

Name - **SAUNDARYA**
Registered Email - 1806516@kiit.ac.in
Topic - Microsoft Azure Cloud Computing (June-July '20)

Under guidance of - **Mr. Rajdeep Das Sir (Verzeo)**

Major Project

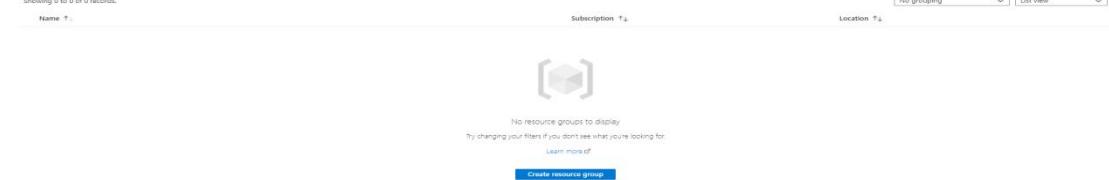
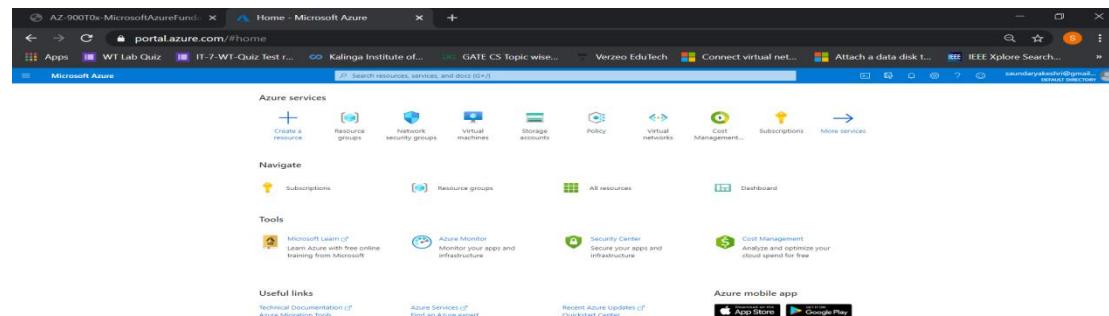
- Creating a Resource Group by name VerzeRG01

- Resource group are like folders which contain all resources (Virtual Networks , Virtual Machines etc)

----- It is a container that holds related resources for an Azure solution. The resources group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource group based on what makes the most sense for your organization.

How to create Resource Group:

1. Sign in to the Azure portal at <https://portal.azure.com>
2. From the All services blade, search for and select Resource Group and then click +Add



3. Fill the required details such as - Resource Group name , Region.
4. Click the **Review + create** button

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more [\(opens in new tab\)](#)

Project details

Subscription * [Azure for Students](#) [View details](#)

Resource group * [VerzeRG01](#) [View details](#)

Resource details

Region * [\(US\) East US](#) [View details](#)

Validation passed

4. After the **Validation is passed** click on **Create**
5. The Resource group named as **VerzeRG01** is created.

Review + create

Validation passed.

Basics Tags Review + create

Subscription: Azure for Students
Resource group: VerzeRG01
Region: East US

Tags

None

Validation passed.

Resource groups

Default Directory

+ Add Manage view Refresh Export to CSV Open query Assign tags Feedback

Showing 1 to 1 of 1 records.

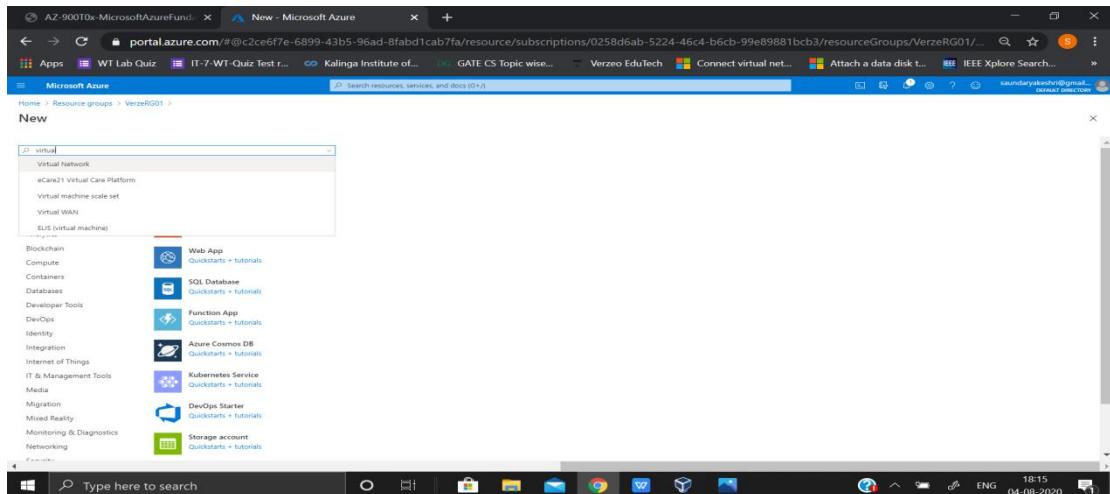
Name	Subscription	Location
VerzeRG01	Azure for Students	East US

No grouping List view

Validation passed.

- Creating Virtual Network (verzvnet01) containing 1 Subnets (Subnet01)

- From the created Resource group(**VerzeRG01**) click on **+Add**, search for and select Virtual networks.



- We name the VNet as - **verzvnet01** with a reserved CIDR block of **192.168.0.0/16** containing 1 subnets

- Subnet01**, using **192.168.1.0/24** as its CIDR block.

3. Click on Next: IP Addresses

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The current step is 'IP Addresses'. A sidebar on the right shows the 'Add subnet' configuration for 'Subnet01' with the address range set to 192.168.1.0/24. The main form shows the basic configuration with the IP address space set to 192.168.0.0/16.

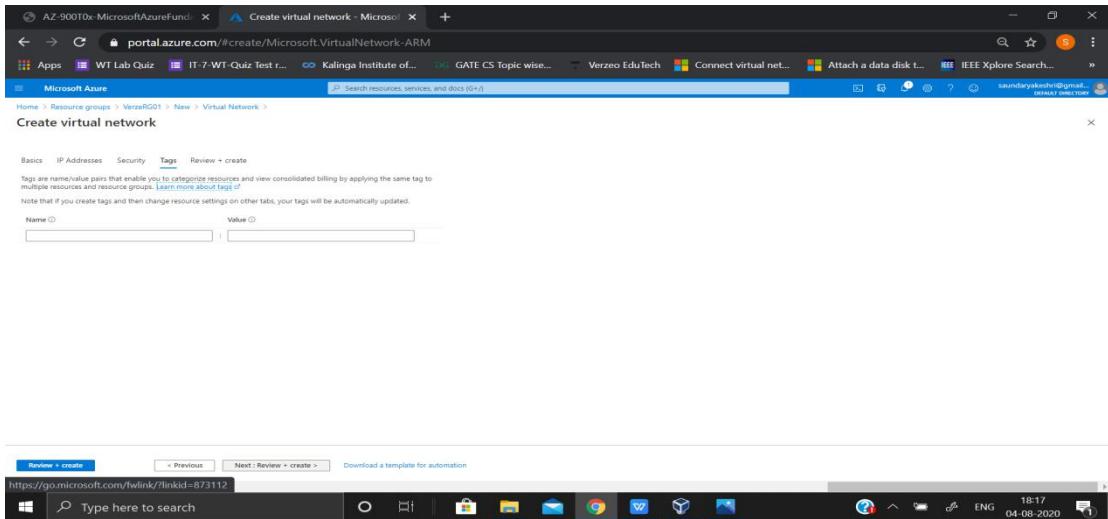
4. After creating the subnet - Subnet01 click on Next:Security

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The current step is 'Security'. The subnet 'Subnet01' is selected with the address range 192.168.1.0/24. The main form shows the security settings, which are currently empty.

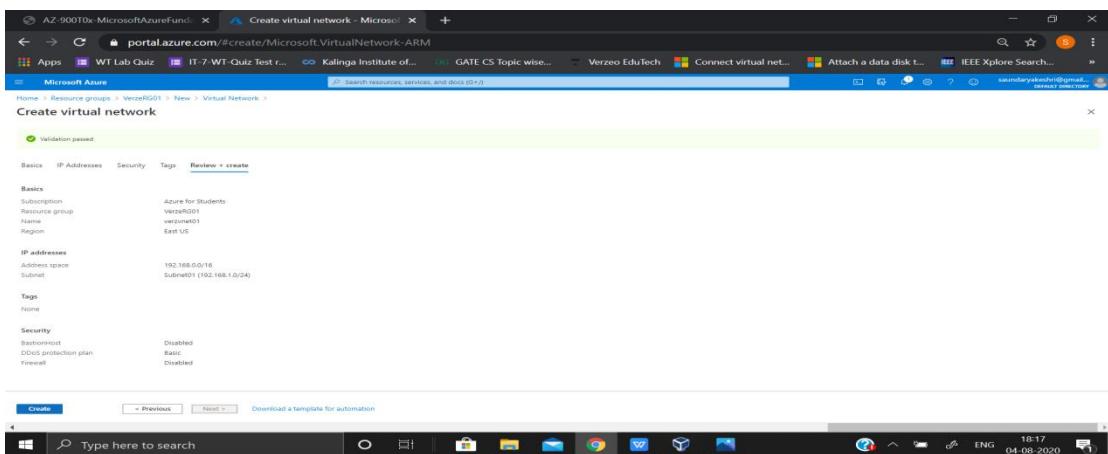
5. Under Security - no changes, click on Next: Tags

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The current step is 'Tags'. The subnet 'Subnet01' is selected with the address range 192.168.1.0/24. The main form shows the tag configuration, which is currently empty.

