**LABS Day 2**

Version 1

**Lab 1 A**

**Get started with Storage Explorer**

* ‎**Overview**

Azure Storage Explorer is a standalone app that enables you to easily work with Azure Storage data on Windows, macOS, and Linux. In this lab, you learn several ways of connecting to and managing your Azure storage accounts.

**Prerequisites**

* [Windows](https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows#tabpanel_Ex4van7STS_windows)
* [macOS](https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows#tabpanel_Ex4van7STS_macos)
* [Linux](https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows#tabpanel_Ex4van7STS_linux)

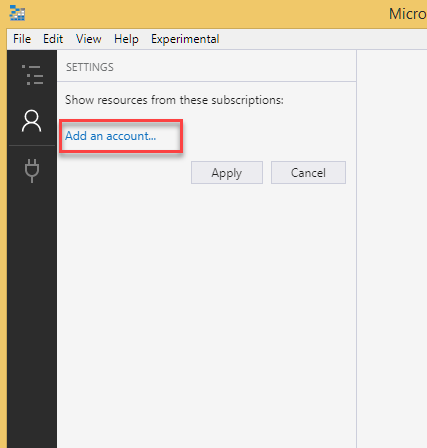
Azure Storage Explorer is supported on the following versions of Windows:

* Windows 10 (recommended)
* Windows 8
* Windows 7

**Task 1** **Connect to a storage account or service**

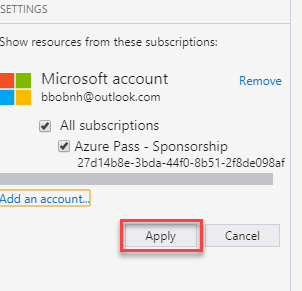
Prequiste: [Download and install Storage Explorer](https://www.storageexplorer.com/)

1. Click the Add an Account button if yours is not already been added

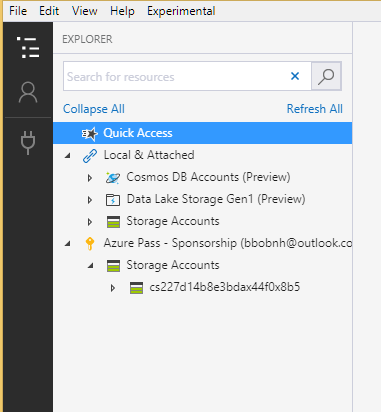


2. Choose **Add an Azure Account**, then click **Sign in..**

3. After signing in click **Apply**



Now you have access to your storage accounts in your subscription



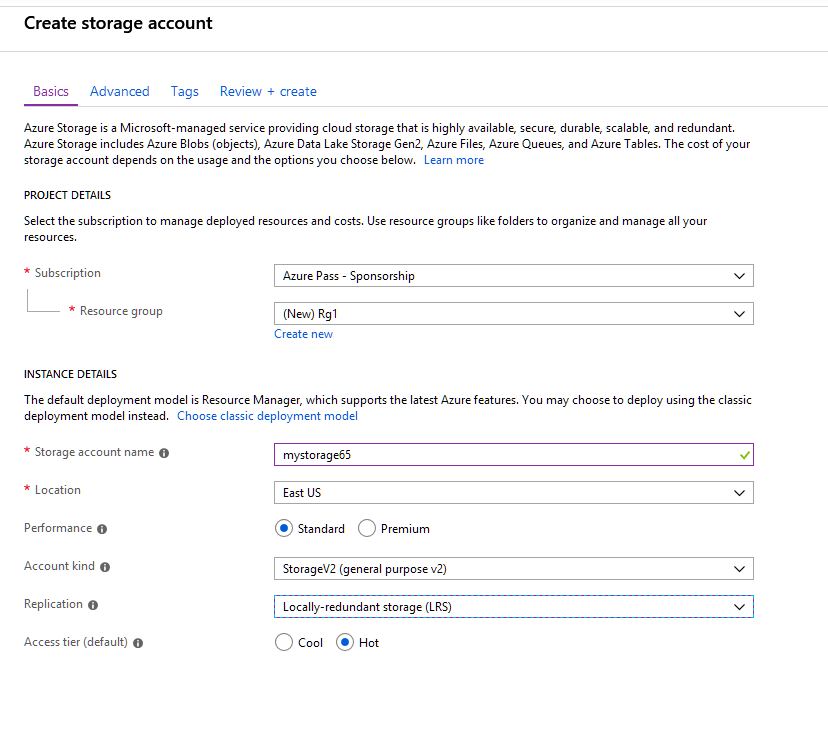
**Task 2 Attach or detach an external storage account**

With Storage Explorer, you can attach to external storage accounts so that storage accounts can be easily shared. This section explains how to attach to (and detach from) external storage accounts.

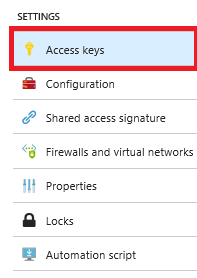
**Get the storage account credentials**

To share an external storage account, the owner of that account must first get the credentials (account name and key) for the account and then share that information with the person who wants to attach to said account. You can obtain the storage account credentials via the Azure portal by doing the following steps:

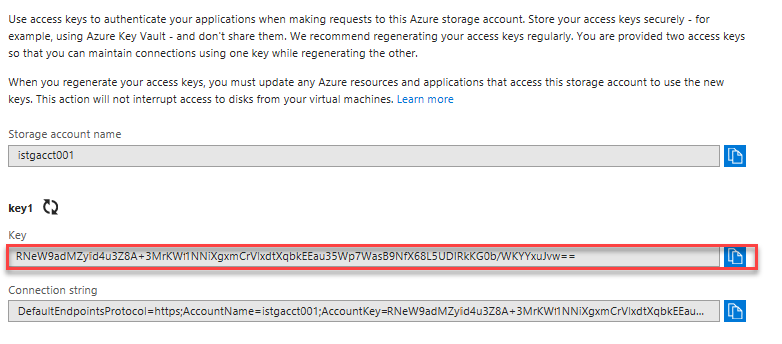
1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Select **Browse**.
3. Select **Storage Accounts**.
4. In the list of **Storage Accounts**, select the desired storage account. Or create a new storage account



1. Click **Review+Create** to create the storage account
2. Select the Storage account you just created, then under **Settings**, select **Access keys**.



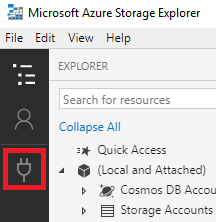
1. Copy the **Storage account name** and **key1**.



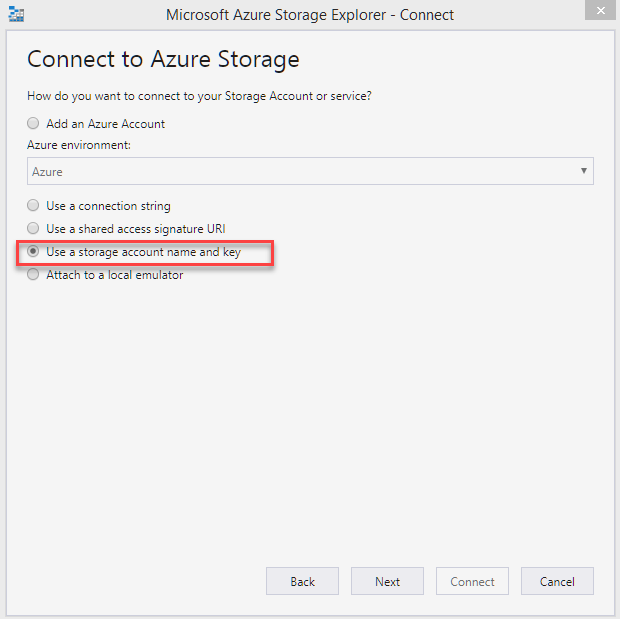
**Task 3 Attach to an external storage account**

To attach to an external storage account, you need the account's name and key. The "Get the storage account credentials" section explains how to obtain these values from the Azure portal. However, in the portal, the account key is called **key1**. So, when Storage Explorer asks for an account key, you enter the **key1** value.

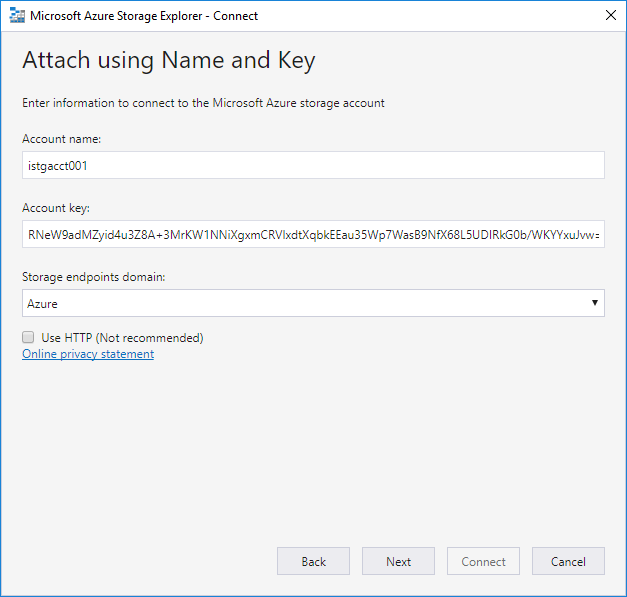
1. In Storage Explorer, open the **Connect Dialog**.



1. In the **Connect Dialog**, choose **Use a storage account name and key**



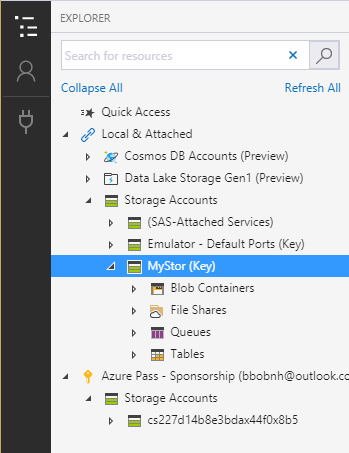
1. Paste your account name in the **Account name** text box, and paste your account key (the **key1** value from the Azure portal) into the **Account key** text box, and then select **Next**.



**Note**

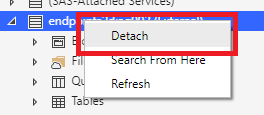
To use a name and key from a national cloud, use the **Storage domain:** dropdown to select the appropriate endpoints domain:

1. Select **Next**.
2. Select **Connect**.
3. After the storage account has successfully been attached, the storage account is displayed with **(External)** appended to its name.



**Task 4 Detach from an external storage account**

1. Right-click the external storage account that you want to detach, and then select **Detach**.



1. In the confirmation message, select **Yes** to confirm the detachment from the external storage account.

**Attach a storage account by using a Shared Access Signature (SAS)**

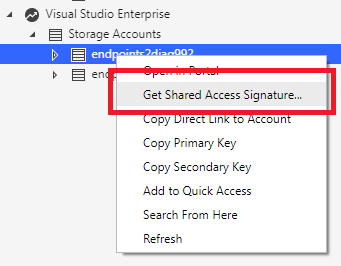
A Shared Access Signature, or [SAS](https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1), lets the admin of an Azure subscription grant temporary access to a storage account without having to provide Azure subscription credentials.

To illustrate this scenario, let's say that UserA is an admin of an Azure subscription, and UserA wants to allow UserB to access a storage account for a limited time with certain permissions:

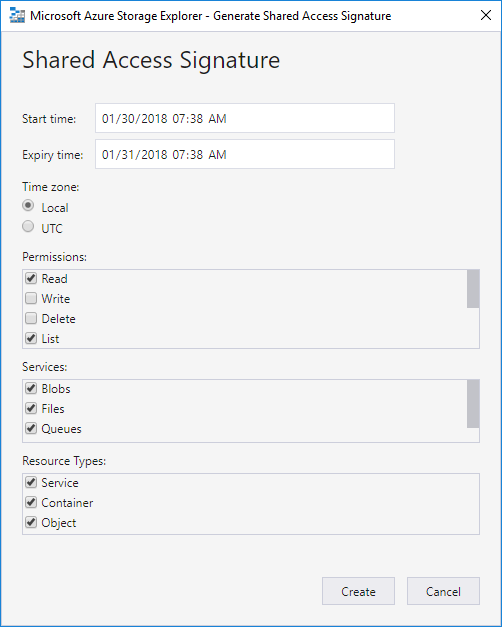
1. UserA generates a SAS connection string for a specific time period and with the desired permissions.
2. UserA shares the SAS with the person (UserB, in this example) who wants access to the storage account.
3. UserB uses Storage Explorer to attach to the account that belongs to UserA by using the supplied SAS.

