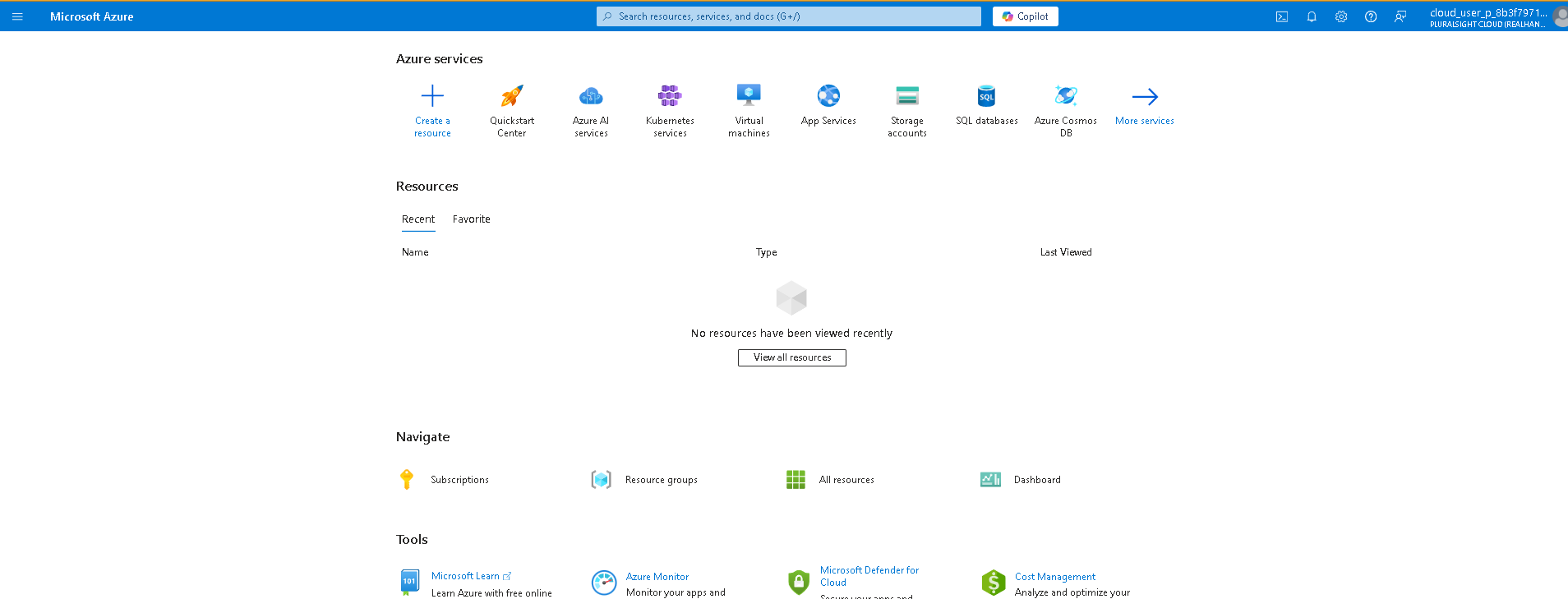
# Lab 07 - Manage Azure Storage

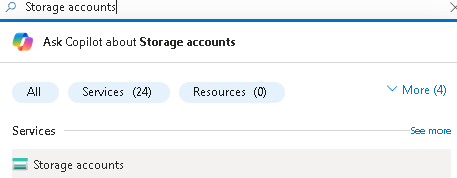
Made by Valeriy Manuilyk <3

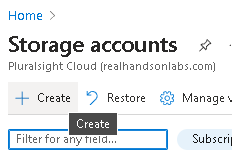
## Task 1: Create and configure a storage account.

1.Sign in to the ****Azure portal**** - https://portal.azure.com.

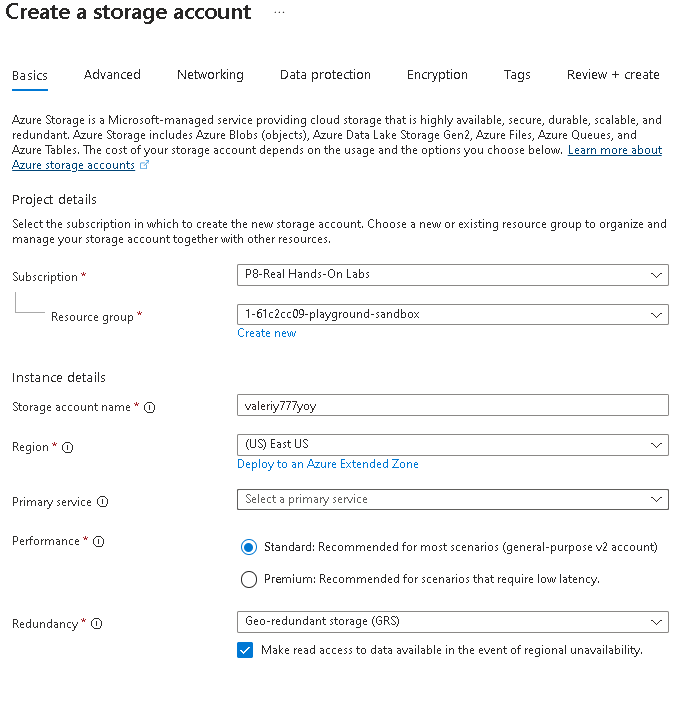


2.Search for and select Storage accounts, and then click ****+ Create****.

