**Module 7: Azure Storage**

**Exercise 1: Manage Azure Storage**

#### Task 1: Provision the lab environment

In this task, you will deploy an Azure virtual machine that you will use later in this lab.

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.

**Note**: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and click **Create storage**.

1. In the toolbar of the Cloud Shell pane, click the **Upload/Download files** icon, in the drop-down menu, click **Upload** and upload the files **az104-07-vm-template.json** and **az104-07-vm-parameters.json** into the Cloud Shell home directory.
2. From the Cloud Shell pane, run the following to create the resource group that will be hosting the virtual machine (replace the [Azure\_region] placeholder with the name of an Azure region where you intend to deploy the Azure virtual machine):

*$location = '[Azure\_region]'*

*$rgName = 'az104-07-rg0'*

*New-AzResourceGroup -Name $rgName -Location $location*

1. From the Cloud Shell pane, run the following to deploy the virtual machine by using the uploaded template and parameter files:

*New-AzResourceGroupDeployment `*

*-ResourceGroupName $rgName `*

*-TemplateFile $HOME/az104-07-vm-template.json `*

*-TemplateParameterFile $HOME/az104-07-vm-parameters.json `*

*-AsJob*

**Note**: Do not wait for the deployments to complete, but proceed to the next task.

1. Close the Cloud Shell pane.

#### Task 2: Create and configure Azure Storage accounts

In this task, you will create and configure an Azure Storage account.

1. In the Azure portal, search for and select **Storage accounts**, and then click **+ Add**.
2. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **the name of a new resource group az104-07-rg1** |
| Storage account name | **any globally unique name between 3 and 24 in length consisting of letters and digits** |
| Location | **the name of an Azure region where you can create an Azure Storage account** |
| Performance | **Standard** |
| Account kind | **Storage (general purpose v2)** |
| Replication | **Read-access geo-redundant storage (RA-GRS)** |

1. Click **Next: Advanced > then click Next: Networking >**, on the **Networking** tab of the **Create storage account** blade, review the available options, accept the default option **Enable Public access from all networks** and click **Review + create,** wait for the validation process to complete and click **Create**.

**Note**: Wait for the Storage account to be created. This should take about 2 minutes.

1. On the deployment blade, click **Go to resource** to display the Azure Storage account blade.
2. On the Azure Storage account blade, in the **Settings** section, click **Configuration**.
3. Click **Upgrade** to change the Storage account kind from **Storage (general purpose v1)** to **StorageV2 (general purpose v2)**.
4. On the **Upgrade storage account** blade, review the warning stating that the upgrade is permanent and will result in billing charges, in the **Confirm upgrade** text box, type the name of the storage account, and click **Upgrade**.

**Note**: You have the option to set the account kind to **StorageV2 (general purpose v2)** at the provisioning time. The previous two steps were meant to illustrate that you also have the option to upgrade existing general purpose v1 accounts.

**Note**: **StorageV2 (general purpose v2)** offers a number of features, such as, for example, access tiering, not available in with general purpose v1 accounts.

**Note**: Review the other configuration options, including **Access tier (default)**, currently set to **Hot**, which you can change, the **Performance**, currently set to **Standard**, which can be set only during account provisioning, and the **Identity-based Directory Service for Azure File Authentication**, which requires Azure Active Directory Domain Services.

1. On the Storage account blade, in the **Settings** section, click **Geo-replication** and note the secondary location. Click the **View all** link under the **Storage endpoints** label and review the **Storage account endpoints** blade.

**Note**: As expected, the **Storage account endpoints** blade contains both primary and secondary endpoints.

1. Switch to the Configuration blade of the Storage account and, in the **Replication** drop-down list, select **Geo-redundant storage (GRS)** and save the change.
2. Switch back to the **Geo-replication** blade and note that the secondary location is still specified. Click the **View all** link under the **Storage endpoints** label and review the **Storage account endpoints** blade.

**Note**: As expected, the **Storage account endpoints** blade contains only primary endpoints.

1. Display again the **Configuration** blade of the Storage account, in the **Replication** drop-down list select **Locally redundant storage (LRS)** and save the change.
2. Switch back to the **Geo-replication** blade and note that, at this point, the Storage account has only the primary location.
3. Display again the **Configuration** blade of the Storage account and set **Access tier (default)** to **Cool**.

**Note**: The cool access tier is optimal for data which is not accessed frequently.

#### Task 3: Manage blob storage

In this task, you will create a blob container and upload a blob into it.