**Task 5 Generate a SAS connection string for the account you want to share**

1. In Storage Explorer, right-click the storage account you want share, and then select **Get Shared Access Signature...**.



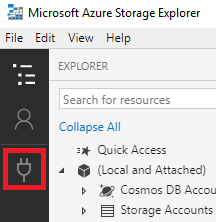
1. In the **Generate Shared Access Signature** dialog box, specify the time frame and permissions that you want for the account, and then click the **Create** button.



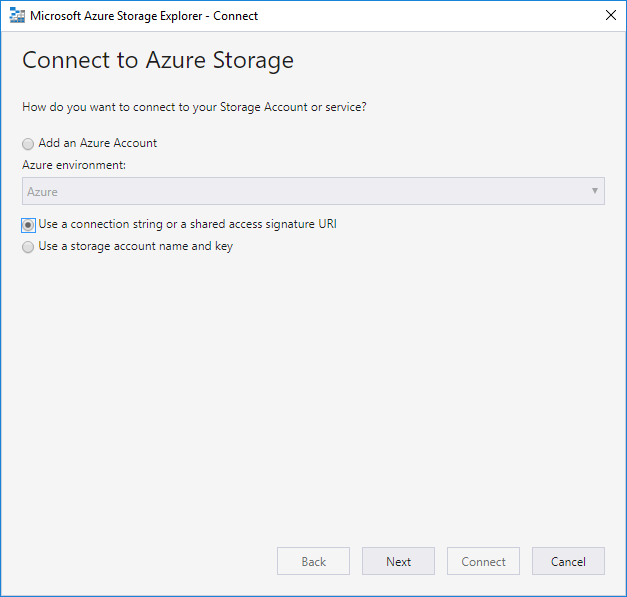
1. Next to the **Connection String** text box, select **Copy** to copy it then click **Close**.

**Task 6 Attach to a storage account by using a SAS Connection String**

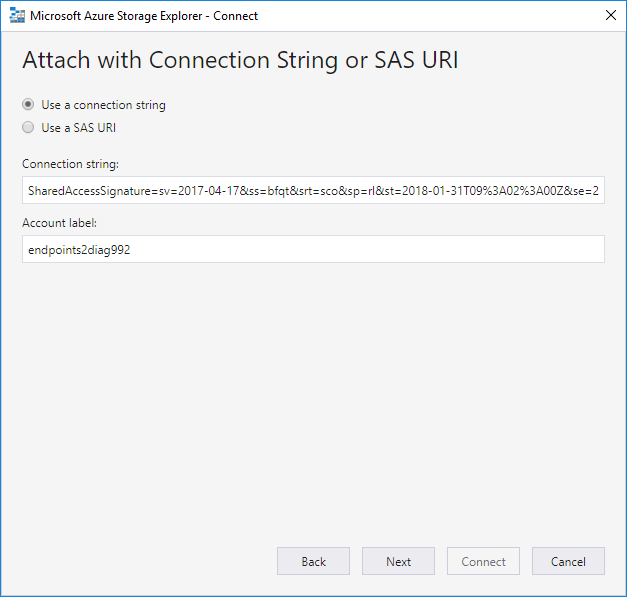
1. In Storage Explorer, open the **Connect Dialog**.



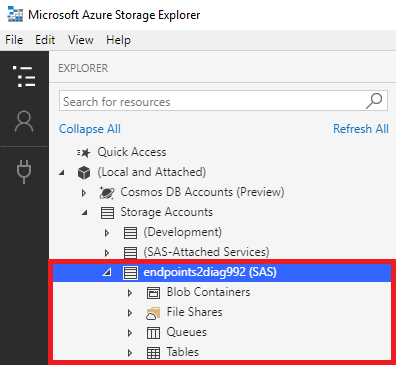
1. In the **Connect Dialog** dialog, choose **Use a connection string** and then click **Next**.



1. Choose **Use a connection string** and paste your connection string into the **Connection string:** field. Click the **Next** button.



1. In the **Connection Summary** dialog box, verify the information. To make changes, select **Back**, and then enter the settings you want.
2. Select **Connect**.
3. After the storage account has successfully been attached, the storage account is displayed with **(SAS)** appended to its name.



**Attach a service by using a Shared Access Signature (SAS)**

The "Attach a storage account by using a SAS" section explains how an Azure subscription admin can grant temporary access to a storage account by generating and sharing a SAS for the storage account. Similarly, a SAS can be generated for a specific service (blob container, queue, table, or file share) within a storage account.

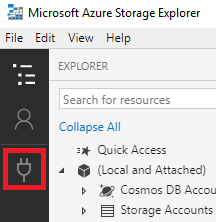
**Generate an SAS for the service that you want to share**

In this context, a service can be a blob container, queue, table, or file share. To generate the SAS for a listed service, see:

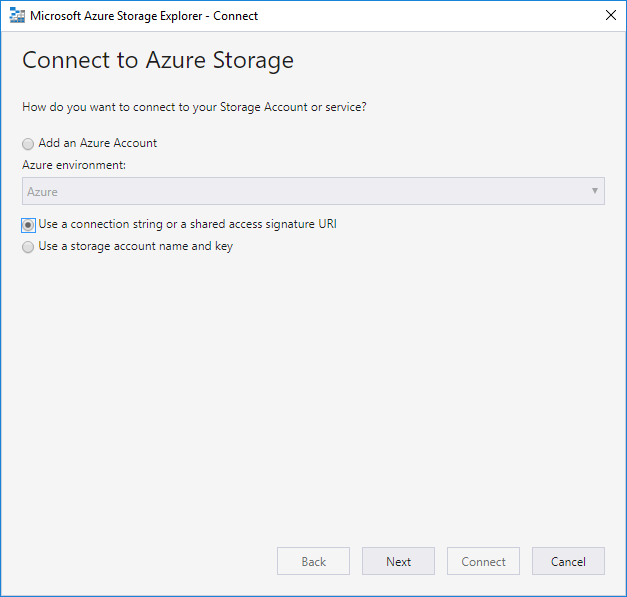
* [Get the SAS for a blob container](https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-explorer-blobs#get-the-sas-for-a-blob-container)

**Task 7 Attach to the shared account service by using a SAS URI**

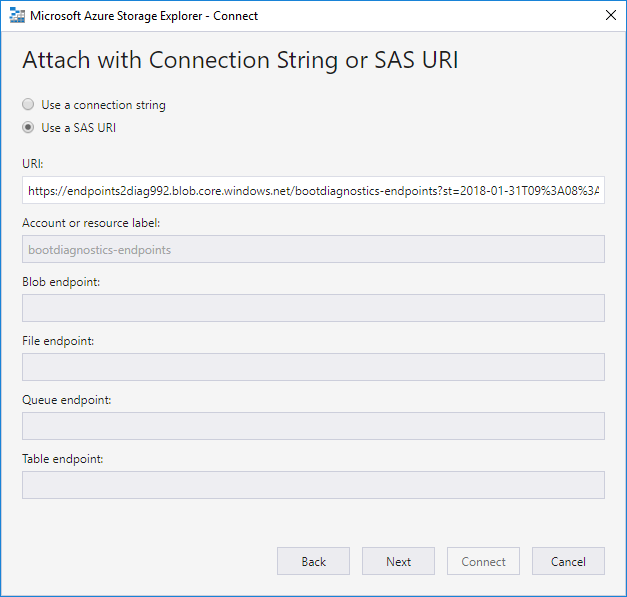
1. In Storage Explorer, open the **Connect Dialog**.



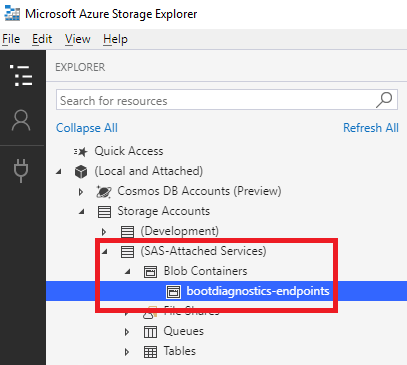
1. In the **Connect Dialog** dialog box, choose **Use a connection string** and then click **Next**.



1. Choose **Use a SAS URI** and paste your URI into the **URI:** field. Click the **Next** button.



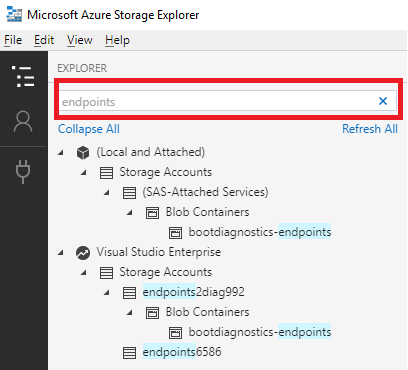
1. In the **Connection Summary** dialog box, verify the information. To make changes, select **Back**, and then enter the settings you want.
2. Select **Connect**.
3. After the service is successfully attached, the service is displayed under the **(SAS-Attached Services)** node.



**Search for storage accounts**

If you need to find a storage resource and do not know where it is, you can use the search box at the top of the left pane to search for the resource.

As you type in the search box, the left pane displays all resources that match the search value you've entered up to that point. For example, a search for **endpoints** is shown in the following screenshot:

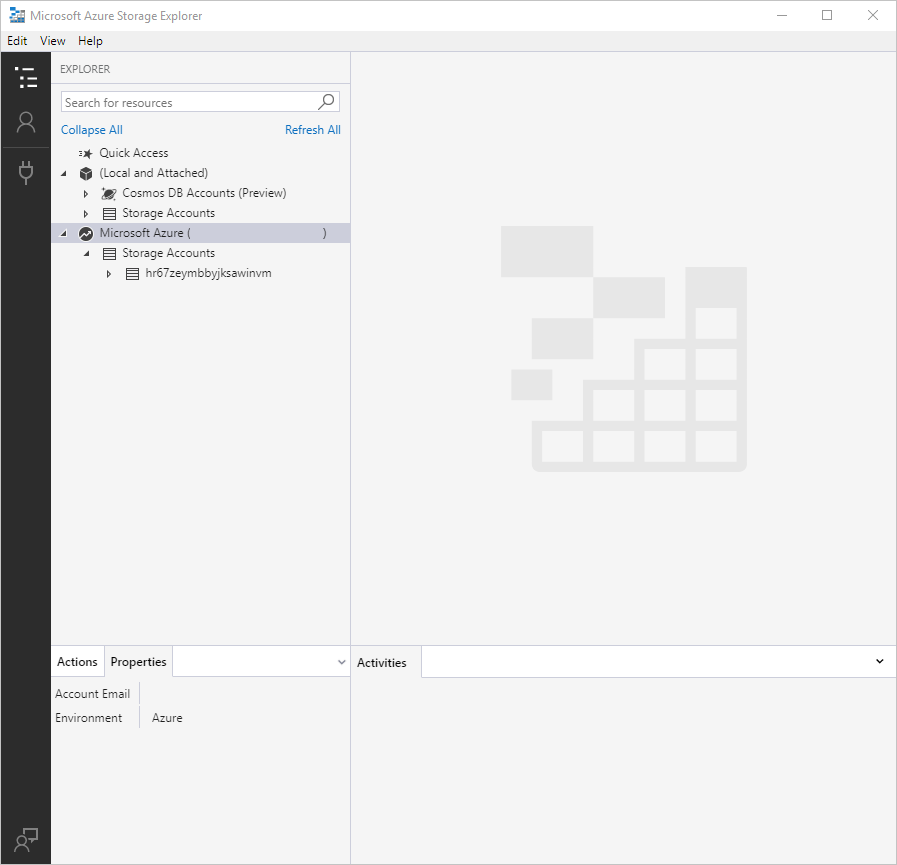


# Lab 1 B

# Use Azure Storage Explorer to create a blob in object storage

* ‎In this lab, you learn how to use [Azure Storage Explorer](https://azure.microsoft.com/features/storage-explorer/) to create a container and a blob. Next, you learn how to download the blob to your local computer, and how to view all of the blobs in a container. You also learn how to create a snapshot of a blob, manage container access policies, and create a shared access signature.