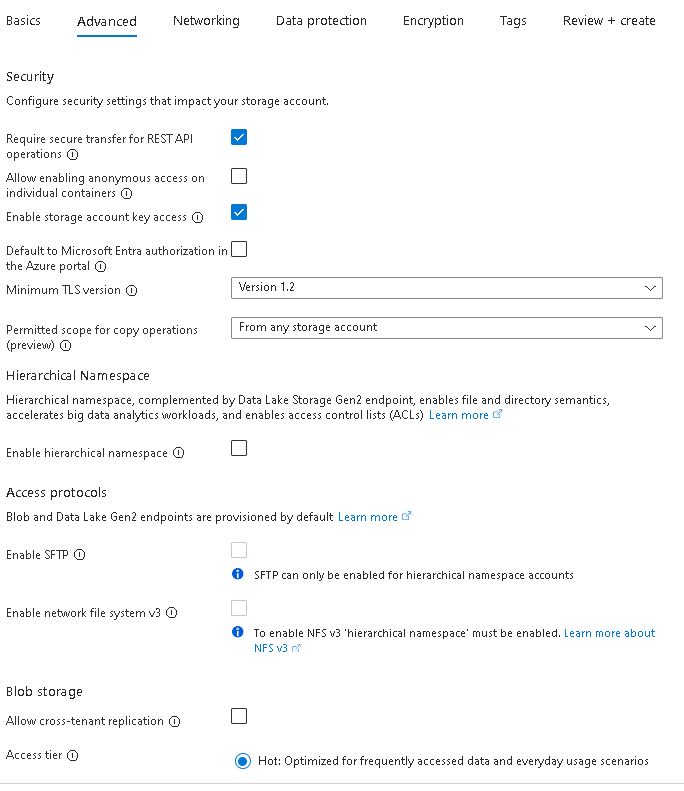




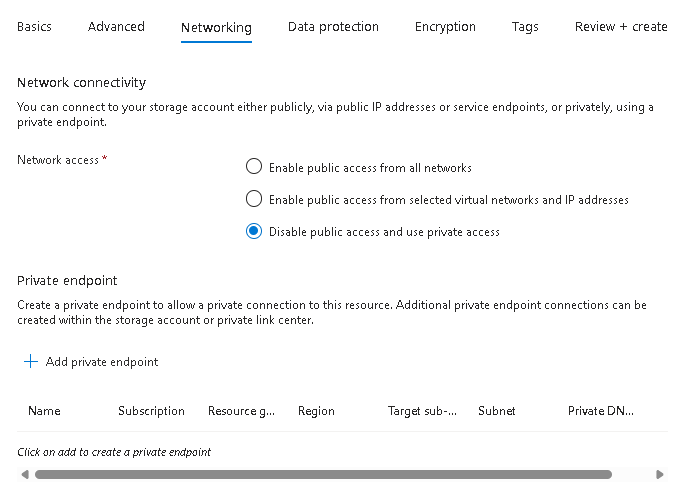
3.On the ****Basics**** tab of the ****Create a storage account**** blade, specify the following settings (leave others with their default values):



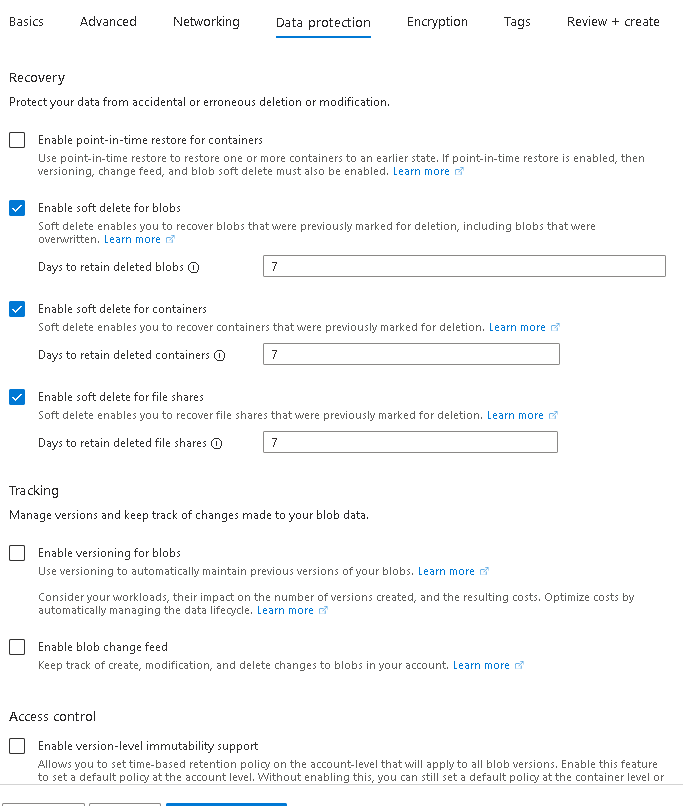
1.On the ****Advanced**** tab, use the informational icons to learn more about the choices. Take the defaults.



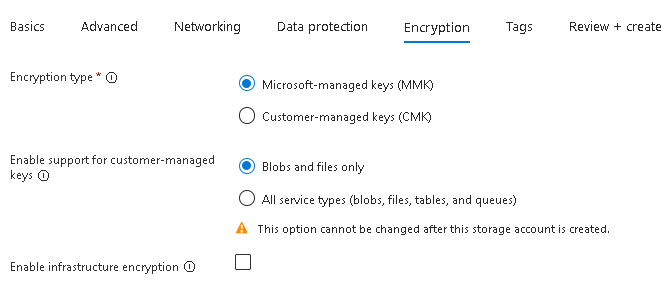
2.On the ****Networking**** tab, review the available options, select ****Disable public access and use private access****.



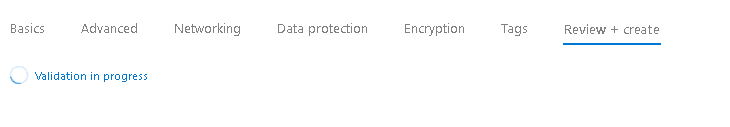
3.Review the ****Data protection**** tab. Notice 7 days is the default soft delete retention policy. Note you can enable blob versioning. Accept the defaults.



