

# NetMaze Explorer

## (Implement and manage virtual networking)

Manual

By  
Vivek Vashisht



Date: 26 August 2024

Contact:

LinkedIn: <https://www.linkedin.com/in/vivek-vashisht04/>

GitHub: <https://github.com/vivekvashisht04/NetMazeExplorer>

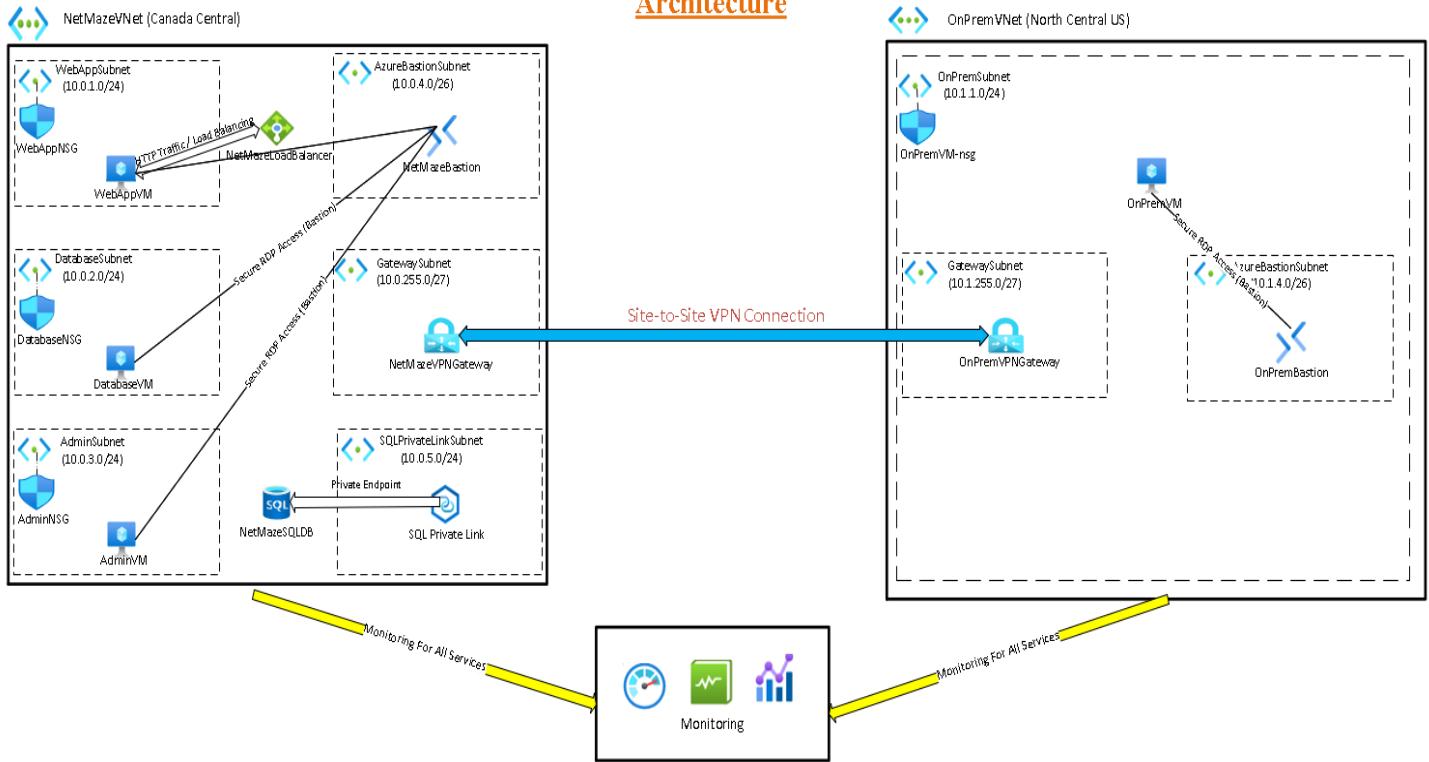
# Table of Contents

- Introduction
- Azure Virtual Network Setup
- On-Premises Network Simulation
- Secure Connectivity
- Resource Deployment
- Network Access Control
- Private Access to Azure PaaS Services
- DNS and Load Balancing
- Access Control
- Performance and Security Testing
- Monitoring and Auditing

# Project Architecture Diagram

## NetMaze Explorer: Azure Hybrid Networking

### Architecture



# Introduction

## **Project Overview**

The NetMaze Explorer: Azure Hybrid Networking Architecture project represents a comprehensive endeavour to create a secure and efficient hybrid networking environment using Microsoft Azure's robust suite of networking services. This project involves establishing a seamless connection between on-premises networks and Azure cloud resources, ensuring secure data transition, effective resource access controls, and optimized network performance.

Throughout the project, I utilized various Azure services such as Virtual Networks, VPN Gateways, Network Security Groups (NSGs), Azure Bastion, and Azure Private Link. The goal was to design and implement a hybrid network infrastructure that meets both security and performance requirements. The project captures the entire process, from initial network setup to the deployment of resources and final testing, ensuring that all components function as intended within a hybrid cloud environment.

## **Purpose of this Documentation**

This document provides a comprehensive, step-by-step guide for replicating the NetMaze Explorer project, complete with instructions and screenshots to ensure clarity. It serves as a resource for understanding how to set up a hybrid network on Azure, beneficial for both students and professionals. The primary goal is to document my project thoroughly, showcasing my technical skills and thought process, and to serve as a professional record for potential employers and the broader community.

## **Prerequisites**

Before starting this project, it's important to have a basic understanding of cloud computing, networking concepts, and the Azure portal. Additionally, you should ensure that you meet the following prerequisites:

1. Azure Subscription: A valid Azure subscription is necessary for deploying and managing resources.
2. Basic Networking Knowledge: Understanding of IP addressing, subnets, and network security concepts.
3. Azure CLI/PowerShell (Optional): Familiarity with Azure CLI or PowerShell can be beneficial for advanced configurations and automation tasks.
4. Text Editor (Optional): A text editor, such as Visual Studio Code, may be useful for managing scripts and configuration files.

This documentation, created to showcase how I completed the project, provides a practical guide to building and managing a hybrid network in Azure, offering key insights and best practices for successfully replicating the NetMaze Explorer project.

# Azure Virtual Network Setup

## 1.1. Creating the Resource Group

First, I created a resource group where I planned to deploy the entire project.

1. I logged into the Azure portal and navigated to the Resource Groups section.
2. I clicked on + Create to start the creation process.
3. For the resource group, I entered the following details:
  - o Resource Group Name: NetMazeRG
  - o Region: Canada Central (I chose this region for the entire project)
4. After filling in the details, I clicked on Review + Create, and then selected Create to finalize the deployment of the resource group.

## 1.2. Deploying the Azure Virtual Network (VNet)

Next, I moved on to deploying the Azure Virtual Network (VNet).

1. I navigated to the Virtual Networks section within the Azure portal.
2. I clicked on + Create to initiate the VNet setup.
3. I entered the necessary details:
  - o Name: NetMazeVNet
  - o Region: Canada Central
  - o IP Address Space: 10.0.0.0/16
4. Once all details were entered, I clicked on Review + Create and then Create to deploy the VNet.

## 1.3. Configuring Subnets

After setting up the VNet, I configured the required subnets to effectively segregate resources.

1. I added the following subnets within the VNet:
  - o WebAppSubnet:
    - IPv4 Address Range: 10.0.1.0/24
  - o DatabaseSubnet:
    - IPv4 Address Range: 10.0.2.0/24
  - o AdminSubnet:
    - IPv4 Address Range: 10.0.3.0/24
2. These subnets were added to ensure efficient resource segregation within the network.

## 1.4. Creating the Gateway Subnet

To prepare for the upcoming site-to-site VPN connection, I created a gateway subnet.

1. I added a GatewaySubnet with the following configuration:
  - o Name: GatewaySubnet
  - o IPv4 Address Range: 10.0.255.0/27
2. This gateway subnet was essential for deploying the VPN gateway in later stages.

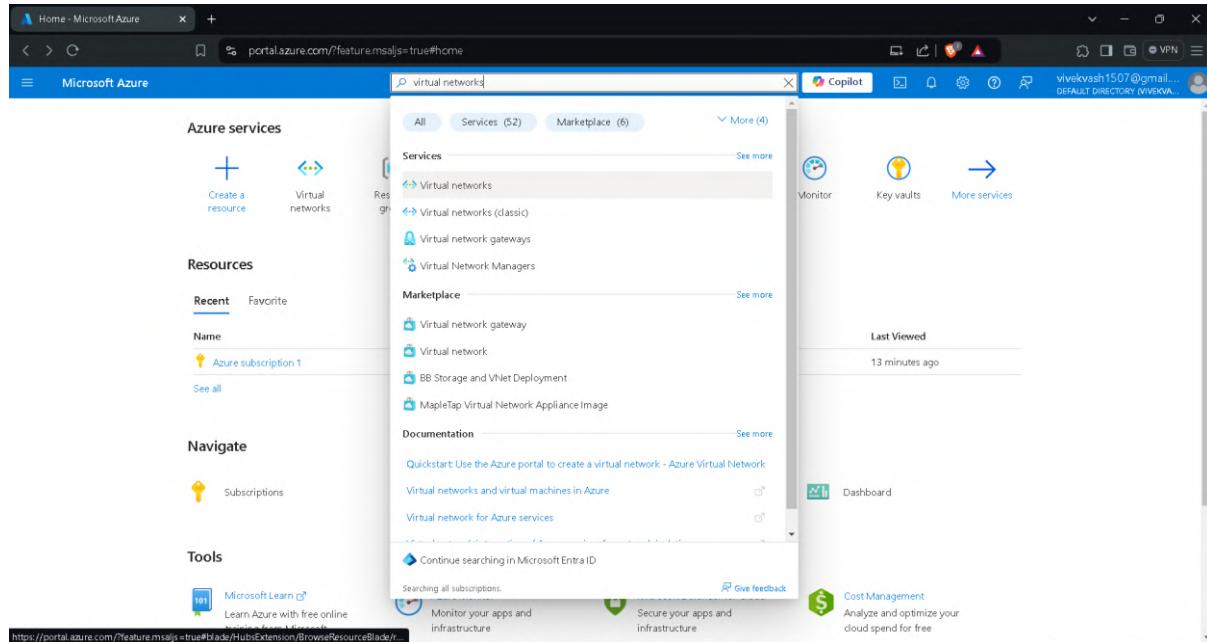
## 1.5. Finalizing the Virtual Network Deployment

To complete the network setup, I reviewed and deployed the VNet.

1. I reviewed the entire VNet configuration by clicking on Review + Create.
2. Finally, I clicked on Create to deploy the NetMazeVNet.

In this section, I established the foundational network infrastructure by creating a resource group, deploying a virtual network, and setting up essential subnets, including a gateway subnet to support secure connections in later phases.

## Screenshots



Create virtual network - Microsoft Azure

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

## Create virtual network

Basics Security IP addresses Tags Review + create

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Azure subscription 1

Resource group \* (New) NetMazeRG

Create new

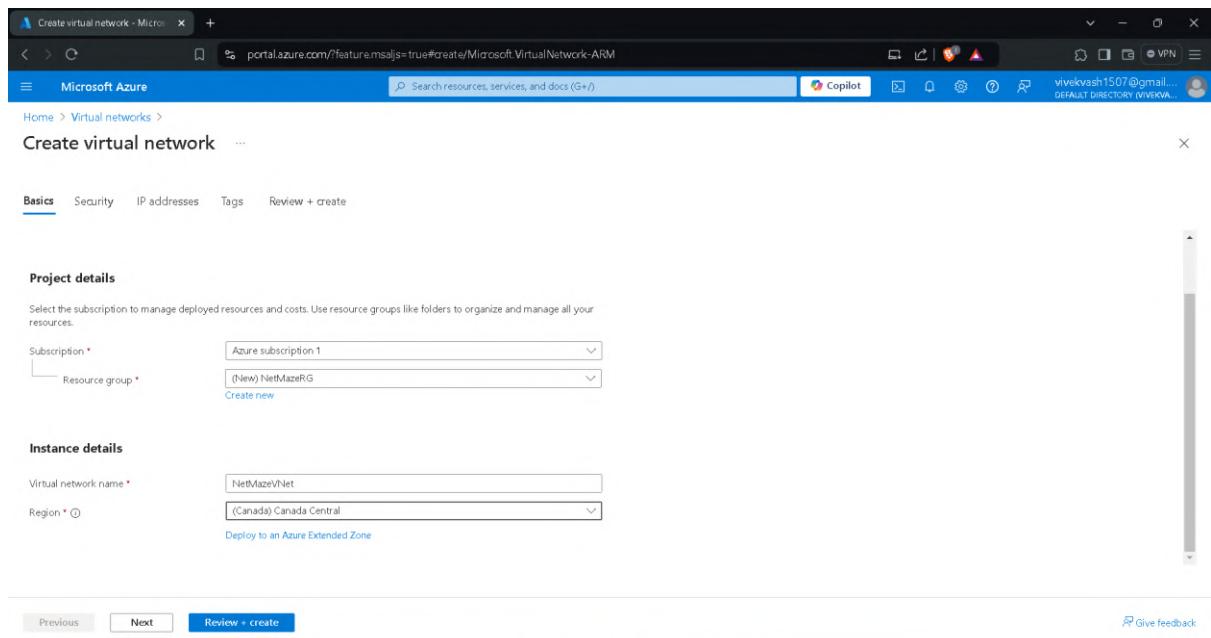
**Instance details**

Virtual network name \* NetMazeVNet

Region \* (Canada) Canada Central

Deploy to an Azure Extended Zone

Previous Next Review + create Give feedback



Create virtual network - Microsoft Azure

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

## Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space | /16 Added address prefix '10.0.0.0/16' to the virtual network

10.0.0.0/16 Delete address space

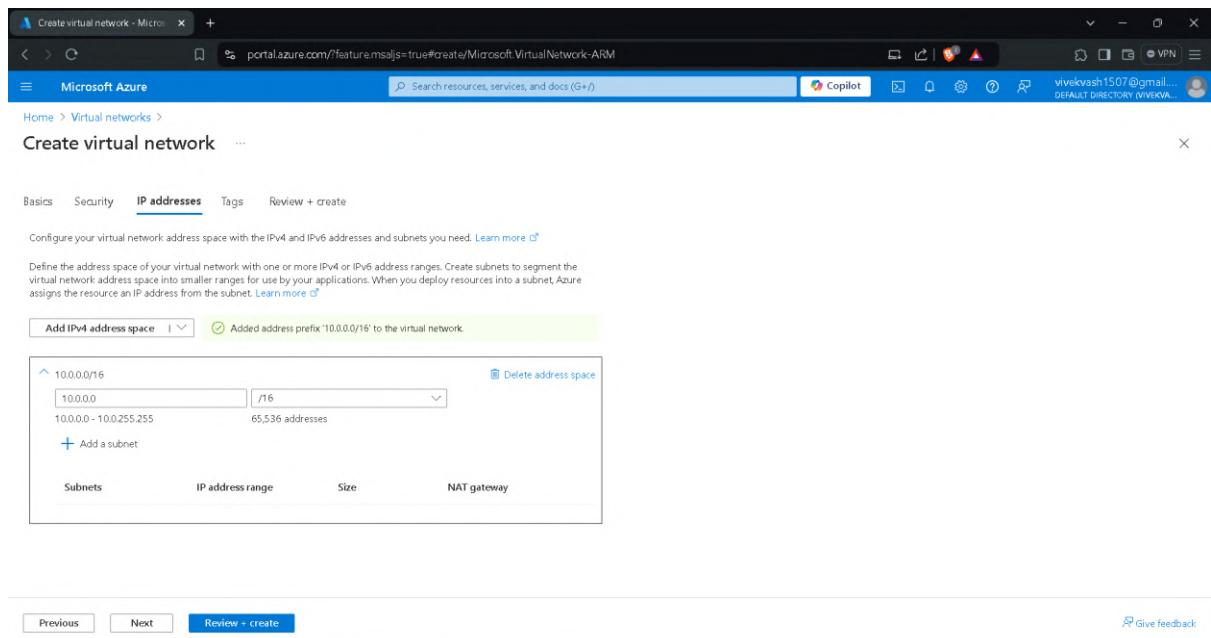
10.0.0.0 /16 65,536 addresses

10.0.0.0 - 10.0.255.255

+ Add a subnet

Subnets	IP address range	Size	NAT gateway

Previous Next Review + create Give feedback



**Add a subnet - Microsoft Azure**

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, it assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space |

10.0.0.0/16  Delete all

10.0.0.0 /16 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
WebAppSubnet	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose  Default  WebAppSubnet

Name \*

IPv4

Include an IPv4 address space

IPv4 address range \*  10.0.0.0/16  
10.0.0.0 - 10.0.255.255

Starting address \*  10.0.1.0

Size  /24 (256 addresses)

Subnet address range  10.0.1.0 - 10.0.1.255

IPv6

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Add Cancel Give feedback

**Add a subnet - Microsoft Azure**

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, it assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space |

10.0.0.0/16  Delete all

10.0.0.0 /16 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
WebAppSubnet	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose  Default  DatabaseSubnet

Name \*

IPv4

Include an IPv4 address space

IPv4 address range \*  10.0.0.0/16  
10.0.0.0 - 10.0.255.255

Starting address \*  10.0.2.0

Size  /24 (256 addresses)

Subnet address range  10.0.2.0 - 10.0.2.255

IPv6

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Add Cancel Give feedback

Add a subnet - Microsoft Azure

portal.azure.com/?feature.msaljs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, assign the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space | ▾

10.0.0.16  
10.0.0 /16  
10.0.0 - 10.0.255.255 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
WebAppSubnet	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-
DatabaseSubnet	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-

Add a subnet

Add a subnet

Subnet purpose Default

Name \* AdminSubnet

IPv4

Include an IPv4 address space

IPv4 address range \* 10.0.0.0/16  
10.0.0 - 10.0.255.255

Starting address \* 10.0.3.0

Size \* /24 (256 addresses)

Subnet address range 10.0.3.0 - 10.0.3.255

IPv6

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Add Cancel Give feedback

Create virtual network - Microsoft Azure

portal.azure.com/?feature.msaljs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Add IPv4 address space | ▾

10.0.0.16  
10.0.0 /16  
10.0.0 - 10.0.255.255 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
WebAppSubnet	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-
DatabaseSubnet	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-
AdminSubnet	10.0.3.0 - 10.0.3.255	/24 (256 addresses)	-

Add a subnet

Add a subnet

Subnet purpose Default

Name \* AdminSubnet

IPv4

Include an IPv4 address space

IPv4 address range \* 10.0.0.0/16  
10.0.0 - 10.0.255.255

Starting address \* 10.0.3.0

Size \* /24 (256 addresses)

Subnet address range 10.0.3.0 - 10.0.3.255

IPv6

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Add Cancel Give feedback

**NetMazeVNet - Microsoft Azure**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > NetMazeVNet-1723872448383 | Overview >

## NetMazeVNet

Virtual network

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Automation

Help

Move Delete Refresh Give feedback

Essentials

Resource group (move) : NetMazeRG

Location (move) : Canada Central

Subscription (move) : Azure subscription 1

Subscription ID : ee9ea131-d6f1-4e0b-bae-b293615685ae

Address space : 10.0.0.0/16

DNS servers : Azure provided DNS service

Flow timeout : Configure

BGP community string : Configure

Virtual network ID : 113e86b0-2f20-4ba2-a3ee-edd26427e642

Tags (edit) : Add tags

Topology Properties Capabilities (5) Recommendations Tutorials

DDoS protection : Not configured

Azure Firewall : Not configured

Peering : Not configured

Microsoft Defender for Cloud : Not configured

Private endpoints : Privately access Azure services without sending traffic across internet.

JSON View

The screenshot shows the Azure Virtual Network overview page for 'NetMazeVNet'. It displays basic information such as the resource group (NetMazeRG), location (Canada Central), and address space (10.0.0.0/16). It also lists several security and connectivity features: DDoS protection, Azure Firewall, Peering, and Microsoft Defender for Cloud, all of which are currently not configured. A 'Private endpoints' section is also present. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Monitoring, Automation, and Help.

**Add a subnet - Microsoft Azure**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Resource groups > NetMazeRG > NetMazeVNet

## NetMazeVNet | Subnets

Virtual network

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS servers

Peering

Service endpoints

Search subnets

+ Subnet + Gateway subnet Refresh Manage u

Name ↑	IPv4 ↑	IPv6 ↑
WebAppSubnet	10.0.1.0/24	-
DatabaseSubnet	10.0.2.0/24	-
AdminSubnet	10.0.3.0/24	-

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose : Virtual Network Gateway

Name \* : GatewaySubnet

IPv4

Include an IPv4 address space

IPv4 address range \* : 10.0.0.0/16  
10.0.0.0 - 10.0.255.255

Starting address \* : 10.0.255.0

Size \* : /27 (32 addresses)

IPv6

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Add Cancel Give feedback

The screenshot shows the 'Add a subnet' dialog for 'NetMazeVNet'. It includes fields for the subnet name ('GatewaySubnet'), IPv4 address range ('10.0.0.0/16'), starting address ('10.0.255.0'), and size ('/27'). There are checkboxes for including an IPv4 address space and selecting a subnet template. A 'Private subnet' section is shown with a preview link. The left sidebar of the Azure portal is visible, showing the 'Subnets' section under 'Connected devices'.

# On-Premises Network Simulation

## 2.1. Deploying the Azure Virtual Network (VNet) for On-Premises Simulation

To simulate an on-premises environment, I used another VNet located in a different Azure region.

- Resource Group Selection:
  - I chose the existing resource group, "NetMazeRG", where the project resources are organized.
- VNet Deployment:
  - I navigated to the Virtual Networks section within the Azure portal.
  - Clicked on + Create to start the deployment process.
  - VNet Name: OnPremVNet
  - Region: North Central US (Selected to represent the on-premises environment)
  - IP Address Space: 10.1.0.0/16
- Finalizing Deployment:
  - After filling in the required details, I clicked on Review + Create and then Create to finalize the deployment of OnPremVNet.

## 2.2. Configuring the Subnet

Within the OnPremVNet, I configured a subnet to support resource segregation.

- Subnet Configuration:
  - Subnet Name: OnPremSubnet
  - IPv4 Address Range: 10.1.1.0/24
  - Starting Address: 10.1.1.0
  - Size: /24 (256 addresses)
- Purpose:
  - This subnet is used to organize resources within the simulated on-premises network.

## 2.3. Creating the Gateway Subnet

To prepare for a future Site-to-Site VPN connection between the on-premises simulation and the main Azure VNet (NetMazeVNet), I set up a Gateway Subnet.

- Gateway Subnet Configuration:
  - Subnet Name: GatewaySubnet
  - IPv4 Address Range: 10.1.255.0/27

- Size: /27 (32 addresses)
- Significance:
  - The GatewaySubnet is essential for deploying a VPN Gateway, enabling secure connectivity between the on-premises simulation and Azure.

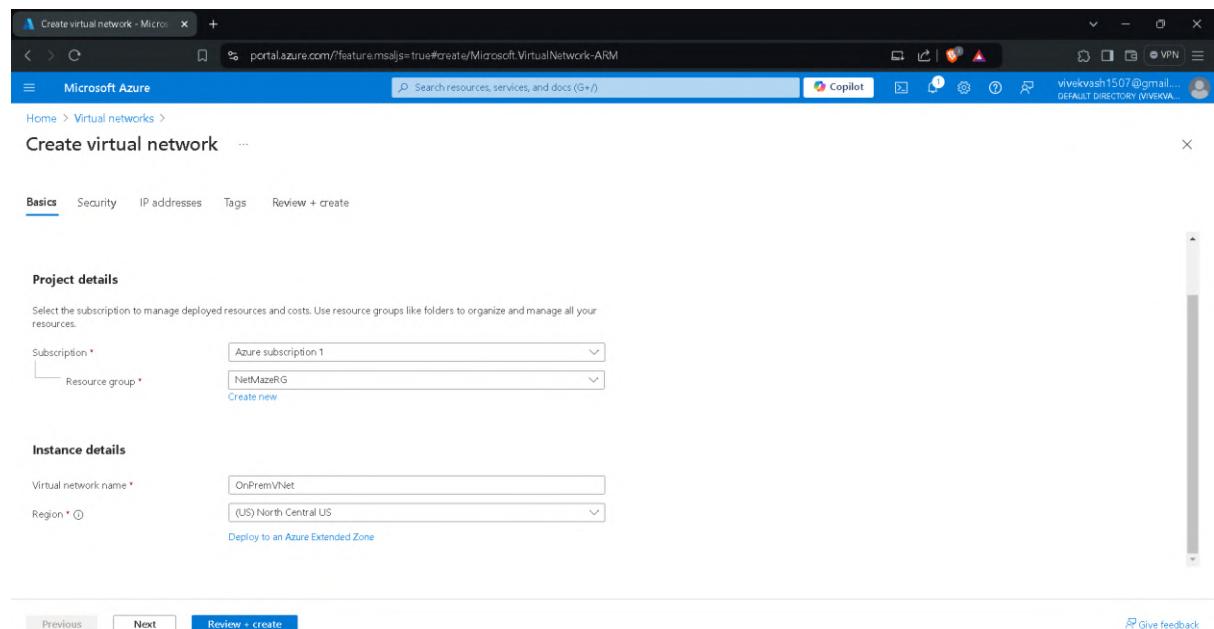
## 2.4. Finalizing the On-Premises VNet Setup

With the OnPremVNet and its subnets configured, I completed the setup process.

- Review and Deployment:
  - I reviewed the entire VNet configuration by clicking on Review + Create.
  - Finally, I clicked on Create to deploy the OnPremVNet.

In this section, I simulated an on-premises environment by creating a separate VNet in a different Azure region, configured with necessary subnets and a GatewaySubnet to support secure connections with the main Azure network in subsequent project phases.

## Screenshots



**Create virtual network - Microsoft Azure**

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space |

10.1.0.0/16

10.1.0.0 /16 65,536 addresses

10.1.0.0 - 10.1.255.255

+ Add a subnet

Subnets IP address range Size NAT gateway

Previous Next Review + create Give feedback

**Add a subnet - Microsoft Azure**

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space |

10.1.0.0/16

10.1.0.0 /16 65,536 addresses

10.1.0.0 - 10.1.255.255

+ Add a subnet

Subnets IP address range Size NAT gateway

**Add a subnet**

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose

Name \*

**IPv4**

Include an IPv4 address space

IPv4 address range \*

Starting address \*

Size

Subnet address range

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

**Private subnet** [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Add Cancel Give feedback

**Create virtual network - Microsoft Azure**

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks >

## Create virtual network

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space

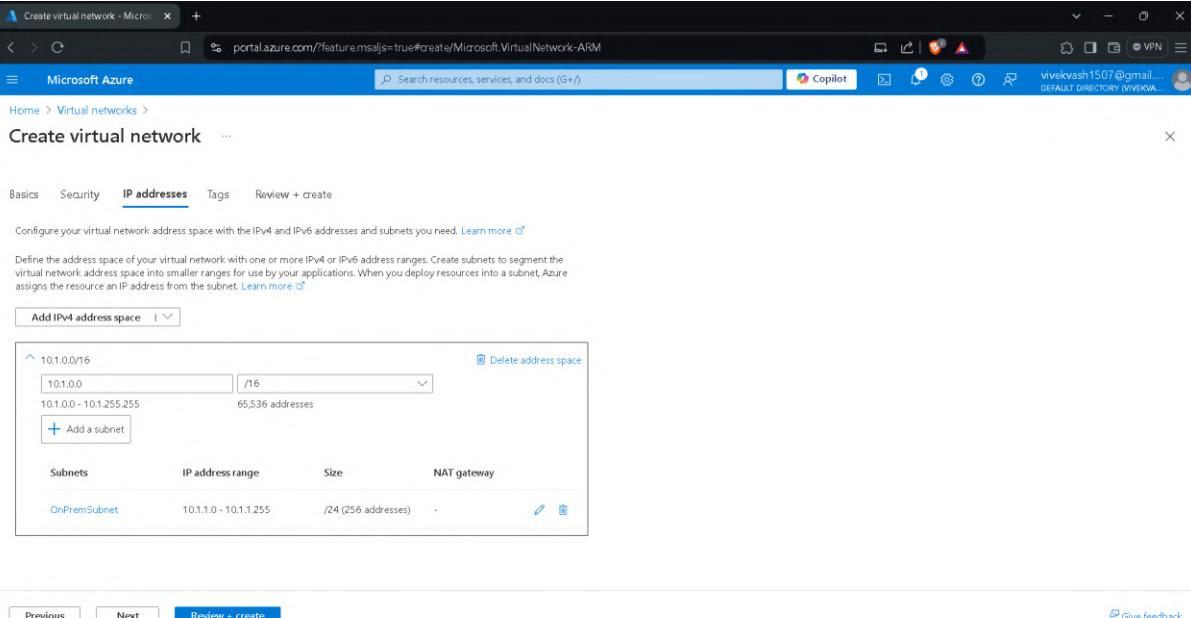
10.1.0.0/16

10.1.0.0 /16 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
OnPremSubnet	10.1.1.0 - 10.1.1.255	/24 (256 addresses)	-

Previous Next Review + create Give feedback



**OnPremVNet - Microsoft Azure**

portal.azure.com/?feature.msajs=true#@vivekvash1507@gmail.com.microsoft.com/resources/subscriptions/e9ea131-d6f1-4e0b-bae... | Copilot | Give feedback

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > OnPremVNet-1723873967232 | Overview >

## OnPremVNet

Virtual network

Search

Move Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Automation

Help

Essentials

Resource group (move) : NetMazeRG

Location (move) : North Central US

Subscription (move) : Azure subscription 1

Subscription ID : e9ea131-d6f1-4e0b-bae-b293615685ae

Address space : 10.1.0.0/16

DNS servers : Azure provided DNS service

Flow timeout : Configure

BGP community string : Configure

Virtual network ID : 0f19b461-1178-4ac6-b28f-84646826945d

JSON View

Topology Properties Capabilities (5) Recommendations Tutorials

DDoS protection

Configure additional protection from distributed denial of service attacks.

Not configured

Azure Firewall

Protect your network with a stateful L3-L7 firewall.

Not configured

Peerings

Seamlessly connect two or more virtual networks.

Not configured

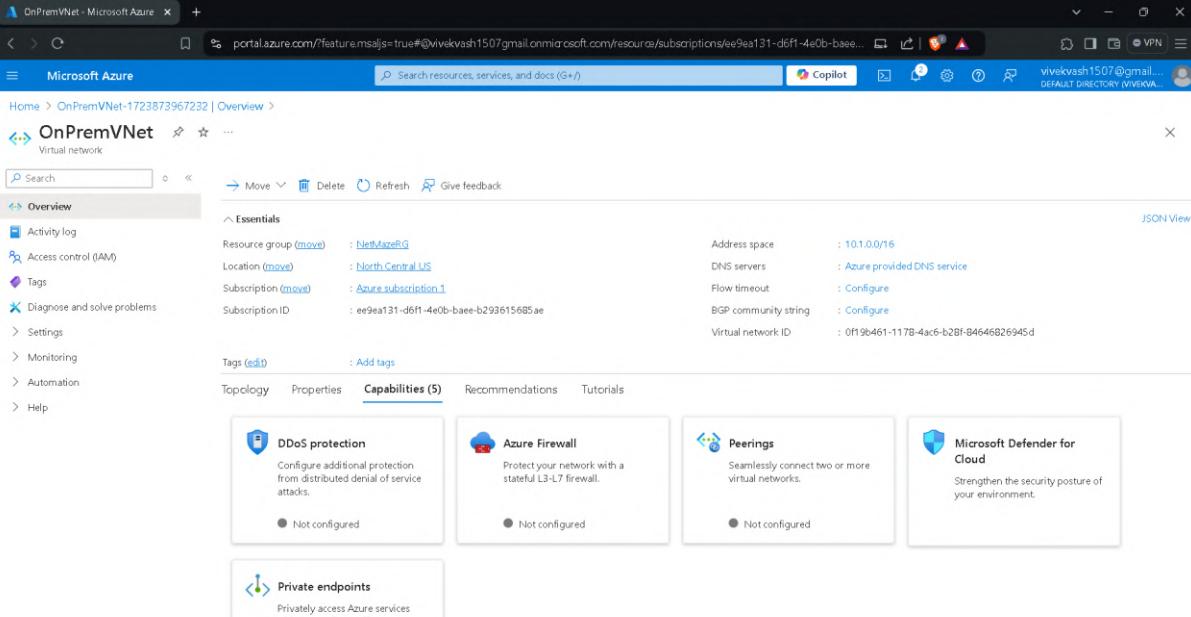
Microsoft Defender for Cloud

Strengthen the security posture of your environment.

Not configured

Private endpoints

Pivately access Azure services without sending traffic across internet



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation options like Home, Resource groups, and Subnets. The main area is titled 'OnPremVNet | Subnets'. On the right, a modal window titled 'Add a subnet' is open. Inside, it says 'Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later.' Below this, there's a section for 'Subnet purpose' set to 'Virtual Network Gateway'. The 'Name' field is filled with 'GatewaySubnet'. Under 'IPv4', there's a checked checkbox for 'Include an IPv4 address space' with a dropdown showing '10.1.0.0/16' and '10.1.0.0 - 10.1.255.255'. The 'Starting address' is set to '10.1.255.0' and the 'Size' is '/27 (32 addresses)'. The 'Subnet address range' is listed as '10.1.255.0 - 10.1.255.31'. There's also a note about private subnets: 'Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet.' At the bottom of the modal are 'Add' and 'Cancel' buttons.

## Secure Connectivity

### 3.1. Deploying the Azure VPN Gateway for NetMazeVNet

#### 3.1.1. Configuring the NetMazeVPNGateway

First, I needed to create a VPN gateway for the NetMazeVNet to establish secure connectivity.

- I logged into the Azure portal and navigated to the Virtual Network Gateway section.
- I clicked on + Create to start the gateway creation process.
- I entered the following details:
  - Name: NetMazeVPNGateway
  - Region: Canada Central
  - Gateway Type: VPN
  - VPN Type: Route-based
  - SKU: VpnGw1
  - Generation: Generation1
  - Virtual Network: NetMazeVNet
  - Subnet: GatewaySubnet (Automatically selected)
  - Public IP Address: Created a new public IP named NetMazeVPNPublicIP

- After filling in the details, I clicked on Review + Create, then selected Create to deploy the NetMazeVPNGateway.

## 3.2. Deploying the Azure VPN Gateway for OnPremVNet

### 3.2.1. Configuring the OnPremVPNGateway

Next, I configured a VPN gateway for the OnPremVNet to simulate the on-premises environment.

- I repeated the previous steps to create a VPN gateway.
- The configurations were as follows:
  - Name: OnPremVPNGateway
  - Region: North Central US
  - Gateway Type: VPN
  - VPN Type: Route-based
  - SKU: VpnGw1
  - Generation: Generation1
  - Virtual Network: OnPremVNet
  - Subnet: GatewaySubnet (Automatically selected)
  - Public IP Address: Created a new public IP named OnPremVPNPublicIP
- After reviewing the settings, I clicked on Review + Create and then selected Create to deploy the OnPremVPNGateway.

## 3.3. Configuring Local Network Gateways

### 3.3.1. Creating OnPremLocalGateway

To enable communication between the two networks, I set up a local network gateway for the on-premises environment.

- I navigated to the Local Network Gateways section in the Azure portal.
- I clicked on + Create to start the configuration process.
- I entered the following details:
  - Name: OnPremLocalGateway
  - Region: North Central US
  - Endpoint: IP Address
  - IP Address: 20.25.207.114 (Public IP of OnPremVPNGateway)
  - Address Space: 10.1.0.0/16 (Address space of OnPremVNet)
- After finalizing the details, I clicked on Review + Create, then selected Create to deploy the OnPremLocalGateway.

### 3.3.2. Creating NetMazeLocalGateway

Similarly, I set up a local network gateway for the Azure environment.

- I repeated the previous steps to create the local network gateway for NetMazeVNet.
- The configurations were as follows:
  - Name: NetMazeLocalGateway
  - Region: Canada Central
  - Endpoint: IP Address
  - IP Address: 52.233.62.7 (Public IP of NetMazeVPNGateway)
  - Address Space: 10.0.0.0/16 (Address space of NetMazeVNet)
- After finalizing the details, I clicked on Review + Create, then selected Create to deploy the NetMazeLocalGateway.

## 3.4. Establishing the Site-to-Site VPN Connection

### 3.4.1. Configuring the Connection from NetMazeVPNGateway

With both VPN gateways and local network gateways deployed, I established the site-to-site VPN connection.

- I navigated to the Connections tab under NetMazeVPNGateway and clicked on + Add.
- I entered the following configurations:
  - Name: NetMazeToOnPrem
  - Connection Type: Site-to-site (IPsec)
  - Virtual Network Gateway: NetMazeVPNGateway
  - Local Network Gateway: OnPremLocalGateway
  - Shared Key (PSK): xyz (same key used for both connections)
- After reviewing the details, I clicked on Create to establish the connection.

### 3.4.2. Configuring the Connection from OnPremVPNGateway

I repeated the same process to create a connection from OnPremVPNGateway.

- I navigated to the Connections tab under OnPremVPNGateway and clicked on + Add.
- The configurations were as follows:
  - Name: OnPremToNetMaze
  - Connection Type: Site-to-site (IPsec)
  - Virtual Network Gateway: OnPremVPNGateway
  - Local Network Gateway: NetMazeLocalGateway

- Shared Key (PSK): xyz (same key used previously)
- After reviewing the details, I clicked on Create to establish the connection.

## 3.5. Verifying the VPN Connection

### 3.5.1. Checking the Connection Status

After establishing the VPN connections, I verified the connection status to ensure both VNets were connected.

- I navigated to the Connections tab under both NetMazeVPNGateway and OnPremVPNGateway.
- I confirmed that the connections NetMazeToOnPrem and OnPremToNetMaze showed the status Connected.

## 3.6. Testing Connectivity

### 3.6.1. Creating Test VMs for Connectivity Check

To ensure communication between the two VNets, I created virtual machines in each VNet.

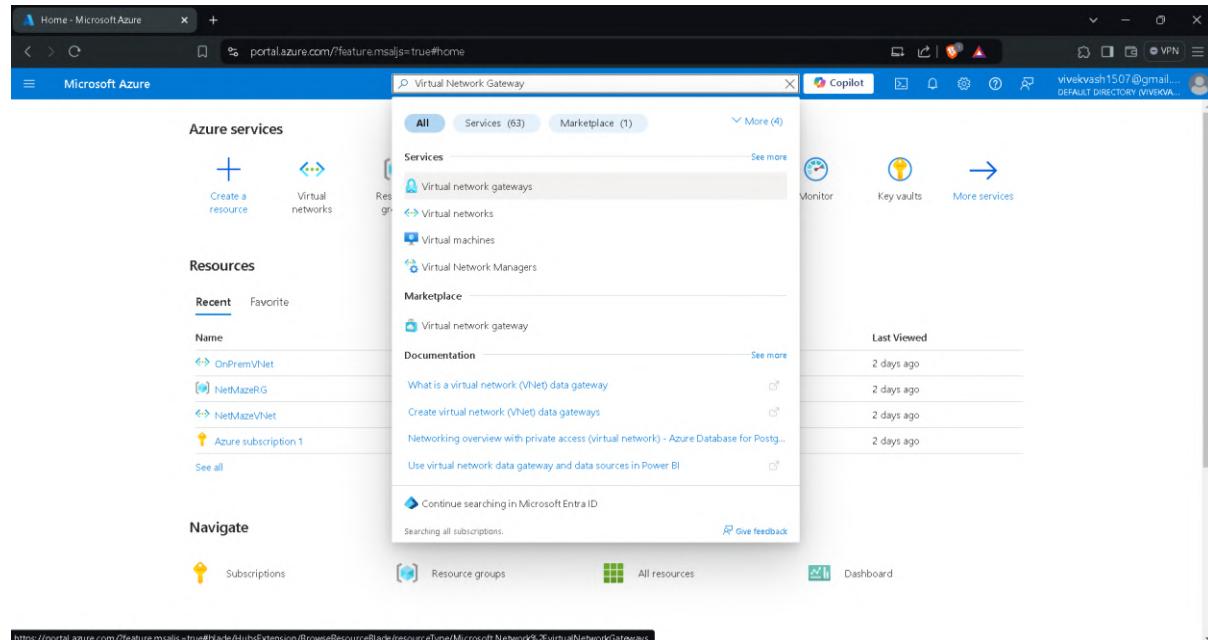
- NetMazeVM:
  - Resource Group: NetMazeRG
  - Location: Canada Central
  - Virtual Network: NetMazeVnet/WebAppSubnet
  - Operating System: Windows
  - Public IP: 20.48.180.245
  - Private IP: 10.0.1.4
- OnPremVM:
  - Resource Group: NetMazeRG
  - Location: North Central US
  - Virtual Network: OnPremVNet/OnPremSubnet
  - Operating System: Windows
  - Public IP: 135.224.21.205
  - Private IP: 10.1.1.4

### 3.6.2. Conducting Ping Test Between VMs

- Ping Test:
  - I used RDP to connect to both VMs and opened CMD in each.
  - Ping 1: From OnPremVM to NetMazeVM (IP: 10.0.1.4)
  - Ping 2: From NetMazeVM to OnPremVM (IP: 10.1.1.4)
  - Both pings were successful, confirming connectivity between the VNets.

In this section, I successfully established a secure site-to-site VPN connection between the simulated on-premises environment and Azure. This involved deploying VPN gateways, configuring local network gateways, and testing connectivity using virtual machines.

## Screenshots



**Create virtual network gateway**

**Basics** Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Azure subscription 1

Resource group NetMazeRG (derived from virtual network's resource group)

**Instance details**

Name \* NetMazeVPNGateway

Region \* Canada Central Deploy to an Azure Extended Zone

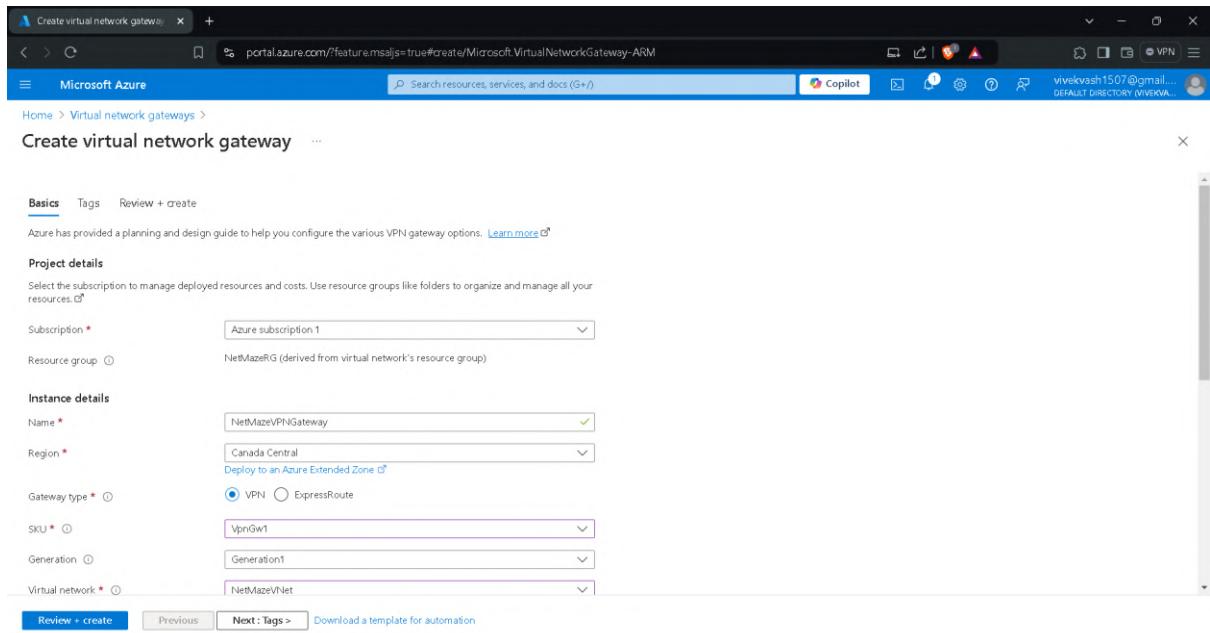
Gateway type \*  VPN  ExpressRoute

SKU \* VpnGw1

Generation Generation1

Virtual network \* NetMazeVNet

**Review + create** **Previous** **Next: Tags >** Download a template for automation



**Create virtual network gateway**

**Virtual network \*** NetMazeVNet Create virtual network

**Subnet** GatewaySubnet (10.0.255.0/27)

Only virtual networks in the currently selected subscription and region are listed.

**Public IP address**

Public IP address \*  Create new  Use existing

Public IP address name \* NetMazeVPNPublicIP

Public IP address SKU Standard

Assignment  Dynamic  Static

Enable active-active mode \*  Enabled  Disabled

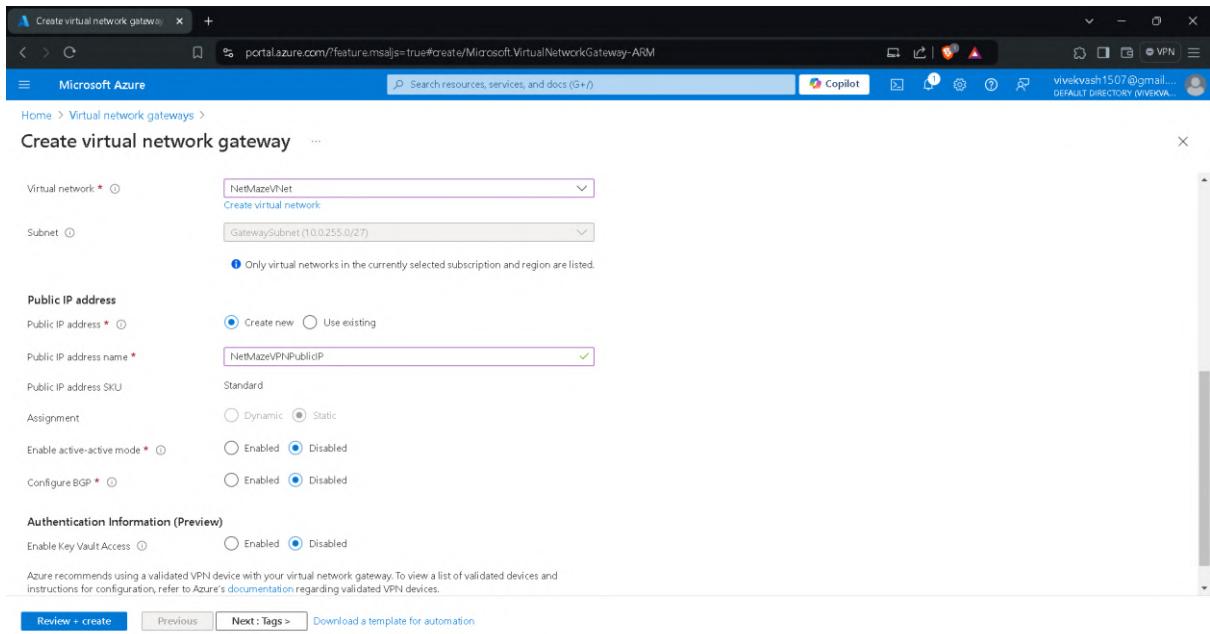
Configure BGP \*  Enabled  Disabled

**Authentication Information (Preview)**

Enable Key Vault Access  Enabled  Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

**Review + create** **Previous** **Next: Tags >** Download a template for automation



A Create virtual network gateway

portal.azure.com/?feature.msaljs=true#create/Microsoft.VirtualNetworkGateway-Azure

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual network gateways >

### Create virtual network gateway

Validation passed

Basics Tags Review + create

**Basics**

Subscription	Azure subscription 1
Resource group	NetMazeRG
Name	NetMazeVPNGateway
Region	Canada Central
SKU	VpnGw1
Generation	Generation1
Virtual network	NetMazeVNet
Subnet	GatewaySubnet (10.0.255.0/27)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	NetMazeVPNPublicIP

**Tags**

Create Previous Next Download a template for automation

NetMazeVPNGateway - Microsoft Azure

portal.azure.com/?feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e69ea131-d6f1-4e0b-bae... Copilot

Microsoft Azure

Search resources, services, and docs (G+)

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Microsoft.VirtualNetworkGateway-202408182946 | Overview >

### NetMazeVPNGateway

Virtual network gateway

Overview Refresh Move Delete

**Essentials**

Resource group (move) : NetMazeRG	SKU : VpnGw1
Location : Canada Central	Gateway type : VPN
Subscription (move) : Azure subscription 1	VPN type : Route-based
Subscription ID : e69ea131-d6f1-4e0b-bae-b293615685ae	Virtual network : NetMazeVNet
Tags (edit) : Add tags	Public IP address : 52.233.62.7 (NetMazeVPNPublicIP)

**Health check**  
Perform a quick health check to detect possible gateway issues  
[Go to Resource health](#)

**Advisor Recommendations**  
Check Critical, Warning, and Informational Recommendations  
[Go to Advisor](#)

**Documentation**  
View guidance on helpful topics related to VPN gateway  
[View documentation](#)

Show data for last 1 hour 6 hours 12 hours 1 day 7 days 30 days

Total tunnel ingress

100B  
90B  
80B  
70B

Total tunnel egress

100B  
90B  
80B  
70B

NetMazeVPNGateway - Microsoft Azure

portal.azure.com/?feature-msaljs=true#vivekvash1507@gmail.onmicrosoft.com/resource/subscriptions/ee9ea131-d6f1-... Copilot

Microsoft Azure

Virtual network gateway

NetMazeVPNGateway

Virtual network gateway

Overview

Essentials

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Connections

Point-to-site configuration

Maintenance

Properties

Locks

Monitoring

Automation

Help

Health check

Perform a quick health check of gateway issues

Go to Resource health

Show data for last 1 hour

Total tunnel ingress

100B

90B

80B

70B

All Services (63) Marketplace (1) More (4)

Virtual network gateways

Virtual networks

Virtual machines

Virtual Network Managers

Marketplace

Virtual network gateway

Documentation

What is a virtual network (VNet) data gateway?

Create virtual network (VNet) data gateways

Networking overview with private access (virtual network) - Azure Database for PostgreSQL

Use virtual network data gateway and data sources in Power BI

Continue searching in Microsoft Entra ID

Give feedback

JSON View

VpnGw1

VPN

Route-based

NetMazeVNet

52.233.62.7 (NetMazeVPNPublicIP)

Documentation

View guidance on helpful topics related to VPN gateway

View documentation

https://portal.azure.com/?feature-msaljs=true#blade/HubsExtension/BrowseResourceBlade/res...

Create virtual network gateway - Microsoft Azure

portal.azure.com/?feature-msaljs=true#create/Microsoft.VirtualNetworkGateway-ARM Copilot

Search resources, services, and docs (G+)

Home > Virtual network gateways >

Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Azure subscription 1

Resource group NetMazeRG (derived from virtual network's resource group)

**Instance details**

Name \* OnPremVPNGateway

Region \* North Central US Deploy to an Azure Extended Zone

Gateway type \*  VPN  ExpressRoute

SKU \* VpnGw1

Generation Generation1

Virtual network \* OnPremVNet

Review + create Previous Next: Tags > Download a template for automation

Create virtual network gateway

Virtual network \*

Subnet

Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address \*  Create new  Use existing

Public IP address name \*

Public IP address SKU Standard

Assignment  Dynamic  Static

Enable active-active mode \*  Enabled  Disabled

Configure BGP \*  Enabled  Disabled

Authentication Information (Preview)

Enable Key Vault Access  Enabled  Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

Validation passed

Basics Tags Review + create

**Basics**

Subscription	Azure subscription 1
Resource group	NetMazeRG
Name	OnPremVPNGateway
Region	North Central US
SKU	VpnGw1
Generation	Generation1
Virtual network	OnPremVNet
Subnet	GatewaySubnet(10.1.255.0/27)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	OnPremVPNPublicIP

**Tags**

None

OnPremVPN Gateway - Microsoft Azure

portal.azure.com/?feature-msaljs=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e99ea131-d6f1-4e0b-bae... Copilot

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

vivekvash1507@gmail.com DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual network gateways >

## OnPremVPNGateway

Virtual network gateway

Overview Refresh Move Delete

Resource group (move) : NetMazeRG  
Location : North Central US  
Subscription (move) : Azure subscription 1  
Subscription ID : ee9ea131-d6f1-4e0b-bae...  
SKU : VpnGw1  
Gateway type : VPN  
VPN type : Route-based  
Virtual network : OnPremVNet  
Public IP address : 20.25.207.114 (OnPremVNetPublicIP)

Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Configuration Connections Point-to-site configuration Maintenance Properties Locks Monitoring Automation Help

Tags (edit) : Add tags

Health check Advisor Recommendations Documentation

Total tunnel ingress Total tunnel egress

Show data for last 1 hour 6 hours 12 hours 1 day 7 days 30 days

1008 1008  
908 908  
808 808  
700 700

Local network gateways - Microsoft Azure

portal.azure.com/?feature-msaljs=true#browse/Microsoft.Network%2Flocalnetworkgateways Copilot

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

vivekvash1507@gmail.com DEFAULT DIRECTORY (VIVEKVA...)

Home >

## Local network gateways

Create Manage view Refresh Export to CSV Open query Assign tags

Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 1 of 1 records.

Name	Resource group	Location	Subscription
OnPremLocalGateway	NetMazeRG	North Central US	Azure subscription 1

< Previous Page 1 of 1 Next > Give feedback

Create local network gateway

portal.azure.com/?feature.msaljs=true#create/Microsoft.LocalNetworkGateway-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (VIVEKVA...)