## Task 1 Log in to Storage Explorer

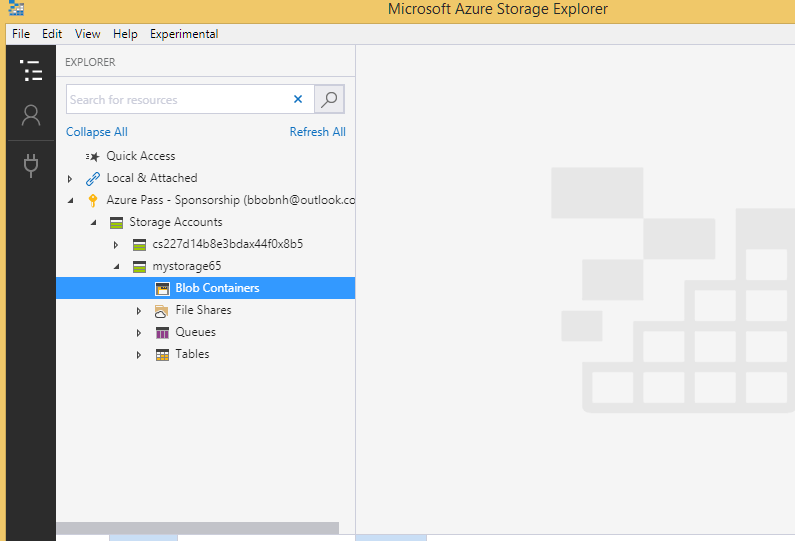


## Task 2 Create a container

Blobs are always uploaded into a container. This allows you to organize groups of blobs like you organize your files on your computer in folders.

To create a container, expand the storage account you created in the proceeding step.

* 1. Select **Blob Containers**, right-click and select **Create Blob Container**. Enter the name for your blob container.



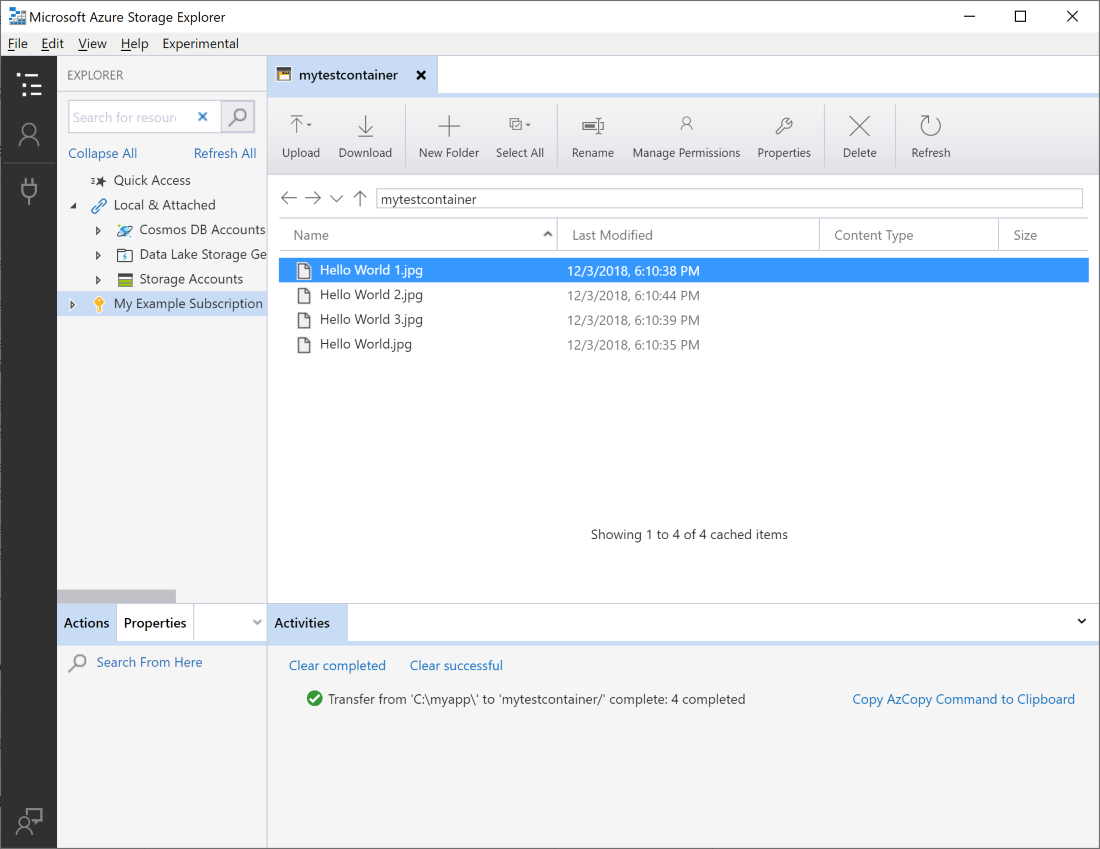
## Task 3 Upload blobs to the container

Blob storage supports block blobs, append blobs, and page blobs. VHD files used to back IaaS VMs are page blobs. Append blobs are used for logging, such as when you want to write to a file and then keep adding more information. Most files stored in Blob storage are block blobs.

* 1. On the container ribbon, select **Upload**. This operation gives you the option to upload a folder or a file.
  2. Choose the files or folder to upload. Select the **blob type**. Acceptable choices are **Append**, **Page**, or **Block** blob.

If uploading a .vhd or .vhdx file, choose **Upload .vhd/.vhdx files as page blobs (recommended)**.

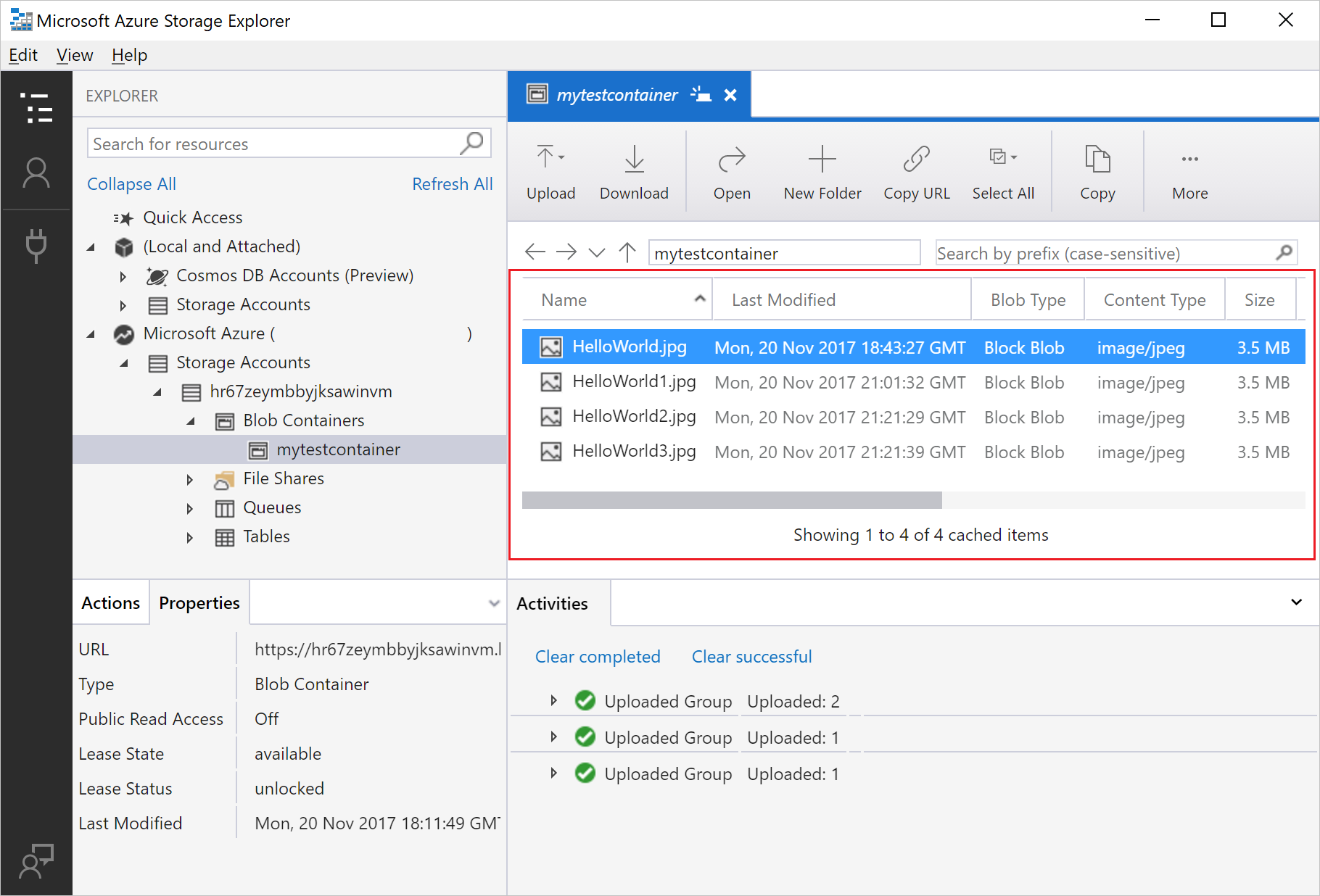
* 1. In the **Upload to folder (optional)** field either a folder name to store the files or folders in a folder under the container. If no folder is chosen, the files are uploaded directly under the container.



When you select **OK**, the files selected are queued to upload, each file is uploaded. When the upload is complete, the results are shown in the **Activities** window.

## Task 4 View blobs in a container

In the **Azure Storage Explorer** application, select a container under a storage account. The main pane shows a list of the blobs in the selected container.

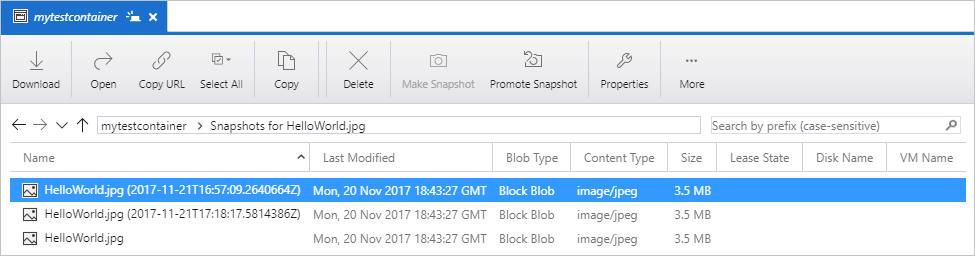


## Task 5 Download blobs

To download blobs using **Azure Storage Explorer**, with a blob selected, select **Download** from the ribbon. A file dialog opens and provides you the ability to enter a file name. Select **Save** to start the download of a blob to the local location.

## Task 6 Manage snapshots

Azure Storage Explorer provides the capability to take and manage [snapshots](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-snapshots) of your blobs. To take a snapshot of a blob, right-click the blob and select **Create Snapshot**. To view snapshots for a blob, right-click the blob and select **Manage Snapshots**. A list of the snapshots for the blob are shown in the current tab.