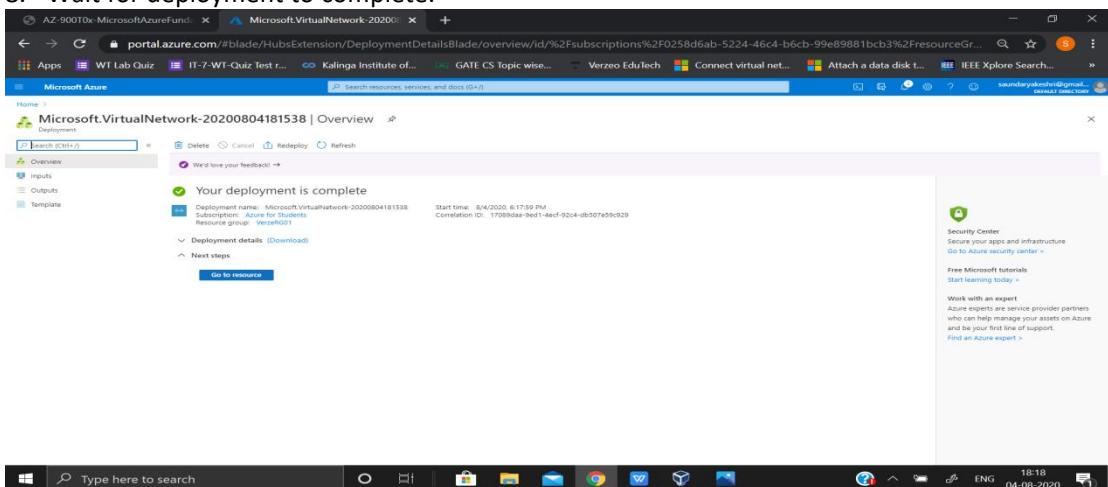
6. Under Tags - no change, click on Next: Review + Create



7. After the *Validation is passed* click on **Create**



8. Wait for deployment to complete.



9. Thus, **verzvnet01** is created having 1 subnet - **Subnet01**

-Creating Virtual Machine (VerzVM01)

1. From the All services blade, search for and select **Resource Group**, and select the resource group that we have created (ex.**VerzeRG01**)
2. To create Virtual Machine **VerzVM01** for **verzvnet01**. Select **verzvnet01**

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar has 'Resource groups' selected. Under 'VerzeRG01', there is a list of resources, including 'verzvnet01'. The main content area displays the details for 'verzvnet01', including its subscription ID, tags, and deployment status.

3. Select **Compute**, and select **Virtual Machine**.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar has 'Compute' selected. Under 'Virtual machine', there are several options listed: SQL Server 2017 Enterprise Windows Server 2016, Reserved VM Instances, Kubernetes Service, Service Fabric Cluster, Web App for Containers, Function App, Batch Service, and Oracle 9i Stretch with backports.

4. Enter the following information under **Basics**, and click on **Next: Disks**

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The 'Create a virtual machine - Microsoft VirtualMachine-ARM' blade is open. In the 'Instance details' section, the following values are entered:

- Virtual machine name: VerzVM01
- Region: US East
- Availability options: No infrastructure redundancy required
- Image: Windows Server 2016 Datacenter
- Azure Spot instance: No
- Size: Standard_D2L_v2

In the 'Administrator account' section, the following values are entered:

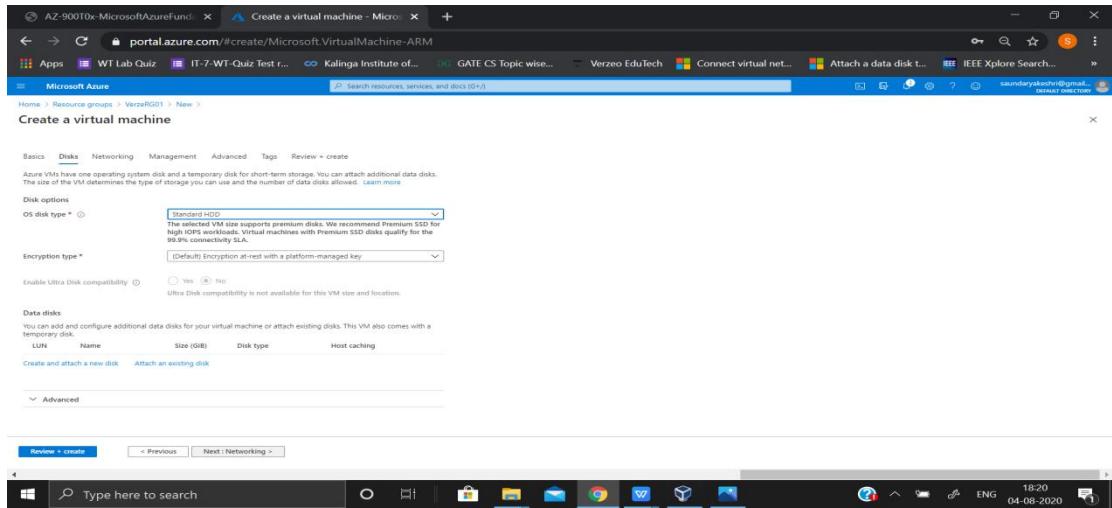
- Username: SaundaryaVM1
- Password: *****
- Confirm password: *****

The 'Inbound port rules' section is expanded, showing:

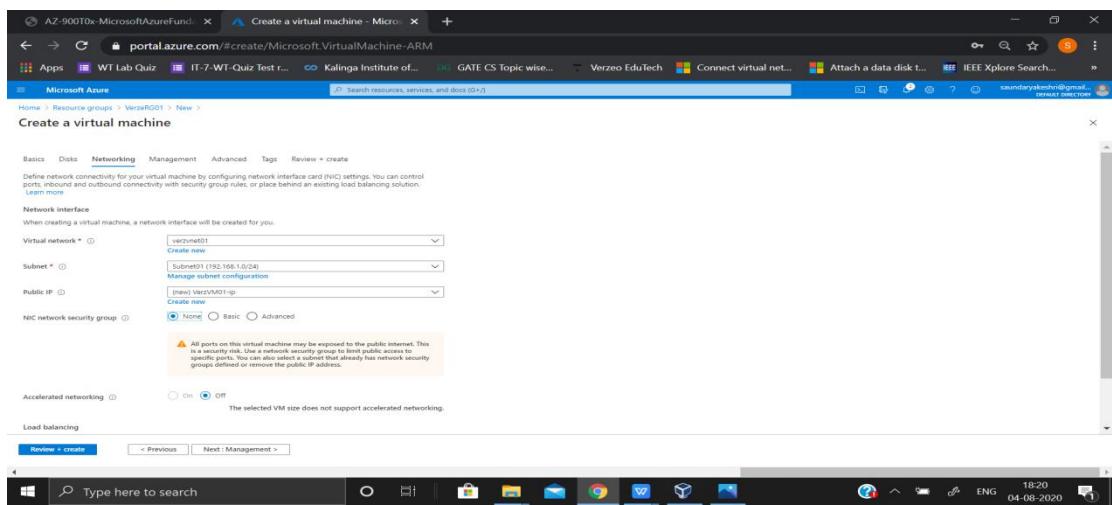
- Public inbound ports: Allow selected ports
- Select inbound ports: RDP (3389)

At the bottom of the blade, there are two buttons: 'Review + create' and 'Next : Disks'.

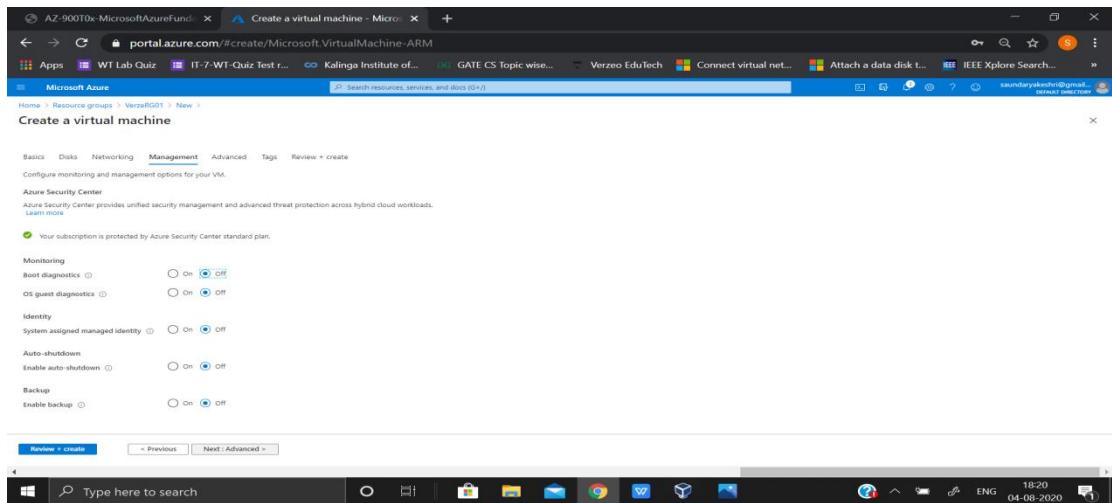
5. Under Disk select OS disk type as **Standard HDD**, keep the remaining as default and then click on **Next: Networking**.



6. Enter the following information under **Networking**, make **NIC network security group as none** and click on **Next: Management**

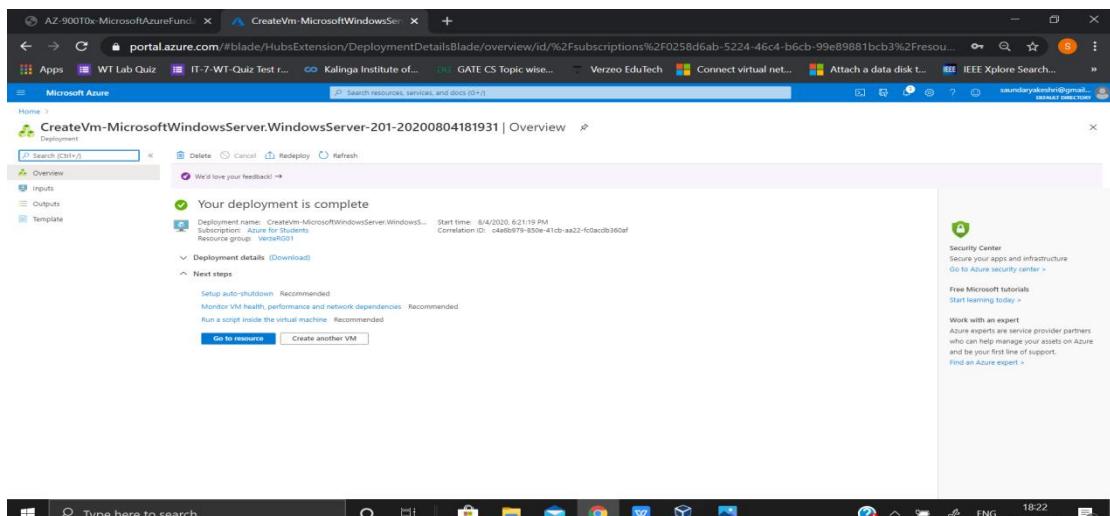
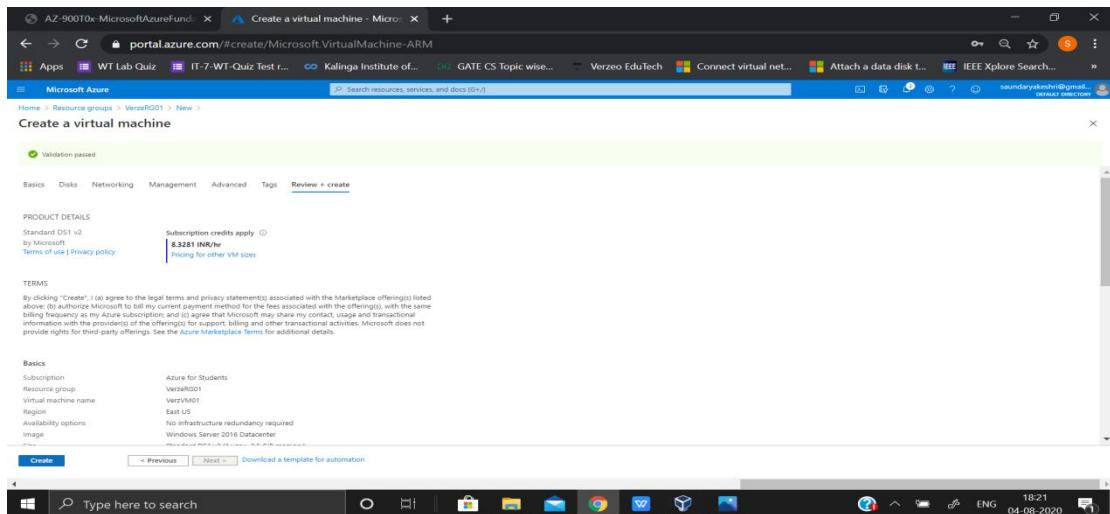


