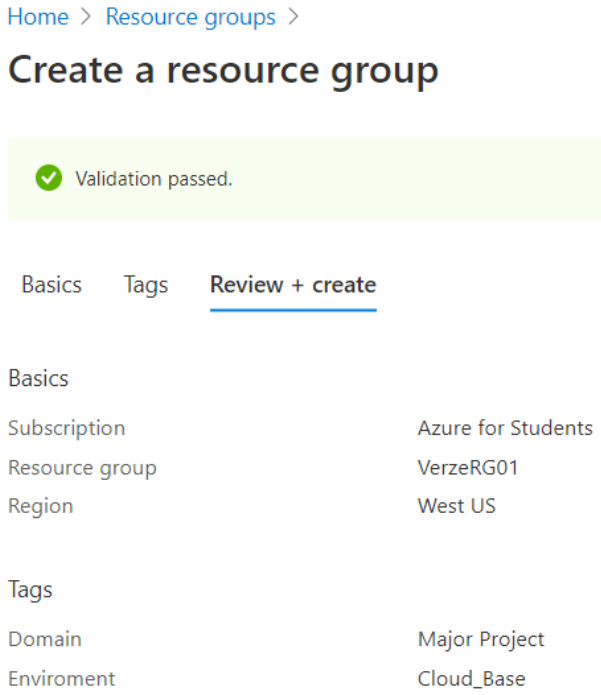
Azure Major Project 03 =>

KUSHAGRA BANSAL

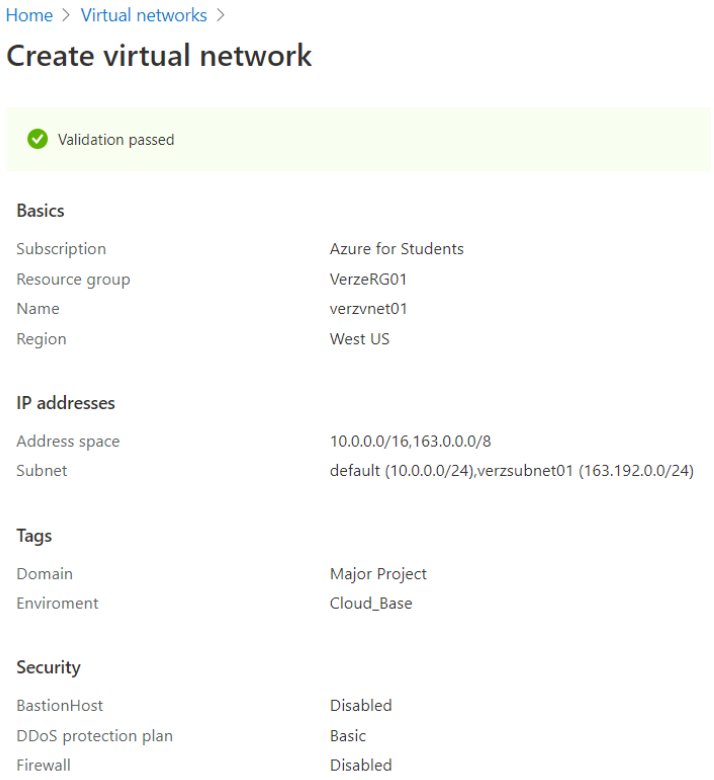
Step-1 : Create a Resource group by Name (VerzeRG01)

Resource groups: A resource group is a logical container into which **Azure resources** like web apps, databases, and storage accounts are deployed and managed.
Resources: Resources are instances of services that you create,like virtual machine,storage,or SQL databases.
Creating a resource group is the first most important thing to do before starting deploying anytime in azure.



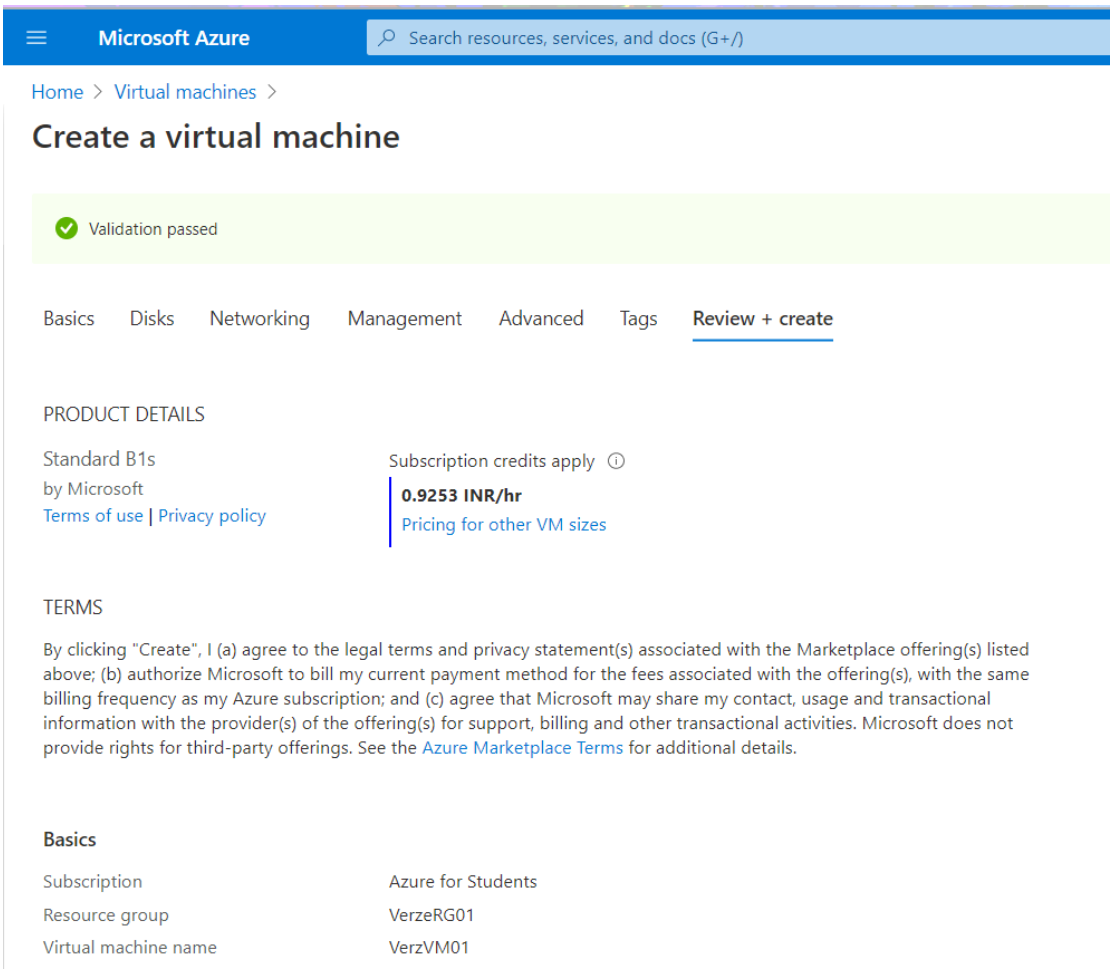
Step-2 : Create a virtual network (verzvnet01)

Azure Virtual Network (**VNet**) is the fundamental building block for your private **network in Azure.**
A **virtual network** is a **network** where all devices, servers, **virtual** machines, and data centers that are connected are done so through software and wireless technology. Results in securecommunicationamong each other, the internet, and on-premises **networks**.



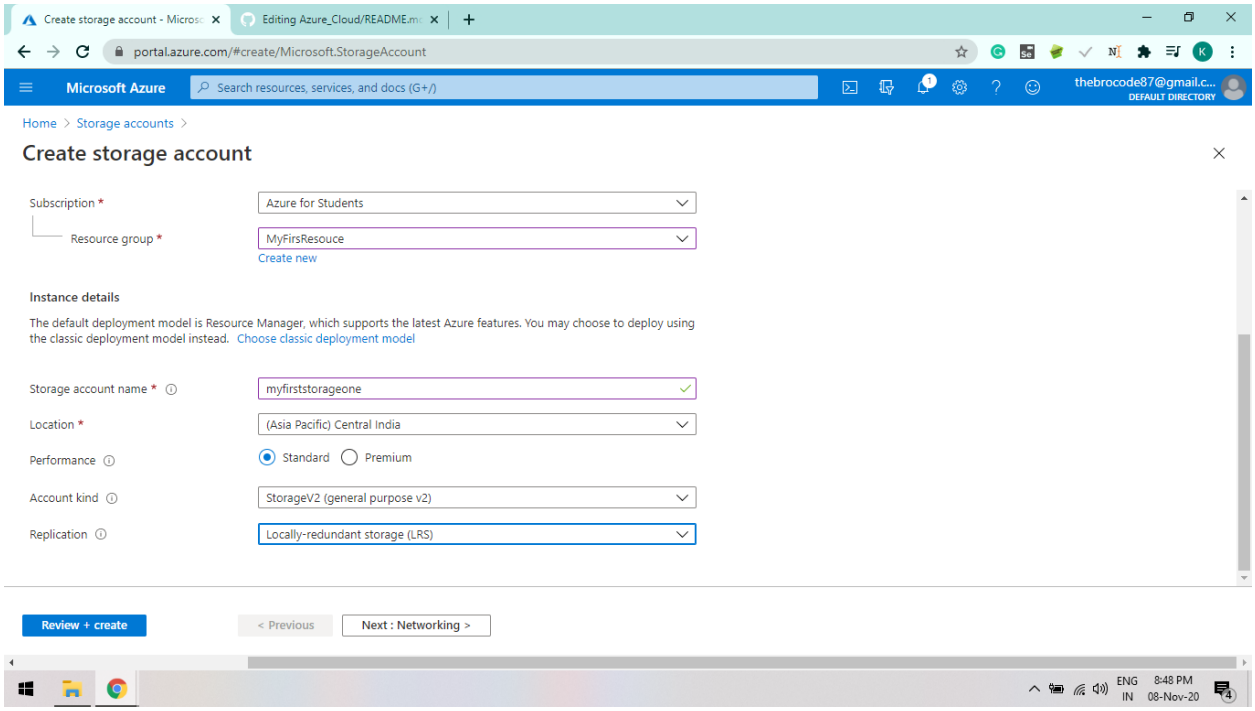
Step-3: Create a virtual machine in the portal(VerzVM01) =>

A **virtual machine** (VM) is a virtual environment that functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off- or on-premises).

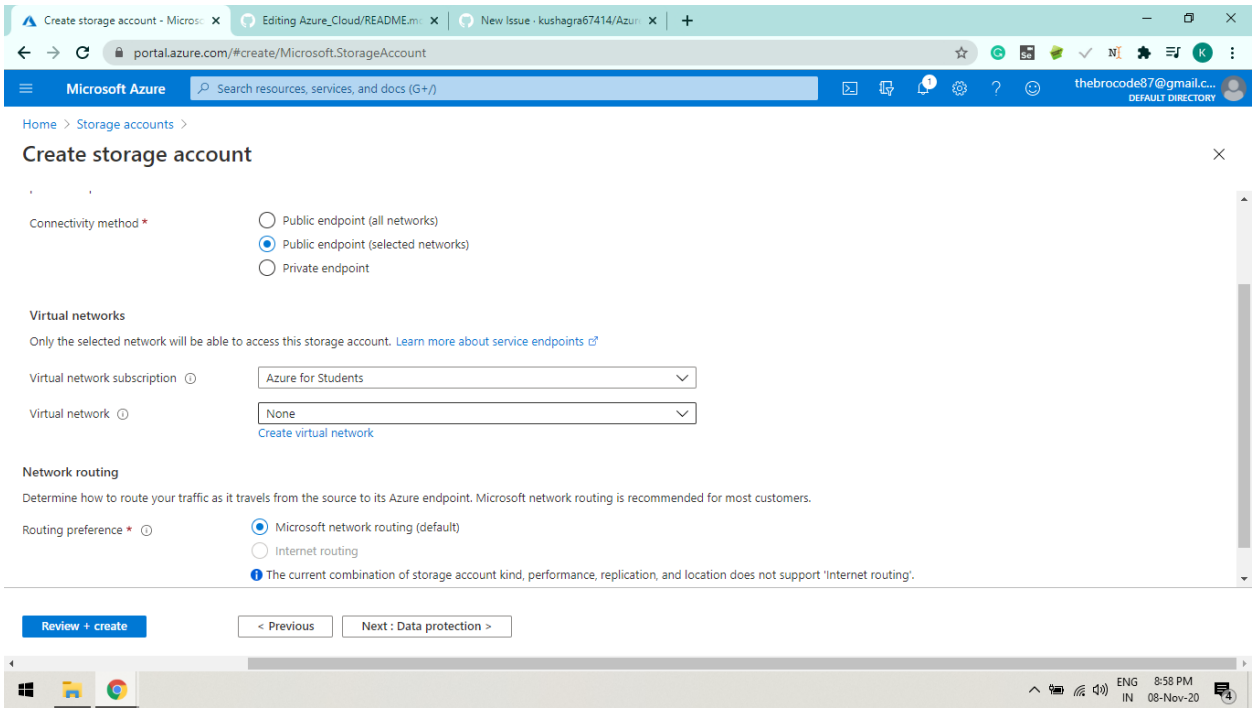


Step-4 : Create blob storage(VerzSTR01)