## Task 7 Manage access policies

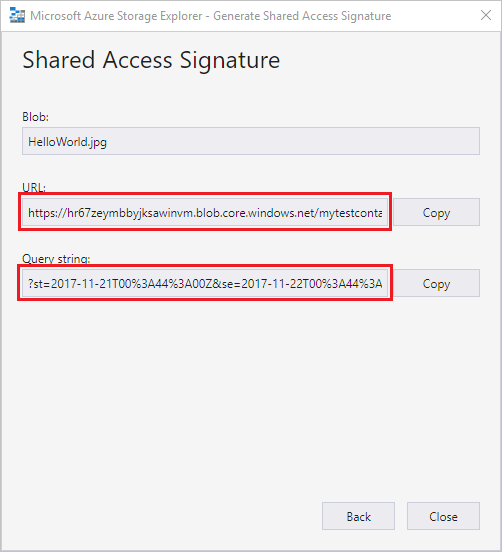
Storage Explorer provides the ability to manage access policies for containers within its user interface. There are two types of secure access policies (SAS), service level and account level. Account level SAS targets the storage account and can apply to multiple services and resources. Service level SAS are defined on a resource under a particular service.

1 To generate a service level SAS, right-click any container and select **Manage Access Policies...**. To generate an account level SAS, right-click on the storage account.

2 Select **Add** to add a new access policy and define the permissions for the policy. When complete select **Save** to save the access policy. This policy is now available for use when configuring a Shared Access Signature.

## Task 8 Work with Shared Access Signatures

Shared Access Signatures (SAS) can be retrieved through Storage Explorer. Right-click a storage account, container, or blob and choose **Get Shared Access Signature...**. Choose the start and expiry time, and permissions for the SAS URL and select **Create**. The full URL with the query string as well as the query string by itself are provided and can be copied from the next screen.



# Lab 2 A

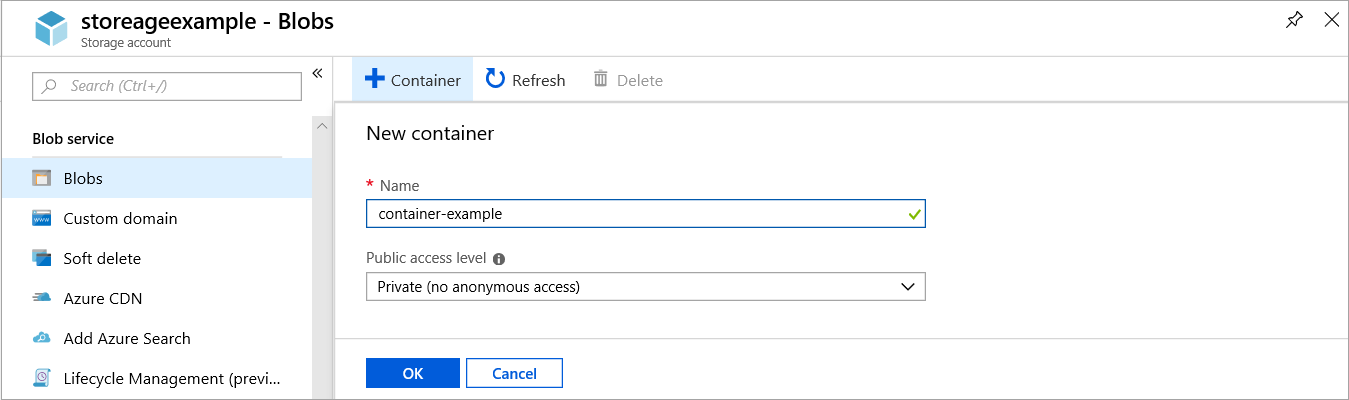
# Exercise 1

# Upload, download, and list blobs with the Azure portal

# Task 1 Create a container

To create a container in the Azure portal, follow these steps:

1. Navigate to your storage account in the Azure portal.
2. In the left menu for the storage account, scroll to the **Blob service** section, then select **Blobs**.
3. Select the **+ Container** button.
4. Type a name for your new container. The container name must be lowercase, must start with a letter or number, and can include only letters, numbers, and the dash (-) character. For more information about container and blob names, see [Naming and referencing containers, blobs, and metadata](https://docs.microsoft.com/rest/api/storageservices/naming-and-referencing-containers--blobs--and-metadata).
5. Set the level of anonymous read access to the container. The default level is **Private (no anonymous access)**.
6. Select **OK** to create the container.

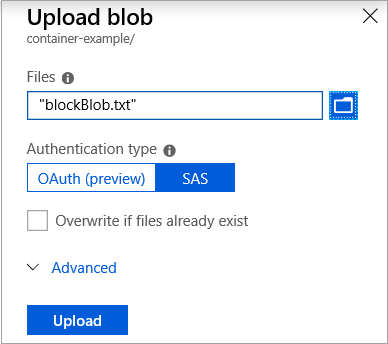


## Task 2 Upload a block blob

Block blobs consist of blocks of data assembled to make a blob. Most scenarios using Blob storage employ block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos. This quickstart shows how to work with block blobs.

To upload a block blob to your new container in the Azure portal, follow these steps:

1. In the Azure portal, navigate to the container you created in the previous section.
2. Select the container to show a list of blobs it contains. Since this container is new, it won't yet contain any blobs.
3. Select the **Upload** button to upload a blob to the container.
4. Browse your local file system to find a file to upload as a block blob, and select **Upload**.



1. Upload as many blobs as you like in this way. You'll see that the new blobs are now listed within the container.

## Task 3 Download a block blob

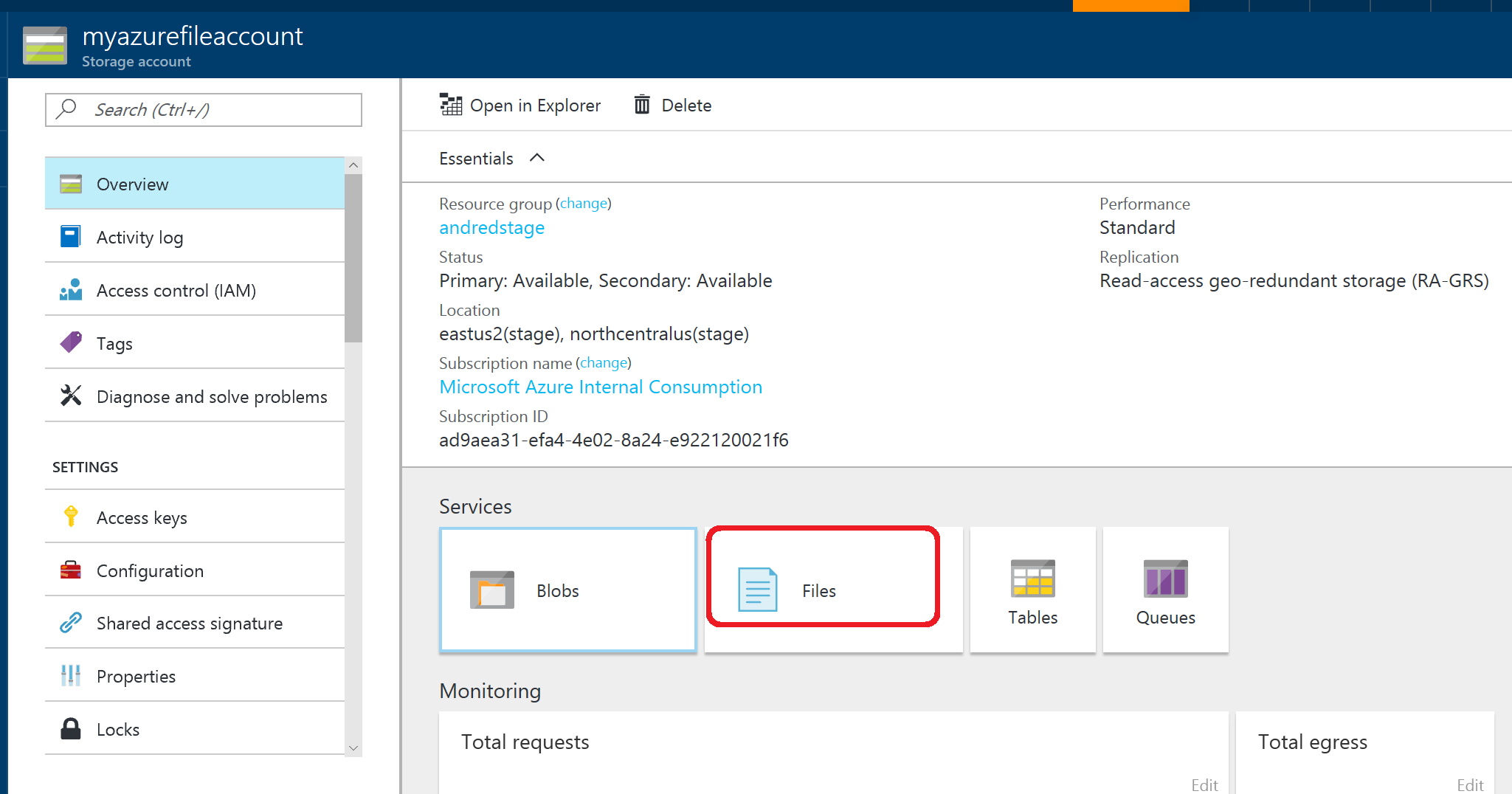
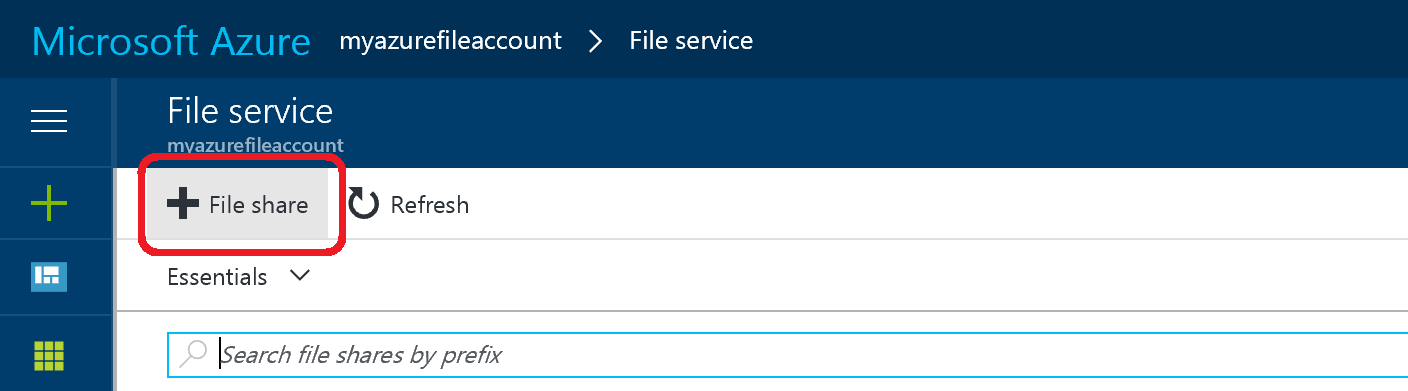
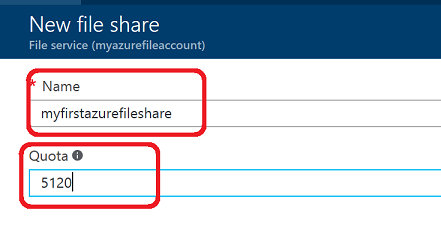
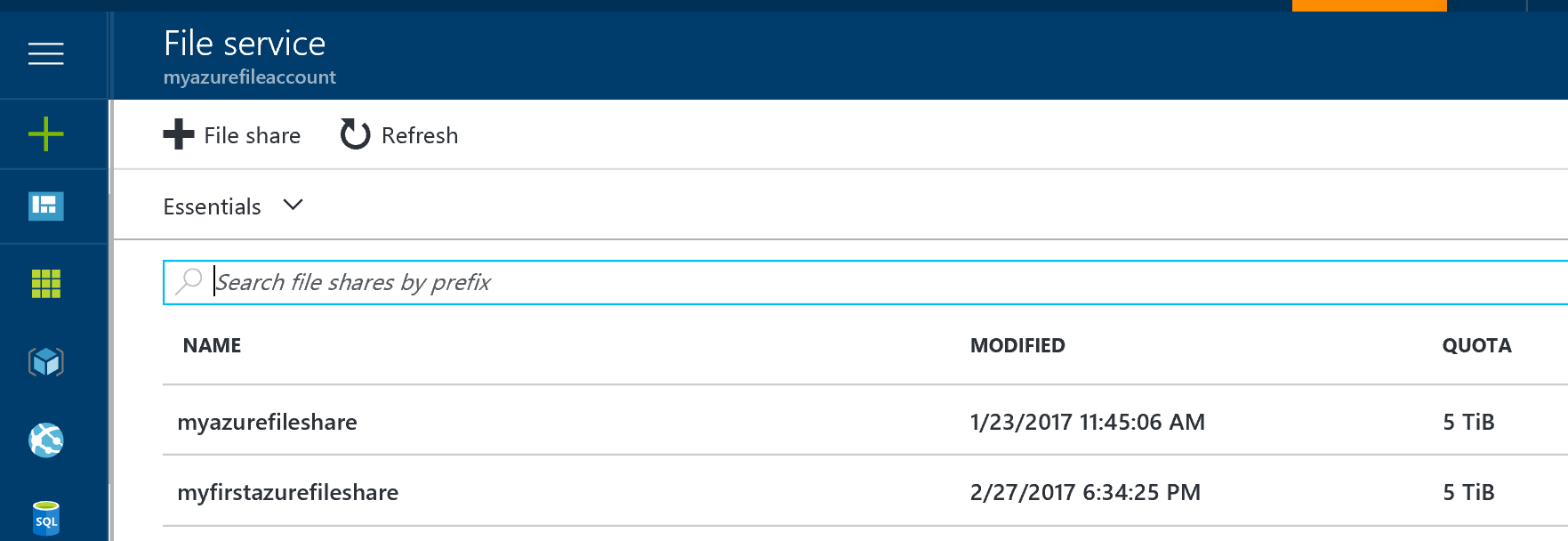
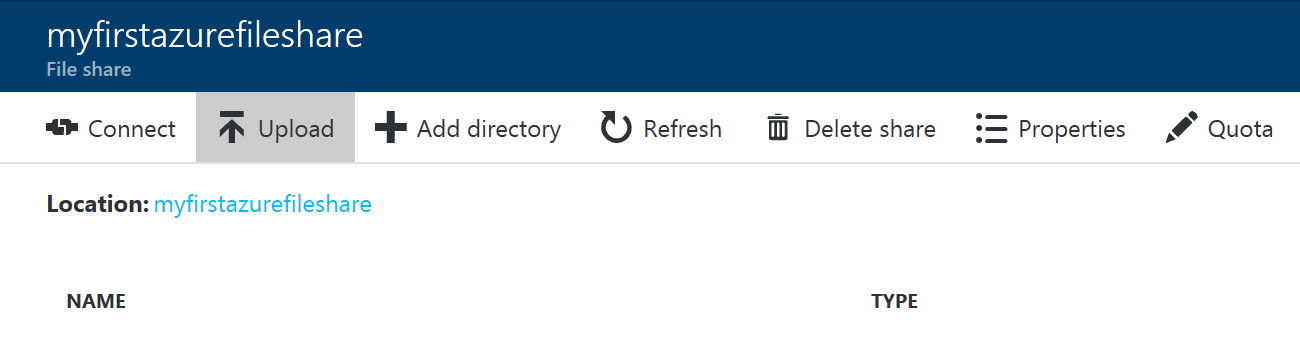
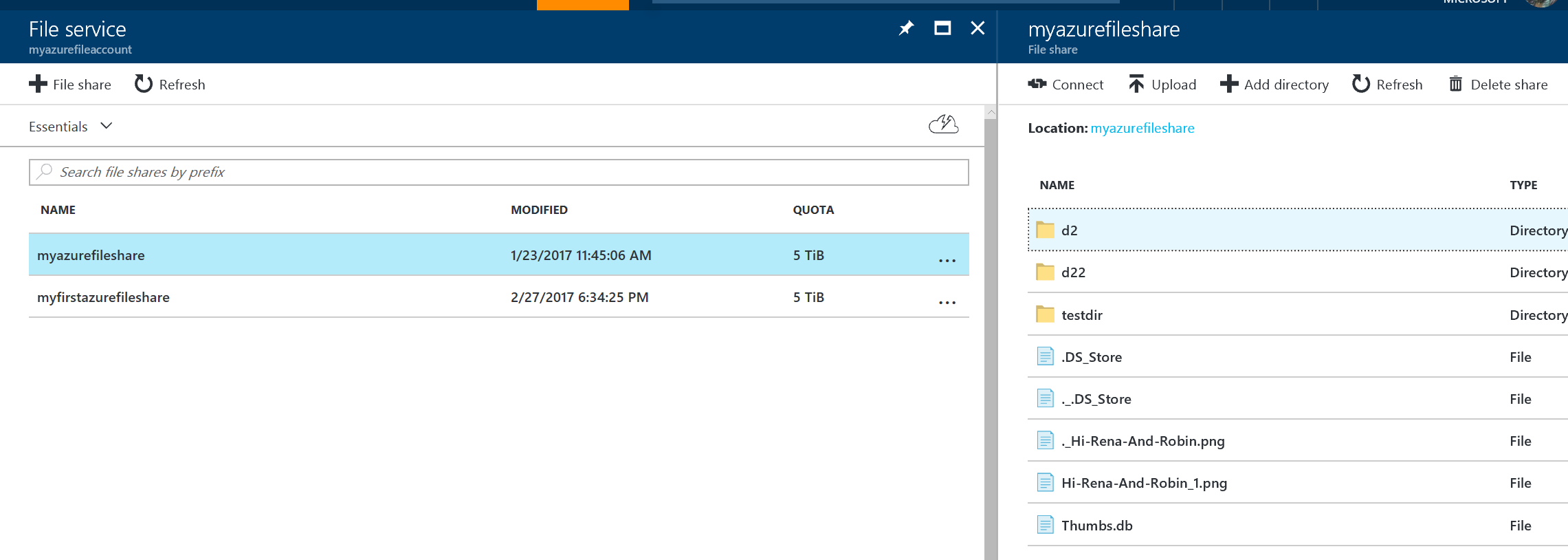
You can download a block blob to display in the browser or save to your local file system. To download a block blob, follow these steps:

1. Navigate to the list of blobs that you uploaded in the previous section.
2. Right-click the blob you want to download, and select **Download**.

# Lab 2 B

# Exercise 1 Create a file share in Azure Files

* ‎**Task 1 Create a file share through the Azure portal**

1. **Go to the Storage Account blade on the Azure portal**:  
   
2. **Click on add File Share button**:  
   
3. **Provide Name and Quota. The Quota's current maximum value is 5 TiB**:  
   
4. **View your new file share**: 
5. **Upload a file**: 
6. **Browse into your file share and manage your directories and files**: 

## Task 2 Create file share

1. **Create a context for your storage account and key** The context encapsulates the storage account name and account key. For instructions on copying your account key from the [Azure portal](https://portal.azure.com/), see [Storage account access keys](https://docs.microsoft.com/en-us/azure/storage/common/storage-account-manage#access-keys).

PowerShell

$storageContext = New-AzStorageContext <storage-account-name> <storage-account-key>

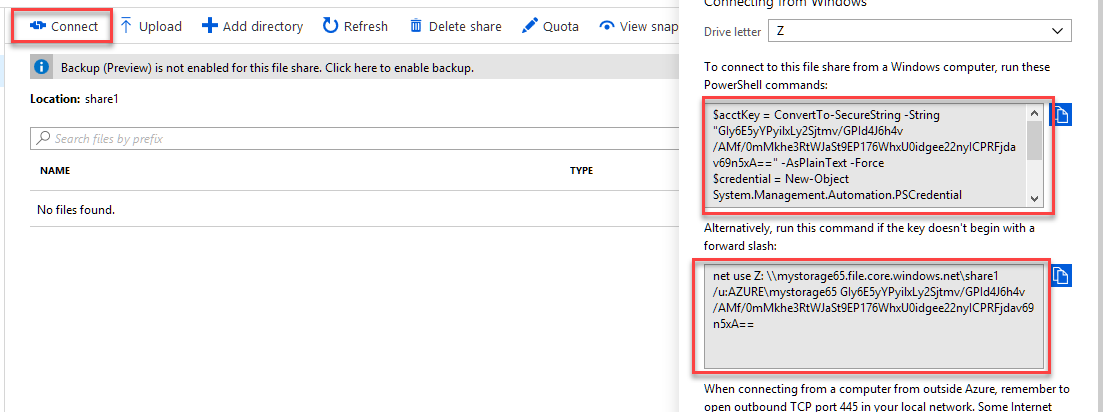
1. **Create a new file share**:

PowerShell

$share = New-AzStorageShare logs -Context $storageContext

**Alternative:**

* + 1. Select the file share then click Connect



* + 1. Open a cmd prompt and copy then paste the **net use** cmd.

**Lab 3**

# Back up Azure file shares

* ‎This Lab explains how to use the Azure portal to back up and restore [Azure file shares](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction).

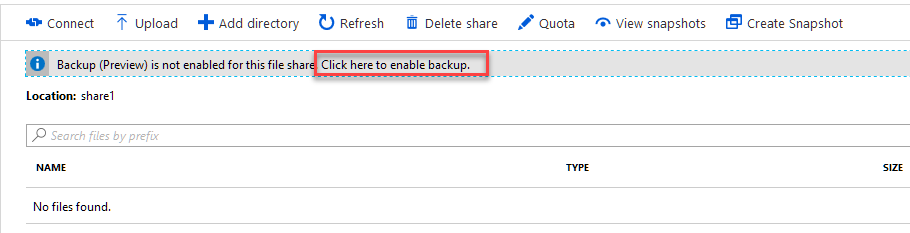
In this Lab, you learn how to:

* Configure a Recovery Services vault to back up Azure Files
* Run an on-demand backup job to create a restore point
* Restore a file or files from a restore point
* Manage Backup jobs
* Stop protection on Azure Files
* Delete your backup data

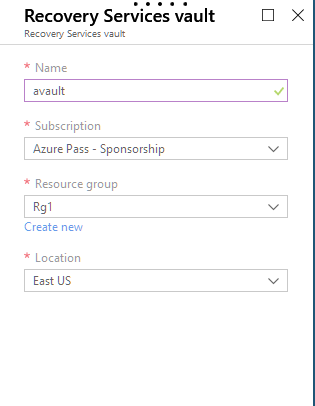
## Task 1 Configuring backup for an Azure file share

All backup data is stored in Recovery Services vaults. This tutorial assumes you already have established an Azure file share. To back up your Azure file share:

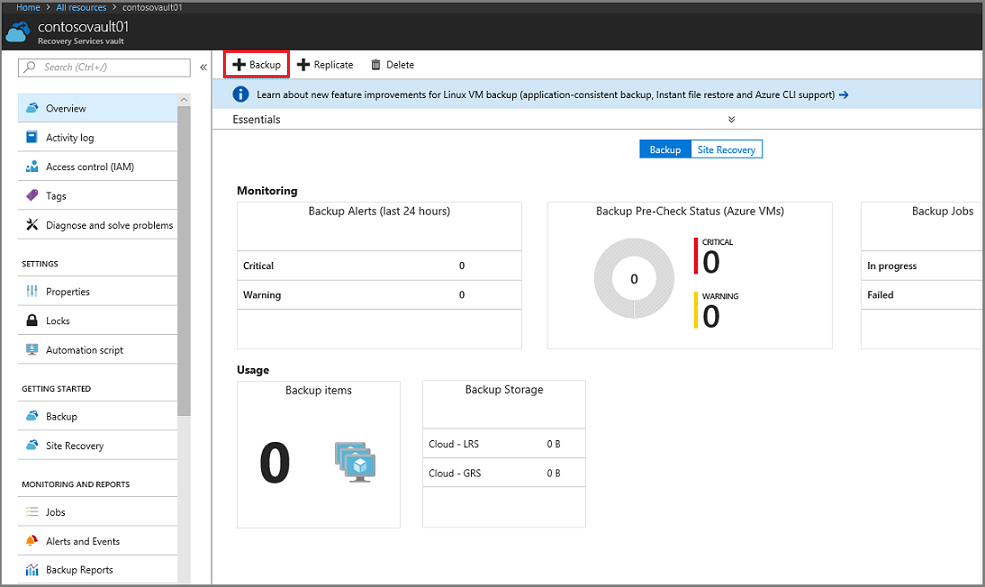
1. Open the share and click **Click here to enable backup**



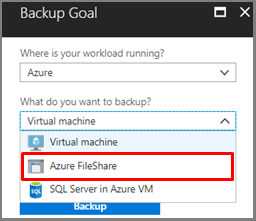
1. Then Click Go to Recovery Services Vault. Then Create a Recovery Services vault in the same region as your file share.