1. On the Storage account blade, in the **Blob service** section, click **Containers**.
2. Click **+ Container** and create a container with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-07-container** |
| Public access level | **Private (no anonymous access)** |

1. In the list of containers, click **az104-07-container** and then click **Upload**.
2. Browse to **LICENSE** on your lab computer and click **Open**.
3. On the **Upload blob** blade, expand the **Advanced** section and specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Authentication type | **Account key** |
| Blob type | **Block blob** |
| Block size | **4 MB** |
| Access tier | **Hot** |
| Upload to folder | **licenses** |

**Note**: Access tier can be set for individual blobs.

1. Click **Upload**.

**Note**: Note that the upload automatically created a subfolder named **licenses**.

1. Back on the **az104-07-container** blade, click **licenses** and then click **LICENSE**.
2. On the **licenses/LICENSE** blade, review the available options.

**Note**: You have the option to download the blob, change its access tier (it is currently set to **Hot**), acquire a lease, which would change its lease status to **Locked** (it is currently set to **Unlocked**) and protect the blob from being modified or deleted, as well as assign custom metadata (by specifying an arbitrary key and value pairs). You also have the ability to **Edit** the file directly within the Azure portal interface, without downloading it first. You can also create snapshots, as well as generate a SAS token (you will explore this option in the next task).

#### Task 4: Manage authentication and authorization for Azure Storage

In this task, you will configure authentication and authorization for Azure Storage.

1. On the **licenses/LICENSE** blade, on the **Overview** tab, click **Copy to clipboard** button next to the **URL** entry.
2. Open another browser window by using InPrivate mode and navigate to the URL you copied in the previous step.
3. You should be presented with an XML-formatted message stating **ResourceNotFound** or **PublicAccessNotPermitted**.

**Note**: This is expected, since the container you created has the public access level set to **Private (no anonymous access)**.

1. Close the InPrivate mode browser window, return to the browser window showing the **licenses/LICENSE** blade of the Azure Storage container, and switch to the the **Generate SAS** tab.
2. On the **Generate SAS** tab of the **licenses/LICENSE** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Permissions | **Read** |
| Start date | **yesterday’s date** |
| Start time | **current time** |
| Expiry date | **tomorrow’s date** |
| Expiry time | **current time** |
| Allowed IP addresses | **leave blank** |
| Allowed protocols | **HTTP** |
| Signing key | **Key 1** |

1. Click **Generate SAS token and URL**.
2. Click **Copy to clipboard** button next to the **Blob SAS URL** entry.
3. Open another browser window by using InPrivate mode and navigate to the URL you copied in the previous step.

**Note**: If you are using Microsoft Edge or Internet Explorer, you should be presented with the **The MIT License (MIT)** page. If you are using Chrome, Microsoft Edge (Chromium) or Firefox, you should be able to view the content of the file by downloading it and opening it with Notepad.

**Note**: This is expected, since now your access is authorized based on the newly generated the SAS token.

**Note**: Save the blob SAS URL. You will need it later in this lab.

1. Close the InPrivate mode browser window, return to the browser window showing the **licenses/LICENSE** blade of the Azure Storage container, and from there, navigate back to the **az104-07-container** blade.
2. Click the **Switch to the Azure AD User Account** link next to the **Authentication method** label.

**Note**: At this point, you no longer have access to the container.

1. On the **az104-07-container** blade, click **Access Control (IAM)**.
2. In the **Add** section, click **Add a role assignment**.
3. On the **Add role assignment** blade, specify the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Role | **Storage Blob Data Owner** |
| Assign access to | **Azure AD user, group, or service principal** |
| Select | **the name of your user account** |

1. Save the change and return to the **Overview** blade of the **az104-07-container** container and verify that you can access to container again.

**Note**: It might take about 5 minutes for the change to take effect.

#### Task 5: Create and configure an Azure Files shares

In this task, you will create and configure Azure Files shares.

**Note**: Before you start this task, verify that the virtual machine you provisioned in the first task of this lab is running.