Home > Local network gateways >

## Create local network gateway

Basics Advanced Review + create

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. [Learn more](#)

**Project details**

Subscription \* Azure subscription 1  
Resource group \* NetMazeRG  
Create new

**Instance details**

Region \* Canada Central  
Name \* NetMazeLocalGateway  
Endpoint (IP address FQDN)  
IP address \* 52.233.62.7  
Address Space(s) 10.0.0.0/16  
Add additional address range

Review + create Previous Next : Advanced >

Create local network gateway

portal.azure.com/?feature.msaljs=true#create/Microsoft.LocalNetworkGateway-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (VIVEKVA...)

Home > Local network gateways >

## Create local network gateway

Validation passed

Basics Advanced Review + create

**Summary**

Name	NetMazeLocalGateway
Subscription	Azure subscription 1
Resource group	NetMazeRG
Region	Canada Central
Endpoint	IP address
IP address	52.233.62.7
Address Space(s)	10.0.0.0/16

Create Previous Next

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (MIVERKA...)

Home > LocalNetworkGatewayCreate-20240819162451 | Overview >

**NetMazeLocalGateway** Local network gateway

Search

Move Delete

Overview Essentials

Activity log Access control (IAM) Tags Settings Configuration Connections Properties Locks Automation Help

Resource group (move) : NetMazeRG Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae6-b293615685ae IP address : 52.233.62.7 Address Space(s) : 10.0.0.0/16 Tags (edit) : Add tags JSON View

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'OnPremLocalGateway - Microsoft' tab, a search bar, and various icons like Copilot, Home, and Help. The main content area is titled 'Microsoft Azure' and shows the 'Local network gateways' section. A breadcrumb trail indicates the path: 'Home > Local network gateways >'. The central focus is the 'OnPremLocalGateway' resource, which is a 'Local network gateway'. The 'Overview' tab is selected, displaying the following details:

- Resource group:** NetMazeRG
- Location:** North Central US
- Subscription:** Azure subscription 1
- Subscription ID:** ee9ea131-d6f1-4e0b-baee-b293615685ae
- IP address:** 20.25.207.114
- Address Space(s):** 10.1.0.0/16

The left sidebar contains a navigation menu with the following items:

- Activity log
- Access control (IAM)
- Tags
- Configuration
- Connections
- Properties
- Locks
- Automation
- Help

OnPremLocalGateway - Microsoft Edge

portal.azure.com/?feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e9ea131-d6f1-4e0b-bae...

Microsoft Azure

Home > Local network gateways > OnPremLocalGateway

## OnPremLocalGateway | Configuration

Local network gateway

Search Save Discard

Overview

Activity log

Access control (IAM)

Tags

Configuration

IP address \* 2025.207.114

Address Space(s) 10.1.0.0/16

Add additional address range

Connections

Properties

Locks

BGP Settings

Configure BGP settings Yes No

Automation

Help

NetMazeVPNGateway - Microsoft Edge

portal.azure.com/?feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e9ea131-d6f1-4e0b-bae...

Microsoft Azure

Home > Virtual network gateways > NetMazeVPNGateway

## NetMazeVPNGateway | Connections

Virtual network gateway

+ Create Manage view ...

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Connections

Point-to-site configuration

Maintenance

Properties

Locks

Monitoring

Automation

Help

Name	Status	Connection type	Peer
NetMazeToOnPrem	Connected	Site-to-site (IPsec)	OnPremLocalGateway

Page 1 of 1

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Edge logo, the title 'NetMazeToOnPrem - Microsoft Edge', the address bar with the URL 'portal.azure.com/?feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resource/subscriptions/e9ea131-df1-4e0b-baa...', and various browser icons. The main header bar has the Microsoft Azure logo, a search bar with the placeholder 'Search resources, services, and docs (G+)', and account information for 'vivekvash1507@gmail...' and 'DEFAULT DIRECTORY (NIVEKVA...)'. Below the header, the breadcrumb navigation shows 'Home > Virtual network gateways > NetMazeVPNGateway | Connections > NetMazeToOnPrem'. The left sidebar contains a tree view with 'Connection' selected at the top, followed by 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Settings' (expanded), 'Authentication', 'Configuration', 'NAT Rules', 'Properties', and 'Locks'. Under 'Monitoring', 'Automation', and 'Help' are also listed. The main content area displays the 'NetMazeToOnPrem' connection details under the 'Essentials' tab. It shows the following information:

Setting	Value
Resource group (move)	: NetMazeRG
Status	: Connected
Location	: Canada Central
Subscription (move)	: Azure subscription 1
Subscription ID	: e9ea131-df1-4e0b-baae-b2936156b5ae
Tags (edit)	: Add tags
Data in	: 0 B
Data out	: 0 B
Virtual network	: NetMazeVNet
Virtual network gateway	: NetMazeVPNGateway
Local network gateway	: OnPremLocalGateway(2025.207.111)

At the bottom right of the content area, there is a 'JSON View' link.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar has a tab for 'OnPremVPNGateway - Microsoft' and a search bar with placeholder text 'Search resources, services, and docs (G+...)'. A 'Copilot' button is also visible. The main content area is titled 'Virtual network gateway' and shows a list of gateways: 'NetMazeVPNGateway' and 'OnPremVPNGateway'. The 'OnPremVPNGateway' card is selected, displaying its 'Connections' page. The title bar for this page is 'OnPremVPNGateway | Connections'. The left sidebar for 'Connections' includes options like 'Point-to-site configuration', 'Maintenance', 'Properties', 'Locks', 'Monitoring', 'Automation', and 'Help'. The main content area shows a table of connections:

Name	Status	Connection type	Peer
OnPremToNetMaze	Connected	Site-to-site (IPsec)	NetMazeLocalGateway

**OnPremToNetMaze - Microsoft Azure**

Home > Virtual network gateways > OnPremVPNGateway | Connections >

**OnPremToNetMaze** Connection

Search Refresh Move Download configuration Delete

**Overview**

Resource group (move) : NetMazeRG  
Status : Connected  
Location : North Central US  
Subscription (move) : Azure subscription 1  
Subscription ID : ee9ea131-d6f1-4e0b-baee-b293615685ae  
Tags (edit) : Add tags

Data in : 0 B  
Data out : 0 B  
Virtual network : OnPremVNet  
Virtual network gateway : OnPremVPNGateway  
Local network gateway : NetMazeLocalGateway (52.233.62.7)

JSON View

Activity log  
Access control (IAM)  
Tags  
Settings  
Authentication  
Configuration  
NAT Rules  
Properties  
Locks  
Monitoring  
Automation  
Help

**NetMazeVM - Microsoft Azure**

Home >

**NetMazeVM** Virtual machine

Search Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

**Overview**

Resource group (move) : NetMazeRG  
Status : Running  
Location : Canada Central  
Subscription (move) : Azure subscription 1  
Subscription ID : ee9ea131-d6f1-4e0b-baee-b293615685ae

Operating system : Windows  
Size : Standard B1s (1 vcpu, 1 GiB memory)  
Public IP address : 204.81.80.245  
Virtual network/subnet : NetMazeVNet/WebAppSubnet  
DNS name : Not configured  
Health state : OK  
Time created : 8/19/2024, 11:10 PM UTC

Tags (edit) : Add tags

**Properties** Monitoring Capabilities (8) Recommendations Tutorials

**Virtual machine**

Computer name	NetMazeVM
Operating system	Windows
VM generation	V2
VM architecture	x64
Agent status	Not Ready

**Networking**

Public IP address	204.81.80.245 (Network interface netmazevm214)
Public IP address (IPv6)	-
Private IP address	10.0.1.4
Private IP address (IPv6)	-
Virtual network/subnet	NetMazeVNet/WebAppSubnet

**OnPremVM - Microsoft Azure**

Microsoft Azure | portal.azure.com/?feature.msaljs=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-4e0b-bae...

Home > OnPremVM

**Overview**

Search

Connect Start Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

**OnPremVM virtual machine agent status is not ready. Troubleshoot the issue →**

**Essentials**

Resource group: NetMazeRG  
Status: Running  
Location: North\_Central\_US  
Subscription: Azure subscription 1  
Subscription ID: ee9ea131-d6f1-4e0b-bae...  
Operating system: Windows  
Size: Standard\_B1s (1 vcpu, 1 GiB memory)  
Public IP address: 135.224.21.205  
Virtual network/subnet: OnPremVNet/OnPremSubnet  
DNS name: Not configured  
Health state: -  
Time created: 8/19/2024, 11:16 PM UTC

**Tags (edit) Add tags**

**Properties** Monitoring Capabilities (8) Recommendations Tutorials

**Virtual machine**

Computer name	OnPremVM	Public IP address	135.224.21.205 (Network interface onpremvm473)
Operating system	Windows	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.1.1.4
VM architecture	x64	Private IP address (IPv6)	-
Agent status	Not Ready	Virtual network/subnet	OnPremVNet/OnPremSubnet

**Networking**

Public IP address	135.224.21.205 (Network interface onpremvm473)
Public IP address (IPv6)	-
Private IP address	10.1.1.4
Private IP address (IPv6)	-
Virtual network/subnet	OnPremVNet/OnPremSubnet

**Virtual machines - Microsoft Azure**

Microsoft Azure | portal.azure.com/?feature.msaljs=true#view/HubsExtension/BrowseResource/resourceType/Microsoft.Compute%2FVirtualMa...

Home > Virtual machines

**Virtual machines**

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Switch to classic Reservations Manage view Refresh Export to CSV Open query Assign tags Start Stop Delete Services Maintenance

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

No grouping List view

Showing 1 to 2 of 2 records.

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
NetMazeVM	Azure subscription 1	NetMazeRG	Canada Central	Running	Windows	Standard_B1s	20.48.180.245	1
OnPremVM	Azure subscription 1	NetMazeRG	North_Central_US	Running	Windows	Standard_B1s	135.224.21.205	1

**OnPremVM (1) - 135.224.21.205:3389 - Remote Desktop Connection**

Administrator: Command Prompt

```
C:\Users\vashisht.vivek>ping 10.0.1.4

Pinging 10.0.1.4 with 32 bytes of data:
Reply from 10.0.1.4: bytes=32 time=18ms TTL=128
Reply from 10.0.1.4: bytes=32 time=18ms TTL=128
Reply from 10.0.1.4: bytes=32 time=18ms TTL=128
MicroLoopReply from 10.0.1.4: bytes=32 time=18ms TTL=128
Edge

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 19ms, Average = 18ms

C:\Users\vashisht.vivek>
```

**NetMazeVM - 20.48.180.245:3389 - Remote Desktop Connection**

Administrator: Command Prompt

```
C:\Users\vivek.vashisht>ping 10.1.1.4

Pinging 10.1.1.4 with 32 bytes of data:
Reply from 10.1.1.4: bytes=32 time=18ms TTL=128

Ping statistics for 10.1.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 18ms, Average = 18ms

C:\Users\vivek.vashisht>
```

# **Resource Deployment**

## 4.1. Deploying the WebAppVM

### 4.1.1. Configuring the WebAppVM

The first step in resource deployment was to create a virtual machine for the web application in the WebAppSubnet.

- I logged into the Azure portal and navigated to the Virtual Machines section.
- I clicked on + Create to start the VM creation process.
- I entered the following details:
  - Name: WebAppVM
  - Resource Group: NetMazeRG
  - Region: Canada Central
  - Availability Options: No infrastructure redundancy required
  - Security Type: Standard
  - Image: Windows Server 2019 Datacenter-Gen2
  - VM Architecture: x64
  - Size: Standard B1s (1 vCPU, 1 GiB memory)
  - Username: webuser
  - Public Inbound Ports: RDP
  - OS Disk Type: Standard SSD LRS
  - Virtual Network: NetMazeVNet
  - Subnet: WebAppSubnet (10.0.1.0/24)
  - Public IP: Created a new public IP named WebAppVM-ip
- After entering the necessary details, I clicked on Review + Create, then selected Create to deploy the WebAppVM.

### 4.1.2. Configuring Web Server (IIS)

Once the WebAppVM was deployed, I configured it to act as a web server.

- I used RDP to connect to the WebAppVM using the public IP address WebAppVM-ip.
- In the Server Manager, I clicked on Add roles and features and selected Web Server (IIS) to install.
- After the installation was complete, I opened Internet Explorer on the WebAppVM and entered <http://localhost/> in the address bar to verify the server's functionality.

#### 4.1.3. Configuring Inbound Security Rules

To ensure the web server was accessible externally, I adjusted the security rules.

- I added an inbound security rule to the WebAppVM-nsg (attached to the NIC of WebAppVM) with the following settings:
  - Source: Any
  - Source Port Ranges: \*
  - Destination: Any
  - Service: HTTP
  - Destination Port Ranges: 80
  - Protocol: TCP
  - Action: Allow
- I also added the same inbound rule in the Windows Defender Firewall with Advanced Security on the WebAppVM.
- Finally, I tested the configuration by accessing the web server using the WebAppVM-ip in both Internet Explorer (WebAppVM) and Brave Browser (local machine). The web server was running successfully.

### 4.2. Deploying the DatabaseVM

#### 4.2.1. Configuring the DatabaseVM

Next, I created a virtual machine for the database in the DatabaseSubnet.

- I returned to the Virtual Machines section and started the creation process for the DatabaseVM.
- The configurations were as follows:
  - Name: DatabaseVM
  - Resource Group: NetMazeRG
  - Region: Canada Central
  - Availability Options: No infrastructure redundancy required
  - Security Type: Standard
  - Image: Ubuntu Server 22.04 LTS - Gen2
  - VM Architecture: x64
  - Size: Standard B1s (1 vCPU, 1 GiB memory)
  - Authentication Type: SSH Public Key
  - Username: databaseuser
  - OS Disk Type: Standard SSD LRS
  - Virtual Network: NetMazeVNet
  - Subnet: DatabaseSubnet (10.0.2.0/24)
  - Public IP: None
  - NIC Network Security Group: Created a new NSG named DatabaseVM-nsg
- I reviewed and created the DatabaseVM.

#### 4.2.2. Installing MySQL Server

After deploying the DatabaseVM, I installed MySQL Server to manage the database.

- I used the SSH using CLI option in the Azure portal to connect to the DatabaseVM.
- I ran the following commands to update the package lists and install MySQL Server:

```
bash
Copy code
sudo apt update
sudo apt install mysql-server -y
sudo systemctl start mysql
sudo systemctl enable mysql
sudo mysql_secure_installation
```

- To verify the installation, I accessed the MySQL monitor using the command:

```
bash
Copy code
sudo mysql -u root -p
```

- I entered the password and executed the command SHOW DATABASES; to view the default databases.

#### 4.3. Deploying the AdminVM

##### 4.3.1. Configuring the AdminVM

The final virtual machine I deployed was for administrative tasks in the AdminSubnet.

- I initiated the creation of the AdminVM with the following configurations:
  - Name: AdminVM
  - Resource Group: NetMazeRG
  - Region: Canada Central
  - Availability Options: No infrastructure redundancy required
  - Security Type: Standard
  - Image: Windows Server 2019 Datacenter-Gen2
  - VM Architecture: x64
  - Size: Standard B1s (1 vCPU, 1 GiB memory)
  - Username: AdminUser
  - Public Inbound Ports: RDP
  - OS Disk Type: Standard SSD LRS
  - Virtual Network: NetMazeVNet
  - Subnet: AdminSubnet (10.0.3.0/24)
  - Public IP: Created a new public IP named AdminVM-ip
- After reviewing the configurations, I clicked on Create to deploy the AdminVM.

#### 4.3.2. Installing Administrative Tools

Once the AdminVM was deployed, I installed various administrative tools and features.

- I used RDP to connect to the AdminVM using the public IP address AdminVM-ip.
- In the Server Manager, I clicked on Add roles and features and installed the following:
  - Failover Clustering
  - Group Policy Management
  - Remote Server Administration Tools
    - Feature Administration Tools
      - Failover Clustering Tools
        - Failover Cluster Management Tools
        - Failover Cluster Module for Windows PowerShell
      - Role Administration Tools
        - AD DS and AD LDS Tools
          - Active Directory module for Windows PowerShell
          - AD DS Tools
            - Active Directory Administrative Center
            - AD DS Snap-Ins and Command-Line Tools
          - AD LDS Snap-Ins and Command-Line Tools
        - DNS Server Tools
  - I also installed the Windows Admin Center from the official Microsoft website.

#### 4.3.3. Verifying Installations

After installing the necessary tools, I verified their installation.

- I accessed the various tools and features through the Tools section in the Server Manager.
- For the Windows Admin Center, I opened a browser and visited <https://AdminVM:443>. After entering the AdminVM credentials, I confirmed that the Windows Admin Center was successfully installed.

In this section, I successfully deployed three critical virtual machines—WebAppVM, DatabaseVM, and AdminVM—withing the NetMazeVNet. Each VM was configured with specific roles, and all installations were verified to ensure proper functionality.

## Screenshots

This screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. The current step is 'Basics'. The configuration includes:

- Subscription: Azure subscription 1
- Resource group: NetMazeRG
- Virtual machine name: WebAppVM
- Region: Canada Central
- Availability options: No infrastructure redundancy required
- Zone options: Self-selected zone
- Security type: Standard
- Image: Windows Server 2019 Datacenter - Gen2
- VM architecture: x64
- Size: Standard B1s (1 vcpu, 1 GB memory)
- Enable Hibernation: No
- Username: webuser
- Public inbound ports: RDP
- Already have a Windows license?: No
- Azure Spot: No

An estimated monthly cost of \$25.60/month is displayed on the right.

This screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. The current step is 'Disks'. The configuration includes:

- OS disk size: Image default
- OS disk type: Standard SSD LRS
- Use managed disks: Yes
- Delete OS disk with VM: Enabled
- Ephemeral OS disk: No

An estimated monthly cost of \$25.60/month is displayed on the right.

Create a virtual machine - Microsoft Azure

portal.azure.com/?feature.msals=true#create/Microsoft.VirtualMachine-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual machines >

## Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

**Management**

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

**Monitoring**

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

**Advanced**

< Previous Next > Create

Download a template for automation Give feedback

Estimated monthly cost  
\$25.60 / month

View cost details

This screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. It displays basic management settings like Microsoft Defender for Cloud (Basic free), system identity (Off), and auto-shutdown (Off). Monitoring options include alerts (Off) and boot diagnostics (Off). Advanced settings show extensions (None), VM applications (None), and disk controller type (SCSI). The estimated monthly cost is \$25.60 per month.

Create a virtual machine - Microsoft Azure

portal.azure.com/?feature.msals=true#create/Microsoft.VirtualMachine-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual machines >

## Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

**Management**

Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

**Monitoring**

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

**Advanced**

< Previous Next > Create

Download a template for automation Give feedback

Estimated monthly cost  
\$25.60 / month

View cost details

This screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. It displays basic management settings like enable hotpatch (Off) and patch orchestration (OS-orchestrated patching). Monitoring options include alerts (Off) and boot diagnostics (Off). Advanced settings show extensions (None), VM applications (None), and disk controller type (SCSI). The estimated monthly cost is \$25.60 per month.

Microsoft Azure

CreateVm-MicrosoftWindowsServer.WindowsServer-201-20240819191825 | Overview

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsServer-201-20240819191825  
Subscription: Azure subscription 1  
Resource group: NetMazeRG

Start time: 8/19/2024, 7:23:59 PM  
Correlation ID: d9be67ca-fd62-4e06-9ebb-c0d2f3f4ce9

Deployment details

Resource	Type	Status	Operation details
WebAppVM	Microsoft.Compute/virtualMachines	OK	Operation details
webappvm824	Microsoft.Network/networkInterfaces	Created	Operation details
WebAppVM-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details
WebAppVM-ip	Microsoft.Network/publicIPAddresses	OK	Operation details

Next steps

- Setup auto-shutdown: Recommended
- Monitor VM health, performance and network dependencies: Recommended
- Run a script inside the virtual machine: Recommended

Go to resource Create another VM

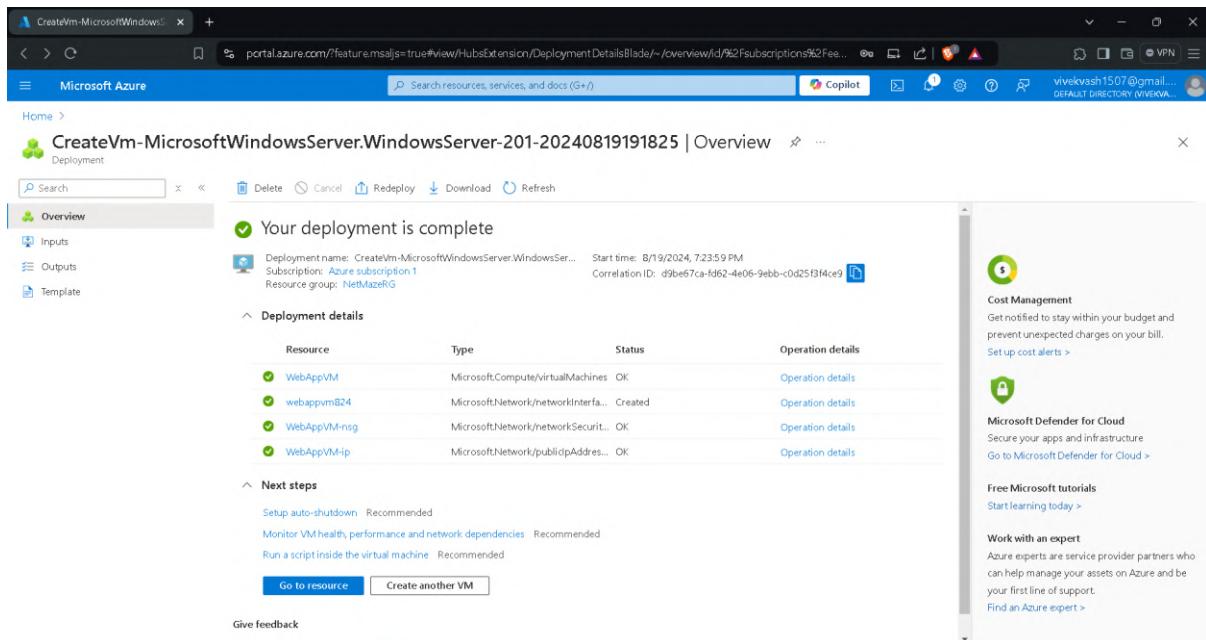
Give feedback

Cost Management

Microsoft Defender for Cloud

Free Microsoft tutorials

Work with an expert



Microsoft Azure

WebAppVM - Microsoft Azure

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Advisors (1 of 1): Enable Trusted Launch foundational excellence, and modern security for Existing Generation 2 VM(s) →

Essentials

Resource group (move): NetMazeRG	Operating system: Windows (Windows Server 2019 Datacenter)
Status: Running	Size: Standard B1s (1 vcpu, 1 GiB memory)
Location: Canada Central	Public IP address: 4.206.185.187
Subscription (move): Azure subscription 1	Virtual network/subnet: NetMazeVNet/WebAppSubnet
Subscription ID: ee9ea131-d6f1-4e0b-bae6-b293615685ae	DNS name: Not configured
	Health state: -
	Time created: 8/20/2024, 1:24 AM UTC

Tags (edit): Add tags

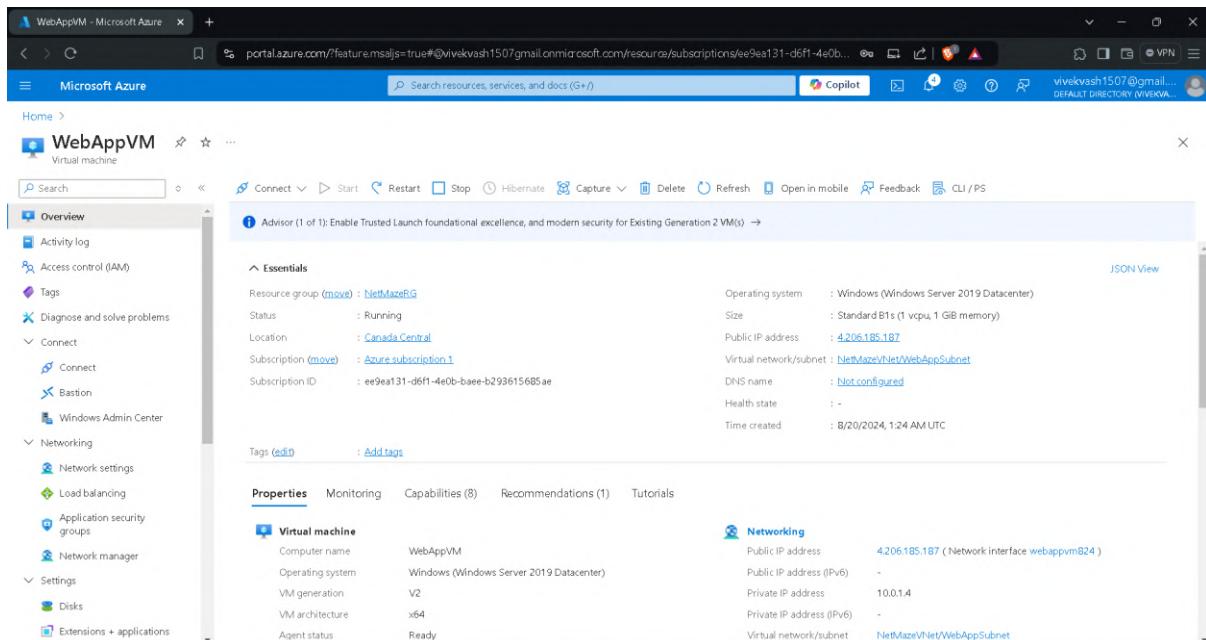
Properties

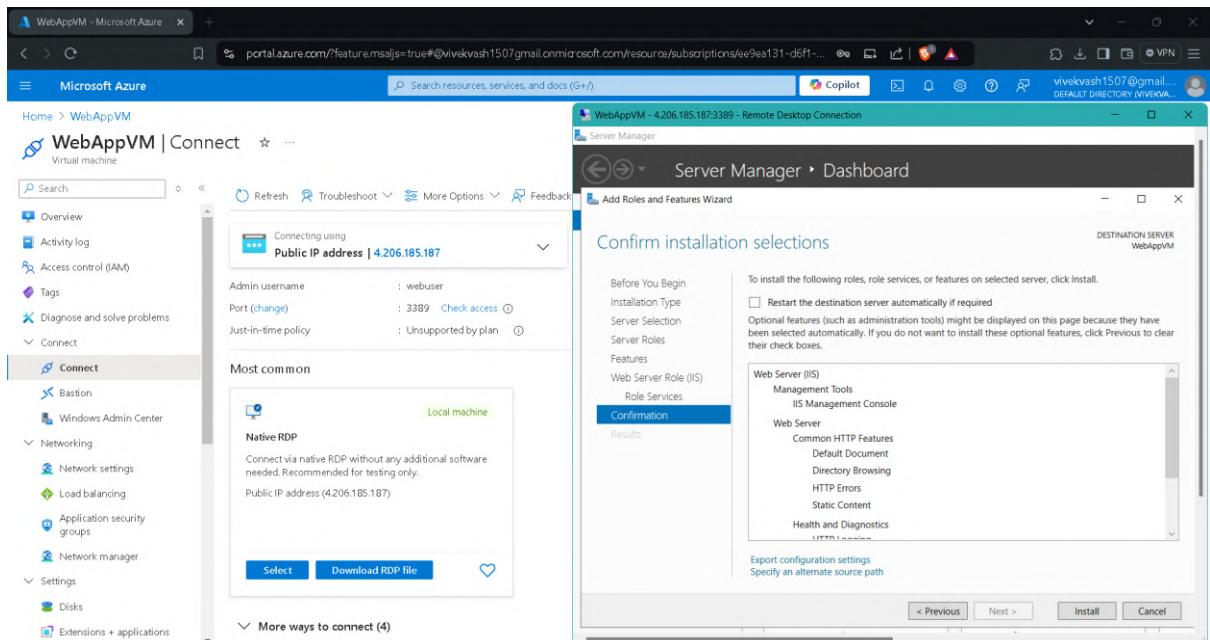
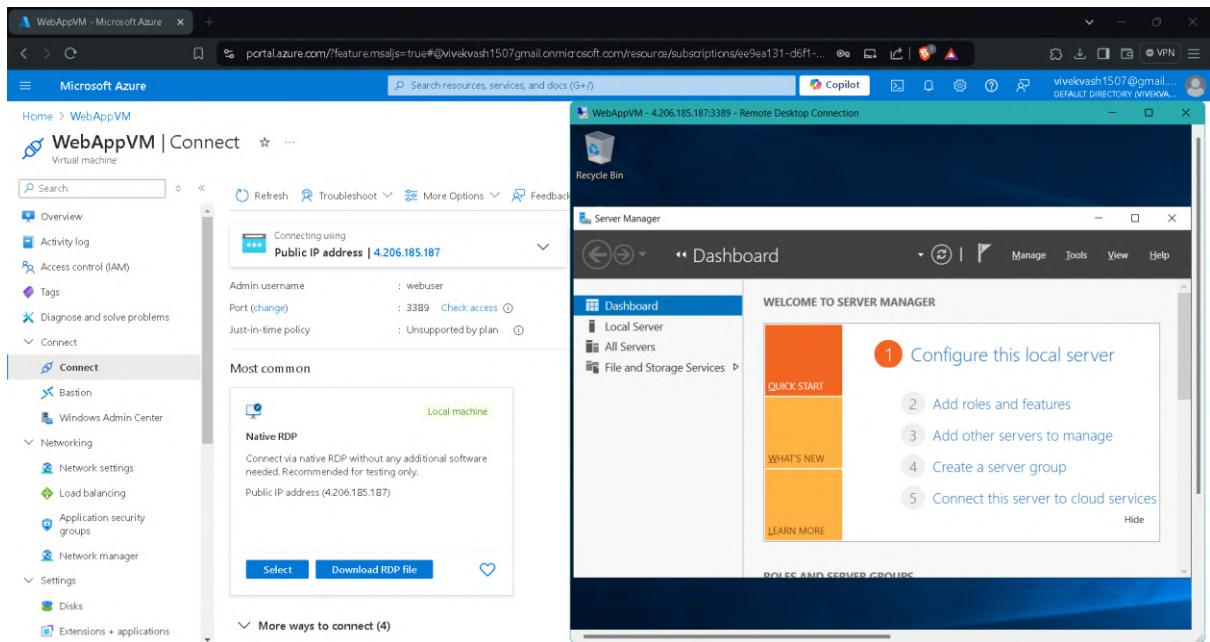
Virtual machine

Computer name: WebAppVM	Operating system: Windows (Windows Server 2019 Datacenter)
VM generation: V2	Private IP address: 10.0.1.4
VM architecture: x64	Private IP address (IPv6): -
Agent status: Ready	Virtual network/subnet: NetMazeVNet/WebAppSubnet

Networking

Public IP address: 4.206.185.187 (Network interface webappvm824)
Public IP address (IPv6): -
Private IP address: 10.0.1.4
Private IP address (IPv6): -





**WebAppVM | Connect**

Connecting using  
Public IP address | 4.206.185.187

Admin username: webuser  
Port (change): 3389 [Check access](#)  
Just-in-time policy: Unsupported by plan

Most common

Native RDP  
Connect via native RDP without any additional software needed. Recommended for testing only.  
Public IP address (4.206.185.187)

Select Download RDP file

**Server Manager - Dashboard**

**Add Roles and Features Wizard**

**Installation progress**

View installation progress

Feature installation  
Installation succeeded on WebAppVM.

Web Server (IIS)  
Management Tools  
IIS Management Console  
Web Server  
Common HTTP Features  
Default Document  
Directory Browsing  
HTTP Errors  
Static Content  
Health and Diagnostics  
HTTP Logging

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

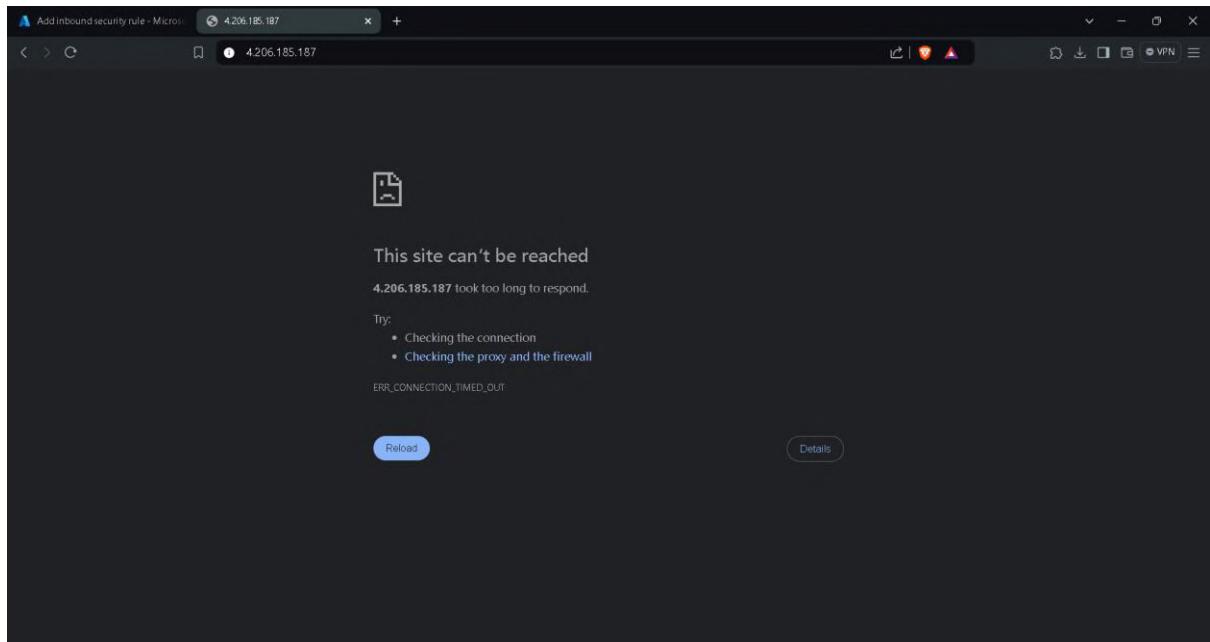
< Previous Next > Close Cancel

**Windows Server**

**Internet Information Services**

Welcome Bienvenue Tervetuloa ようこそ Benvenuto 歓迎 Bienvenido Hoş geldiniz กรונם הוגאים Bem-vindo Viteje 欢迎 Bienvenido Valkommen 환영합니다 Добро пожаловать Üdvözöljük

Microsoft Willkommen Velkommen Witamy



Microsoft Azure

Home > Virtual machines > WebAppVM

WebAppVM | Network settings

Rules

Network security group WebAppVM-nsg (attached to networkInterface: webappvmB24)

Inbound port rules (4)

Priority	Name	Port	Protocol
300	RDP	3389	TCP
65000	AllowWhitelisted	Any	Any
65001	AllowAzureLoadBalancerInbound	Any	Any
65500	DenyAllInbound	Any	Any

Outbound port rules (3)

Add Cancel

WebAppVM - Microsoft Azure | 4.206.185.187:3389 - Remote Desktop Connection

Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Ov...	Prog...	Local Ad...	Remote A...	Protocol	Local Port	Remot...	Authoriz...	Authorized Computer...
Allow HTTP	All	Yes	Allow	No	%Sys...	Any	Any	Any	TCP	80	Any	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%Sys...	Any	Any	TCP	9955	Any	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%Sys...	Any	Any	UDP	Any	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retri...	All	No	Allow	No	SYST...	Any	Any	TCP	80	Any	Any	Any
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache...	All	No	Allow	No	SYST...	Any	Any	TCP	80,443	Any	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discover...	All	No	Allow	No	%Sys...	Any	Local sub...	UDP	3702	Any	Any	Any
Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private...	Yes	Allow	No	%Sys...	Any	PlayTo Re...	TCP	2177	Any	Any	Any
Cast to Device functionality (qWave-UDP-In)	Cast to Device functionality	Private...	Yes	Allow	No	%Sys...	Any	PlayTo Re...	UDP	2177	Any	Any	Any
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%Sys...	Any	Any	UDP	PlayTo Disc...	Any	Any	Any
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	Syst...	Any	Any	TCP	10246	Any	Any	Any
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Public	Yes	Allow	No	Syst...	Any	PlayTo Re...	TCP	10246	Any	Any	Any
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Private	Yes	Allow	No	Syst...	Any	Local sub...	TCP	10246	Any	Any	Any
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%Sys...	Any	Local sub...	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%Sys...	Any	PlayTo Re...	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%Sys...	Any	Any	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%Sys...	Any	Local sub...	TCP	23554, 235...	Any	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%Sys...	Any	Any	TCP	23554, 235...	Any	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%Sys...	Any	PlayTo Re...	TCP	23554, 235...	Any	Any	Any
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	COM+ Network Access	All	No	Allow	No	%Sys...	Any	TCP	135	Any	Any	Any
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	No	%Sys...	Any	Any	TCP	RPC Dyna...	Any	Any	Any
COM+ Remote Administration (DCOM-In)	COM+ - Remote Administration	All	No	Allow	No	%Sys...	Any	Any	TCP	135	Any	Any	Any
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow	No	Syst...	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow	No	Syst...	Any	Any	ICMPv4	Any	Any	Any	Any
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%Sys...	Any	Any	UDP	67	Any	Any	Any
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%Sys...	Any	Any	UDP	546	547	Any	Any
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	Syst...	Any	Any	IGMP	Any	Any	Any	Any
Core Networking - IPIHTPS (TCP-In)	Core Networking	All	Yes	Allow	No	Syst...	Any	Any	TCP	IPIHTPS	Any	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	Syst...	Any	Any	IPv6	Any	Any	Any	Any
Core Networking - Multicast Listener Don...	Core Networking	All	Yes	Allow	No	Syst...	Any	Local sub...	ICMPv6	Any	Any	Any	Any

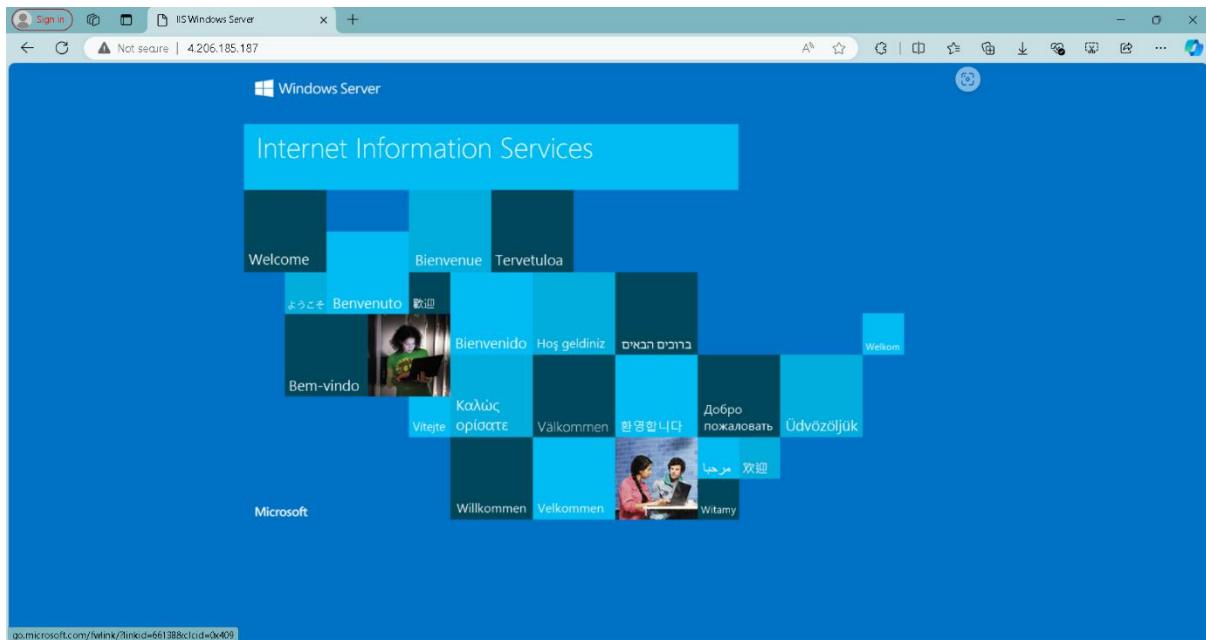
Actions

- New R...
- Filter -
- Filter -
- Filter -
- View
- Export...
- Help
- Allow HTTP
- Disable...
- Cut
- Copy
- Delete
- Proper...
- Help

WebAppVM - Microsoft Azure | 4.206.185.187 | portal.azure.com/?feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e69ea131-d6f1-...

IIS Windows Server | http://4.206.185.187/ | Search... | Microsoft | IIS Windows Server

## Internet Information Services



A screenshot of the Microsoft Azure portal interface. The top navigation bar shows "Create a virtual machine - Microsoft Azure" and the URL "portal.azure.com/?feature.msaljs=true#create/Microsoft.VirtualMachine-ARM". The main content area is titled "Create a virtual machine" and includes a "Validation passed" message. There are three buttons: "Help me create a low cost VM", "Help me create a VM optimized for high availability", and "Help me choose the right VM size for my workload". The "Basics" configuration section lists various parameters: Subscription (Azure subscription 1), Resource group (NetMazeRG), Virtual machine name (DatabaseVM), Region (Canada Central), Availability options (No infrastructure redundancy required), Zone options (Self-selected zone), Security type (Standard), Image (Ubuntu Server 22.04 LTS - Gen2), VM architecture (x64), Size (Standard B1s (1 vCPU, 1 GiB memory)), Enable Hibernation (No), Authentication type (SSH public key), Username (databaseuser), SSH Key format (RSA), Key pair name (DatabaseSSHkey), and Azure Spot (No). To the right, an "Estimated monthly cost" box displays "\$11.11 / month" with a "View cost details" link. At the bottom, there are "Previous" and "Next >" buttons, a "Create" button, and links for "Download a template for automation" and "Give feedback".

Create a virtual machine - Microsoft Azure

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualMachine-ARM

Microsoft Azure

Home > Virtual machines >

## Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

**Disk**

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

**Networking**

Virtual network	NetMazeVNet
Subnet	DatabaseSubnet (10.0.2.0/24)
Public IP	None
NIC network security group	(new) DatabaseVM-nsg
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Disabled

Estimated monthly cost  
\$11.11 / month

View cost details

< Previous Next > Create Download a template for automation Give feedback

Create a virtual machine - Microsoft Azure

portal.azure.com/?feature.msajs=true#create/Microsoft.VirtualMachine-ARM

Microsoft Azure

Home > Virtual machines >

## Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Delete NIC when VM is deleted Disabled

**Management**

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Enable hotpatch	Off
Patch orchestration options	Azure-orchestrated patching (preview); patches will be installed by Azure
Reboot setting	Reboot if required

**Monitoring**

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

Estimated monthly cost  
\$11.11 / month

View cost details

< Previous Next > Create Download a template for automation Give feedback

<https://portal.azure.com/?feature.msajs=true#view/flbExtension/DeploymentDetailsBlade/~/overview/d/%2Fsubscriptions%2F>

# CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20240819212216 | Overview

Your deployment is complete

Deployment name: CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20240819212216 Start time: 8/19/2024, 9:30:19 PM Subscription: Azure subscription Correlation ID: Be290329-f01e-4b79-be85-e1c2672258fc Resource group: NetMazeRG

**Deployment details**

Resource	Type	Status	Operation details
DatabaseVM	Microsoft.Compute/virtualMachines	OK	<a href="#">Operation details</a>
databasevm246	Microsoft.Network/networkInterfaces	Created	<a href="#">Operation details</a>
DatabaseVM-nsg	Microsoft.Network/networkSecurityGroups	OK	<a href="#">Operation details</a>

**Next steps**

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

[Go to resource](#) [Create another VM](#)

Give feedback [Tell us about your experience with deployment](#)

**Cost Management**  
Get notified to stay within your budget and prevent unexpected charges on your bill. [Set up cost alerts >](#)

**Microsoft Defender for Cloud**  
Secure your apps and infrastructure. [Go to Microsoft Defender for Cloud >](#)

**Free Microsoft tutorials**  
[Start learning today >](#)

**Work with an expert**  
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

<https://portal.azure.com/?feature.msajs=true#vivikvash1507@gmail.com/microsoft.com/resources/subscriptions/e9ea131-d6f1-4e0b-baee-b293615685ae>

# DatabaseVM | Overview

Virtual machine

Connect Start Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

**Overview**

**Essentials**

Resource group: <a href="#">(move)</a> NetMazeRG	Operating system: Linux (Ubuntu 22.04)
Status: Running	Size: Standard B1s (1 vcpu, 1 GB memory)
Location: Canada Central	Public IP address: -
Subscription: <a href="#">(move)</a> Azure subscription 1	Virtual network/subnet: <a href="#">NetMazeVNet/DatabaseSubnet</a>
Subscription ID: e9ea131-d6f1-4e0b-baee-b293615685ae	DNS name: -
	Health state: -
	Time created: 8/20/2024, 3:30 AM UTC

Tags: [\(edit\)](#) [Add tags](#)

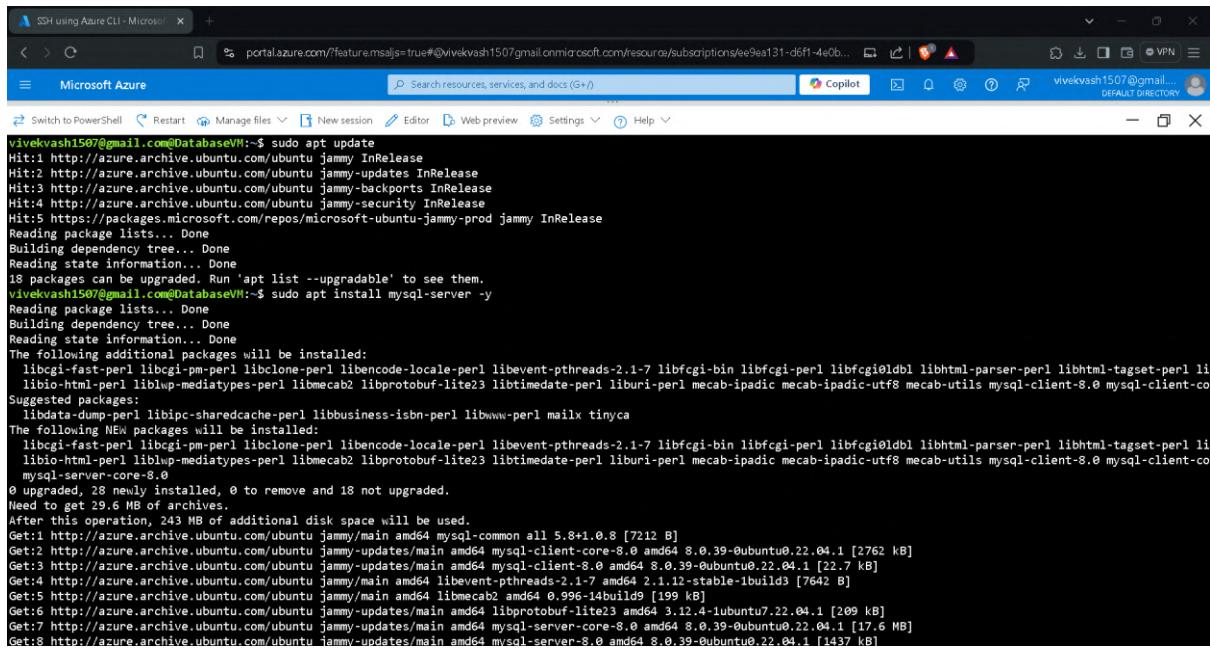
**Properties** Monitoring Capabilities (7) Recommendations Tutorials

**Virtual machine**

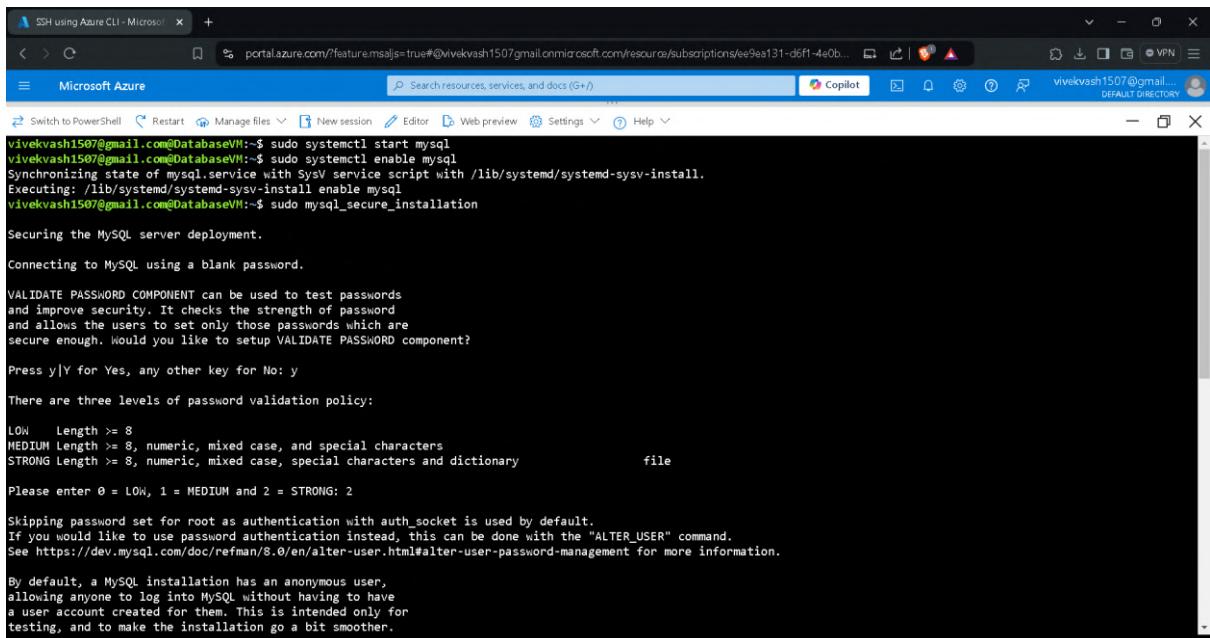
Computer name: DatabaseVM	Public IP address:
Operating system: Linux (Ubuntu 22.04)	Public IP address (IPv6): -
VM generation: V2	Private IP address: 10.0.2.4
VM architecture: x64	Private IP address (IPv6): -
Agent status: Ready	Virtual network/subnet: <a href="#">NetMazeVNet/DatabaseSubnet</a>
Agent version: 2.11.1.4	DNS name: -
Hibernation: Disabled	