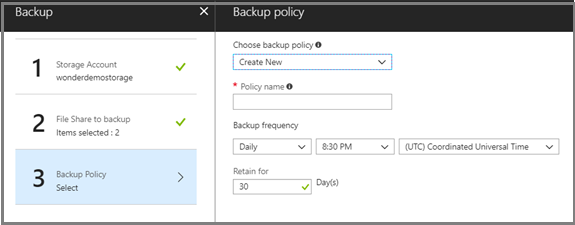
1. Then open the vault and click Backup



1. In the **Backup Goal** menu, from **What do you want to backup?**, choose Azure FileShare.



1. Select your storage account
2. Select your file share
3. After choosing your File Shares, the Backup menu switches to the **Backup policy**. From this menu either select an existing backup policy, or create a new one, and then click **Enable Backup**.



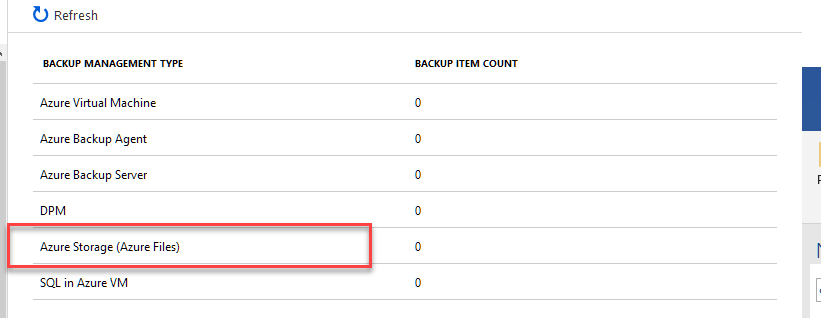
After establishing a backup policy, a snapshot of the File Shares will be taken at the scheduled time, and the recovery point is retained for the chosen period.

## Task 2 Create an on-demand backup

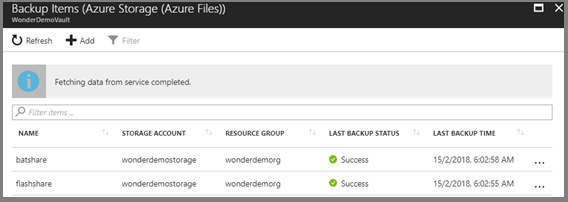
Occasionally you may want to generate a backup snapshot, or recovery point, outside of the times scheduled in the backup policy. A common time to generate an on-demand backup is right after you've configured the backup policy. Based on the schedule in the backup policy, it may be hours or days until a snapshot is taken. To protect your data until the backup policy engages, initiate an on-demand backup. Creating an On-demand backup is often required before you make planned changes to your file shares.

### To create an on-demand backup

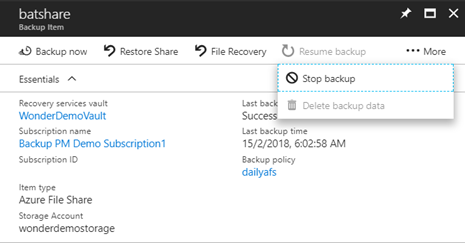
1. Open the Recovery Services vault that contains the file share recovery points, and click **Backup Items**. The list of Backup Item types appears.



1. From the list, select **Azure Storage (Azure Files)**. The list of Azure file shares appears.



1. From the list of Azure file shares, select the desired file share. The Backup Item menu for the selected file share opens.

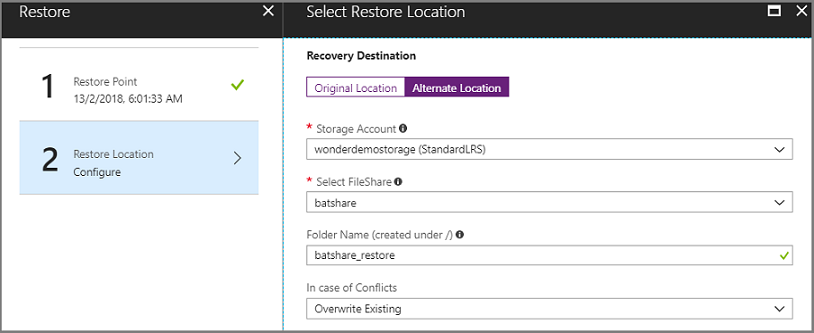


1. From the Backup Item menu, click **Backup Now**. Because this is an on-demand backup job, there is no retention policy associated with the recovery point. The **Backup Now** dialog opens. Specify the last day you want to retain the recovery point.



## Task 3 Restore from backup of Azure file share

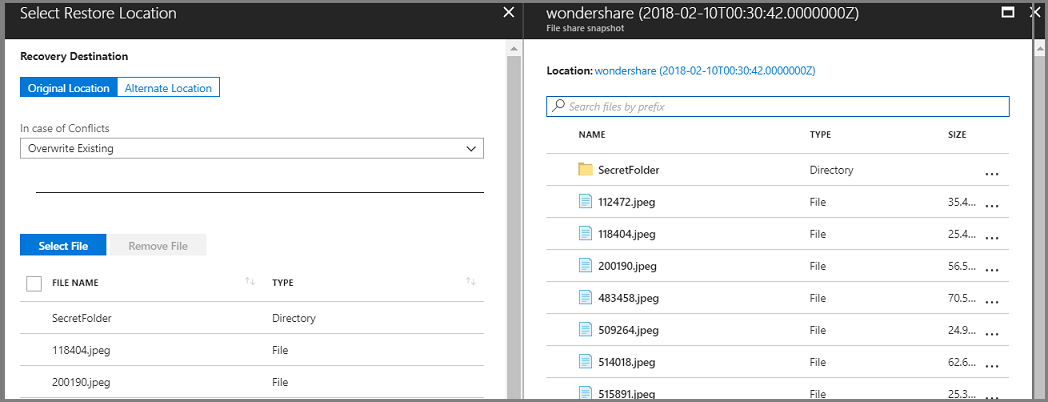
If you need to restore an entire file share or individual files or folders from a Restore Point, head to the Backup Item as detailed in the previous section. Choose **Restore Share** to restore an entire file share from a desired Point-in-time. From the list of Restore Points that show up, select one to be able to Overwrite your current file share or Restore this to an alternate file share in the same region.



## Task 4 Restore individual files or folders from backup of Azure file shares

Azure Backup provides the ability to browse a Restore Point within the Azure portal. To restore a file or folder of your choice, click on File Recovery from the Backup Item page and choose from the list of Restore Points. Select the Recovery Destination and then click **Select File** to browse the restore point.

1. Select the file or folder of your choice and **Restore**.



## Task 5 Manage Azure file share backups

You can execute several management tasks for File share backups on the **Backup Jobs** page, including:

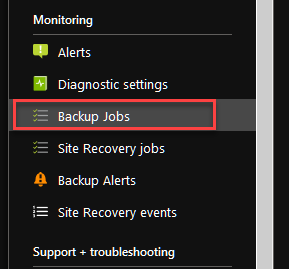
* [Monitor jobs](https://docs.microsoft.com/en-us/azure/backup/backup-azure-files#monitor-jobs)
* [Create a new policy](https://docs.microsoft.com/en-us/azure/backup/backup-azure-files#create-a-new-policy)
* [Stop protection on a file share](https://docs.microsoft.com/en-us/azure/backup/backup-azure-files#stop-protecting-an-azure-file-share)
* [Resume protection on a file share](https://docs.microsoft.com/en-us/azure/backup/backup-azure-files#resume-protection-for-azure-file-share)
* [Delete backup data](https://docs.microsoft.com/en-us/azure/backup/backup-azure-files#delete-backup-data)

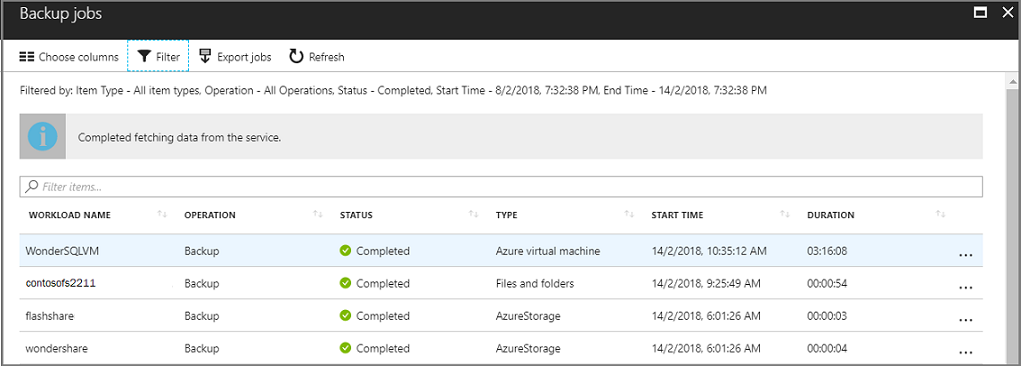
### Monitor jobs

You can monitor the progress of all jobs on the **Backup Jobs** page.

To open the **Backup Jobs** page:

1. Open the Recovery Services vault you want to monitor, and in the Recovery Services vault menu, under the **Monitoring** section click **Backup** **Jobs**.



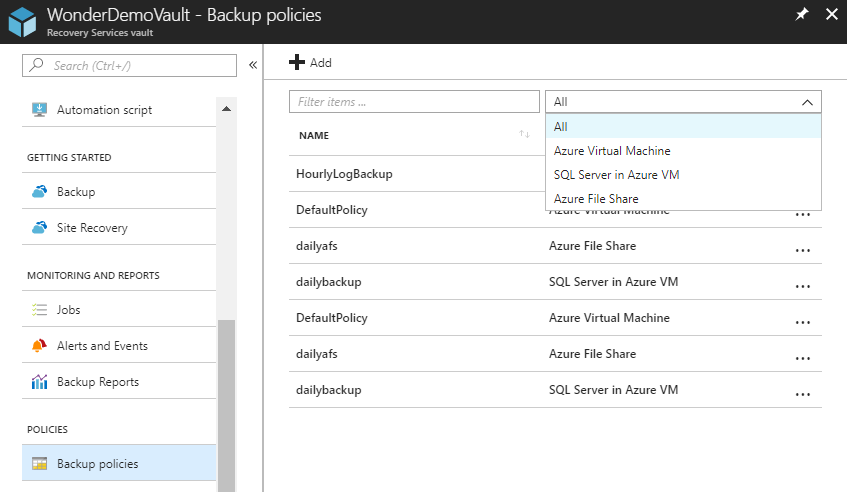
The list of Backup jobs and the status of those jobs appears. 

### Task 6 Create a new policy

You can create a new policy to back up Azure file shares from the **Backup Policies** of the Recovery Services vault. All policies created when you configure Backup for file shares show up with the Policy Type as Azure file Share.