1. In the Azure portal, navigate back to the blade of the storage account you created in the first task of this lab and, in the **File service** section, click **File shares**.
2. Click **+ File share** and create a file share with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-07-share** |
| Quota | **1024** |

1. Click the newly created file share and click **Connect**.
2. On the **Connect** blade, ensure that the **Windows** tab is selected, and click **Copy to clipboard**.
3. In the Azure portal, search for and select **Virtual machines**, and, in the list of virtual machines, click **az104-07-vm0**.
4. On the **az104-07-vm0** blade, in the **Operations** section, click **Run command**.
5. On the **az104-07-vm0 - Run command** blade, click **RunPowerShellScript**.
6. On the **Run Command Script** blade, paste the script you copied earlier in this task into the **PowerShell Script** pane and click **Run**.
7. Verify that the script completed successfully.
8. Replace the content of the **PowerShell Script** pane with the following script and click **Run**:

New-Item -Type Directory -Path 'Z:\az104-07-folder'

New-Item -Type File -Path 'Z:\az104-07-folder\az-104-07-file.txt'

1. Verify that the script completed successfully.
2. Navigate back to the **az104-07-share** file share blade, click **Refresh**, and verify that **az104-07-folder** appears in the list of folders.
3. Click **az104-07-folder** and verify that **az104-07-file.txt** appears in the list of files.

#### Task 6: Manage network access for Azure Storage

In this task, you will configure network access for Azure Storage.

1. In the Azure portal, navigate back to the blade of the storage account you created in the first task of this lab and, in the **Settings** section, click **Firewalls and virtual networks**.
2. Click the **Selected networks** option and review the configuration settings that become available once this option is enabled.

**Note**: You can use these settings to configure direct connectivity between Azure virtual machines on designated subnets of virtual networks and the storage account by using service endpoints.

1. Click the checkbox **Add your client IP address** and save the change.
2. Open another browser window by using InPrivate mode and navigate to the blob SAS URL you generated in the previous task.
3. You should be presented with the content of **The MIT License (MIT)** page.

**Note**: This is expected, since you are connecting from your client IP address.

1. Close the InPrivate mode browser window, return to the browser window showing the **licenses/LICENSE** blade of the Azure Storage container, and open Azure Cloud Shell pane.
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.
4. From the Cloud Shell pane, run the following to attempt downloading of the LICENSE blob from the **az104-07-container** container of the storage account (replace the [blob SAS URL] placeholder with the blob SAS URL you generated in the previous task):

Invoke-WebRequest -URI '[blob SAS URL]'

1. Verify that the download attempt failed.

**Note**: You should receive the message stating **AuthorizationFailure: This request is not authorized to perform this operation**. This is expected, since you are connecting from the IP address assigned to an Azure VM hosting the Cloud Shell instance.

1. Close the Cloud Shell pane.

#### Clean up resources

**Note**: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges.

1. In the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.
2. List all resource groups created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-07\*'*

1. Delete all resource groups you created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-07\*' | Remove-AzResourceGroup -Force -AsJob*

**Note**: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.

**Exercise 2: Implement Azure File Sync**

#### Task 1: Provision the lab environment

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.
4. In the toolbar of the Cloud Shell pane, click the **Upload/Download files** icon, in the drop-down menu, click **Upload** and upload the files **az104-07b-vm-template.json** and **az104-07b-vm-parameters.json** into the Cloud Shell home directory.
5. From the Cloud Shell pane, run the following to create the resource group that will be hosting the virtual machine (replace the [Azure\_region] placeholder with the name of an Azure region where you intend to deploy the Azure virtual machine):

*$location = '[Azure\_region]'*

*$rgName = 'az104-07b-rg0'*

*New-AzResourceGroup -Name $rgName -Location $location*

1. From the Cloud Shell pane, run the following to deploy the virtual machine by using the uploaded template and parameter files:

*New-AzResourceGroupDeployment `*

*-ResourceGroupName $rgName `*

*-TemplateFile $HOME/az104-07b-vm-template.json `*

*-TemplateParameterFile $HOME/az104-07b-vm-parameters.json `*

*-AsJob*

#### Task 2: Create an Azure Storage account and a file share

1. In the Azure portal, search for and select **Storage accounts**, and then click **+ Add**.
2. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **the name of a new resource group az104-07b-rg0** |
| Storage account name | **any globally unique name between 3 and 24 in length consisting of letters and digits** |
| Location | **the name of an Azure region where you can create an Azure Storage account** |
| Performance | **Standard** |
| Account kind | **Storage (general purpose v2)** |
| Replication | **Locally-redundant storage (LRS)** |

1. Click **Next: Advanced > then click Next: Networking >**, on the **Networking** tab of the **Create storage account** blade, review the available options, accept the default option **Enable Public access from all networks** and click **Review + create,** wait for the validation process complete and click **Create**.

