.

**(SKIP IT FOR TIME BEING)**

Module 5 – Managing Storage

Files and Folders Backup

In this exercise, you will set up Azure Backup to backup on-premises files and folders.

Note: If you are having trouble with this lab, return to the course and watch the

demonstration on backing up files and folders.

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click More services.

3. Type recovery services in the filter to reveal the available options for managing recovery

services in the Azure Portal. Mark Recovery Services vault as a favorite to add it to your

Hub menu.

4. On the Recovery Services vault blade, fill in the following values to create a new

recovery services vault. Click Create when you are finished entering the information.

Note: You must select a resource group with a virtual machine in your location.

• Name: <your choice

• Subscription: <your subscription>

• Resource Group: Create a new resource group <your choice>

• Location: <your location>

5. On the menu bar, monitor the alerts for progress as the new recovery services vault is

created.

6. On the Hub menu, click Recovery Services vault. Confirm that the new recovery services

vault has been created.

7. Select your recovery services vault.

8. On the Settings blade, explore the available options for managing the recovery services

vault, such as backup, site recovery, jobs, and backup policies. Click Backup.

9. For the backup goal, use the following information and then click OK.

• Where is your workload running? On-Premises

• What do you want to backup? Files and Folders {notice the other choices}

10. Click the Click here to prepare your infrastructure for backup to Azure icon.

11. Install the appropriate Backup Agent to your client or server machine and step through

the Wizard.

• Select an installation and cache folder.

• Specify how you want to connect to the Internet.

• Acknowledge any prerequisite software that needs to be installed.

12. While you wait for the backup installatin to complete, download the vault credentials

from the portal. These credentials will be used to register the machine in the vault.

13. When the Wizard finishes, click the Proceed to Registration link.

14. Browse to your vault credentials file.

15. Provide encryption settings for passphrase and location to save the passphrase.

16. Wait for the server registration to complete.

17. When the Microsoft Azure Backup wizard displays, select Schedule Backup.

18. Proceed through the Wizard making your selections.

19. After you have created the backup schedule, select Backup Now. Monitor the backup to

ensure it succeeds.

20. Return the portal and your recovery services vault.

21. Confirm that your files and folders have been backed up and are now safely in the vault.

**(SKIP IT FOR TIME BEING)**

**Virtual Machine Backup**

**In this exercise, you will set up Azure Backup to backup a virtual machine. For this exercise you**

**will need a virtual machine.**

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. On the Hub menu, click More services.

3. Click Recovery Services vault.

4. On the Recovery Services vault blade, click Add.

5. On the Recovery Services vault blade, fill in the following values to create a new

recovery services vault. Click Create when you are finished entering the information.

Note: You must select a resource group with a virtual machine in your location.

• Name: <your choice

• Subscription: <your subscription>

• Resource Group: Create a new resource group <your choice>

• Location: <your location>

6. On the menu bar, monitor the alerts for progress as the new recovery services vault is

created.

7. On the Hub menu, click Recovery Services vault. Confirm that the new recovery services

vault has been created.

8. Select your recovery services vault.

9. On the Settings blade, explore the available options for managing the recovery services

vault, such as backup, site recovery, jobs, and backup policies. Click Backup.

10. For the backup goal, use the following information and then click OK.

• Where is your workload running? Azure

• What do you want to backup? Virtual machine

11. On Backup policy, notice there are two backup policies: DefaultPolicy and Create New.

12. Select Create New and take a minute to review the different frequency and retention

settings.

13. Select DefaultPolicy, and click OK.

14. For items to backup, click the checkbox next to your virtual machine and then click

Select.

15. Click OK to complete the backup configuration.

16. On the menu bar, monitor the alerts for progress as the new backup configuration is

deployed.

17. On the Recovery Services vault page you can also monitor your backup job.

**(SKIP IT FOR TIME BEING)**

**Storage Analytics(Portal)**

**In this exercise, you will enable storage monitoring and customize storage metrics and logging.**

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. In the Azure Portal, select Storage Accounts.

3. Double-click on a subscription where you’d like to configure storage analytics.

4. Select Diagnostics under the Monitoring blade.

5. By default, Blob, Table, Queue, and File metrics are enabled.

6. By default, Blob, Table, and Queue logging is not enabled. Notice there is no File logging.

7. Notice the Retention is set to zero. Experiment with the slider, that goes up to 365

days.

8. Change to the Blob Service blade, and select Metrics.

9. On the table, click Edit (top right corner).

10. Experiment as you like with selecting or removing the different metrics that are

available. Also, notice you can change the time range and chart type.

11. Below the table notice smaller graphs (egress, latency, and success) that can be pinned

to your dashboard.

12. As you have time review the File Service, Table Service, and Queue Service Metrics.

13. On the Storage Account Monitoring blade, select Alert Rules.

14. Click Add Alert.

15. On Add alert rule page, review the different Metrics that are available. These are the

same metrics you saw earlier.

16. Review the different Conditions and Periods that can be set.

17. Notice the Email owners, contributors, and readers checkbox.

18. As you have time and interest, create an alert.

**Shared Access Signature (Portal)**

**In this exercise, you will create a Shared Access Signature (SAS) for accessing a storage object.**

1. Navigate to the new Azure Portal at https://portal.azure.com and sign in.

2. Access your storage account, and under Settings select Shared access signature.

3. Read about the SAS and review the options. Notice you can create a SAS for a very

specific object such as a Blob container, or yo can create a SAS that accessing all types of

object in your storage account. Also notice you can specify the Allowed permissions and

the Start and expiry date/times.

4. Give a file object read access. Be sure to allow access during today’s timeframe.

5. Click Generate SAS and notice the SAS token and service URLs that are created.

6. Look closely at the SAS token. Notice the different parts including start time (st), expiry

time (se), resource (sr), and signature (sig).

7. Copy the SAS token to Notepad.

8. Locate a file object in your storage account, and using Properties obtain the file URL.

9. Append the SAS token to the file URL and you should be able to access the file in a

browser window.

10. As you have time, experiment with other settings.