**Networking**

Public IP address:	-
Private IP address:	10.0.2.4
Virtual network/subnet:	<a href="#">NetMazeVNet/DatabaseSubnet</a>
DNS name:	-



```
vivekvash1507@gmail.com@DatabaseVM:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/repos/microsoft-ubuntu-jammy-prod jammy InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
18 packages can be upgraded. Run 'apt list --upgradable' to see them.
vivekvash1507@gmail.com@DatabaseVM:~$ sudo apt install mysql-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcgifast-perl libcgipm-perl libclone-perl libencode-locale-perl libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgioldbl libhtml-parser-perl libhtml-tagset-perl libhttp-keepalive-perl libhttp-mediatypes-perl libmecab2 libprotobuf-lite23 libtimedate-perl liburi-perl mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0
Suggested packages:
  libdata-dump-perl libipc-sharedcache-perl libbusiness-isbn-perl libwww-perl mailx tinyca
The following NEW packages will be installed:
  libcgifast-perl libcgipm-perl libclone-perl libencode-locale-perl libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgioldbl libhtml-parser-perl libhtml-tagset-perl libhttp-keepalive-perl libhttp-mediatypes-perl libmecab2 libprotobuf-lite23 libtimedate-perl liburi-perl mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0
0 upgraded, 28 newly installed, 0 to remove and 18 not upgraded.
Need to get 29.6 MB of archives.
After this operation, 243 MB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 mysql-common all 5.8+1.0.8 [7212 B]
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client-core-8.0 amd64 8.0.39-0ubuntu0.22.04.1 [2762 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-client-8.0 amd64 8.0.39-0ubuntu0.22.04.1 [22.7 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-pthreads-2.1-7 amd64 2.1.12-stable-1build3 [7642 B]
Get:5 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 libmecab2 amd64 0.996-14build9 [199 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libprotobuf-lite23 amd64 3.12.4-1ubuntu7.22.04.1 [209 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-server-core-8.0 amd64 8.0.39-0ubuntu0.22.04.1 [17.6 MB]
Get:8 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-server-8.0 amd64 8.0.39-0ubuntu0.22.04.1 [1437 kB]
```



```
vivekvash1507@gmail.com@DatabaseVM:~$ sudo systemctl start mysql
vivekvash1507@gmail.com@DatabaseVM:~$ sudo systemctl enable mysql
Synchronizing state of mysql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mysql
vivekvash1507@gmail.com@DatabaseVM:~$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y

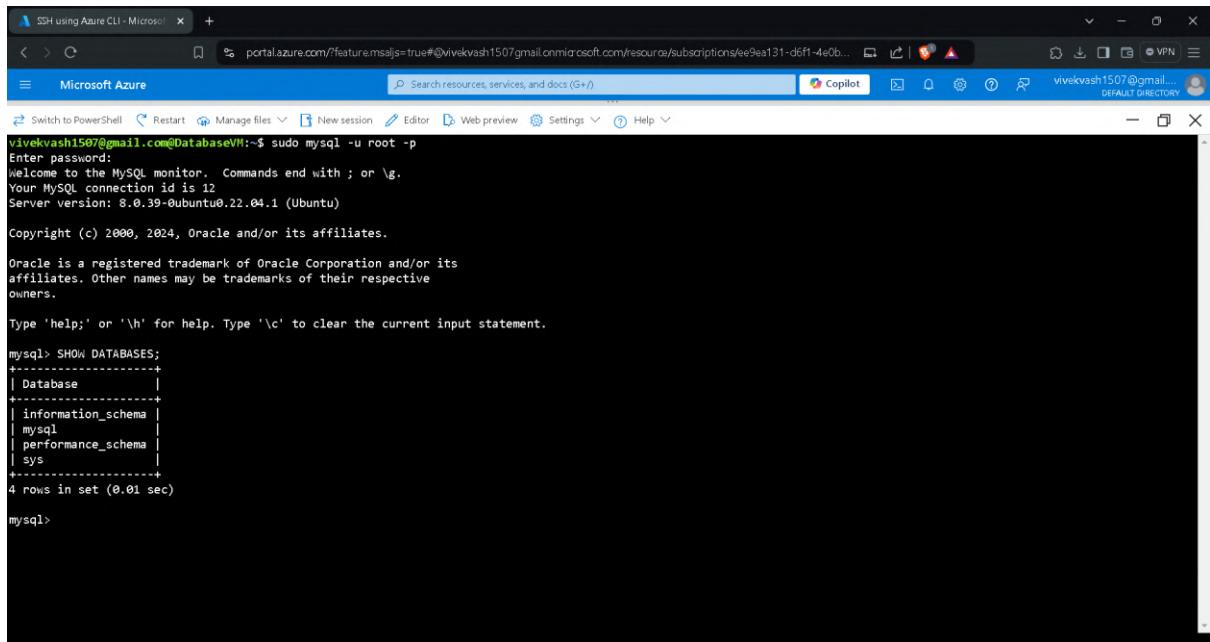
There are three levels of password validation policy:

LOW   Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary      file

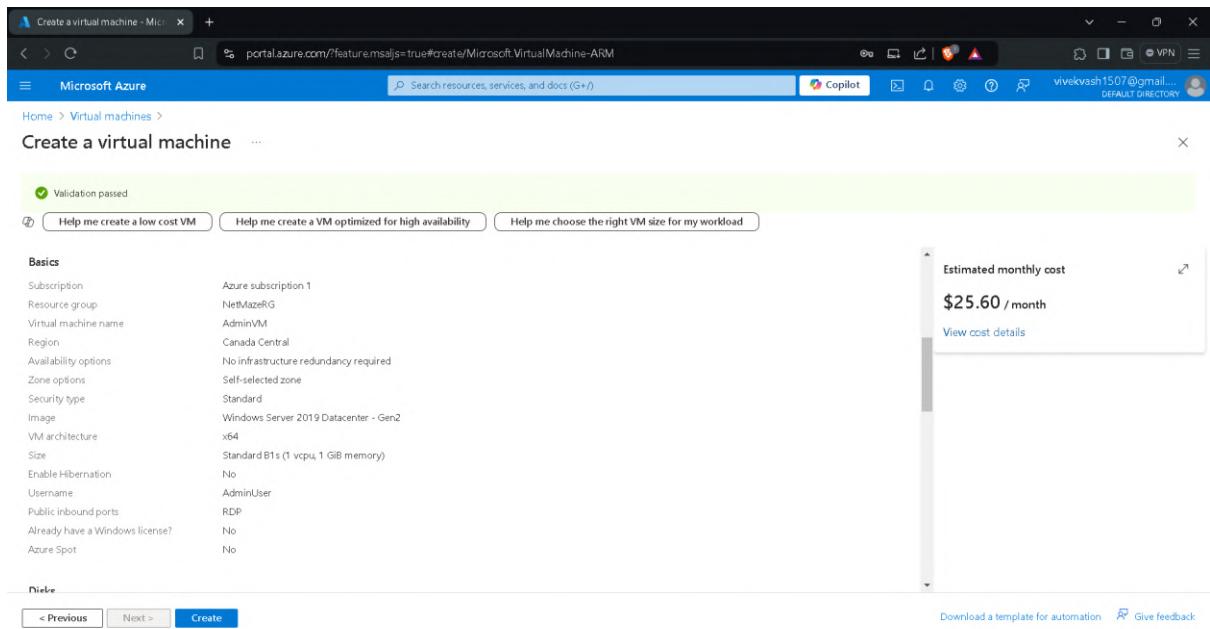
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2

Skipping password set for root as authentication with auth_socket is used by default.
If you would like to use password authentication instead, this can be done with the "ALTER_USER" command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management for more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
```



vivekvash1507@gmail.com@DatabaseVM:~\$ sudo mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 12  
Server version: 8.0.39-Ubuntu0.22.04.1 (Ubuntu)  
Copyright (c) 2000, 2024, Oracle and/or its affiliates.  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| information\_schema |  
| mysql |  
| performance\_schema |  
| sys |  
+-----+  
4 rows in set (0.01 sec)  
mysql>



Validation passed

Help me create a low cost VM   Help me create a VM optimized for high availability   Help me choose the right VM size for my workload

**Basics**

Subscription	Azure subscription 1
Resource group	NetMazeRG
Virtual machine name	AdminVM
Region	Canada Central
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vCPU, 1 GiB memory)
Enable Hibernation	No
Username	AdminUser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

**Disk**

Estimated monthly cost  
**\$25.60 / month**  
View cost details

< Previous   Next >   **Create**   Download a template for automation   Give feedback

Create a virtual machine - Microsoft Azure

portal.azure.com/?feature-msaljs=true#create/Microsoft.VirtualMachine-AzVM

Microsoft Azure

Home > Virtual machines >

## Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

**Disk**

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

**Networking**

Virtual network	NetvflazeVNet
Subnet	AdminSubnet (10.0.3.0/24)
Public IP	(new) AdminVM-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

**Management**

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

**Monitoring**

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

**Advanced**

Estimated monthly cost: \$25.60 / month

View cost details

< Previous Next > Create Download a template for automation Give feedback

Create a virtual machine - Microsoft Azure

portal.azure.com/?feature-msaljs=true#create/Microsoft.VirtualMachine-AzVM

Microsoft Azure

Home > Virtual machines >

## Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

**Management**

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

**Monitoring**

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

**Advanced**

Estimated monthly cost: \$25.60 / month

View cost details

< Previous Next > Create Download a template for automation Give feedback

**CreateVm-MicrosoftWindowsServerWindowsServer-201-20240819222950 | Overview**

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServerWindowsServer-201-20240819222950 Start time: 8/19/2024, 10:32:20 PM  
Subscription: Azure subscription 1 Correlation ID: bedb4b88-4163-45c3-983f-fb80bce85e15

Resource	Type	Status	Operation details
AdminVM	Microsoft.Compute/virtualMachines	OK	<a href="#">Operation details</a>
adminvm606	Microsoft.Network/networkInterfaces	Created	<a href="#">Operation details</a>
AdminVM-nsg	Microsoft.Network/networkSecurityGroups	OK	<a href="#">Operation details</a>
AdminVM-ip	Microsoft.Network/publicIPAddresses	OK	<a href="#">Operation details</a>

**Next steps**

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

[Go to resource](#) [Create another VM](#)

**Give feedback**

**Cost Management**  
Get notified to stay within your budget and prevent unexpected charges on your bill.  
[Set up cost alerts >](#)

**Microsoft Defender for Cloud**  
Secure your apps and infrastructure.  
[Go to Microsoft Defender for Cloud >](#)

**Free Microsoft tutorials**  
[Start learning today >](#)

**Work with an expert**  
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.  
[Find an Azure expert >](#)

**AdminVM - Microsoft Azure**

**AdminVM** Virtual machine

**Overview**

**AdminVM** virtual machine agent status is not ready. Troubleshoot the issue →

Essentials	Properties
Resource group: NetMazeRG Status: Running Location: Canada Central Subscription: Azure subscription 1 Subscription ID: ee9ea131-d6f1-4e0b-bae6-b293615685ae	Operating system: Windows Size: Standard B1s (1 vcpu, 1 GiB memory) Public IP address: 52.228.78.61 Virtual network/subnet: NetMazeVNet/AdminSubnet DNS name: Not configured Health state: - Time created: 8/20/2024, 4:32 AM UTC

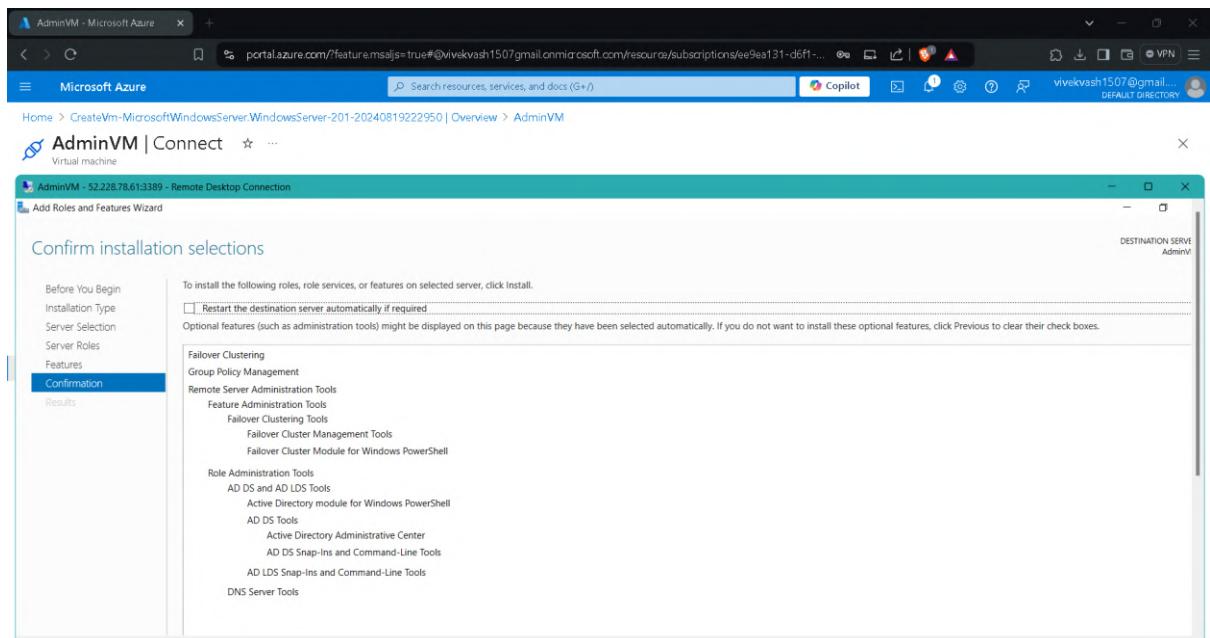
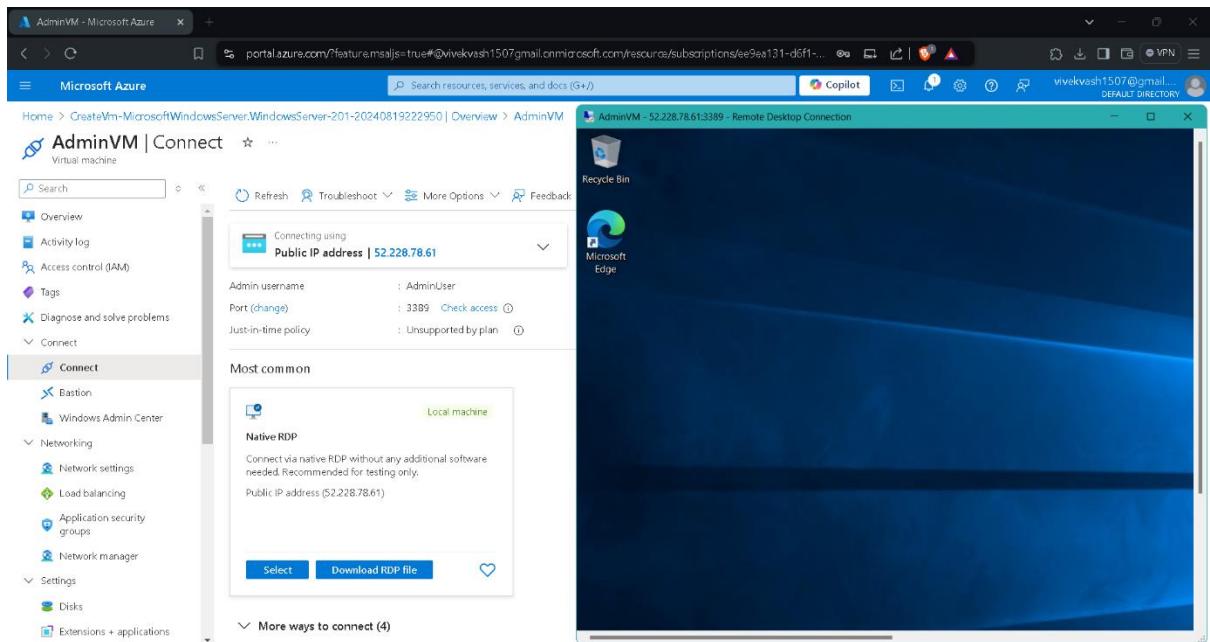
**Properties** **Monitoring** **Capabilities (8)** **Recommendations** **Tutorials**

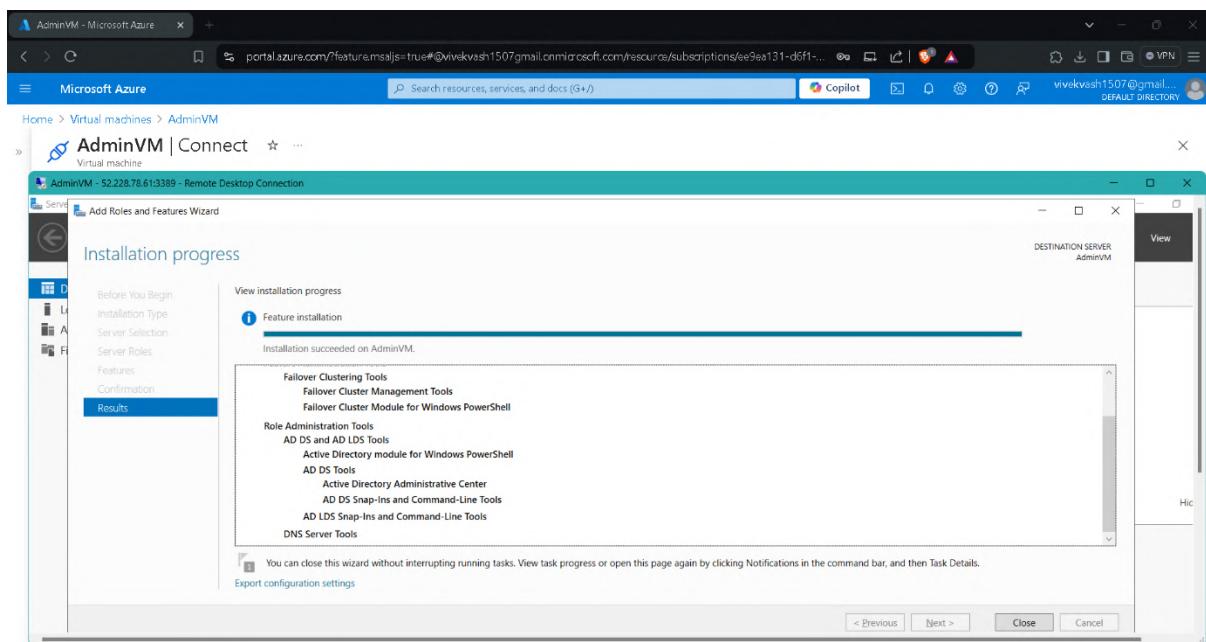
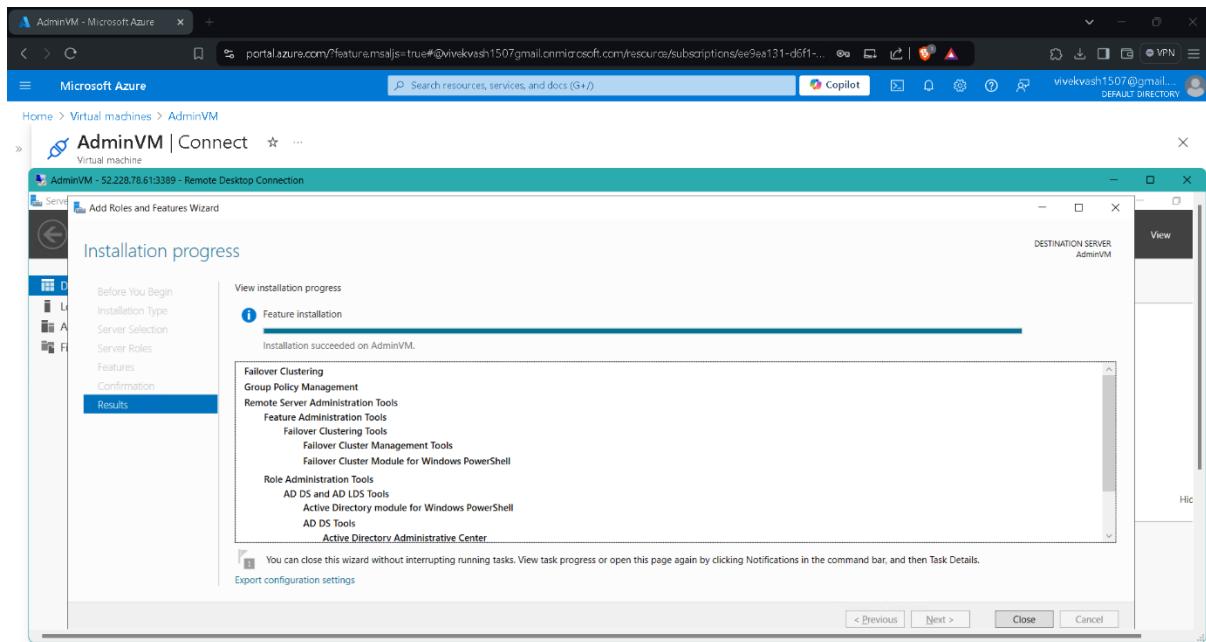
**Virtual machine**

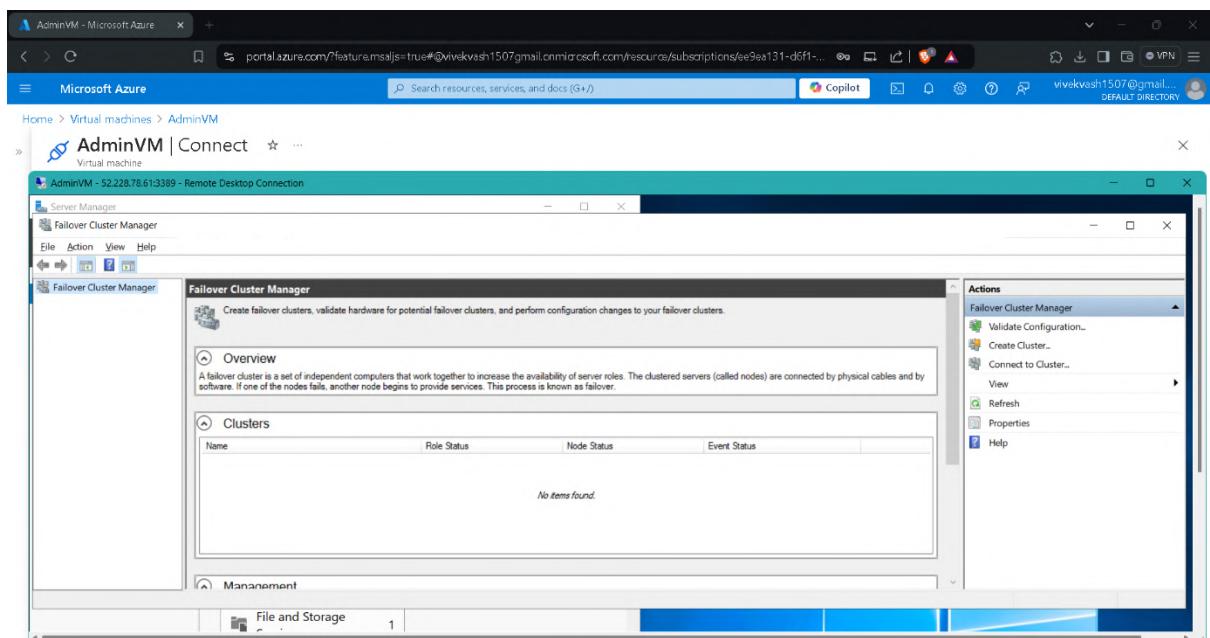
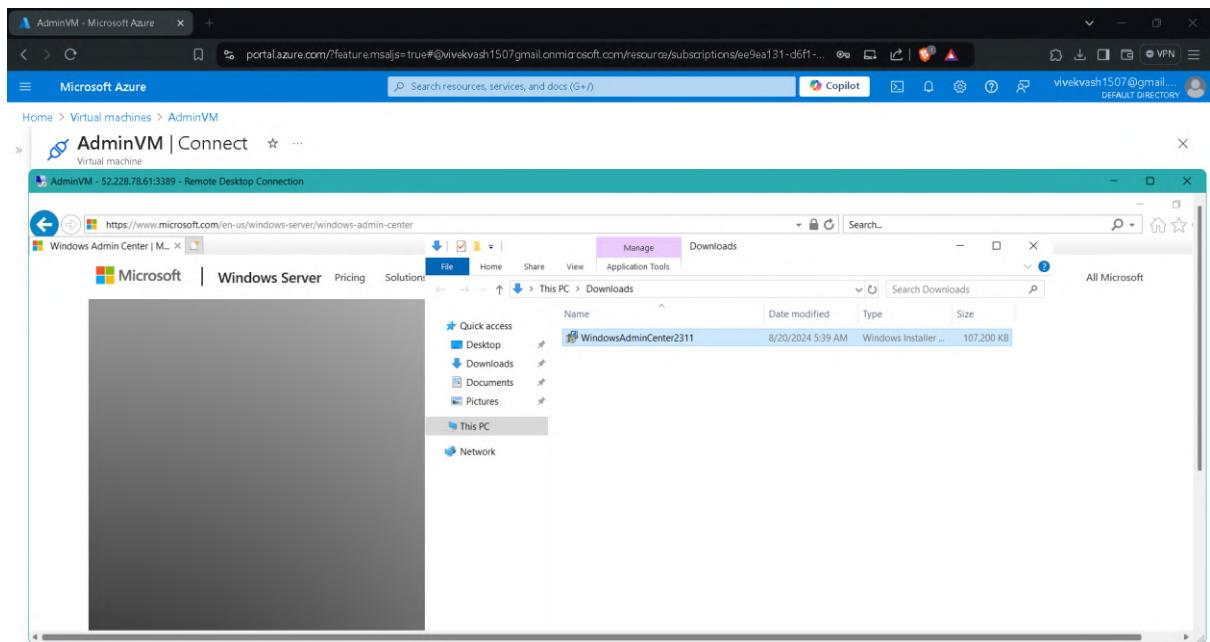
Computer name: AdminVM	Operating system: Windows
VM generation: V2	VM architecture: x64
Agent status: Not Ready	

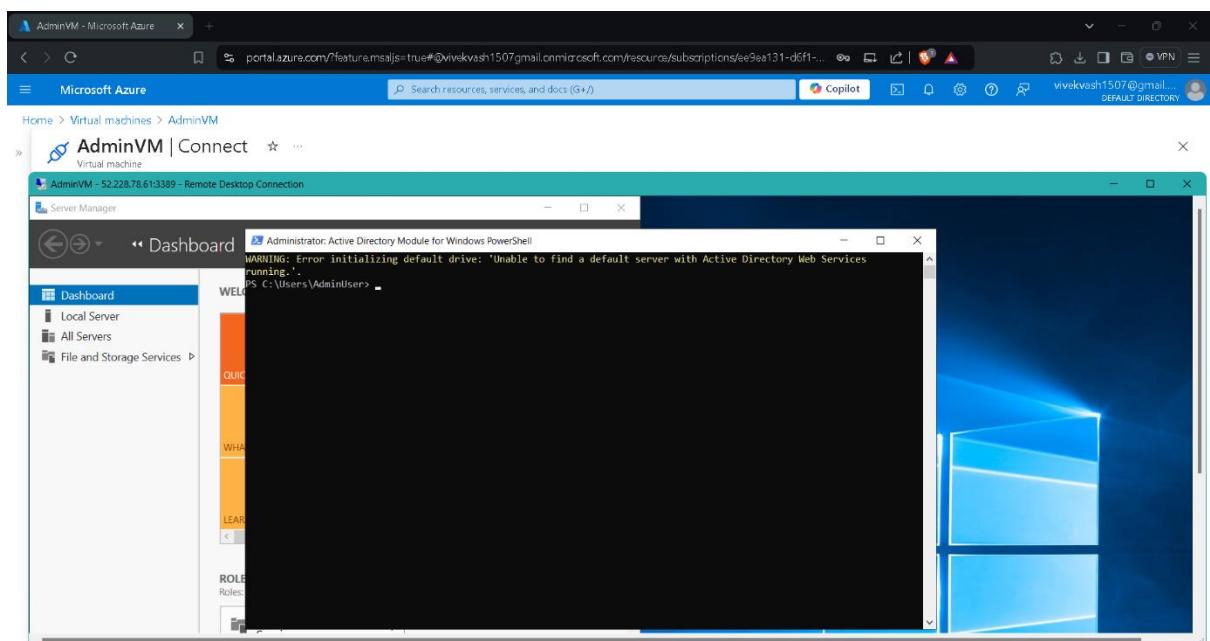
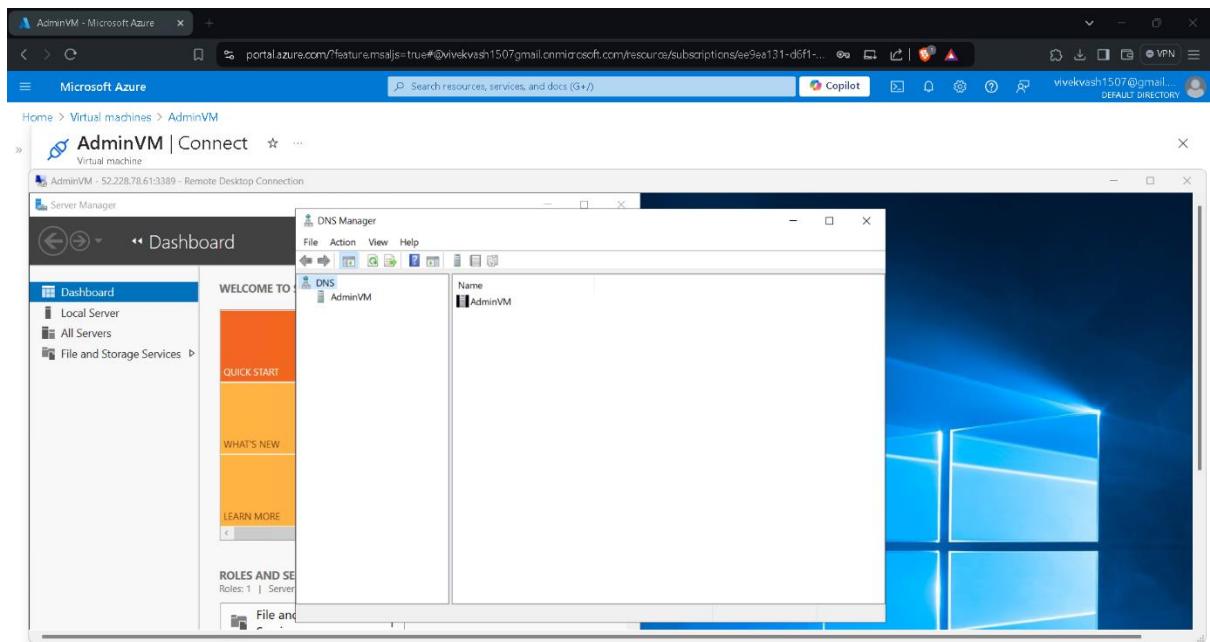
**Networking**

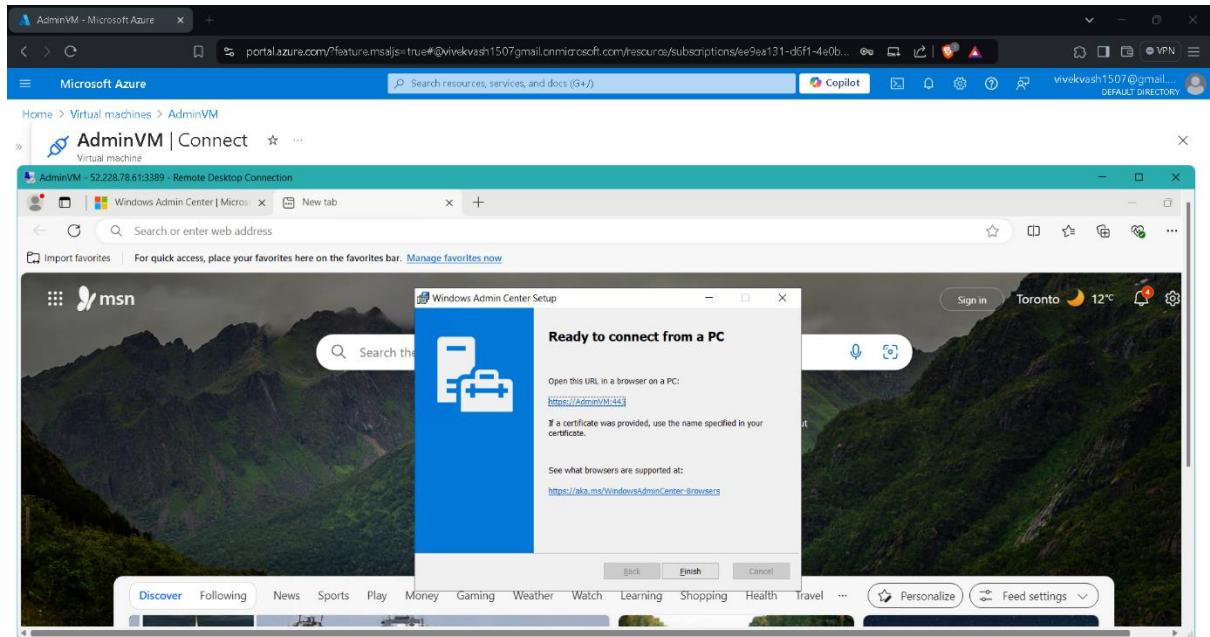
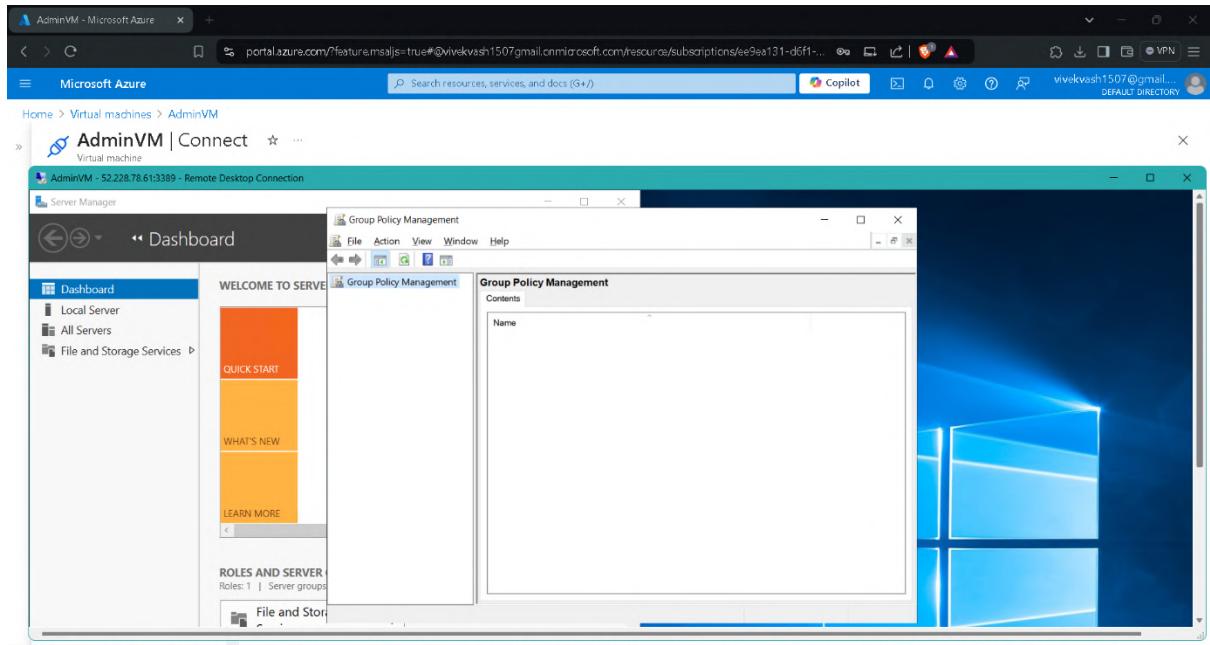
Public IP address: 52.228.78.61 (Network interface adminvm606)	Private IP address (IPv6): -
Private IP address: 10.0.3.4	Private IP address (IPv6): -
Virtual network/subnet: NetMazeVNet/AdminSubnet	

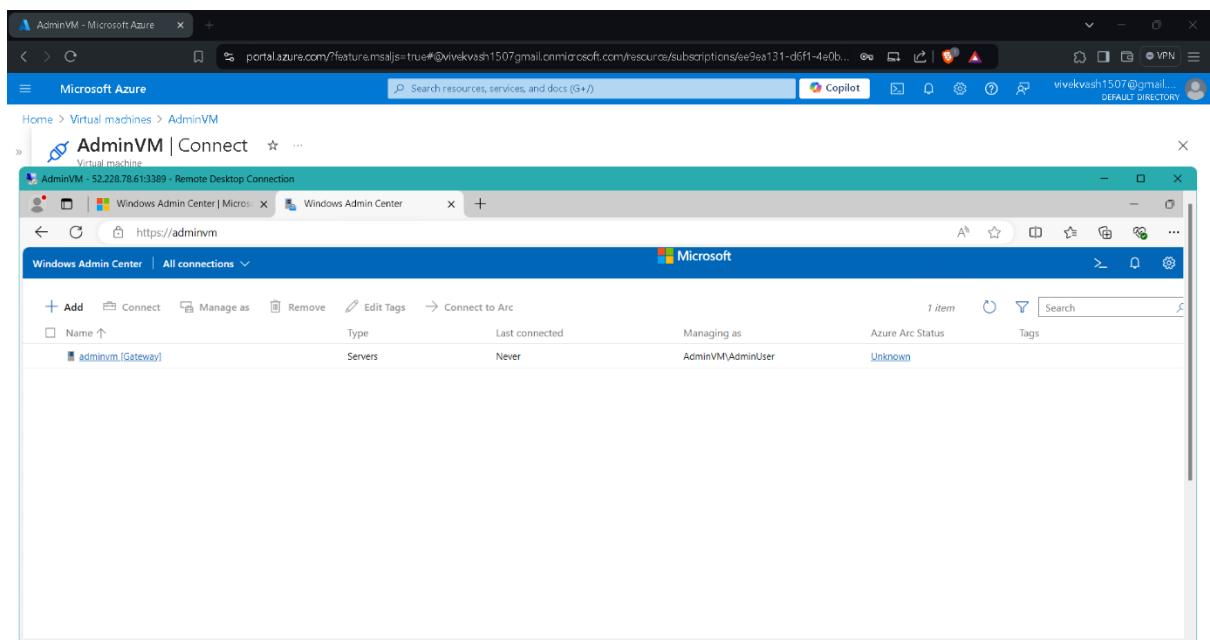
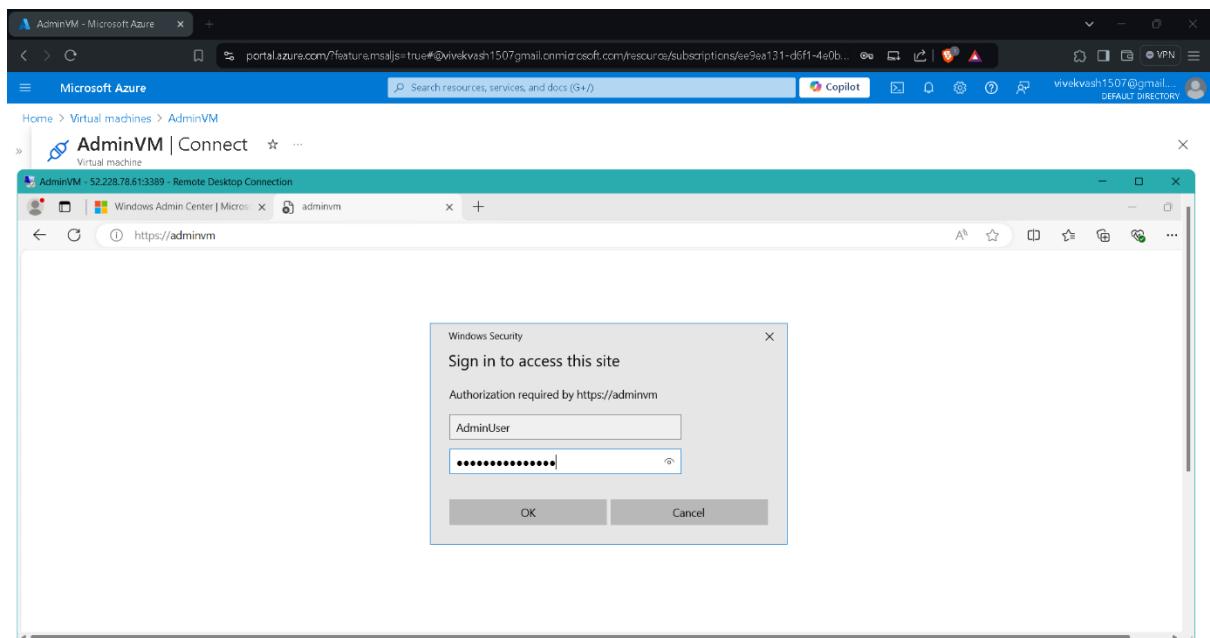












```

Administrator: Command Prompt
C:\Users\AdminUser>ping 10.0.1.4

PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp_seq=1 ttl=128 time=0.823 ms
64 bytes from 10.0.1.4: icmp_seq=2 ttl=128 time=1.08 ms
64 bytes from 10.0.1.4: icmp_seq=3 ttl=128 time=1.84 ms
64 bytes from 10.0.1.4: icmp_seq=4 ttl=128 time=1.44 ms
64 bytes from 10.0.1.4: icmp_seq=5 ttl=128 time=0.718 ms
64 bytes from 10.0.1.4: icmp_seq=6 ttl=128 time=1.21 ms
64 bytes from 10.0.1.4: icmp_seq=7 ttl=128 time=1.01 ms
64 bytes from 10.0.1.4: icmp_seq=8 ttl=128 time=0.764 ms
64 bytes from 10.0.1.4: icmp_seq=9 ttl=128 time=2.00 ms
64 bytes from 10.0.1.4: icmp_seq=10 ttl=128 time=0.937 ms
^C
--- 10.0.1.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9041ms
rtt min/avg/max/mdev = 0.718/1.201/2.198/0.463 ms
vivekvash1507@gmail.com@DatabaseVM:~$ ping 10.0.3.4

PING 10.0.3.4 (10.0.3.4) 56(84) bytes of data.
64 bytes from 10.0.3.4: icmp_seq=1 ttl=128 time=0.961 ms
64 bytes from 10.0.3.4: icmp_seq=2 ttl=128 time=1.92 ms
64 bytes from 10.0.3.4: icmp_seq=3 ttl=128 time=1.24 ms
64 bytes from 10.0.3.4: icmp_seq=4 ttl=128 time=1.13 ms
64 bytes from 10.0.3.4: icmp_seq=5 ttl=128 time=1.28 ms
64 bytes from 10.0.3.4: icmp_seq=6 ttl=128 time=1.52 ms
^C
--- 10.0.3.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.961/1.341/1.921/0.308 ms
vivekvash1507@gmail.com@DatabaseVM:~$ 

```

## Network Access Control

### 5.1. Creating the WebAppNSG

To ensure proper access control within the WebAppSubnet, I created a Network Security Group (NSG) named WebAppNSG.

- I logged into the Azure portal and navigated to the Network Security Groups section.
- I clicked on + Create to start the creation process.
- I entered the following details:
  - Name: WebAppNSG
  - Resource Group: NetMazeRG
  - Region: Canada Central
- After entering the necessary details, I clicked on Review + Create and then selected Create to deploy the WebAppNSG.

### 5.1.2. Associating WebAppNSG with the WebAppSubnet

After deploying the WebAppNSG, I associated it with the WebAppSubnet.

- I navigated to the Subnets tab within the WebAppNSG.
- I clicked on + Associate, selected NetMazeVNet as the virtual network, and chose WebAppSubnet as the subnet.
- I clicked on OK to finalize the association.

### 5.1.3. Configuring Inbound Security Rules

To allow only specific types of traffic into the WebAppSubnet, I configured the following inbound security rules:

- Rule 1:
  - Priority: 100
  - Name: Allow-HTTP-80
  - Port: 80
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow
- Rule 2:
  - Priority: 110
  - Name: Allow-HTTPS-443
  - Port: 443
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow

These rules ensured that the WebAppVM was accessible via HTTP and HTTPS.

## 5.2. Creating the DatabaseNSG

### 5.2.1. Configuring the DatabaseNSG

Next, I created a Network Security Group named DatabaseNSG to secure the DatabaseSubnet.

- I initiated the creation process similar to the WebAppNSG.
- The configurations were as follows:
  - Name: DatabaseNSG

- Resource Group: NetMazeRG
- Region: Canada Central
- I deployed the DatabaseNSG by clicking on Review + Create and then Create.

### 5.2.2. Associating DatabaseNSG with the DatabaseSubnet

After deploying the DatabaseNSG, I associated it with the DatabaseSubnet.

- I navigated to the Subnets tab within the DatabaseNSG.
- I clicked on + Associate, selected NetMazeVNet as the virtual network, and chose DatabaseSubnet as the subnet.
- I clicked on OK to complete the association.

### 5.2.3. Configuring Inbound Security Rules

To secure database access, I configured the following inbound security rules:

- Rule 1:
  - Priority: 100
  - Name: Allow-MySQL-3306
  - Port: 3306
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow
- Rule 2:
  - Priority: 110
  - Name: Allow-SSH-22
  - Port: 22
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow

These rules allowed MySQL and SSH access to the DatabaseVM.

## 5.3. Creating the AdminNSG

### 5.3.1. Configuring the AdminNSG

The final NSG created was the AdminNSG for securing the AdminSubnet.

- I followed the same process as for the previous NSGs.
- The configurations were as follows:
  - Name: AdminNSG
  - Resource Group: NetMazeRG
  - Region: Canada Central
- I deployed the AdminNSG by clicking on Review + Create and then Create.

### 5.3.2. Associating AdminNSG with the AdminSubnet

After deploying the AdminNSG, I associated it with the AdminSubnet.

- I navigated to the Subnets tab within the AdminNSG.
- I clicked on + Associate, selected NetMazeVNet as the virtual network, and chose AdminSubnet as the subnet.
- I clicked on OK to finalize the association.

### 5.3.3. Configuring Inbound Security Rules

To control access to the AdminVM, I configured the following inbound security rules:

- Rule 1:
  - Priority: 100
  - Name: Allow-RDP-3389
  - Port: 3389
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow
- Rule 2:
  - Priority: 110
  - Name: Allow-SSH-22
  - Port: 22
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow

These rules ensured that the AdminVM was accessible via RDP and SSH.

In this phase of the project, I implemented strict network access control by creating and configuring Network Security Groups (NSGs) for each subnet. These NSGs were associated with the respective subnets to enforce specific inbound rules, ensuring that only valid and authorized traffic could access the resources within the NetMazeVNet.

## Screenshots

This screenshot shows the 'Create network security group' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. In the 'Project details' section, 'Subscription' is set to 'Azure subscription 1' and 'Resource group' is set to 'NetMazeRG'. In the 'Instance details' section, 'Name' is 'WebAppNSG' and 'Region' is 'Canada Central'. At the bottom, there are buttons for 'Review + create' and 'Next : Tags >'. A note says 'Download a template for automation'.

This screenshot shows the 'Associate subnet' dialog in the Microsoft Azure portal. It is associated with the 'WebAppNSG' network security group. The 'Associate' button is highlighted. The 'Associate subnet' section shows 'Virtual network' set to 'NetMazeVNet (NetMazeRG)' and 'Subnet' set to 'WebAppSubnet'. An 'OK' button is at the bottom right.

**WebAppNSG - Microsoft Azure**

Microsoft Azure | portal.azure.com/?feature.msals=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-4e0b... | Copilot | Help | Settings | Log out | vivekvash1507@gmail... | DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual machines > WebAppVM | Network settings > WebAppNSG

### WebAppNSG | Inbound security rules

Network security group

Search Add Hide default rules Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	Allow-HTTP-80	80	TCP	Any	Any	Allow
110	Allow-HTTPS-443	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn... Any	Any	AzureLoadBalancer	Any	Allow	
65500	DenyAllInBound	Any	Any	Any	Any	Deny

<https://go.microsoft.com/fwlink/?linkid=2174617>

**WebAppNSG - Microsoft Azure**

Microsoft Azure | portal.azure.com/?feature.msals=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-4e0b... | Copilot | Help | Settings | Log out | vivekvash1507@gmail... | DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual machines > WebAppVM | Network settings >

### WebAppNSG

Network security group

Search Move Delete Refresh Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Custom security rules : 2 inbound, 0 outbound  
Associated with : 1 subnets, 0 network interfaces

Resource group (move) : NetMazeRG  
Location : Canada Central  
Subscription (move) : Azure subscription 1  
Subscription ID : ee9ea131-d6f1-4e0b-baee-b293615685ae  
Tags (edit) : Add tags

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	Allow-HTTP-80	80	TCP	Any	Any	Allow
110	Allow-HTTPS-443	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn... Any	Any	AzureLoadBalancer	Any	Allow	
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

WebAppVM-nsg - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

vivekvash1507@gmail.com DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual machines > WebAppVM | Network settings > WebAppVM-nsg

## WebAppVM-nsg | Inbound security rules

Network security group

Search Add Hide default rules Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
310	Allow-HTTP-80	80	TCP	Any	Any	Allow
320	Allow-HTTPS-443	443	TCP	Any	Any	Allow
65000	AllowWhitelist	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Create network security group - Microsoft Azure

portal.azure.com/?feature-msaljs=true#create/Microsoft.NetworkSecurityGroup-ARM

Microsoft Azure

Search resources, services, and docs (G+)

vivekvash1507@gmail.com DEFAULT DIRECTORY (VIVEKVA...)

Home > Network security groups >

## Create network security group

Basics Tags Review + create

Project details

Subscription \* Azure subscription 1 ✓

Resource group \* NetMazeRG ✓ Create new

Instance details

Name \* DatabaseNSG ✓

Region \* Canada Central ✓

Review + create < Previous Next: Tags > Download a template for automation

**Associate subnet**

Virtual network: NetMazeVNet (NetMazeRG)

Subnet: DatabaseSubnet

OK

**DatabaseNSG | Inbound security rules**

Priority ↑	Name ↑	Port = all	Protocol = all	Source = all	Destination = all	Action ↑
100	Allow-MySQL-3306	3306	TCP	Any	Any	Allow
110	Allow-SSH-22	22	TCP	Any	Any	Allow
65000	AllowVhInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

DatabaseNSG - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

vivekvash1507@gmail.com Copilot

DatabaseNSG Network security group

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Resource group (move) : NetMazeRG Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae6-b293615685ae Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound Associated with : 1 subnets, 0 network interfaces

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	Allow-MySQL-3306	3306	TCP	Any	Any	Allow
110	Allow-SSH-22	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

JSON View

DatabaseVM-nsg - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

vivekvash1507@gmail.com Copilot

DatabaseVM-nsg Network security group

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Resource group (move) : NetMazeRG Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae6-b293615685ae Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound Associated with : 0 subnets, 1 network interfaces

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
1000	default-allow-ssh	22	TCP	Any	Any	Allow
1010	Allow-MySQL	3306	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

JSON View

**Create network security group**

**Basics** Tags Review + create

**Project details**

Subscription \* Azure subscription 1  
Resource group \* NetMazeRG Create new

**Instance details**

Name \* AdminNSG  
Region \* Canada Central

**Review + create** < Previous Next : Tags > Download a template for automation

**Associate subnet - Microsoft Azure**

**AdminNSG | Subnets**

**Associate subnet**

Virtual network: NetMazeVNet (NetMazeRG)  
Subnet \* AdminSubnet

**OK**

AdminNSG - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Microsoft.NetworkSecurityGroup-20240820160723 | Overview > AdminNSG

## AdminNSG | Inbound security rules

Network security group

Search

Add Hide default rules Refresh Delete Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Help

Filter by name

Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑ Destination ↑ Action ↑

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-RDP-3389	3389	TCP	Any	Any	Allow
110	Allow-SSH-22	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

AdminNSG - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Microsoft.NetworkSecurityGroup-20240820160723 | Overview > AdminNSG

## AdminNSG

Network security group

Move Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Help

Resource group (move) : NetMazeRG

Location : Canada Central

Subscription (move) : Azure subscription 1

Subscription ID : ee9ea131-d6f1-4e0b-baee-b293615685ae

Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

Filter by name

Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑ Destination ↑ Action ↑

Custom security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-RDP-3389	3389	TCP	Any	Any	Allow
110	Allow-SSH-22	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-RDP-3389	3389	TCP	Any	Any	Allow
110	Allow-SSH-22	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar shows the navigation path: Home > Network security groups > AdminVM-nsg. The main content area displays the NSG details under the 'Overview' tab. It shows the resource group (NetMazeRG), location (Canada Central), subscription (Azure subscription 1), and subscription ID (ee9ea131-d6f1-4e0b-bae6-b293615685ae). Under the 'Inbound security rules' section, there are four entries:

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
310	Allow-SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

Under the 'Outbound security rules' section, there are three entries:

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

## Secure Administrative Access

### 6.1. Creating Azure Bastion Subnet

#### 6.1.1. Configuring the Azure Bastion Subnet

To enable secure and seamless RDP and SSH access to my virtual machines without exposing them to the public internet, I implemented Azure Bastion. The first step was to create a dedicated subnet for Azure Bastion in the NetMazeVNet.

- I logged into the Azure portal and navigated to the Virtual Networks section.
- I selected NetMazeVNet and then went to the Subnets tab.
- I clicked on + Subnet to create a new subnet.
- I entered the following details:
  - Name: AzureBastionSubnet
  - IPv4 Address Range: 10.0.4.0/26
- I clicked on OK to finalize the subnet creation.

## 6.2. Deploying Azure Bastion

### 6.2.1. Creating the NetMaze Bastion

With the Azure Bastion subnet in place, I proceeded to deploy the Azure Bastion service within the NetMazeVNet.

- I navigated to the Azure Bastion section in the Azure portal.
- I clicked on + Create to start the deployment.
- I entered the following configurations:
  - Resource Group: NetMazeRG
  - Region: Canada Central
  - Tier: Standard
  - Instance Count: 2
  - Virtual Network: NetMazeVNet
  - Subnet: AzureBastionSubnet (10.0.4.0/26)
  - Public IP Address: Create new
    - Public IP Address Name: NetMazeBastionPIP
- In the Advanced tab, I enabled Copy and paste and IP-based connection.
- I clicked on Create to deploy the NetMazeBastion.

### 6.2.2. Dissociating Public IPs from VMs

After deploying the NetMazeBastion, I removed the public IP addresses from the virtual machines to ensure they are not exposed to the public internet.

- I navigated to the Public IP addresses section in the Azure portal.
- I selected AdminVM-ip, dissociated it from the AdminVM NIC, and deleted the IP address.
- I repeated this process for the public IPs of DatabaseVM, WebAppVM, and OnPremVM.

## 6.3. Testing Azure Bastion Connectivity

### 6.3.1. Connecting to AdminVM via Azure Bastion

To verify that the Azure Bastion service was working correctly, I tested the connection to AdminVM.

- I navigated to the Virtual Machines section in the Azure portal.
- I selected AdminVM and went to the Bastion tab.

- I entered the credentials (Username and VM Password) and clicked on Connect.
- A new tab opened, and I was successfully connected to AdminVM through Azure Bastion.

### 6.3.2. Connecting to DatabaseVM via Azure Bastion

I repeated the same steps to connect to DatabaseVM using Azure Bastion.

- I navigated to DatabaseVM in the Virtual Machines section.
- In the Bastion tab, I entered the credentials (Username and selected the Databasesshkey.pem local file).
- I clicked on Connect, and a new tab opened, successfully connecting me to DatabaseVM via Azure Bastion.

### 6.3.3. Connecting to WebAppVM via Azure Bastion

Lastly, I verified the connection to WebAppVM through Azure Bastion.

- I navigated to WebAppVM in the Virtual Machines section.
- In the Bastion tab, I entered the credentials (Username and VM Password).
- I clicked on Connect, and a new tab opened, confirming a successful connection to WebAppVM via Azure Bastion.

## 6.4. Extending Azure Bastion to On-PremVNet

### 6.4.1. Creating Azure Bastion Subnet in OnPremVNet

To extend the secure connectivity to the simulated on-premises environment, I created a dedicated Azure Bastion subnet in the OnPremVNet.

- I navigated to OnPremVNet in the Azure portal and went to the Subnets tab.
- I clicked on + Subnet and entered the following details:
  - Name: AzureBastionSubnet
  - IPv4 Address Range: 10.1.4.0/26
- I clicked on OK to finalize the subnet creation.

#### 6.4.2. Deploying OnPrem Bastion

Next, I deployed Azure Bastion for the OnPremVNet to secure administrative access to the OnPremVM.

- I navigated to the Azure Bastion section in the Azure portal and clicked on + Create.
- I entered the following configurations:
  - Resource Group: NetMazeRG
  - Region: North Central US
  - Tier: Standard
  - Instance Count: 2
  - Virtual Network: OnPremVNet
  - Subnet: AzureBastionSubnet (10.1.4.0/26)
  - Public IP Address: Create new
    - Public IP Address Name: OnPremBastionPIP
- In the Advanced tab, I enabled Copy and paste and IP-based connection.
- I clicked on Create to deploy the OnPremBastion.

