

Microsoft Certified Associate: Azure Administrator AZ-104

Project

***Connecting Internet Workloads Using Vnet
Peering and Assigning a Custom Role for
Operating These Workloads***

Submitted by –

Soham Bhagwan Salunke

Introduction –

The Rand Enterprises Corporation is evaluating Azure as a deployment platform. To help the company with its evaluation, we need to create virtual networks in the region specified by Rand Enterprises Corporation. We have to create test virtual machines in two virtual networks, establish connectivity between the two networks via VNet peering, and ensure connectivity is established properly.

To test the platform, Rand Enterprises Corporation wants to onboard an employee on the company's default Azure Active Directory and assign a Custom RBAC role, under which they will be able to read the network and storage along with the VM. Under this custom RBAC, the employee should also be given permission to start and restart the VM. We have to onboard the employee under the default Azure AD and create a custom RBAC for the role of computer operator for this employee.

As a security measure, we need to ensure that the onboarded user can only access the resources mentioned in the custom role and adhere to the principle of least privilege.

SYSTEM REQUIREMENTS SPECIFICATIONS

System requirements are expressed in a software requirement document. The Software requirement specification (SRS) is the official statement of what is required of the system developers. This requirement document includes the requirements definition and the requirement specification. The software requirement document is not a design document. It should set out what the system should do without specifying how it should be done. The requirement set out in this document is complete and consistent.

The software specification document satisfies the following:-

- It specifies the external system behaviors.
- It specifies constraints on the implementation.
- It is easy to change.
- It serves as reference tool for system maintainers.
- It record forethought about the life cycle of the system.
- It characterizes acceptable response to undesired events.

Tools required:

- Azure account with administrator access
- Subscription Name : Azure for Students

Implementation:

• Create Resource Group –

Resource Group Name: RandEnterprisesCorporation

Screenshot -

The screenshot shows the Azure portal interface for the 'RandEnterprisesCorporation' resource group. The left sidebar lists other resource groups: NetworkWatcherRG, Project1, and RandEnterprisesCorporation. The main content area displays the 'Overview' tab for the selected resource group. It shows the subscription is 'Azure for Students', the subscription ID is 'ec255728-b1d3-4d90-a314-f5272ce00889', and it has 6 succeeded deployments. The 'Resources' section lists 12 records, including VMs, public IP addresses, network security groups, network interfaces, and disks, all located in Central US.

Name	Type	Location
vm1	Virtual machine	Central US
vm1-ip	Public IP address	Central US
vm1-nsg	Network security group	Central US
vm1939	Network Interface	Central US
vm1_OsDisk_1_fb30383d30df412baeb219d5a7d797ce	Disk	Central US

• Create Two Virtual Networks –

Virtual Network 1 Name : vnet-1

Virtual Network 2 Name : vnet-2

Screenshot –

The screenshot shows the Microsoft Azure portal interface with the title 'Virtual networks - Microsoft Azure'. The URL in the address bar is 'portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Network%2FvirtualNetworks'. The page displays a list of two virtual networks: 'vnet-1' and 'vnet-2'. The table includes columns for Name, Resource group, Location, and Subscription. Both entries belong to the 'RandEnterprisesCorporation' resource group, are located in 'Central US', and are associated with 'Azure for Students'.

Name	Resource group	Location	Subscription
vnet-1	RandEnterprisesCorporation	Central US	Azure for Students
vnet-2	RandEnterprisesCorporation	Central US	Azure for Students

At the bottom of the screen, the Windows taskbar shows the date and time as '8:40 PM 8/21/2022' and the weather as '23°C Mostly cloudy'.