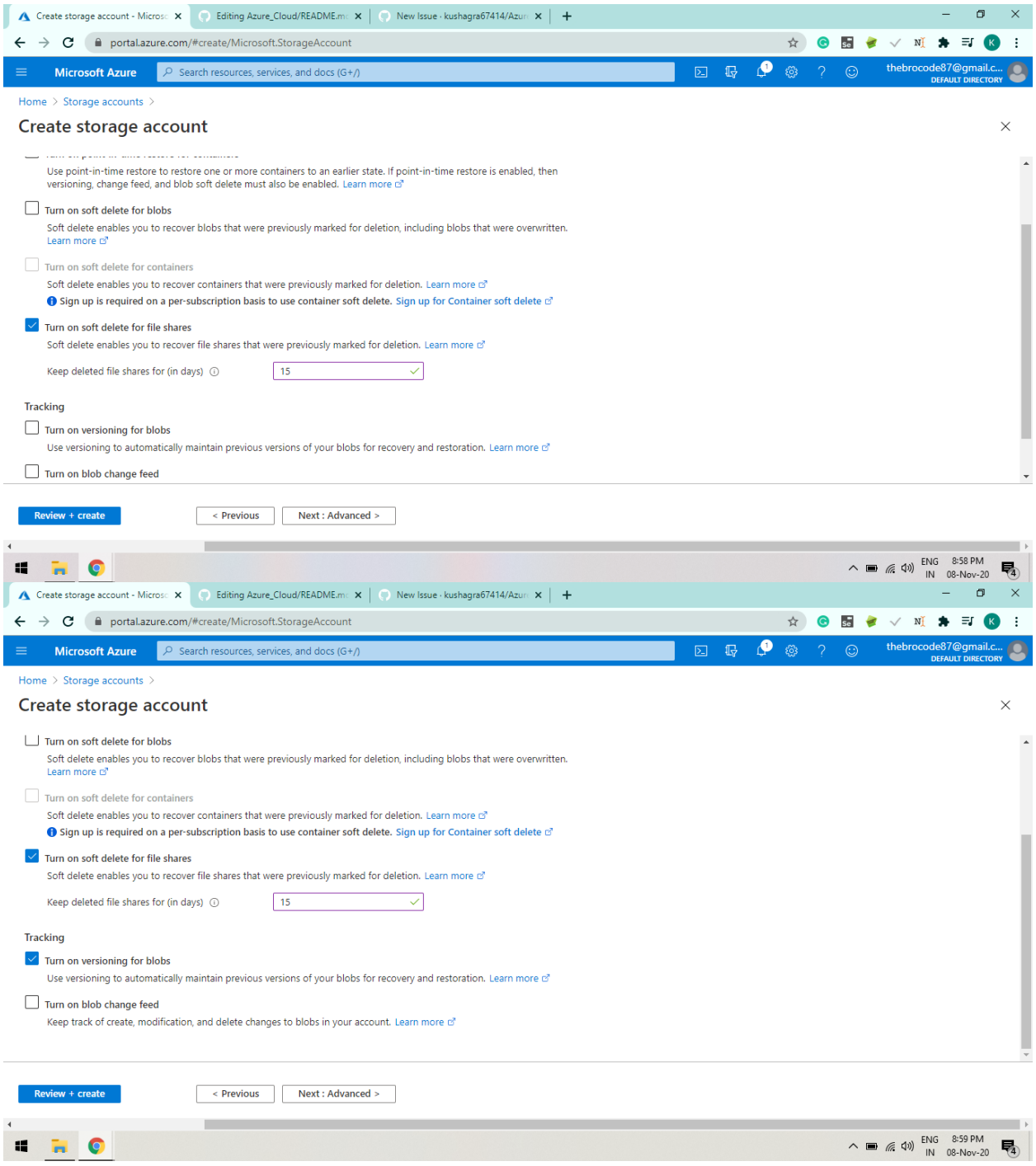
1. go to Storage Account.



2. Networking: default configurations

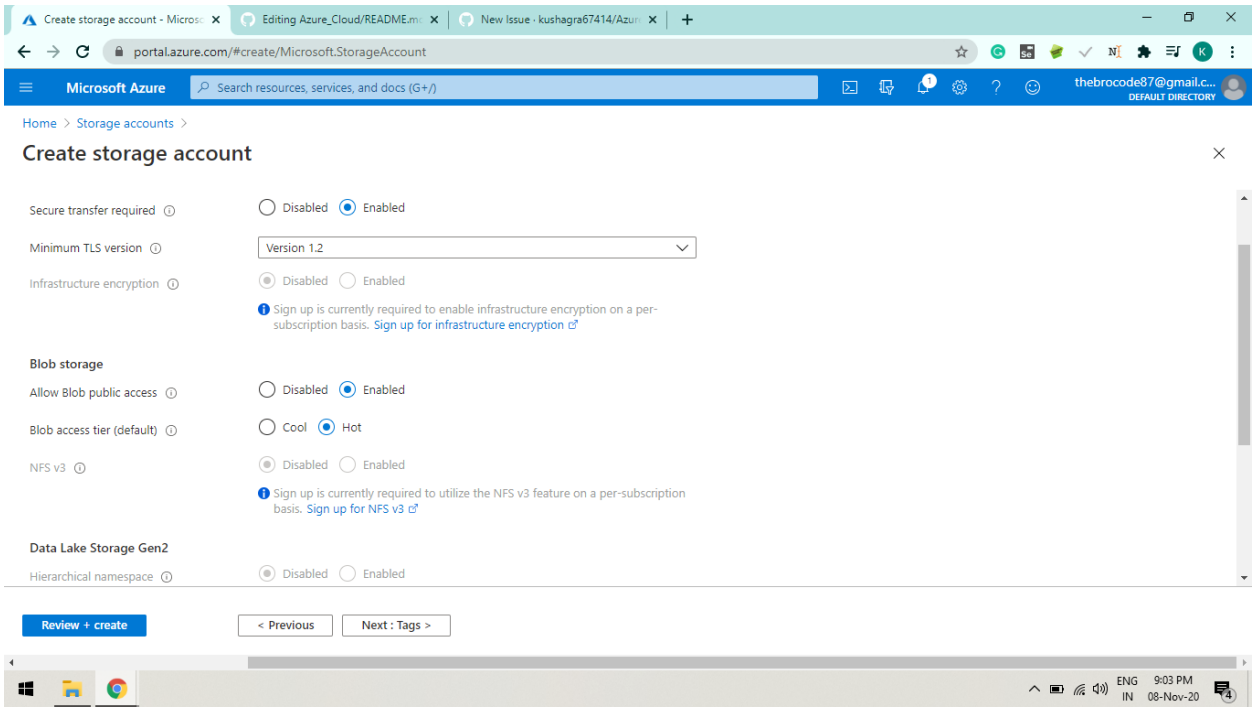


3. Data Protection: Turn on SOFT DELETE for BLOBS AND FILE SHARES

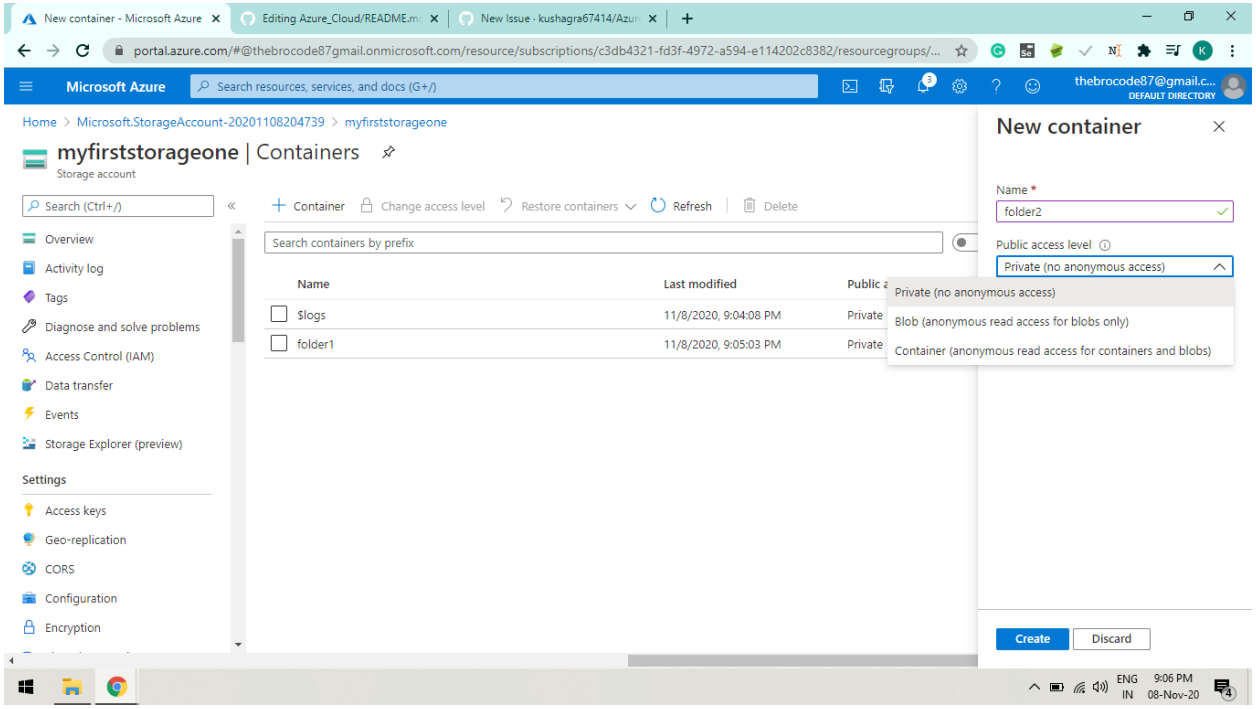


Here,

4. Advance :

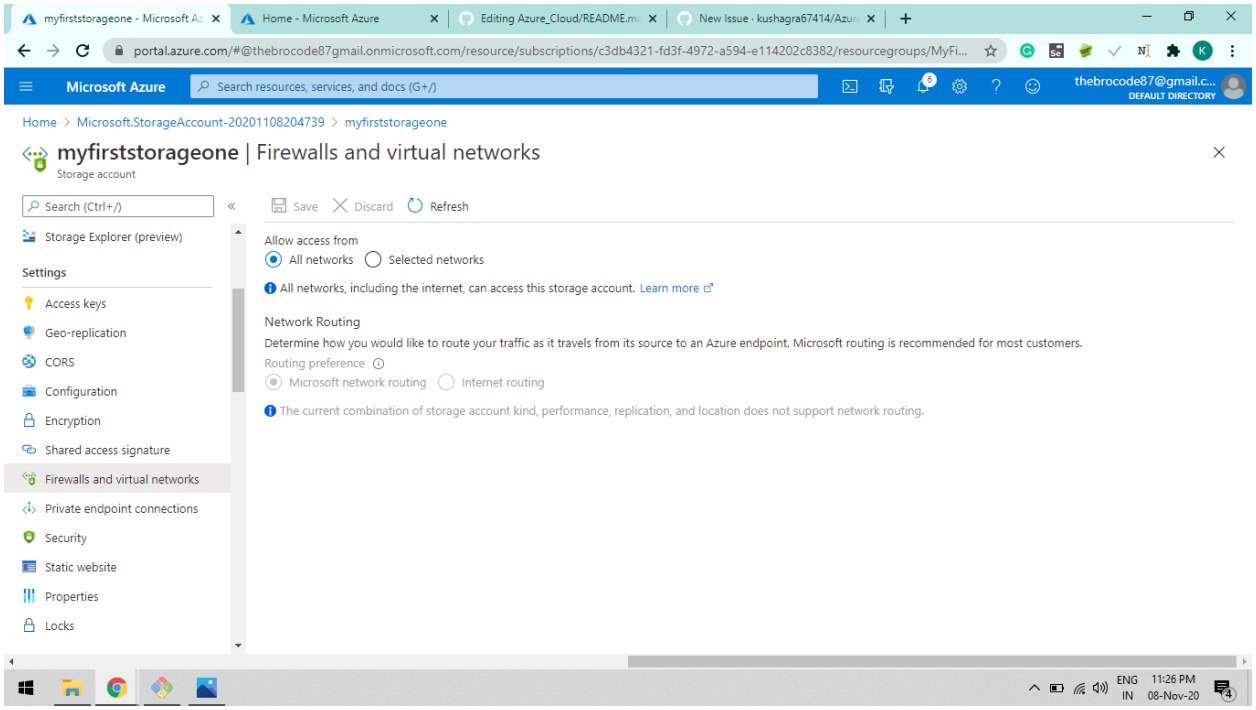


Now create the container, 5. Go To Container, option you will see inside your storage account

