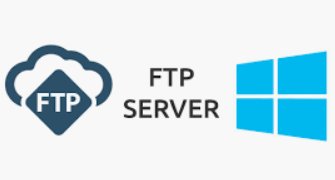
**Assignment**:

**Direction**:

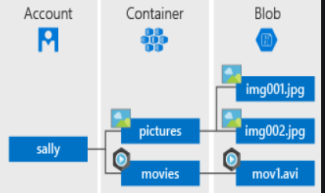
1. **FTP Server:**

Customers 🡪(files) 🡪 FTP Server 🡪 (Mounted share path) Application server (Private network)

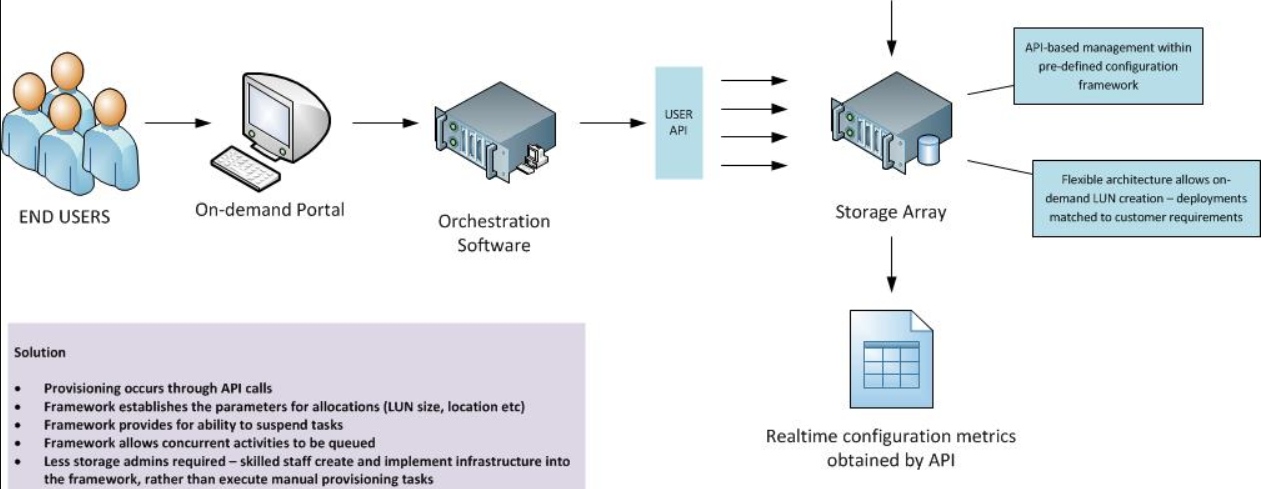
 🡪 🡪

1. **Blob Storage:**

Customers 🡪 (Files) 🡪 Block Blob Storage 🡪 ((Files) Local drive) 🡪 Windows🡪Application hosted on the server

 🡪  🡪  🡪

1. **Through API:**



**STEPS**:

**FTP SERVER:**

1. Deploy one windows VM and enable FTP Service through service manager and also setup advance permission for AD Users to protect users data from unauthorised access.
2. Create AD users and group
3. Mount the FTP data drive to the application server.
4. Application can fetch the data from the mount path and execute it.

**BLOB STORAGE:**

1. We have to create a storage container (Blob Storage). Create a group with read permission.
2. We will create a group with limited permission and provision access to the users.
3. We will grant a Customer limited permissions to objects in your storage account for a specified period of time and with a specified set of permissions, without having to share our account access keys by using [shared access signature (**SAS**)](https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1)
4. Direct access data from storage to application server through API by adding a route to serve the file in your API.

**[OR]**

1. Grant our Application (Windows) server’s system-assigned managed identity access to a storage account.
2. Give full permission to the app server of the drive to Application server so that the data it can fetch the data and execute them.

**Procedure to implement steps:**

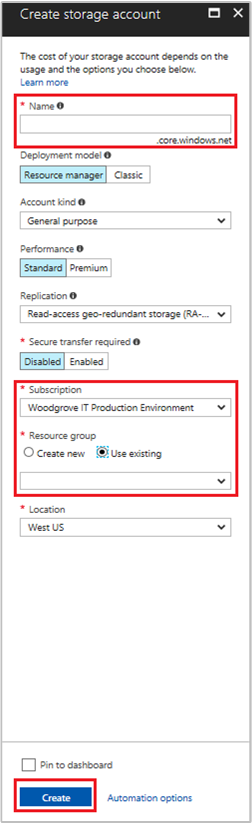
**Create and grant access to the users in storage containers:**

* [**Download and install Storage Explorer**](https://www.storageexplorer.com/)
* [**Connect to an Azure storage account or service**](https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer#connect-to-a-storage-account-or-service)
* **Create a blob container in a storage account**
* **Grant your Windows VM's system-assigned managed identity access to a storage account**
* **Get an access and use it to call Azure Storage**

**Create a storage account**

If you don't already have one, you will now create a storage account. You can also skip this step and grant your VM's system-assigned managed identity access to the keys of an existing storage account.