#### 6.4.3. Testing Azure Bastion Connectivity for OnPremVM

Finally, I verified the connection to OnPremVM through Azure Bastion.

- I navigated to OnPremVM in the Virtual Machines section of the Azure portal.
- I went to the Bastion tab, entered the credentials (Username and VM Password), and clicked on Connect.
- A new tab opened, confirming a successful connection to OnPremVM via Azure Bastion.

In this phase of the project, I successfully implemented Azure Bastion to provide secure, seamless RDP and SSH access to all virtual machines within the NetMazeVNet and OnPremVNet without exposing them to the public internet. The connections were tested and verified to ensure that the Azure Bastion service was functioning as expected.

## Screenshots

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes Home, Virtual networks, NetMazeVNet, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peering, and Service endpoints. The main content area displays the 'Subnets' blade for the NetMazeVNet virtual network. A modal dialog titled 'Add a subnet' is open, prompting for subnet configuration. The 'Subnet purpose' dropdown is set to 'Azure Bastion'. The 'Name' field is populated with 'AzureBastionSubnet'. Under 'IPv4', the 'Include an IPv4 address space' checkbox is checked, and the 'IPv4 address range' is set to '10.0.0.0/16'. The 'Starting address' is '10.0.4.0' and the 'Size' is '/26 (64 addresses)'. The 'Subnet address range' is '10.0.4.0 - 10.0.4.63'. Under 'IPv6', there is a note stating 'This virtual network has no IPv6 address ranges.' The 'Private subnet' section contains a note about private subnets enhancing security by not providing default outbound access. At the bottom of the dialog are 'Add' and 'Cancel' buttons.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes Home, Virtual networks, NetMazeVNet, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peering, and Service endpoints. The main content area displays the 'Create a Bastion' blade for the NetMazeVNet virtual network. The 'Basics' tab is selected. The 'Project details' section requires a 'Subscription' (Azure subscription 1) and a 'Resource group' (NetMazeRG). The 'Instance details' section requires a 'Name' (NetMazeBastion), 'Region' (Canada Central), 'Availability zone' (None), 'Tier' (Standard), and an 'Instance count' (2). The 'Configure virtual networks' section requires a 'Virtual network' (NetMazeVNet). At the bottom of the blade are 'Review + create', 'Previous', 'Next : Advanced >', and 'Download a template for automation' buttons.

**Create a Bastion - Microsoft Azure**

portal.azure.com/?feature\_msjs=true#view/Microsoft\_Azure\_HybridNetworking/CreateBastionHostBlade/\_provisioningContent

**Microsoft Azure**

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks > NetMazeVNet | Bastion >

## Create a Bastion

Configure virtual networks

Virtual network \*  Create new

Subnet \*  Manage subnet configuration

Configure IP Address

IP Address  Public IP address  Private IP address

Public IP address

Public IP address \*  Create new  Use existing

Public IP address name \*

Public IP address SKU Standard

Assignment  Dynamic  Static

Availability zone None

[Review + create](#) [Previous](#) [Next : Advanced >](#) [Download a template for automation](#)

**Create a Bastion - Microsoft Azure**

portal.azure.com/?feature\_msjs=true#view/Microsoft\_Azure\_HybridNetworking/CreateBastionHostBlade/\_provisioningContent

**Microsoft Azure**

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (VIVEKVA...)

Home > Virtual networks > NetMazeVNet | Bastion >

## Create a Bastion

Basics **Advanced** Tags Review + create

Bastion Features

Bastion allows web based RDP access to your vnet VM. [Learn more](#)

Copy and paste  IP-based connection

Kerberos authentication  Native client support  Shareable Link  Session recording (Preview)

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

Create a Bastion

Validation passed

Basics Advanced Tags Review + create

Summary

**Basics**

Name	NetMazeBastion
Subscription	Azure subscription 1
Resource group	NetMazeRG
Region	Canada Central
Availability zone	None
Virtual network	NetMazeVNet
Tier	Standard
Subnets	AzureBastionSubnet
Public IP address	NetMazeBastionIP
Internet-facing	2
Copy and paste	Enabled
IP-based connection	Enabled
Kerberos authentication	Disabled
Shareable Link	Disabled
Session recording (Preview)	Disabled
Native client support	Disabled
Private Bastion	Disabled

**Create** Previous Next Download a template for automation

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the title 'NetMazeBastion - Microsoft A...', a search bar with placeholder 'Search resources, services, and docs (G+)', and various icons for Copilot, Help, and settings. Below the header, the main content area displays the 'Overview' page for the 'NetMazeBastion' host. On the left, a sidebar menu lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings', 'Monitoring', 'Automation', and 'Help'. The 'Overview' section contains details such as Resource group (NetMazeRG), Location (Canada Central), Subscription (Azure subscription 1), and Subscription ID (ee9ea131-d6f1-4e0b-baee-b293615685ae). It also shows the Virtual network/subnet (NetMazeVNet/AzureBastionSubnet), Public DNS name (bst-92db639b-64f6-4184-b327-600f105bfaf.bastion.azure.com), Public IP address (NetMazeBastionPIP), Tier (Standard), Provisioning state (Succeeded), and Availability zone (None). A 'Tags' section allows for editing or adding tags. At the bottom, there are tabs for 'Sessions' and 'Tutorials', and a table titled 'Sessions' with columns: SessionId, StartTime (UTC), TargetSubscriptionId, ResourceType, TargetHostName, TargetResourceGro..., UserName, TargetIPAddress, and Protocol. The table currently shows 'No results.'

Screenshot of Microsoft Azure portal showing the "AdminVM-ip" Public IP address dissociation confirmation dialog.

**Overview**

**Dissociation confirmation**

This action will permanently dissociate the public IP address 'AdminVM-ip' from network interface card 'adminvm606'.

**Yes**   **No**

**Essentials**

- Resource group (move) **NetMazeRG**
- Location (move) **Canada Central**
- Subscription (move) **Azure subscription 1**
- Subscription ID **ee9ea131-d6f1-4e0b-bae6-b293615685ae**

**SKU** Standard

**Tier** Regional

**Virtual machine** AdminVM

**Routing preference** Microsoft network

**Tags** (edit) Add tags

**Get Started** Properties Tutorials

Screenshot of Microsoft Azure portal showing the "AdminVM-ip" Public IP address deletion confirmation dialog.

**Overview**

**Delete public IP address**

Do you want to delete the public IP address 'AdminVM-ip'?

**Yes**   **No**

**Essentials**

- Resource group (move) **NetMazeRG**
- Location (move) **Canada Central**
- Subscription (move) **Azure subscription 1**
- Subscription ID **ee9ea131-d6f1-4e0b-bae6-b293615685ae**

**SKU** Standard

**Tier** Regional

**IP address**

**Virtual machine** AdminVM

**Routing preference** Microsoft network

**Tags** (edit) Add tags

**Get Started** Properties Tutorials

The screenshot shows the Microsoft Azure portal interface for managing Public IP addresses. On the left, a sidebar lists various IP addresses, including 'NetMazeBastionPIP', 'NetMazeVPNPublicIP', 'OnPremVM-IP', 'OnPremVPNPublicIP', 'pip-netmazevnet-canadacentral-database... (selected)', and 'WebAppVM-IP'. The main panel displays the details for the selected IP address, 'pip-netmazevnet-canadacentral-database...'. A modal dialog titled 'Dissociation confirmation' is open, stating: 'This action will permanently dissociate the public IP address 'pip-netmazevnet-canadacentral-database... from network interface card 'databasevm246''. It contains two buttons: 'Yes' (highlighted in blue) and 'No'.

This screenshot is identical to the previous one, showing the 'Dissociation confirmation' dialog. The only difference is the text within the dialog, which now reads: 'Do you want to delete the public IP address 'pip-netmazevnet-canadacentral-database...?'. The 'Yes' button is highlighted in blue.

WebAppVM-ip - Microsoft Azure

portal.azure.com/?feature.msals=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-... Copilot

Microsoft Azure

Home > Public IP addresses >

## Public IP addresses

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

- NetMazeBastionPIP
- NetMazeVPNPublicIP
- OnPremVM-ip
- OnPremVPNPublicIP
- WebAppVM-ip

WebAppVM-ip

Public IP address

Overview Activity log Access control (IAM) Tags Settings Monitoring Automation Help

Essentials

Resource group (move) NetMazeRG SKU Standard Location (move) Canada Central Tier Regional Subscription (move) Azure subscription 1 Subscription ID ee9ea131-d6f1-4e0b-baee-b293615685ae

Dissociation confirmation

This action will permanently dissociate the public IP address 'WebAppVM-ip' from network interface card 'webappvmB24'.  webappvmB24 (Network interface card)

Yes No

Virtual machine WebAppVM Routing preference Microsoft network

Tags (edit) Add tags

Get Started Properties Tutorials

WebAppVM-ip - Microsoft Azure

portal.azure.com/?feature.msals=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-... Copilot

Microsoft Azure

Home > Public IP addresses >

## Public IP addresses

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

- NetMazeBastionPIP
- NetMazeVPNPublicIP
- OnPremVM-ip
- OnPremVPNPublicIP
- WebAppVM-ip

WebAppVM-ip

Public IP address

Overview Activity log Access control (IAM) Tags Settings Monitoring Automation Help

Essentials

Resource group (move) NetMazeRG SKU Standard Location (move) Canada Central Tier Regional IP address

Delete public IP address

Do you want to delete the public IP address 'WebAppVM-ip'?

Yes No

Virtual machine WebAppVM Routing preference Microsoft network

Tags (edit) Add tags

Get Started Properties Tutorials

OnPremVM-ip - Microsoft Azure

Home > Public IP addresses >

### Public IP addresses

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

- NetMazeBastionPIP
- NetMazeVPNPublicIP
- OnPremBastionPIP
- OnPremVM-ip**
- OnPremVPNPublidP

Search

Overview

Associate Dissociate Delete Move Refresh Open in mobile Give feedback

\*\*\* Saving network interface

Saving network interface 'onpremvm473'.

OnPremVM-ip

Public IP address

Activity log

Access control (IAM)

Tags

Settings

Monitoring

Automation

Help

Resource group (move) NetMazeRG

Location (move) North Central US

Subscription (move) Azure subscription 1

Subscription ID ee9ea131-d6f1-4e0b-baee-b293615685ae

SKU Standard

Tier Regional

Dissociation confirmation

This action will permanently dissociate the public IP address 'OnPremVM-ip' from network interface card 'onpremvm473' (Network interface card)

Yes No

Virtual machine OnPremVM

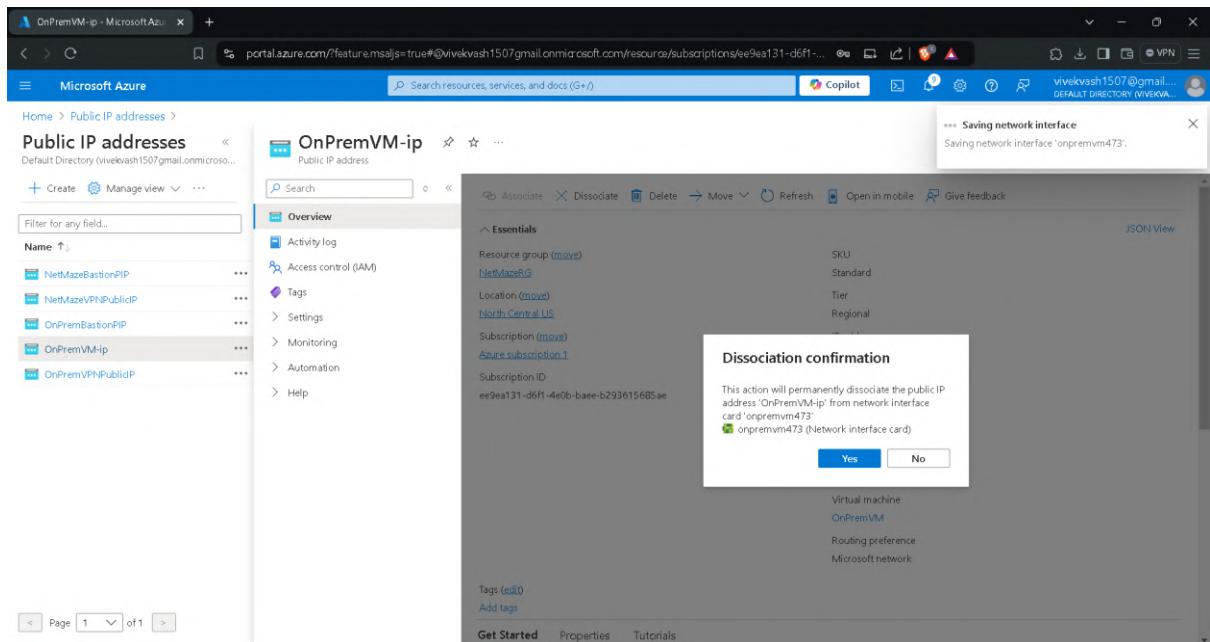
Routing preference Microsoft network

Tags (edit) Add tags

Get Started Properties Tutorials

Page 1 of 1

JSON View



OnPremVM-ip - Microsoft Azure

Home > Public IP addresses >

### Public IP addresses

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

- NetMazeBastionPIP
- NetMazeVPNPublicIP
- OnPremBastionPIP
- OnPremVM-ip**
- OnPremVPNPublidP

Search

Overview

Associate Dissociate Delete Move Refresh Open in mobile Give feedback

Delete public IP address

Do you want to delete the public IP address 'OnPremVM-ip'?

Yes No

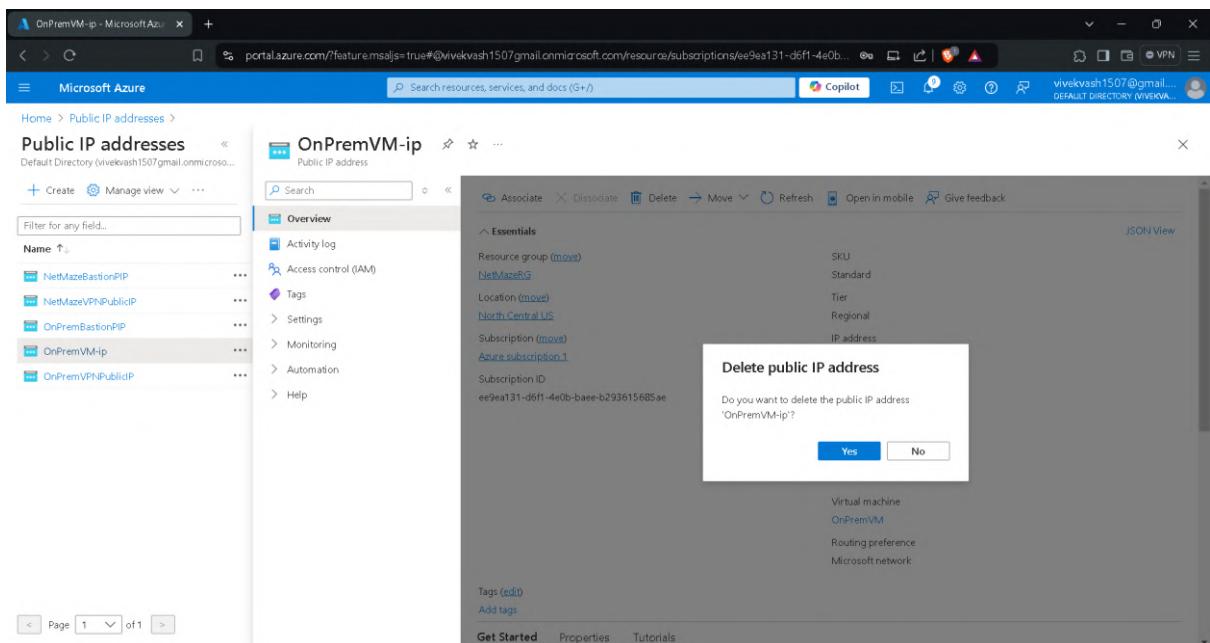
Virtual machine OnPremVM

Routing preference Microsoft network

Tags (edit) Add tags

Get Started Properties Tutorials

Page 1 of 1



Public IP addresses - Microsoft Azure

Microsoft Azure

Public IP addresses

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

No grouping List view

Show 1 to 4 of 4 records.

Name	Resource group	Location	Subscription
NetMazeBastionPIP	NetMazeRG	Canada Central	Azure subscription 1
NetMazeVPNPIP	NetMazeRG	Canada Central	Azure subscription 1
OnPremBastionPIP	NetMazeRG	North Central US	Azure subscription 1
OnPremVPNPIP	NetMazeRG	North Central US	Azure subscription 1

< Previous Page 1 of 1 Next >

Give feedback

AdminVM - Microsoft Azure

Microsoft Azure

Virtual machines > AdminVM

Virtual machines

Default Directory (vivekvash1507@gmail.onmicrosoft.com)

+ Create Switch to classic

Filter for any field...

Name

- AdminVM
- DatabaseVM
- OnPremVM
- WebAppVM

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Connect Connect Bastion Windows Admin Center Networking Network settings Load balancing Application security groups Network manager Settings Disks Extensions + applications

Using Bastion: NetMazeBastion Provisioning State: Succeeded

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Protocol: RDP SSH Port: 3389 Keyboard Language: English (US)

Authentication Type: VM Password Username: AdminUser VM Password: [REDACTED]

Show Open in new browser tab

Tell us what you think of the Bastion experience

Page 1 of 1

The screenshot shows the Windows Admin Center interface. On the left, a sidebar displays 'Device specifications' for 'AdminVM', including details like Device name, Processor, Installed RAM, and System type. A 'Rename this PC' button is visible. On the right, a main pane titled 'Windows Admin Center | All connections' lists a single item: 'adminvm [Gateway]' of type 'Servers', which has never connected. The status bar at the bottom shows the date and time as 8/21/2024 at 12:09 AM.

The screenshot shows the Microsoft Azure portal's 'Virtual machines' section. The 'DatabaseVM' virtual machine is selected. In the center, the 'Bastion' blade is open, showing connection settings for 'NetMazeBastion'. The provisioning state is 'Succeeded'. Connection settings include 'Protocol' set to 'SSH', 'Port' set to '22', 'Authentication Type' set to 'SSH Private Key from Local File', 'Username' set to 'databaseuser', and 'Local File' set to 'Databasesesskey.pem'. A 'Connect' button is present at the bottom. The status bar at the bottom shows the URL as https://portal.azure.com/?feature-msaljs=true#vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-...

The screenshot shows a terminal window titled "DatabaseVM - Microsoft Azure". The user is connected via SSH to a MySQL monitor on a Ubuntu 22.04.1 server. The session starts with the MySQL prompt:

```
databaseuser@DatabaseVM:~$ sudo mysql -u root -p
```

After entering the password, the MySQL monitor displays the following information:

```
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 15
Server version: 8.0.39-Ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

The user then runs the command:

```
mysql> SHOW DATABASES;
```

which lists the available databases:

```
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| sys |  
+-----+  
4 rows in set (0.00 sec)
```

Finally, the user exits the MySQL monitor:

```
mysql> 
```

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the "Virtual machines" section, specifically focusing on the "Bastion" connection settings for a "WebAppVM".

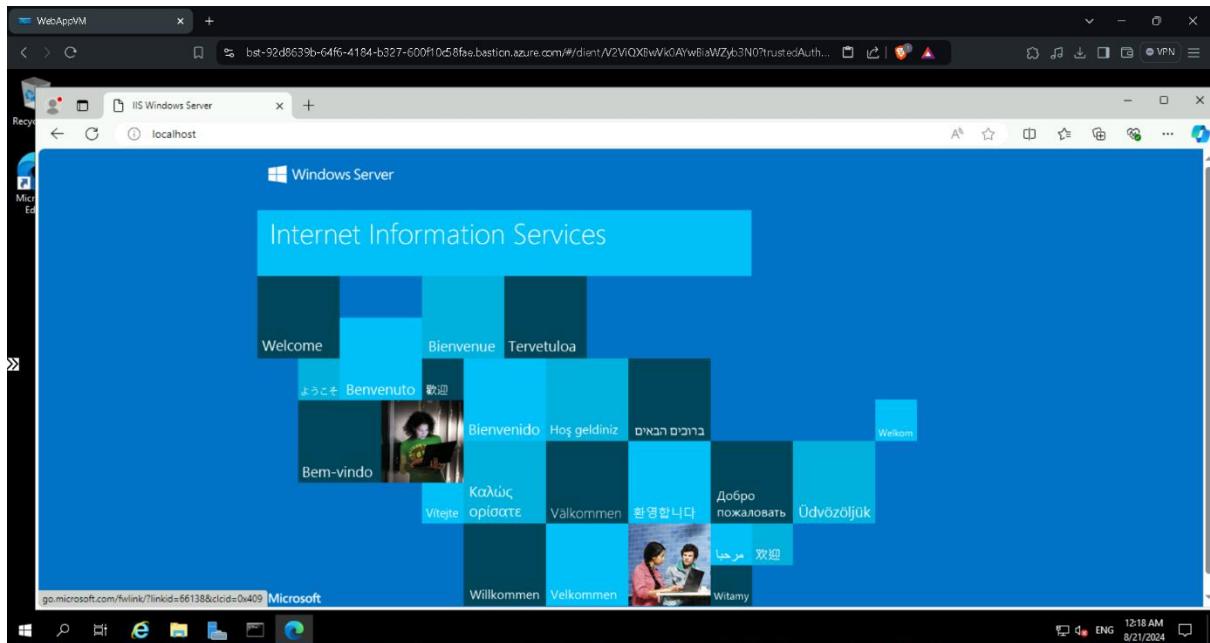
The left sidebar shows a list of virtual machines: AdminVM, DatabaseVM, OnPremVM, and WebAppVM. The "WebAppVM" is selected.

The main pane displays the "WebAppVM | Bastion" configuration page. It includes a search bar, a navigation bar with "Copilot", and a message about using Bastion with "NetMazeBastion".

The "Provisioning State" is listed as "Succeeded". Below it, there are fields for "Connection Settings": "Protocol" (set to RDP), "Port" (set to 3389), and "Keyboard Language" (set to English (US)).

The "Authentication Type" dropdown is set to "VM Password". The "Username" field contains "webuser" and the "VM Password" field contains a masked password. A "Show" button is present next to the password field. A checkbox for "Open in new browser tab" is checked.

At the bottom, there is a feedback link: "Tell us what you think of the Bastion experience".



The screenshot shows the Microsoft Azure portal with the URL "portal.azure.com/?feature\_msajs=true#@" in the address bar. The user is navigating through the "Virtual networks" section, specifically the "OnPremVNet" resource. On the left, there's a sidebar with various options like Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peerings, and Service endpoints. The "Subnets" option is currently selected. The main content area is titled "Add a subnet" and contains a form for configuring a subnet. It includes fields for "Name" (set to "AzureBastionSubnet"), "Subnet purpose" (set to "Azure Bastion"), "IPv4" (with a range of "10.1.0.0/16" and "Starting address" of "10.1.4.0"), and "IPv6" (with a note that "This virtual network has no IPv6 address ranges"). There's also a "Private subnet" section with a preview note about enhancing security. At the bottom, there are "Add" and "Cancel" buttons, and a "Give feedback" link.

Create a Bastion - Microsoft Azure

portal.azure.com/?feature.msaljs=true#view/Microsoft\_Azure\_HybridNetworking/CreateBastionHostBlade/\_provisioning...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (vivekvash1507@gmail...)

Home > Virtual networks > OnPremVNet | Bastion >

## Create a Bastion

Validation passed

Basics Advanced Tags **Review + create**

Summary

Basics

Name	OnPremBastion
Subscription	Azure subscription 1
Resource group	NetMazeRG
Region	North Central US
Availability zone	None
Virtual network	OnPremVNet
Tier	Standard
Subnets	AzureBastionSubnet
Public IP address	OnPremBastionPIP
Instance count	2
Copy and paste	Enabled
IP-based connection	Enabled
Kerberos authentication	Disabled
Shareable Link	Disabled
Session recording (Preview)	Disabled
Native client support	Disabled
Private Bastion	Disabled

Create Previous Next Download a template for automation

OnPremBastion - Microsoft Azure

portal.azure.com/?feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-4e0b-b293615685ae...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (vivekvash1507@gmail...)

Home > Microsoft.BastionHost-20240820183340 | Overview >

## OnPremBastion

Bastion

Connect Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Automation

Help

Essentials

Resource group (move)	: NetMazeRG
Location	: North Central US
Subscription (move)	: Azure subscription 1
Subscription ID	: ee9ea131-d6f1-4e0b-b293615685ae

Virtual network/subnet : OnPremVNet/AzureBastionSubnet

Public DNS name : bst-b1d4e42b-41fd-45c1-b35f-9b7404c4b132.bastion.azure.com

Public IP address : OnPremBastionPIP

Tier : Standard

Provisioning state : Succeeded

Availability zone : None

Tags (edit) : Add tags

Sessions Tutorials

SessionId	StartTime (UTC)	TargetSubscriptionId	ResourceType	TargetHostName	TargetResourceGro...	UserName	TargetIPAddress	Protocol
No results.								

OnPremVM - Microsoft Azure

Microsoft Azure

Home > OnPremVM

OnPremVM | Bastion

Virtual machine

Using Bastion: OnPremBastion

Provisioning State: Succeeded

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Protocol: RDP

Port: 3389

Keyboard Language: English (US)

Authentication Type: VM Password

Username: vashishtvivek

VM Password: [REDACTED]

Show

Open in new browser tab

Tell us what you think of the Bastion experience

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

OnPremVM - Microsoft Azure

OnPremVM

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.6189]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\vashishtvivek>ping 10.0.1.4

Pinging 10.0.1.4 with 32 bytes of data:
Reply from 10.0.1.4: bytes=32 time=18ms TTL=128
Reply from 10.0.1.4: bytes=32 time=17ms TTL=128
Reply from 10.0.1.4: bytes=32 time=18ms TTL=128
Reply from 10.0.1.4: bytes=32 time=18ms TTL=128

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 18ms, Average = 17ms

C:\Users\vashishtvivek>
```

About

Device specifications

Device name	OnPremVM
Processor	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz 2.29 GHz
Installed RAM	1.00 GB
Device ID	BA62BCD-BA55-48D2-A667-04C315D6C4D1
Product ID	00430-00000-00000-AA250
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Rename this PC

IIS Windows Server

http://10.0.1.4/

Windows Server

Internet Information Services

Welcome Bienvenue Tervetuloa

ようこそ Benvenuto 歡迎

Bem-vindo Bienvenido Hoş geldiniz ברוכים הבאim

Колұс Viteje орләтте Välkommen 환영합니다 مرحباً 欢迎

Willkommen Velkommen Witamy

Welkom

Microsoft

12:45 AM 8/21/2024 ENG

# **Private Access to Azure PaaS Services**

## **7.1. Configuring the Private Link Subnet**

### **7.1.1. Adding the SQLPrivateLink Subnet**

To securely access Azure PaaS services, such as Azure SQL Database, over a private endpoint within my VNet, I needed to configure a dedicated subnet for Azure Private Link.

- I logged into the Azure portal and navigated to the Virtual Networks section.
- I selected NetMazeVNet and then went to the Subnets tab.
- I clicked on + Subnet to create a new subnet.
- I entered the following details:
  - Name: SQLPrivateLinkSubnet
  - IPv4 Address Range: 10.0.5.0/24
- I clicked on OK to finalize the subnet creation.

## **7.2. Deploying the Azure SQL Database**

### **7.2.1. Creating the SQL Database**

Next, I proceeded to deploy an Azure SQL Database within the NetMazeVNet. This database would later be accessed securely via Azure Private Link.

- In the Azure portal, I navigated to the SQL Databases section and clicked on + Create.
- I entered the following configurations:
  - Resource Group: NetMazeRG
  - Region: Canada Central
  - Server: (new) netmazesqlserver
  - Authentication Method: Use SQL authentication
  - Server Admin Login: sqladmin
  - Password: Entered a secure password
  - Compute + Storage: General Purpose - Serverless: Standard-series (Gen5), 2 vCores, 32 GB Storage, zone-redundant disabled
- I opted for the default settings for other configurations and clicked on Create to deploy the NetMazeSQLDB.

## 7.3. Configuring Azure Private Link

### 7.3.1. Creating a Private Endpoint

To ensure that the Azure SQL Database can be accessed securely within the VNet, I configured an Azure Private Link by creating a private endpoint.

- In the Azure portal, I searched for the Private Link Center and navigated to the Private Endpoints tab.
- I clicked on + Create to set up a new private endpoint.
- I entered the following configurations:
  - Resource Group: NetMazeRG
  - Network Interface Name: SQLPrivateLink-nic
  - Region: Canada Central
- In the Resource tab:
  - Connection Method: Connect to an Azure Resource in my directory
  - Resource Type: MicrosoftSql/servers
  - Resource: netmazesqlserver
  - Target Sub-resource: sqlServer
- In the Virtual Network tab:
  - Virtual Network: NetMazeVNet (NetMazeRG)
  - Subnet: SQLPrivateLinkSubnet
- In the DNS tab:
  - Integrate with private DNS zone: Yes
  - I deployed the Private DNS zone within NetMazeRG.
- I clicked on Create to finalize the deployment of the private endpoint named SQLPrivateLink.

## 7.4. Testing Connectivity to Azure SQL Database

### 7.4.1. Verifying SQL Database Connectivity via Private Link

To verify the secure connectivity to the NetMazeSQLDB via Azure Private Link, I conducted a connectivity test from the AdminVM.

- I navigated to AdminVM in the Virtual Machines section of the Azure portal.
- I accessed the Bastion tab, entered the credentials (Username and VM Password), and clicked on Connect.
- After connecting to AdminVM, I installed the Microsoft Command Line Utilities for SQL Server.
- I opened Windows PowerShell (Administrator) and verified the installation with the following command:

```
sqlcmd --version
```

- I then connected to NetMazeSQLDB using the following commands:

```
sqlcmd -S netmazesqlserver.database.windows.net -U sqladmin -P <YourPassword>
```

- To confirm the connection, I executed the following SQL command to list the databases:

```
1> SELECT name FROM sys.databases;  
2> GO
```

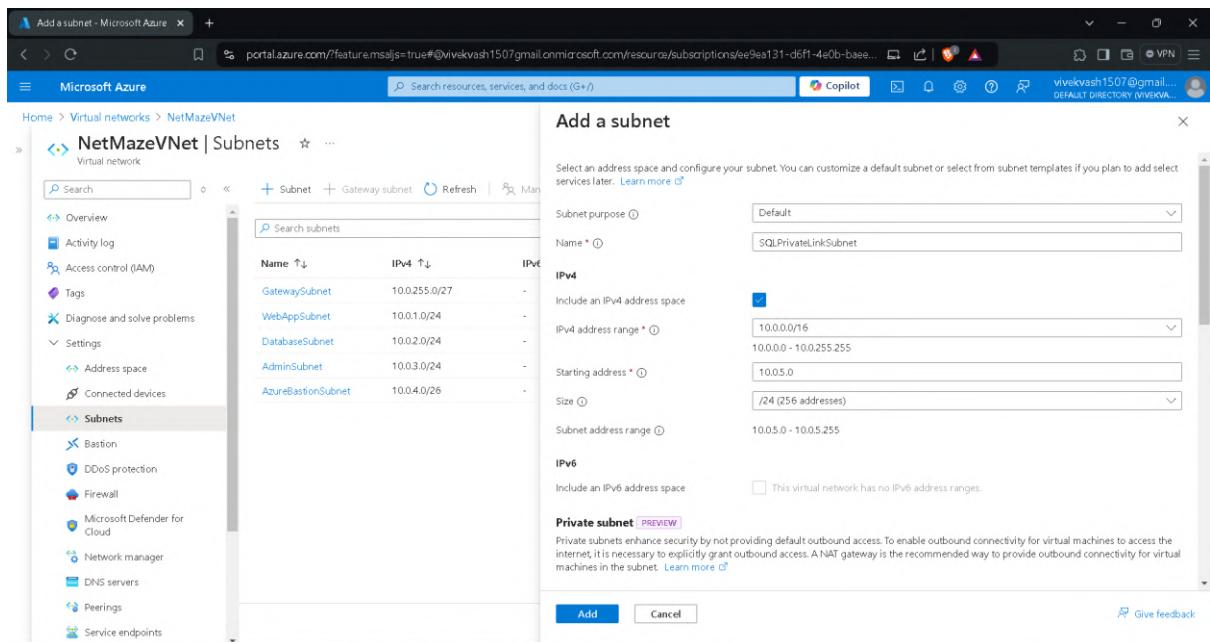
- The output confirmed the existence of the NetMazeSQLDB database.

```
master  
NetMazeSQLDB
```

```
(2 rows affected)
```

In this phase of the project, I successfully implemented Azure Private Link to securely access the Azure SQL Database within the NetMazeVNet. The process involved configuring a dedicated subnet for the private link, deploying the SQL database, and setting up a private endpoint. The connectivity was verified to ensure that the database could be accessed securely over the private network without traversing the public internet.

## Screenshots



NetMazeVNet - Microsoft Azure

portal.azure.com/?feature.msaljs=true#blade/HubExtension/BrowseResourceBlade/r...

vivekvash1507@gmail...  
DEFAULT DIRECTORY (vivekvash1507@gmail.com)

Microsoft Azure

NetMazeVNet | Subnets

Virtual network

All Services (32) Marketplace (31) More (4)

Services

Subnet Gateway subnet

Search subnets

Name ↑↓ IPv4

GatewaySubnet 10.0.0.0/16

WebAppSubnet 10.0.1.0/16

DatabaseSubnet 10.0.2.0/16

AdminSubnet 10.0.3.0/16

AzureBastionSubnet 10.0.4.0/16

SQLPrivateLinkSubnet 10.0.5.0/16

Marketplace

See more

SQL databases

SQL servers

SQL elastic pools

SQL managed instances

SQL Database

Azure SQL

Azure Synapse Analytics

SQL server (logical server)

Documentation

Create a single database - Azure SQL Database

Import a bacpac file to create a database in Azure SQL Database - Azure SQL Data...

Connect to Azure SQL with Microsoft Entra authentication and SqlClient - ADO.NET...

Continue searching in Microsoft Entra ID

Give feedback

https://portal.azure.com/?feature.msaljs=true#blade/HubExtension/BrowseResourceBlade/r...

Create SQL Database Server - Microsoft Azure

portal.azure.com/?feature.msaljs=true#view/SqAzureExtension/SharedCreateServer/sNewServer~/true/subscriptionId/e9ea131-d6f1-4e0b-bae...

vivekvash1507@gmail...  
DEFAULT DIRECTORY (vivekvash1507@gmail.com)

Microsoft Azure

Home > SQL databases > Create SQL Database

Create SQL Database Server

Server details

Enter required settings for this server, including providing a name and location. This server will be created in the same subscription and resource group as your database.

Server name \*

netmazesqlserver

database.windows.net

Location \*

(Canada) Canada Central

Authentication

Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

Select your preferred authentication methods for accessing this server. Create a server admin login and password to access your server with SQL authentication, select only Microsoft Entra authentication [Learn more](#) using an existing Microsoft Entra user, group, or application as Microsoft Entra admin [Learn more](#), or select both SQL and Microsoft Entra authentication.

Authentication method

Use Microsoft Entra-only authentication

Use both SQL and Microsoft Entra authentication

OK

Screenshot of the Microsoft Azure portal showing the "Create SQL Database Server" page. The location is set to "Canada (Canada Central)". Under "Authentication", the "Use SQL authentication" option is selected. The server admin login is "sqladmin", and the password is "\*\*\*\*\*". The confirm password field also contains "\*\*\*\*\*". A note at the top states: "Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)".

Screenshot of the Microsoft Azure portal showing the "Create SQL Database" page. The "Review + create" tab is selected. The "Product details" section shows a "SQL database by Microsoft" and the "Estimated cost" is "Storage cost 0.00 USD / month + Compute cost 0.000000 USD / vCore second". The "Cost summary" section shows a "General Purpose (GP\_S\_Gen5\_2)" configuration with "0.00 USD" cost per GB. The "Overage billing" is "Disabled". The "Terms" section contains legal disclaimers. At the bottom, there are "Create" and "Previous" buttons, and a link to "Download a template for automation".

**Create SQL Database**

**Basics**

Subscription	Azure subscription 1
Resource group	NetMazeRG
Region	Canada Central
Database name	NetMazeSQLDB
Server	(new) netmazerqlserver
Authentication method	SQL authentication
Server admin login	sqladmin
Compute + storage	General Purpose - Serverless: Standard-series (Gen5), 2 vCores, 32 GB storage, zone redundant disabled
Backup storage redundancy	Locally-redundant backup storage
Overage billing	Disabled

**Networking**

Allow Azure services and resources to access this server	No
Private endpoint	None
Minimum TLS version	1.2
Connection Policy	Default

**Security**

[Create](#) [< Previous](#) [Download a template for automation](#)

**Create SQL Database**

**Security**

Identity	Not enabled
Transparent data encryption (Server level)	Service-managed key selected
Database level customer-managed key	Not configured
Database level user assigned managed identity	Not configured
Advanced data security	Not now
Always encrypted with secure enclaves	Not configured
Sql Ledger(Database)	Disabled
Digest Storage	Disabled

**Additional settings**

Use existing data	Blank
Collation	SQL_Latin1_General_CI_AS
Maintenance window	System default (5pm to 8am)

**Tags**

[Create](#) [< Previous](#) [Download a template for automation](#)

Microsoft Azure

NetMazeSQLDB (netmazesqlserver/NetMazeSQLDB) Overview

SQL database

Search Copy Restore Export Set server firewall Delete Connect with... Feedback

Overview Essentials

Activity log Resource group (move) : NetMazeRG Status : Online Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae-b239615685ae Server name : netmazesqlserver.database.windows.net Connection strings : Show database connection strings Pricing tier : Free - General Purpose - Serverless: Gen5, 2 vCores Overage billing : Disabled Free monthly vCore amo... : 100,000 vCore seconds remaining Earliest restore point : No restore point available

Tags (edit) : Add tags

Getting started Monitoring Properties Features Notifications (0) Integrations Tutorials

Start working with your database

Configure access Connect to application Start developing Mirror database in Fabric

Configure network access to your SQL server. Learn more Use connection strings to connect to your SQL database from your applications and favorite tools. Work in your database by using tools to add, modify and query data. Compare tools Replicate existing databases in Fabric, and help your team achieve streamlined ETL and operational analytics goals. Learn more

Microsoft Azure

netmazesqlserver - Microsoft Azure

All services > Resource groups > NetMazeRG > SQLPrivateLink

netmazesqlserver SQL server

Create database New elastic pool New dedicated SQL pool (formerly SQL DW) Import database Reset password Move Delete Feedback

Overview Essentials

Activity log Resource group (move) : NetMazeRG Status : Available Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae-b239615685ae Server admin : sqladmin Networking : Show networking settings Microsoft Entra admin : Not configured Server name : netmazesqlserver.database.windows.net

Tags (edit) : Add tags

Notifications (0) Features (6)

All Security (4) Performance (1) Recovery (1)

<b>Microsoft Entra admin</b> Allows you to centrally manage identity and access to your Azure SQL databases. NOT CONFIGURED	<b>Microsoft Defender for SQL</b> Vulnerability Assessment and Advanced Threat Protection. NOT CONFIGURED	<b>Automatic tuning</b> Monitors and tunes your database automatically to optimize performance. CONFIGURED
<b>Auditing</b> Track database events and writes them to an audit log in Azure storage. NOT CONFIGURED	<b>Failover groups</b> Automatically manages replication, connectivity and failover for a set of databases. NOT CONFIGURED	<b>Transparent data encryption</b> Encryption at rest for your databases, backups, and logs. SERVICE-MANAGED KEY

Microsoft Azure

NetMazeSQLDB (netmazesqlserver/Net)

Overview

Activity log

Tags

Diagnose and solve problems

Query editor (preview)

Mirror database in Fabric (preview)

Compute + storage

Connection strings

Maintenance

Properties

Locks

Data management

Replicas

Sync to other databases

Integrations

Configure access

Configure network access to your SQL server. Learn more

Use connection strings to connect to your SQL database from your applications and favorite tools.

Work in your database by using tools to add, modify and query data. Compare tools

Give feedback

What is Azure Private Link?

Configure your private link - Azure Monitor

Enable Azure Private Link as a simplified deployment - Azure Databricks

Continue searching in Microsoft Entra ID

Private link services

Private Link

Azure Arc Private Link Scopes

Azure Monitor Private Link Scopes

Marketplace

Private Link Service (Your Service)

Azure Monitor Private Link Scope

Azure Synapse Analytics (private link hubs)

Azure Arc Private Link Scope

Documentation

What is Azure Private Link?

Configure your private link - Azure Monitor

Enable Azure Private Link as a simplified deployment - Azure Databricks

base

Mirror database in Fabric

Replicate existing databases in Fabric, and help your team achieve streamlined ETL and operational analytics goals. Learn more

https://portal.azure.com/?feature.msaljs=true#/blade/Microsoft\_Azure\_Network/PrivateLinkC...

Microsoft Azure

Private Link Center | Private endpoints

Search resources, services, and docs (G+)

Create Manage view Refresh Export to CSV Open query Assign tags Delete Generate hostfile

Subscription equals all Resource group equals all Location equals all Add filter

No grouping List view

Private endpoints

Private link services

Azure Arc private link scopes

Azure Monitor private link scopes

Resources

Active connections

Supported resources

< >

No private endpoints to display

Try changing or clearing your filters.

Learn more

Give feedback

[Create a private endpoint - Microsoft Azure](#)

portal.azure.com/?feature.msals=true#view/Microsoft\_Azure\_Network/CreatePrivateEndpointBlade

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekvash1507)

Home > Private Link Center | Private endpoints >

## Create a private endpoint

Basics Resource Virtual Network DNS Tags Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

**Project details**

Subscription \*  ✓

Resource group \*  ✓

[Create new](#)

**Instance details**

Name \*  ✓

Network Interface Name \*  ✓

Region \*  ✓

< Previous Next : Resource >

[Create a private endpoint - Microsoft Azure](#)

portal.azure.com/?feature.msals=true#view/Microsoft\_Azure\_Network/CreatePrivateEndpointBlade

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekvash1507)

Home > Private Link Center | Private endpoints >

## Create a private endpoint

Basics Resource Virtual Network DNS Tags Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method:

Connect to an Azure resource in my directory.

Connect to an Azure resource by resource ID or alias.

Subscription \*  ✓

Resource type \*  ✓

Resource \*  ✓

Target sub-resource \*  ✓

< Previous Next : Virtual Network >

[Create a private endpoint - Microsoft Azure](#)

portal.azure.com/?feature.msaljs=true#view/Microsoft\_Azure\_Network/CreatePrivateEndpointBlade

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Private Link Center | Private endpoints >

## Create a private endpoint

Basics Resource Virtual Network DNS Tags Review + create

**Networking**

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network: NetMazeVNet (NetMazeRG) ✓

Subnet \*: SQLPrivateLinkSubnet ✓

Network policy for private endpoints: Disabled (edit)

**Private IP configuration**

Dynamically allocate IP address

Statically allocate IP address

**Application security group**

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

+ Create

Application security group

< Previous Next : DNS >

[Create a private endpoint - Microsoft Azure](#)

portal.azure.com/?feature.msaljs=true#view/Microsoft\_Azure\_Network/CreatePrivateEndpointBlade

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Private Link Center | Private endpoints >

## Create a private endpoint

Basics Resource Virtual Network DNS Tags Review + create

**Private DNS integration**

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone:  Yes  No

Configuration name: privatelink-database-wind...

Subscription: Azure subscription 1

Resource group: NetMazeRG

Private DNS zone: (new) privatelink.database...

< Previous Next : Tags >

SQLPrivateLink - Microsoft Azure

portal.azure.com/?feature.msals=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-4e0b... Copilot VPN

Microsoft Azure

Home > Microsoft.PrivateEndpoint-20240820215626 | Overview >

SQLPrivateLink

Private endpoint

Search Delete Refresh

Overview

Activity log Access control (IAM) Tags Diagnose and solve problems Settings Monitoring Automation Help

Resource group (move) : NetMazeRG Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae6-b293615685ae Provisioning state : Succeeded

Virtual network/subnet : NetMazeVNet/SQLPrivateLinkSubnet Network interface : SQLPrivateLinkNIC Private link resource : netmazegsqlserver Target sub-resource : sqlServer Connection status : Approved Request/Response : Auto-approved

Tags (edit) : Add tags JSON View

Give feedback

AdminVM - Microsoft Azure

portal.azure.com/?feature.msals=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/ee9ea131-d6f1-4e0b... Copilot VPN

Microsoft Azure

All services > Resource groups > NetMazeRG >

AdminVM

Virtual machine

Search Connect Start Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

Activity log Access control (IAM) Tags Diagnose and solve problems Connect Connect Bastion Windows Admin Center Networking Network settings Load balancing Application security groups Network manager

Settings Disks Extensions + applications

Advisors (1 of 1): Enable Trusted Launch foundational excellence, and modern security for Existing Generation 2 VM(s) →

Essentials

Resource group (move) : NETMAZERG Status : Running Location : Canada Central Subscription (move) : Azure subscription 1 Subscription ID : ee9ea131-d6f1-4e0b-bae6-b293615685ae

Operating system : Windows (Windows Server 2019 Datacenter) Size : Standard D2s v3 (2 vcpus, 8 GiB memory) Public IP address : - Virtual network/subnet : NetMazeVNet/AdminSubnet DNS name : - Health state : - Time created : 8/20/2024, 4:32 AM UTC

Tags (edit) : Add tags

Properties Monitoring Capabilities (8) Recommendations (1) Tutorials

Virtual machine

Computer name : AdminVM Operating system : Windows (Windows Server 2019 Datacenter) VM generation : V2 VM architecture : x64 Agent status : Ready

Networking

Public IP address : - Private IP address : 10.0.3.4 Virtual network/subnet : NetMazeVNet/AdminSubnet

AdminVM - Microsoft Azure

Microsoft Azure

All services > Resource groups > NetMazeRG > AdminVM

AdminVM | Bastion

Using Bastion: NetMazeBastion

Provisioning State: Succeeded

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Protocol: RDP

Port: 3389

Keyboard Language: English (US)

Authentication Type: VM Password

Username: AdminUser

VM Password: [REDACTED]

Show

Open in new browser tab

Tell us what you think of the Bastion experience

AdminVM - Microsoft Azure

AdminVM

bst-92d0639b-64f6-4184-b327-600f10x58fae.bastion.azure.com/#/client/QWRtaW5WTQBAJG/pZn/vCQ=?trustedAuthority...

Download Microsoft® Command Line Utilities 14.0 for SQL Server®

Maximize the everyday with Microsoft 365

Get online protection, secure cloud storage, and innovative apps designed to fit your needs—all in one plan.

For 1 person   For up to 6 people

Microsoft | Download Center Windows Office Web browsers Developer tools Xbox

All Microsoft Search Cart Sign in

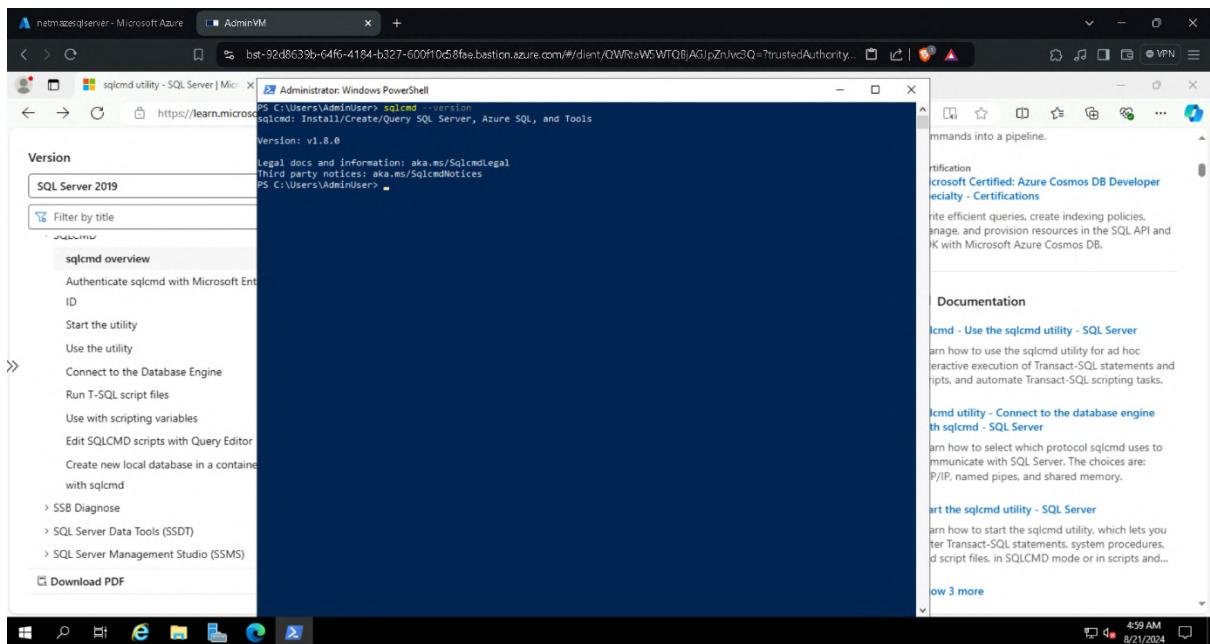
Important! Selecting a language below will dynamically change the complete page content to that language.

Select language English Download

Back To Top

Microsoft Command Line Utilities 14.0 for SQL Server

4:38 AM ENG 8/21/2024



```
Administrator: Windows PowerShell
PS C:\Users\AdminUser> sqlcmd -version
sqlcmd: Install/Create/Query SQL Server, Azure SQL, and Tools
Version: v1.8.0
Legal docs and information: aka.ms/SqlcmdLegal
Third party notices: aka.ms/SqlcmdNotices
PS C:\Users\AdminUser>
```

The screenshot shows a Windows PowerShell window with the following details:

- Title Bar:** AdminVM
- Content Area:**

```
Administrator: Windows PowerShell
PS C:\Users\AdminUser> sqlcmd -version
sqlcmd: Install/Create/Query SQL Server, Azure SQL, and Tools
Version: v1.8.0
Legal docs and information: aka.ms/SqlcmdLegal
Third party notices: aka.ms/SqlcmdNotices
PS C:\Users\AdminUser> sqlcmd -S netmazesqlserver.database.windows.net -U sqladmin -P [REDACTED]
PS C:\Users\AdminUser> SELECT name FROM sys.databases;
PS C:\Users\AdminUser> GO
Name
-----
master
model
msdb
tempdb
netmazesQLDB
(2 rows affected)
1>
```
- Bottom Status Bar:** 4: 9:13 AM 8/24/2024

# **DNS and Load Balancing**

## 8.1. Configuring Azure Load Balancer

### 8.1.1. Creating the Load Balancer

To distribute traffic across the virtual machines (VMs) in the WebApp Subnet, I implemented an Azure Load Balancer.

- I logged into the Azure portal and navigated to the Load Balancers section.
- I clicked on + Create to start the load balancer creation process.
- In the Basics tab, I entered the following details:
  - Resource Group: NetMazeRG
  - Region: Canada Central
  - SKU: Standard (Recommended)
  - Type: Internal
- In the Frontend IP Configuration tab:
  - Name: InternalFrontendIP
  - Type: Private
  - Virtual Network: NetMazeVNet
  - Subnet: WebAppSubnet (10.0.1.0/24)
  - Assignment: Static
  - IP Address: 10.0.1.10
- In the Backend Pools tab, I configured the backend pool:
  - Backend Pool Name: WebAppPool
  - Virtual Network: NetMazeVNet
  - Backend Pool Configuration: NIC
- I added the IP configurations for the WebAppVM:
  - Resource Name: WebAppVM
  - Resource Group: NetMazeRG
  - Type: Virtual Machine
  - IP Configuration: ipconfig1
  - IP Address: 10.0.1.4
- In the Inbound Rules tab:
  - Rule Name: HTTPRule
  - IP Version: IPv4
  - Frontend IP Address: InternalFrontendIP (10.0.1.10)
  - Backend Pool: WebAppPool
  - Protocol: TCP
  - Port: 80
  - Backend Port: 80
  - Health Probe: HTTPProbe (TCP:80) (Created during configuration)
  - Session Persistence: None
  - Idle Timeout (Minutes): 4

- After entering all the details, I clicked on Review + Create and then Create to deploy the NetMazeLoadBalancer.

## 8.2. Configuring Private DNS Zone

### 8.2.1. Creating the Private DNS Zone

To manage custom domain names for resources within the VNet, I configured a Private DNS Zone.

- In the Azure portal, I navigated to the Private DNS Zones section and clicked on + Create.
- I entered the following configurations:
  - Resource Group: NetMazeRG
  - Name: netmaze.local
  - Region: Canada Central
- I clicked on Create to deploy the DNS zone.

### 8.2.2. Linking the DNS Zone to the Virtual Network

After creating the Private DNS Zone, I linked it to the NetMazeVNet to ensure automatic registration of VMs.

- I navigated to the Virtual Network Links tab within the netmaze.local DNS zone and clicked on + Add.
- I entered the following details:
  - Link Name: NetMazeVNetLink
  - Virtual Network: NetMazeVNet (NetMazeRG)
  - Enable Auto Registration: Ticked
- I clicked on Create to finalize the link. The NetMazeVNetLink was successfully created with the status Completed.

## 8.3. Verifying DNS Configuration

### 8.3.1. Testing DNS Resolution

To ensure that the DNS configuration was successful and that the VMs were properly registered within the DNS zone, I performed a DNS resolution test.