7. In the management section turn everything **Off**, and click on **Review + create**.



8. After the verification is passed.

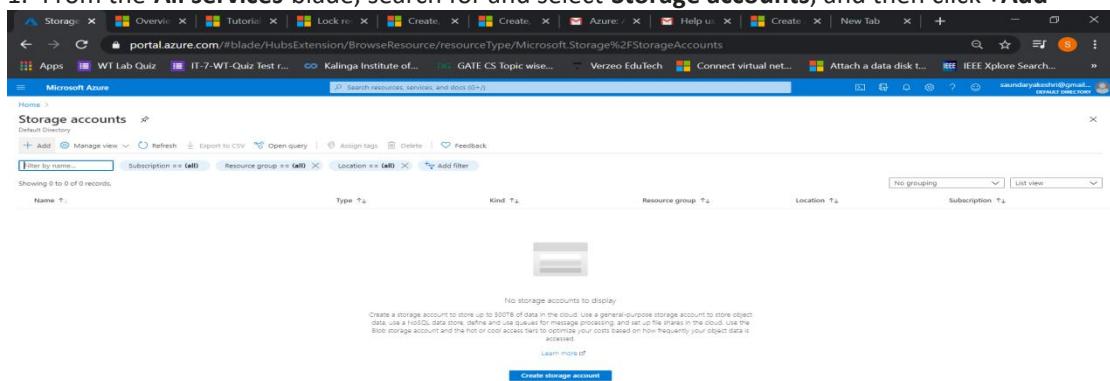
9. Click on **Create**. Wait for the **VM02** to deploy



- Creating a Blob Storage (verzstr1)

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

1. From the All services blade, search for and select **Storage accounts**, and then click **+Add**



2. Enter the following information and click on **Next: Networking**

Subscription * Azure for Students

Resource group * Verzeo001
Create new

Storage account name *

Location *

Performance Standard Premium

Account kind

Replication

Access tier (default) Hot Cool

Review + create < Previous Next : Networking >

3. Select the appropriate option under **Networking** and click on **Next:Data protection**

Networking

Network connectivity
You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method Allow endpoint (all networks)
 Public endpoint (selected networks)
 Private endpoint
 All networks will be able to access this storage account.
Learn more about connectivity methods [?](#)

Network routing
Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * Microsoft network routing (default)
 Internet routing

Review + create < Previous Next : Data protection >

4. Select the appropriate option under **Data protection** and click on **Next: Advanced**

Data protection

Blob soft delete Enabled
 Disabled

File share soft delete Enabled
 Disabled

Versioning Enabled
The current combination of subscription, storage account kind, performance, replication and location does not support versioning.

Review + create < Previous Next : Advanced >

5. Select the appropriate option under **Advanced** and click on **Review + create**

6. After the **Validation is passed** click on **Create** .

7. Wait for deployment to complete.

8. Go to the created Storage account- **verzstr1** and scroll to the **Blob service** section, and then click **Containers**.

9. Click **+ Container** and fill the information. When done click on **create**

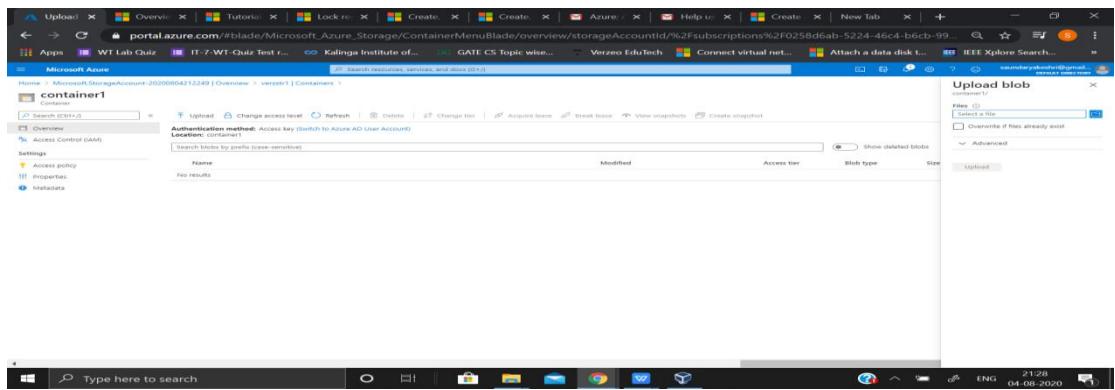
The screenshot shows the Microsoft Azure Storage Account Overview for the account 'verzstr1'. On the left, the 'Containers' blade is open under the 'Blob service' category. It displays a table with one row: 'You don't have any containers yet. Click + Container to get started.' At the top right of the blade, there are buttons for '+ Container', 'Change access level', 'Refresh', and 'Delete'. The main content area shows a search bar 'Search containers by prefix:' and a table with columns: Name, Last modified, Public access level, and Lease state.

10. The container named **container1** is created.

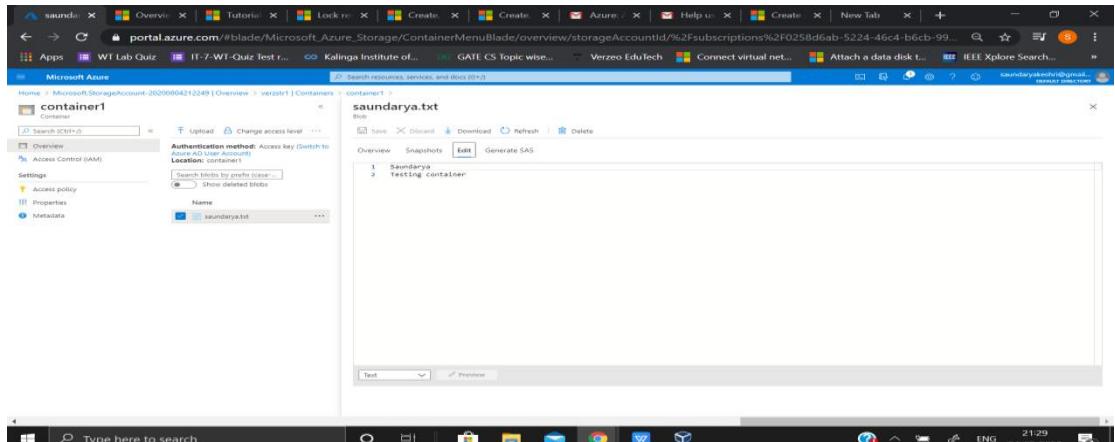
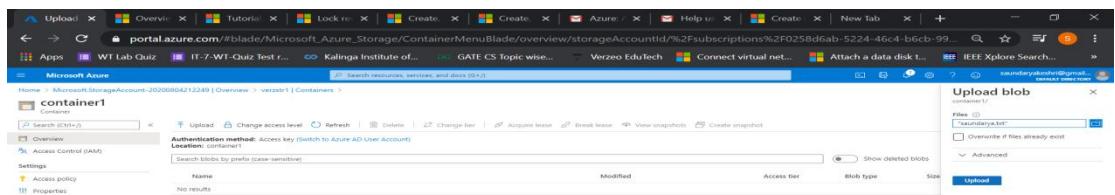
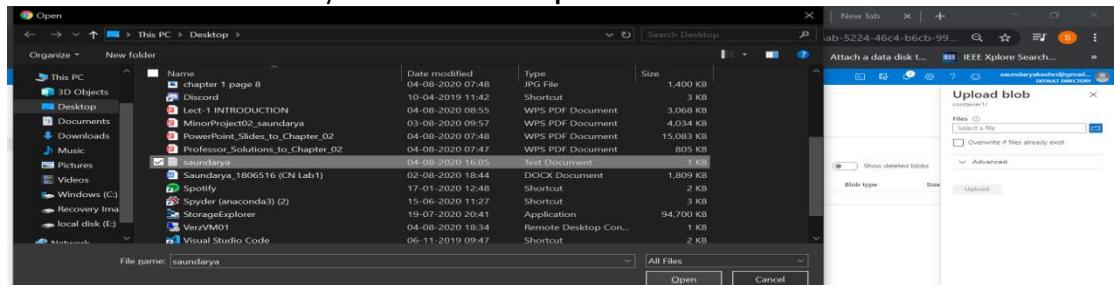
The screenshot shows the Microsoft Azure Storage Account Overview for the account 'verzstr1'. The 'Containers' blade is open. A new container named 'container1' is being created. The 'Name' field contains 'container1'. Under 'Public access level', the dropdown menu is set to 'Private (no anonymous access)'. At the bottom right of the blade, there are 'Create' and 'Discard' buttons. The status bar at the bottom right indicates '21:27 04-08-2020'.

11. Click on the container created i.e **container1** and click on **Upload**

The screenshot shows the Microsoft Azure Storage Account Overview for the account 'verzstr1'. The 'Containers' blade is open, and the 'container1' blade is currently active. The table in the 'container1' blade shows one item: 'container1' with a last modified date of '5/6/2020, 9:27:09 AM', a public access level of 'Private', and a lease state of 'Available'. The status bar at the bottom right indicates '21:27 04-08-2020'.