• Create Test Virtual Machines –

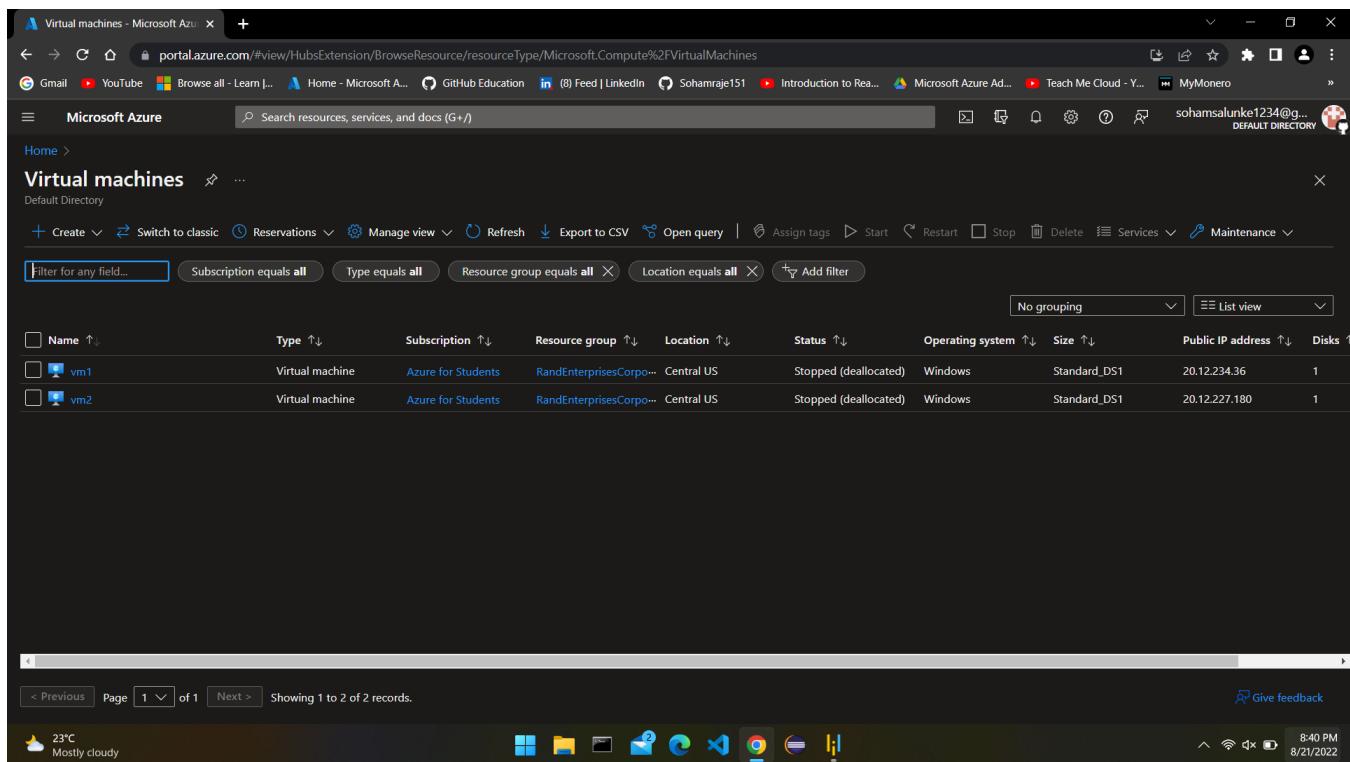
We have created two test virtual machines on two different virtual networks

As,

Virtual machine 1 (vm1) on vnet-1

Virtual machine 2 (vm2) on vnet-2

Screenshot –



The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The URL in the browser is portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Compute%2FVirtualMachines. The page title is "Virtual machines - Microsoft Azure". The main content area displays a table of virtual machines:

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
vm1	Virtual machine	Azure for Students	RandEnterprisesCorpo...	Central US	Stopped (deallocated)	Windows	Standard_DS1	20.12.234.36	1
vm2	Virtual machine	Azure for Students	RandEnterprisesCorpo...	Central US	Stopped (deallocated)	Windows	Standard_DS1	20.12.227.180	1

At the bottom of the table, it says "Showing 1 to 2 of 2 records." The portal has a dark theme, and the status bar at the bottom shows the date and time as 8:40 PM on 8/21/2022.

● VNet Peering –

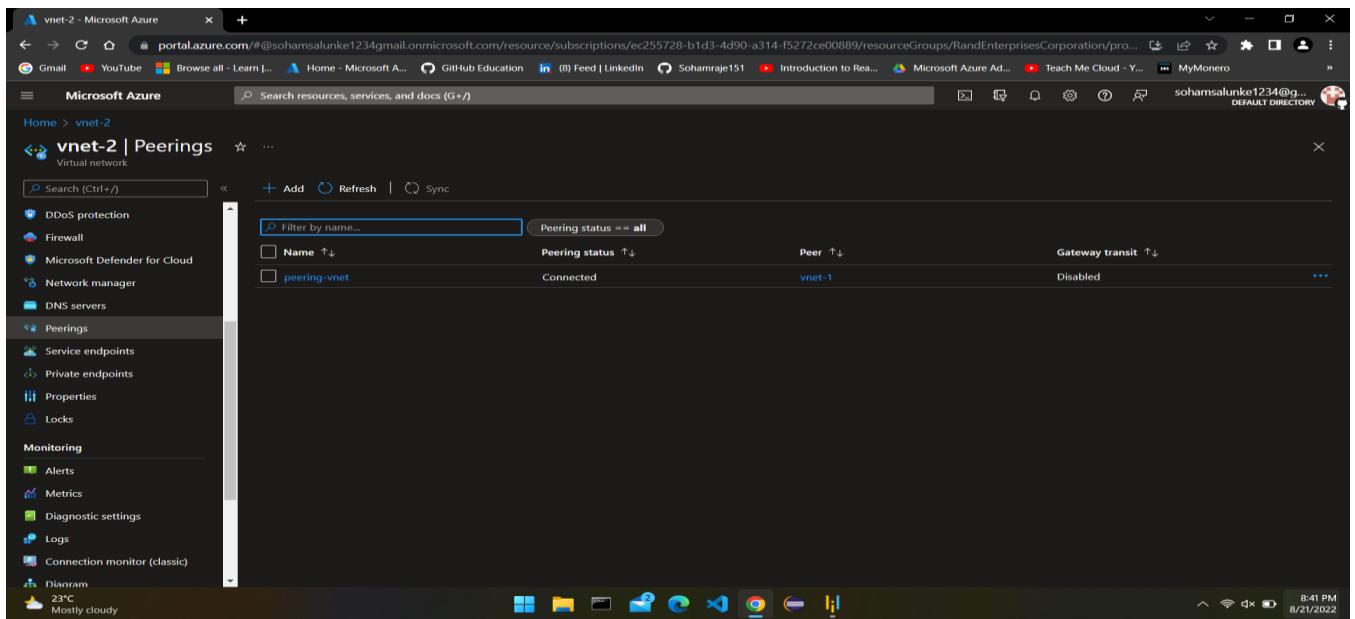
connectivity established between the two networks via VNet peering, and ensured that connectivity is established properly.