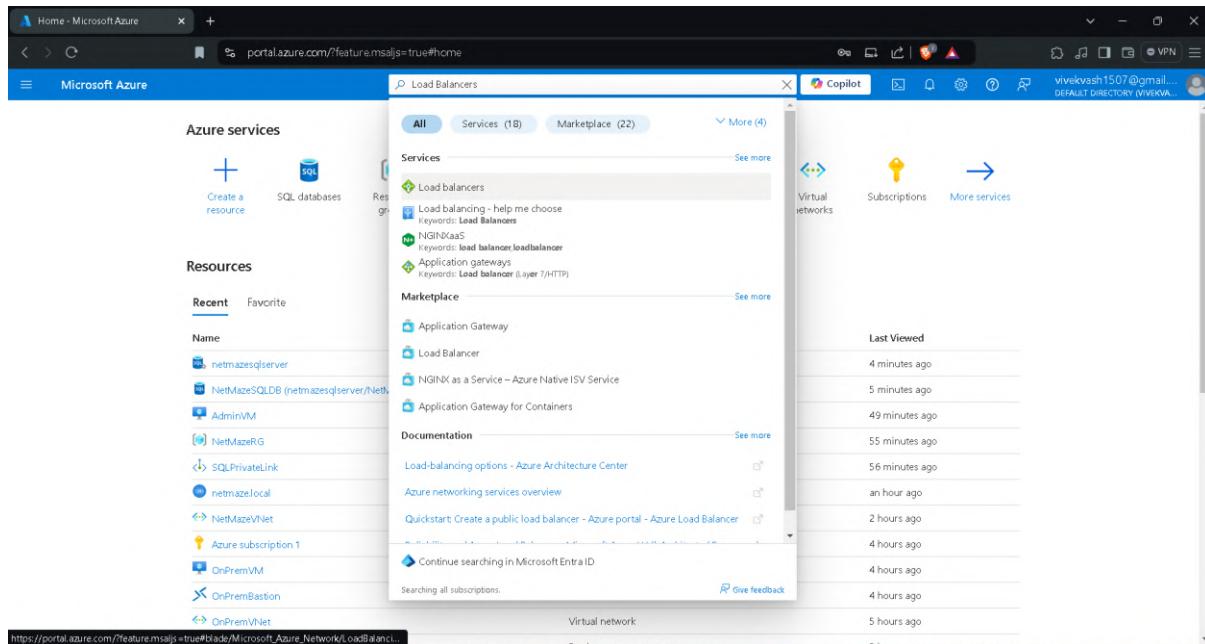
- I used Bastion to connect to the AdminVM.
- I opened the Command Prompt in the AdminVM and ran the following command:

```
nslookup webappvm.netmaze.local
```

- The command successfully returned the private IP address of the WebAppVM (10.0.1.4), confirming that the DNS setup was correctly configured.

In this phase, I successfully configured Azure DNS and implemented a load balancer to distribute traffic across the WebApp Subnet. The process included setting up a Private DNS Zone, linking it to the VNet, and configuring the Azure Load Balancer to manage traffic. The configurations were verified through DNS resolution testing, ensuring that all resources were correctly registered and accessible within the private network.

## Screenshots



**Load balancing - Microsoft Azure**

Microsoft Azure

Load balancing | Load Balancer

Search  + Create Manage view Refresh Export to CSV Open query Assign tags

Overview Load Balancing Services Application Gateway Front Door and CDN profiles Load Balancer Traffic Manager

Subscription equals all Resource group equals all Location equals all Filter for  Create Add filter No grouping List view

Showing 0 to 0 of 0 records.

Name ↑ Resource group ↑ Location ↑ Subscription ↑

No load balancers to display

Azure Load Balancer enables your applications to be highly available and scalable. You can scale up and down based on your traffic patterns. Azure Load Balancer is best suited for network traffic requiring high performance and ultra-low latency.

Learn more about Load balancers

Give feedback

This screenshot shows the Microsoft Azure portal's Load Balancer management page. The left sidebar has 'Load Balancer' selected under 'Load Balancing Services'. The main area displays a message stating 'No load balancers to display' with a brief description of what Azure Load Balancer does. It includes a 'Learn more about Load balancers' link and a 'Give feedback' button.

**Create load balancer - Microsoft Azure**

Microsoft Azure

Create load balancer

BASICS Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

Load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more](#).

**Project details**

Subscription \*  Resource group \*  [Create new](#)

**Instance details**

Name \*  Region \*   
 Standard (Recommended)  Gateway  Basic (Retiring soon)

Type \*  Public  Internal  Regional

Review + create < Previous Next : Frontend IP configuration > Download a template for automation Give feedback

This screenshot shows the 'Create load balancer' wizard in the Microsoft Azure portal, starting at the 'Basics' step. It requires filling out 'Project details' like subscription and resource group, and 'Instance details' such as name, region, and SKU. The 'Internal' type is chosen for the load balancer. Navigation buttons like 'Review + create' and 'Next : Frontend IP configuration >' are visible at the bottom.

[InternalFrontendIP - Microsoft Azure](https://portal.azure.com/?feature.msaljs=true#create/Microsoft.LoadBalancer-ARM)

Microsoft Azure | portal.azure.com/?feature.msaljs=true#create/Microsoft.LoadBalancer-ARM

Search resources, services, and docs (G+)

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Load balancing | Load Balancer > Create load balancer ...

Basics Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

A frontend IP configuration is an IP address used for inbound and/or outbound communication as defined within load balancing, inbound NAT, and outbound rules.

+ Add a frontend IP configuration

Name ↑↓	IP address ↑↓	Virtual network ↑↓
InternalFrontendIP	10.0.1.10	NetMazeVNet

InternalFrontendIP

NetMazeLoadBalancer

Name \* InternalFrontendIP

Type Private

Virtual network \* NetMazeVNet

Subnet \* WebAppSubnet(10.0.1.0/24)

Assignment Static

IP address \* 10.0.1.10

Availability zone \* No Zone

Used by

The list of load balancing rules, inbound NAT rules, inbound NAT pools, and outbound rules using this IP address.

Name Type

Save Cancel Give feedback

[WebAppPool - Microsoft Azure](https://portal.azure.com/?feature.msaljs=true#view/Microsoft_Azure_Network/RegionalLBBackendPoolManage.ReadView/load...)

Microsoft Azure | portal.azure.com/?feature.msaljs=true#view/Microsoft\_Azure\_Network/RegionalLBBackendPoolManage.ReadView/load...

Search resources, services, and docs (G+)

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Load balancing | Load Balancer > Create load balancer > WebAppPool ...

Name \* WebAppPool

Virtual network NetMazeVNet

Backend Pool Configuration NIC IP address

IP configurations

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

+ Add | Remove

Resource Name	Resource group	Type	IP configuration	IP Address	Availability set
WEBAPPVVM	NETMAZERG	Virtual machine	ipconfig1	10.0.1.4	-

Used by

The list of load balancing rules, inbound NAT rules, and outbound rules using this backend pool.

Save Cancel Give feedback

Create load balancer - Microsoft Azure

portal.azure.com/?feature.msaljs=true#create/Microsoft.LoadBalancer-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekva...)

Home > Load balancing | Load Balancer >

## Create load balancer

Basics Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

A backend pool is a collection of resources to which your load balancer can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, and containers.

+ Add a backend pool

Name	Virtual network	Resource Name	Network interface	IP address	Availability zone	Admin state
WebAppPool	NetMazeVNet	WEBAPPVM	webappvm824	10.0.1.4	-	None

Review + create < Previous Next : Inbound rules > Download a template for automation Give feedback

HTTPRule - Microsoft Azure

portal.azure.com/?feature.msaljs=true#create/Microsoft.LoadBalancer-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekva...)

Home > Load balancing | Load Balancer >

## Create load balancer

Basics Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

Load balancing rule

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. The load balancing rule uses a health probe to monitor the status of the backend pool instances.

+ Add a load balancing rule

Name ↑	Frontend IP configuration ↑	Backend pool ↑	Health probe ↑
HTTPRule	InternalFrontendIP	WebAppPool	HTTPProbe

Inbound NAT rule

An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.

+ Add an inbound nat rule

Name ↑	Frontend IP configuration ↑	Service ↑	Target
Add a rule to get started			

HTTPRule

NetMazeLoadbalancer

Name \* HTTPRule

IP Version \* IPv4

Frontend IP address \* InternalFrontendIP (10.0.1.10)

Backend pool \* WebAppPool

High availability ports

Protocol TCP

Port \* 80

Backend port \* 80

Health probe \* HTTPProbe (TCP:80)

Session persistence None

Idle timeout (minutes) 4

Save Cancel Give feedback

Review + create < Previous Next : Outbound rule > Download a template for automation Give feedback

NetMazeLoadBalancer - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com...  
DEFAULT DIRECTORY (VIVEKVA...)

Home > Microsoft.LoadBalancer-20240820230905 | Overview >

## NetMazeLoadBalancer

Load balancer

Move Delete Refresh Give feedback

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Automation

Help

Resource group (move) : NetMazeRG

Location : Canada Central

Subscription (move) : Azure subscription 1

Subscription ID : ee9ea131-d6f1-4e0b-baee-b293615685ae

SKU : Standard

Backend pool : WebAppPool (1 virtual machine)

Load balancing rule : HTTPRule (Tcp:80)

Health probe : HTTPProbe (Tcp:80)

NAT rules : 0 inbound

Tier : Regional

Tags (edit) : Add tags

See more

Configure high availability and scalability for your applications

Create highly-available and scalable applications in minutes by using built-in load balancing for cloud services and virtual machines. Azure Load Balancer supports TCP/UDP-based protocols and protocols used for real-time voice and video messaging applications. [Learn more](#)

Balance IPv4 and IPv6 addresses

Build highly reliable applications

Secure your networks

View frontend IP configuration

View health probes

View inbound NAT rules

[Create Private DNS Zone - Microsoft Edge](#)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekayash1507@gmail.com  
DEFAULT DIRECTORY (NIVAKA)

Home > Private DNS zones >

## Create Private DNS Zone

**Basics**   Private DNS Zone Editor   Tags   Review + Create

A Private DNS zone provides name resolution services within virtual networks. A Private DNS zone is accessible only from the virtual networks that it is linked to and can't be accessed over internet. For example you can create a Private DNS zone named contoso.com and then create DNS records like www.contoso.com in this zone. You can then link the zone to one or more virtual networks. [Learn more](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  [Create new](#)

### Instance details

Name \*

Resource group location \*

[Review + create](#)   [< Previous](#)   [Next : Private DNS Zone Editor >](#)

A Create Private DNS Zone - Microsoft Azure

portal.azure.com/?feature.msaljs=true#view/Microsoft\_Azure\_PrivateDNS/PrivateDnsZoneCreate/ReactView/\_provisioningCompleted

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Private DNS zones >

## Create Private DNS Zone

Validation passed

Basics Private DNS Zone Editor Tags Review + Create

View automation template

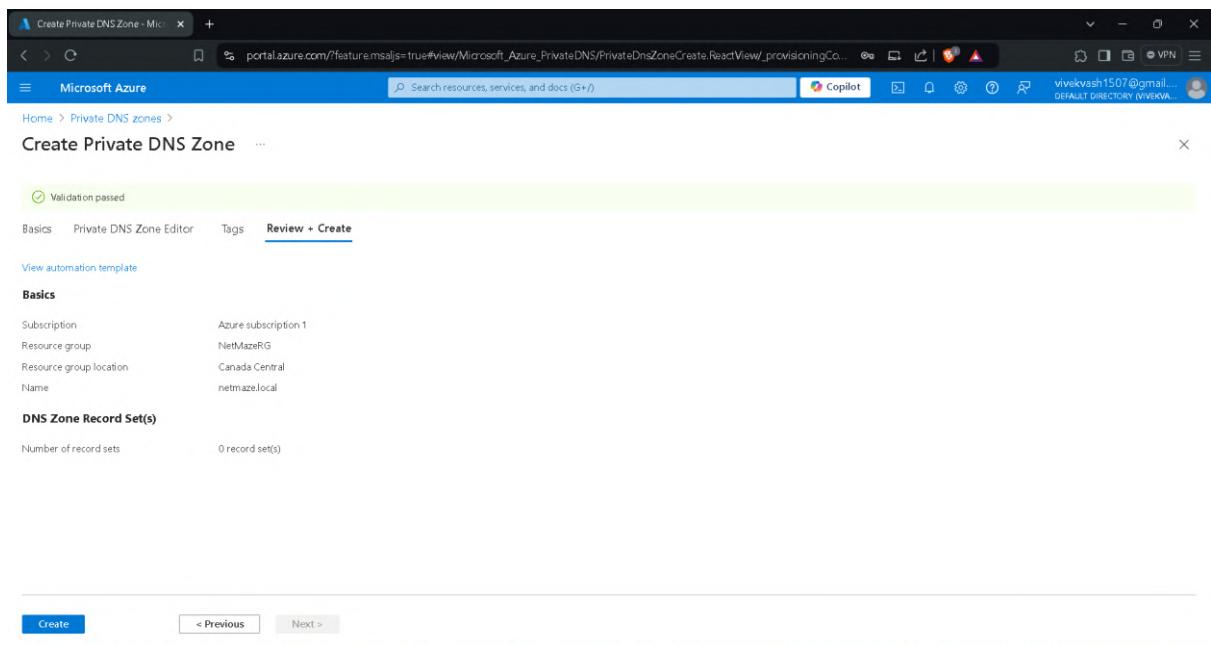
**Basics**

Subscription: Azure subscription 1  
Resource group: NetMazeRG  
Resource group location: Canada Central  
Name: netmaze.local

**DNS Zone Record Set(s)**

Number of record sets: 0 record set(s)

Create < Previous Next >



A Add Virtual Network Link - Microsoft Azure

portal.azure.com/?feature.msaljs=true#view/Microsoft\_Azure\_PrivateDNS/AddVnetLinkReactView/zoneResourceId/%2Fsubscriptions%2F

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > netmaze.local | Virtual Network Links >

## Add Virtual Network Link

netmaze.local

Link name \*: NetMazeVNetLink

**Virtual network details**

Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones. Virtual networks with Classic deployment model are not supported.

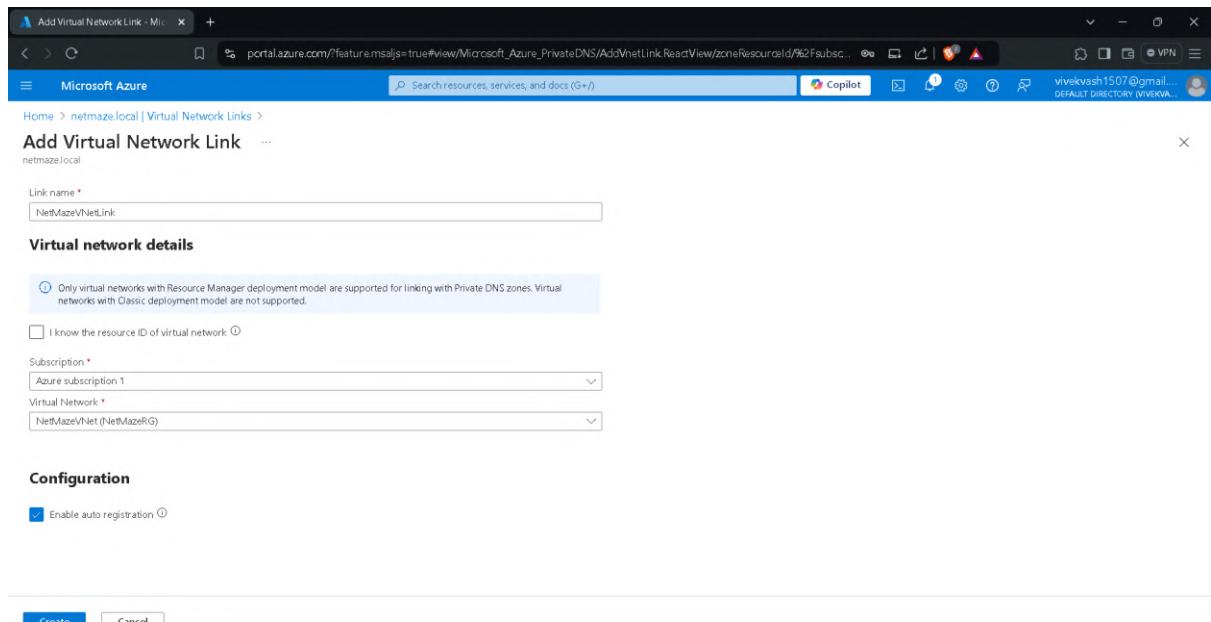
I know the resource ID of virtual network

Subscription: Azure subscription 1  
Virtual Network: NetMazeVNet (NetMazeRG)

**Configuration**

Enable auto registration

Create Cancel



netmazelocal - Microsoft Azure

Home > netmazelocal

## netmazelocal | Virtual Network Links

Private DNS zone

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Properties Locks DNS Management Recordsets Virtual Network Links Monitoring Alerts Metrics Advisor recommendations Automation CLI / PS

+ Add Refresh Delete

Search virtual network links

0 Virtual Network links selected

Link Name	Link Status	Virtual Network	Auto-Registration
netmazenetlink	Completed	NetMazeVNet	Enabled

vivekvash1507@gmail.com DEFAULT DIRECTORY (vivekva...)

netmazelocal - Microsoft Azure

Home > netmazelocal

## netmazelocal | Recordsets

Private DNS zone

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Properties Locks DNS Management Recordsets Virtual Network Links Monitoring Alerts Metrics Advisor recommendations Automation CLI / PS

Search

Fetched 8 record set(s). 0 record sets selected

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azuresprivatedns-hostmicrosft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
adminvm	A	10	10.0.3.4	True
databasevm	A	10	10.0.2.4	True
vm000000	A	10	10.0.4.4	True
vm000001	A	10	10.0.4.5	True
vpngw000000	A	10	10.0.255.4	True
vpngw000001	A	10	10.0.255.5	True
webappvm	A	10	10.0.1.4	True

vivekvash1507@gmail.com DEFAULT DIRECTORY (vivekva...)

Microsoft Azure

netmaze.local - Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekvash1507)

Home > netmaze.local

Private DNS zone

Overview

Import Export Move Refresh Delete

Essentials

Resource group (move) : NetMazeRG  
Location : Global  
Subscription (move) : Azure subscription 1  
Subscription ID : ee9ea131-d6f1-4e0b-bae6-b293615685ae  
Tags (edit) : Add tags

Records : 8  
Virtual Network Links : 1  
Virtual Network Links Wt... : 1

JSON View

Monitoring Capabilities Tutorials Tools + SDKs Recommendations (0)

Azure Monitor Tools

Get alerted to issues Create alerts to monitor resource health, usage, cost and more.

Get started with Log Analytics Leverage the value of the data in Azure Monitoring Logs and perform complex operations with minimal code.

Monitor at scale with Insights Get visibility into the resource's performance and health, accounting for different processes and interconnected dependencies.

Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Settings Properties Locks  
DNS Management Records Virtual Network Links  
Monitoring Automation Help

Microsoft Azure

AdminVM - Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekvash1507)

Home > AdminVM

AdminVM | Bastion

Virtual machine

Using Bastion: NetMazeBastion

Provisioning State: Succeeded

Please enter username and password to your virtual machine to connect using Bastion.

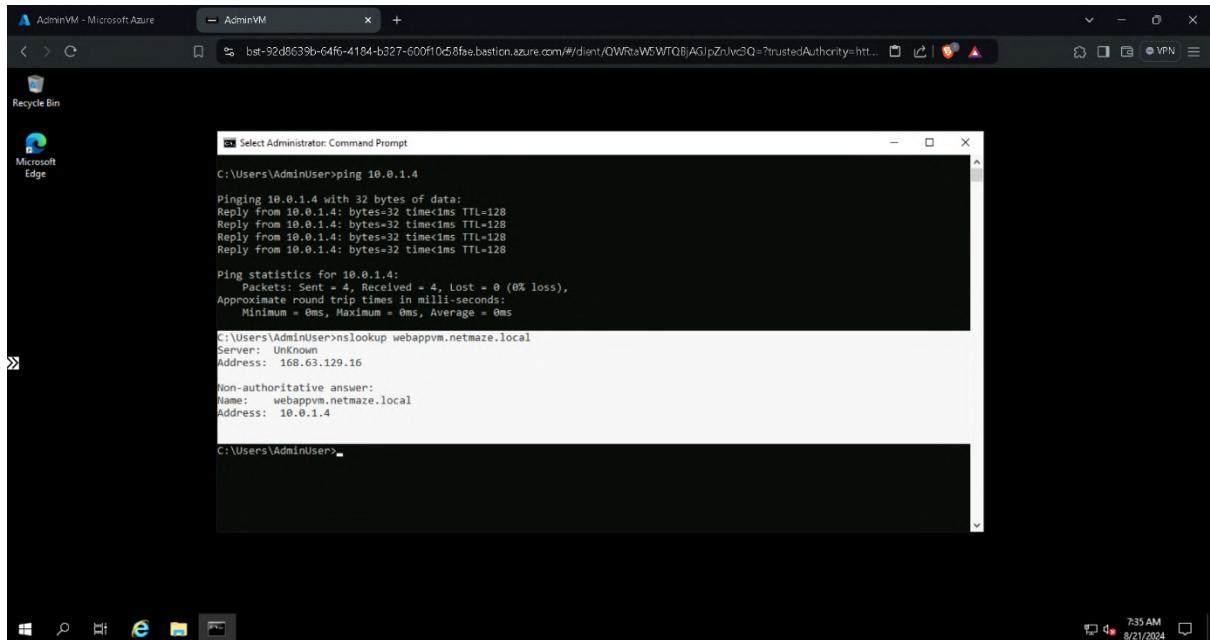
Connection Settings

Protocol: RDP  
Port: 3389  
Keyboard Language: English (US)

Authentication Type: VM Password  
Username: AdminUser  
VM Password:  Show  
Open in new browser tab

Tell us what you think of the Bastion experience

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Connect Connect Bastion Windows Admin Center Networking Network settings Load balancing Application security groups Network manager Settings Disks Extensions + applications



## Access Control

### 9.1. Updating the Network Security Groups (NSGs)

After completing the DNS and Load Balancing phase, the final step in securing the network was to update the Network Security Groups (NSGs) to reflect the project's workflow. This involved refining inbound security rules to ensure that traffic was properly managed and that only authorized connections were allowed.

#### 9.1.1. Configuring WebAppNSG

To ensure secure access to the WebAppVM, I configured the WebAppNSG with the following inbound security rules:

- Priority: 100
  - Name: Allow-RDP-AdminVM

- Port: 3389
  - Protocol: TCP
  - Source: 10.0.3.4 (Private IP address of AdminVM)
  - Destination: 10.0.1.4 (Private IP address of WebAppVM)
  - Action: Allow
- Priority: 110
  - Name: Deny-RDP-OnPremVM-and-DatabaseVM
  - Port: 3389
  - Protocol: TCP
  - Source: 10.1.1.0/24 (Address Space of OnPremSubnet) and 10.0.2.4 (Private IP address of DatabaseVM)
  - Destination: 10.0.1.4 (Private IP address of WebAppVM)
  - Action: Deny
- Priority: 120
  - Name: Allow-HTTPS-443
  - Port: 443
  - Protocol: TCP
  - Source: 10.1.0.0/16 (Address Space of OnPremVNet)
  - Destination: Any
  - Action: Allow
- Priority: 130
  - Name: Allow-HTTP-OnPremVM-ILB
  - Port: 80
  - Protocol: TCP
  - Source: 10.1.0.0/16 (Address Space of OnPremVNet)
  - Destination: Virtual Network
  - Action: Allow
- Priority: 140
  - Name: Deny-HTTP-Unauthorized-ILB
  - Port: 80
  - Protocol: TCP
  - Source: Any
  - Destination: Virtual Network
  - Action: Deny
- Priority: 150
  - Name: Allow-ILB-Probe
  - Port: 80
  - Protocol: TCP
  - Source: Virtual Network
  - Destination: Virtual Network
  - Action: Allow

### 9.1.2. Configuring DatabaseNSG

Next, I updated the DatabaseNSG to control access to the database server. The following rules were implemented:

- Priority: 100
  - Name: Allow-MySQL-3306
  - Port: 3306
  - Protocol: TCP
  - Source: Any
  - Destination: Any
  - Action: Allow
- Priority: 110
  - Name: Allow-SSH-AdminVM
  - Port: 22
  - Protocol: TCP
  - Source: 10.0.3.0/24 (Address Space of AdminSubnet)
  - Destination: 10.0.2.4 (Private IP address of DatabaseVM)
  - Action: Allow
- Priority: 120
  - Name: Deny-SSH-OnPrem
  - Port: 22
  - Protocol: TCP
  - Source: 10.1.0.0/16 (Address Space of OnPremVNet)
  - Destination: 10.0.2.4 (Private IP address of DatabaseVM)
  - Action: Deny

### 9.1.3. Reviewing AdminNSG and AdminVM-nsg (Attached with NIC of AdminVM)

Lastly, I reviewed the AdminNSG and AdminVM-nsg to ensure that it aligned with the project's security requirements. The rules configured in earlier phases were validated to ensure secure administrative access.

In this phase, I updated the NSGs to ensure proper access control within the network. By fine-tuning the security rules, I was able to secure the environment while allowing necessary communications between the resources.

## Screenshots

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The URL is <https://portal.azure.com/#feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e9ea131-d6f1-4e0b...>. The page title is "WebAppNSG - Microsoft Azure". The left sidebar shows "Microsoft Azure" with "Virtual machines" selected, followed by "WebAppVM | Network settings" and "WebAppNSG". The main content area is titled "WebAppNSG | Inbound security rules" under "Network security group". It includes a search bar, filter buttons (Priority, Name, Port, Protocol, Source, Destination, Action), and a table of rules:

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-RDP-AdminVM	3389	TCP	10.0.3.4	10.0.1.4	Allow
110	Deny-RDP-OnPremVM-and-DatabaseVM	3389	TCP	10.1.0/24,10.0.2.4	10.0.1.4	Deny
120	Allow-HTTPS-443	443	TCP	10.1.0/16	Any	Allow
130	Allow-HTTP-OnPremVM-ILB	80	TCP	10.1.0/16	VirtualNetwork	Allow
140	⚠ Deny-HTTP-Unauthorized-ILB	80	TCP	Any	VirtualNetwork	Deny
150	Allow-ILB-Probe	80	TCP	VirtualNetwork	VirtualNetwork	Allow
65000	AllowVhnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The URL is <https://portal.azure.com/#feature.msaljs=true#@vivekvash1507@gmail.onmicrosoft.com/resources/subscriptions/e9ea131-d6f1-4e0b...>. The page title is "WebAppVM-nsq - Microsoft Azure". The left sidebar shows "Microsoft Azure" with "Virtual machines" selected, followed by "WebAppVM | Network settings" and "WebAppVM-nsq". The main content area is titled "WebAppVM-nsq | Inbound security rules" under "Network security group". It includes a search bar, filter buttons (Priority, Name, Port, Protocol, Source, Destination, Action), and a table of rules:

Priority	Name	Port	Protocol	Source	Destination	Action
300	Allow-RDP-AdminVM	3389	TCP	10.0.3.4	10.0.1.4	Allow
310	Deny-RDP-OnPremVM-and-DatabaseVM	3389	TCP	10.1.0/24,10.0.2.4	10.0.1.4	Deny
320	Allow-HTTPS-443	443	TCP	10.1.0/16	Any	Allow
330	Allow-HTTP-OnPremVM-ILB	80	TCP	10.1.0/16	VirtualNetwork	Allow
350	⚠ Deny-HTTP-Unauthorized-ILB	80	TCP	Any	VirtualNetwork	Deny
360	Allow-ILB-Probe	80	TCP	VirtualNetwork	VirtualNetwork	Allow
65000	AllowVhnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

DatabaseNSG - Microsoft Azure AdminVM OnPremVM

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

vivekvash1507@gmail... DEFAULT DIRECTORY

Home > Virtual machines > DatabaseVM | Network settings > DatabaseNSG

## DatabaseNSG | Inbound security rules

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Search Add Hide default rules Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	Allow-MySQL-3306	3306	TCP	Any	Any	Allow
110	Allow-SSH-AdminVM	22	TCP	10.0.0/24	10.0.2.4	Allow
120	Deny-SSH-OnPrem	22	TCP	10.1.0.0/16	10.0.2.4	Deny
65000	AllowVhettinBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

DatabaseVM-nsg - Microsoft Azure AdminVM OnPremVM

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

vivekvash1507@gmail... DEFAULT DIRECTORY

Home > Virtual machines > DatabaseVM | Network settings > DatabaseVM-nsg

## DatabaseVM-nsg | Inbound security rules

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Search Add Hide default rules Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
1010	Allow-MySQL	3306	TCP	Any	Any	Allow
1020	Allow-SSH-AdminVM	22	TCP	10.0.0/24	10.0.2.4	Allow
1030	Deny-SSH-OnPrem	22	TCP	10.1.0.0/16	10.0.2.4	Deny
65000	AllowVhettinBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

<https://portal.azure.com/?feature-msaljs=true#home>

# Performance and Security Testing

In this phase of the project, I simulated various network scenarios to test performance and security, such as data transitions between on-premises and Azure environments. I also attempted to access resources from outside the permitted paths to validate the security configurations in place.

## 10.1. Checked Load Balancer Functionality

### 1. Connecting to OnPremVM:

- o I used Bastion to connect to the OnPremVM.

### 2. Creating and Running the PowerShell Script:

- o I created a PowerShell script named `TestLoadBalancer.ps1` on the desktop of OnPremVM. The script was designed to send multiple requests to the Load Balancer to verify its functionality.

#### Script Content:

```
$url = "http://10.0.1.10/"
$numRequests = 50
$concurrentRequests = 2

for ($i = 1; $i -le $numRequests; $i++) {
    Invoke-WebRequest -Uri $url -UseBasicParsing | Out-Null

    if ($i % $concurrentRequests -eq 0) {
        Start-Sleep -Seconds 1
    }
}

Write-Host "Completed $numRequests requests."
```

- o I opened Windows PowerShell (Administrator) on the OnPremVM and ran the `TestLoadBalancer.ps1` script.

**Result:** The script completed successfully with the message "Completed 50 requests."

### 3. Verifying Load Balancer Metrics:

- o After running the script, I checked the metrics of the `NetMazeLoadBalancer` in the Azure portal, such as Byte Count and Packet Count from the Monitoring tab.
- o **Result:** The Load Balancer was functioning correctly, and the metrics confirmed successful handling of the traffic.

## 10.2. Tested Data Transition Between On-Premises and Azure

### 1. Ping Tests:

- I connected to OnPremVM using Bastion and performed ping tests to verify connectivity with Azure VMs.

#### Commands Executed:

- ping 10.0.1.4 (Private IP address of WebAppVM)  
**Result:** 100% successful.
- ping 10.0.2.4 (Private IP address of DatabaseVM)  
**Result:** 100% successful.
- ping 10.0.3.4 (Private IP address of AdminVM)  
**Result:** 100% successful.

### 2. Traceroute Tests:

- From OnPremVM, I performed traceroute tests to Azure VMs to verify the data path.

#### Commands Executed:

- tracert 10.0.1.4 (WebAppVM's Private IP Address)  
**Result:** Trace successfully completed.
- tracert 10.0.2.4 (DatabaseVM's Private IP Address)  
**Result:** Trace successfully completed.
- tracert 10.0.3.4 (AdminVM's Private IP Address)  
**Result:** Trace successfully completed.

## 10.2.1 Tested Data Transfer

### 1. Configuring SSH on OnPremVM and WebAppVM:

- I ensured that OpenSSH.Client and OpenSSH.Server were installed and running on both OnPremVM and WebAppVM.

#### Commands Used:

```
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH'  
Start-Service sshd  
Set-Service -Name sshd -StartupType 'Automatic'
```

### 2. Creating and Transferring the Test File to WebAppVM:

- I created a text file named DataTransferTest in the Documents folder of OnPremVM with the following content:

This file is for Testing the Data Transfer Between ONPrem Vm  
and the Azure VM

Sign  
Vivek Vashisht

- I opened Windows PowerShell (Administrator) and ran the following command to transfer the file:

```
scp C:\Users\vashisht.vivek\Documents\DataTransferTest.txt
webuser@10.0.1.4:C:\Users\webuser\Documents\TestingDataTransfer
```

- **Result:** The command was successful. The DataTransferTest file was successfully transferred from OnPremVM to WebAppVM.
- **Verification:** I confirmed the presence of the DataTransferTest file in the TestingDataTransfer folder on WebAppVM.

### 3. Transferring the Test File to DatabaseVM:

- I ensured that the ssh.service was active and running on DatabaseVM using the following commands:

```
sudo systemctl status ssh
sudo systemctl enable ssh
```

- I connected to OnPremVM, generated a public/private RSA key pair, and saved it in the .ssh directory. The key was copied to the authorized\_keys file on DatabaseVM with the following command:

```
chmod 600 .ssh/authorized_keys
```

- I then updated the DataTransferTest file on OnPremVM with the following content:

```
This file is for Testing the Data Transfer Between OnPrem Vm
and the Azure VM
```

```
!!!! THIS IS FOR THE DatabaseVM !!!!
```

```
Sign
Vivek Vashisht
```

- I ran the following command to transfer the file to DatabaseVM:

```
scp C:\Users\vashisht.vivek\Documents\DataTransferTest.txt
databaseuser@10.0.2.4:/home/databaseuser/Documents/
```

- **Result:** The command was successful after resolving a permission error by changing ownership and permissions on the target folder. The DataTransferTest file was successfully transferred from OnPremVM to DatabaseVM.

#### 4. Transferring the Test File to AdminVM:

- I ensured that OpenSSH.Client and OpenSSH.Server were installed and running on AdminVM using the same commands as before.
- I updated the DataTransferTest file on OnPremVM with the following content:

```
This file is for Testing the Data Transfer Between OnPrem Vm  
and the Azure VM
```

```
!!!! THIS IS FOR THE AdminVM !!!
```

```
Sign  
Vivek Vashisht
```

- I ran the following command to transfer the file to AdminVM:

```
scp C:\Users\vashisht.vivek\Documents\DataTransferTest.txt  
AdminUser@10.0.3.4:C:\Users\AdminUser\Documents\DataTransferTes  
ting
```

- **Result:** The command was successful. The DataTransferTest file was successfully transferred from OnPremVM to AdminVM.
- **Verification:** I confirmed the presence of the DataTransferTest file in the DataTransferTesting folder on AdminVM.

### 10.3. Tested Azure-to-Azure Communication

#### Objective:

The goal was to test data transfer and communication between VMs within the NetMazeVNet (Azure-to-Azure communication).

#### 1. Ping Tests Between VMs:

- First, I performed ping tests from AdminVM to other VMs within the same virtual network to verify connectivity.

#### Commands Executed:

- ping 10.0.1.4 (Private IP address of WebAppVM)  
**Result:** 100% successful.
- ping 10.0.2.4 (Private IP address of DatabaseVM)  
**Result:** 100% successful.

#### 2. Data Transfer Test from AdminVM to WebAppVM:

- After confirming successful ping tests, I proceeded to test data transfer within the VMs.

### **Steps Taken:**

- I created a text file named DataTRFtest in the TestingDATATransferInAZ folder in the Documents directory on AdminVM. The content of the file was:

```
This file is for the Testing Purpose of  
Azure-to-Azure Communication  
!!! This is for WebAppVM !!!
```

- I opened PowerShell on AdminVM and ran the following command to transfer the file to WebAppVM:

```
scp  
C:\Users\AdminUser\Documents\TestingDATATransferInAZ\DataTRFtes  
t.txt  
webuser@10.0.1.4:C:\Users\webuser\Documents\AzuretoAzureDataTra  
nsfer
```

- **Result:** The command was successful. The DataTRFtest file was successfully sent from AdminVM to WebAppVM.
- **Verification:** I navigated to the AzuretoAzureDataTransfer folder in the Documents directory on WebAppVM and confirmed the presence of the DataTRFtest file.

### **3. Data Transfer Test from AdminVM to DatabaseVM:**

- Next, I tested data transfer from AdminVM to DatabaseVM.

### **Steps Taken:**

- I updated the content of the DataTRFtest file on AdminVM to:

```
This file is for the Testing Purpose of  
Azure-to-Azure Communication  
!!! This is for DatabaseVM !!!
```

- I saved the file in the TestingDATATransferInAZ folder in the Documents directory on AdminVM.

- I then ran the following command to transfer the file to DatabaseVM:

```
scp  
C:\Users\AdminUser\Documents\TestingDATATransferInAZ\DataTRFtes  
t.txt databaseuser@10.0.2.4:/home/databaseuser/Documents/
```

- **Result:** The command was successful. The `DataTRFtest` file was successfully sent from AdminVM to DatabaseVM.
- **Verification:** I navigated to the `Documents` directory on DatabaseVM and confirmed the presence of the `DataTRFtest` file.

By completing these tests, I successfully validated Azure-to-Azure communication and data transfer between VMs within the NetMazeVNet. The network scenarios were simulated successfully, ensuring the integrity and functionality of the internal network communication.

## 10.4. Validation of the Security Configurations

To ensure the security configurations were correctly implemented, I conducted five specific tests: HTTP Access, SSH Access, Accessing Blocked Port, ICMP (Ping), and NSG Logs Monitoring.

### Test 1: HTTP Access

1. **Unauthorized HTTP Access:**
  - **Objective:** Attempt to access the WebAppVM from an unauthorized source (AdminVM) to validate the restriction in place.
  - **Steps Taken:**
    - Connected to AdminVM using Bastion.
    - Opened Internet Explorer and entered `http://10.0.1.4/` in the search bar.
  - **Result:** Access was denied, confirming that the Web Server (IIS) hosted on WebAppVM was inaccessible from AdminVM as expected.
2. **Authorized HTTP Access:**
  - **Objective:** Verify that authorized access from OnPremVM to WebAppVM is allowed.
  - **Steps Taken:**
    - Connected to OnPremVM using Bastion.
    - Opened Internet Explorer and entered `http://10.0.1.4/` in the search bar.
  - **Result:** Access was successful, and the Web Server (IIS) hosted on WebAppVM was accessible from OnPremVM.

## Test 2: Testing SSH Access

### 1. Unauthorized SSH Access:

- **Objective:** Test the denial of SSH access to DatabaseVM from an unauthorized source (OnPremVM).
- **Steps Taken:**
  - Connected to OnPremVM using Bastion.
  - Opened PowerShell and entered the command:

```
ssh databaseuser@10.0.2.4
```

- **Result:** The connection attempt timed out, confirming that SSH access from OnPremVM to DatabaseVM was correctly restricted.

### 2. Authorized SSH Access:

- **Objective:** Verify that SSH access to DatabaseVM from AdminVM is allowed.
- **Steps Taken:**
  - Connected to AdminVM using Bastion.
  - Opened PowerShell and entered the command:

```
ssh databaseuser@10.0.2.4
```

- **Result:** SSH access was successful, confirming that AdminVM could securely connect to DatabaseVM.

## Test 3: Accessing Blocked Port (WebAppVM)

### 1. Unauthorized Port Access:

- **Objective:** Test the denial of access to a blocked port (3389) on WebAppVM from an unauthorized source (OnPremVM).
- **Steps Taken:**
  - Connected to OnPremVM using Bastion.
  - Opened PowerShell and entered the command:

```
telnet 10.0.1.4 3389
```

- **Result:** The connection failed, indicating that the port was correctly blocked for OnPremVM.

## 2. Authorized Port Access:

- **Objective:** Ensure that AdminVM can access the blocked port (3389) on WebAppVM.
- **Steps Taken:**
  - Connected to AdminVM using Bastion.
  - Opened PowerShell and entered the command:

```
telnet 10.0.1.4 3389
```

- **Result:** The command was successful, with a blank screen and blinking cursor, confirming that AdminVM could access the blocked port.

## Test 4: ICMP (Ping)

### 1. ICMP Access from AdminVM to WebAppVM:

- **Objective:** Validate ICMP (ping) access between AdminVM and WebAppVM.
- **Steps Taken:**
  - Ensured that an inbound rule allowing ICMP traffic was created in the "Windows Defender Firewall with Advanced Security" for both AdminVM and WebAppVM.
  - Connected to AdminVM using Bastion.
  - Opened the Command Prompt and entered:

```
ping 10.0.1.4
```

- **Result:** The ping was 100% successful.

### 2. ICMP Access from DatabaseVM to WebAppVM:

- **Objective:** Validate ICMP (ping) access between DatabaseVM and WebAppVM.
- **Steps Taken:**
  - Connected to DatabaseVM using Bastion.
  - Entered the command:

```
ping 10.0.1.4
```

- **Result:** The ping was 100% successful.

### 3. ICMP Access from OnPremVM to WebAppVM:

- **Objective:** Validate ICMP (ping) access between OnPremVM and WebAppVM.
- **Steps Taken:**
  - Ensured that an inbound rule allowing ICMP traffic was created in the "Windows Defender Firewall with Advanced Security" for OnPremVM.
  - Connected to OnPremVM using Bastion.
  - Entered the command:

```
ping 10.0.1.4
```

- **Result:** The ping was 100% successful.

## Test 5: NSG Logs Monitor

### 1. Setup and Monitoring:

- **Objective:** Monitor the security group flow logs to verify the effectiveness of the security rules in place.
- **Steps Taken:**
  - Navigated to Network Watcher in the Azure portal.
  - Selected the Flow logs tab under Logs in Network Watcher and clicked on "+ create."
  - Configuration details:
    - **Location:** Canada Central
    - **Storage Account:** Created a new account named netmazensg with general-purpose v1, Replication: LRS, Resource Group: NetMazeRG.
    - **Flow Log Name:** WebAppNSG-netmazerg-flowlog
    - **Target Resource:** Selected WebAppNSG as the resource, Target Resource Type: Network security group.
  - Clicked on Create.
- **Result:** Successfully set up the flow logs.

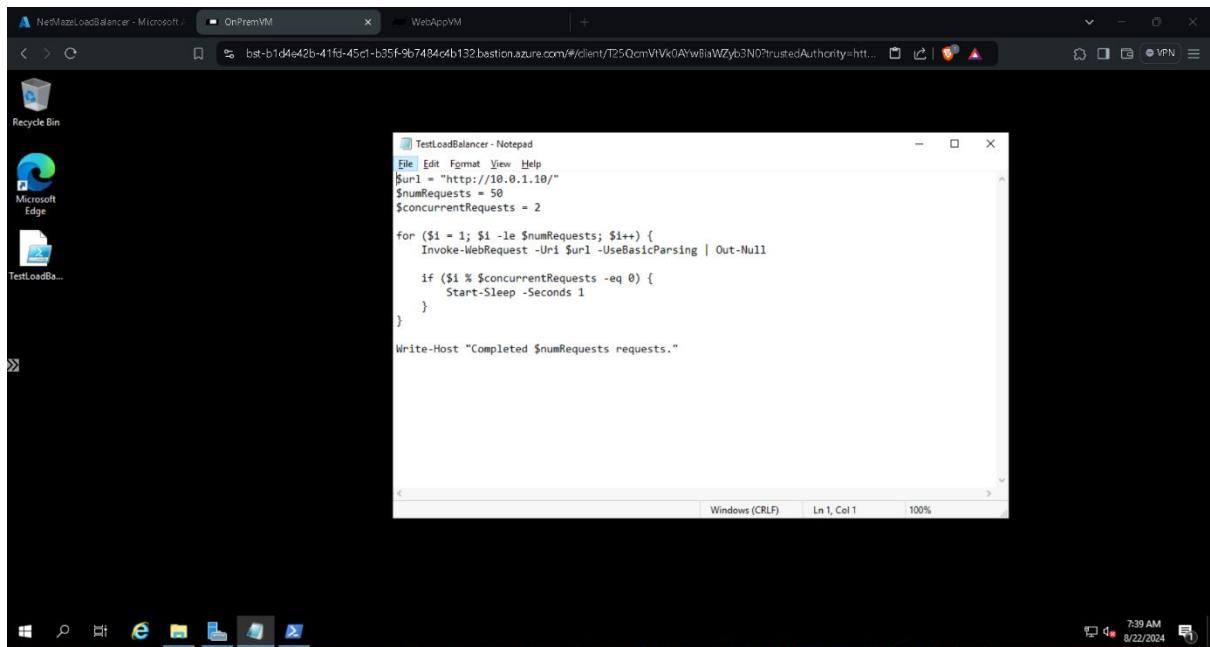
### 2. Testing and Validation:

- **Objective:** Verify the flow logs reflect denied HTTP access attempts.
- **Steps Taken:**
  - Connected to AdminVM using Bastion.
  - Opened Internet Explorer and entered `http://10.0.1.4/`.
  - The HTTP access was denied as expected.
  - Navigated to the storage account netmazensg, went to the containers tab, and downloaded the `PT1H.json` file from the Blob storage.
  - Opened the file in VS Code.
- **Result:** The flow logs displayed data indicating that the `UserRule_Deny-HTTP-Unauthorized-ILB` rule worked successfully, confirming that unauthorized HTTP access was denied.

## **Conclusion:**

The validation of security configurations through these tests confirmed that the network security rules were implemented effectively. All tests produced expected results, ensuring that the resources within the NetMazeVNet are securely managed and accessed according to the defined policies. This completes the Performance and Security Testing phase of the project.

## Screenshots



NetMazeLoadBalancer - Microsoft Edge

OnPremVM WebAppVM

bst-b1d4e42b-41fd-45c1-b35f-9b7484c4b132.bastion.azure.com/#/client/T250cnVtVk0AYwIaWZyb3N0?trustedAuthority=http://

Select Administrator: Windows PowerShell

PS C:\Users\vashisht.vivek\Desktop> ls

Directory: C:\Users\vashisht.vivek\Desktop

Mode	LastWriteTime	Length	Name
-a----	8/22/2024 7:39 AM	314	TestLoadBalancer.ps1

PS C:\Users\vashisht.vivek\Desktop> .\TestLoadBalancer.ps1

Completed 58 requests.

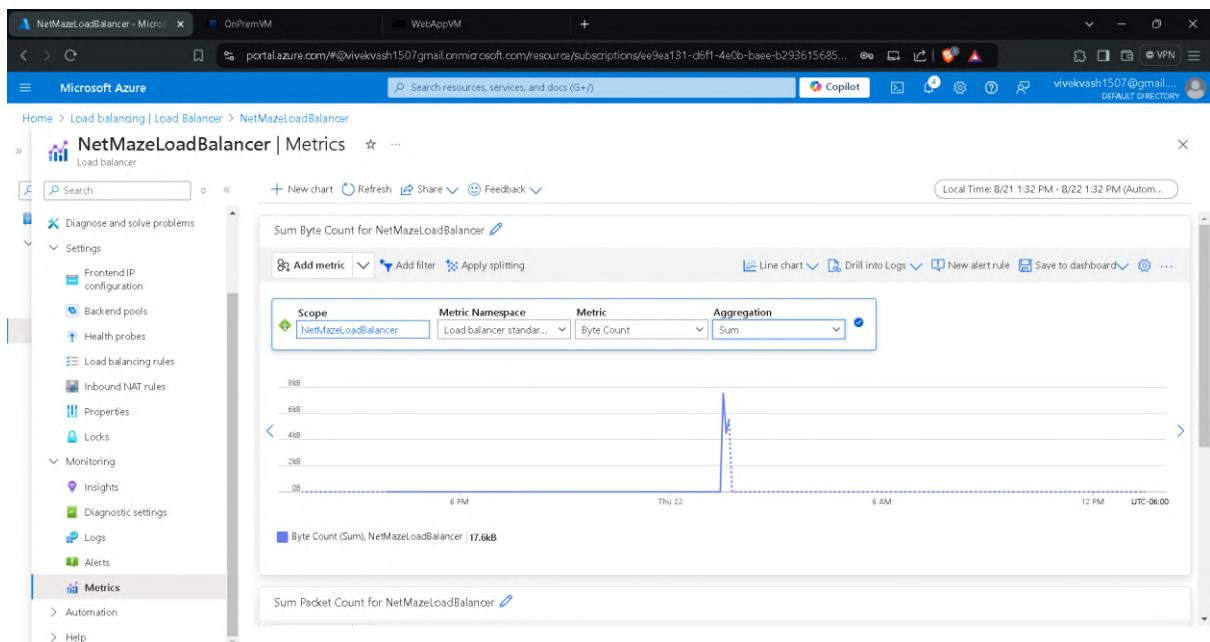
PS C:\Users\vashisht.vivek\Desktop>

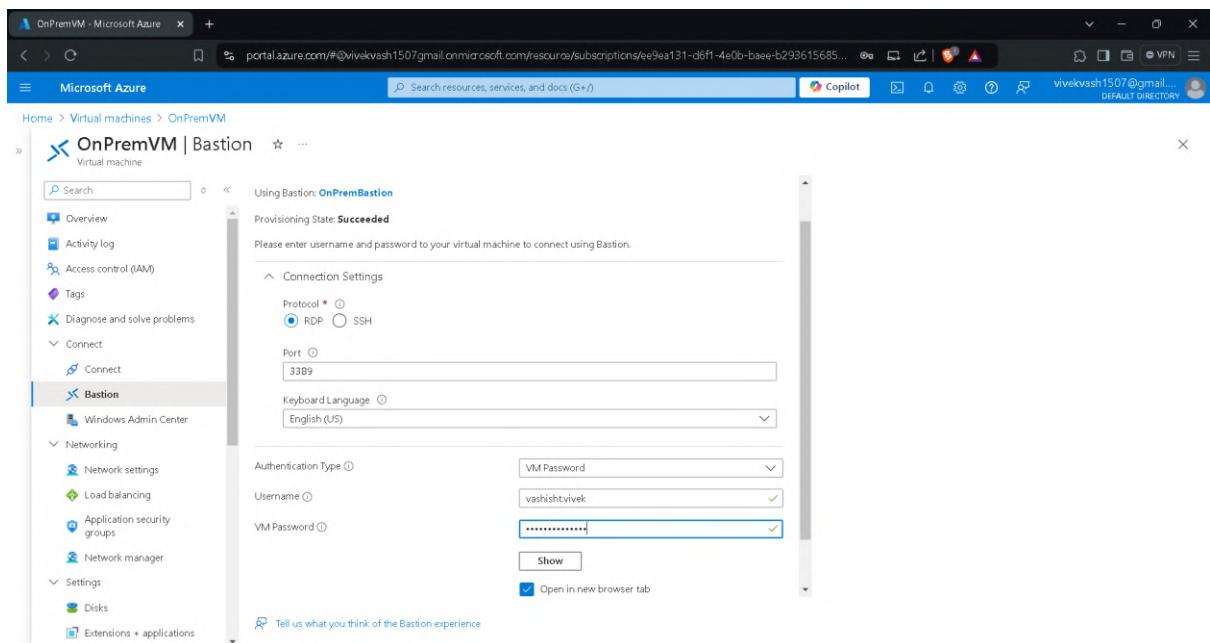
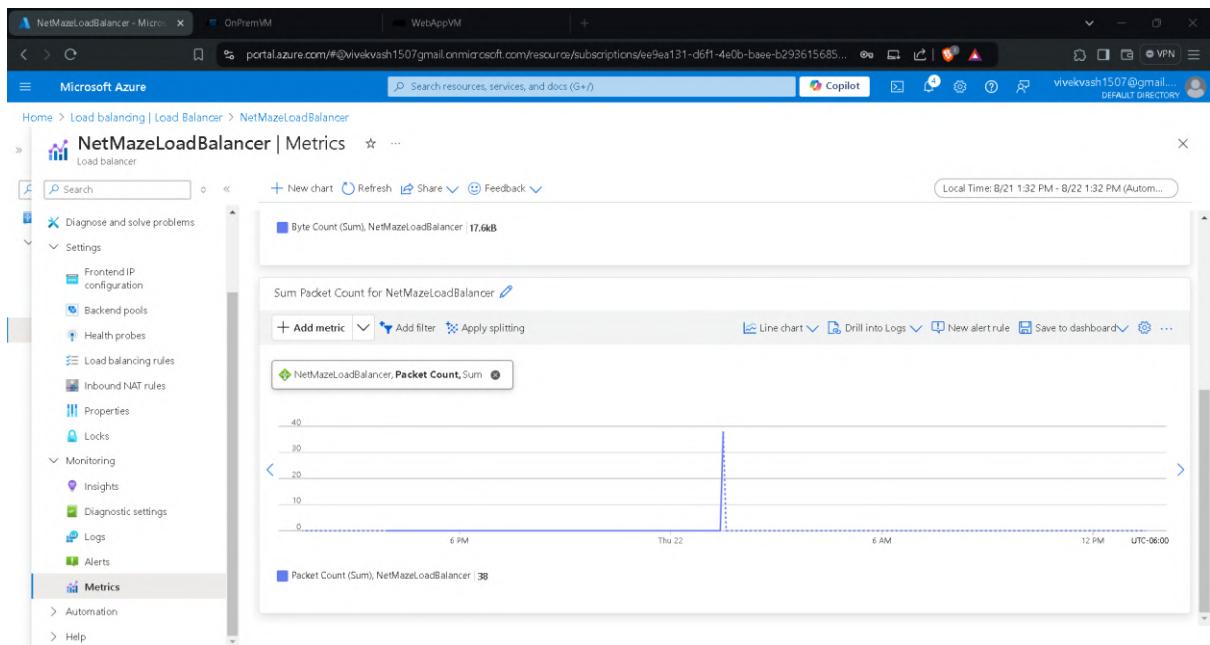
Recycle Bin

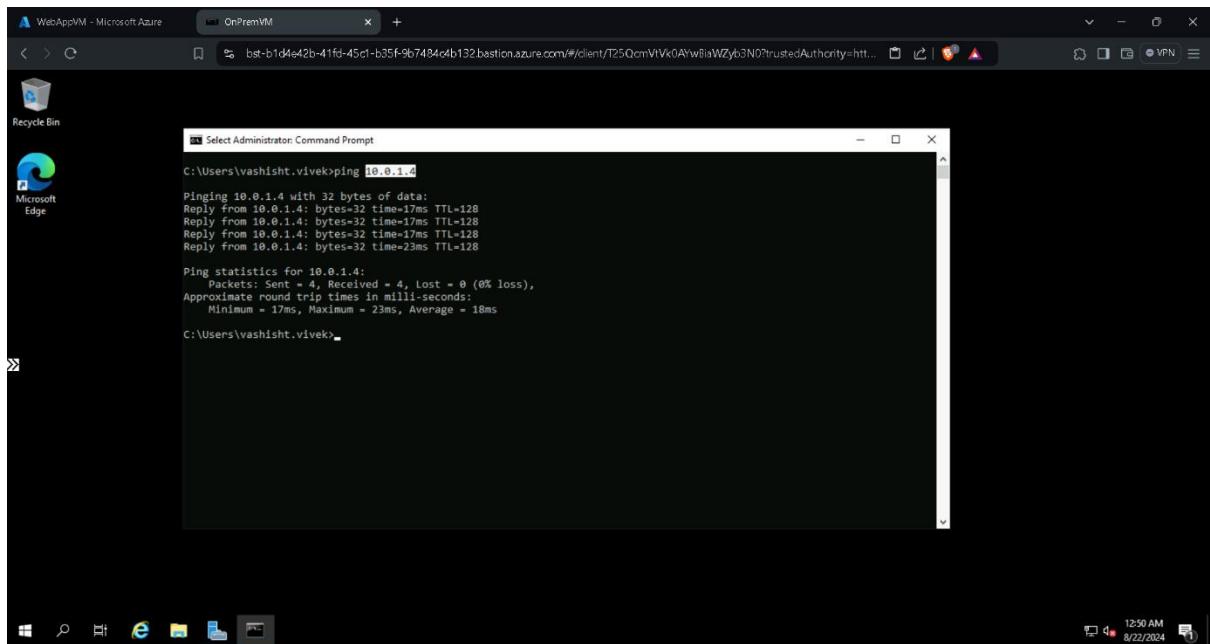
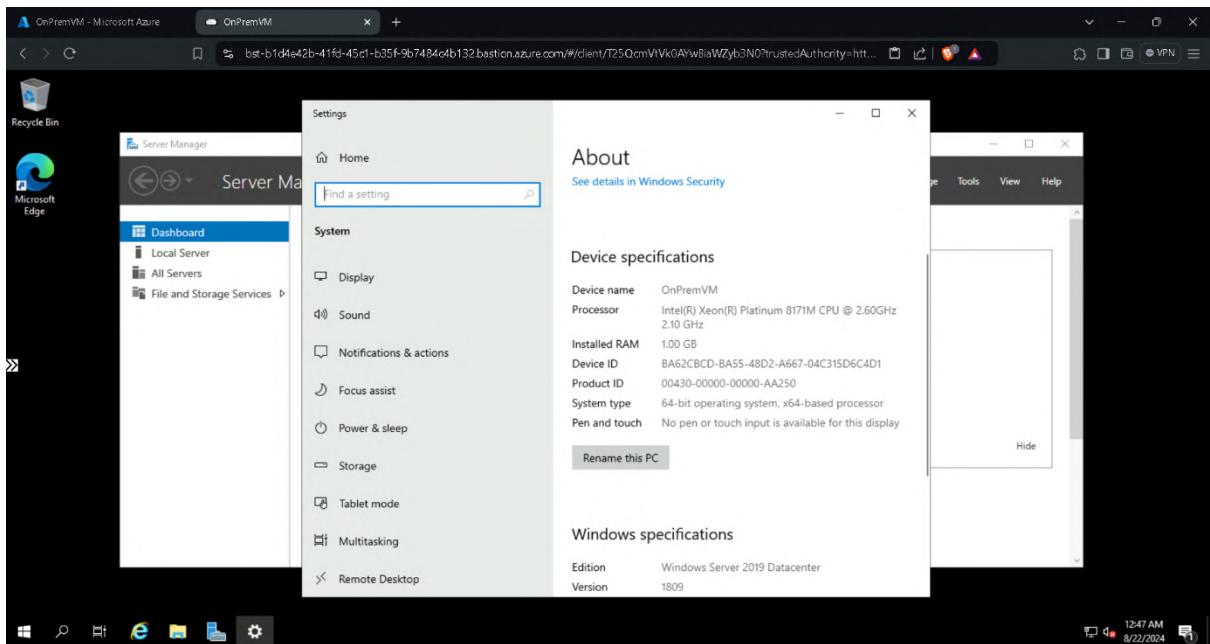
Microsoft Edge

TestLoadBa...