**Note**: Wait for the Storage account to be created. This should take about 2 minutes.

1. In the Azure portal, navigate to the blade representing the newly provisioned storage account.
2. From the storage account blade, display its File Shares blade.
3. From the storage account **File shares** blade, create a new file share with the following settings:

* Name: az104-07bshare
* Tier: Transaction optimized

Task 3: Prepare Windows Server 2019 for use with Azure File Sync

1. In the Azure portal, navigate to the **az104-07b-vm1** blade.
2. From the **az104-07b-vm1** blade, connect to the Azure VM via the RDP protocol and, when prompted to sign in, provide the following credentials:

* Admin Username: **Student**
* Admin Password: **Pa55w.rd1234**

1. Within the RDP session, start a Windows PowerShell session as administrator.
2. From the Windows PowerShell console, install the latest Az PowerShell module by running the following:

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

Find-PackageProvider -Name NuGet | Install-PackageProvider -Force



Install-Module -Name Az -AllowClobber

**Note: When prompted, confirm that you want to proceed with the installation from PSGallery repository, keep the above PS windows open while the installation finish.**

1. In **Server Manager**, navigate to **File and Storage Services**, locate the data disk attached to the Azure VM, initialize it as a **GPT** disk, and use **New Volume Wizard** to create a single volume occupying entire disk with the following settings:

* Drive letter: S
* File system: NTFS
* Allocation unit size: Default
* Volume label: Data

1. From the Windows PowerShell console, set up a file share by running the following:

$directory = New-Item -Type Directory -Path 'S:\az104-07bshare'

New-SmbShare -Name $directory.Name -Path $directory.FullName -FullAccess 'Administrators' -ReadAccess Everyone

Copy-Item -Path 'C:\WindowsAzure\\*' -Destination $directory.FullName –Recurse

**Note: To populate the file share with sample data, we use content of the C:\WindowsAzure folder, which should contain about 60 MB worth of files**

Task 4: Run Azure File Sync evaluation tool

1. Within the RDP session to the Azure VM, from the Windows PowerShell console, check whether the **S:\az104-07bshare** file share does not have any compatibility issues with the Azure File Sync:

Invoke-AzStorageSyncCompatibilityCheck -Path 'S:\az104-07bshare'

1. Review the results and verify that no compatibility issues have been found.

Task 5: Deploy the Storage Sync Service

1. Within the RDP session to the Azure VM, in Server Manager, navigate to the Local Server view and turn off temporarily **IE Enhanced Security Configuration**.
2. Within the RDP session download Microsoft Edge Browser from this link <https://www.microsoft.com/en-us/edge> then install it.
3. Within the RDP session to the Azure VM, start Microsoft Edge, browse to the Azure portal at [**http://portal.azure.com**](http://portal.azure.com) and sign in by using the same Microsoft account you used previously in this lab.
4. In the Azure portal, navigate to the **New** blade.
5. From the **New** blade, search Azure Marketplace for **Azure File Sync**.
6. Use the list of search results to navigate to the **Deploy Azure File Sync** blade.
7. From the **Deploy Azure File Sync** blade, create a Storage Sync Service with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **the name of a new resource group az104-07b-rg1** |
| Name | **az104-07b-ss** |
| Region | **the name of an Azure region where you can create an Azure Storage account** |

Task 6: Install the Azure File Sync Agent

1. Within the RDP session, start another instance of Microsoft Edge, browse to Microsoft Download Center at [**https://go.microsoft.com/fwlink/?linkid=858257**](https://go.microsoft.com/fwlink/?linkid=858257) and download the Azure File Sync Agent Windows Installer file **StorageSyncAgent\_WS2019.msi**.
2. Once the download completes, run the Storage Sync Agent Setup wizard with the default settings to install Azure File Sync Agent.
3. After the Azure File Sync agent installation completes, the **Azure File Sync - Server Registration** wizard will automatically start.

Task 7: Register the Windows Server with Storage Sync Service

1. From the initial page of the **Azure File Sync - Server Registration** wizard, sign in by using the same Microsoft account you used previously in this lab.
2. Tenant ID
3. On the **Choose a Storage Sync Service** page of the **Azure File Sync - Server Registration** wizard, specify the following settings to register:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Tenant ID | **the tenant ID of the Azure AD subscription** |
| Resource group | **the name of a new resource group az104-07b-rg1** |
| Storage Sync Service | **az104-07b-ss** |