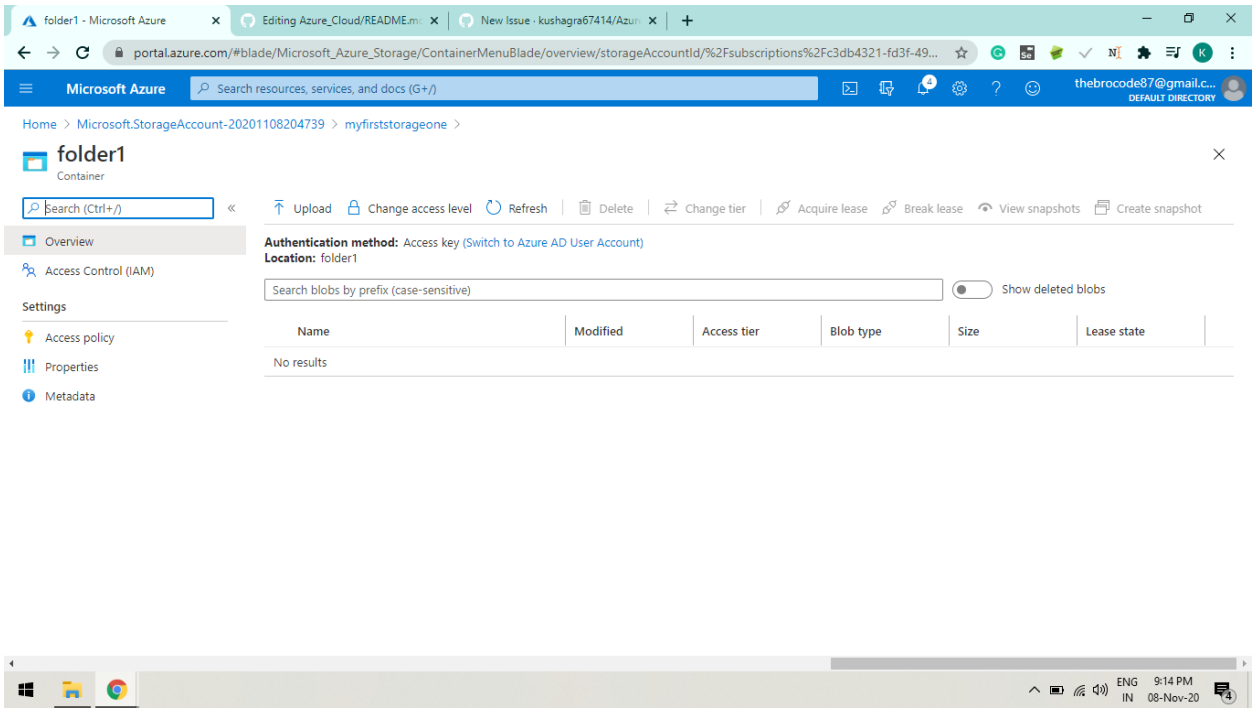


When you will access it, it will show "AUTHORIZATION FAILED" because At starting we didnt provide any network and our default setting is "SELECTED NETWORK" Which include no network connection. thats why the error comes.

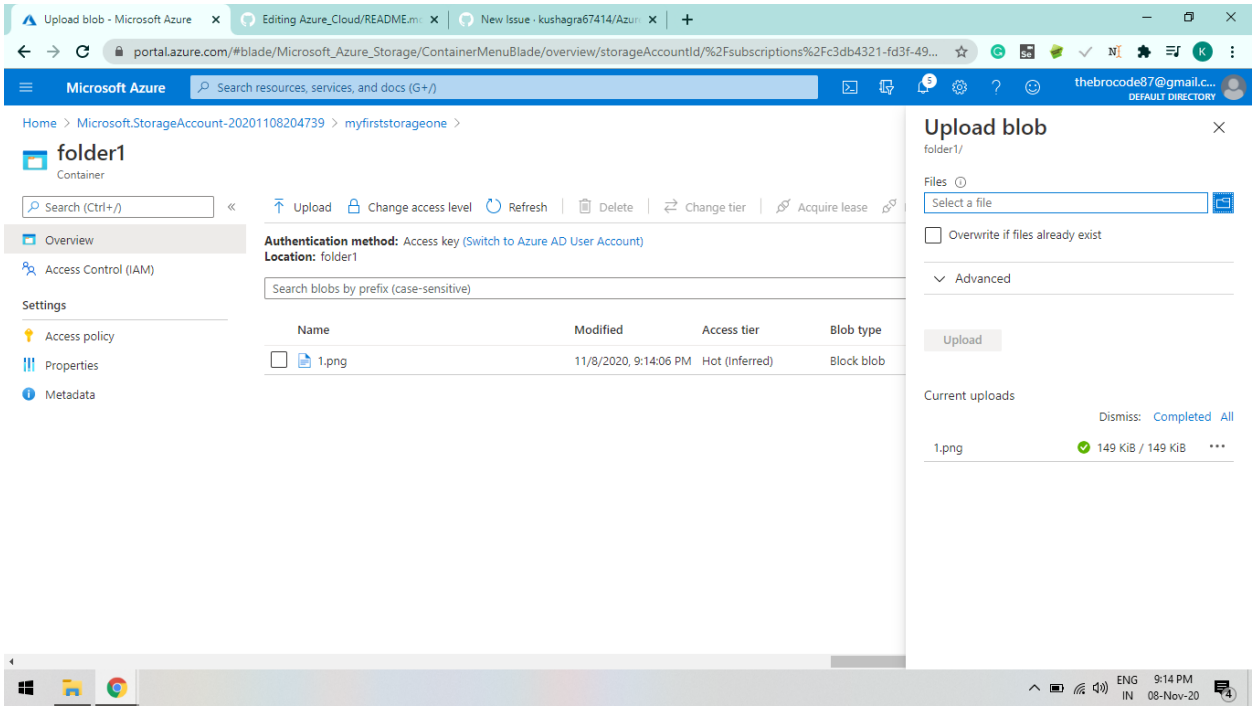
6. Go to "FIREWALLS AND VIRTUAL NETWORKS" and Select "ALL NETWORKS"



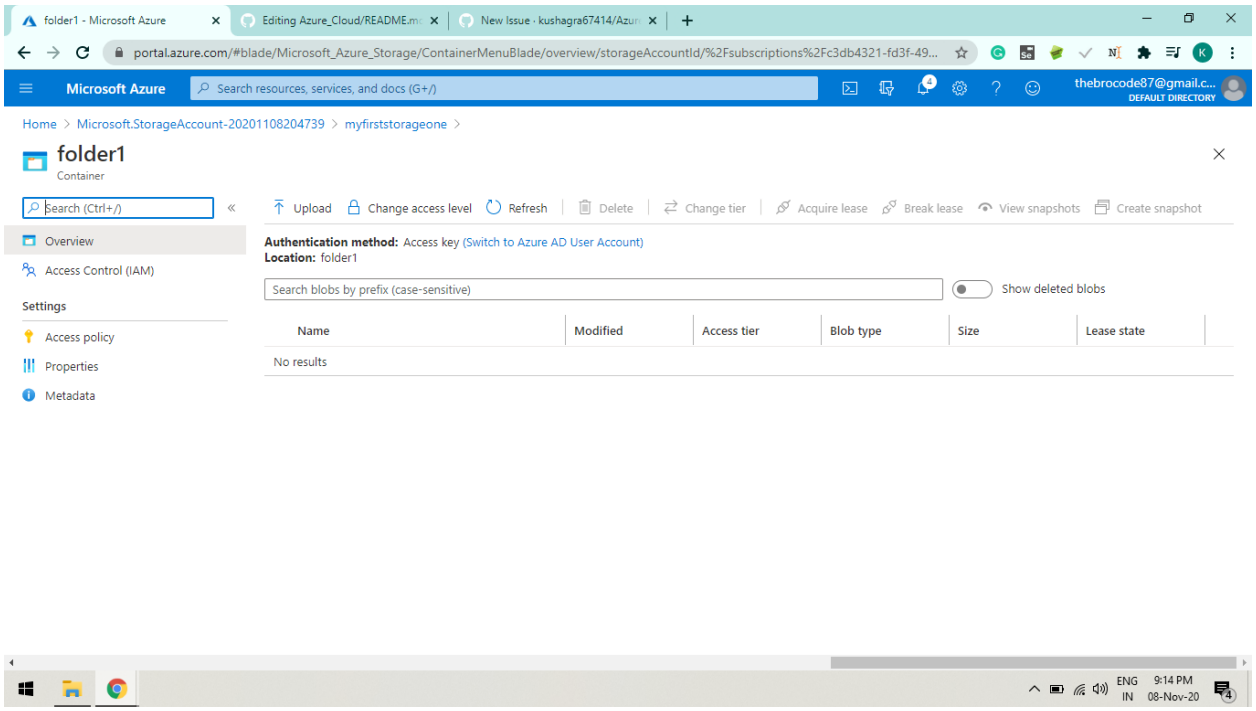
after this when you will access it again it will give the access to the container.



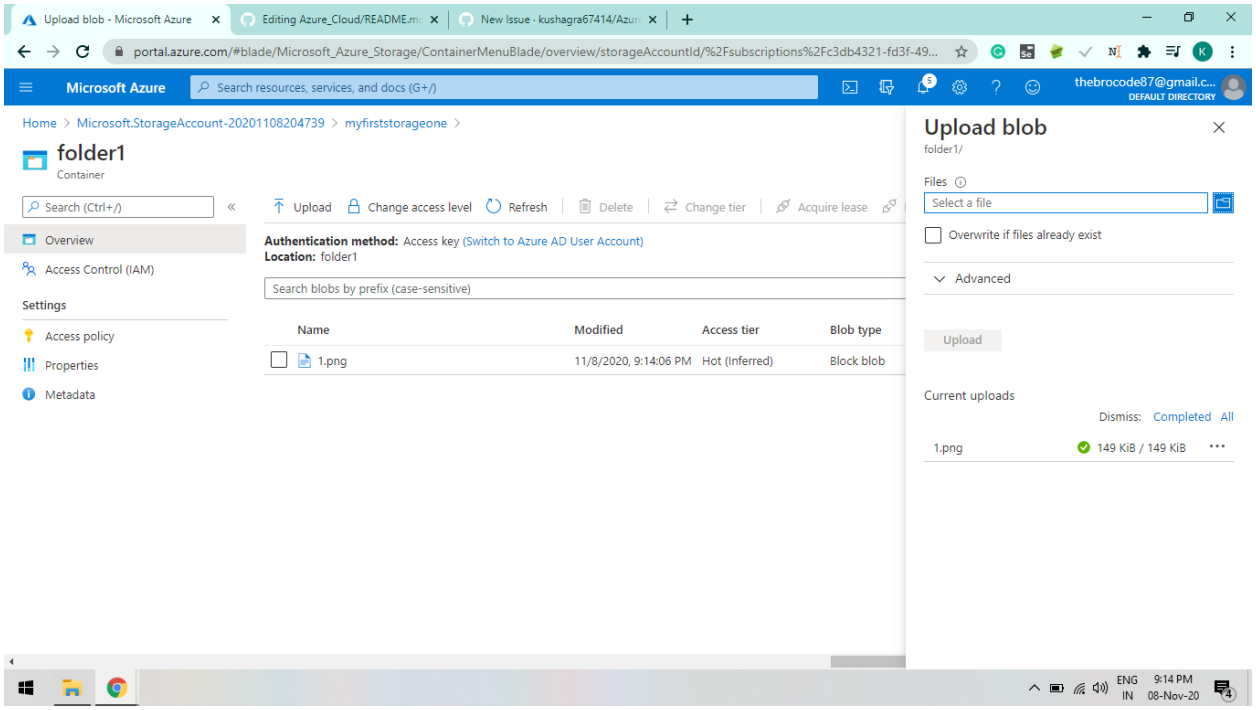
7. Now you can add any data just go to "UPLOAD" AND select data what you want from your local machine.