4.Review the ****Encryption**** tab. Notice the additional security options. Accept the defaults.

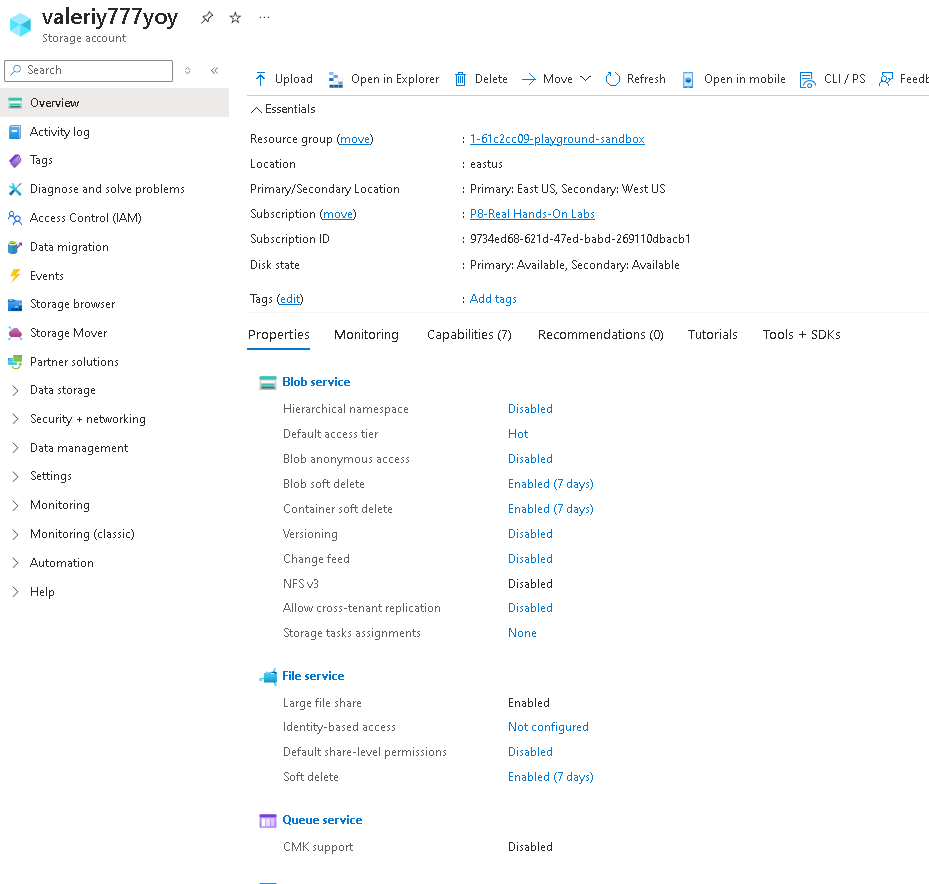


5.Select ****Review****, wait for the validation process to complete, and then click ****Create****.

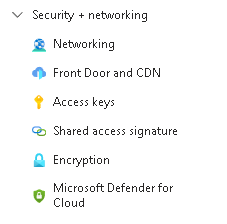


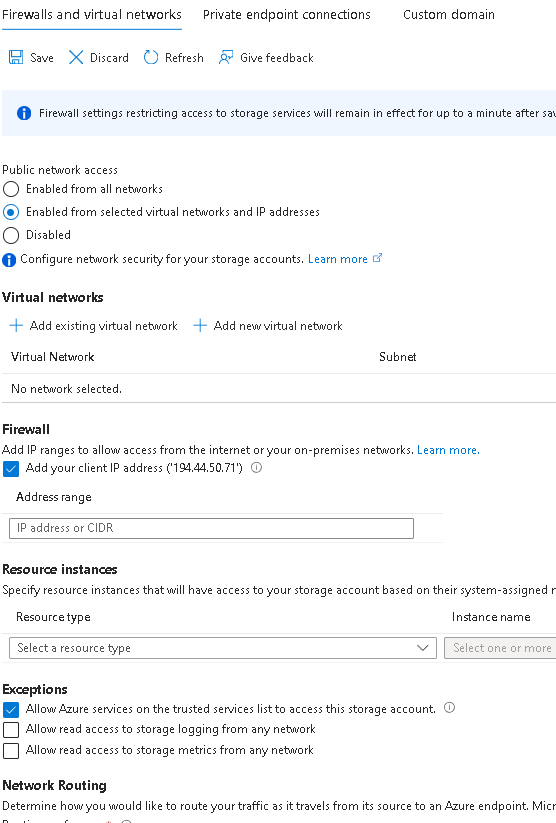
6.Once the storage account is deployed, select ****Go to resource****.

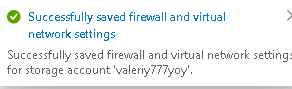
7.Review the ****Overview**** blade and the additional configurations that can be changed. These are global settings for the storage account. Notice the storage account can be used for Blob containers, File shares, Queues, and Tables.



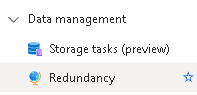
8.In the ****Security + networking**** section, select ****Networking****. Notice public network access is disabled.