Screenshot –

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar is visible, showing the current path: Home > vnet-1 > vnet-1 | Peering. The main content area displays the 'Peering' section for the 'vnet-1' virtual network. A table lists one peering connection:

Name	Peer	Peering status	Gateway transit
test	vnet-2	Connected	Disabled

The table includes a search bar at the top and filter options for 'Name' and 'Peering status'. The status column shows 'all' as the filter. The bottom right corner of the screen shows the Windows taskbar with various pinned icons and the date/time as 8/21/2022, 8:41 PM.



- **Onboard the employee under the default Azure AD –**

User – employee

User principle name -

computer_operator@sohamsalunke1234@gmail.onmicrosoft.com

Job title – Computer Operator

Company name – Rand Enterprises Corporation

Screenshot -

The screenshot shows the Microsoft Azure portal interface for managing users. The user profile for 'employee' is displayed, showing details such as first name (Computer), last name (Operator), and principal name (computer_operator@sohamsalunke1234gmail.onmicrosoft.com). The user is assigned to the 'Rand Enterprises Corporation' and holds a job title of 'Computer Operator'. The account is enabled and located in the United States.

- **Assign a custom RABC role –**

Assign a Custom RBAC role, under which they will be able to read the network and storage along with the VM. Under this custom RBAC, the employee should also be given permission to start and restart the VM. We have to onboard the employee under the default Azure AD and create a custom RBAC for the role of computer operator for this employee.

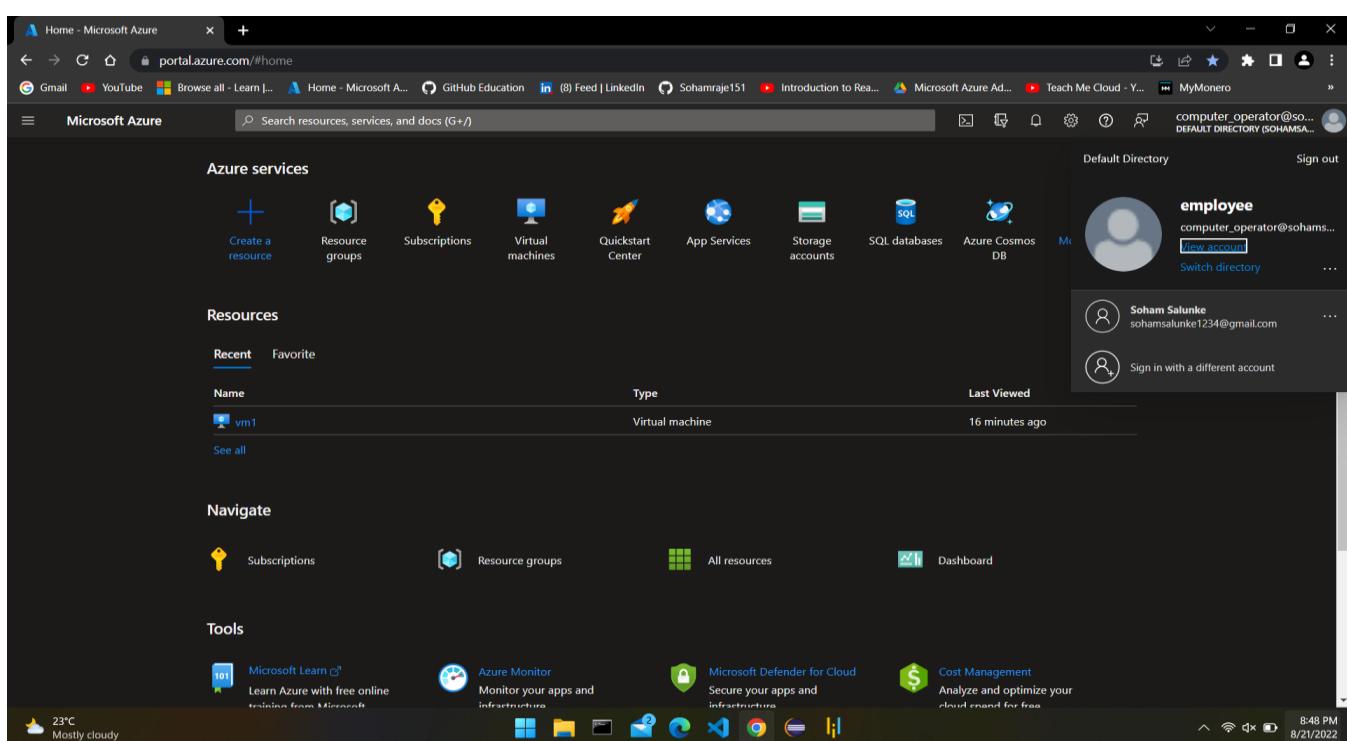
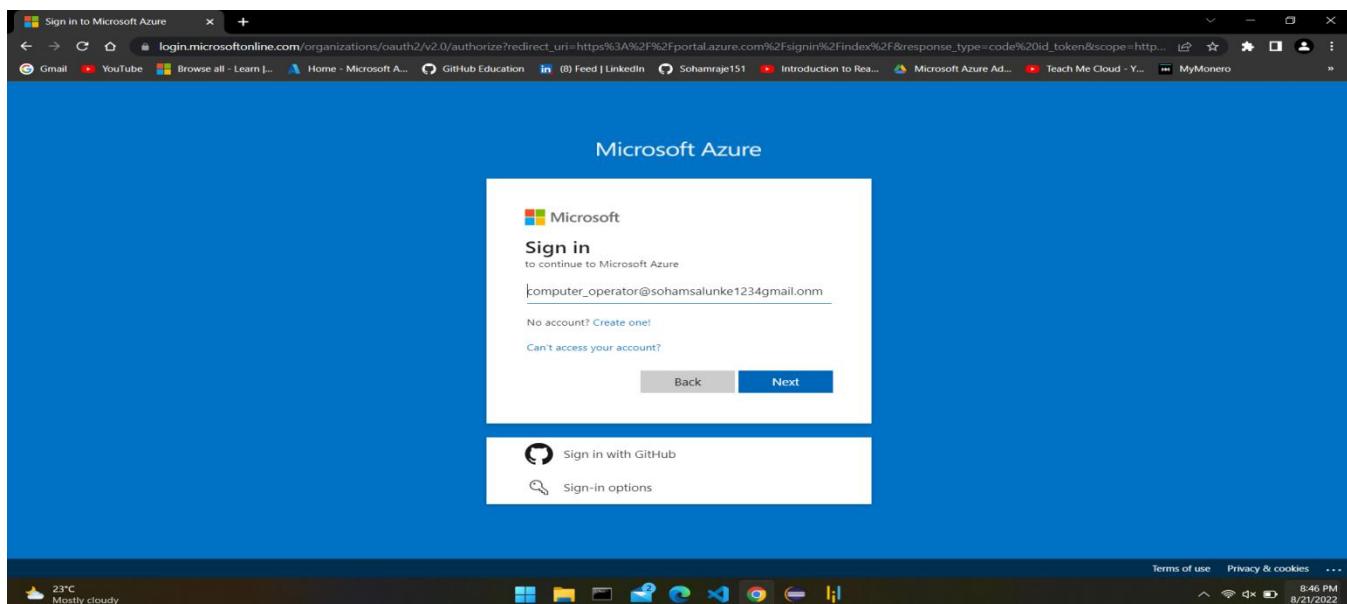
Screenshot –