7:40 AM 8/22/2024







```
C:\Users\vasishth.vivek>ping 10.0.1.4

Pinging 10.0.1.4 with 32 bytes of data:
Reply from 10.0.1.4: bytes=32 time=17ms TTL=128
Reply from 10.0.1.4: bytes=32 time=17ms TTL=128
Reply from 10.0.1.4: bytes=32 time=17ms TTL=128
Reply from 10.0.1.4: bytes=32 time=23ms TTL=128

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 23ms, Average = 18ms

C:\Users\vasishth.vivek>ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time=16ms TTL=64
Reply from 10.0.2.4: bytes=32 time=18ms TTL=64
Reply from 10.0.2.4: bytes=32 time=18ms TTL=64
Reply from 10.0.2.4: bytes=32 time=24ms TTL=64

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 24ms, Average = 19ms

C:\Users\vasishth.vivek>
```

```
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 23ms, Average = 18ms

C:\Users\vasishth.vivek>ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time=16ms TTL=64
Reply from 10.0.2.4: bytes=32 time=18ms TTL=64
Reply from 10.0.2.4: bytes=32 time=18ms TTL=64
Reply from 10.0.2.4: bytes=32 time=24ms TTL=64

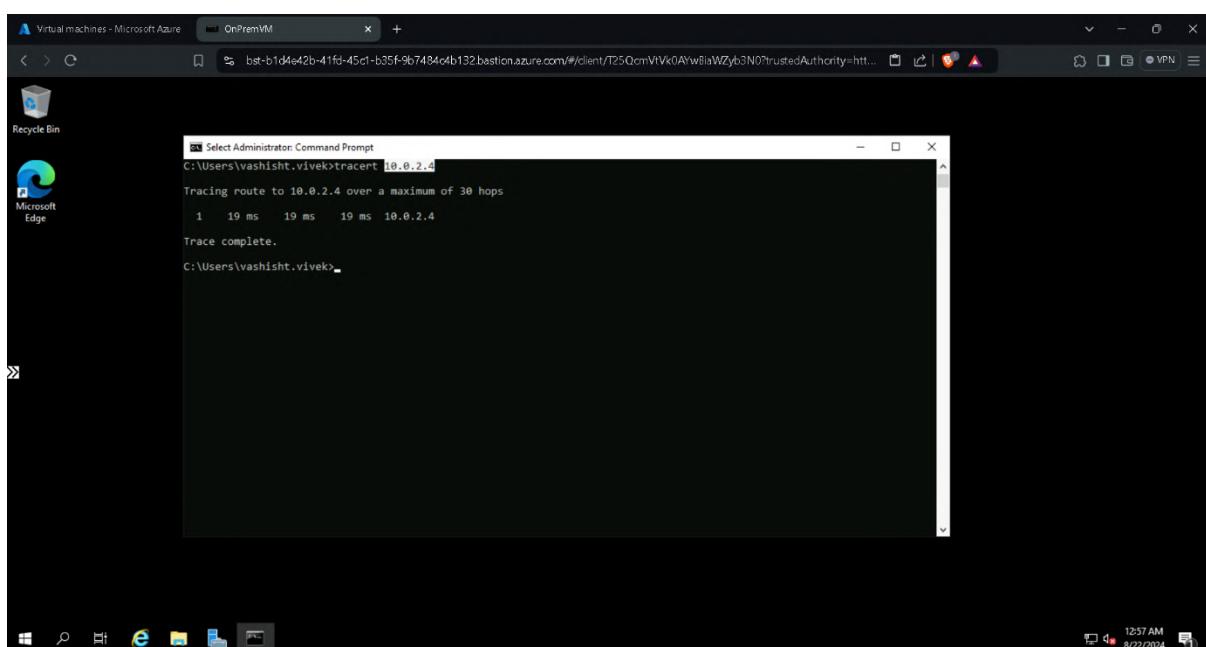
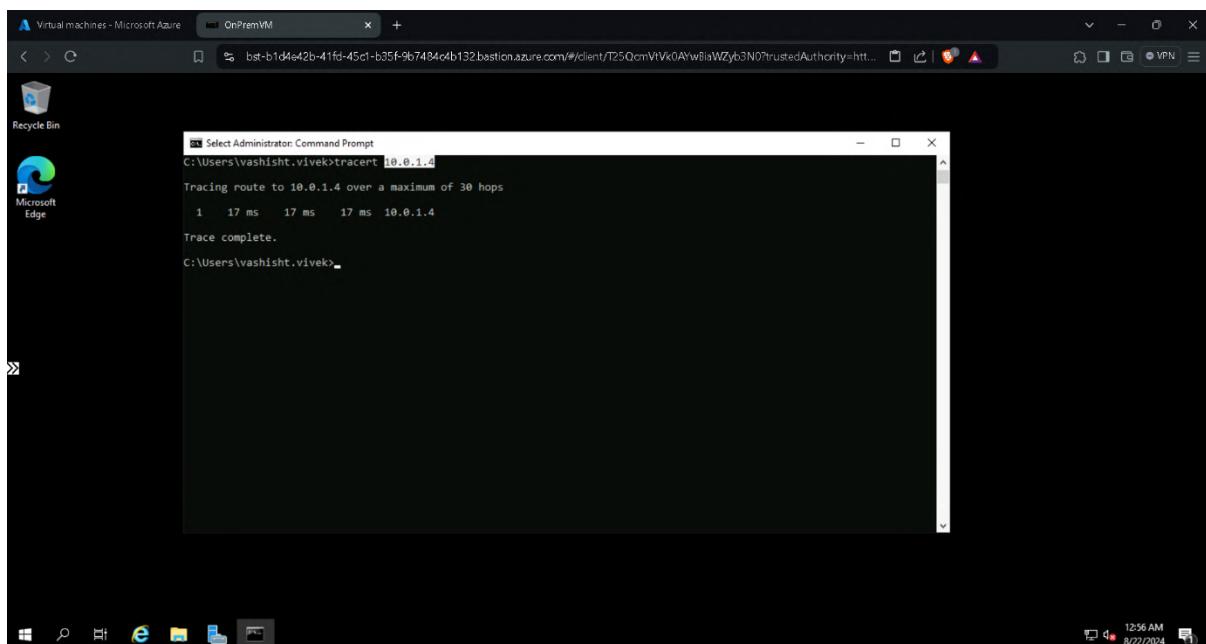
Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 24ms, Average = 19ms

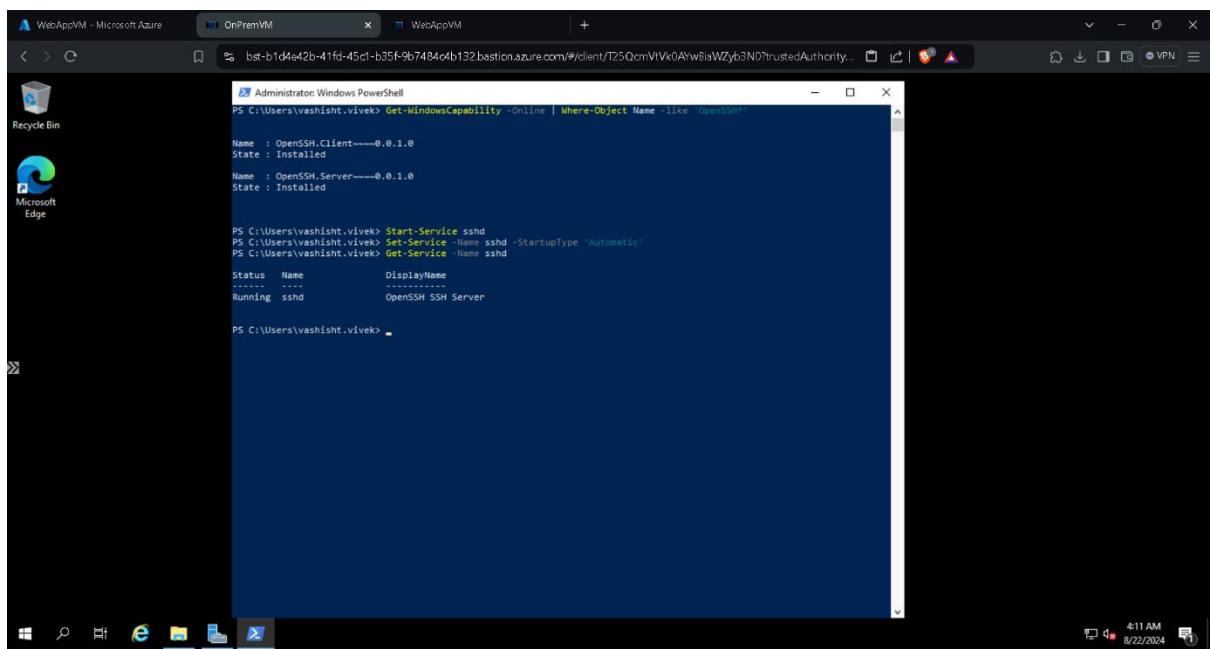
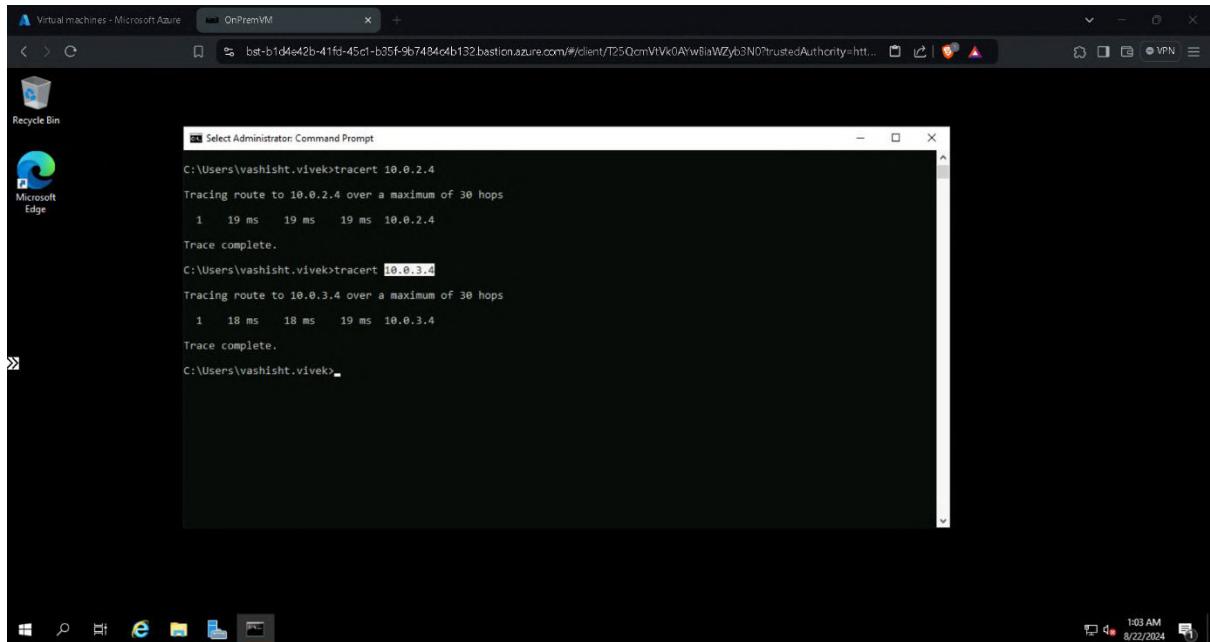
C:\Users\vasishth.vivek>ping 10.0.3.4

Pinging 10.0.3.4 with 32 bytes of data:
Reply from 10.0.3.4: bytes=32 time=19ms TTL=128

Ping statistics for 10.0.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 19ms, Average = 19ms

C:\Users\vasishth.vivek>
```





```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\webuser> Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*'

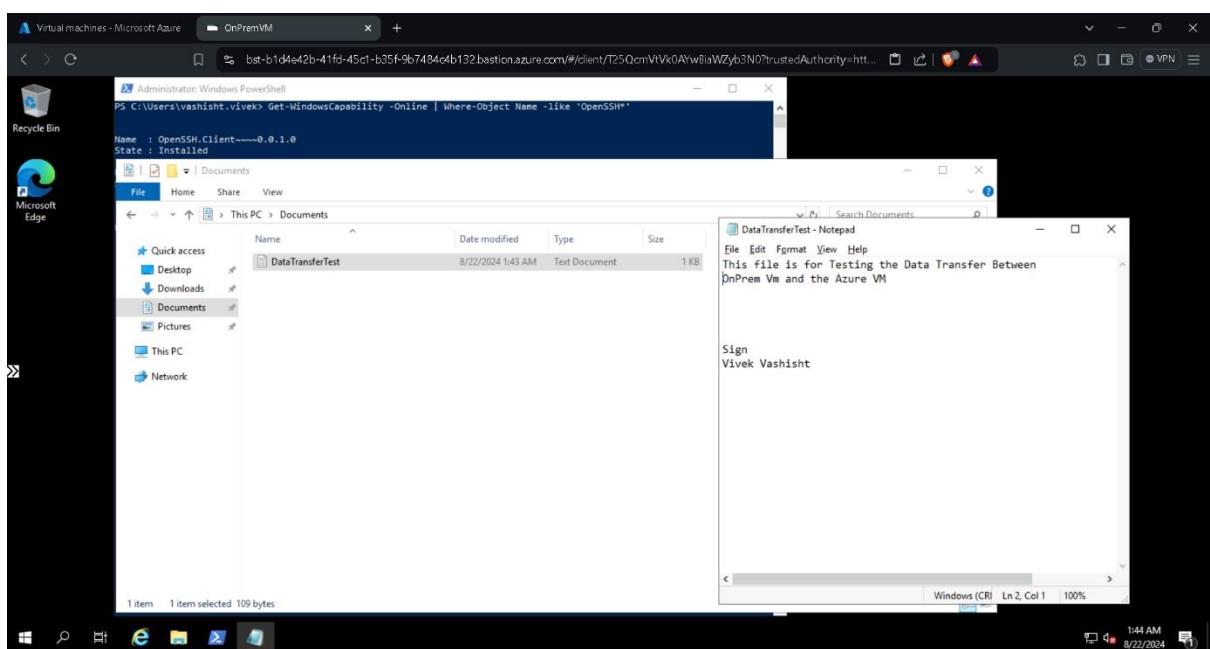
Name : OpenSSH.Client----0.0.1.0
State : Installed

Name : OpenSSH.Server----0.0.1.0
State : Installed

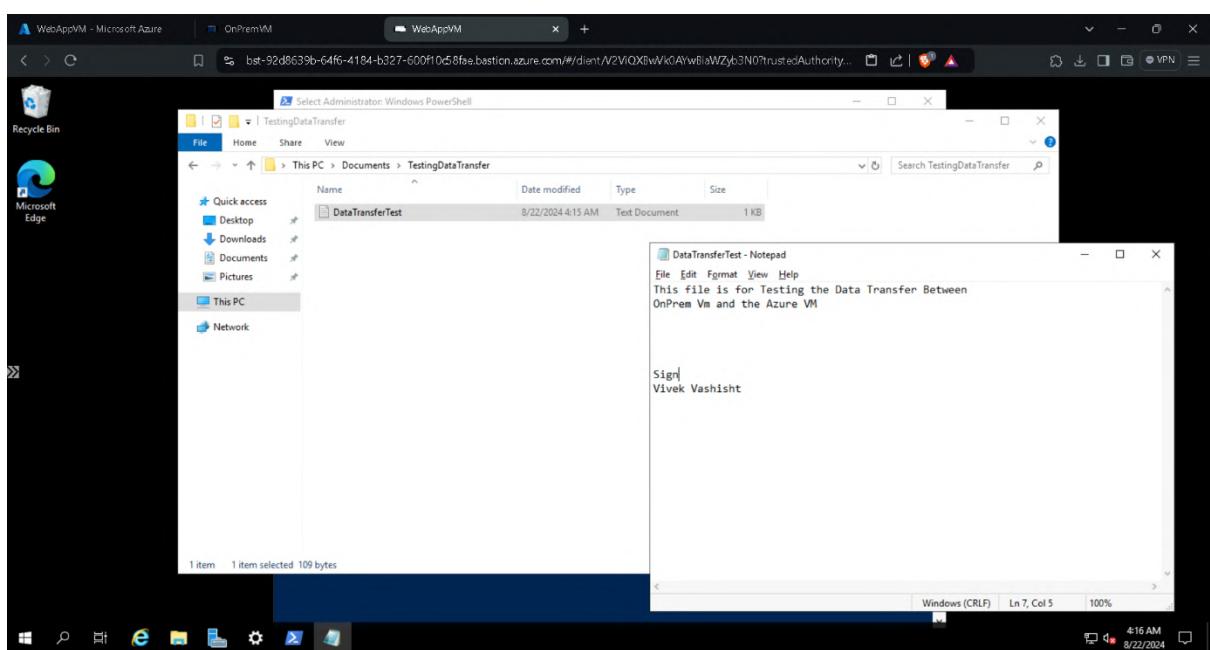
PS C:\Users\webuser> Start-Service sshd
PS C:\Users\webuser> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Users\webuser> Get-Service -Name sshd

Status   Name               DisplayName
Running  sshd              OpenSSH SSH Server

PS C:\Users\webuser>
```

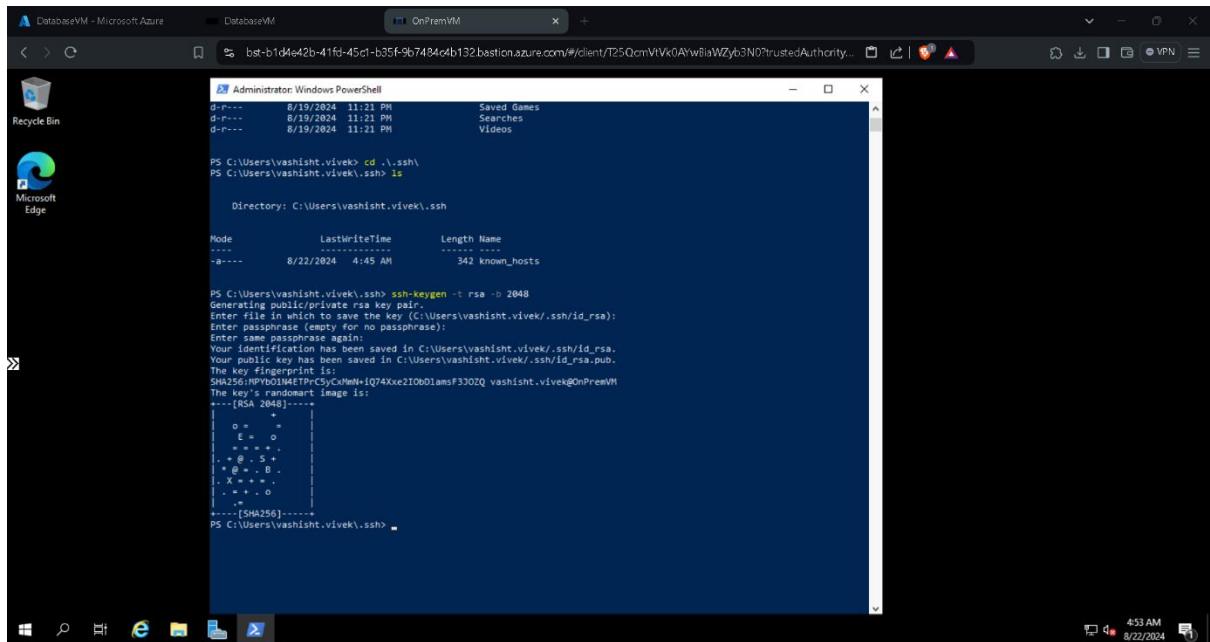


A screenshot of a Windows desktop environment. In the center, there is a PowerShell window titled "Administrator: Windows PowerShell" with the command `scp C:\Users\vashiht.vivek\Documents\DataTransferTest.txt webuser@10.0.1.4:C:\Users\webuser` running. Below the command, a progress bar shows the transfer of "DataTransferTest.txt" at 100% completion with a speed of 6.8KB/s. The desktop background is black, and the taskbar at the bottom shows icons for File Explorer, Microsoft Edge, and Task View. The system tray in the bottom right corner indicates the date as 8/22/2024 and the time as 4:15 AM.



```
A DatabaseVM - Microsoft Azure DatabaseVM OnPremVM +  
vivekvash1507@gmail.com@DatabaseVM:~$ sudo systemctl status ssh  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)  
   Active: active (running) since Wed 2024-08-21 21:52:55 UTC; 6h ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
 Main PID: 632 (sshd)  
    Tasks: 1 (limit: 1053)  
   Memory: 6.8M  
     CPU: 88ms  
    Group: /system.slice/ssh.service  
          └─632 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Aug 22 04:27:21 DatabaseVM aad_certhandler[1466]: Version: 1.0.0.27190001; user: vivekvash1507@gmail.com  
Aug 22 04:27:21 DatabaseVM aad_certhandler[1466]: This is an Azure machine  
Aug 22 04:27:22 DatabaseVM sshd[1463]: Certificate extension "displayname@sshservice.azure.net" is not supported  
Aug 22 04:27:22 DatabaseVM sshd[1463]: Certificate extension "oid@sshservice.azure.net" is not supported  
Aug 22 04:27:22 DatabaseVM sshd[1463]: Certificate extension "tid@sshservice.azure.net" is not supported  
Aug 22 04:27:22 DatabaseVM sshd[1463]: pam_aad(sshd:account): AadAuthorize, Version: 1.0.0.27190001; correlationId: c14c5319-d51e-4644-adb3-20c32707b22b  
Aug 22 04:27:22 DatabaseVM sshd[1463]: pam_aad(sshd:account): This is an Azure machine  
Aug 22 04:27:22 DatabaseVM sshd[1463]: pam_aad(sshd:account): Login granted for vivekvash1507@gmail.com as an admin.  
Aug 22 04:27:23 DatabaseVM sshd[1463]: Accepted publickey for vivekvash1507@gmail.com from 10.0.4.5 port 35532 ssh2: RSA-CERT SHA256:RzI9HaR6osHYCqQ4e1fwFK+v  
Aug 22 04:27:23 DatabaseVM sshd[1463]: pam_unix(sshd:session): session opened for user vivekvash1507@gmail.com(uid=7162338) by (uid=0)  
lines 1-22/22 (END)  
vivekvash1507@gmail.com@DatabaseVM:~$ sudo systemctl enable ssh  
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable ssh  
vivekvash1507@gmail.com@DatabaseVM:~$ ip a | grep inet  
  inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
      inet 10.0.2.4/24 metric 100 brd 10.0.2.255 scope global eth0  
        inet6 fe80::6245:bfff:fe60:4ebd/64 scope link  
vivekvash1507@gmail.com@DatabaseVM:~$
```

```
A DatabaseVM - Microsoft Azure DatabaseVM OnPremVM +  
vivekvash1507@gmail.com@DatabaseVM:~$ ls  
Administrator: Windows PowerShell  
PS C:\Users\vashishht.vivek> ls  
  
Directory: C:\Users\vashishht.vivek  
  
Mode LastWriteTime Length Name  
---- ----- ----   
d---- 8/22/2024 4:13 AM .ssh  
d-r-- 8/19/2024 11:21 PM Contacts  
d-r-- 8/19/2024 11:21 PM Desktop  
d-r-- 8/22/2024 1:42 AM Documents  
d-r-- 8/19/2024 11:21 PM Downloads  
d-r-- 8/19/2024 11:21 PM Favorites  
d-r-- 8/19/2024 11:21 PM Links  
d-r-- 8/19/2024 11:21 PM Music  
d-r-- 8/19/2024 11:21 PM Pictures  
d-r-- 8/19/2024 11:21 PM Saved Games  
d-r-- 8/19/2024 11:21 PM Searches  
d-r-- 8/19/2024 11:21 PM Videos  
  
PS C:\Users\vashishht.vivek> cd .\ssh\  
PS C:\Users\vashishht.vivek> ls  
  
Directory: C:\Users\vashishht.vivek\.ssh  
  
Mode LastWriteTime Length Name  
---- ----- ----   
-a--- 8/22/2024 4:45 AM 342 known_hosts  
  
PS C:\Users\vashishht.vivek> ssh-keygen -t rsa -b 2048  
Generating public/private rsa key pair.  
Enter file in which to save the key (C:/Users/vashishht.vivek/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in C:/Users/vashishht.vivek/.ssh/id_rsa.  
Your public key has been saved in C:/Users/vashishht.vivek/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:HPYQxD1M4ETPrCs5yCxMhM+I074Xxe2IObDlamsf3J0ZQ vashishht.vivek@OnPremVM  
The key's randomart image is:  
-----[RSA 2048]----
```

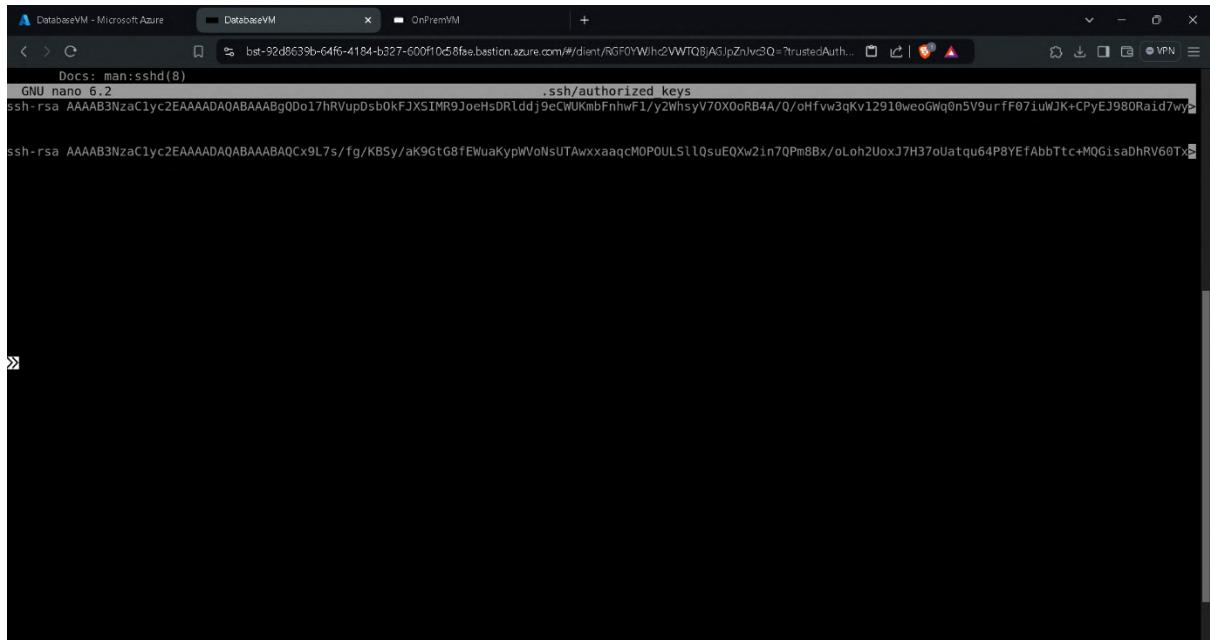


```
Administrator: Windows PowerShell
d-r-- 8/19/2024 11:21 PM Saved Games
d-r-- 8/19/2024 11:21 PM Searches
d-r-- 8/19/2024 11:21 PM Videos

PS C:\Users\vashisht.vivek> cd .\ssh\
PS C:\Users\vashisht.vivek\ssh> ls

Mode LastWriteTime Length Name
---- ----- 342 known_hosts

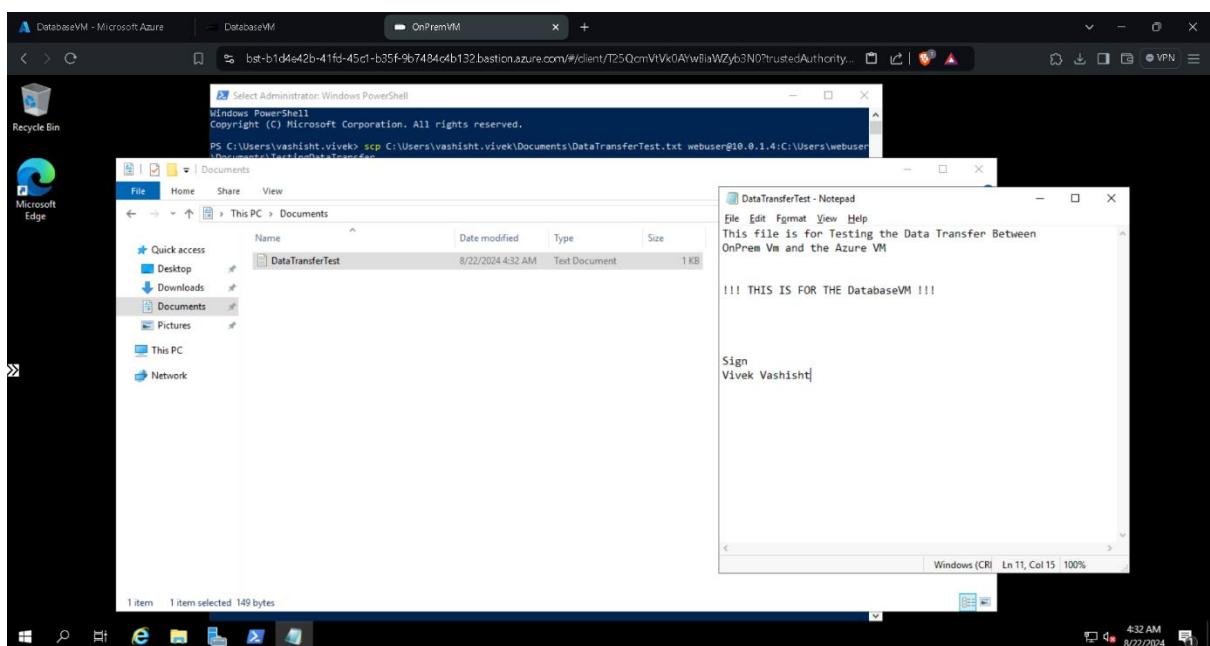
PS C:\Users\vashisht.vivek> ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (C:/Users/vashisht.vivek/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:/Users/vashisht.vivek/.ssh/id_rsa.
Your public key has been saved in C:/Users/vashisht.vivek/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:HPYb01M4ETPrC5yCxMhN1o74Xxe2I0bD1amsF33OZQ vashisht.vivek@OnPremVM
The key's randomart image is:
----[RSA 2048]----+
|          = |
|         o = |
|        E = o |
|       + = o |
|      * @ = S |
|     . * @ = B |
|    . . . = o |
|     . =       |
----[SHA256]----+
PS C:\Users\vashisht.vivek>
```

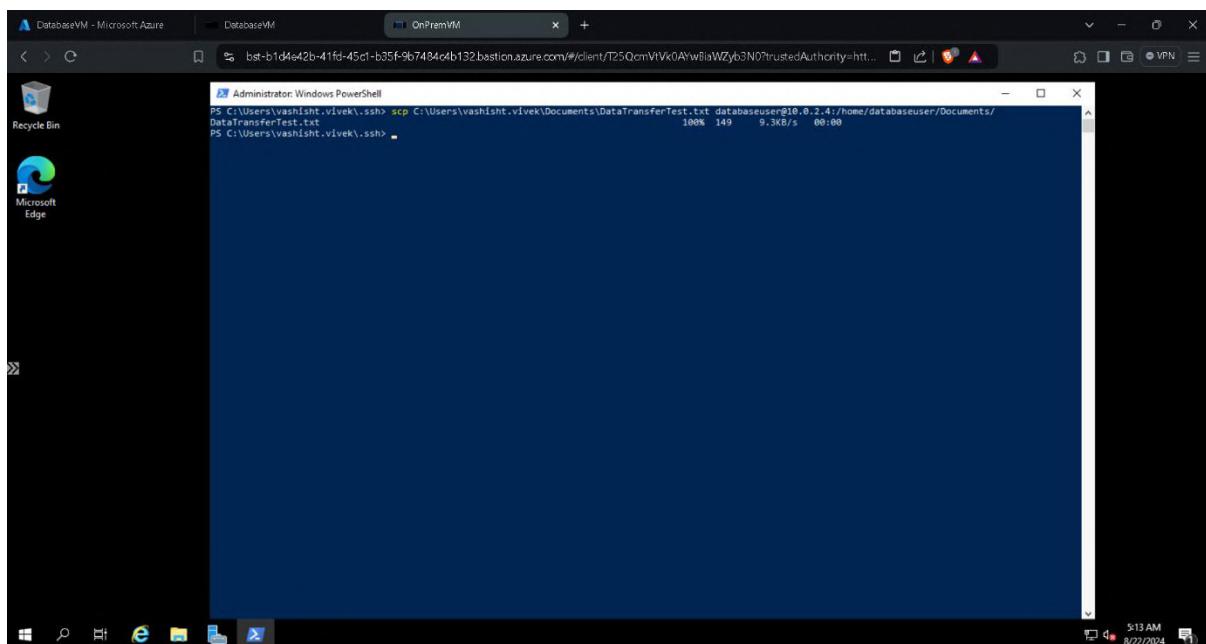


```
Docs: man:sshd(8)
GNU nano 6.2 .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQg0Do17hRVupDsb0kFJSIMR9JoeHsDRljj9eCWUKmbFnhwF1/y2WhsyV70X0oRB4A/0/oHfvw3qKv12910weoGWq0n5V9urff07iuWJK+CPyEJ980Ra1d7wyw
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCx9L7s/fg/KBSy/aK9GtG8fEWuaKypWVoNsUTAwxxaaqcMOP0ULS1lQsuEQxw2ln7Qm8Bx/oLoh2UoxJ7H37oUatqu64P8YEfAbbTtc+MQGisaDhRV60Tx
```

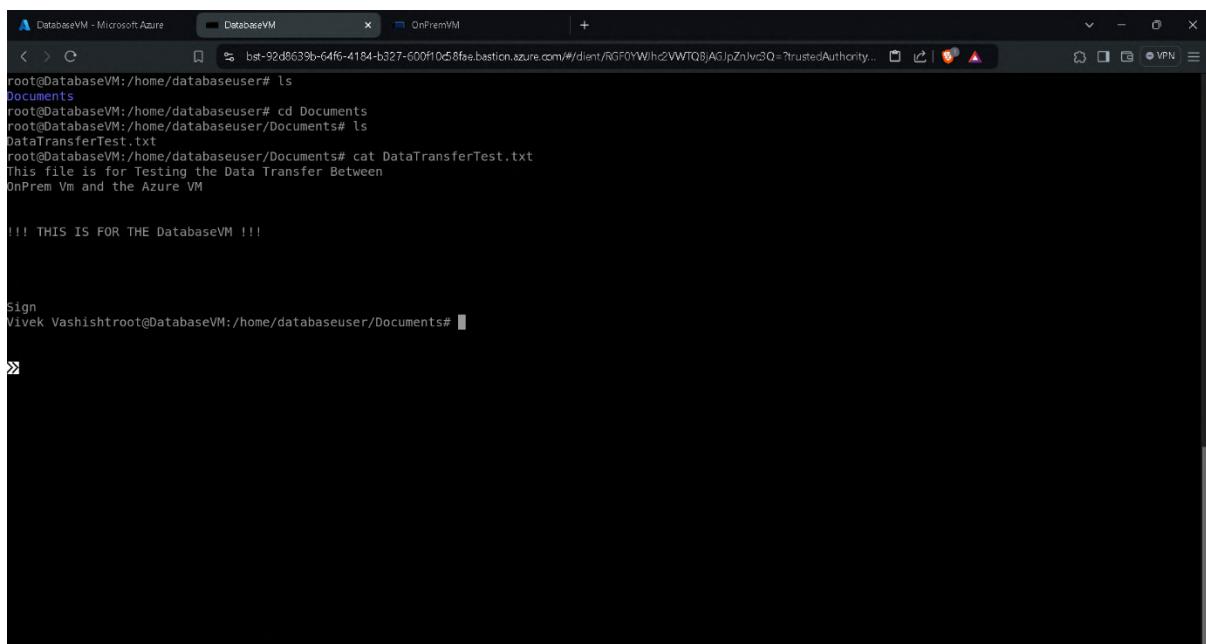
```
A DatabaseVM - Microsoft Azure DatabaseVM OnPremVM +  
bst-92d8639b-64f6-4184-b327-600f1058fae.bastion.azure.com/#/client/RGF0YWlh2VWTQBAGJpZnJvc3Q=?trustedAuthority...  
root@DatabaseVM:/home/databaseuser# chmod 600 .ssh/authorized_keys  
root@DatabaseVM:/home/databaseuser#  
root@DatabaseVM:/home/databaseuser#
```

```
A DatabaseVM - Microsoft Azure DatabaseVM OnPremVM +  
bst-92d8639b-64f6-4184-b327-600f1058fae.bastion.azure.com/#/client/RGF0YWlh2VWTQBAGJpZnJvc3Q=?trustedAuthority...  
root@DatabaseVM:/home/databaseuser/Documents# cd /home/databaseuser/  
root@DatabaseVM:/home/databaseuser# ls -ld Documents  
drwxr-xr-x 2 root root 4096 Aug 22 04:43 Documents  
root@DatabaseVM:/home/databaseuser# sudo chown databaseuser:databaseuser /home/databaseuser/Documents  
root@DatabaseVM:/home/databaseuser# ls -ld Documents  
drwxr-xr-x 2 databaseuser databaseuser 4096 Aug 22 04:43 Documents  
root@DatabaseVM:/home/databaseuser# chmod 755 /home/databaseuser/Documents  
root@DatabaseVM:/home/databaseuser#
```





```
Administrator: Windows PowerShell
PS C:\Users\vashishht.vivek\ssh> scp C:\Users\vashishht.vivek\Documents\DataTransferTest.txt databaseuser@10.0.2.4:/home/databaseuser/Documents/
DataTransferTest.txt          100% 149    9.3KB/s  00:00
PS C:\Users\vashishht.vivek\ssh>
```



```
root@DatabaseVM:~/home/databaseuser# ls
Documents
root@DatabaseVM:~/home/databaseuser# cd Documents
root@DatabaseVM:~/home/databaseuser/Documents# ls
DataTransferTest.txt
root@DatabaseVM:~/home/databaseuser/Documents# cat DataTransferTest.txt
This file is for Testing the Data Transfer Between
OnPrem VM and the Azure VM

!!! THIS IS FOR THE DatabaseVM !!!

Sign
Vivek Vashishth root@DatabaseVM:~/home/databaseuser/Documents#
```

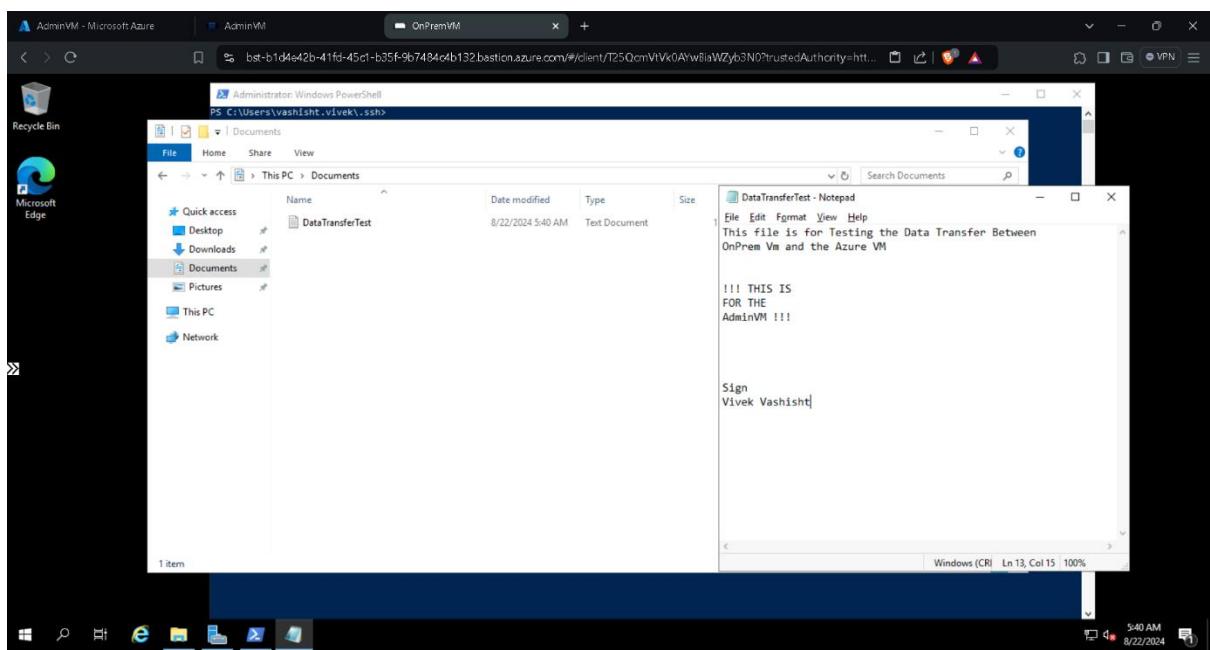
A screenshot of a Windows desktop environment within an Azure VM. The taskbar at the bottom shows icons for Start, Search, Task View, Edge browser, File Explorer, Taskbar settings, and a system tray with battery and network status. In the center, a PowerShell window titled 'Administrator: Windows PowerShell' is open. The command PS C:\Users\AdminUser> Get-WindowsCapability | Where-Object Name -like 'OpenSSH\*' is run, displaying the following output:

```
Name : OpenSSH.Client----0.0.1.0
State : Installed

Name : OpenSSH.Server----0.0.1.0
State : Installed

PS C:\Users\AdminUser> Start-Service sshd
PS C:\Users\AdminUser> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Users\AdminUser> Get-Service -Name sshd
Status   Name               DisplayName
-----   --name--           --displayname--
Running  sshd              OpenSSH SSH Server

PS C:\Users\AdminUser>
```



Administrator: Windows PowerShell

```
PS C:\Users\washisht.vivek1.ssh> scp C:\Users\washisht.vivek\Documents\DataTransferTest.txt AdminUser@10.0.3.4:C:\Users\AdminUser\Documents\DataTransferTestin^
g
The authenticity of host '10.0.3.4 (10.0.3.4)' can't be established.
ECDSA key fingerprint is SHA256:ImuBapMsBBBNW@b1Q0mXbV7oFg@R334CbMfJk7g.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.0.3.4' (ECDSA) to the list of known hosts.
AdminUser@10.0.3.4's password:
DataTransferTest.txt
100% 150 4.7KB/s 00:00
PS C:\Users\washisht.vivek1.ssh>
```

Select Administrator: Windows PowerShell

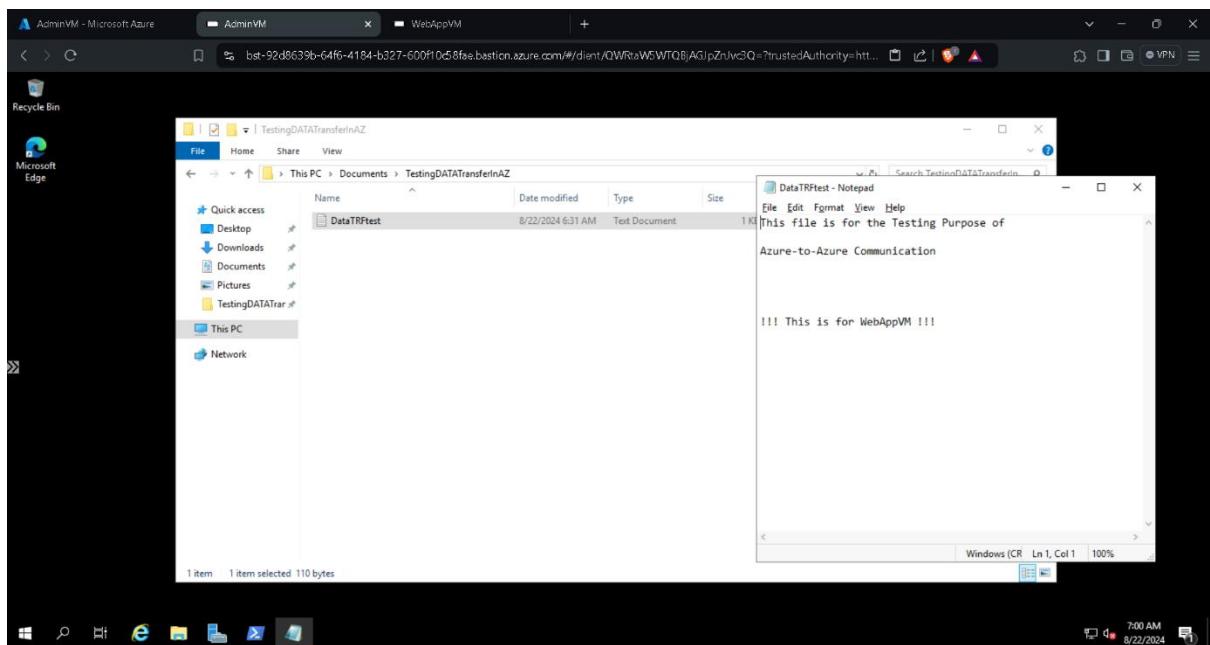
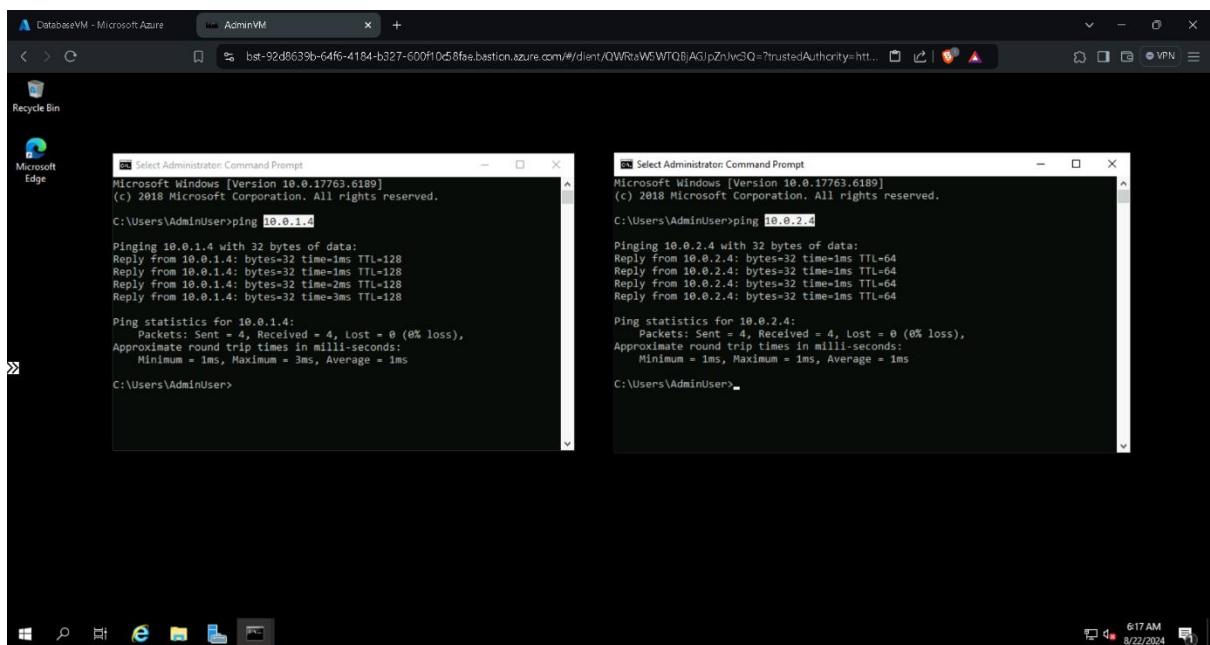
```
PS C:\Users\AdminUser> Get-WindowsCapability -Online | Where-Object Name -like "compositi^
ng
This PC > Documents > DataTransferTesting
```