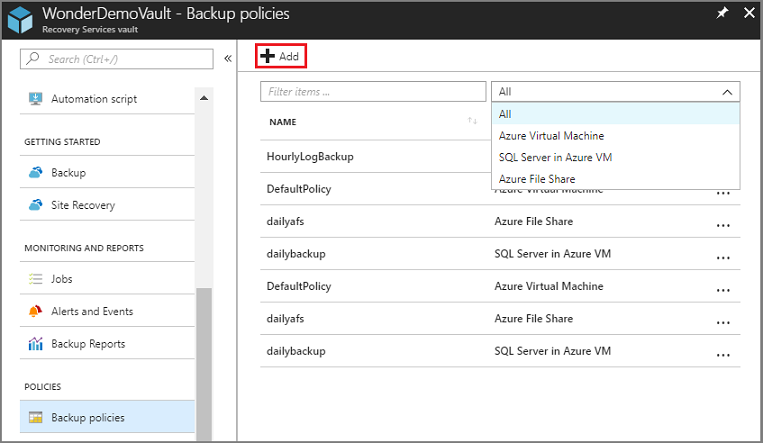
To view the existing Backup policies:

* Open the Recovery Services vault you want, and in the Recovery Services vault menu, click **Backup policies**. All Backup policies are listed.

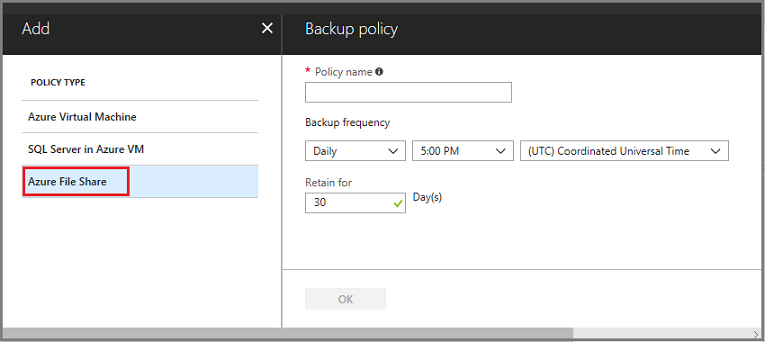


To create a new Backup policy:

1. In the Recovery Services vault menu, click **Backup policies**.
2. In the list of Backup policies, click **Add**.



1. In the **Add** menu, select **Azure File Share**. The Backup policy menu for Azure file share opens. Provide the name for the policy, backup frequency, and retention range for the recovery points. Click OK when you have defined the policy.



### Task 7 Stop protecting an Azure file share

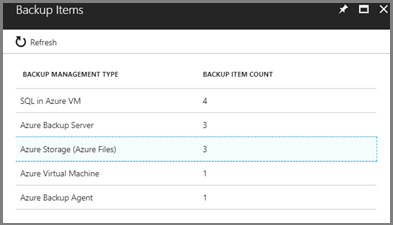
If you choose to stop protecting an Azure file share, you are asked if you want to retain the recovery points. There are two ways to stop protecting Azure file shares:

* Stop all future backup jobs and delete all recovery points, or
* Stop all future backup jobs but leave the recovery points

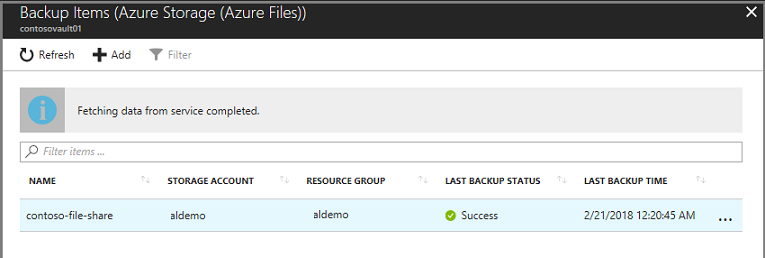
There may be a cost associated with leaving the recovery points in storage as the underlying snapshots created by Azure Backup will be retained. However, the benefit of leaving the recovery points is you can restore the File share later, if desired. For information about the cost of leaving the recovery points, see the pricing details. If you choose to delete all recovery points, you can't restore the File share.

To stop protection for an Azure file share:

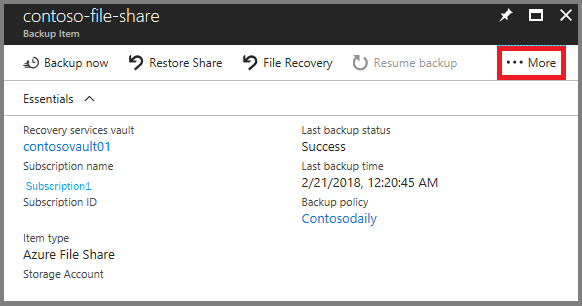
1. Open the Recovery Services vault that contains the file share recovery points, and click **Backup Items**. The list of Backup Item types appears.



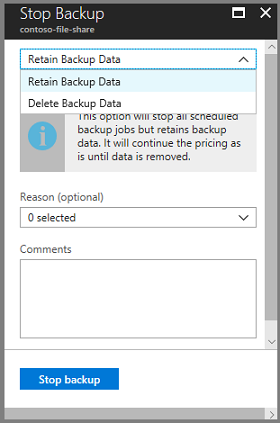
1. In the **Backup Management Type** list, select **Azure Storage (Azure Files)**. The list of Backup Items for (Azure Storage (Azure Files)) appears.



1. In the list of Backup Items (Azure Storage (Azure Files)), select the backup item you want to stop.
2. In the Azure file share items, click the **More** menu, and select **Stop Backup**.



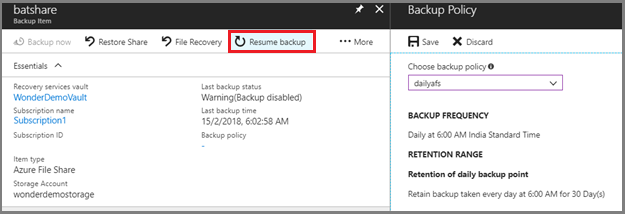
1. From the Stop Backup menu, choose **Delete Backup Data** and click **Stop Backup**.



### Resume protection for Azure file share

If the Retain Backup Data option was chosen when protection for the file share was stopped, then it's possible to resume protection. If the **Delete Backup Data** option was chosen, then protection for the file share can't resume.

To resume protection for the file share, go to the Backup Item and click Resume Backup. The Backup Policy opens and you can choose a policy of your choice to resume backup.



### Delete Backup data

You can delete the backup of a file share during the Stop backup job, or any time after you have stopped protection.

It may even be beneficial to wait days or weeks before deleting the recovery points.

Unlike restoring recovery points, when deleting backup data, you can't choose specific recovery points to delete.

If you choose to delete your backup data, you delete all recovery points associated with the item.

The following procedure assumes the Backup job for the virtual machine has been stopped. Once the Backup job is stopped, the Resume backup and Delete Backup Data options are available in the Backup item dashboard. Click Delete Backup Data and type the name of the File share to confirm deletion. Optionally, provide a Reason to delete or Comment.

**Lab 4**

# Exercise 1 Create an Azure CDN profile and endpoint

* ‎In this Lab, you enable Azure Content Delivery Network (CDN) by creating a new CDN profile and CDN endpoint. After you have created a profile and an endpoint, you can start delivering content to your customers.

## Task 1 Log in to the Azure portal

Log in to the [Azure portal](https://portal.azure.com/) with your Azure account.

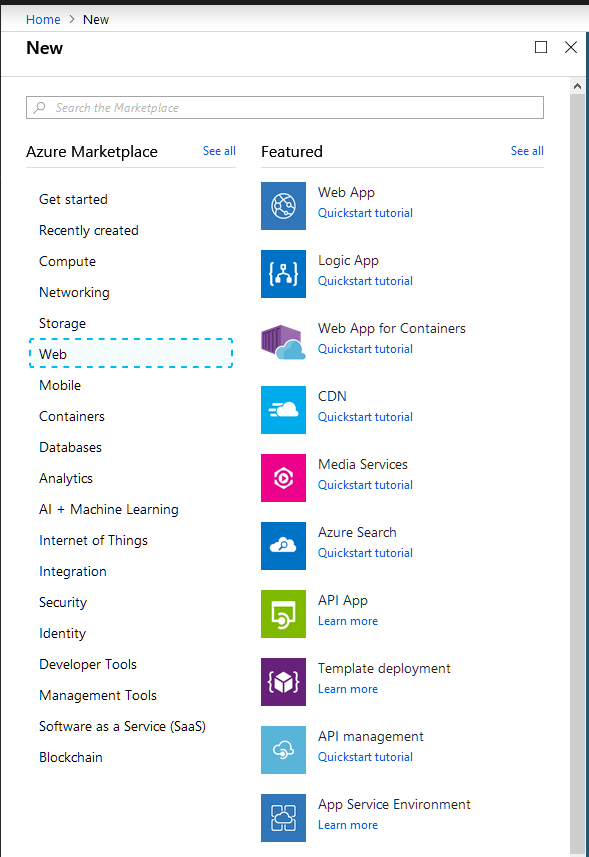
## Task 2 Create a new CDN profile

A CDN profile is a container for CDN endpoints and specifies a pricing tier.

1. In the Azure portal, in the upper left, select **Create a resource**.

The **New** pane appears.

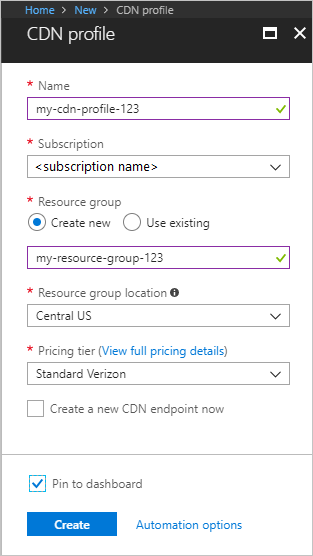
1. Select **Web**, then select **CDN**.



The **CDN profile** pane appears.

1. For the CDN profile settings, use the values specified in the following table:

| **Setting** | **Value** |
| --- | --- |
| **Name** | Enter **my-cdn-profile-123** for your profile name. This name must be globally unique; if it is already in use, you may enter a different name. |
| **Subscription** | Select an Azure subscription from the drop-down list. |
| **Resource group** | Select **Create new** and enter my-resource-group-123 for your resource group name. This name must be globally unique. If it is already in use, you may enter a different name or you can select **Use existing** and select **my-resource-group-123** from the drop-down list. |
| **Resource group location** | IF a location can be selected select East US from the drop-down list. |
| **Pricing tier** | Select **Standard Verizon** from the drop-down list. |
| **Create a new CDN endpoint now** | Leave unselected. |



1. Select **Create** to create the profile.

For **Azure CDN Standard from Microsoft** profiles only, profile completion usually completes in two hours.

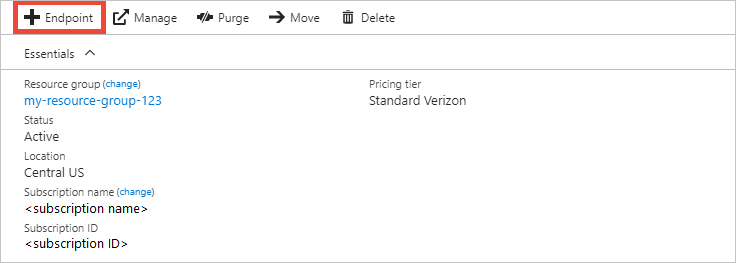
## Task 3 Create a new CDN endpoint

After you've created a CDN profile, you can use it to create an endpoint.

1. In the Azure portal, select in your dashboard the CDN profile that you created. If you can't find it, select **All services**, then select **CDN profiles**. In the **CDN profiles** page, select the profile that you want to use.

The CDN profile page appears.