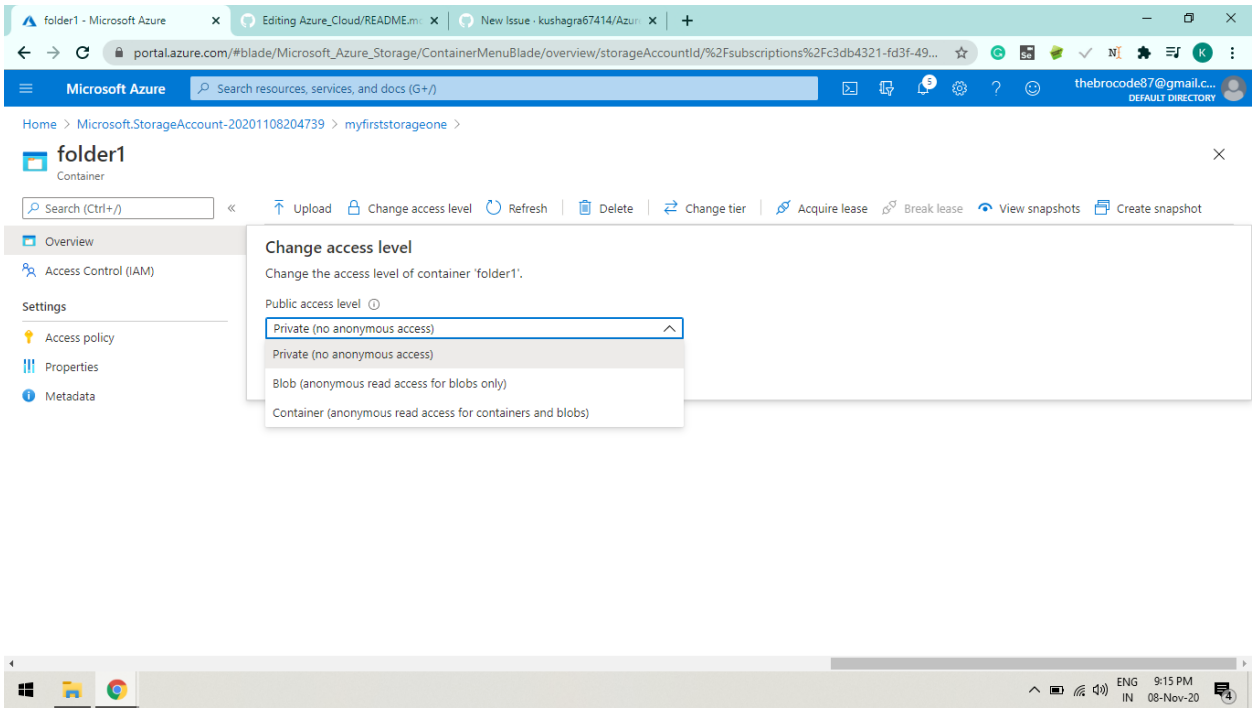
after this when you will access it again it will give the access to the container.



7. Now you can add any data just go to "UPLOAD" AND select data what you want from your local machine.



8. Now if you copied the link and try to run it, it will show you an error because access level is set to a private. go to "CHANGE ACCESS LEVEL" and change it too BLOB or CONTAINER.

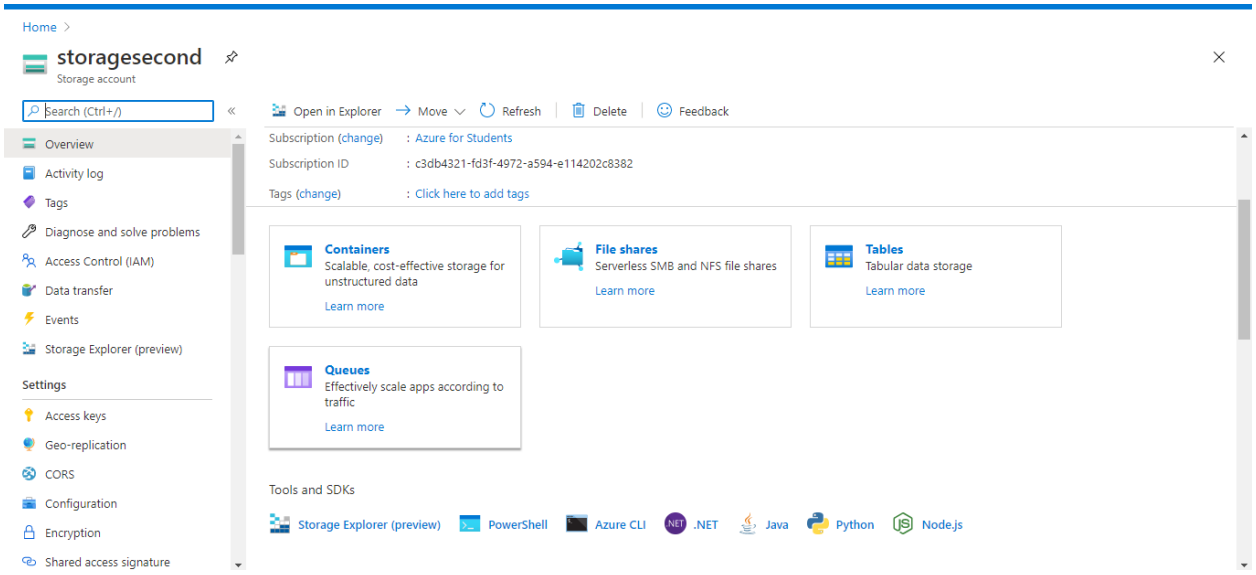


b. Create a File Share (Verzfs01)and mount on the (VerzVM01)

=> How to create a drive at your local machine using Azure Cloud.

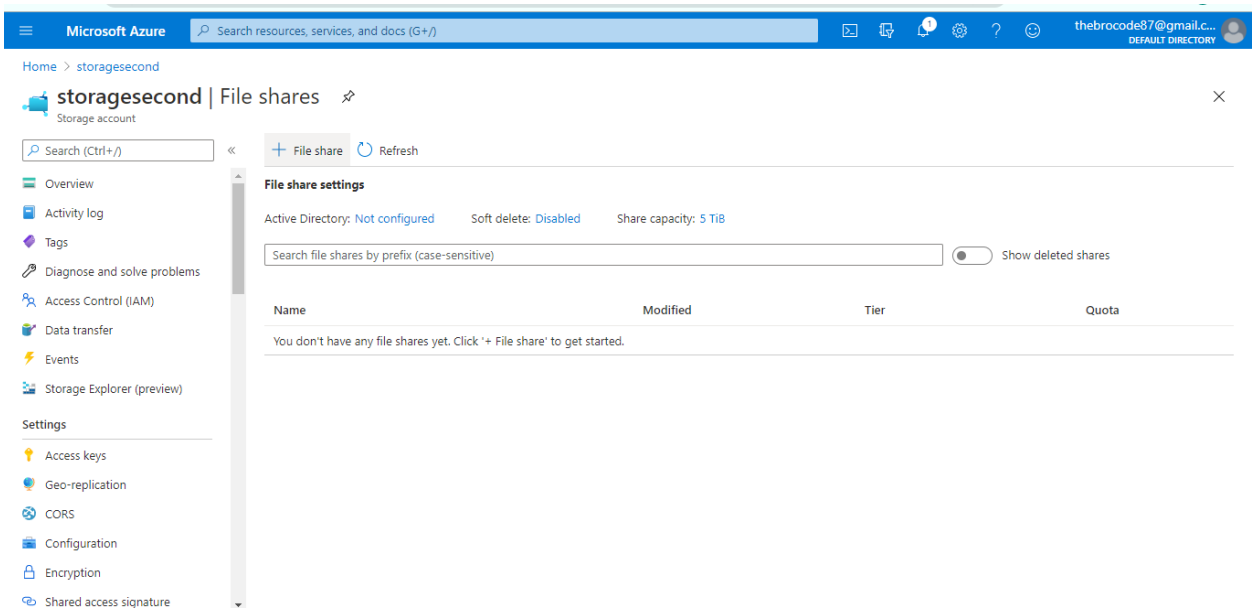
Step-1:

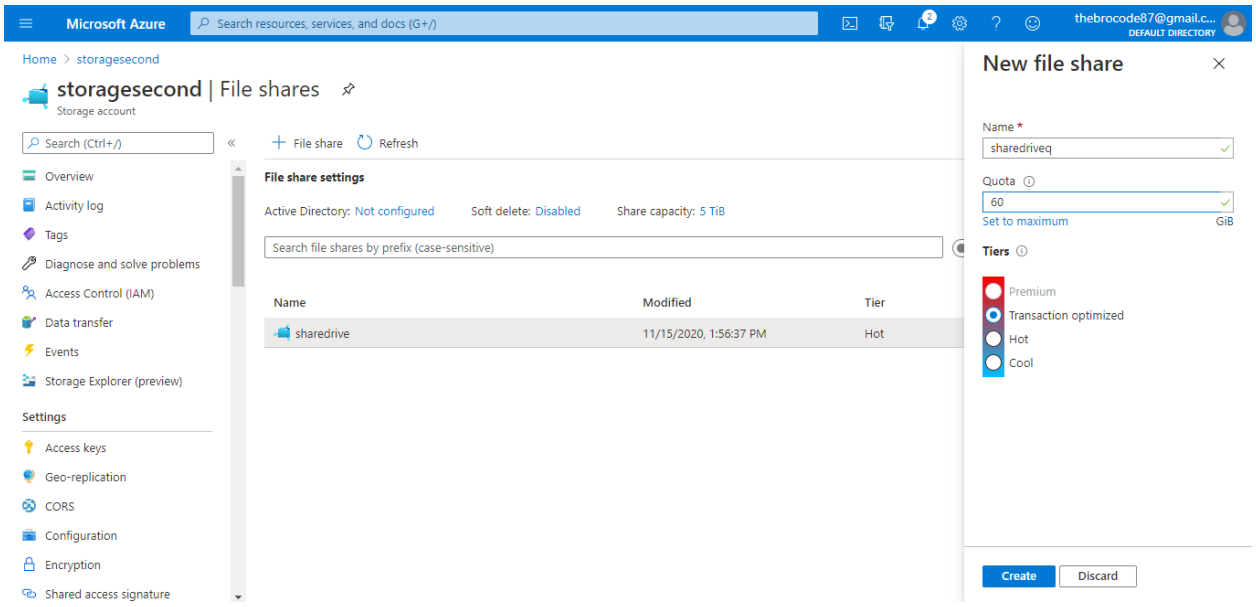
Create a Storage Account say "storagesecond" and go to File shares



Step-2:

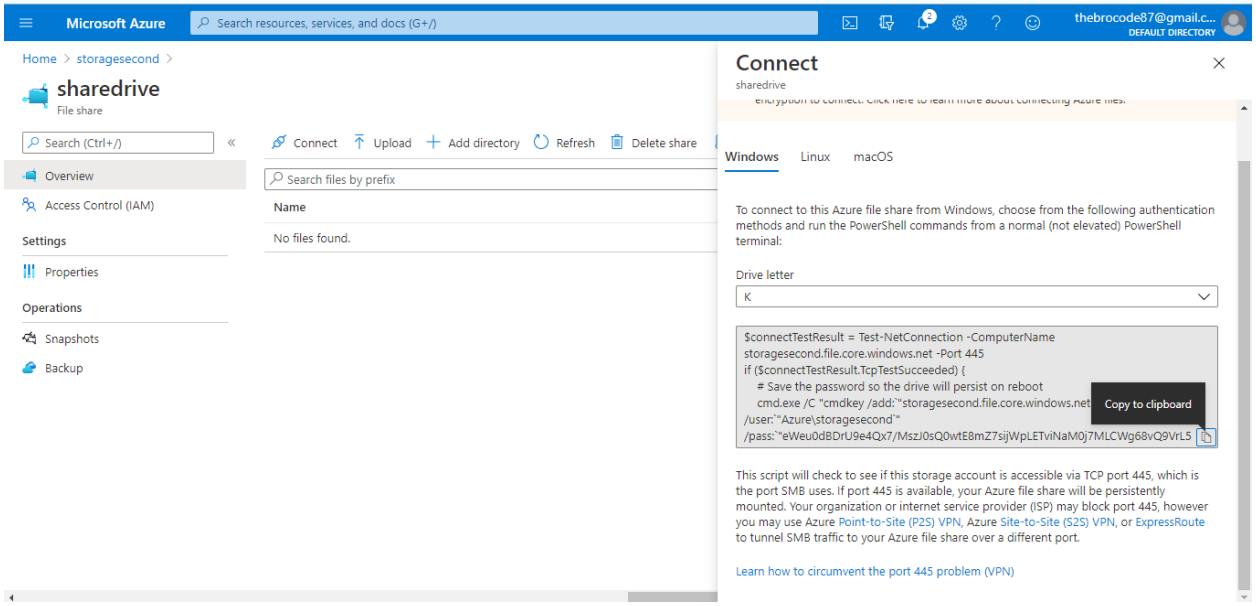
Create a file in "FILE SHARES" let say sharedrive

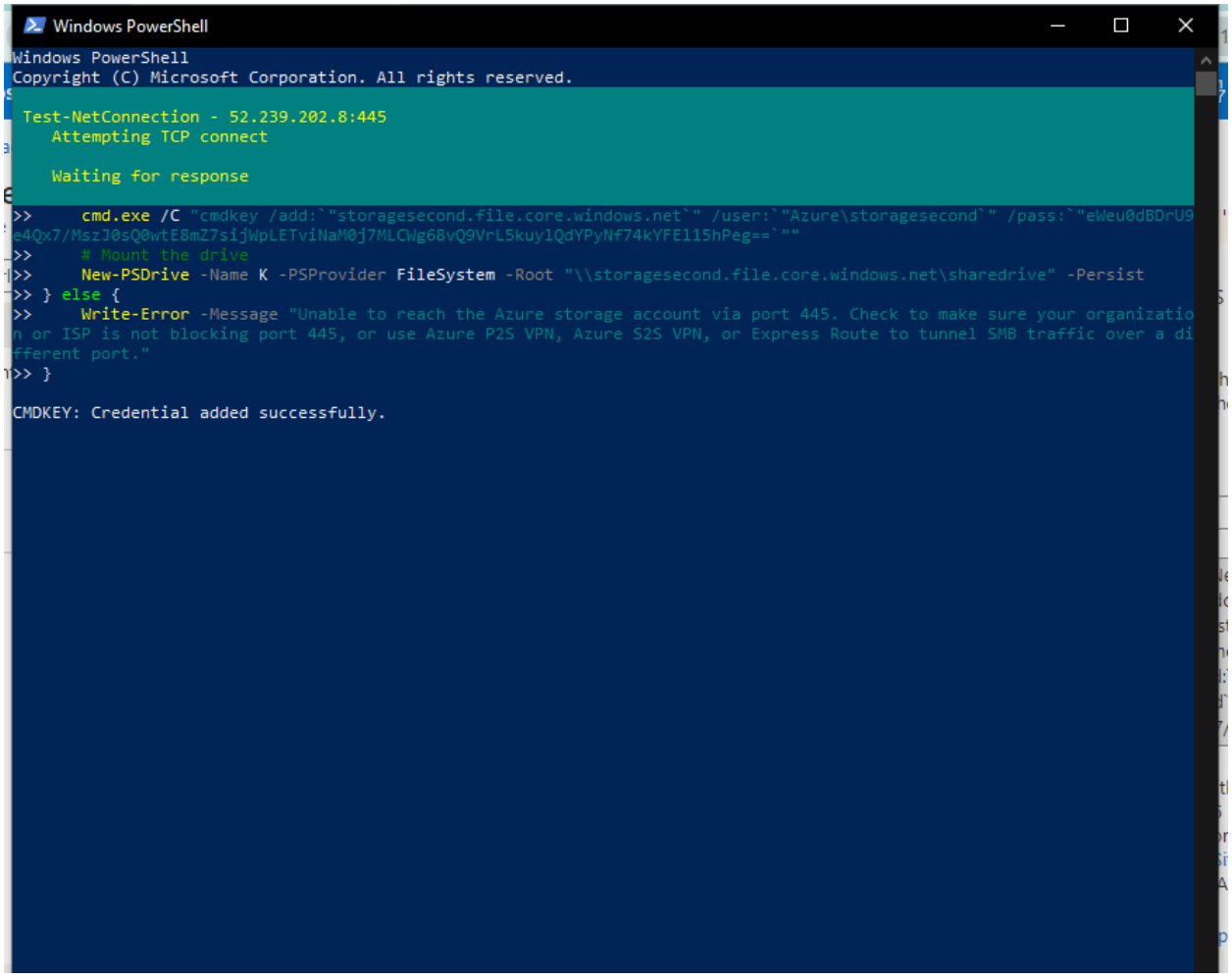




Step-3:

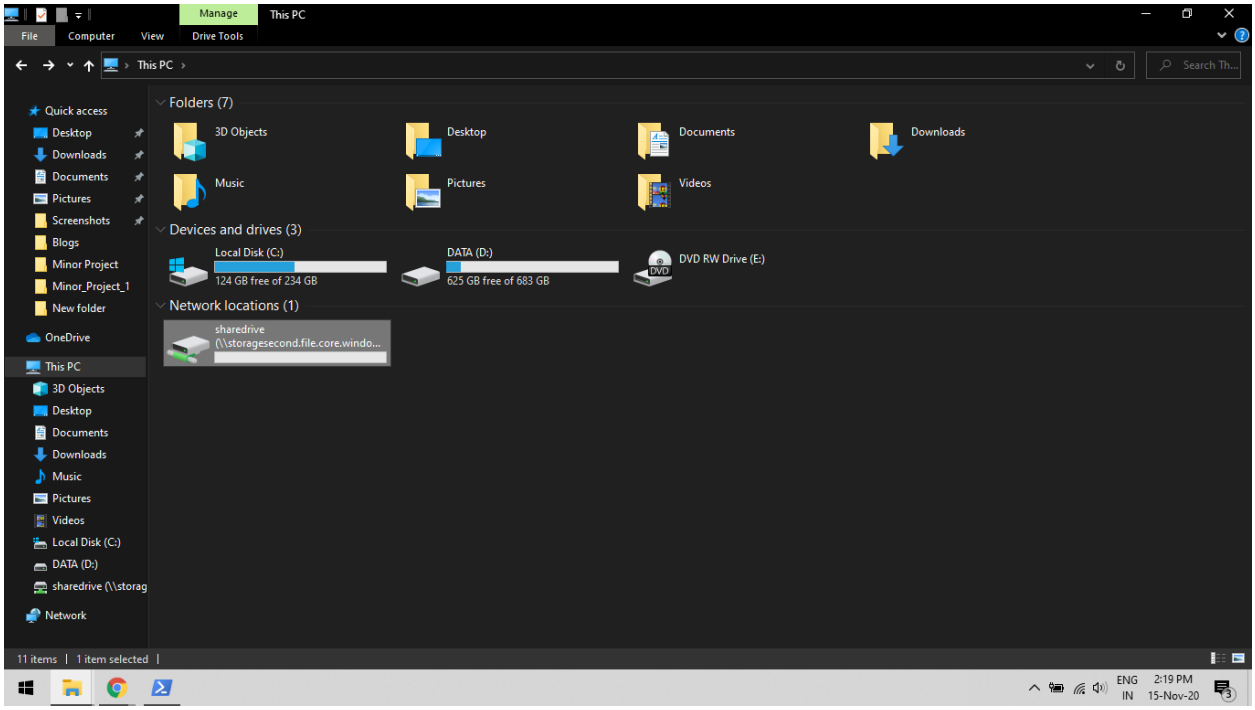
Open the sharedrive and click to connect. You will get a Script for WINDOWS, LINUX AND MACOS. Here we will use windows script to to connect. and script is run on the powershell. Open Start> type powershell press enter and after the Windows PowerShell open paste the script.


Microsoft Azure
Search resources, services, and docs (G+/)
thebrocode87@gmail.c...
DEFAULT DIRECTORY
Home > storagesecond >
sharedrive
File share
Search (Ctrl+/)
Overview
Access Control (IAM)
Settings
Properties
Operations
Snapshots
Backup
Connect
Upload
Add directory
Refresh
Delete share
Search files by prefix
Name
No files found.
Connect
sharedrive
Windows
Linux
macOS
To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:
Drive letter
K
$connectTestResult = Test-NetConnection -ComputerName storagesecond.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
# Save the password so the drive will persist on reboot
cmd.exe /C "cmdkey /add:`"storagesecond.file.core.windows.net
/user:`"Azure\storagesecond`"
/pass:`"eWeu0dBDrU9e4Qx7/MszJ0sQ0wtE8mZ7sijWpLETviNaM0j7MLCWg68vQ9VrL5
Copy to clipboard
This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure Point-to-Site (P2S) VPN, Azure Site-to-Site (S2S) VPN, or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port.
Learn how to circumvent the port 445 problem (VPN)


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Test-NetConnection - 52.239.202.8:445
Attempting TCP connect
Waiting for response
>> cmd.exe /C "cmdkey /add:`"storagesecond.file.core.windows.net`" /user:`"Azure\storagesecond`" /pass:`"eWeu0dBDrU9e4Qx7/MszJ0sQ0wtE8mZ7sijWpLETviNaM0j7MLCWg68vQ9VrL5kuy1QdYPyNf74kYFE115hPeg==`""
>> # Mount the drive
>> New-PSDrive -Name K -PSProvider FileSystem -Root "\\storagesecond.file.core.windows.net\sharedrive" -Persist
>> } else {
>> Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
>> }
CMDKEY: Credential added successfully.