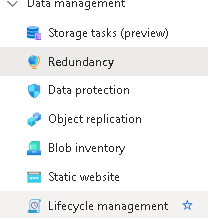


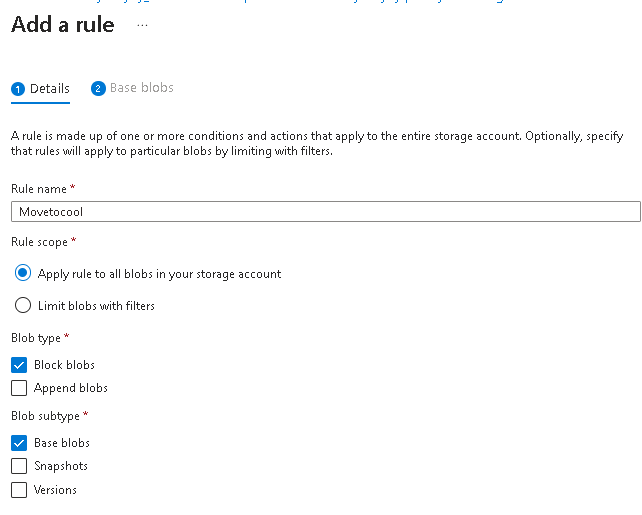
9.In the ****Data management**** section, view the ****Redundancy**** blade. Notice the information about your primary and secondary data center locations.

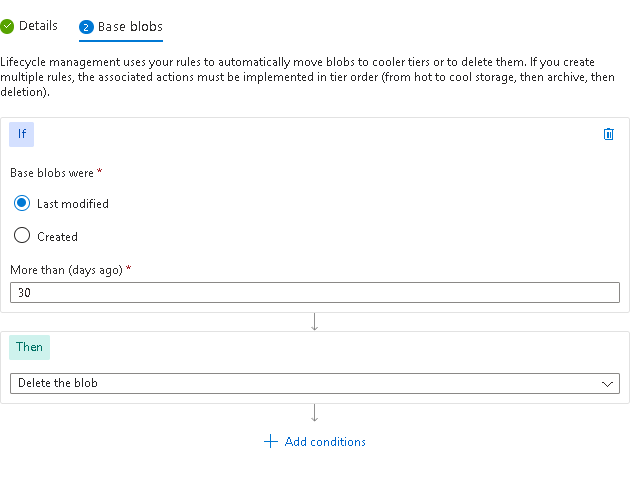




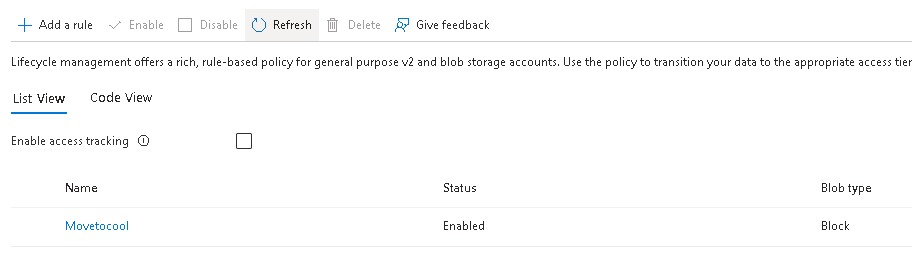
10.In the ****Data management**** section, select ****Lifecycle management****, and then select ****Add a rule****.







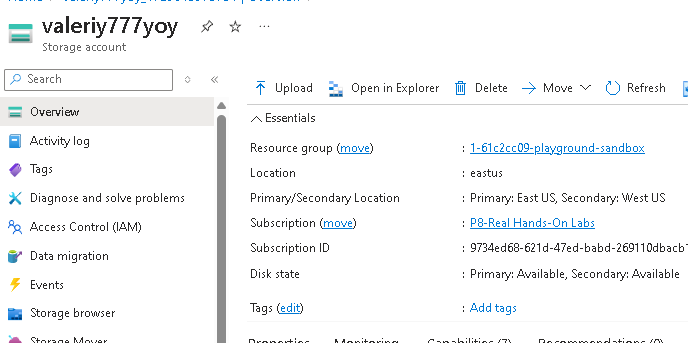




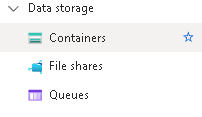
## Task 2: Create and configure secure blob storage

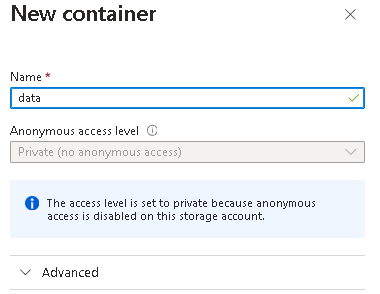
### Create a blob container and a time-based retention policy

1.Continue in the Azure portal, working with your storage account.



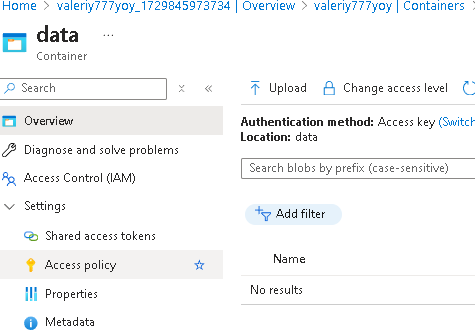
2.In the ****Data storage**** section, click ****Containers****.



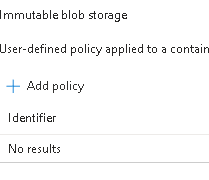


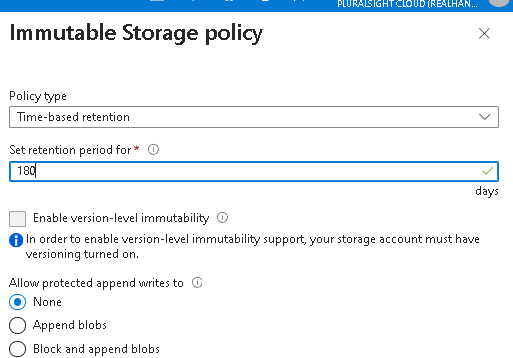


4.On your container, scroll to the ellipsis (…) on the far right, select ****Access Policy****.