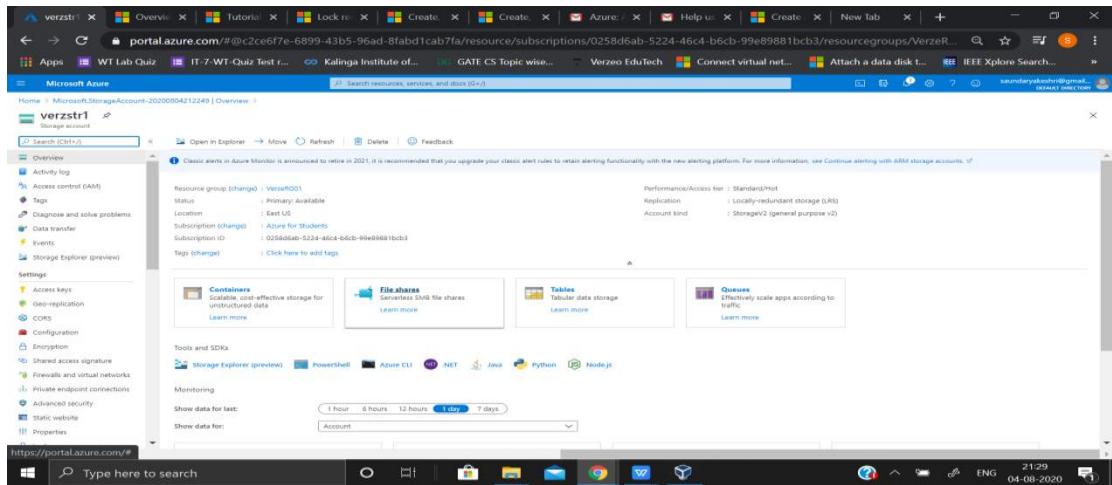


12. Browse to a file in our system and click on upload



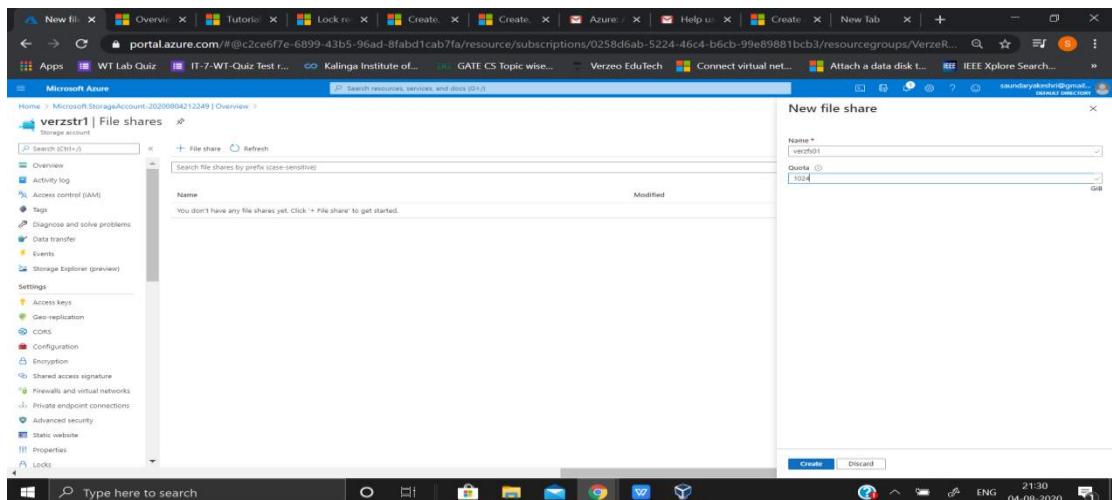
Create a File Share (Verzfs01) and mount on the (VerzVM01)

1. Go to the storage account **verzstr1** and select **File share**.

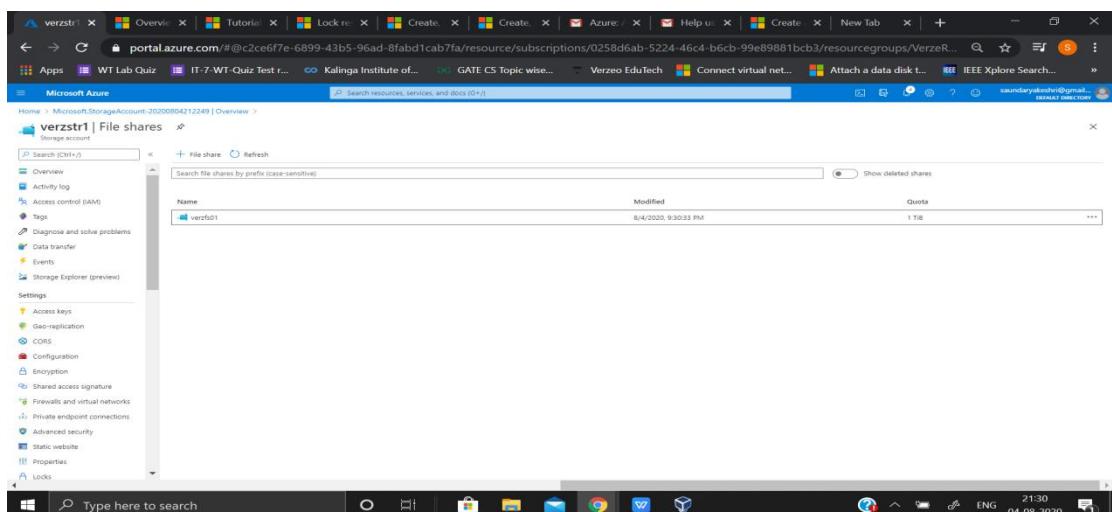


The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation links for the storage account 'verzstr1'. The main content area displays the 'Overview' page for the storage account. On the right side, there is a section titled 'File shares' which lists 'verzfs01' as a service-based SMB file share.

2. Click on **+File share** a section will pop at the right corner fill the details and then click on **create**.



The screenshot shows the 'New file share' dialog box overlaid on the 'Overview' page of the storage account. The dialog box has fields for 'Name' (set to 'verzfs01') and 'Quota' (set to '1024'). The 'Create' button is visible at the bottom of the dialog.



The screenshot shows the 'File shares' table after the new file share 'verzfs01' has been created. The table lists one item: 'verzfs01' with a 'Modified' date of '8/4/2020, 9:30:23 PM' and a 'Quota' of '1 TiB'.

3. File share **verzfs01** is created.

4. Go to the created file share **verzfs01** and click on **connect**

The screenshot shows the Microsoft Azure Storage Account overview page for 'verzfs01'. On the left, there's a navigation pane with 'Overview', 'Access Control (IAM)', 'Properties', 'Operations', 'Snapshots', and 'Backup'. The main area displays the file share details, including a search bar for files and a 'Connect' button. A note at the top right says 'Secure transfer required' is enabled on the storage account. Below it, there are tabs for 'Windows', 'Linux', and 'macOS', each with a dropdown for 'Drive letter'. The Windows section contains a PowerShell command to connect:

```
Connect-NetConnection -ComputerName verzstr1 -Port 445  
if ($connectTestResult.TopTestSucceeded) {  
    # Save the password so the drive will persist on reboot  
    cmd.exe /C "cmdkey /add:verzstr1.file.core.windows.net /user:'Azure\verzstr1'"  
    /pass:'AVPdYzP19dqZkexz1b0C9MgZEVApA/vzNQFQfvPQdgDwqGJ5QCPVzIgZ  
    mHdgQfHh3Bjy-k4sAkg"  
}  
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 ExpressRoute, Azure FEB (Express Encrypted Bandwidth), or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port.
```

Learn how to circumvent the port 445 problem (VPN)

5. Select the drive letter to mount the share to

6. Copy the provided script in the powershell of our Virtual Machine **VerzVM01**

The screenshot shows the Microsoft Azure Storage Account overview page for 'verzfs01'. The interface is identical to the previous one, with the 'Windows' tab selected for connecting. The PowerShell command is identical to the one shown in the previous screenshot:

```
Connect-NetConnection -ComputerName verzstr1 -Port 445  
if ($connectTestResult.TopTestSucceeded) {  
    # Save the password so the drive will persist on reboot  
    cmd.exe /C "cmdkey /add:verzstr1.file.core.windows.net /user:'Azure\verzstr1'"  
    /pass:'AVPdYzP19dqZkexz1b0C9MgZEVApA/vzNQFQfvPQdgDwqGJ5QCPVzIgZ  
    mHdgQfHh3Bjy-k4sAkg"  
}  
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 ExpressRoute, Azure FEB (Express Encrypted Bandwidth), or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port.
```

Learn how to circumvent the port 445 problem (VPN)

The screenshot shows an Administrator Windows PowerShell window. The command entered is:

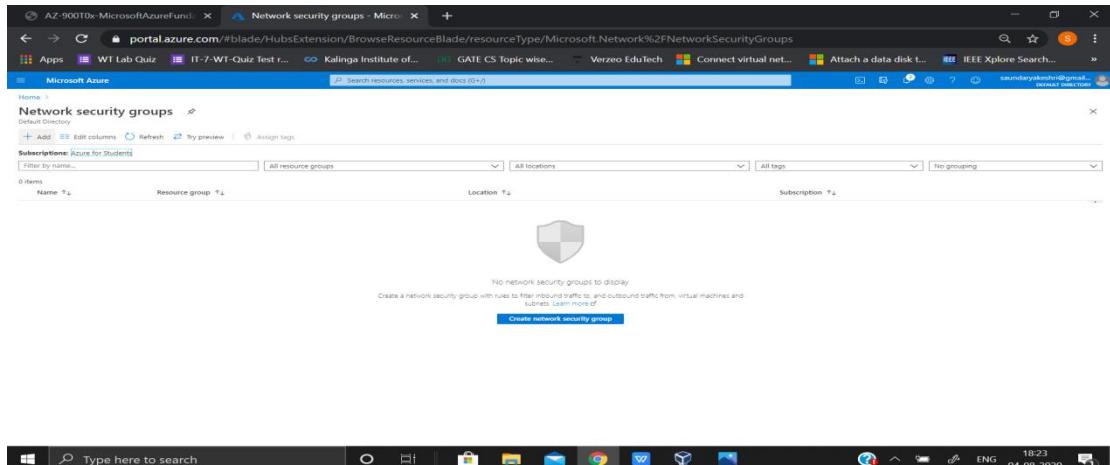
```
PS C:\Users\SaundaryaVM1> $connectTestResult = Test-NetConnection -ComputerName verzstr1.file.core.windows.net -Port 445  
PS C:\Users\SaundaryaVM1> if ($connectTestResult.TopTestSucceeded) {  
PS C:\Users\SaundaryaVM1>     cmd.exe /C "cmdkey /add:verzstr1.file.core.windows.net /user:'Azure\verzstr1'"  
PS C:\Users\SaundaryaVM1>     /pass:'AVPdYzP19dqZkexz1b0C9MgZEVApA/vzNQFQfvPQdgDwqGJ5QCPVzIgZ  
PS C:\Users\SaundaryaVM1>     New-PSSDrive -Name Z -PSProvider FileSystem -Root "\\\verzstr1.file.core.windows.net\verzfs01" -Persist  
PS C:\Users\SaundaryaVM1>     Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization's ISP is not blocking port 445, or use Azure F2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."  
PS C:\Users\SaundaryaVM1>
```

PS C:\Users\SaundaryaVM1> CMDKEY: Credential added successfully.
PS C:\Users\SaundaryaVM1> Name Used (GB) Free (GB) Provider Root
PS C:\Users\SaundaryaVM1> Z 0.00 1024.00 Filesystem \\\verzstr1.file.core.windows.net...