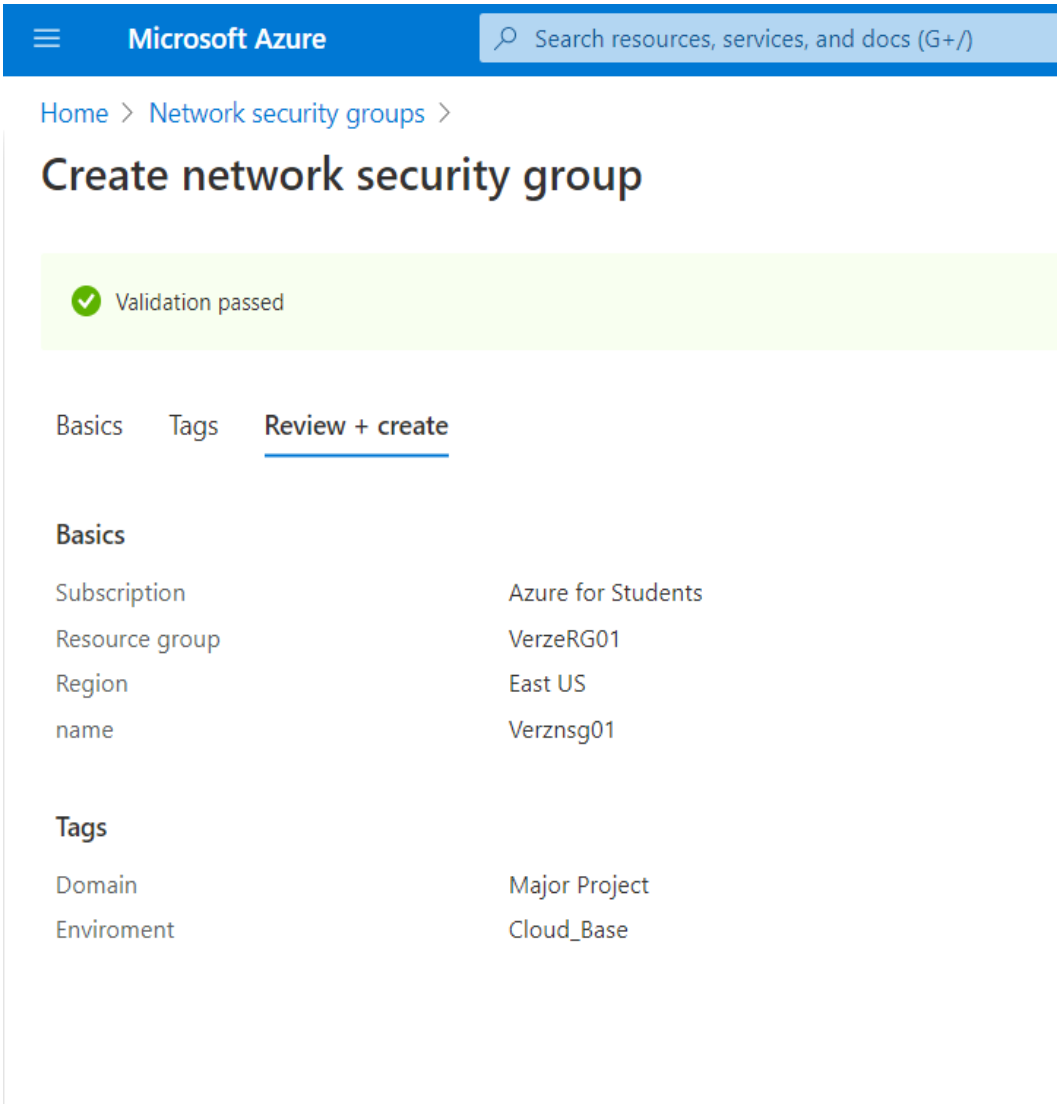
Step-4:

Go to your "This pc" and you will a File share storage.

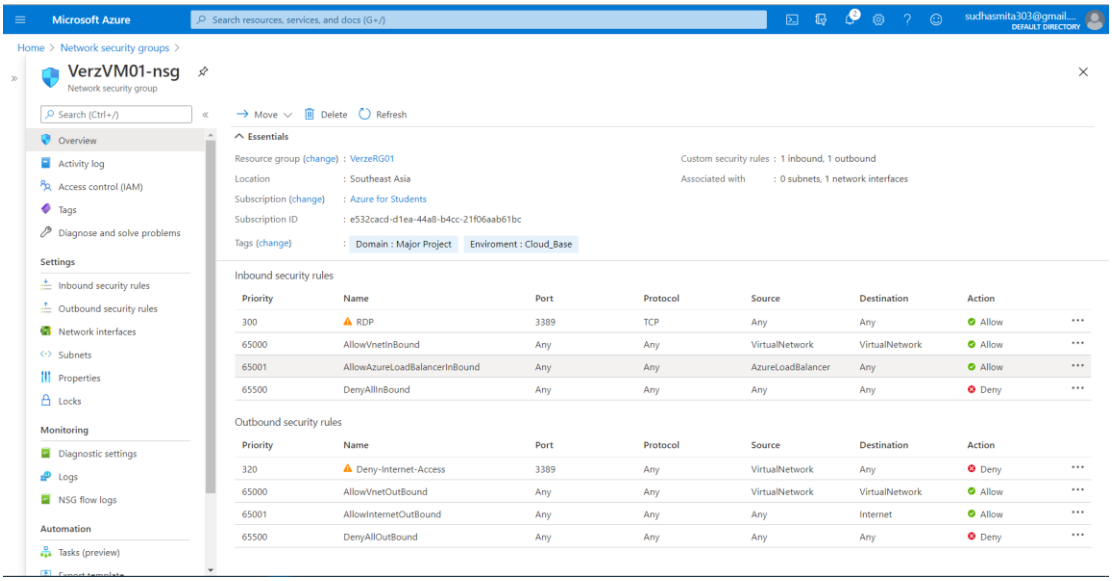


Step-5 : Create a network security group

Network Security Groups provide control over **network** traffic flowing in and out of your services running in **Azure**. **Network Security Groups** can also be applied to a Subnet in a Virtual Network thus they provide an efficient mechanism to administer access control rule updates across multiple VMs. A **Network Security Group** contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of **Azure** resources



Step-6 & 7: Configure an inbound security port rule to allow RDP and an outbound security port rule to deny Internet access.



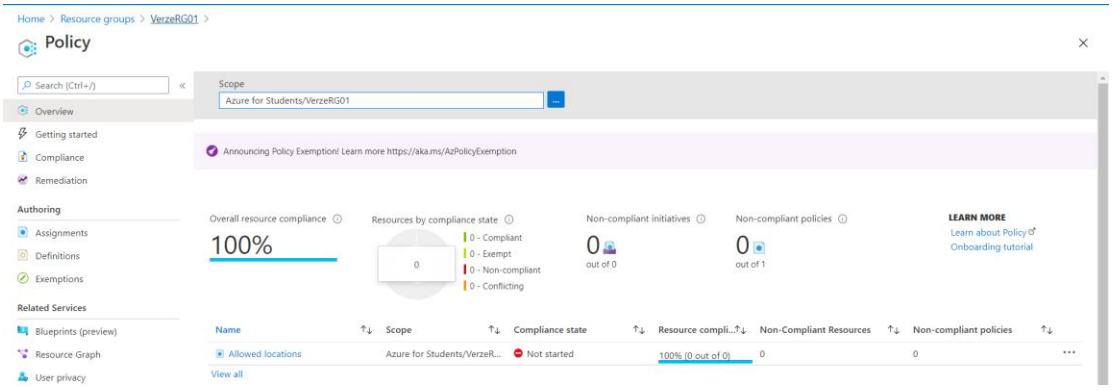
Inbound and Outbound =>

A network security group contains Rules that allow or deny inbound network traffic to,or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.The below Screen Shot represents an inbound security port rule that allow RDP and an outbound security port rule deny Internet access.

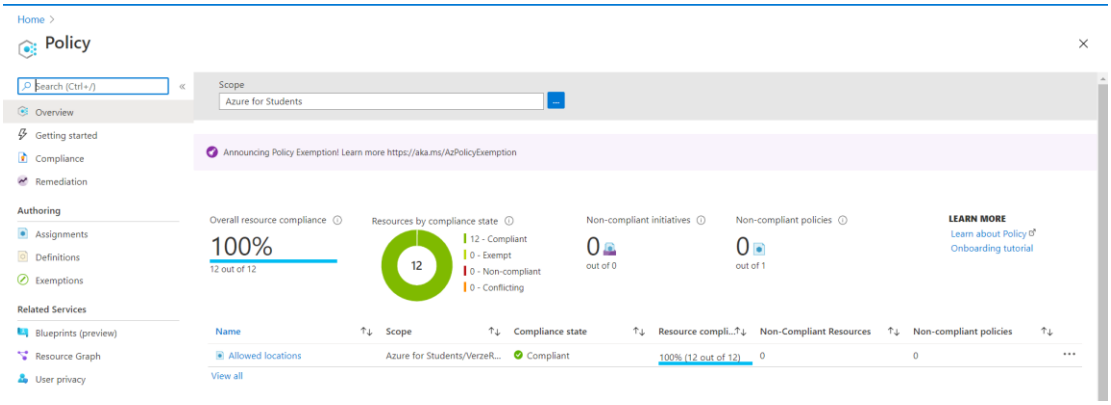
Step-8 : Create an Azure Policy to only allow certain locations (Southeast Asia), try to create a resource in any other location and check the policy evaluation.(You can use any other region)

Azure policy establishes conventions for resources. Policy describes resource compliance conditions and the effect to take if a condition is met. It helps us **manage and prevent IT issues** with policy definitions that enforces rules and effects for our resources. In Azure policy the business rules,described in JSON format, are known as **Policy** definitions. Allowed only certain locations[Southeast Asia].

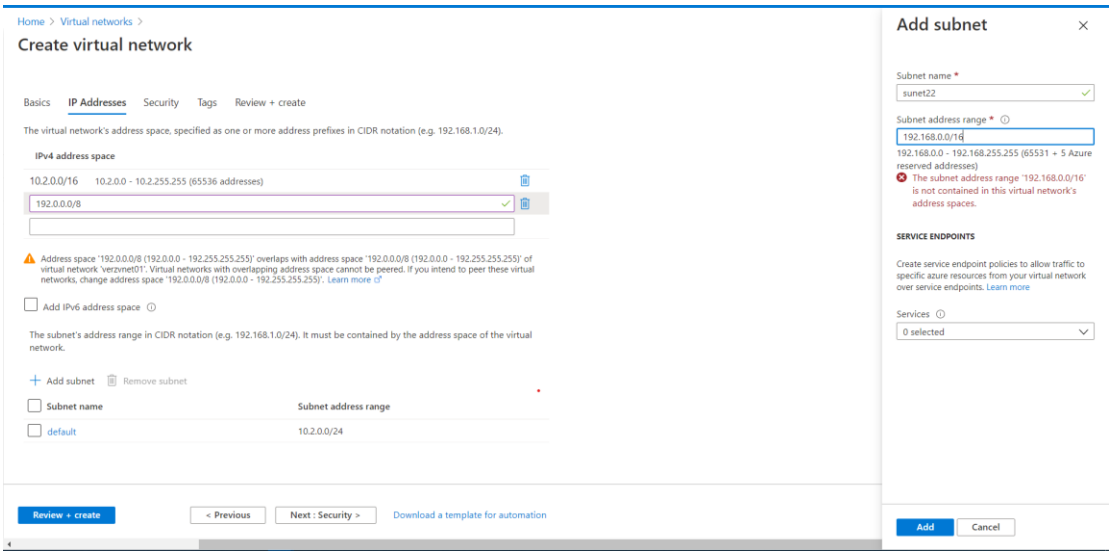
1. Policy not started =>



2. Policy Started =>



We can't create a resource in any other location.It restricts the available Locations for new resources.

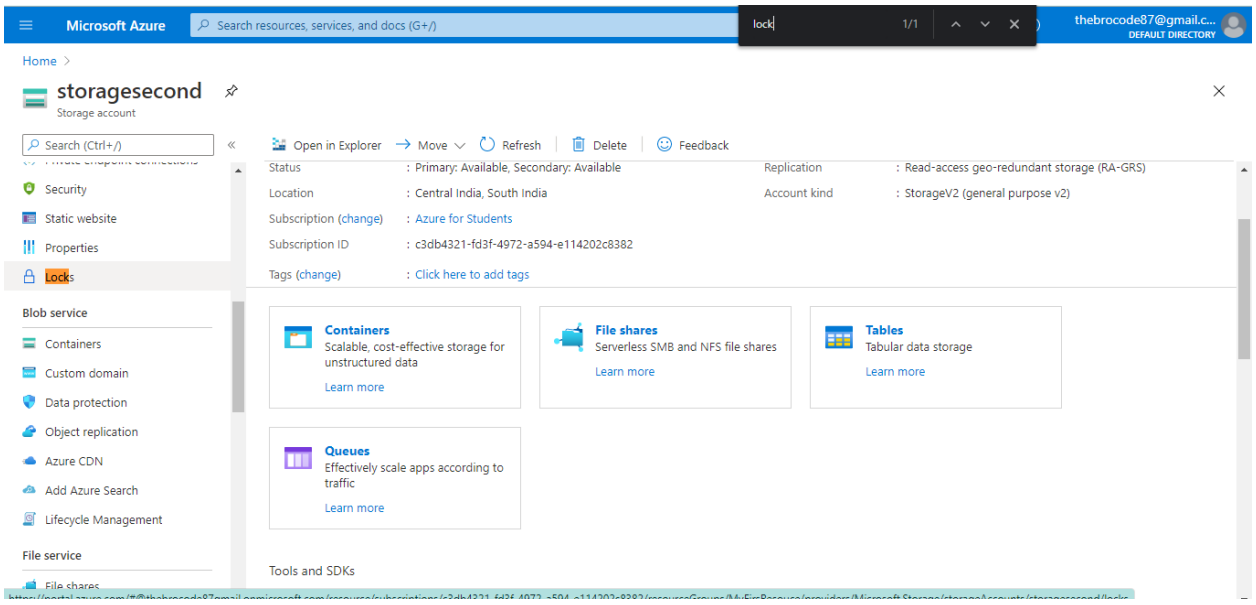


Step-9: Apply a lock on the (VerzeRG01) and test if you are allowed to delete any resource.