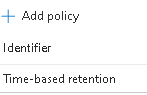
5.In the ****Immutable blob storage**** area, select ****Add policy****.





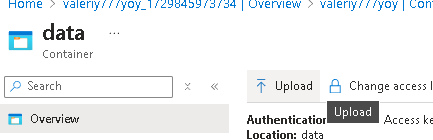
6.Select ****Save****.



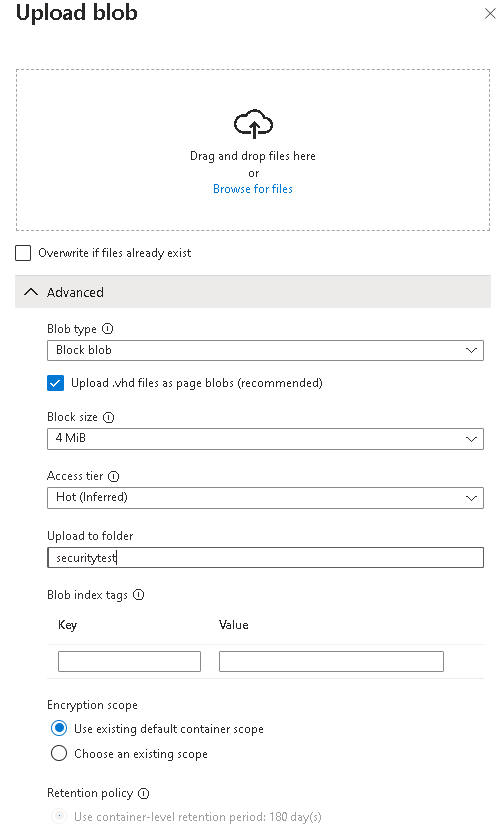


### Manage blob uploads

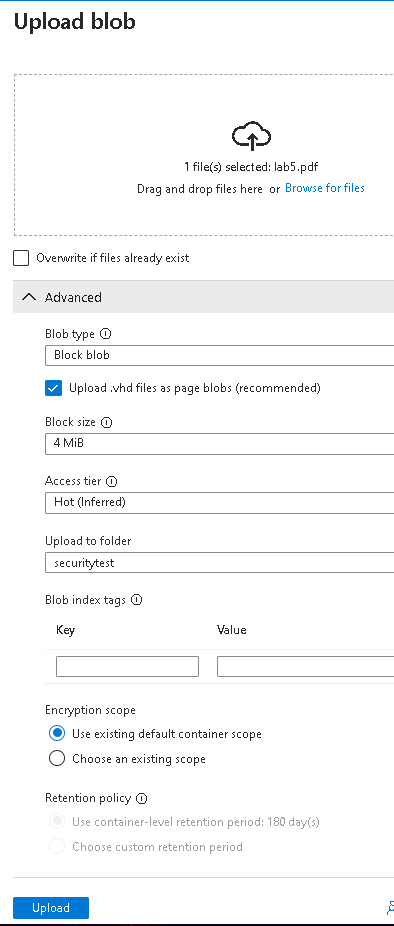
1.Return to the containers page, select your ****data**** container and then click ****Upload****.



2.On the ****Upload blob**** blade, expand the ****Advanced**** section.



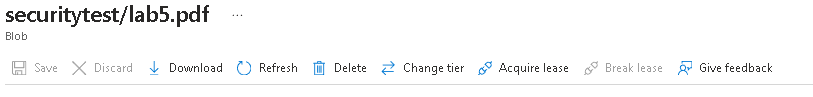
3.Click ****Upload****



4.Confirm you have a new folder, and your file was uploaded.

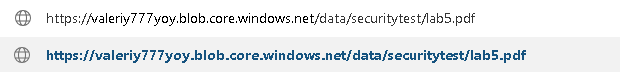


5.Select your upload file and review the options including ****Download****, ****Delete****, ****Change tier****, and ****Acquire lease****.

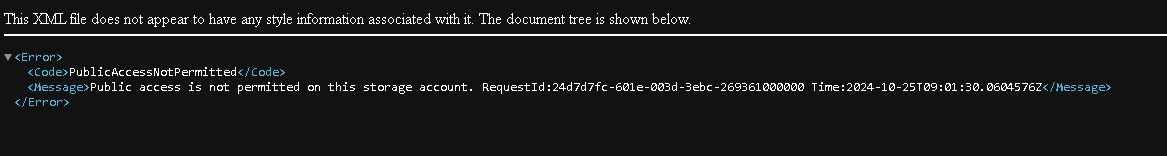


6.Copy the file ****URL**** and paste into a new ****Inprivate**** browsing window.



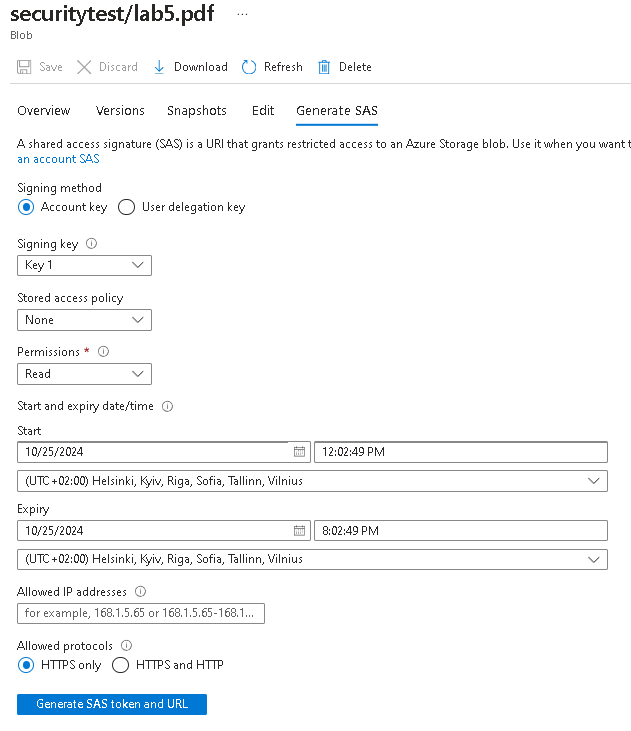


7.You should be presented with an XML-formatted message stating ****ResourceNotFound**** or ****PublicAccessNotPermitted****.