1. When prompted, sign in again by using the same Microsoft account you used previously in this lab.

Task 8: Create a sync group and a cloud endpoint

1. Within the RDP session to the Azure VM, in the Azure portal, navigate to the **az104-07b-ss** Storage Sync Service blade.
2. From the **az104-07b-ss** Storage Sync Service blade, navigate to the **Sync group** blade and create a new sync group with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Sync group name | **az104-07b-syncgroup1** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Storage account | the resource id of the storage account you created in the previous exercise |
| Azure File Share | **az104-07bshare** |

Task 9: Create a server endpoint

1. Within the RDP session to the Azure VM, in the Azure portal, from **az104-07b-ss** Storage Sync Service blade, navigate to the **az104-07b-syncgroup1** blade.
2. From the **az1000202b-syncgroup1** blade, navigate to the **Add server endpoint** blade and create a new server endpoint with the following settings:

* Registered server: **az104-07b-vm1**
* Path: **S:\az104-07bshare**
* Cloud Tiering: **Enabled**
  + - Always preserve the specified percentage of free space on the volume: **15**
    - Only cache files that were accessed or modified within the specified number of days: **30**

Task 10: Validate Azure File Sync operations

1. Within the RDP session to the Azure VM, in the Azure portal, monitor the health status of the server endpoint **az104-07b-vm1** on the **az104-07b-syncgroup1** blade, as it changes from **Provisioning** to **Pending** and, eventually, to a green checkmark.

**Note: You should be able to proceed to the next step after a few minutes.**

1. In the Azure portal, navigate to the blade for the storage account you created earlier in the lab, switch to the **Files** tab and then click **az104-07bshare**.
2. On the **az104-07bshare** blade, click **Connect**.
3. From the **Connect** blade, copy into Clipboard the PowerShell commands that connect to the file share from a Windows computer.
4. Within the RDP session, start a **Windows PowerShell ISE** session.
5. From the Windows PowerShell ISE session, open the script pane and paste into it the content of your local Clipboard.
6. Execute the script and verify that its output confirms successful mapping of the Z: drive to the Azure Storage File Service share.
7. Within the RDP session, start File Explorer, navigate to the Z: drive, and verify that it contains the same content as **S:\az104-07bshare**
8. Display the Properties window of individual folders on the Z: drive, review the Security tab, and note that the entries represent NTFS permissions assigned to the corresponding folders on the S: drive.

Clean up resources

1. In the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.
2. List all resource groups created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-07\*'*

1. Delete all resource groups you created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-07\*' | Remove-AzResourceGroup -Force -AsJob*

**Note: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.**

**Exercise 3: Configure static website hosting**

#### Task 1: Provision the lab environment

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.
4. From the Cloud Shell pane, run the following to create the resource group that will be hosting the virtual machine (replace the [Azure\_region] placeholder with the name of an Azure region where you intend to deploy the Azure virtual machine):

*$location = '[Azure\_region]'*

*$rgName = 'az104-07c-rg0'*

*New-AzResourceGroup -Name $rgName -Location $location*

1. Close the Cloud Shell pane.

#### Task 2: Create and configure Azure Storage accounts

In this task, you will deploy a Static website into the Azure Store Account.

1. In the Azure portal, search for and select **Storage accounts**, and then click **+ Add**.
2. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **the name of a new resource group az104-07c-rg0** |
| Storage account name | **any globally unique name between 3 and 24 in length consisting of letters and digits** |
| Location | **the name of an Azure region where you can create an Azure Storage account** |
| Performance | **Standard** |
| Account kind | **Storage (general purpose v2)** |
| Replication | **Locally-redundant storage (LRS)** |

1. Click **Next: Advanced > then click Next: Networking >**, on the **Networking** tab of the **Create storage account** blade, review the available options, accept the default option **Enable Public access from all networks** and click **Review + create,** wait for the validation process to complete and click **Create**.

**Note**: Wait for the Storage account to be created. This should take about 2 minutes.

1. On the deployment blade, click **Go to resource** to display the Azure Storage account blade.
2. On the Azure Storage account blade, in the **Data storage** section, click **Containers**.
3. On the **Containers** click **+ Container** with the following settings, then click **Create**:

* Name: $web
* Public access level: Private (no anonymous access)

1. On the Azure Storage account blade, in the **Data management** section, click **Static website** and then click **Enabled**, enter the following settings to configure a Static website then click **Save**:

* Index document name: index.html
* Error document path: 404.html

1. Take note the URL assigned as primary endpoint.
2. Open any Internet browser and then enter the URL noted above.

#### Clean up resources

1. In the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.
2. List all resource groups created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-07\*'*

1. Delete all resource groups you created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-07\*' | Remove-AzResourceGroup -Force -AsJob*

**Note: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.**