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings' (with 'Deployments', 'Security', 'Policies', 'Properties', 'Locks'), 'Cost Management' (with 'Cost analysis', 'Cost alerts (preview)', 'Budgets'), and a weather widget ('23°C Mostly cloudy'). The main content area is titled 'RandEnterprisesCorporation | Access control (IAM)' and shows 'Role assignments'. It indicates there are 2 items (2 Users) listed. The table below shows the details:

Name	Type	Role	Scope	Condition
employee computer_operator@sohamsalunke1234@gmail.com	User	Owner	This resource	None
Soham Salunke sohamsalunke1234@gmail.com	User	Owner	Subscription (Inherited)	None

- **Login with user account and Test virtual machines , connectivity using VNet Peering –**

1. Login –



2. Start virtual machines –

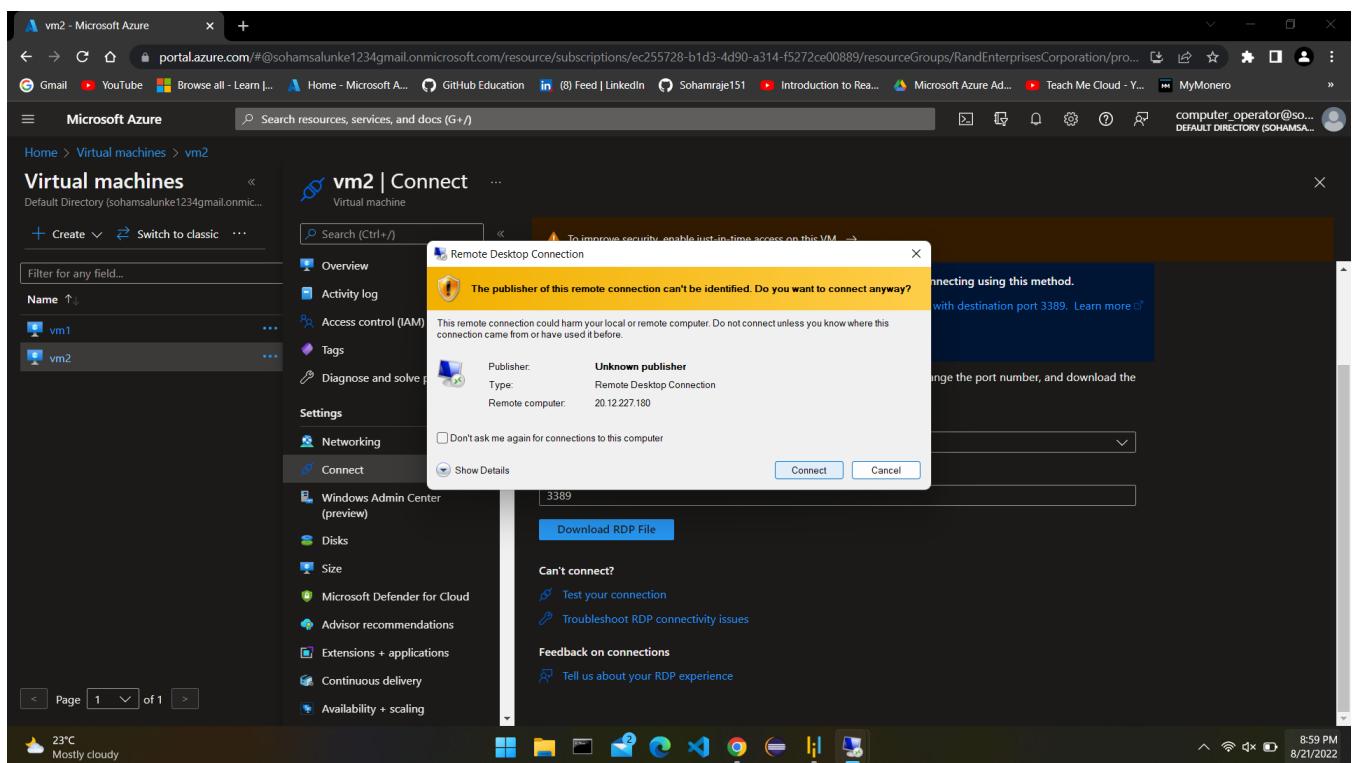
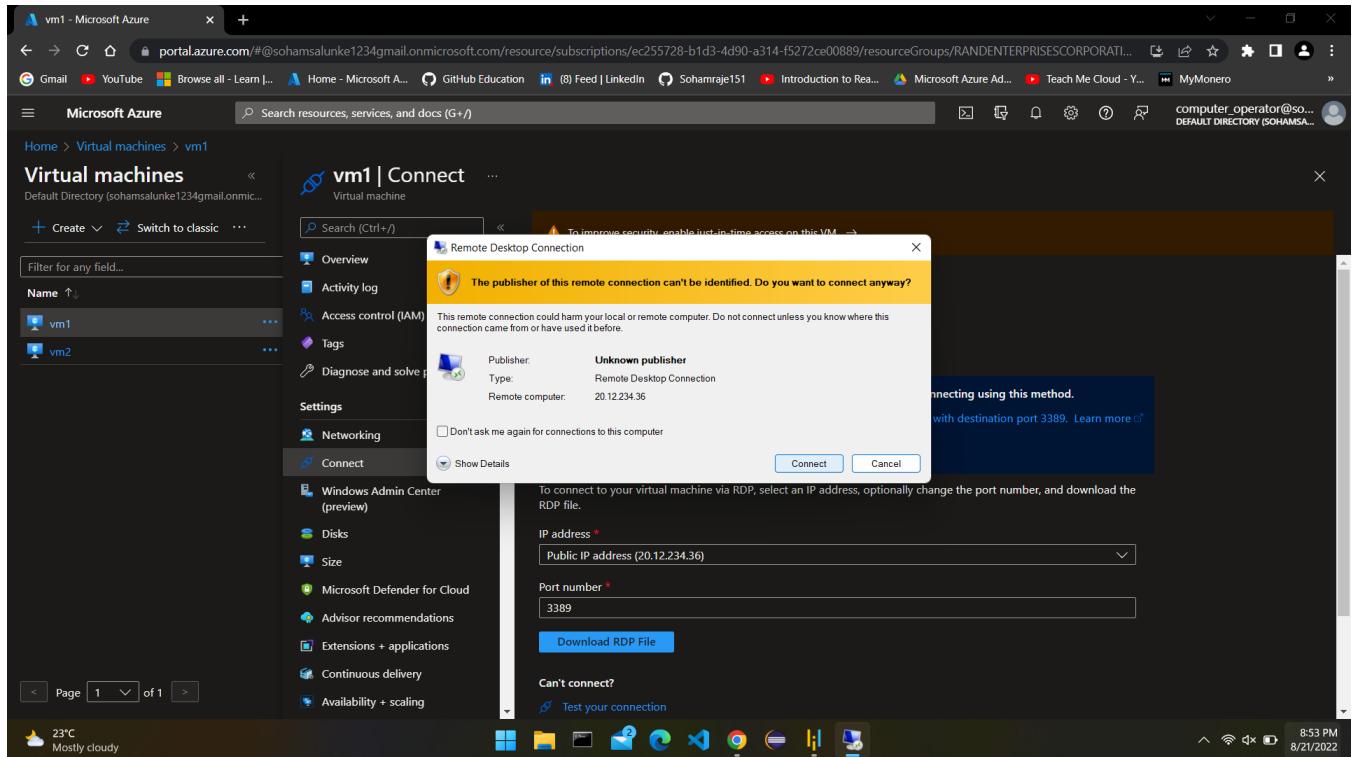
A screenshot of the Microsoft Azure portal showing a confirmation dialog. The title bar says "Virtual machines - Microsoft Azure". The URL in the address bar is "portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Compute%2FVirtualMachines". The main content area shows a table of two virtual machines: "vm1" and "vm2". Both are currently "Stopped (deallocated)". A confirmation message at the top asks, "Do you want to start all the selected virtual machines? This operation will start all the virtual machines selected below." Below the message are "Yes" and "No" buttons. The table has columns for Name, Type, Subscription, Resource group, Location, Status, and a checkbox column for selection.