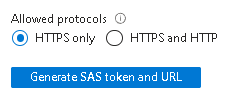


### Configure limited access to the blob storage

1.Select your uploaded file and then on the ****Generate SAS**** tab. You can also use the ellipsis (…) to the far right. Specify the following settings (leave others with their default values):



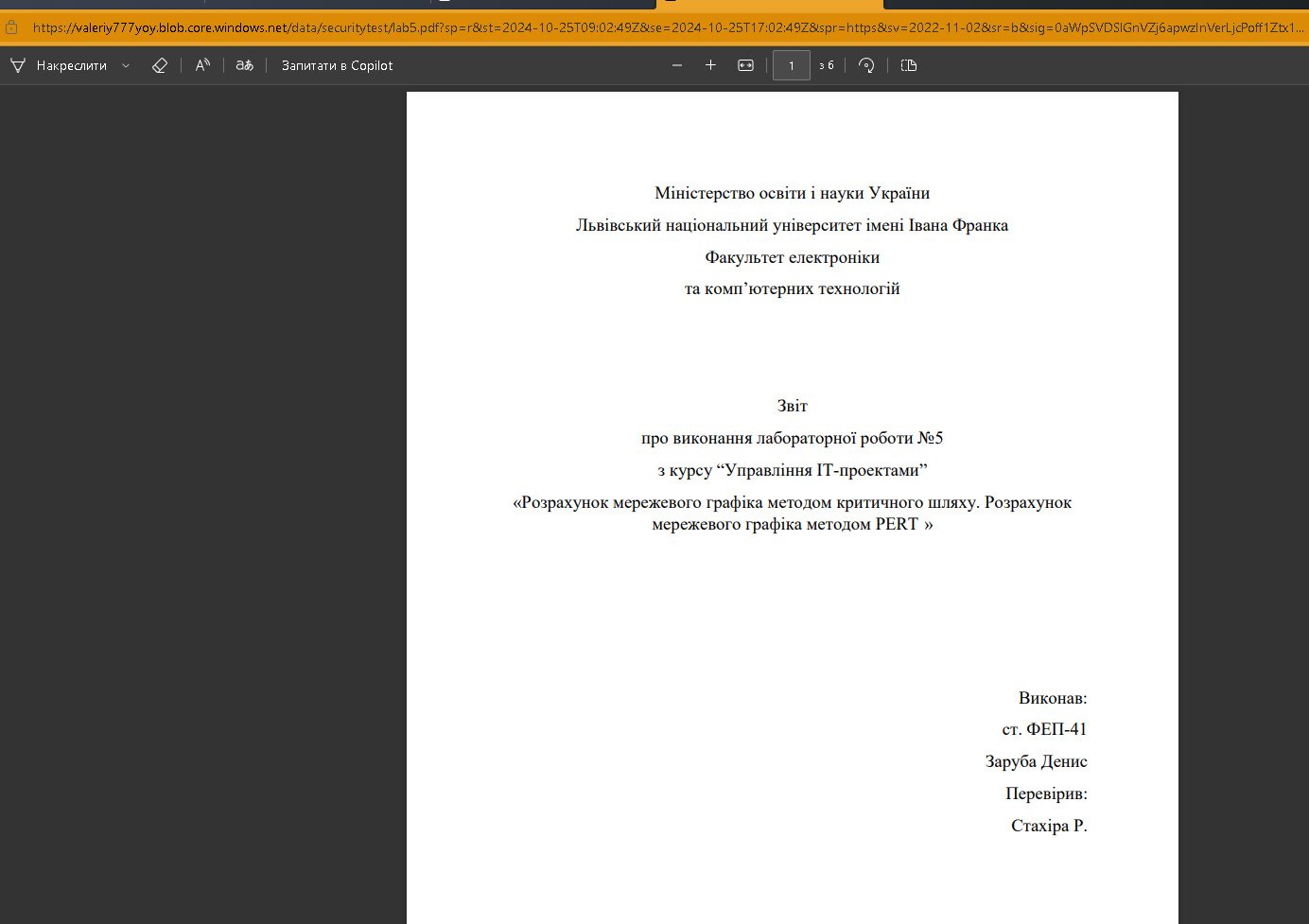
2.Click ****Generate SAS token and URL****.



3.Copy the ****Blob SAS URL**** entry to the clipboard.



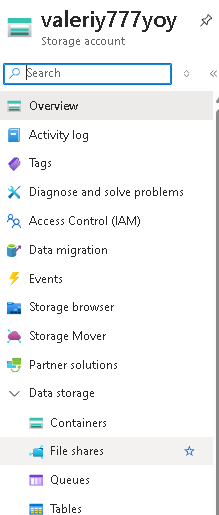
4.Open another InPrivate browser window and navigate to the Blob SAS URL you copied in the previous step.