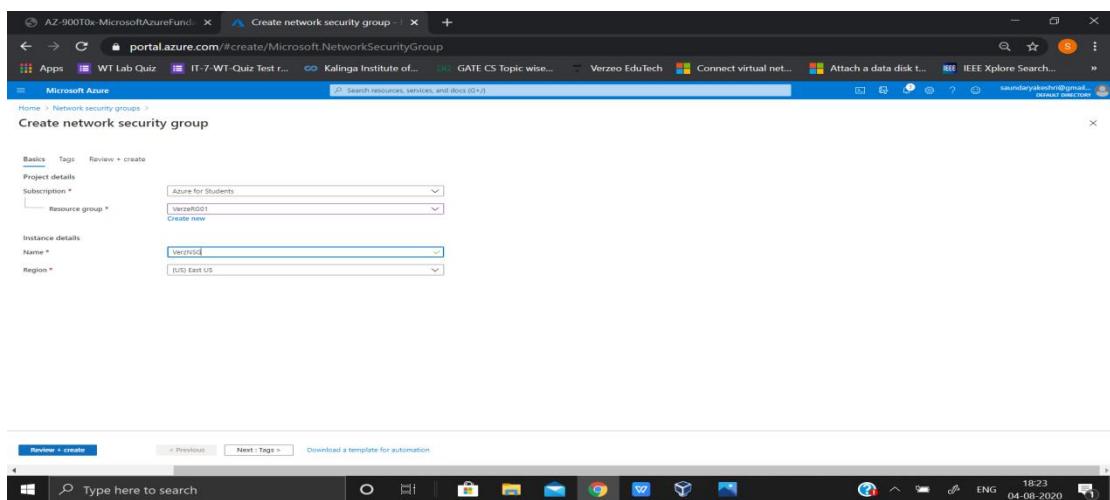
7. File **verzfs01** is mounted on virtual machine **VerzVM01** successfully.

-Creating a Network Security Group

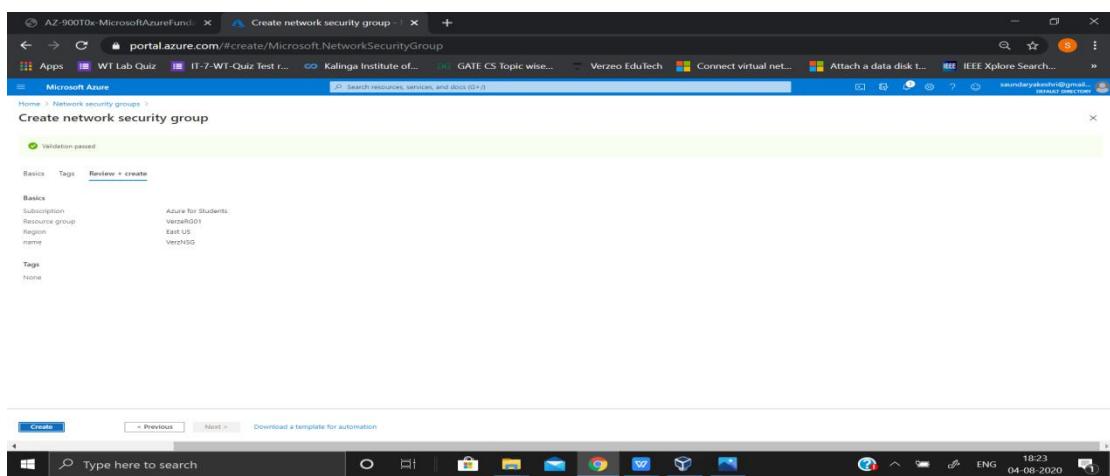
- From the all service blade, search for and select Network Security Group and click +Add.



- Fill the required information and click on Review+Create



- After the Validation is passed click on Create .



4. Wait for deployment to complete.

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#blade/HubsExtension/DeploymentDetailsBlade/overview/id/%2Fsubscriptions%2F0258d6ab-5224-46c4-b6cb-99e89881bcb3%2FresourceGroups%2FVerzRG01%2FresourceGroups%2FVerzNSG01%2Fdeployments%2F02ce6f7e-6899-43b5-96ad-8fabd1cab7fa/resource/subscriptions/0258d6ab-5224-46c4-b6cb-99e89881bcb3>. The page displays a deployment summary for 'Microsoft.NetworkSecurityGroup-20200804182328'. It shows the deployment is complete, started at 8/4/2020 6:24:02 PM, and was successful. The deployment ID is 728d78f-01b6-4ca0-b099-9a8bd43128ea. There are links to 'Go to resource' and 'Go to dashboard'.

5. Thus the Network Security Group - **VerzNSG** is created

But when we try to connect to our virtual machine it shows:

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#blade/Microsoft_Azure_Virtual_Machines/VMListBlade/VMList/resourceId%3D02ce6f7e-6899-43b5-96ad-8fabd1cab7fa/resource/subscriptions/0258d6ab-5224-46c4-b6cb-99e89881bcb3/resourceGroups/VerzRG01%2FresourceGroups/VerzNSG01%2FvirtualMachines/VerzVM01. The page shows the 'Virtual machines' blade with 'VerzVM01' selected. A 'Connect' button is highlighted. A 'Remote Desktop Connection' dialog box is open, displaying an error message: 'Remote Desktop can't connect to the remote computer for one of these reasons: 1) Remote access to the server is not enabled, 2) The remote computer is turned off, 3) The remote computer is not available on the network.' It also says to make sure the remote computer is turned on and connected to the network, and that remote access is enabled. There are 'OK' and 'Help' buttons at the bottom.

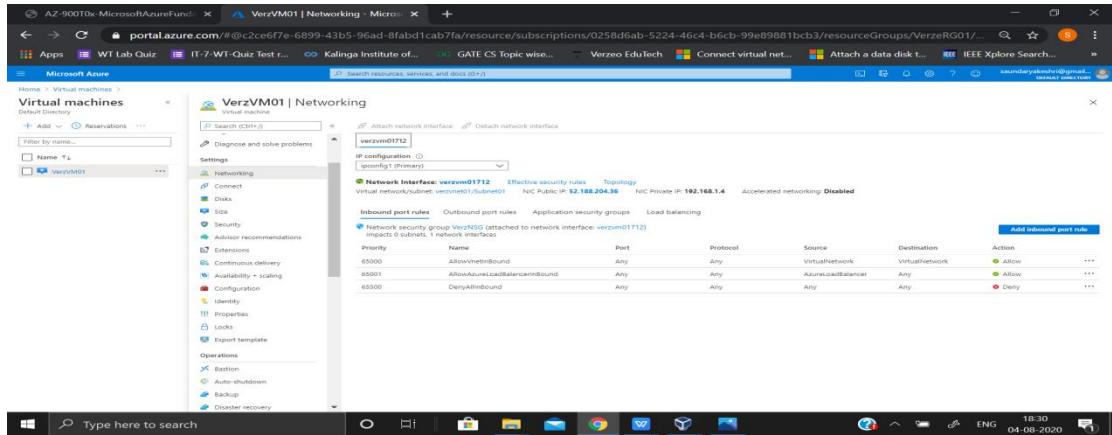
6. Go to **VerzNSG** and click on **+Associate**

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#blade/Microsoft_Azure_NetworkSecurityGroup/NetworkInterfacesBlade/Overview/resourceId%3D02ce6f7e-6899-43b5-96ad-8fabd1cab7fa/resource/subscriptions/0258d6ab-5224-46c4-b6cb-99e89881bcb3/resourceGroups/VerzRG01%2FresourceGroups/VerzNSG01%2FnetworkInterfaces/VerzNI01. The page shows the 'VerzNSG | Network interfaces' blade. The 'Associate' button is highlighted. A search bar at the top right shows 'Search network interfaces'.

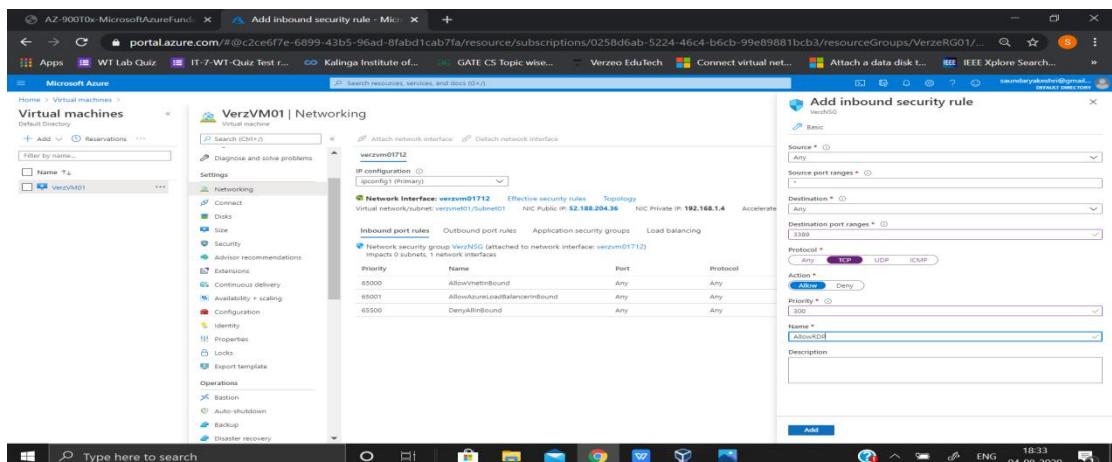
7. And select the virtual machine **VerzVM01** to associate **VerzNSG** with **VerzVM01**.