	Name	Type	Subscription	Resource group	Location	Status
<input checked="" type="checkbox"/>	vm1	Virtual machine	Azure for Students	RandEnterprisesCorpo...	Central US	Stopped (deallocated)
<input checked="" type="checkbox"/>	vm2	Virtual machine	Azure for Students	RandEnterprisesCorpo...	Central US	Stopped (deallocated)

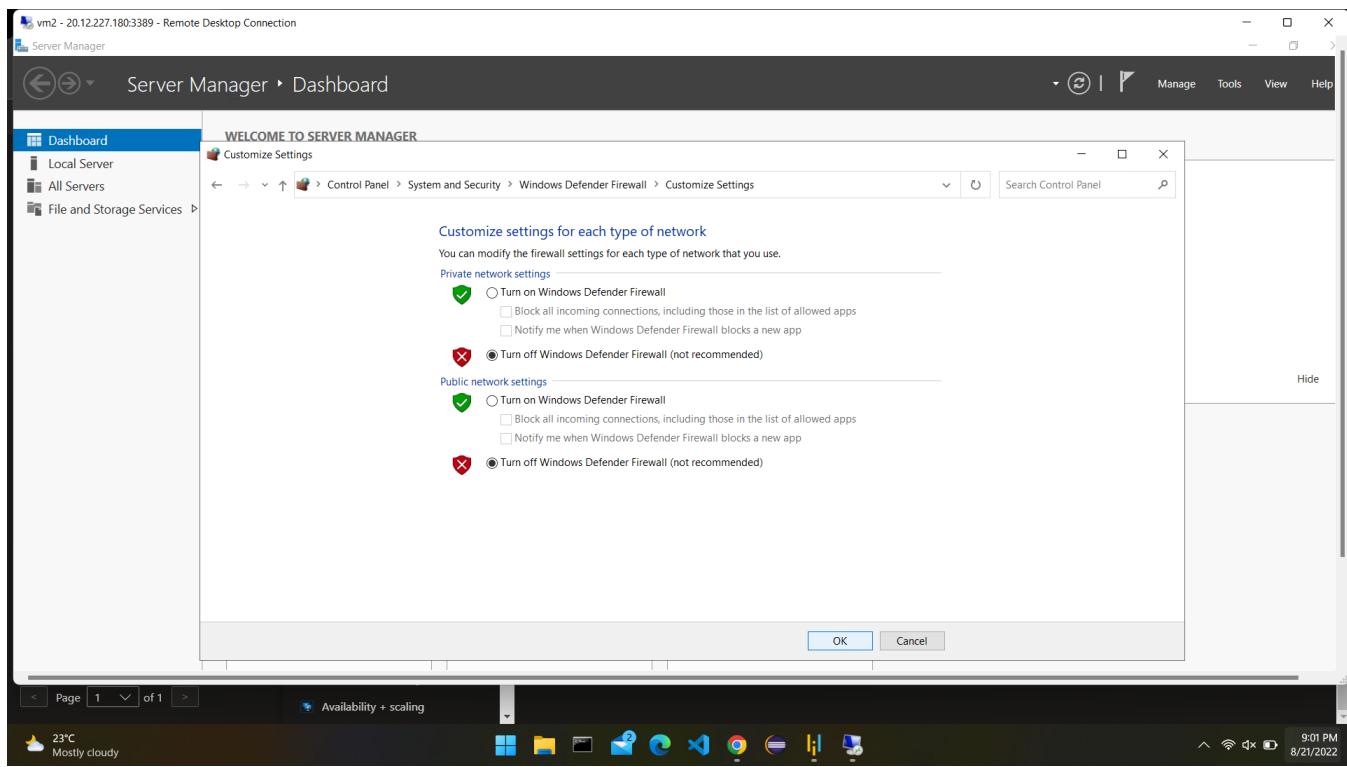
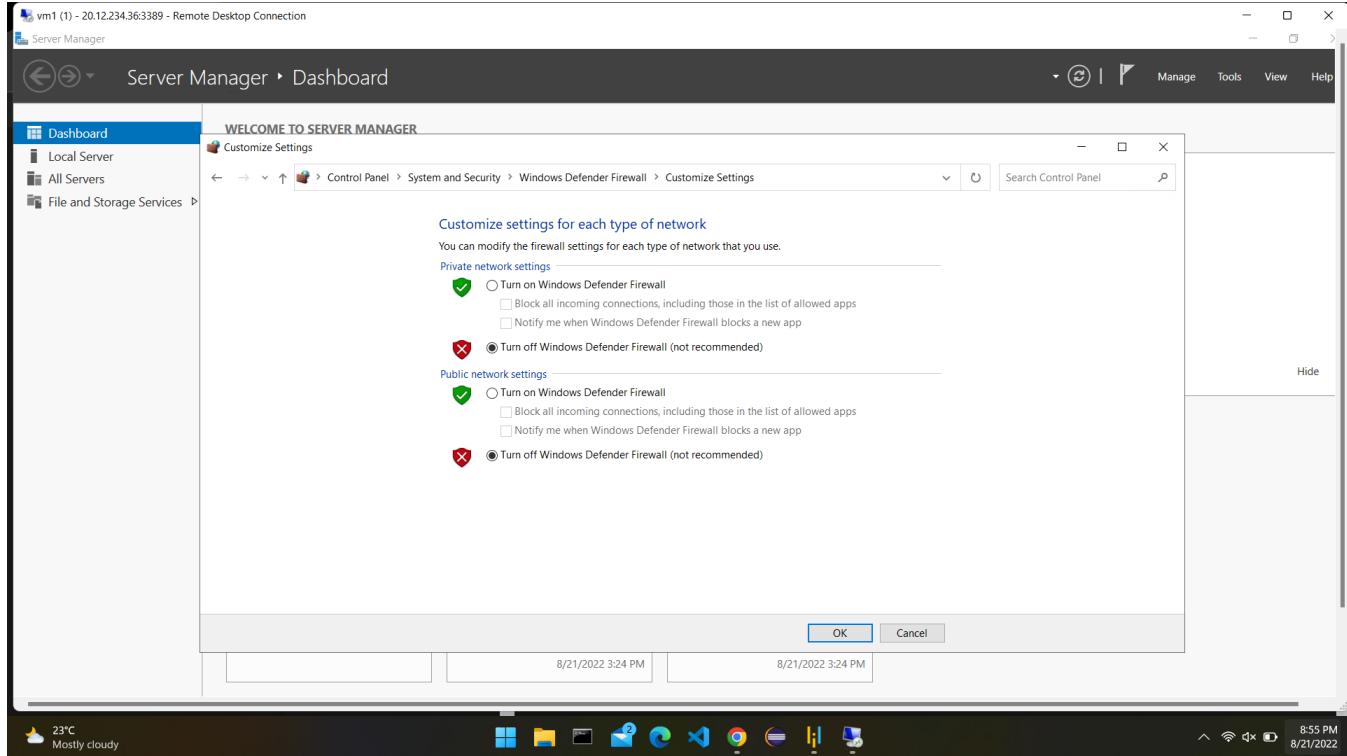
A screenshot of the Microsoft Azure portal showing the virtual machines list. The title bar says "Virtual machines - Microsoft Azure". The URL in the address bar is "portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Compute%2FVirtualMachines". The main content area shows a table of two virtual machines: "vm1" and "vm2". Both are now listed as "Running". Above the table, there are filter options: "Filter for any field...", "Subscription equals all", "Type equals all", "Resource group equals all", "Location equals all", and "Add filter". To the right of the main content, there is a "Notifications" sidebar with a single notification: "Executed start command on 2 selected items" (Succeeded: 2, Failed: 0, Canceled: 0). The status bar at the bottom shows "23°C Mostly cloudy" and the date "8/21/2022".