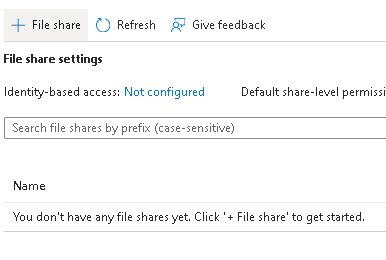
## Task 3: Create and configure an Azure File storage

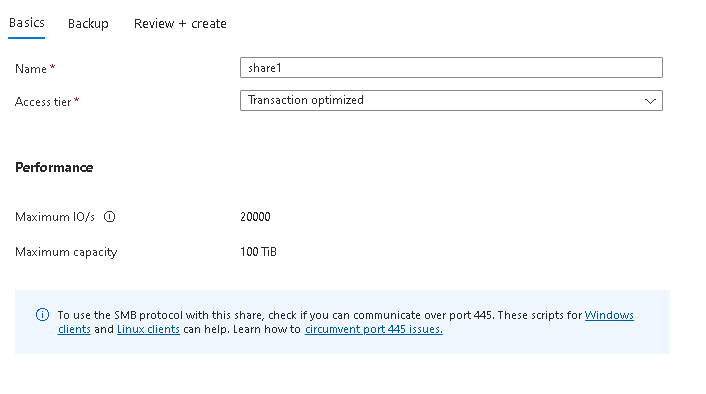
### Create the file share and upload a file

1.In the Azure portal, navigate back to your storage account, in the ****Data storage**** section, click ****File shares****.



2.Click ****+ File share**** and on the ****Basics**** tab give the file share a name, share1.

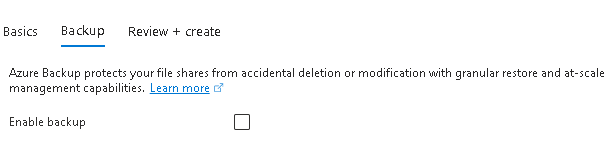




3.Notice the ****Access tier**** options. Keep the default ****Transaction optimized****.



4.Move to the ****Backup**** tab and ensure ****Enable backup**** is ****not**** checked. We are disabling backup to simplify the lab configuration.

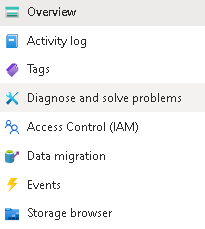


5.Click ****Review + create****, and then ****Create****. Wait for the file share to deploy.

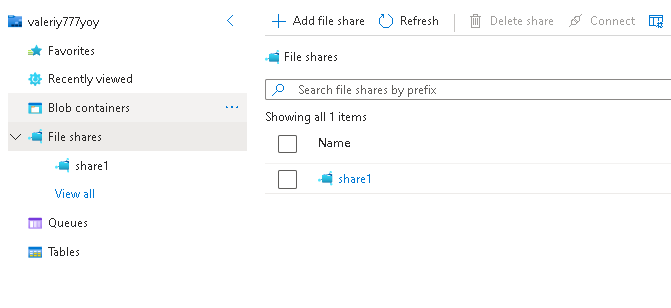


### Explore Storage Browser and upload a file

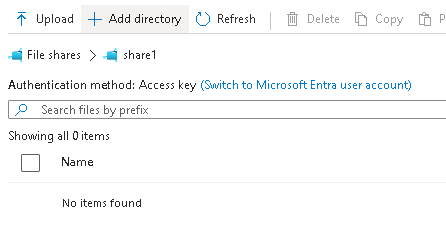
1.Return to your storage account and select ****Storage browser****. The Azure Storage Browser is a portal tool that lets you quickly view all the storage services under your account.



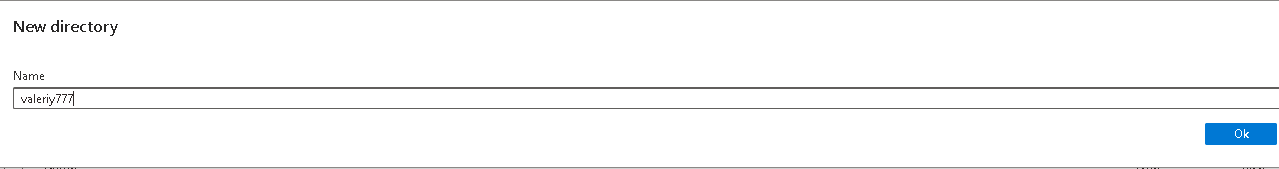
2.Select ****File shares**** and verify your ****share1**** directory is present.

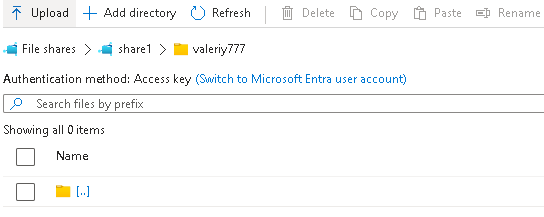


3.Select your ****share1**** directory and notice you can ****+ Add directory****. This lets you create a folder structure.



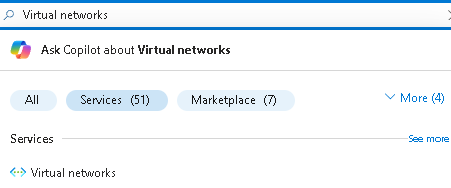
4.Select ****Upload****. Browse to a file of your choice, and then click ****Upload****.



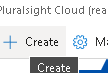


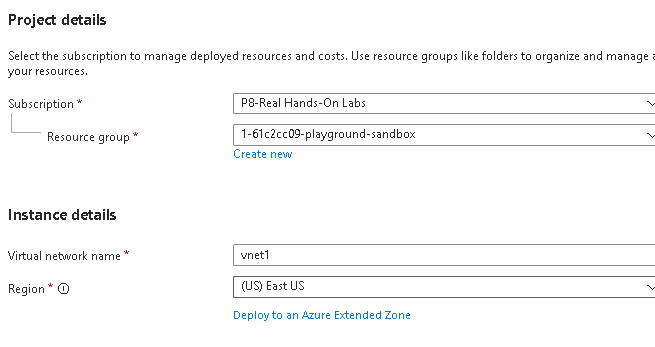
### Restrict network access to the storage account

1.In the portal, search for and select ****Virtual networks****.