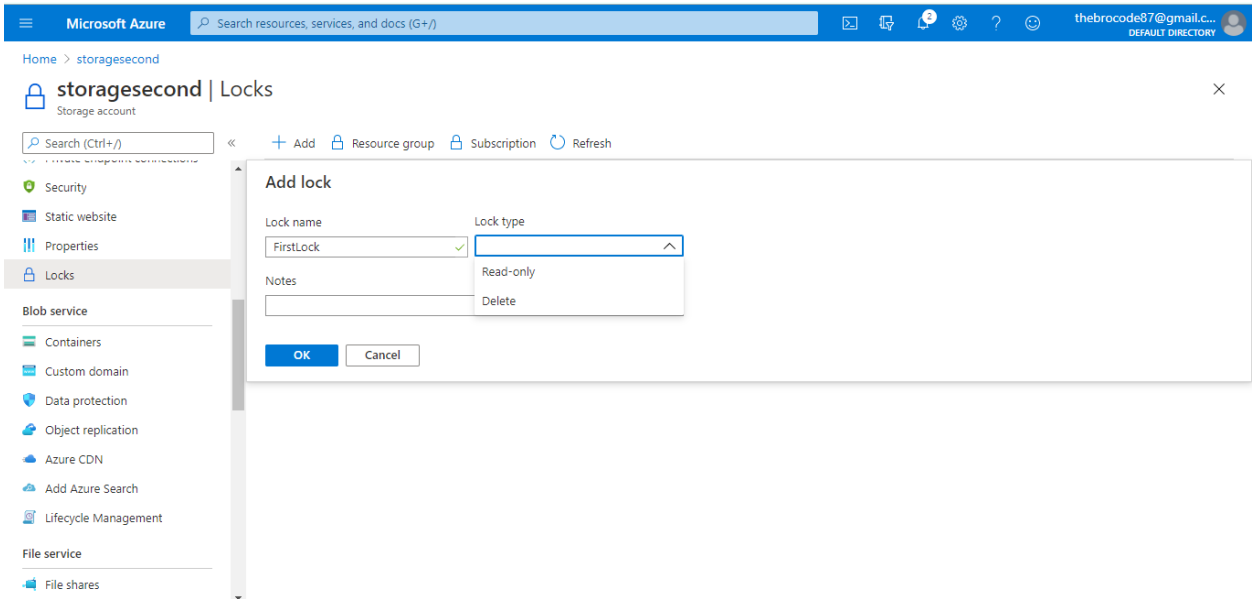
Here, we are creating the lock on storage account resources. Types of Locks:

1. Read-Only => here we can only read the data can't modify or delete
2. Delete => here we can modify but can't delete

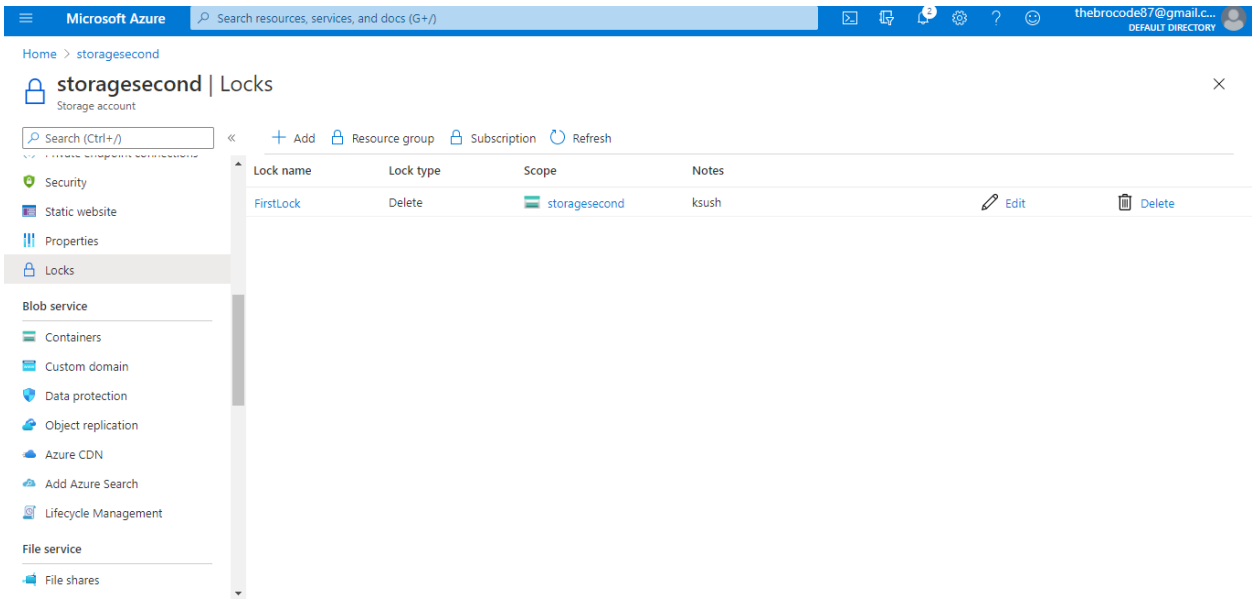
Step-1: First create a Storage Account and go to locks.



Step-2: Click on add and you will see types of lock. Select as per your requirement and give a lock name and press ok.

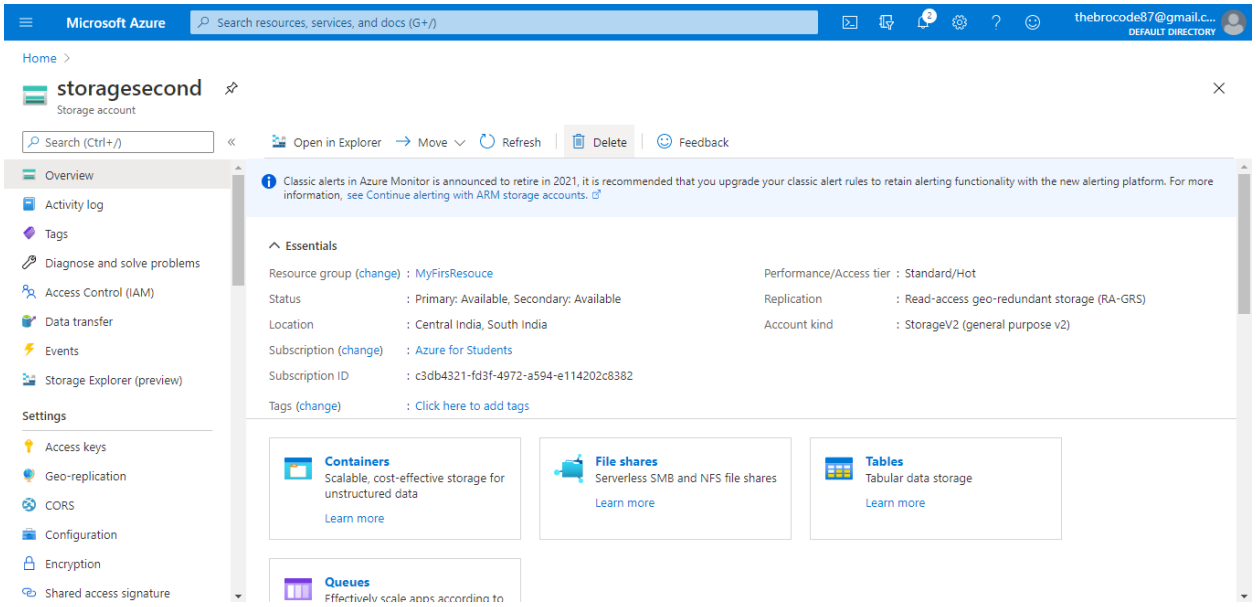


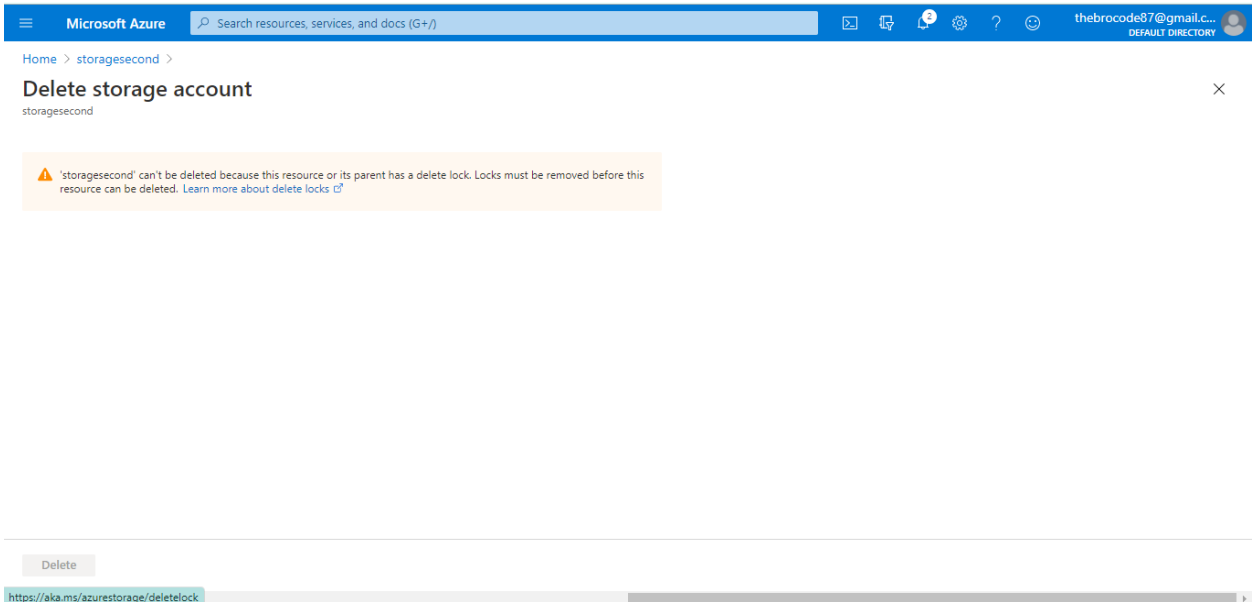
Step-3: You will a lock add in your "LOCKS" section



Step-4:

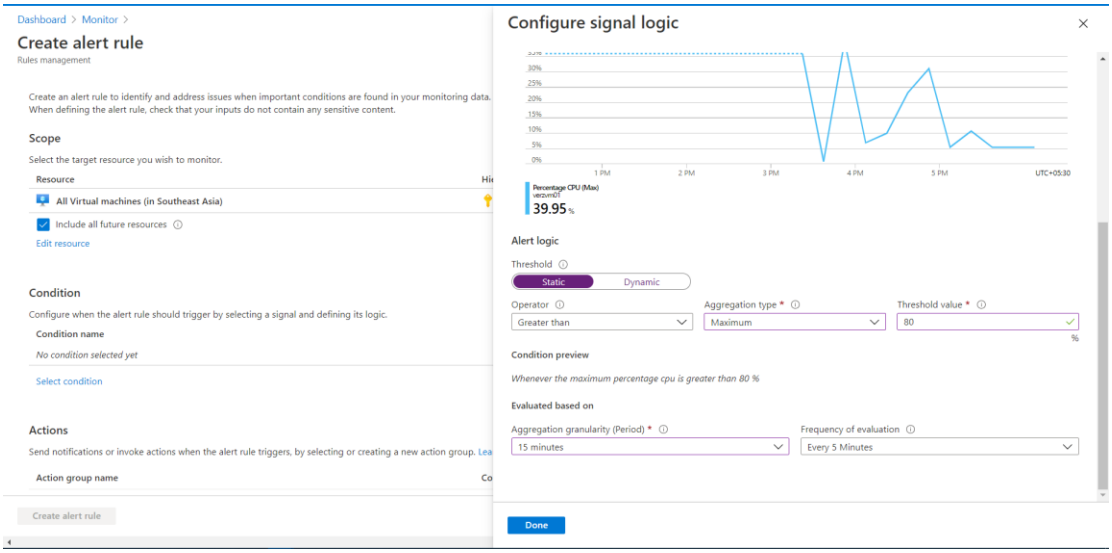
go to overview and try to delete the storage account your will see an alert option for not being able to get delete