	Name	Type	Subscription	Resource group	Location	Status
<input type="checkbox"/>	vm1	Virtual machine	Azure for Students	RANDENTERPRISES...CO...	Central US	Running
<input type="checkbox"/>	vm2	Virtual machine	Azure for Students	RANDENTERPRISES...CO...	Central US	Running

3. Connect both Virtual machines through RDP –



4.Turn Off firewall settings of both virtual machines –



5. Check VNet Peerings –

vnet-1 - Microsoft Azure

portal.azure.com/#@sohamsalunke123@gmail.onmicrosoft.com/resource/subscriptions/ec255728-b1d3-4d90-a314-f5272ce00889/resourceGroups/RandEnterprisesCorporation/pro...

Gmail YouTube Browse all - Learn ... Home - Microsoft A... GitHub Education LinkedIn Sohamraje151 Introduction to Re... Microsoft Azure Ad... Teach Me Cloud - Y... MyMonero

Microsoft Azure Search resources, services, and docs (G+/-)

computer_operator@so...
DEFAULT DIRECTORY SOHAMSA...

Home > Virtual networks > vnet-1

Virtual networks

Default Directory (sohamsalunke123@gmail.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name	Peering status	Peer	Gateway transit
vnet-1	Connected	vnet-2	Disabled
vnet-2	Connected	vnet-1	Disabled

Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS servers
Peerings
Service endpoints
Private endpoints
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings

Page 1 of 1

23°C Mostly cloudy 8:57 PM 8/21/2022

vnet-2 - Microsoft Azure

portal.azure.com/#@sohamsalunke123@gmail.onmicrosoft.com/resource/subscriptions/ec255728-b1d3-4d90-a314-f5272ce00889/resourceGroups/RandEnterprisesCorporation/pro...