-Configure an inbound security port rule to allow RDP

1. Go to the Virtual Machine **VerzVM01** under **Setting** click on **Networking**
2. Select **Add inbound port rule**

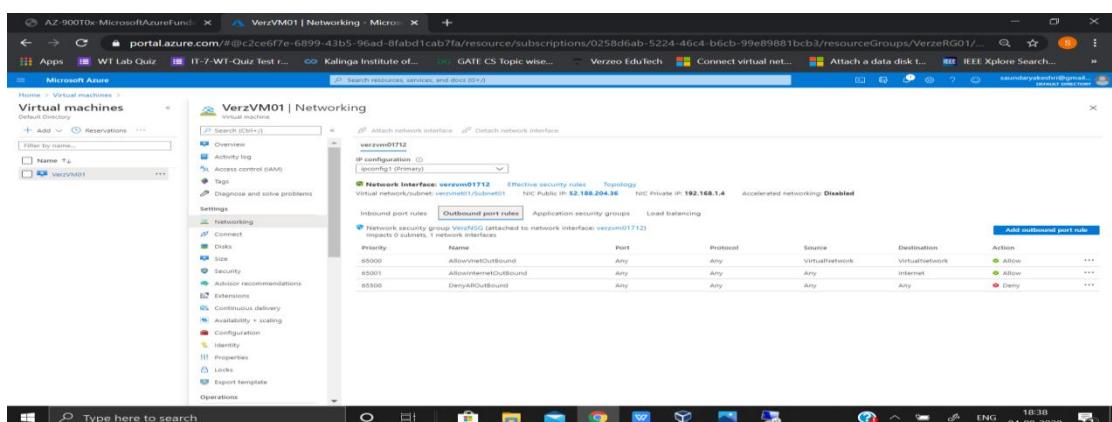


3. Fill the details and click on **+Add**



-Configure an outbound security port rule to deny Internet access

4. Go to the Virtual Machine **VerzVM01** under **Setting** click on **Networking**
5. Select **Add outbound port rule**



6. Fill the details and click on +Add

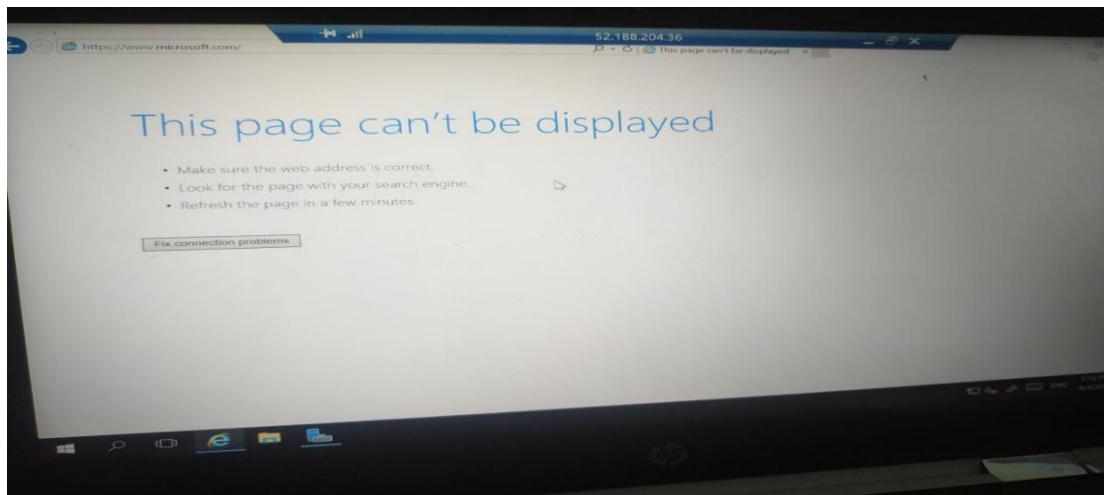
The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual machines' blade is open, displaying a list of virtual machines including 'VerzVM01'. In the center, the 'Networking' settings for 'VerzVM01' are shown, specifically the 'Outbound port rules' section. A new rule is being added, as indicated by the 'Add outbound security rule' dialog box on the right. The dialog box contains the following configuration:

- Source:** Any
- Source port ranges:** Topology
- Destination:** Internet
- Destination port ranges:** All
- Protocol:** Any (TCP, UDP, ICMP)
- Action:** Deny
- Priority:** 300
- Name:** Denyinternet
- Description:** (empty)

Result - we can connect to Virtual machine **VerzVM01** using RDP and the Internet connection is denied in **VerzVM01**

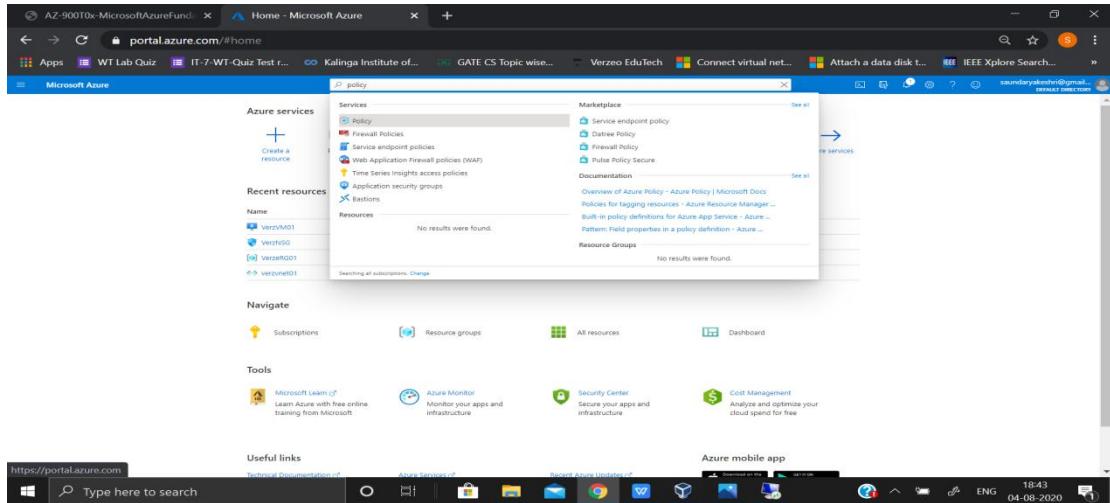
The screenshot shows the 'Connect' blade for the 'VerzVM01' virtual machine. A 'Windows Security' dialog box is overlaid on the page, prompting for credentials to connect to the IP address 52.188.204.36. The dialog box contains the following fields:

- Username: SaundaryaVM1
- Password: (redacted)
- Remember me: (unchecked)

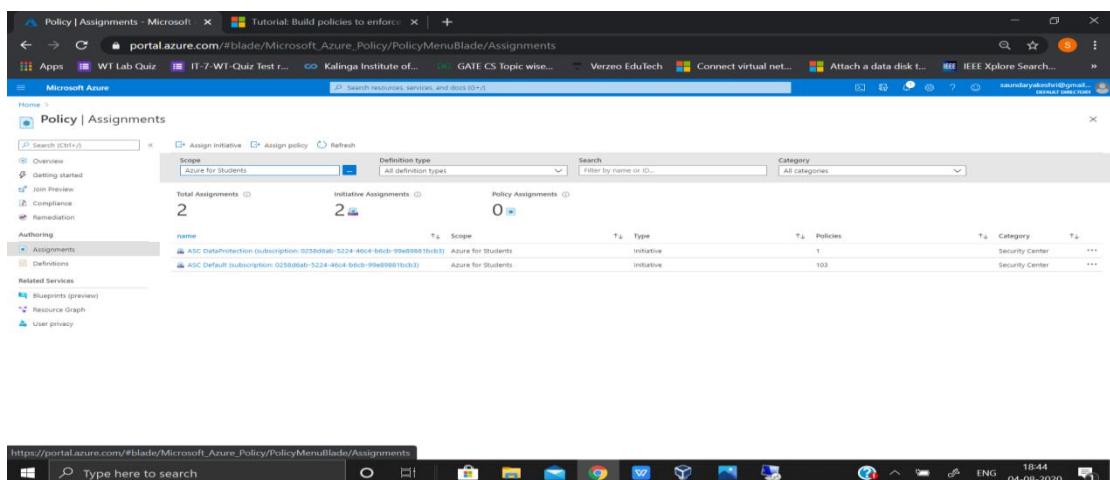


- Create an Azure Policy to only allow certain locations

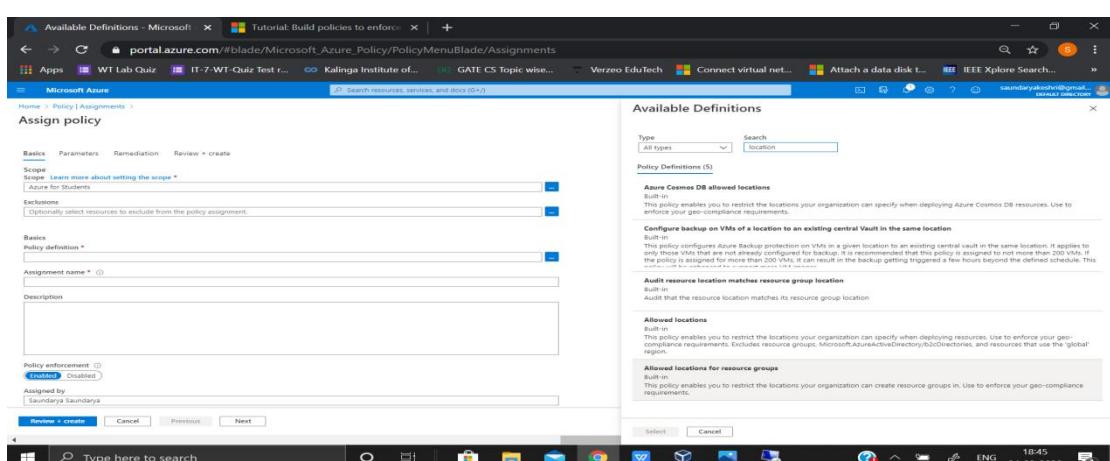
1. From the all service blade, search for and select **Policy** and click **+Add**.

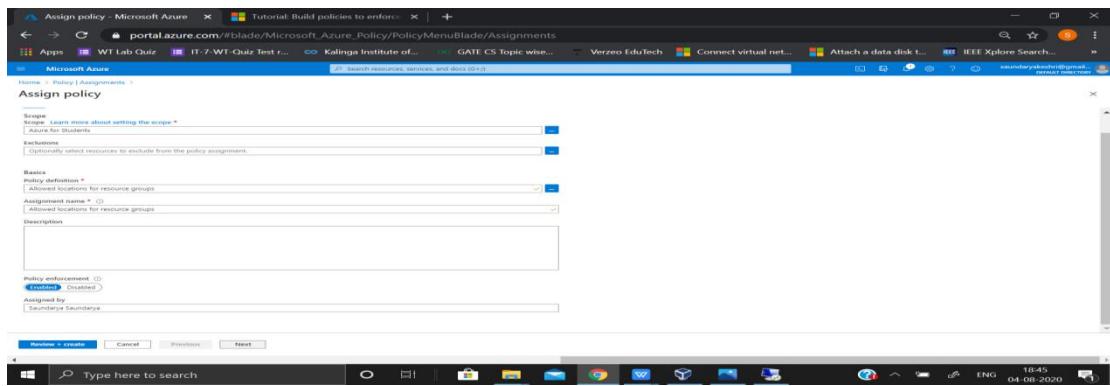


2. Under **Authoring** select **Assignments** and then select **Assign policy**

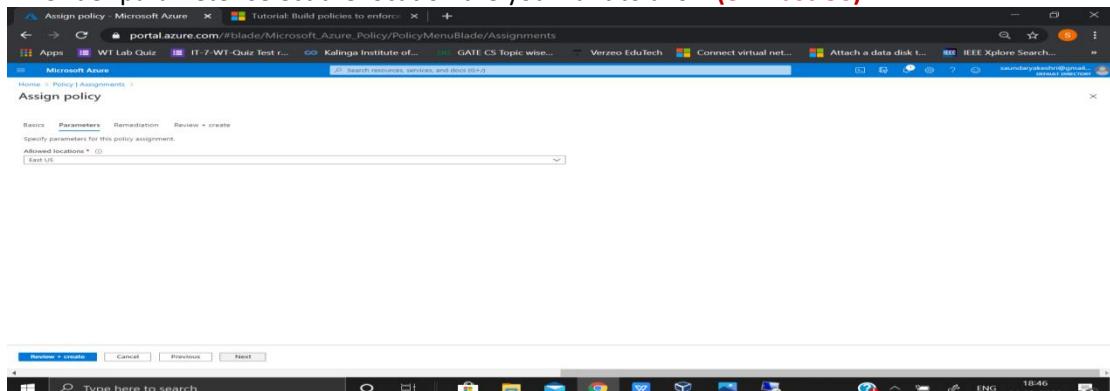


3. Fill the required information and under **Available Definitions** choose **policy definition** as - **Allowed location for Resource group**