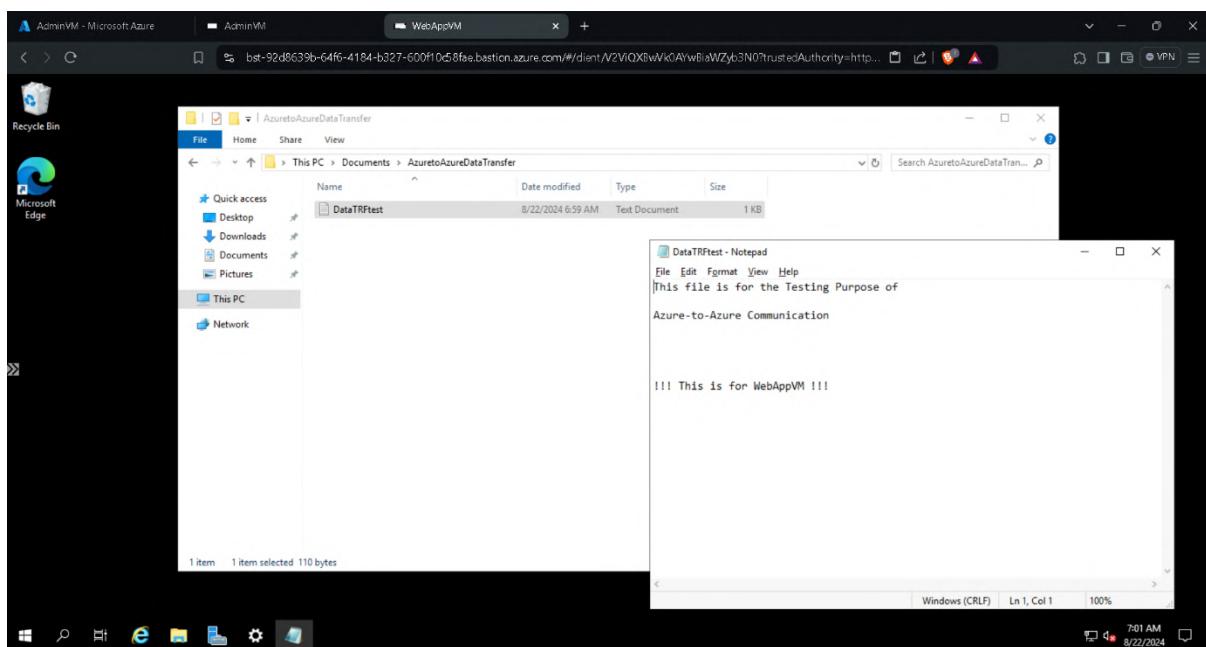
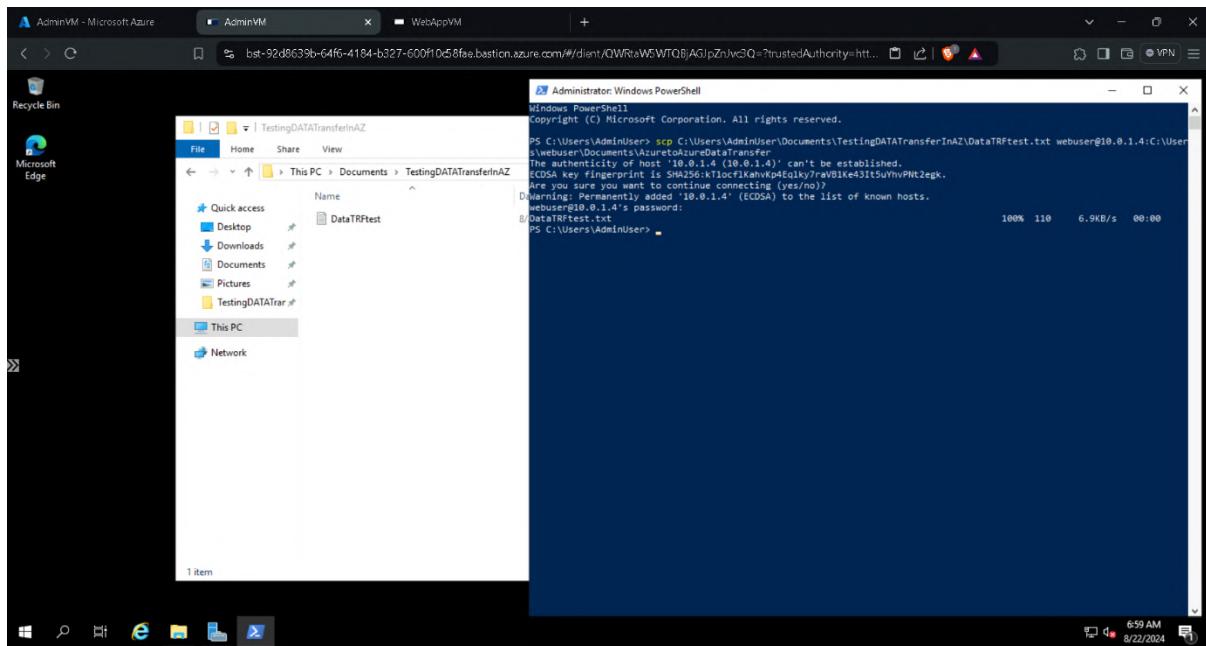
Name	Date modified	Type	Size
DataTransferTest	8/22/2024 5:50 AM	Text Document	150 bytes

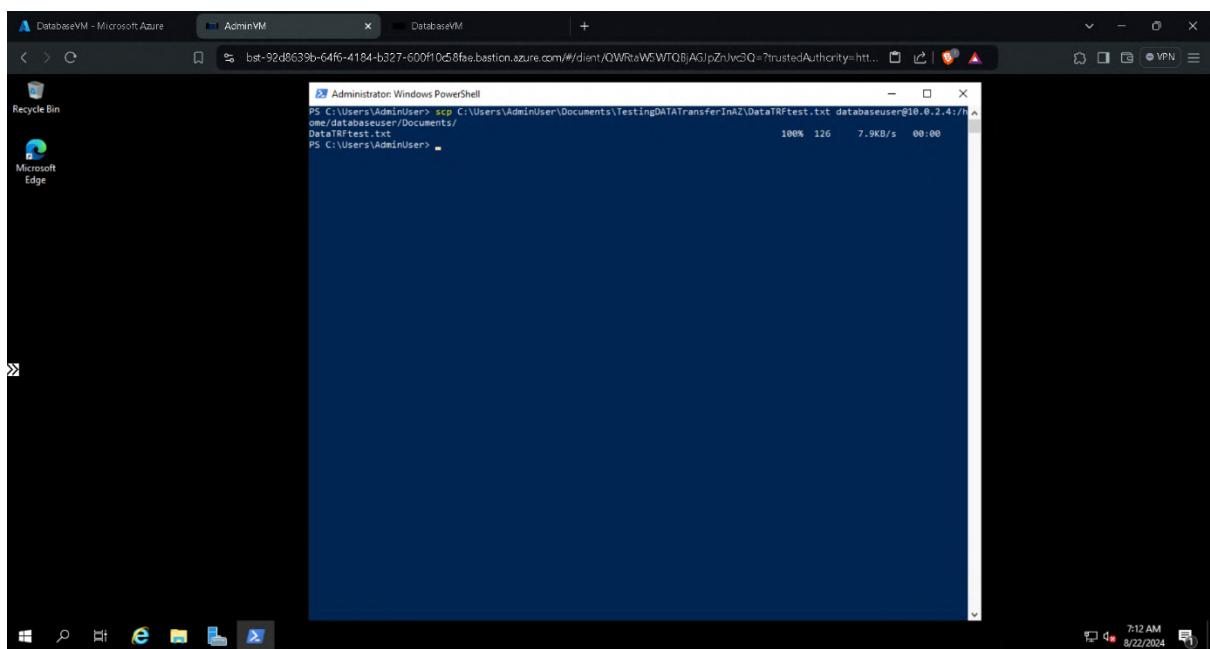
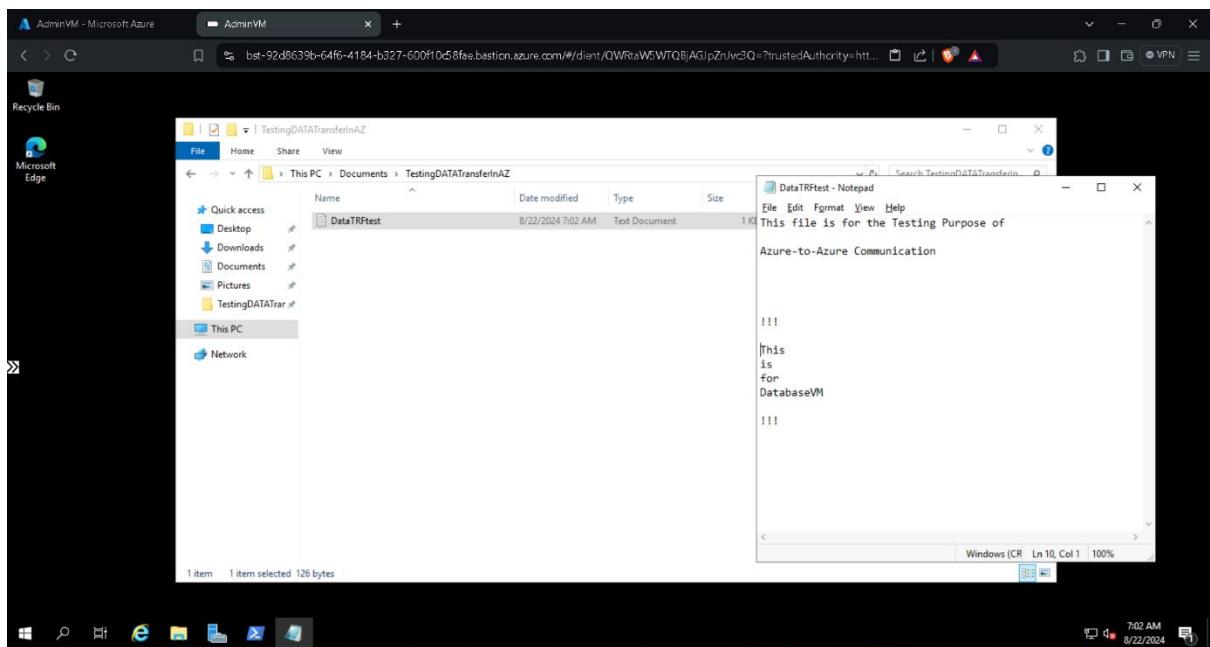
File Transfer - Notepad

```
Windows (CR Ln 9, Col 1) 100%
DataTransferTest - Notepad
File Edit Format View Help
This file is for Testing the Data Transfer Between
OnPrem Vm and the Azure VM

!!! THIS IS
FOR THE
AdminVM !!!
|
Sign
Vivek Vashisht
```



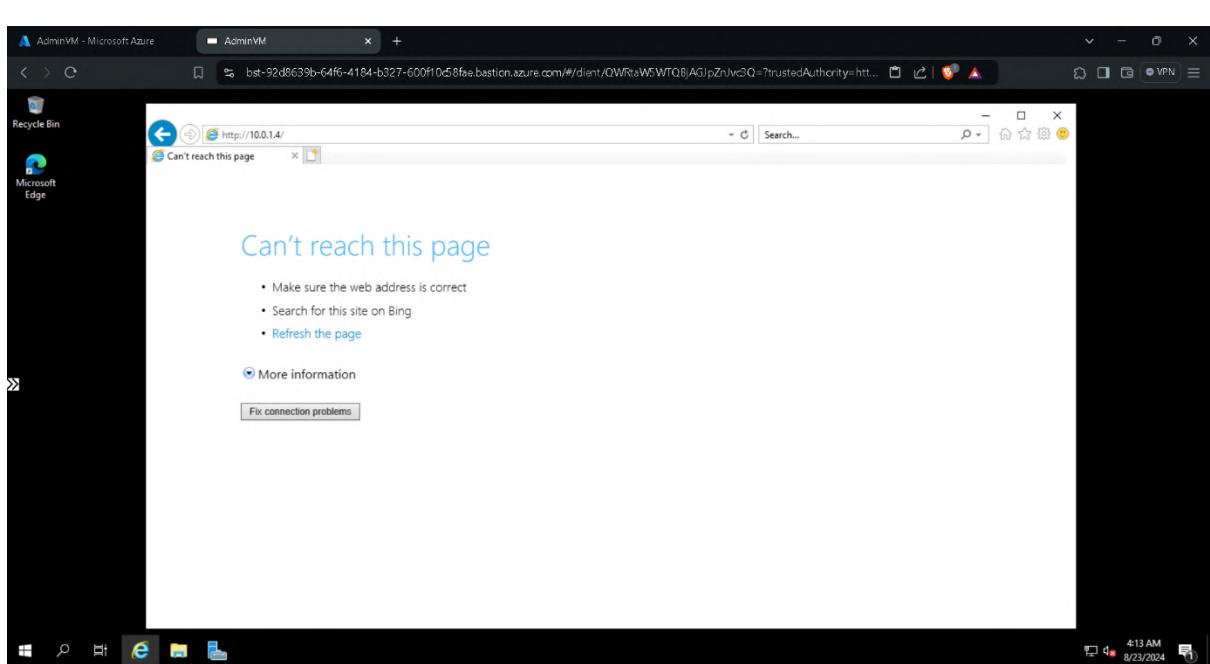


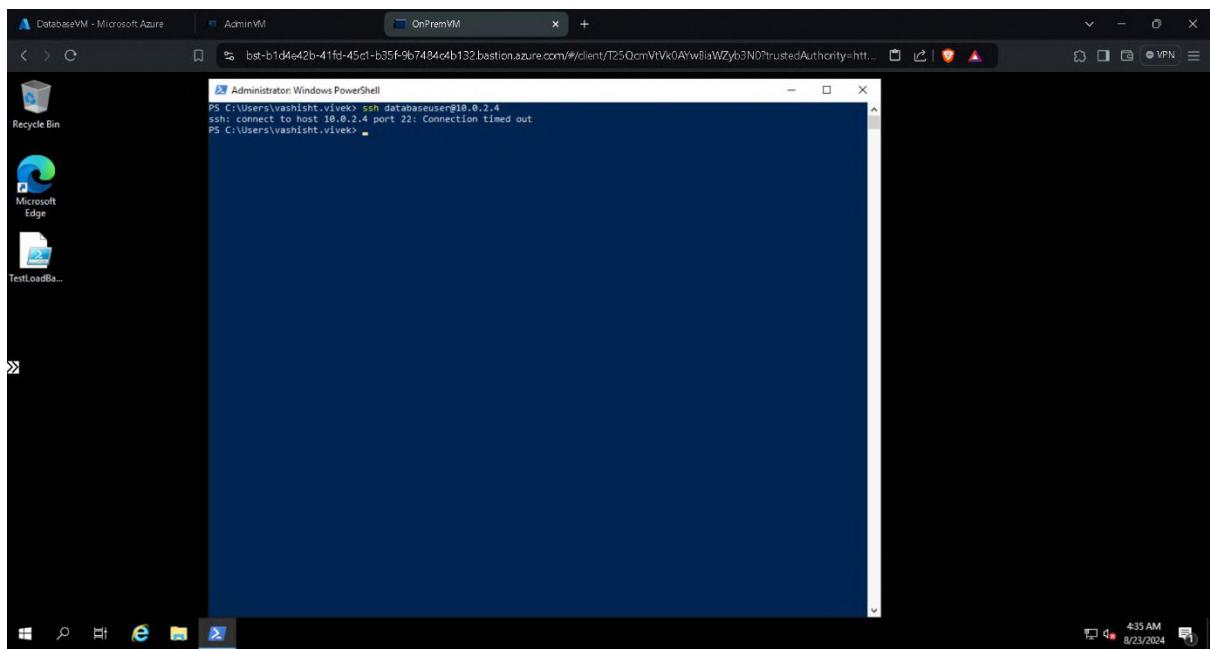
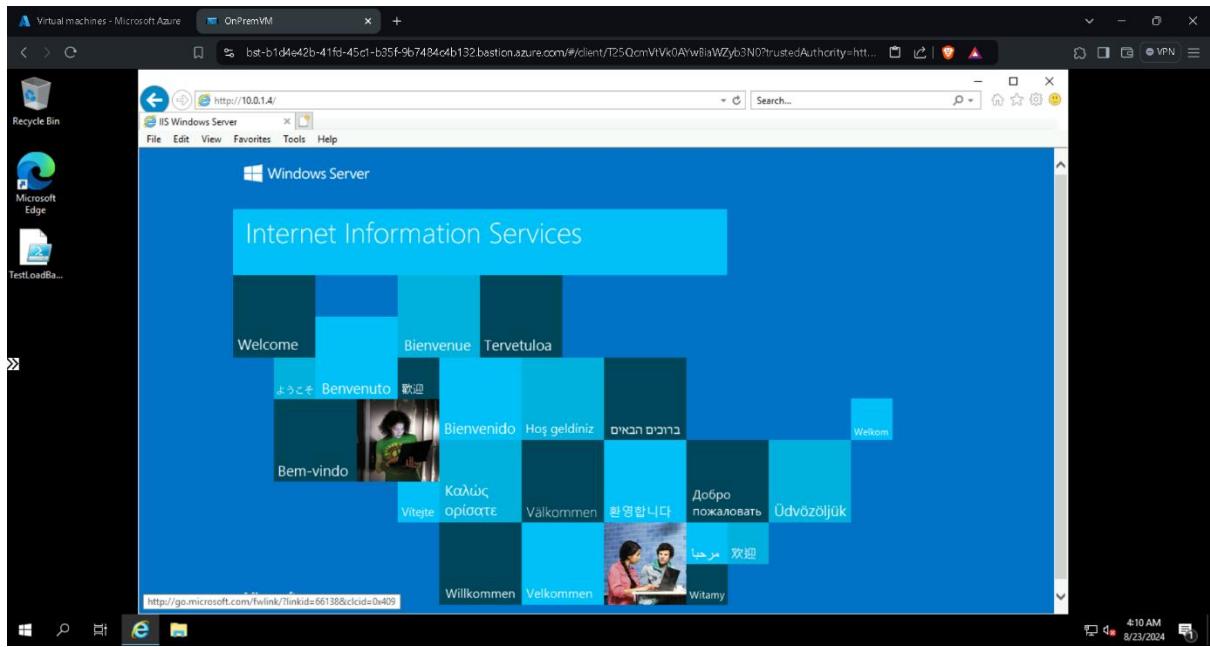


A screenshot of a terminal window titled "DatabaseVM - Microsoft Azure" on the left and "AdminVM" on the right. The AdminVM window shows a command-line session:

```
root@DatabaseVM:/home/databaseuser/Documents# ls
DataTRTest.txt DataTransferTest.txt
root@DatabaseVM:/home/databaseuser/Documents# cat DataTRTest.txt
This file is for the Testing Purpose of
Azure-to-Azure Communication

!!!
This
is
for
DatabaseVM
!!!root@DatabaseVM:/home/databaseuser/Documents#
```





```
PS C:\Users\AdminUser> ssh databaseuser@10.0.2.4
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1025-azure x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Aug 23 04:32:55 UTC 2024
System load: 0.0      Processes:          105
Usage of /: 1.8% of 28.89GB   Users logged in:    0
Memory usage: 734M      IPv4 address for eth0: 10.0.2.4
Swap usage: 0M

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

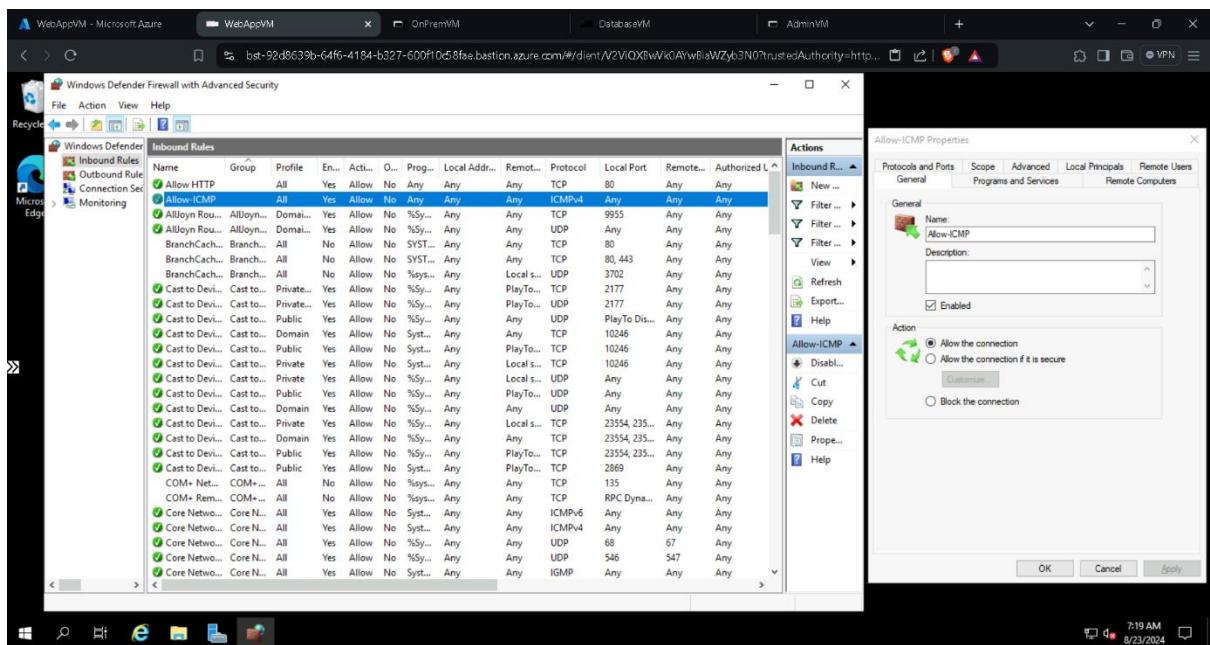
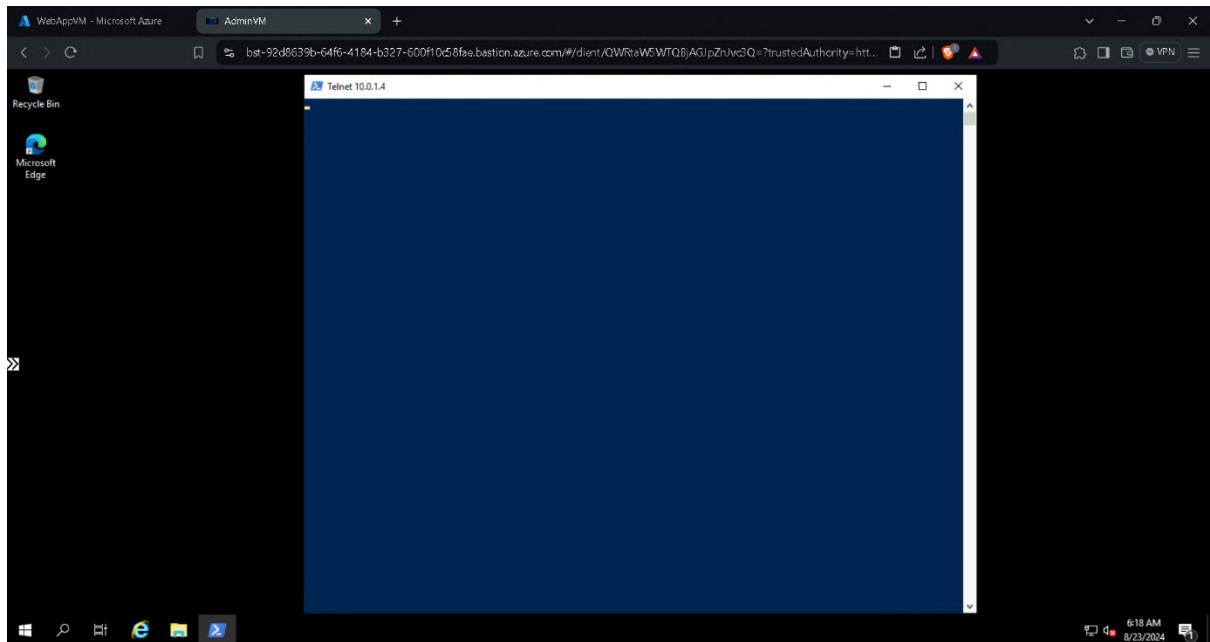
Expanded Security Maintenance For Applications is not enabled.

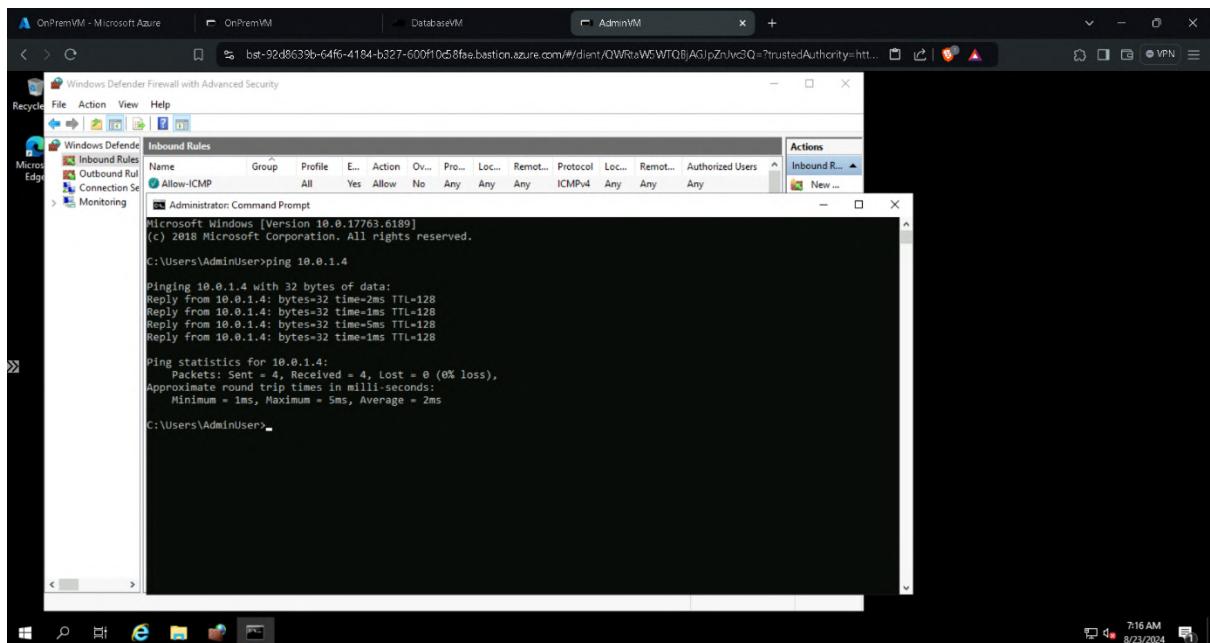
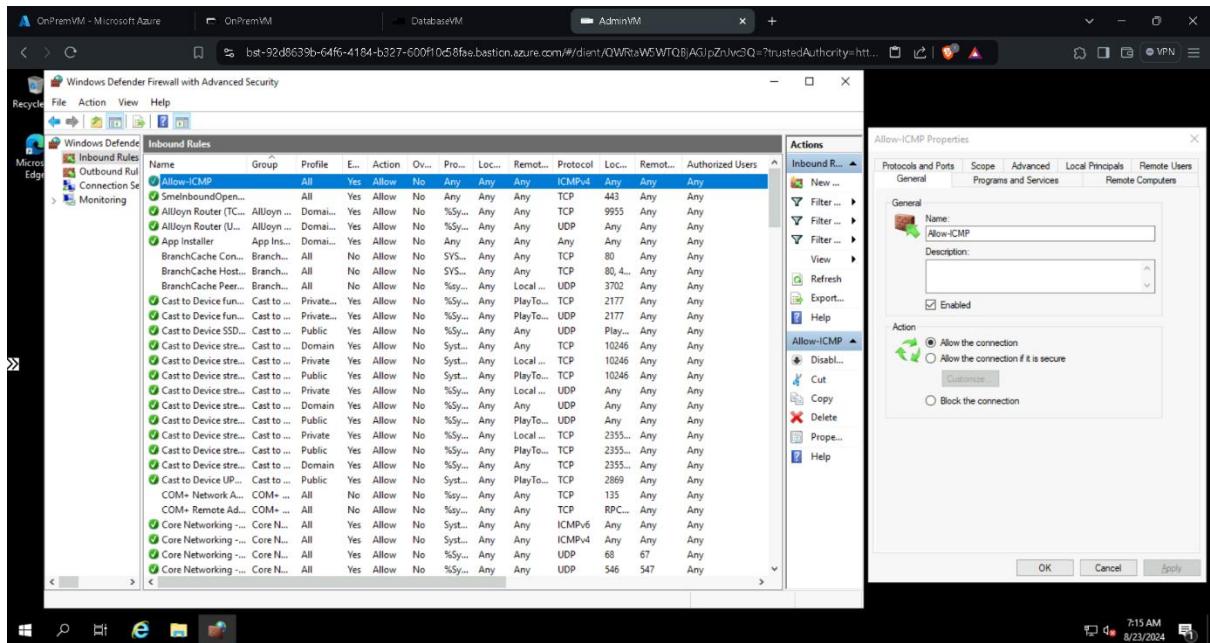
9 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Aug 21 00:11:25 2024 from 10.0.4.4
databaseuser@DatabaseVM: ~
```

```
Administrator: Windows PowerShell
PS C:\Users\vashishth.vivek> telnet 10.0.1.4 3389
Connecting To 10.0.1.4...could not open connection to the host, on port 3389: Connect failed
PS C:\Users\vashishth.vivek>
```

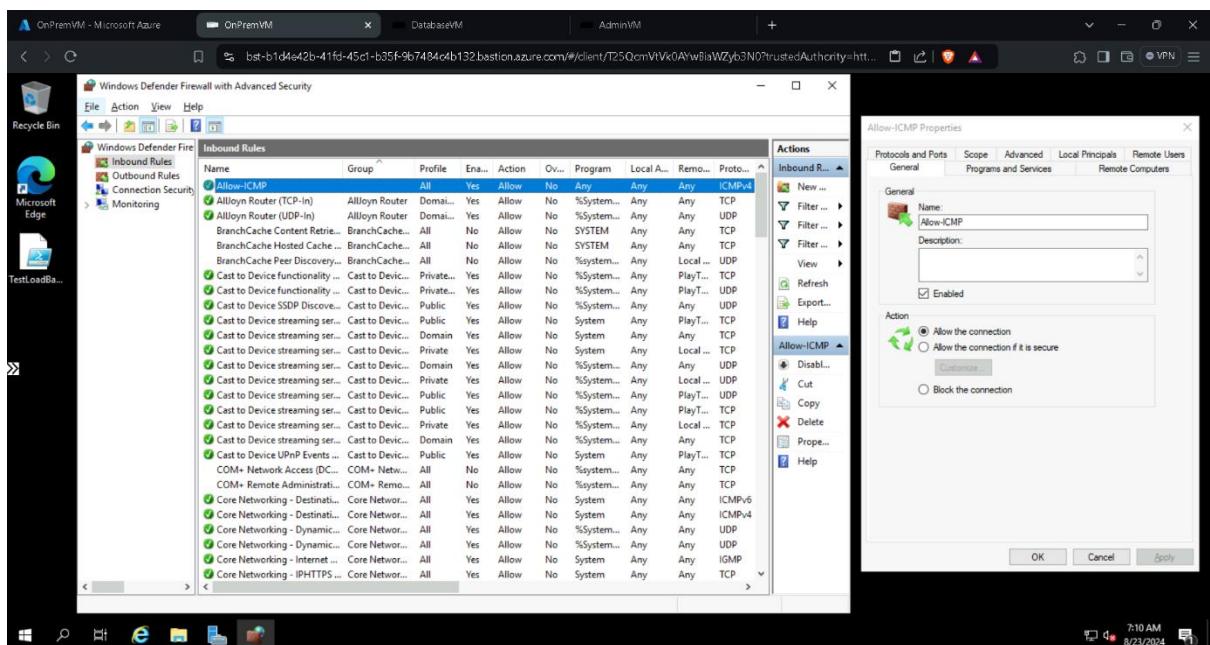


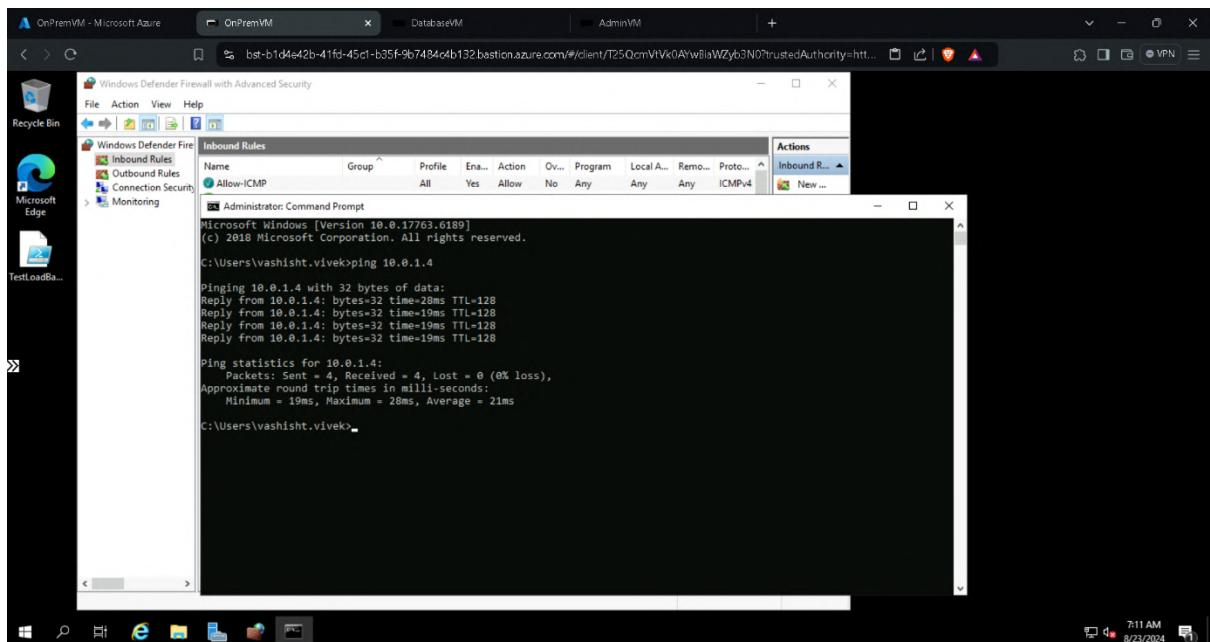


```

OnPremVM - Microsoft Azure
OnPremVM DatabaseVM AdminVM
vivekvash1507@gmail.com@DatabaseVM:~$ ping 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp seq=1 ttl=128 time=1.61 ms
64 bytes from 10.0.1.4: icmp seq=2 ttl=128 time=1.56 ms
64 bytes from 10.0.1.4: icmp seq=3 ttl=128 time=2.97 ms
64 bytes from 10.0.1.4: icmp seq=4 ttl=128 time=1.12 ms
64 bytes from 10.0.1.4: icmp seq=5 ttl=128 time=1.16 ms
64 bytes from 10.0.1.4: icmp seq=6 ttl=128 time=1.65 ms
64 bytes from 10.0.1.4: icmp seq=7 ttl=128 time=1.33 ms
64 bytes from 10.0.1.4: icmp seq=8 ttl=128 time=1.35 ms
64 bytes from 10.0.1.4: icmp seq=9 ttl=128 time=1.43 ms
64 bytes from 10.0.1.4: icmp seq=10 ttl=128 time=2.21 ms
64 bytes from 10.0.1.4: icmp seq=11 ttl=128 time=1.35 ms
64 bytes from 10.0.1.4: icmp seq=12 ttl=128 time=1.85 ms
64 bytes from 10.0.1.4: icmp seq=13 ttl=128 time=2.14 ms
64 bytes from 10.0.1.4: icmp seq=14 ttl=128 time=1.45 ms
64 bytes from 10.0.1.4: icmp seq=15 ttl=128 time=1.20 ms
^C
--- 10.0.1.4 ping statistics ---
20 packets transmitted, 15 received, 0% packet loss, time 14021ms
rtt min/avg/max/mdev = 1.124/1.624/2.965/0.476 ms
vivekvash1507@gmail.com@DatabaseVM:~$ 

```





The screenshot shows the Microsoft Azure Network Watcher overview page. The left sidebar includes options like Get started, Monitoring (Topology, Connection monitor, Traffic Analytics), Network diagnostic tools, Metrics, and Logs. The main area displays a table of resources, with the first two entries being "NetworkWatcher\_canadacentral" and "NetworkWatcher\_northcentralus", both associated with "Azure subscription 1" and located in "Canada Central" and "North Central US" respectively.

Name	Subscription	Location
NetworkWatcher_canadacentral	Azure subscription 1	Canada Central
NetworkWatcher_northcentralus	Azure subscription 1	North Central US

**Network Watcher - Microsoft Azure**

portal.azure.com/?feature.msajs=true#view/Microsoft\_Azure\_Network/NetworkWatcherMenuBlade~/flowLogs

Microsoft Azure

Home > Network Watcher

Network Watcher | Flow logs

Search  Create Manage view Refresh Export to CSV Open query Assign tags Enable Disable Delete

Overview Get started Monitoring Network diagnostic tools Metrics Logs

Flow logs Migrate flow logs Diagnostic logs

Subscription equals all Resource group equals all Location equals all Filter for any item... Add filter

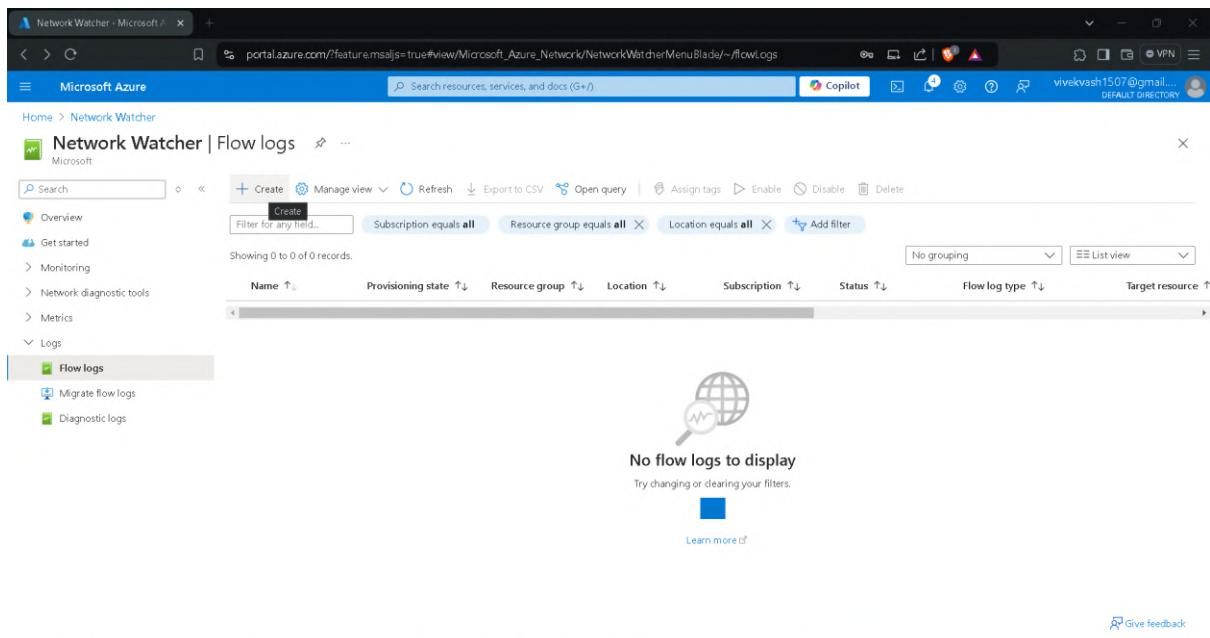
No grouping List view

Name Provisioning state Resource group Location Subscription Status Flow log type Target resource

No flow logs to display

Try changing or clearing your filters.

Learn more ↗ Give feedback ↗



**Create storage account - Microsoft Azure**

portal.azure.com/?feature.msajs=true#create/Microsoft.NSGFlowLog-ARM

Microsoft Azure

Home > Network Watcher | Flow logs > Create a flow log

Create storage account

Virtual network Select target resource

Flow Log Name	Resource	Resource Group	Target Resource Type
WebAppNSG-netmazer...	WebAppNSG	netmazer	Network security group

Instance details

Select storage account

You'll be charged normal data rates for storage and transactions when you send data to a storage account.

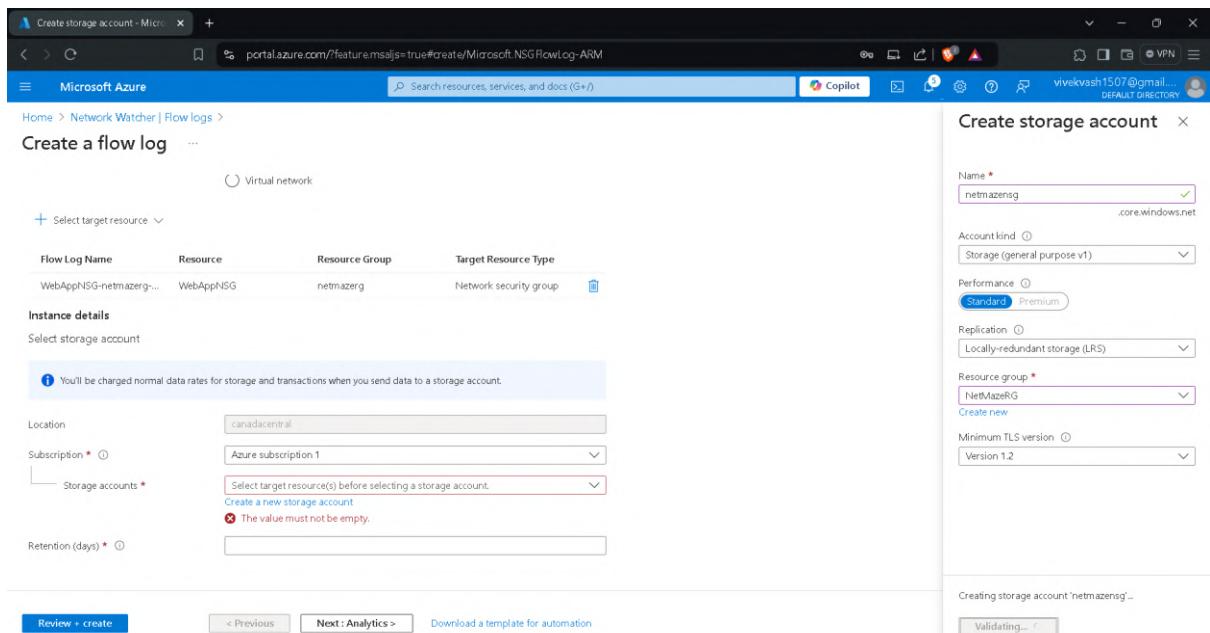
Location: canadacentral  
Subscription: Azure subscription 1  
Storage accounts: Select target resource(s) before selecting a storage account. Create a new storage account  
Retention (days):

Name: netmazer

Account kind: Storage (general purpose v1)  
Performance: Standard Premium  
Replication: Locally-redundant storage (LRS)  
Resource group: NetMazeRG  
Minimum TLS version: Version 1.2

Creating storage account 'netmazer'...

Review + create < Previous Next : Analytics > Download a template for automation Validating...



Create a flow log - Microsoft Azure

portal.azure.com/?feature.msals=true#create/Microsoft.NSGFlowLog-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY

Home > Network Watcher | Flow logs >

Create a flow log ...

Validation passed

Basics Analytics Tags Review + create

**Basics**

Subscription	Azure subscription 1
Resource	WebAppNSG
Location	canadacentral
Flow Log Name	WebAppNSG-netmazerg-flowlog
Storage accounts	netmazeng

**Analytics**

Flow logs version	2
Flow Log Type	Network security group
Enable traffic analytics	No

**Tags**

None

Create < Previous Next > Download a template for automation

The screenshot shows the 'Create a flow log' wizard in the Azure portal. It's on the 'Review + create' step. The 'Validation passed' message is displayed. The 'Basics' section shows the subscription is 'Azure subscription 1', the resource is 'WebAppNSG', the location is 'canadacentral', the flow log name is 'WebAppNSG-netmazerg-flowlog', and the storage account is 'netmazeng'. The 'Analytics' section shows the flow log version is 2, the type is 'Network security group', and traffic analytics are disabled. There are no tags assigned. At the bottom, there are buttons for 'Create', navigation arrows, and a download template link.

Flow logs - Microsoft Azure

portal.azure.com/?feature.msals=true#view/HubsExtension/BrowseResource/resourceType/microsoft.network%2Fnetworkw...  
Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY

Home > Microsoft.NSGFlowLog-20240823013932 | Overview >

Flow logs ...

Default Directory

+ Create Manage view Refresh Export to CSV Open query Assign tags Enable Disable Delete

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

No grouping List view

Name	Provisioning state	Resource group	Location	Subscription	Status	Flow log type	Target resour...	Storage account
WebAppNSG-netmazerg-flowlog (NetworkWatcher_canadacentr...	Succeeded	NetworkWatcherRG	Canada Central	Azure subscription 1	Enabled	Network security group	WebAppNSG	netmazeng

< Previous Page 1 of 1 Next > Give feedback

The screenshot shows the 'Flow logs' overview page for the 'WebAppNSG-netmazerg-flowlog' resource. It lists one record: 'WebAppNSG-netmazerg-flowlog (NetworkWatcher\_canadacentr...)' with a provisioning state of 'Succeeded', located in 'NetworkWatcherRG' resource group, in 'Canada Central' location, and associated with 'Azure subscription 1'. The status is 'Enabled' and the flow log type is 'Network security group'. The target resource is 'WebAppNSG' and the storage account is 'netmazeng'. Navigation buttons for previous, next pages, and a feedback link are at the bottom.

WebAppNSG - Microsoft Azure AdminVM

portal.azure.com/?feature.msaljs=true#vivekvash1507@gmail.onmicrosoft.com/resource/subscriptions/e9ea131-d6f1-... Copilot

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

vivekvash1507@gmail... DEFAULT DIRECTORY

Home > WebAppNSG

WebAppNSG | Inbound security rules

Network security group

Search Add Hide default rules Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Priority ↑	Name ↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	Allow-RDP-AdminVM	3389	TCP	10.0.3.4	10.0.1.4	Allow
110	Deny-RDP-OnPremVM-and-Database	3389	TCP	10.1.0.2/4,10.0.2.4	10.0.1.4	Deny
120	Allow-HTTPS-443	443	TCP	10.1.0.0/16	Any	Allow
130	Allow-HTTP-OnPremVM-ILB	80	TCP	10.1.0.0/16	VirtualNetwork	Allow
140	⚠ Deny-HTTP-Unauthorized-ILB	80	TCP	Any	VirtualNetwork	Deny
150	Allow-ILB-Probe	80	TCP	VirtualNetwork	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

WebAppNSG - Microsoft Azure AdminVM

bst-92d8639b-64f6-4184-b327-600f10x56faa.bastion.azure.com/#/client/QWRtaWEWTQJAGlpZnJvCQ=?trustedAuthority...

Recycle Bin Microsoft Edge Can't reach this page http://10.0.1.4/

Can't reach this page

- Make sure the web address is correct
- Search for this site on Bing
- Refresh the page

More information Fix connection problems

8:01 AM 8/23/2024

Microsoft Azure

Home > Storage accounts > netmazeng

netmazeng | Containers

Storage account

Search containers by prefix

Name	Last modified	Anonymous access level	Lease state
insights-logs-networksecuritygroupflowevent	8/23/2024, 1:45:17 AM	Private	Available

Containers

- File shares
- Queues
- Tables

Security + networking

Data management

Settings

Monitoring

Monitoring (classic)

Microsoft Azure

Home > Storage accounts > netmazeng | Containers >

insights-logs-networksecuritygroupflowevent

Container

Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots Create snapshot Give feedback

Authentication method: Access key (Switch to Microsoft Entra user account)  
Location: insights-logs-networksecuritygroupflowevent / resources / SUBSCRIPTIONS / EE9EA131-D6F1-4E0B-BAEE-B293615685AE / RESOURCEGROUPS / NETMAZERG / PROVIDERS / MICROSOFT.NETWORK / NETWORKSECURITYGROUPS / WEBAPNNSG / y=2024 / m=08 / d=23 / h=07 / m=00 / macAddress=000D3AE8B0EF

Search blobs by prefix (case-sensitive)

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
{} [..]						
PT1H.json	8/23/2024, 2:01:16 AM			Block blob	37.2 kB	Available

## **Monitoring and Auditing**

## 11.1. Creating Log Analytics Workspaces

First, I needed to create Log Analytics Workspaces to centralize monitoring and diagnostics data for the project's resources.

- **NetMazeWorkspace:**
    - I logged into the Azure portal and navigated to the **Log Analytics Workspaces** section.
    - Clicked on + Create to initiate the workspace creation process.
    - Entered the following details:
      - **Resource Group Name:** NetMazeRG
      - **Region:** Canada Central
      - **Workspace Name:** NetMazeWorkspace
    - After filling in the details, I clicked on Review + Create and then selected Create to finalize the deployment.

- **OnPremWorkspace:**
  - Repeated the same process to create another Log Analytics Workspace.
  - Entered the following details:
    - **Resource Group Name:** NetMazeRG
    - **Region:** North Central US
    - **Workspace Name:** OnPremWorkspace
  - After filling in the details, I clicked on `Review + Create` and then selected `Create` to finalize the deployment.

## 11.2. Enabling Monitoring

Next, I enabled monitoring on key network resources, including VPN Gateways, NSGs, SQL Database, and Load Balancer.

- **VPN Gateways:**
  - I navigated to the **Azure Monitor** section in the Azure portal and selected **Diagnostics Settings**.
  - **NetMazeVPNGateway:**
    - Selected `NetMazeVPNGateway` as the resource.
    - Clicked on `+ Add Diagnostic Setting` and configured it with the following details:
      - **Diagnostic Setting Name:** `NetMazeVPNGatewayDiagnostics`
      - **Logs:** Selected `allLogs`
      - **Metrics:** Selected `AllMetrics`
      - **Destination:** Sent to Log Analytics Workspace (`NetMazeWorkspace`)
    - Clicked on `Save` to apply the settings.
  - **OnPremVPNGateway:**
    - Repeated the same steps to configure diagnostics for `OnPremVPNGateway`.
    - Sent the logs and metrics to the `OnPremWorkspace`.
- **NSGs:**
  - I enabled monitoring on all Network Security Groups (NSGs) by following similar steps:
    - Selected each NSG individually in the **Diagnostics Settings** of Azure Monitor.
    - Configured and saved the diagnostics settings for each with the appropriate Log Analytics Workspace.

The following NSGs were configured:

- **WebAppNSG:** Sent to NetMazeWorkspace
- **DatabaseNSG:** Sent to NetMazeWorkspace
- **AdminNSG:** Sent to NetMazeWorkspace
- **OnPremVM-nsg:** Sent to OnPremWorkspace
- **WebAppVM-nsg:** Sent to NetMazeWorkspace
- **DatabaseVM-nsg:** Sent to NetMazeWorkspace
- **AdminVM-nsg:** Sent to NetMazeWorkspace

- **SQL Database:**

- I enabled monitoring on the SQL Databases:
  - **NetMazeSQLDB:**
    - Selected netmazesqlserver/NetMazeSQLDB as the resource.
    - Configured the diagnostic settings to include all relevant logs and metrics.
    - Sent to NetMazeWorkspace.
  - **dbmaster:**
    - Selected netmazesqlserver/master as the resource.
    - Configured the diagnostic settings similarly and sent them to NetMazeWorkspace.

- **Load Balancer:**

- I enabled monitoring on the Load Balancer:
  - Selected NetMazeLoadBalancer as the resource.
  - Configured the diagnostic settings to include all relevant logs and metrics.
  - Sent to NetMazeWorkspace.

### 11.3. Setting Up Alerts

After enabling monitoring, I set up alerts for key events, such as unauthorized SSH attempts and VPN Gateway downtime.

- **Unauthorized SSH Attempts Alert:**

- I went to the **Alerts** tab in Azure Monitor and clicked on + Alert Rule.
- **Scope:** Selected DatabaseNSG as the resource.
- **Condition:**
  - Selected Custom Log Search.
  - Entered the following query to detect unauthorized SSH attempts:

```

AzureDiagnostics
| where ResourceType == "NETWORKSECURITYGROUPS"
| where OperationName == "NetworkSecurityGroupEvents"
| where ruleName_s == "UserRule_Deny-SSH-OnPrem"
| where conditions destinationPortRange_s == "22-22"

```

- Set the alert to trigger when there are 5 or more occurrences within 5 minutes.
- **Actions:** Created an action group to send an email notification to vivekvash1507@gmail.com.
- **Details:** Named the alert Unauthorized SSH Attempt Alert and set its severity to 0 - Critical.

- **VPN Gateway Downtime Alert:**

- I set up a similar alert for VPN Gateway downtime:
  - **Scope:** Selected NetMazeVPNGateway and OnPremVPNGateway as the resources.
  - **Condition:** Chose Resource Health with a signal name of Resource health set to Unavailable.
  - **Actions:** Created an action group for email notifications.
  - **Details:** Named the alert VPN Gateway Downtime Alert with a global region.

## 11.4. Reviewing Logs and Metrics

To ensure that everything was functioning as expected, I reviewed logs and metrics.

- **Logs:**

- To test the Unauthorized SSH Attempts Alert, I attempted to SSH into DatabaseVM from OnPremVM.
- As expected, the attempt was denied.
- I then ran a Kusto Query in the NetMazeWorkspace to confirm that the denial was logged:

```

AzureDiagnostics | where ResourceType ==
"NETWORKSECURITYGROUPS"

```

- The results confirmed that the SSH attempt was blocked by the UserRule\_Deny-SSH-OnPrem rule.

- **Metrics:**

- I reviewed key metrics to monitor resource performance:
  - Created a chart for **Percentage CPU** usage across all VMs.
  - Monitored **Health Probe Status** for NetMazeLoadBalancer.

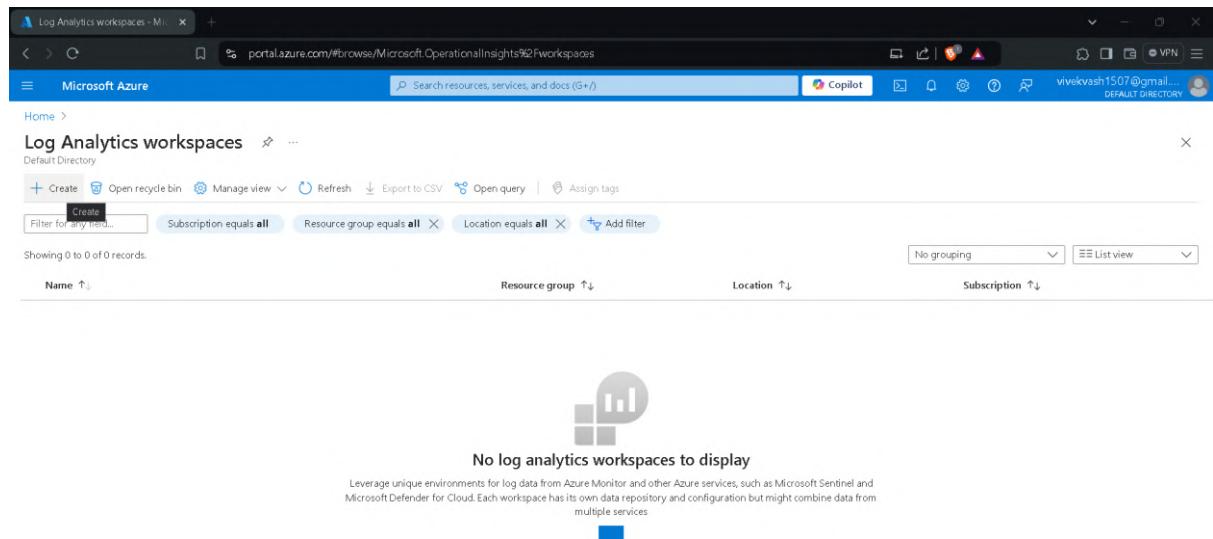
- Reviewed **App CPU percentage** for the SQL databases (NetMazeSQLDB and dbmaster).
- Created charts for **Max Gateway Outbound Flows** and **Avg Tunnel Bandwidth** for NetMazeVPNGateway and OnPremVPNGateway.