Gmail YouTube Browse all - Learn ... Home - Microsoft A... GitHub Education LinkedIn Sohamraje151 Introduction to Re... Microsoft Azure Ad... Teach Me Cloud - Y... MyMonero

Microsoft Azure Search resources, services, and docs (G+/-)

computer_operator@so...
DEFAULT DIRECTORY SOHAMSA...

Home > Virtual networks > vnet-2

Virtual networks

Default Directory (sohamsalunke123@gmail.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

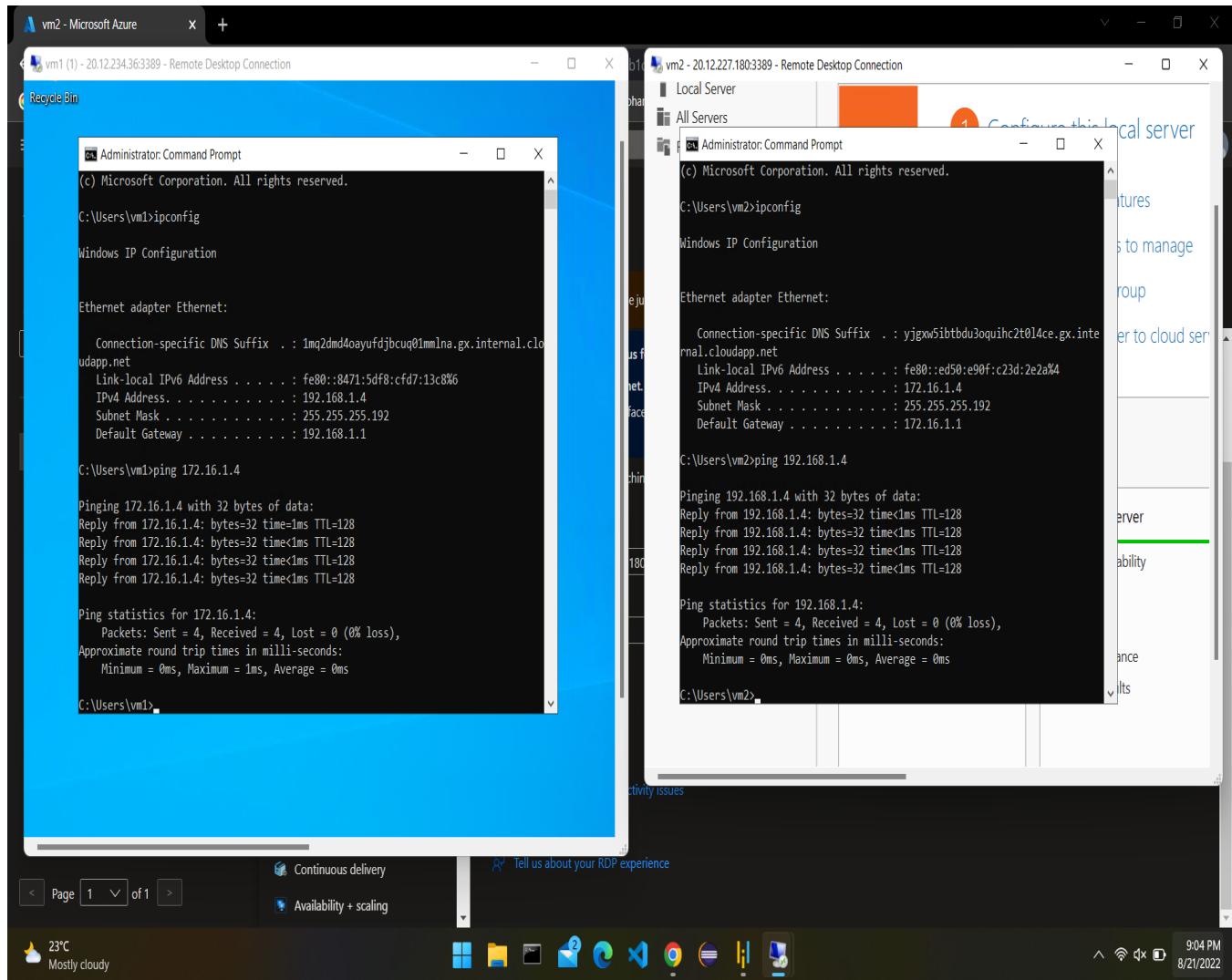
Name	Peering status	Peer	Gateway transit
vnet-1	Connected	vnet-2	Disabled
vnet-2	Connected	vnet-1	Disabled

Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS servers
Peerings
Service endpoints
Private endpoints
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings

Page 1 of 1

23°C Mostly cloudy 8:58 PM 8/21/2022

6. establish connectivity between the two networks via VNet peering, and ensure connectivity is established properly on both Virtual Machines –



Expected Deliverables:

- Identify the networks
- Workload deployed to these networks
- Establishing the connectivity between these networks
- Onboard a user
- Create and assign a custom role to the user.