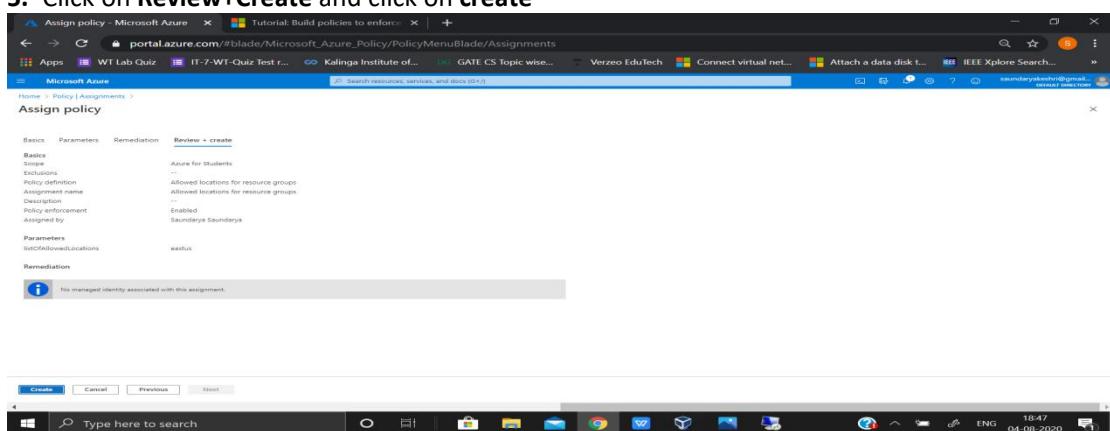




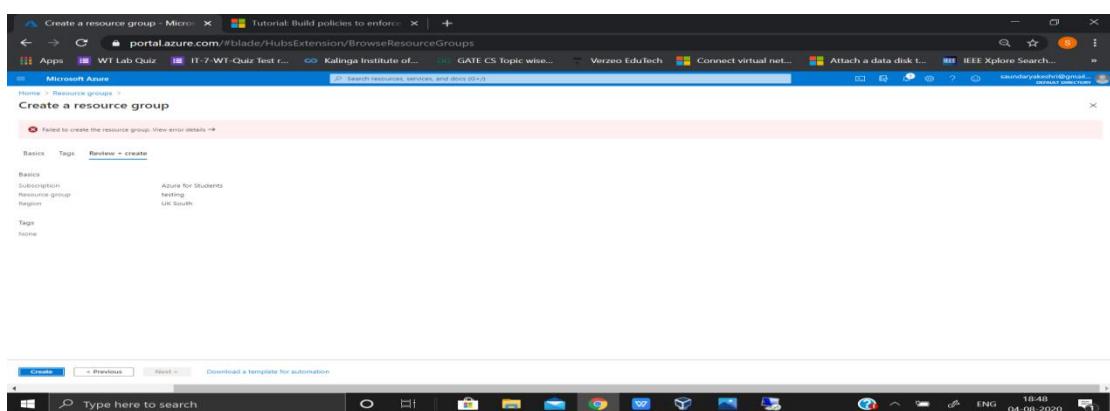
4. Under parameter select the location the you want to allow (ex- East US)



5. Click on Review+Create and click on create



Result - cannot create resource group anywhere except East US



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

1. Go to the Resource group VerzeRG01 and under setting click on Locks.

Name	Type	Location
VerzeRG01	Resource group	East US
Verzev0101	Virtual machine	East US
verzev0101-ip	Public IP address	East US
verzev010112	Network interface	East US
verzev0101_disk_1_3266029409845186e5674bc7abce99	Disk	East US
verzev0101	Virtual network	East US

2. Click on +Add

Lock name	Lock type	Scope	Notes
LockResource	Delete	verzeRG01	No Deleting

The lock **LockResource** is created which don't allow us to delete the resource belonging to the Resource Group **VerzeRG01**.

Result - We are not able to delete any Resource in Resource Group **VerzeRG01**

Deleted virtual network
Do you want to delete the virtual network 'verzvnet01'?

Device	Type	IP Address	Subnet
verzvnet01T12	Network interface	192.168.1.4	Subnet01

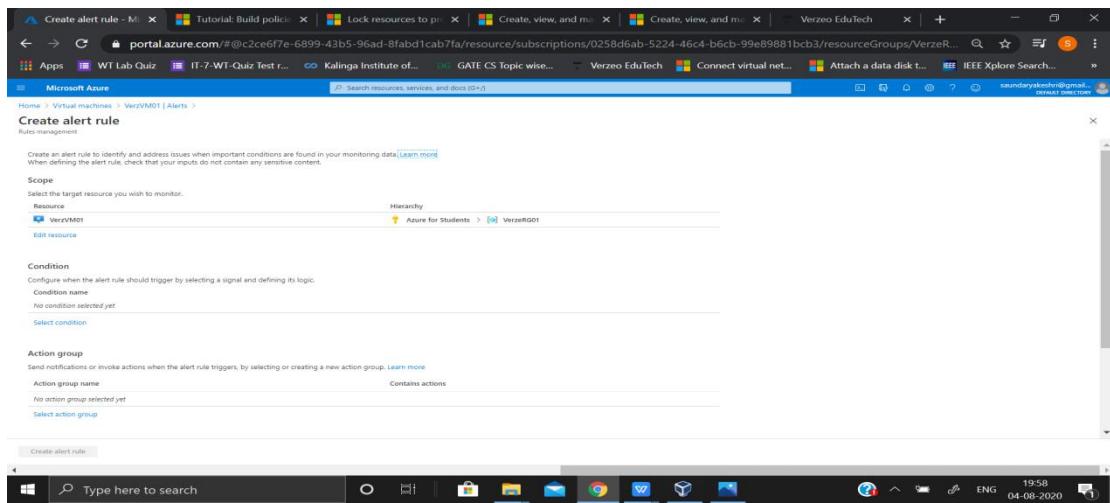
1 Failed to delete virtual network 6:55 PM
Failed to delete virtual network 'verzvnet01'. Error: The scope 'verzvnet01' cannot perform delete operation because following scope(s) are locked: 'VerzeRG01'. Please remove the lock and try again.

-Setup CPU Threshold alert for the VM (VerzVM01)

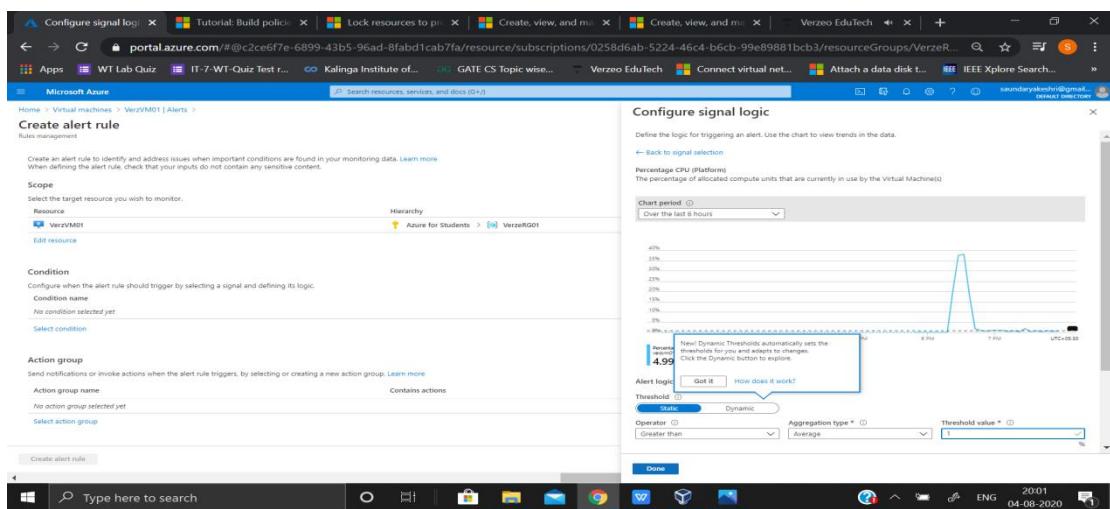
1. Go to the created virtual machine **VerzVM01** and under **Monitoring** section click on **Alert** and click on **+ New alert rule**

New alert rule
Subscription: Azure for Students
Resource group: VerzeRG01
Virtual machine: VerzVM01
Time range: Past 24 hours

Pay attention to what matters.
Configure alert rules and attend to fired alerts to efficiently monitor your Azure resources.

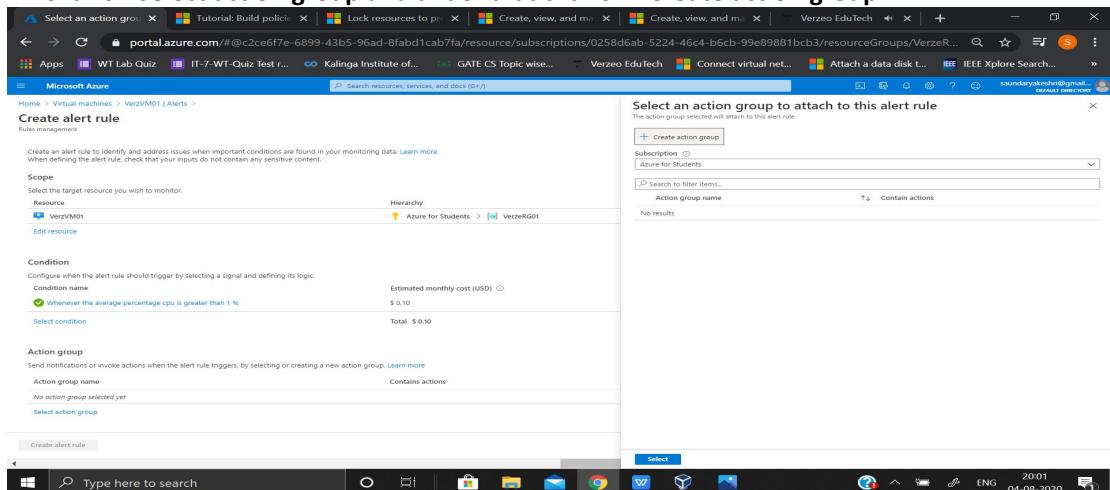


2. Click on **Select condition**. Select the appropriate option (**set threshold value as 1**) and fill the required field and click on **Done**



Create Action (Verzactgrp) Group for the above alert with your email id.
- Check if you are receiving the alert