2.Select ****+ Create****. Select your resource group. and give the virtual network a ****name****, vnet1.

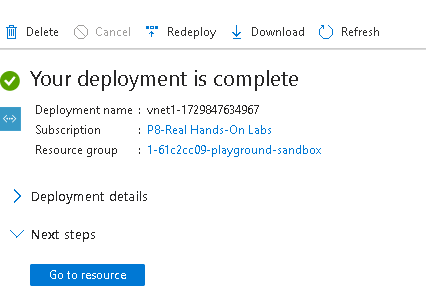




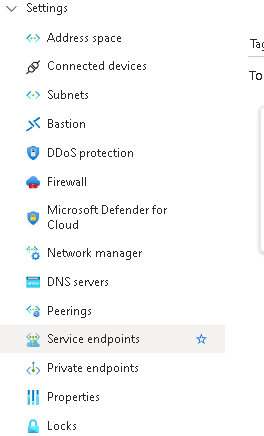
3.Take the defaults for other parameters, select ****Review + create****, and then ****Create****.

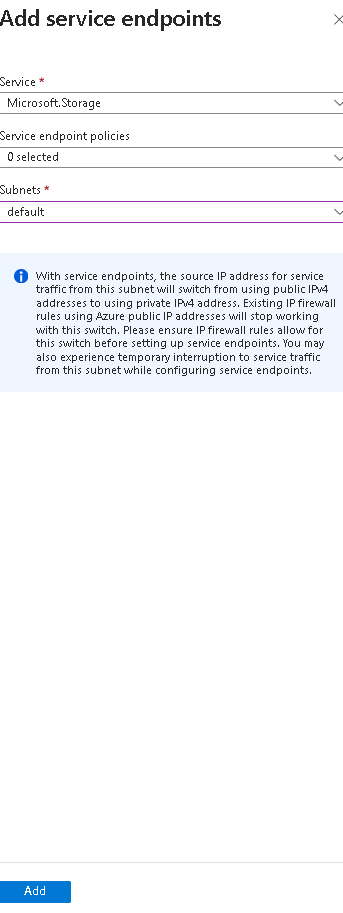


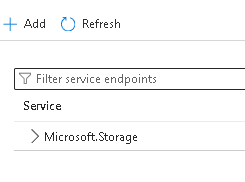
4.Wait for the virtual network to deploy, and then select ****Go to resource****.



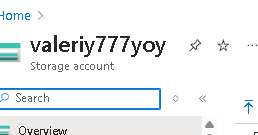
5.In the ****Settings**** section, select the ****Service endpoints**** blade.



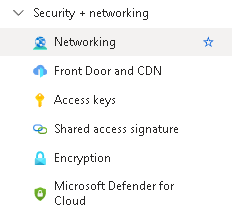




6.Return to your storage account.

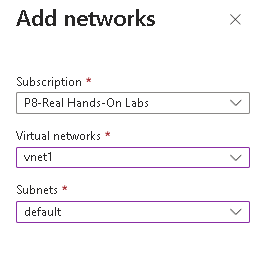


7.In the ****Security + networking**** section, select the ****Networking**** blade.



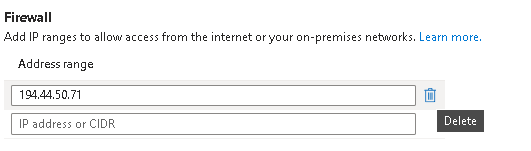
8.Select ****add existing virtual network**** and select ****vnet1**** and ****default**** subnet, select ****Add****.



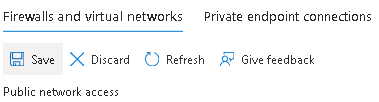


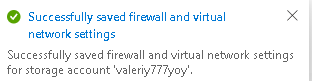


9.In the ****Firewall**** section, ****Delete**** your machine IP address. Allowed traffic should only come from the virtual network.

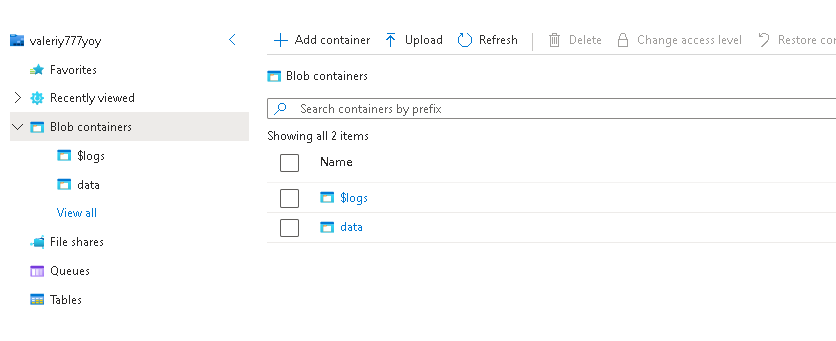


10.Be sure to ****Save**** your changes.





11.Select the ****Storage browser**** and ****Refresh**** the page. Navigate to your file share or blob content.



**Сonclusion:**

An Azure storage account contains all your Azure Storage data objects: blobs, files, queues, and tables. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS.

Azure storage provides several redundancy models including Locally redundant storage (LRS), Zone-redundant storage (ZRS), and Geo-redundant storage (GRS).

Azure blob storage allows you to store large amounts of unstructured data on Microsoft’s data storage platform. Blob stands for Binary Large Object, which includes objects such as images and multimedia files.

Azure file Storage provides shared storage for structured data. The data can be organized in folders.

Immutable storage provides the capability to store data in a write once, read many (WORM) state. Immutable storage policies can be time-based or legal-hold.