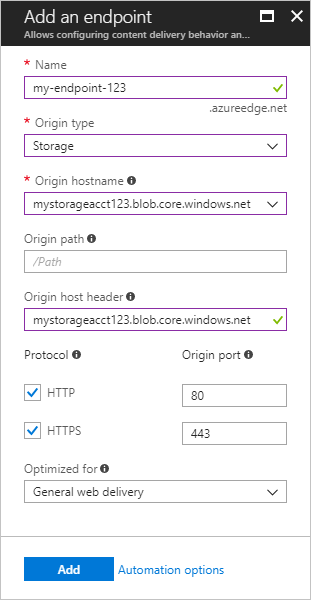
1. Select **Endpoint**.



The **Add an endpoint** pane appears.

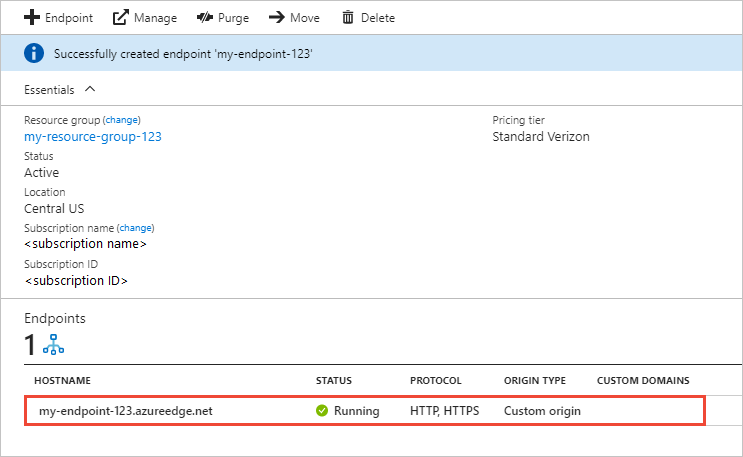
1. For the endpoint settings, use the values specified in the following table:

| **Setting** | **Value** |
| --- | --- |
| **Name** | Enter **my-endpoint-123**for your endpoint hostname. This name must be globally unique; if it is already in use, you may enter a different name. This name is used to access your cached resources at the domain <endpoint name>.azureedge.net. |
| **Origin type** | Select **Storage**. |
| **Origin hostname** | Select your storage account |
| **Origin path** | Leave blank. |
| **Origin host header** | Leave the default generated value. |
| **Protocol** | Leave the default **HTTP** and **HTTPS** options selected. |
| **Origin port** | Leave the default port values. |
| **Optimized for** | Leave the default selection, **General web delivery**. |



1. Select **Add** to create the new endpoint.

After the endpoint is created, it appears in the list of endpoints for the profile.



Because it takes time for the registration to propagate, the endpoint isn't immediately available for use:

* + For **Azure CDN Standard from Microsoft** profiles, propagation usually completes in 10 minutes.
  + For **Azure CDN Standard from Akamai** profiles, propagation usually completes within one minute.
  + For **Azure CDN Standard from Verizon** and **Azure CDN Premium from Verizon** profiles, propagation usually completes within 90 minutes.

# Exercise 2 Set Azure CDN caching rules

**Note**

Azure CDN caching rules are available only for **Azure CDN Standard from Verizon** and **Azure CDN Standard from Akamai**. For **Azure CDN Premium from Verizon**, use the [Azure CDN rules engine](https://docs.microsoft.com/en-us/azure/cdn/cdn-rules-engine) in the **Manage** portal for similar functionality.

This tutorial describes how you can use Azure Content Delivery Network (CDN) caching rules to set or modify default cache expiration behavior both globally and with custom conditions, such as a URL path and file extension. Azure CDN provides two types of caching rules:

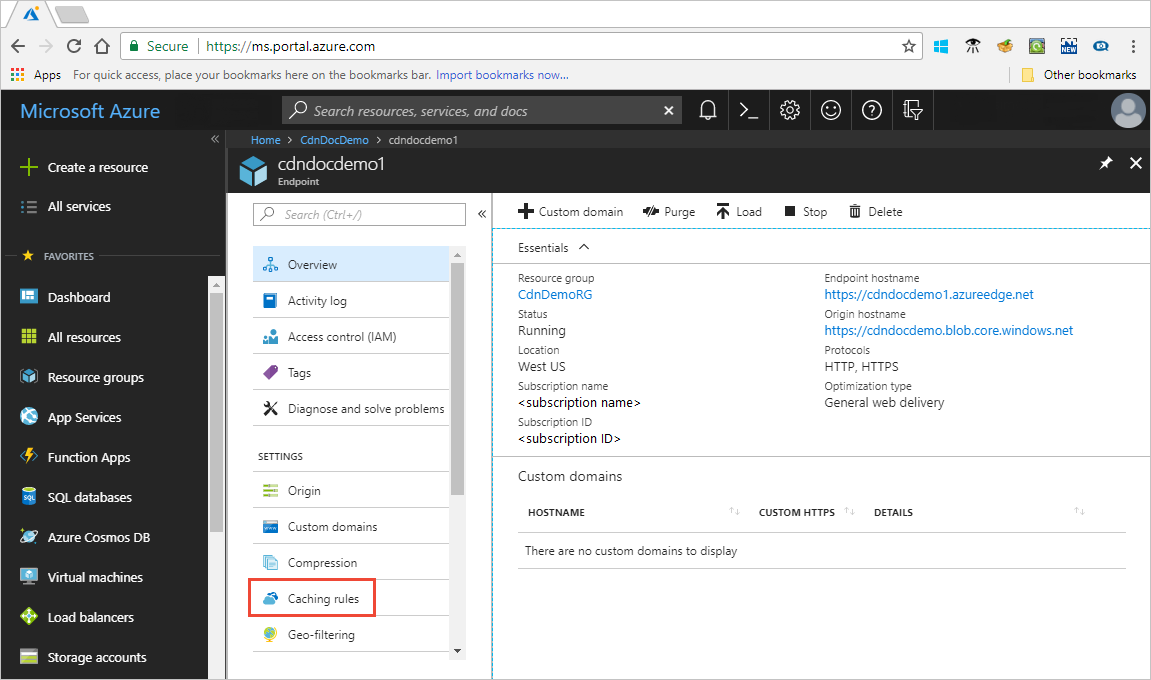
* Global caching rules: You can set one global caching rule for each endpoint in your profile, which affects all requests to the endpoint. The global caching rule overrides any HTTP cache-directive headers, if set.
* Custom caching rules: You can set one or more custom caching rules for each endpoint in your profile. Custom caching rules match specific paths and file extensions, are processed in order, and override the global caching rule, if set.

In this Lab, you learn how to:

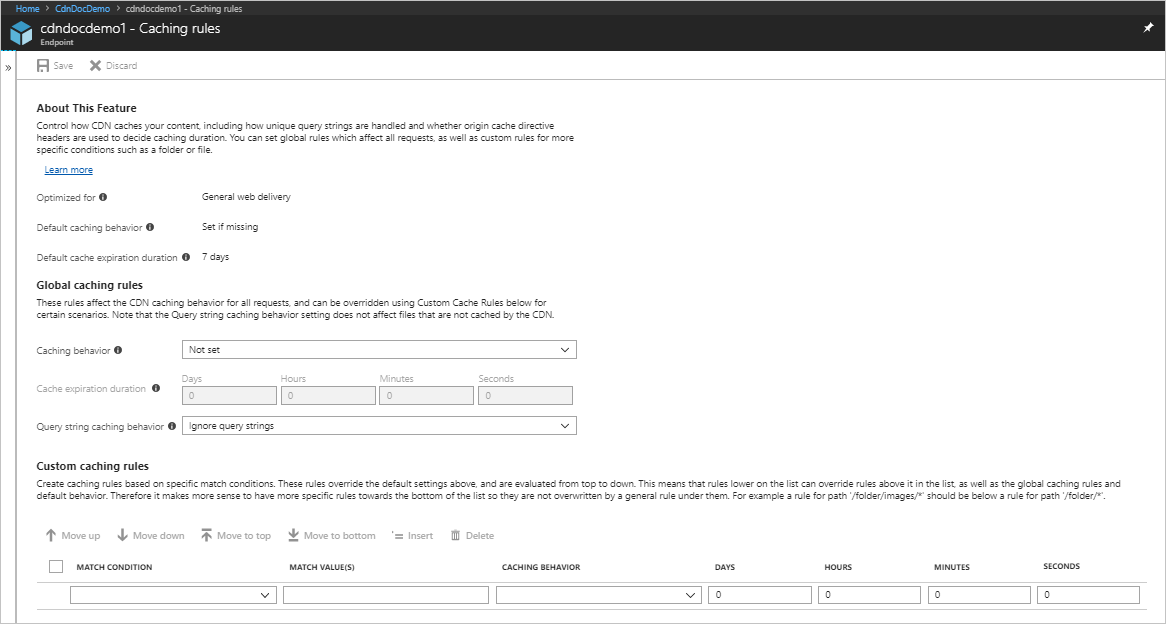
* Open the caching rules page.
* Create a global caching rule.
* Create a custom caching rule.

## Task 1 Open the Azure CDN caching rules page

1. In the [Azure portal](https://portal.azure.com/), select a CDN profile, then select an endpoint.
2. In the left pane under Settings, select **Caching rules**.



The **Caching rules** page appears.

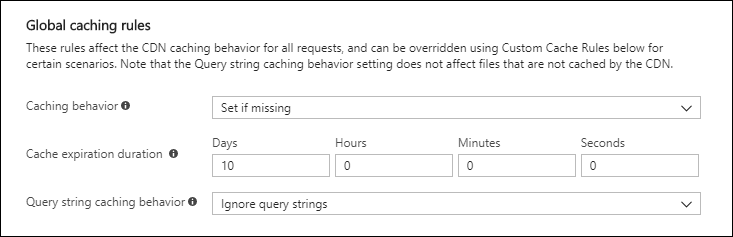


## Task 2 Set global caching rules

Create a global caching rule as follows:

1. Under **Global caching rules**, set **Query string caching behavior** to **Ignore query strings**.
2. Set **Caching behavior** to **Set if missing**.
3. For **Cache expiration duration**, enter 10 in the **Days** field.

The global caching rule affects all requests to the endpoint. This rule honors the origin cache-directive headers, if they exist (Cache-Control or Expires); otherwise, if they are not specified, it sets the cache to 10 days.

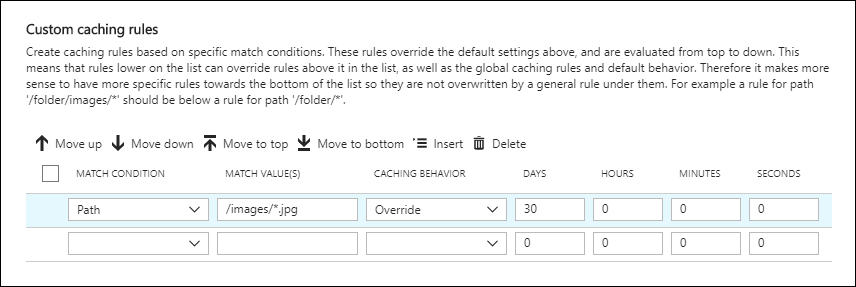


## Task 3 Set custom caching rules

Create a custom caching rule as follows:

1. Under **Custom caching rules**, set **Match condition** to **Path** and **Match value** to /images/\*.jpg.
2. Set **Caching behavior** to **Override** and enter 30 in the **Days** field.

This custom caching rule sets a cache duration of 30 days on any .jpg image files in the /images folder of your endpoint. It overrides any Cache-Control or Expires HTTP headers that are sent by the origin server.



## Task 4 Clean up resources

In the preceding steps, you created caching rules. If you no longer want to use these caching rules, you can remove them by performing these steps:

1. Select a CDN profile, then select the endpoint with the caching rules you want to remove.
2. In the left pane under Settings, select **Caching rules**.
3. Under **Global caching rules**, set **Caching behavior** to **Not set**.
4. Under **Custom caching rules**, select the check box next to the rule you want to delete.
5. Select **Delete**.
6. From the top of the page, select **Save**.