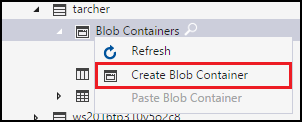
1. Click the +/Create new service button found on the upper left-hand corner of the Azure portal.
2. Click Storage, then Storage Account, and a new "Create storage account" panel will display.
3. Enter a name for the storage account, which you will use later.
4. Deployment model and Account kind should be set to "Resource manager" and "General purpose", respectively.
5. Ensure the Subscription and Resource Group match the ones you specified when you created your VM in the previous step.
6. Click Create.

****

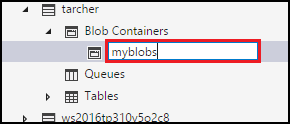
**Create a blob container in a storage account:**

The following steps illustrate how to create a blob container within Storage Explorer.

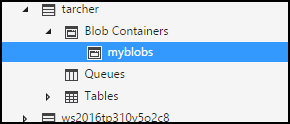
1. Open Storage Explorer.
2. In the left pane, expand the storage account within which you wish to create the blob container.
3. Right-click **Blob Containers**, and - from the context menu - select **Create Blob Container**.



1. A text box will appear below the **Blob Containers** folder. Enter the name for your blob container. See [Create a container](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-quickstart-blobs-dotnet#create-a-container) for information on rules and restrictions on naming blob containers.



1. Press **Enter** when done to create the blob container, or **Esc** to cancel. Once the blob container has been successfully created, it will be displayed under the **Blob Containers** folder for the selected storage account.

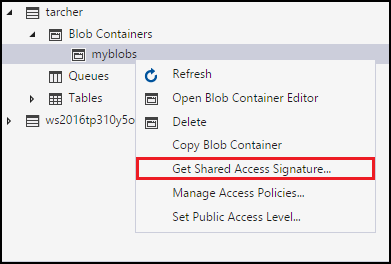


**Get the SAS for a blob container:**

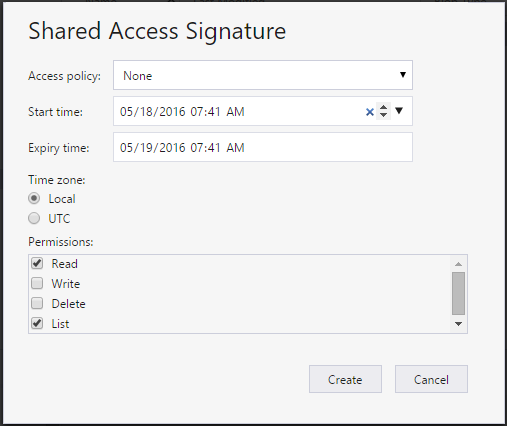
A [shared access signature (**SAS**)](https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1) provides delegated access to resources in your storage account. This means that you can grant a client limited permissions to objects in your storage account for a specified period of time and with a specified set of permissions, without having to share your account access keys.

The following steps illustrate how to create a SAS for a blob container:

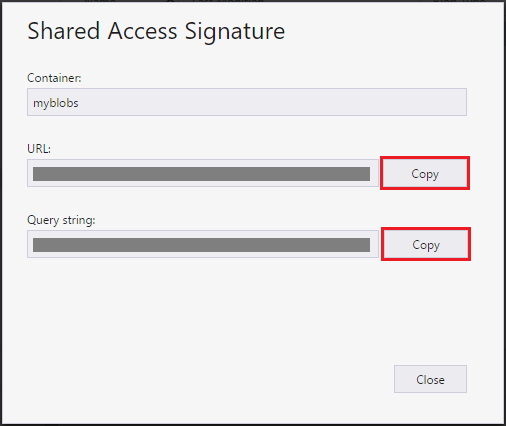
1. Open Storage Explorer.
2. In the left pane, expand the storage account containing the blob container for which you wish to get a SAS.
3. Expand the storage account's **Blob Containers**.
4. Right-click the desired blob container, and - from the context menu - select **Get Shared Access Signature**.



1. In the **Shared Access Signature** dialog, specify the policy, start and expiration dates, time zone, and access levels you want for the resource.



1. When you're finished specifying the SAS options, select **Create**.
2. A second **Shared Access Signature** dialog will then display that lists the blob container along with the URL and QueryStrings you can use to access the storage resource. Select **Copy** next to the URL you wish to copy to the clipboard.



1. When done, select **Close**.

**FTP Server:**

**Enable FTP Service through service manager: perfer the link**

<https://social.technet.microsoft.com/wiki/contents/articles/12364.windows-server-2012-ftp-installation.aspx>

or

<https://vpsie.com/knowledge-base/how-to-setup-ftp-server-users-on-windows-2012-r2/>

**API**:

A cloud storage API is an application program interface that connects a locally-based application to a cloud-based storage system, so that a user can send data to it and access and work with data stored in it. To the application, the cloud storage system is just another target device, like tape or disk-based storage.