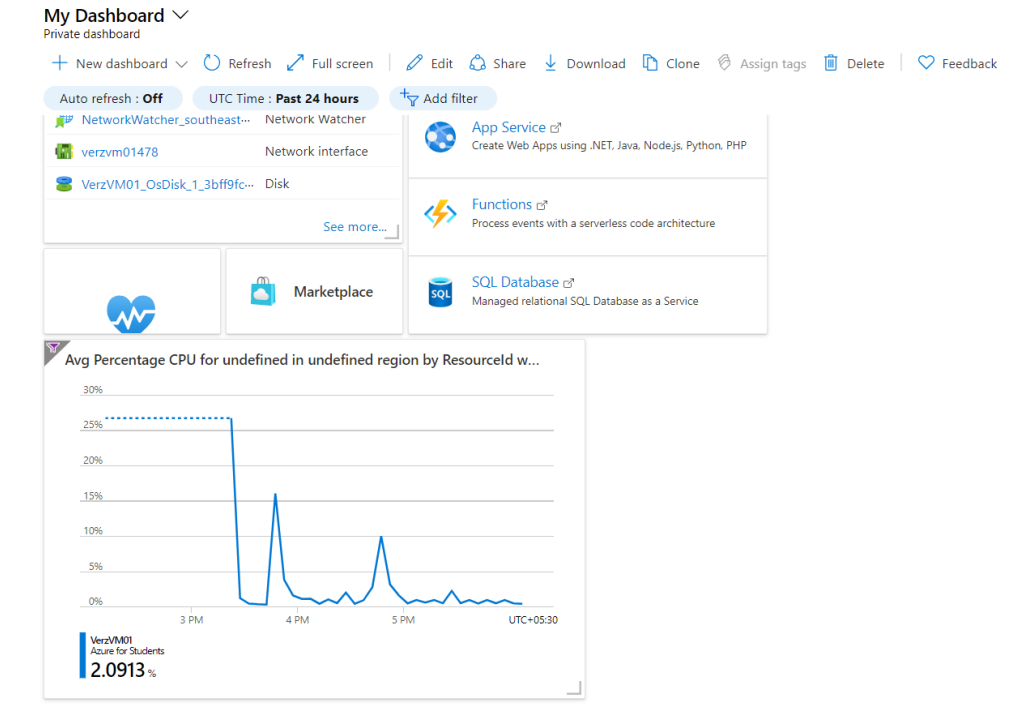




Step-10: Setup CPU Threshold alert for the VM (VerzVM01)

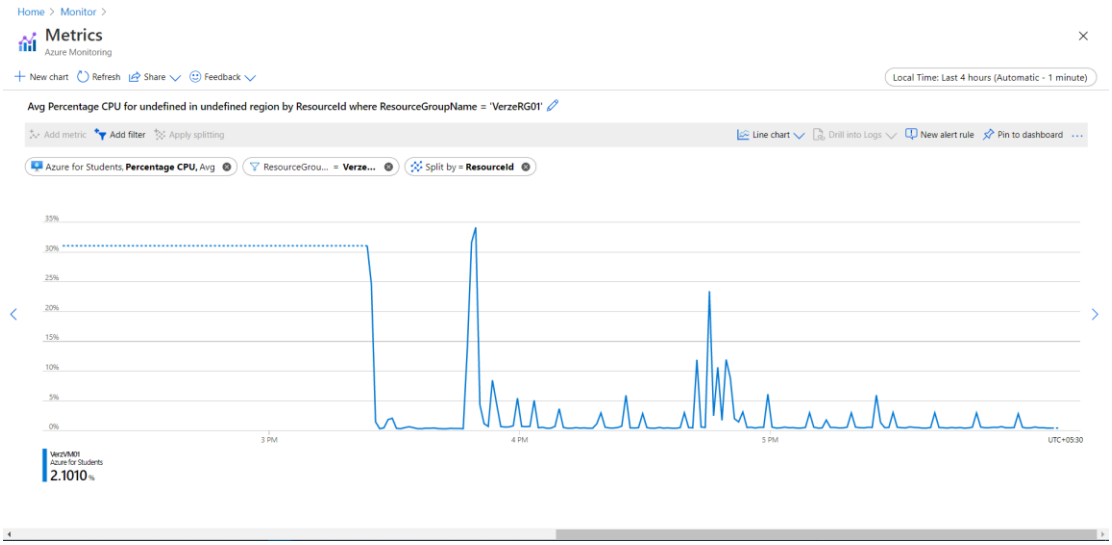
Dynamic Threshold on VM CPU percentage metrics.An alert will be created for the VM with a value that exceeds the threshold.





https://portal.azure.com/#@87b5bac5-a32b-4172-9c1a-4ea123018d62/resource/subscriptions/e532cacd-d1ea-44a8-b4cc-21f06aab61bc/resourcegroups/VerzeRG01/providers/Microsoft.C

Metrics Monitor =>



Condition

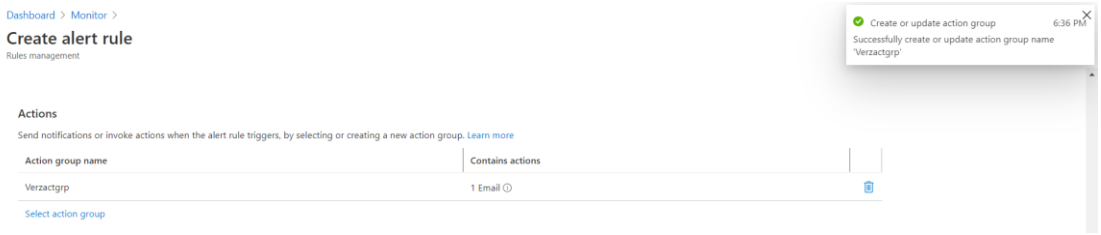
Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name	Time series monitored	Estimated monthly cost (USD)
Whenever the maximum percentage cpu is greater than 80 %	1	$ 0.10
Select condition	1	Total $ 0.10

Metric alerts on multiple resources can include only one condition.

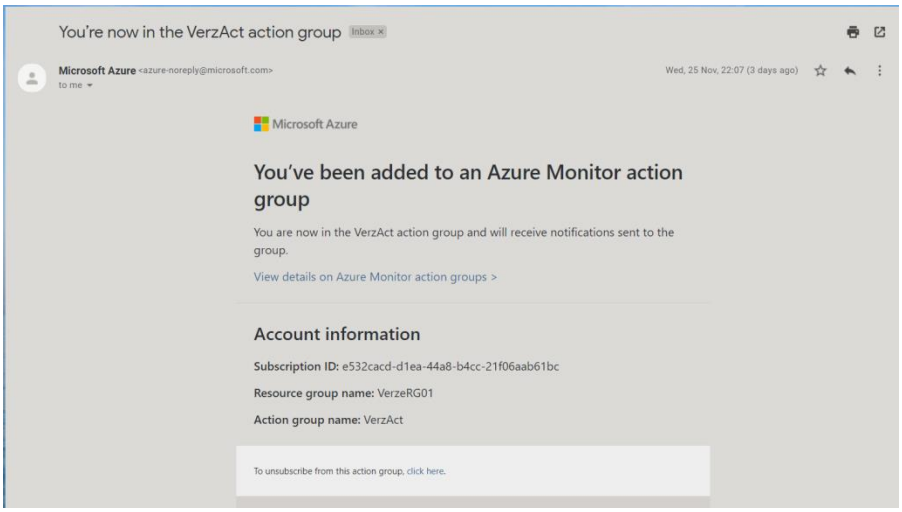
Step-11 : Create Action(Verzactgrp) Group for the above alert with your email id.

Action Group =>



Step-12: Check if you are receiving the alert

The alert with my email id =>

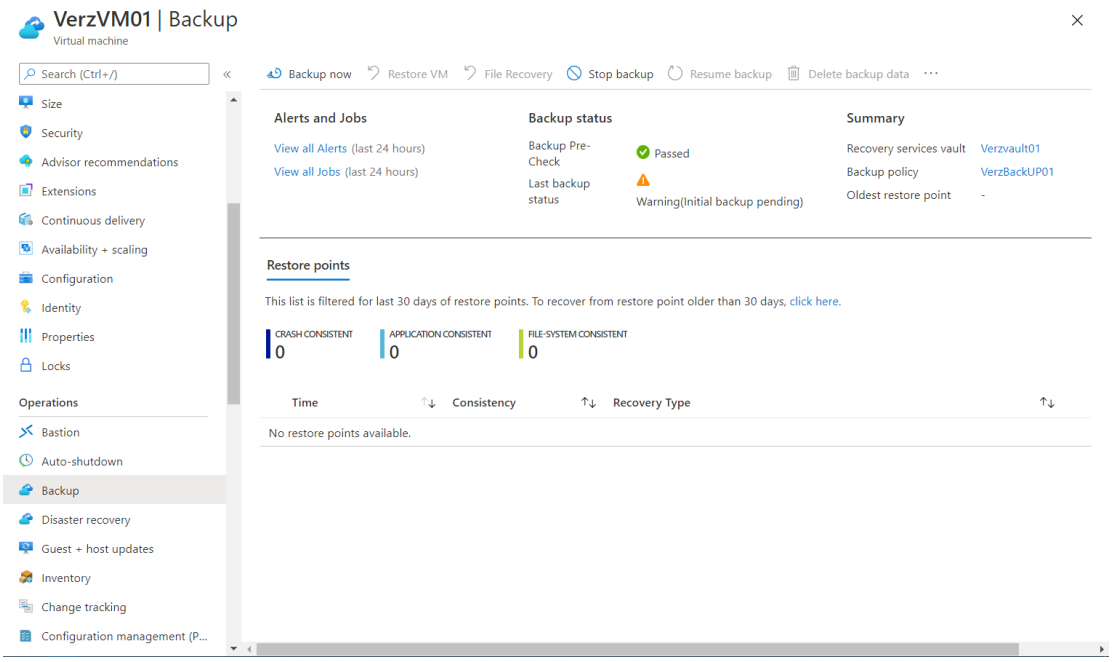


Step-13: Create a Recovery Services vault (Vezvault01) in the Resource Group (VerzeRG01)

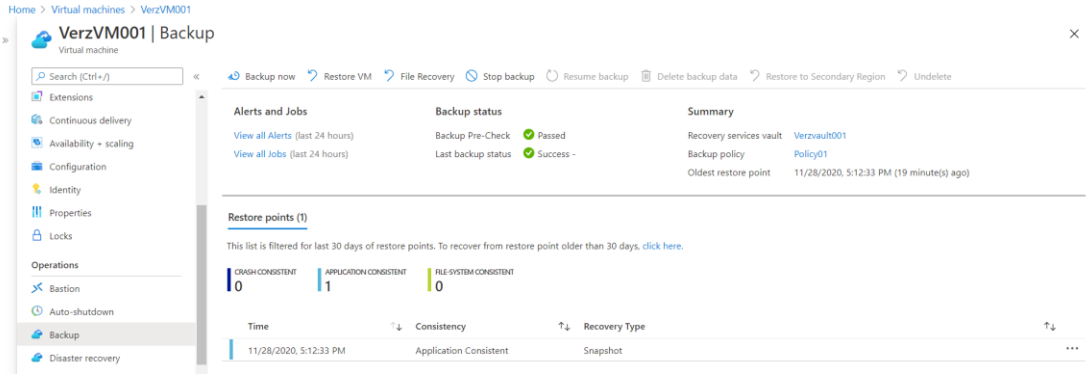
1. Recovery Service Vault is a storage entity in Azure that houses data.The data is typically copies of data,or configuration information for VMs,workloads, or workstations. Recovery service vaults suport system center DPM,windows server,Azure Backup Server, more.

Step-14: Setup Backup for the Virtual Machine (VerzVM01) and ensure backup is completed successfully.

Azure Backup Service provides simple, secure, cost-effective solutions to backup your data and recover it from the Microsoft Azure Cloud.



Successfully completed the backup process. =>



Thank You !!!!
Kushagra Bansal !