1. Click on **Select action group** and under that click on **+Create action group**

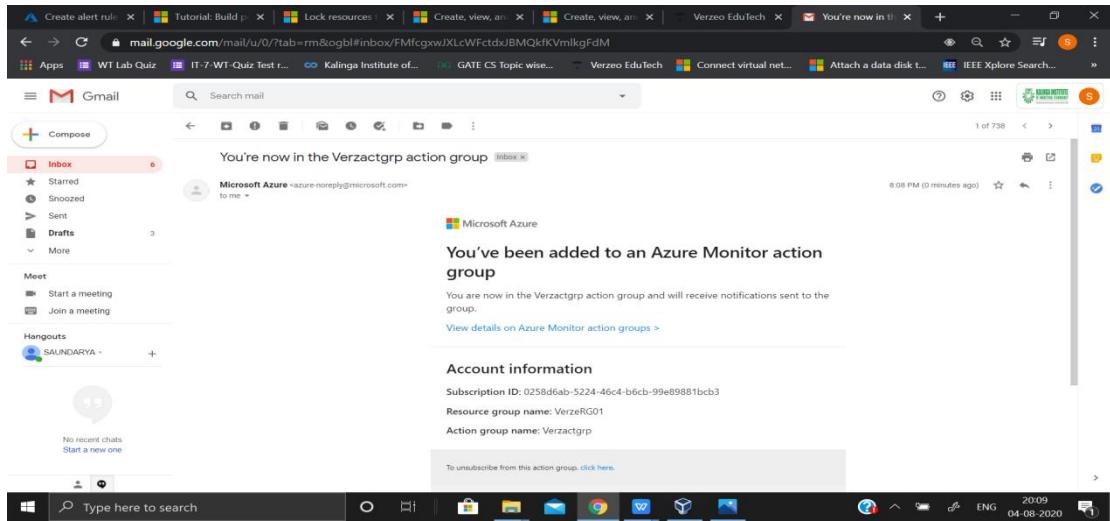


3. Filled the required field also provide the name of action group (ex- **Verzactgrp) and click on Next:Notification**

4. Select the Notification Type as Email/SMS message/Voice provide your email id and give the notification type some name (ex - **CPU Throughput) and click on Review+Create**

5. Click on Create.

6. After the successfully creation of action group we will receive a mail in registered email id.



7. Now select the created action group and fill the remaining information and click on **Create alert rule**

8. Thus the alert group **verzactgrp** is created

The screenshot shows the 'All Alerts' blade in the Azure portal. A search bar at the top finds 'verzactgrp'. Below it, a table lists an alert named 'Alert' with severity 'Sev3' and status 'Fired' for resource 'vervm01'. The alert is associated with monitor service 'Platform' and signal type 'Metric'. It was fired at 8/4/2020, 8:44 PM. The alert is linked to a subscription 'Azure for Students'.

Create a Recovery Services vault (Vezvault01) in the Resource Group (VerzeRG01)

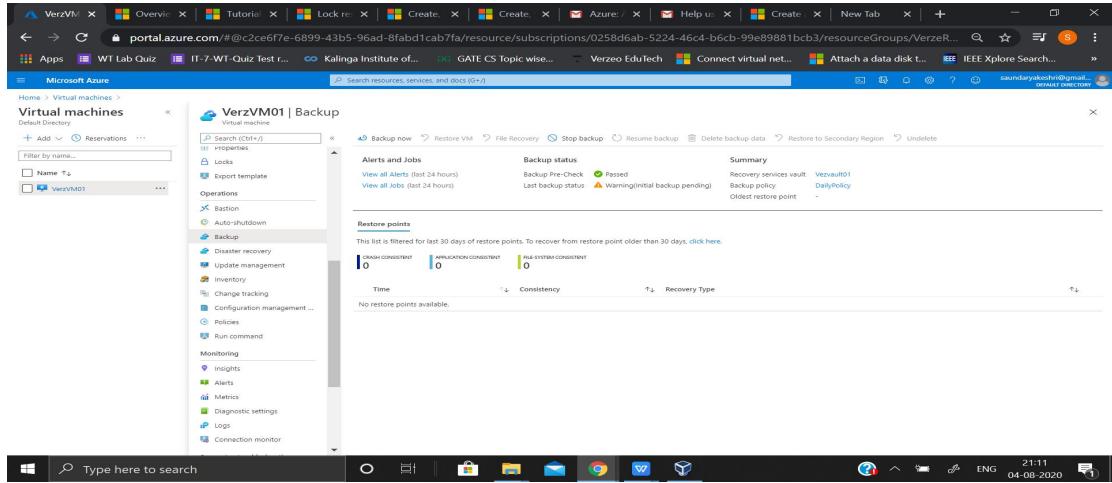
1. Go to the Virtual machine created **VerzVM01** and under **Operations** click on **Backup**, and select **Create new**. mention the vault name - **Vezvault01**
choose a Resource group - **VerzeRG01**
And choose a backup policy - **(new)DailyPolicy**
and click on **create**.
2. Wait for validation to pass and deployment to complete.

The first screenshot shows the 'VerzVM01 | Backup' blade. Under 'Operations', 'Backup' is selected. A 'Create new' dialog is open, setting the 'Recovery Service vault' to 'Vezvault01', 'Resource group' to 'VerzeRG01', and 'Backup policy' to '(new)DailyPolicy'. The status shows 'Validating...'.

The second screenshot shows the 'ConfigureVMProtection-20207421813 | Overview' blade. It displays a message 'Your deployment is complete' with details: Deployment ID 'ConfigureVMProtection-20207421813', Start time '8/4/2020, 9:08:58 PM', Correlation ID '75d42c2a-7044-4dcf-aad0-29a2e03426fe', and Next steps. The status bar indicates the deployment completed at 21:08 on 04-08-2020.

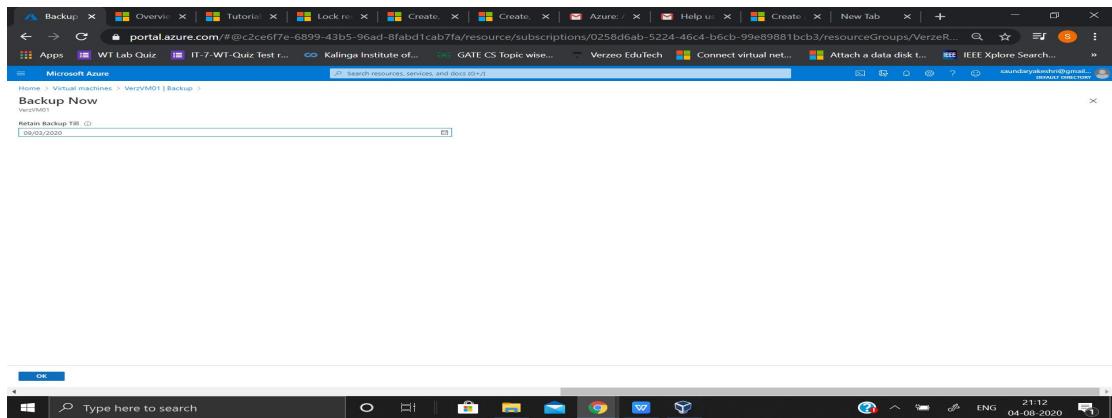
- Setup Backup for the Virtual Machine (VerzVM01) and ensure backup is completed successfully.

1. Go to the Virtual machine created **VerzVM01** and under **Operations** click on **Backup** and click on **Backup now**



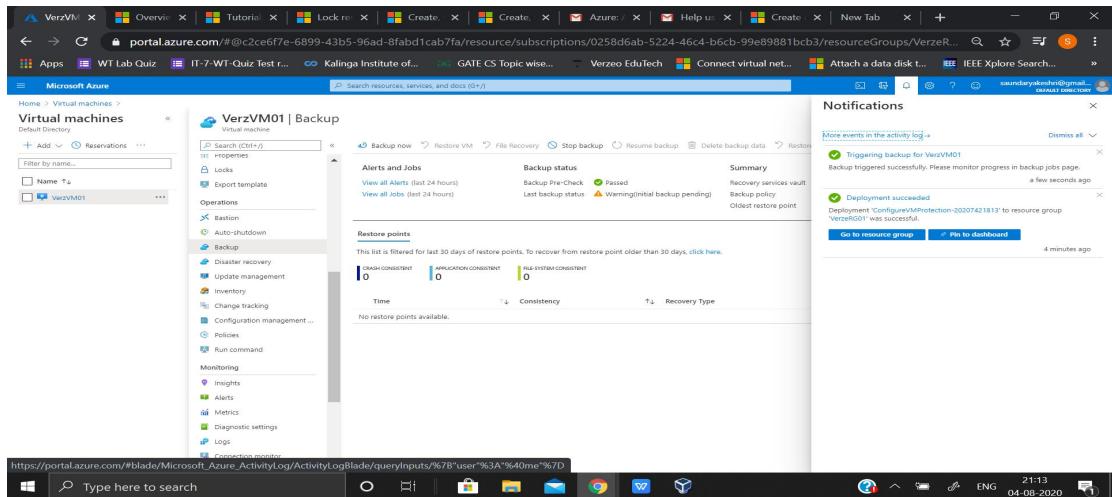
The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled 'Virtual machines' and lists 'VerzVM01'. The main content area is titled 'VerzVM01 | Backup'. It has tabs for 'Backup now', 'Restore VM', 'File Recovery', 'Stop backup', 'Resume backup', 'Delete backup data', and 'Restore to Secondary Region'. Below these tabs, there are sections for 'Alerts and Jobs', 'Backup status', and 'Summary'. Under 'Backup status', it shows 'Backup Pre-Check' as 'Passed' and 'Last backup status' as 'Warning(initial backup pending)'. The 'Summary' section indicates 'Recovery services vault' as 'VerzVault01', 'Backup policy' as 'DailyPolicy', and 'Oldest restore point'. A 'Restore points' section shows no available points. At the bottom, there is a search bar and a taskbar with various icons.

2. Select the backup retain date and click on **OK**



The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled 'Virtual machines' and lists 'VerzVM01'. The main content area is titled 'Backup Now' and shows a dropdown menu for 'Retain Backup Till' set to '09/03/2020'. At the bottom right, there is a large 'OK' button. The taskbar at the bottom includes a search bar and various icons.

Result - Backup triggered successfully.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled 'Virtual machines' and lists 'VerzVM01'. The main content area is titled 'VerzVM01 | Backup'. It has tabs for 'Backup now', 'Restore VM', 'File Recovery', 'Stop backup', 'Resume backup', 'Delete backup data', and 'Restore to Secondary Region'. Below these tabs, there are sections for 'Alerts and Jobs', 'Backup status', and 'Summary'. Under 'Backup status', it shows 'Backup Pre-Check' as 'Passed' and 'Last backup status' as 'Warning(initial backup pending)'. The 'Summary' section indicates 'Recovery services vault' as 'VerzVault01', 'Backup policy' as 'DailyPolicy', and 'Oldest restore point'. A 'Notifications' panel on the right shows a message: 'Triggering backup for VerzVM01' and 'Backup triggered successfully. Please monitor progress in backup jobs page.' Below this, another message says 'Deployment succeeded' with the note 'ConfigureVMProtection-20207421813' was successful. At the bottom, there is a search bar and a taskbar with various icons.