## 11.5. Finalizing Monitoring and Auditing

To centralize monitoring, I added all created charts to the Azure Dashboard for real-time monitoring of network performance and security events.

- **Summary:**
  - Enabled comprehensive monitoring across VPN Gateways, NSGs, SQL Databases, and Load Balancers.
  - Set up critical alerts for unauthorized SSH attempts and VPN Gateway downtime.
  - Reviewed logs and metrics to ensure everything was functioning correctly.
  - Centralized all monitoring data in the Azure Dashboard for ongoing oversight.

## Screenshots



[Create Log Analytics workspace](https://portal.azure.com/#create/Microsoft.LogAnalyticsOMS)

Microsoft Azure

Home > Log Analytics workspaces >

## Create Log Analytics workspace

**BASICS** Tags Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

**Project details**

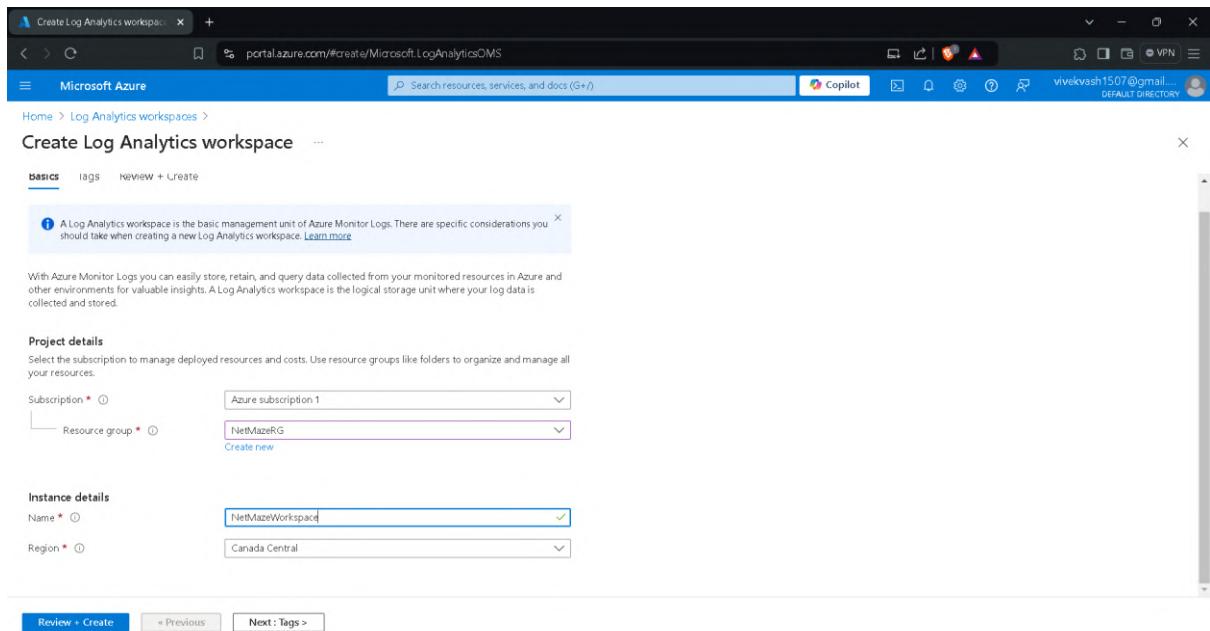
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*  Resource group \*

**Instance details**

Name \*  Region \*

**Review + Create** **< Previous** **Next : Tags >**



[NetMazeWorkspace - Microsoft Log Analytics workspace](https://portal.azure.com/#/vivekvash1507@gmail.com/microsoft/LogAnalyticsOMS/Overview)

Microsoft Azure

Home > Microsoft Log Analytics workspace | Overview >

## NetMazeWorkspace

Log Analytics workspace

Search Delete

**Overview**

**Essentials**

Resource group ( <a href="#">move</a> )	: <a href="#">netmazerg</a>
Status	: Active
Location	: <a href="#">Canada Central</a>
Subscription ( <a href="#">move</a> )	: <a href="#">Azure subscription 1</a>
Subscription ID	: ee9ea131-d6f1-4e0b-baee-b293615685ae
Tags ( <a href="#">edit</a> )	: <a href="#">Add tags</a>

Get Started Recommendations

**Get started with Log Analytics**

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

**1 Connect a data source**

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)  
Windows and Linux Agents management  
Storage account log  
System Center Operations Manager

**2 Configure monitoring solutions**

Add monitoring solutions that provide insights for applications and services in your environment

[View solutions](#)

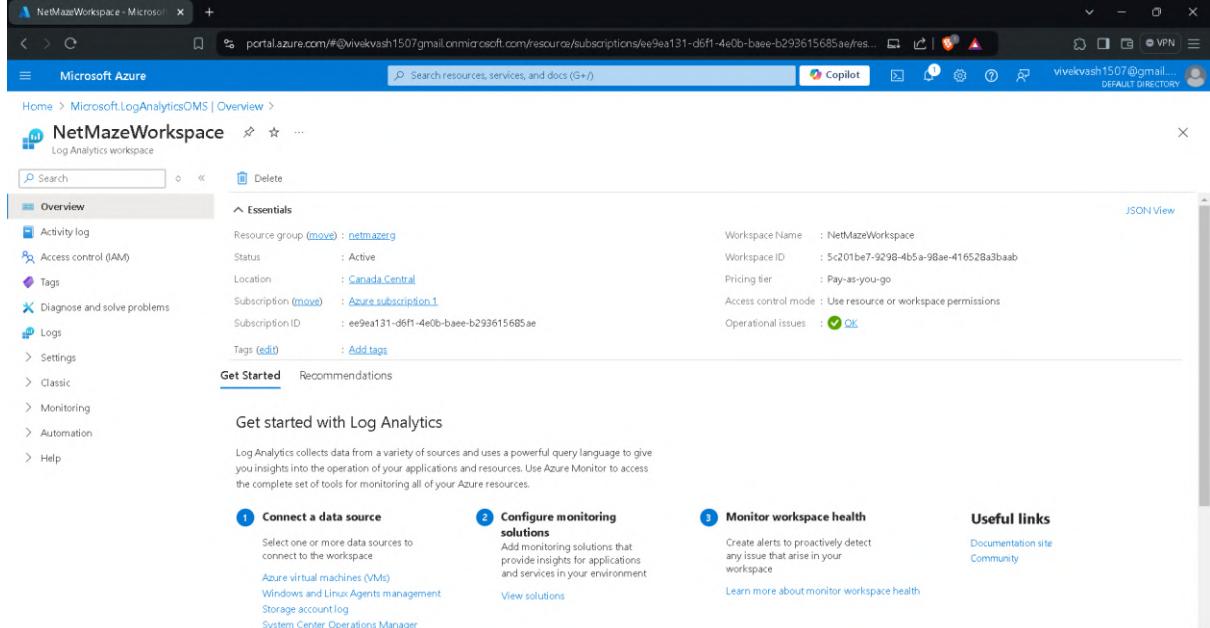
**3 Monitor workspace health**

Create alerts to proactively detect any issue that arise in your workspace

[Learn more about monitor workspace health](#)

**Useful links**

Documentation site  
Community



**OnPremWorkspace - Microsoft**

Microsoft Azure

Home > Log Analytics workspaces >

## OnPremWorkspace

Log Analytics workspace

Search Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Settings

- Tables
- Agents
- Usage and estimated costs
- Data export
- Network isolation
- Linked storage accounts
- Properties
- Locks

Get Started Recommendations

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)  
Windows and Linux Agents management  
Storage account log  
System Center Operations Manager

2 Configure monitoring solutions

Add monitoring solutions that provide insights for applications and services in your environment

View solutions

3 Monitor workspace health

Create alerts to proactively detect any issue that arise in your workspace

Learn more about monitor workspace health

Useful links

Documentation site  
Community

JSON View

This screenshot shows the 'OnPremWorkspace' Log Analytics workspace in the Microsoft Azure portal. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Settings, Tables, Agents, Usage and estimated costs, Data export, Network isolation, Linked storage accounts, Properties, and Locks. The main content area displays workspace details such as Resource group (netmazer), Status (Active), Location (North Central US), Subscription (Azure subscription 1), and Subscription ID (ee9ea131-d6f1-4e0b-bae6-b293615685ae). It also shows operational issues with a green checkmark and 'OK'. Below this, there's a 'Get Started' section with 'Recommendations' and a 'Get started with Log Analytics' summary. The 'Essentials' section provides a quick overview of workspace configuration and monitoring.

**Monitor - Microsoft Azure**

Microsoft Azure

Home >

## Monitor | Overview

Overview Tutorials

The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date. →

Insights

Use curated monitoring views for specific Azure resources. [View all insights](#)

<b>Application insights</b> Monitor your app's availability, performance, errors, and usage. <a href="#">View More</a>	<b>Container Insights</b> Gain visibility into the performance and health of your controllers, nodes, and containers. <a href="#">View More</a>	<b>VM Insights</b> Monitor the health, performance, and dependencies of your VMs and VM scale sets. <a href="#">View More</a>	<b>Network Insights</b> View the health and metrics for all deployed network resources. <a href="#">View More</a>
--	---	---	---

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. [Learn more about monitoring](#)

<b>Metrics</b> Create charts to monitor and investigate the usage and performance of your Azure resources. <a href="#">View More</a>	<b>Alerts</b> Get notified and respond using alerts and actions. <a href="#">View More</a>	<b>Logs</b> Analyze and diagnose issues with log queries. <a href="#">View More</a>	<b>Workbooks</b> View, create and share interactive reports. <a href="#">View More</a>
		<b>Azure Monitor SCOM managed instance</b>	<b>Managed Prometheus</b>

[https://portal.azure.com/?feature.msajs=true#view/Microsoft\\_Azure\\_Monitoring/AzureMonitoringBrowseBlade/-/overview](https://portal.azure.com/?feature.msajs=true#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/-/overview)

This screenshot shows the 'Monitor | Overview' page in the Microsoft Azure portal. The left sidebar includes options like Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Investigator (preview), Insights, Applications, Virtual Machines, Storage accounts, Containers, Networks, SQL (preview), and Azure Cosmos DB. The main content area features sections for Insights (Application insights, Container Insights, VM Insights, Network Insights) and Detection, triage, and diagnosis (Metrics, Alerts, Logs, Workbooks, Azure Monitor SCOM managed instance, Managed Prometheus). A note at the top indicates that Log Analytics agents will be unsupported by August 31, 2024, and users are encouraged to migrate to VM Insights on Azure Monitor agent.

**Monitor | Diagnostic settings**

Subscription: Azure subscription 1 Resource group: NetMazeRG Resource type: Virtual network gateways Resource: NetMazeVPNGateway

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. [Learn more about diagnostic settings](#)

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
No diagnostic settings defined					

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Gateway Diagnostic Logs
- Tunnel Diagnostic Logs
- Route Diagnostic Logs
- IKE Diagnostic Logs
- P2S Diagnostic Logs
- AllMetrics

Log Analytics workspaces

Azure Stack HCI

Service Bus (preview)

... Insights Hub

Managed Services

Managed Prometheus

Azure Managed Grafana

Azure Monitor SCOM managed instance

Settings

Diagnostic settings

Data Collection Rules

Data Collection Endpoints

Azure Monitor pipelines (preview)

Autoscale

Private Link Scopes

Support + Troubleshooting

**Diagnostic setting - Microsoft**

Diagnostic setting name: NetMazeVPNGatewayDiagnostics

Destination details

Logs

Category groups: allLogs (checked), Audit (unchecked)

Categories: Gateway Diagnostic Logs (checked), Tunnel Diagnostic Logs (checked), Route Diagnostic Logs (checked), IKE Diagnostic Logs (checked), P2S Diagnostic Logs (checked)

Metrics

AllMetrics (checked)

Send to Log Analytics workspace (checked)

Subscription: Azure subscription 1

Log Analytics workspace: NetMazeWorkspace (canadacentral)

Archive to a storage account (unchecked)

Stream to an event hub (unchecked)

Send to partner solution (unchecked)

**Diagnostic setting - Microsoft/**

portal.azure.com/?feature.msajs=true#view/Microsoft\_Azure\_Monitoring/ServiceDiagnosticsSettingsUpdateBlade/diagnosticsSetting

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekvash1507)

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#).

Diagnostic setting name \* OnPremVPNGatewayDiagnostics

**Logs**

Category groups  allLogs  Audit

Categories  Gateway Diagnostic Logs  Tunnel Diagnostic Logs  Route Diagnostic Logs  IKE Diagnostic Logs  P2S Diagnostic Logs

**Destination details**

Send to Log Analytics workspace

Subscription Azure subscription 1

Log Analytics workspace OnPremWorkspace (northcentralus)

Archive to a storage account

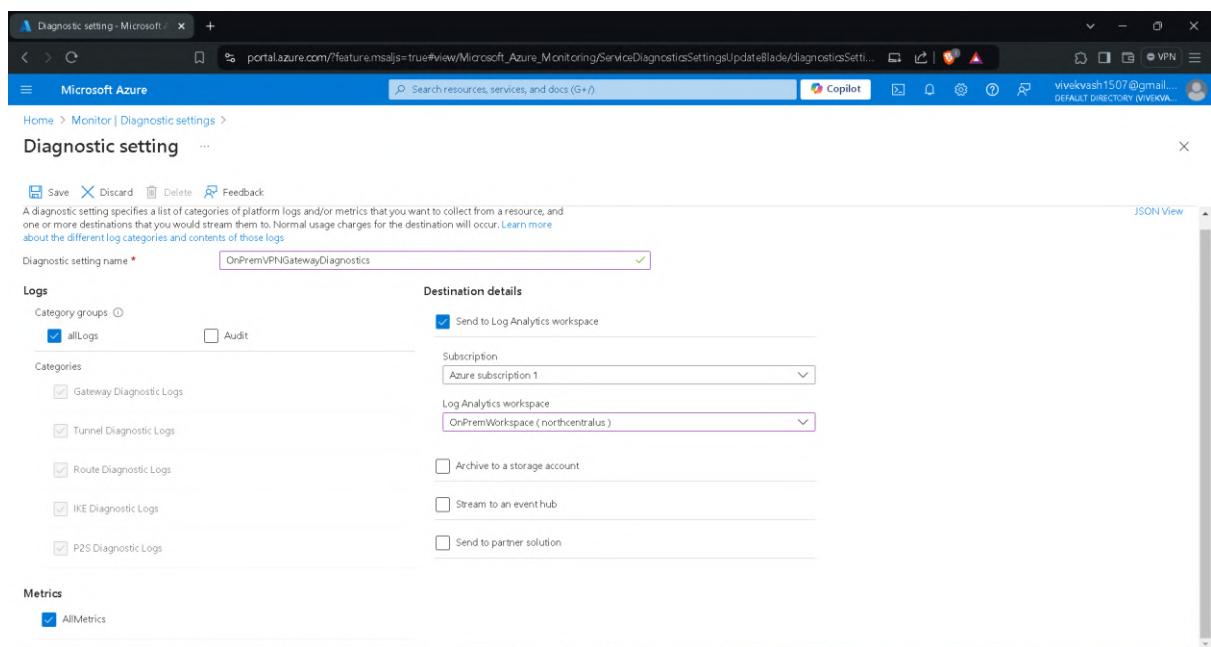
Stream to an event hub

Send to partner solution

**Metrics**

AllMetrics

JSON View



**Monitor - Microsoft Azure**

portal.azure.com/?feature.msajs=true#view/Microsoft\_Azure\_Monitoring/AzureMonitoringBrowseBlade/-/diagnosticLogs

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekvash1507)

Home > Monitor

## Monitor | Diagnostic settings

Subscription \* Azure subscription 1 Resource group \* NetMazeRG Resource type \* Virtual network gateways Resource

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostics status
NetMazeVPNGateway	Virtual network gateway	NetMazeRG	Enabled
OnPremVPNGateway	Virtual network gateway	NetMazeRG	Enabled

... Insights Hub

Managed Services

Managed Prometheus

Azure Managed Grafana

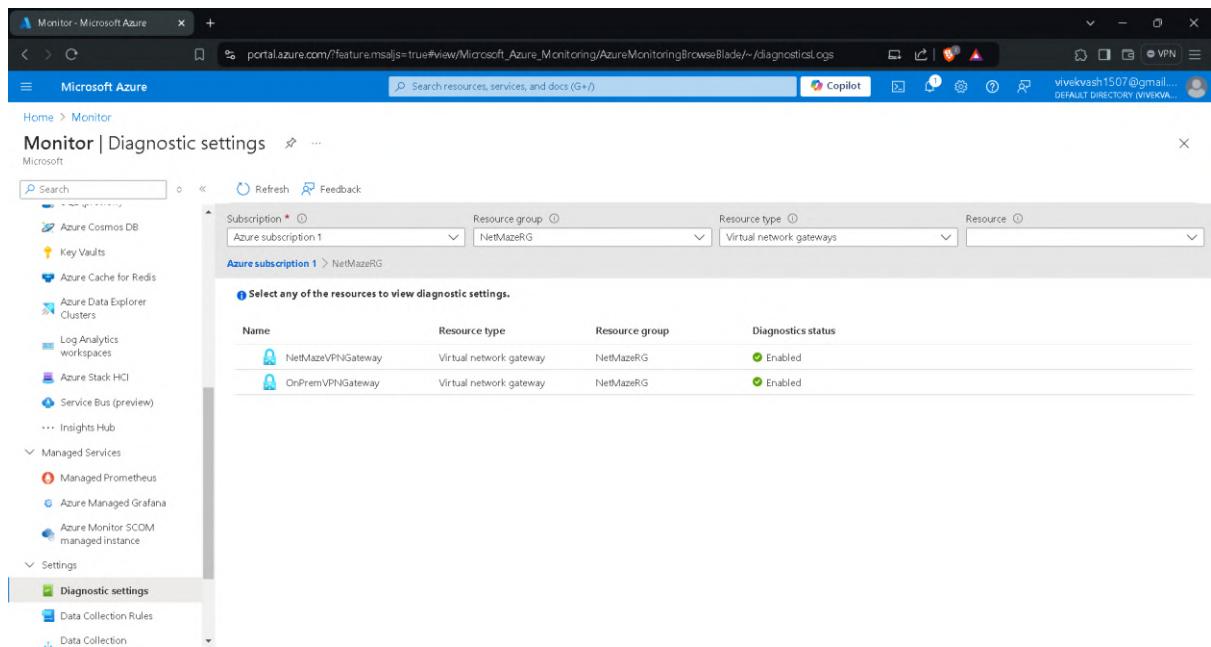
Azure Monitor SCOM managed instance

Settings

Diagnostic settings

Data Collection Rules

Data Collection



Diagnostic setting - Microsoft Azure

portal.azure.com/?feature.msljs=true#view/Microsoft\_Azure\_Monitoring/ServiceDiagnosticsSettingsUpdateBlade/diagnosticsSetting

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more](#) about the different log categories and contents of those logs.

Diagnostic setting name \*

WebAppNSG-Diagnostics

Logs

Category groups (radio button)

allLogs

Categories

Network Security Group Event

Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription

Azure subscription 1

Log Analytics workspace

NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

Diagnostic setting - Microsoft Azure

portal.azure.com/?feature.msljs=true#view/Microsoft\_Azure\_Monitoring/ServiceDiagnosticsSettingsUpdateBlade/diagnosticsSetting

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more](#) about the different log categories and contents of those logs.

Diagnostic setting name \*

DatabaseNSG-Diagnostics

Logs

Category groups (radio button)

allLogs

Categories

Network Security Group Event

Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription

Azure subscription 1

Log Analytics workspace

NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

**Diagnostic setting - Microsoft** +

portal.azure.com/?feature.msajs=true#view/Microsoft\_Azure\_Monitoring/ServiceDiagnosticsSettingsUpdateBlade/diagnosticsSetting

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekva...)

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more](#) about the different log categories and contents of those logs.

Diagnostic setting name \*

AdminNSG-Diagnostics

Logs

Category groups

allLogs

Categories

Network Security Group Event

Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription

Azure subscription 1

Log Analytics workspace

NetMazeWorkspace (canadaeast)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

**Diagnostic setting - Microsoft** +

portal.azure.com/?feature.msajs=true#view/Microsoft\_Azure\_Monitoring/ServiceDiagnosticsSettingsUpdateBlade/diagnosticsSetting

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (vivekva...)

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more](#) about the different log categories and contents of those logs.

Diagnostic setting name \*

OnPremVM-nsg-Diagnostics

Logs

Category groups

allLogs

Categories

Network Security Group Event

Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription

Azure subscription 1

Log Analytics workspace

OnPremWorkspace (northcentralus)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

Diagnostic setting - Microsoft Azure

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name \* WebAppVM-nsg-Diagnostics ✓

Logs

Category groups: allLogs

Categories:

- Network Security Group Event
- Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

Diagnostic setting - Microsoft Azure

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name \* DatabaseVM-nsg-Diagnostics ✓

Logs

Category groups: allLogs

Categories:

- Network Security Group Event
- Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

**Diagnostic setting - Microsoft**

Microsoft Azure | Diagnostic settings

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs.](#)

Diagnostic setting name \* AdminVM-nsg-Diagnostics

Logs

Category groups  allLogs

Categories

Network Security Group Event

Network Security Group Rule Counter

Destination details

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

JSON View

This screenshot shows the 'Diagnostic setting' blade in the Azure portal. It's titled 'AdminVM-nsg-Diagnostics'. Under 'Logs', 'allLogs' is selected. In 'Destination details', 'Send to Log Analytics workspace' is checked, with 'Azure subscription 1' and 'NetMazeWorkspace (canadacentral)' selected. There are also options for 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution'.

**Monitor - Microsoft Azure**

Microsoft Azure | Monitor

Monitor | Diagnostic settings

Search Refresh Feedback

Subscription: Azure subscription 1 | Resource group: NetMazeRG | Resource type: Network security groups | Resource:

Azure subscription 1 > NetMazeRG

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostics status
OnPremVM-nsg	Network security group	NetMazeRG	Enabled
WebAppVM-nsg	Network security group	NetMazeRG	Enabled
DatabaseVM-nsg	Network security group	NetMazeRG	Enabled
AdminVM-nsg	Network security group	NetMazeRG	Enabled
WebAppNSG	Network security group	NetMazeRG	Enabled
DatabaseNSG	Network security group	NetMazeRG	Enabled
AdminNSG	Network security group	NetMazeRG	Enabled

Navigation sidebar:

- Search
- Refresh
- Feedback
- Home
- Monitor
- Diagnostic settings
- Data Collection Rules
- Data Collection

This screenshot shows the 'Monitor | Diagnostic settings' blade. It lists network security groups (NSGs) under 'Azure subscription 1 > NetMazeRG'. All NSGs have 'Diagnostics status' set to 'Enabled'. The left sidebar shows navigation links like Home, Monitor, Diagnostic settings, Data Collection Rules, and Data Collection.

**Diagnostic setting**

Diagnostic setting name \* NetMazeSQLDB-Diagnostics

**Logs**

Category groups  allLogs  audit

Categories

- SQL Insights
- Automatic tuning
- Query Store Runtime Statistics
- Query Store Wait Statistics
- Errors
- Database Wait Statistics
- Timeouts
- Blocks

**Destination details**

Send to Log Analytics workspace

Subscription Azure subscription 1

Log Analytics workspace NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

**Diagnostic setting**

Diagnostic setting name \* dbmaster-Diagnostics

**Logs**

Category groups  allLogs  audit

Categories

- SQL Insights
- Automatic tuning
- Query Store Runtime Statistics
- Query Store Wait Statistics
- Errors
- Database Wait Statistics
- Timeouts
- Blocks

**Destination details**

Send to Log Analytics workspace

Subscription Azure subscription 1

Log Analytics workspace NetMazeWorkspace (canadacentral)

Archive to a storage account

Stream to an event hub

Send to partner solution

Diagnostic setting - Microsoft Azure

Diagnostic setting - Microsoft Azure

Microsoft Azure

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

Diagnostic setting name \* dbmaster-Diagnostics ✓

**Logs**

Category groups   allLogs  audit

Categories

SQL Insights  
 Automatic tuning  
 Query Store Runtime Statistics  
 Query Store Wait Statistics  
 Errors  
 Database Wait Statistics  
 Timeouts  
 Blocks

**Destination details**

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: NetMazeWorkspace (canadaeast)

Archive to a storage account  
 Stream to an event hub  
 Send to partner solution

Diagnostic setting - Microsoft Azure

Diagnostic setting - Microsoft Azure

Microsoft Azure

Home > Monitor | Diagnostic settings >

## Diagnostic setting

Save Discard Delete Feedback

Diagnostic setting name \* NetMazeLoadBalancer-Diagnostics ✓

**Logs**

Category groups   allLogs  audit

Categories

Load Balancer Health Event

**Metrics**

AllMetrics

**Destination details**

Send to Log Analytics workspace

Subscription: Azure subscription 1

Log Analytics workspace: NetMazeWorkspace (canadaeast)

Archive to a storage account  
 Stream to an event hub  
 Send to partner solution

JSON View

The screenshot shows the Microsoft Azure portal interface for 'Monitor | Diagnostic settings'. The left sidebar includes links for Home, Monitor, Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters, Log Analytics workspaces, Azure Stack HCI, Service Bus (preview), Insights Hub, Managed Services (Managed Prometheus, Azure Managed Grafana, Azure Monitor SCOM managed instance), Settings (Diagnostic settings, Data Collection Rules, Data Collection), and a search bar. The main content area displays a table for a 'Load balancers' resource named 'NetMazeLoadBalancer' under 'Azure subscription 1 > NetMazeRG'. The table columns are Name, Resource type, Resource group, and Diagnostics status, all showing 'Enabled'. A note at the top says 'Select any of the resources to view diagnostic settings.'

## Alerts:

### Unauthorized SSH Attempts Alert:

The screenshot shows the Microsoft Azure portal interface for 'Create an alert rule'. The left sidebar includes links for Home, Monitor | Alerts, and a search bar. The main content area is titled 'Create an alert rule' and has tabs for Scope, Condition, Actions, Details, Tags, and Review + create. Under Scope, it shows a selected scope for 'DatabaseNSG' under 'Azure subscription 1 > NetMazeRG'. At the bottom, there are navigation buttons: 'Review + create', 'Previous', and 'Next: Condition >'.

Select a signal - Microsoft Azure

Microsoft Azure

Create an alert rule

Scope Condition Actions Details Tags Review + create

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

Signal name \*

Custom log search [See all signals](#)

Define the logic for triggering an alert. Use the chart to view trends in the data. [Learn more](#)

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query \*

```
AzLogAnalytics
| where ResourceType == "NETWORKSECURITYGROUPS"
| where OperationName == "NetworkSecurityGroupEvents"
| where ruleName_s == "userRule_Deny-SSH-OnPrem"
| where conditions_destinationPortRange_s == "22-22"
```

View result and edit query in Logs [Edit](#)

Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Review + create Previous Next: Actions > Apply Cancel

Select a signal

Search by signal name Signal type: All Signal source: All

Signal name Signal source

Log search Log Analytics

Activity log

- All Administrative operations Administrative
- Create or Update Network Security Group (Network Security Group) Administrative
- Delete Network Security Group (Network Security Group) Administrative
- Join Network Security Group (Network Security Group) Administrative

Apply Cancel

Create an alert rule - Microsoft Azure

DatabaseNSG - Microsoft Azure

OnPremVM

Microsoft Azure

Create an alert rule

Scope Condition Actions Details Tags Review + create

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

Signal name \*

Custom log search [See all signals](#)

Define the logic for triggering an alert. Use the chart to view trends in the data. [Learn more](#)

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query \*

```
AzLogAnalytics
| where ResourceType == "NETWORKSECURITYGROUPS"
| where OperationName == "NetworkSecurityGroupEvents"
| where ruleName_s == "userRule_Deny-SSH-OnPrem"
| where conditions_destinationPortRange_s == "22-22"
```

View result and edit query in Logs [Edit](#)

Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Review + create Previous Next: Actions >

Create an alert rule

**Measurement**

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Measure: Table rows

Aggregation type: Count

Aggregation granularity: 5 minutes

**Split by dimensions**

Use dimensions to monitor specific time series and provide context to the fired alert. Dimensions can be either number or string columns. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately.

Dimension name	Operator	Dimension values	Include all future values
Select dimension	=	0 selected	<input type="checkbox"/>
		Add custom value	

**Alert logic**

Operator: Greater than or equal to

Threshold value: 5

[Review + create](#) [Previous](#) [Next: Actions >](#)

**Create an alert rule**

**Actions**

An action group is a set of actions that can be applied to an alert rule. [Learn more](#)

Select actions

- Use quick actions (preview)  
Select one or more of the quick actions.
- Use action groups  
Add an existing action group or create a new one.
- None

Quick actions

Quick actions not configured yet

Manage quick actions

**Use quick actions (preview)**

**Details**

Action group name \*

Display name \*

**Actions**

Email

Email Azure Resource Manager Role

Azure mobile app notification

**Review + create** **Previous** **Next: Details >** **Save** **Cancel**

**Create an alert rule**

**Project details**

Select the subscription and resource group in which to save the alert rule.

Subscription \* ⓘ

Resource group \* ⓘ

**Alert rule details**

Severity \* ⓘ

Alert rule name \* ⓘ

Alert rule description ⓘ

Region \* ⓘ

**Identity**

Controls which identities can access the alert rule. This will determine the notifications, access to alert rules, and other configurations when the alert rule triggers.

[Review + create](#) [Previous](#) [Next: Tags >](#)

Alert rules - Microsoft Azure

portal.azure.com/?feature.msals=true#view/Microsoft\_Azure\_Monitoring\_Alerts/AlertRulesBlade/subscriptions/%E2%80%9C...>

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (vivekvash1507)

Home > Monitor | Alerts >

Alert rules

+ Create | Columns | Refresh | Export to CSV | Open query | Delete | Enable | Disable

Subscription: Azure subscription 1 | Target scope: all | Target resource type: all | Signal type: all | Severity: all | Add tag filter | More (1) | No grouping

Name ↑↓	Condition	Severity ↑↓	Target scope	Target resource type	Signal type ↑↓	Status ↑↓
Unauthorized SSH Attempt Alert	Table rows >= 5	0 - Critical	DatabaseNSG	Network security group	Log search	Enabled
VPN Gateway Downtime Alert	Previous resource status=All, C...	4 - Verbose	NetMazeVPNGateway, OnPremVPNGateway	Virtual network gateway	Resource health	Enabled

Showing 1 - 2 of 2 results.

Give feedback

## VPN Gateway Downtime Alert:

Monitor - Microsoft Azure

portal.azure.com/?feature.msals=true#view/Microsoft\_Azure\_Monitoring/AzureMonitoringBrowseBlade/~/alertsV2

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...  
DEFAULT DIRECTORY (vivekvash1507)

Home > Monitor

Monitor | Alerts

Overview

Activity log

Alerts

Metrics

Logs

Change Analysis

Service health

Workbooks

Investigator (preview)

Insights

Applications

Virtual Machines

Storage accounts

Containers

Networks

SQL (preview)

Azure Cosmos DB

Key Vaults

View as timeline (preview) | + Create | Alert rules | Action groups | Alert processing rules | Prometheus rule groups | Change user response | Actions | Refresh

New: View alerts visualized on Alert rule

Action group: Alert rule

Subscription: ee9ea131-d6f1-4e0b-bae-b293615685ae

Time range: Past 24 hours | Alert condition: Fired | Add filter | More (1)

Total alerts	Critical	Error	Warning	Informational	Verbose
1	0	0	0	0	0

Name ↑↓ | Severity ↑↓ | Affected resource ↑↓ | Alert condition ↑↓ | User response ↑↓ | Fire time ↑↓

No alerts found

Try changing your search or choose a different scope level if you don't see what you're looking for.

**Create an alert rule**

**Scope** Condition Actions Details Tags Review + create

Create an alert rule to identify and address issues when important conditions are found in your monitoring data. [Learn more](#)

+ Select scope

Resource	Hierarchy
NetMazeVPNGateway	Azure subscript... > NetMazeRG
OnPremVPNGateway	Azure subscript... > NetMazeRG

[Review + create](#) [Previous](#) [Next: Condition >](#)

**Select a signal**

**Condition**

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

Signal name \*  Select a signal [See all signals](#)

**Select a signal**

Search by signal name Signal type : All Signal source : All

Signal name	Signal source
Resource health	Resource health
All Administrative operations	Administrative
Creates or updates a VirtualNetworkGateway (VirtualNetworkGateway)	Administrative
Deletes a virtualNetworkGateway (VirtualNetworkGateway)	Administrative
Disconnect virtual network gateway vpn connections (VirtualNetworkGateway)	Administrative
Generate VpnClient package for virtualNetworkGateway (VirtualNetworkGateway)	Administrative
Generate VpnProfile package for VirtualNetworkGateway (VirtualNetworkGateway)	Administrative
Get Per Vpn Client Connection Health for VirtualNetworkGateway (VirtualNetworkGate...	Administrative
Get Vpnclient Ipsec parameters for VirtualNetworkGateway P2S client (VirtualNetwork...	Administrative

[Review + create](#) [Previous](#) [Next: Actions >](#)

**Create an alert rule**

Scope Condition Actions Details Tags Review + create

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

Signal name \*  See all signals

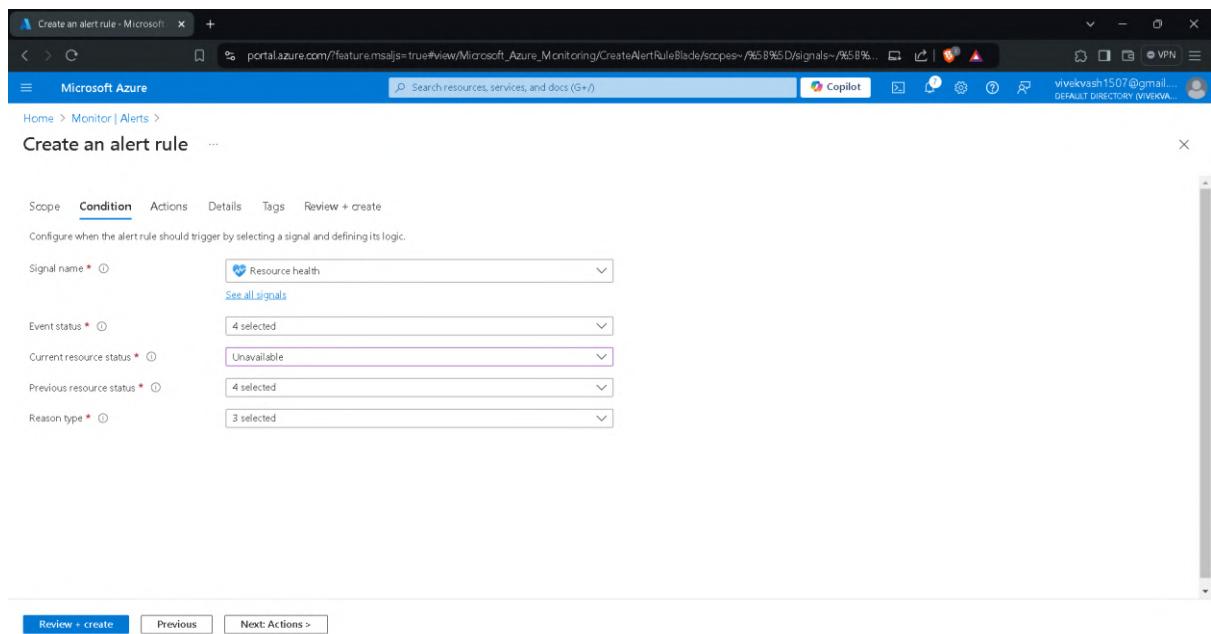
Event status \*

Current resource status \*

Previous resource status \*

Reason type \*

**Review + create** **Previous** **Next: Actions >**



**Create an alert rule**

Scope Condition **Actions** Details Tags Review + create

An action group is a set of actions that can be applied to an alert rule. [Learn more](#)

Select actions

Use quick actions (preview)  
Select one or more of the quick actions.

Use action groups  
Add an existing action group or create a new one.

None

Quick actions

**Quick actions not configured yet**

[Manage quick actions](#)

**Use quick actions (preview)**

Details

Action group name \*

Display name \*

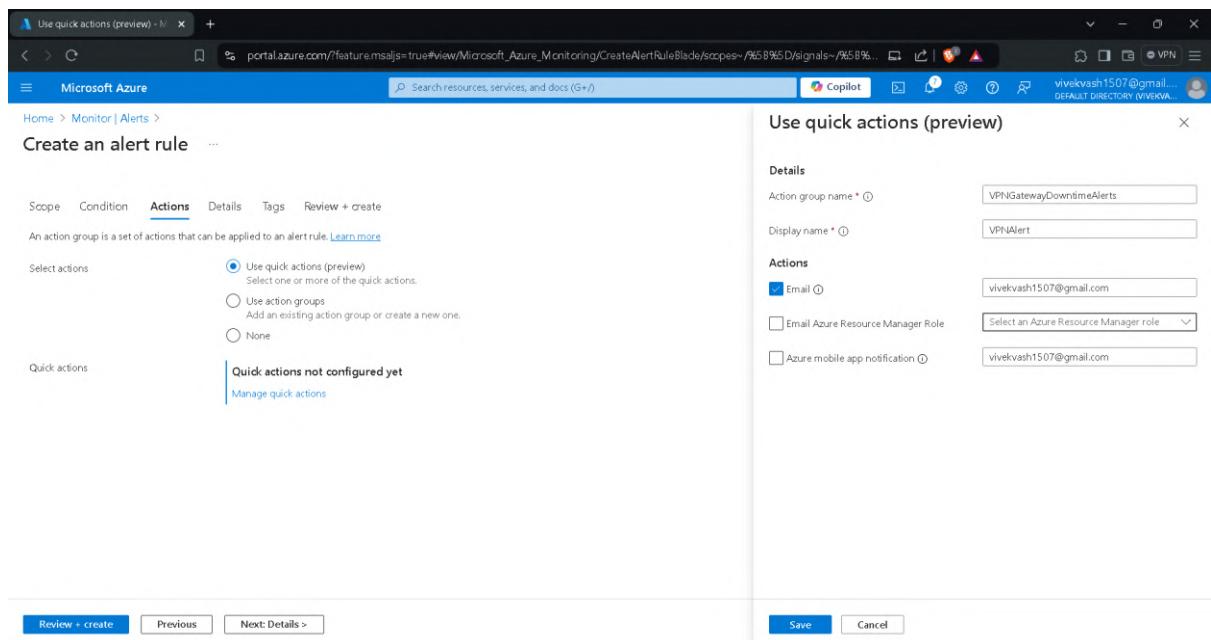
Actions

Email

Email Azure Resource Manager Role

Azure mobile app notification

**Review + create** **Previous** **Next: Details >** **Save** **Cancel**



**Create an alert rule - Microsoft**

portal.azure.com/?feature-msaljs=true#view/Microsoft\_Azure\_Monitoring/CreateAlertRuleBlade/scopes-/%5B%5D/signals-/%5B%5D/

Microsoft Azure

Home > Monitor | Alerts > Create an alert rule

**Details**

Scope Condition Actions Details Tags Review + create

**Project details**

Select the subscription and resource group in which to save the alert rule.

Subscription: Azure subscription 1

Resource group: NetMazeRG

Region: Global

**Alert rule details**

Alert rule name: VPN Gateway Downtime Alert

Alert rule description: This alert triggers if the VPN Gateway experiences downtime

**Advanced options**

Review + create Previous Next: Tags >

**VPN Gateway Downtime Alert**

Activity log alert rule

Overview

Name: VPN Gateway Downtime Alert

Resource group: NetMazeRG

Location: Global

Subscription: Azure subscription 1

Severity: 4 - Verbose

Description: This alert triggers if the VPN Gateway experiences downtime

Tags: (edit) Add tags

Scope

Subscription: Azure subscription 1

Resource types: Virtual network gateways

Resource groups: NetMazeRG

Resources: NetMazevPNGateway, OnPremvPNGateway

Showing 1 - 1 of 1 results.

Give feedback

## Logs and Metrics:

The screenshot shows the Microsoft Azure Log Analytics workspace interface. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Logs (which is selected). The main area has a search bar and a 'New Query' button. A query is running: `AzureDiagnostics | where ResourceType == "NETWORKSECURITYGROUPS"`. The results table shows several rows of data, each with a timestamp, resource ID, category, resource group, and subscription ID. The table includes columns for generated UTC, ResourceId, Category, ResourceGroup, and SubscriptionId.

generated [UTC]	ResourceId	Category	ResourceGroup	SubscriptionId
24/2024, 3:03:46.12 AM	/SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE... /SUBSCRIPTIONS/EE9EA131-D6F1-4E0B-BAE...	NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent NetworkSecurityGroupEvent	NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG NETMAZERG	ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131 ee9ea131

The screenshot shows the Microsoft Azure Monitor dashboard. It features a sidebar with 'Azure services' (Create a resource, Subscriptions), 'Resources' (Recent, Favorite, Name), and 'Navigate' (Subscriptions). The main area displays a search bar and a 'Services' section with a list of items like Monitor, Azure Native New Relic Service, and Azure Monitor workspaces. Below this are sections for 'Marketplace', 'Documentation', and a 'Last Viewed' list. At the bottom, there's a search bar for 'Continue searching in Microsoft Entra ID' and a 'Dashboard' button.

**Monitor - Microsoft Azure**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

## Monitor | Overview

The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date.

### Overview

Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Investigator (preview), Insights, Managed Services, Settings, Support + Troubleshooting.

### Insights

Use curated monitoring views for specific Azure resources. [View all insights](#)

**Application insights**: Monitor your app's availability, performance, errors, and usage. [View More](#)

**Container Insights**: Gain visibility into the performance and health of your controllers, nodes, and containers. [View More](#)

**VM Insights**: Monitor the health, performance, and dependencies of your VMs and VM scale sets. [View More](#)

**Network Insights**: View the health and metrics for all deployed network resources. [View More](#)

### Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. [Learn more about monitoring](#)

**Metrics**: Create charts to monitor and investigate the usage and performance of your Azure resources. [View More](#)

**Alerts**: Get notified and respond using alerts and actions. [View More](#)

**Logs**: Analyze and diagnose issues with log queries. [View More](#)

**Workbooks**: View, create and share interactive reports. [View More](#)

**Change Analysis**

**Diagnostic Settings**

**Azure Monitor SCOM managed instance**

**Managed Prometheus**

**Select a scope - Microsoft Azure**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail.com

DEFAULT DIRECTORY (VIVEKVA...)

## Monitor | Metrics

Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Investigator (preview), Insights, Managed Services, Settings, Support + Troubleshooting.

### Select a scope

**Browse** **Recent**

Resource types: All resource types Locations: All locations

Search to filter items...

Scope	Resource type	Location
<input checked="" type="checkbox"/> Azure subscription 1	Subscription	-
<input type="checkbox"/> NetMazeRG	Resource group	-
<input type="checkbox"/> NetworkWatcherRG	Resource group	-

**Why can't I select multiple resources?** Azure limits selections to one resource type and one location. Please refine your scope.

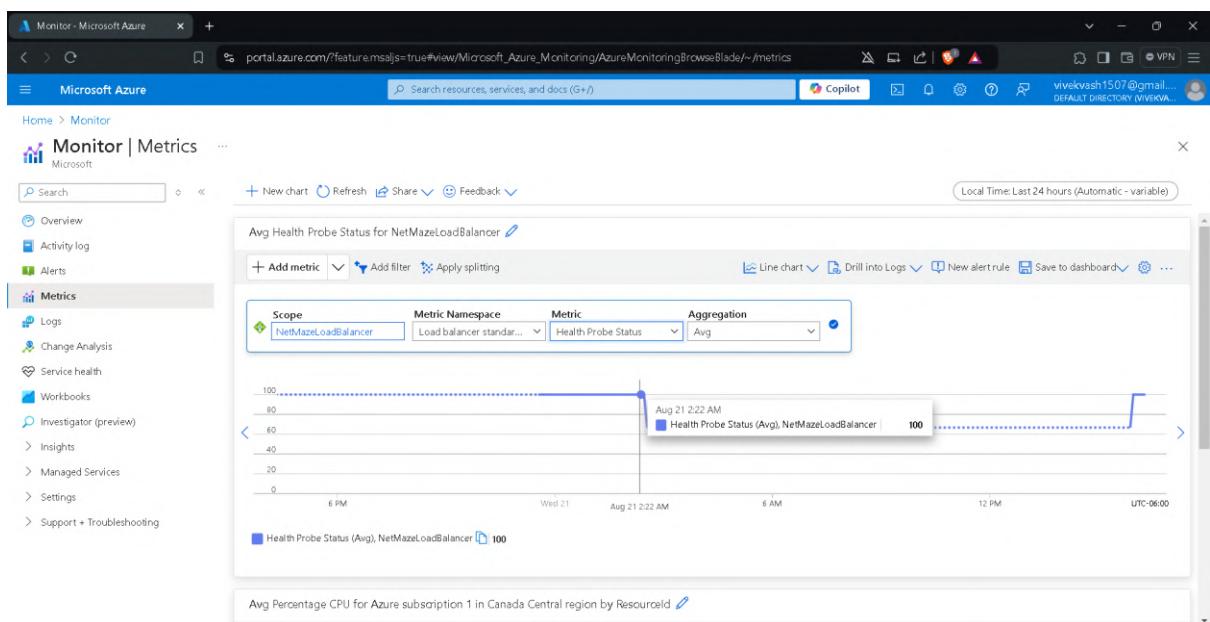
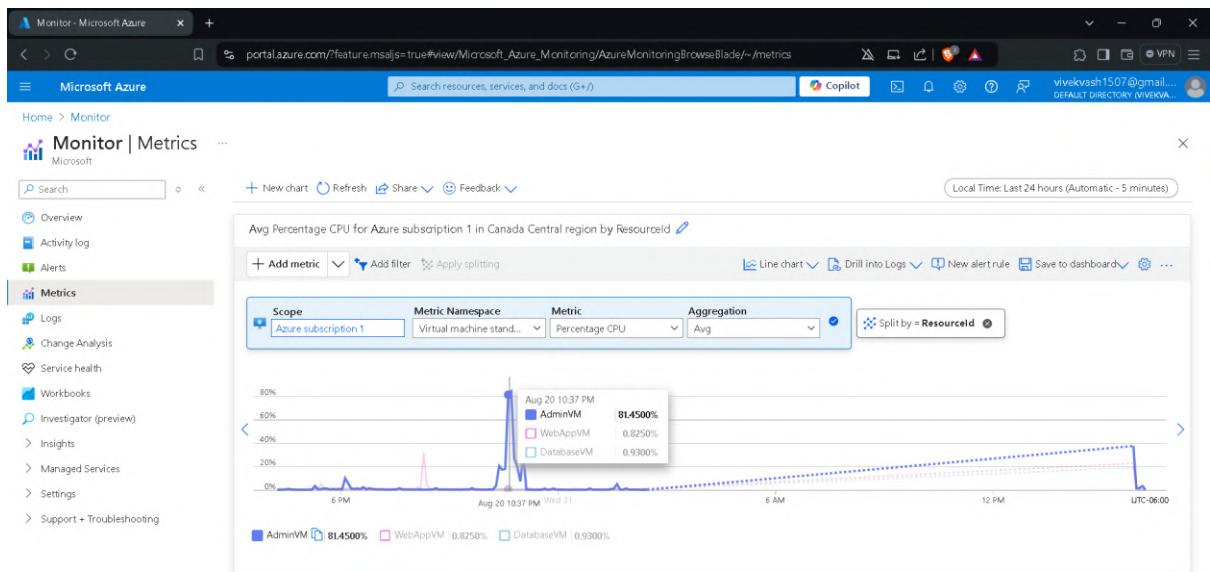
**Refine scope**

Resource type \*: Virtual machines Location \*: Canada Central

**Selected scopes** 1 scope

> Azure subscription 1 Subscription

Apply Cancel Clear all selections



Screenshot of the Microsoft Azure Monitor Metrics blade showing the "Select a scope" dialog.

The dialog lists resources under "Scope" and "Resource type".

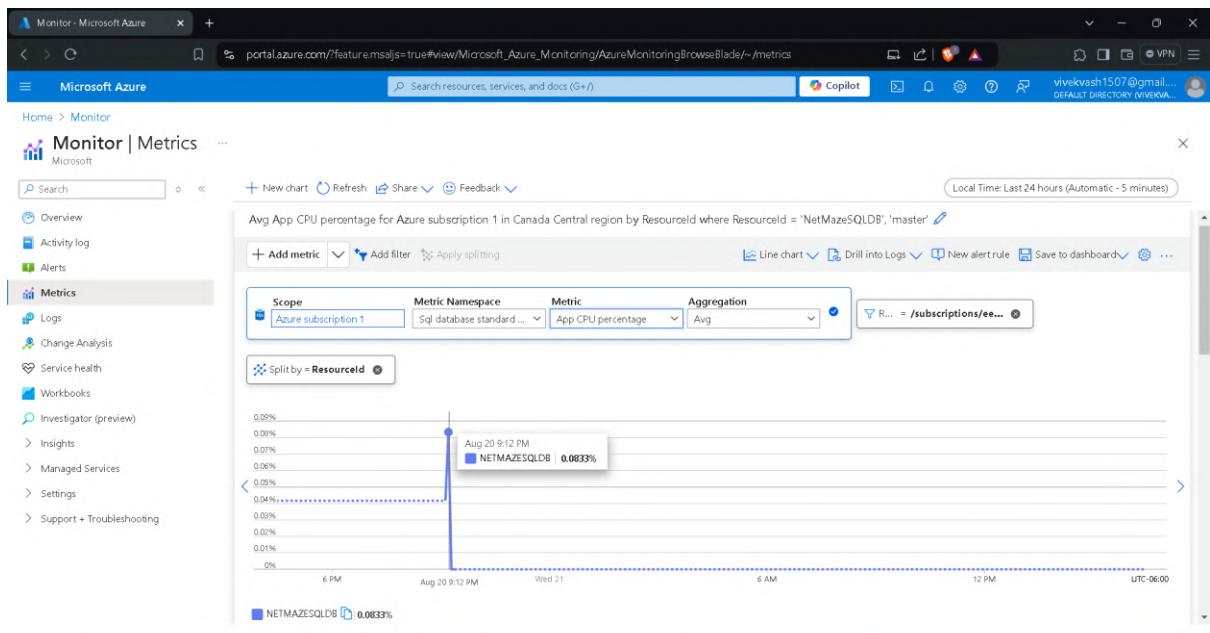
Scope	Resource type	Location
Azure subscription 1	Subscription	-
NetMazeRG	Resource group	-
master	SQL database	Canada Central
NetMazeSQLDB	SQL database	Canada Central

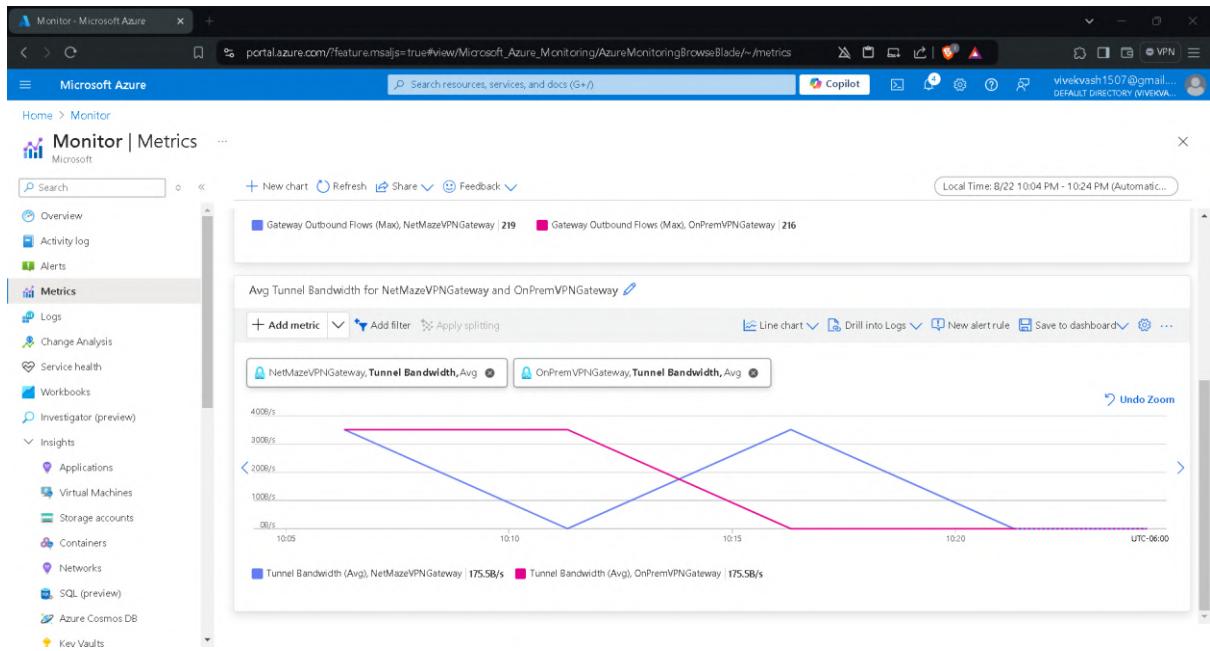
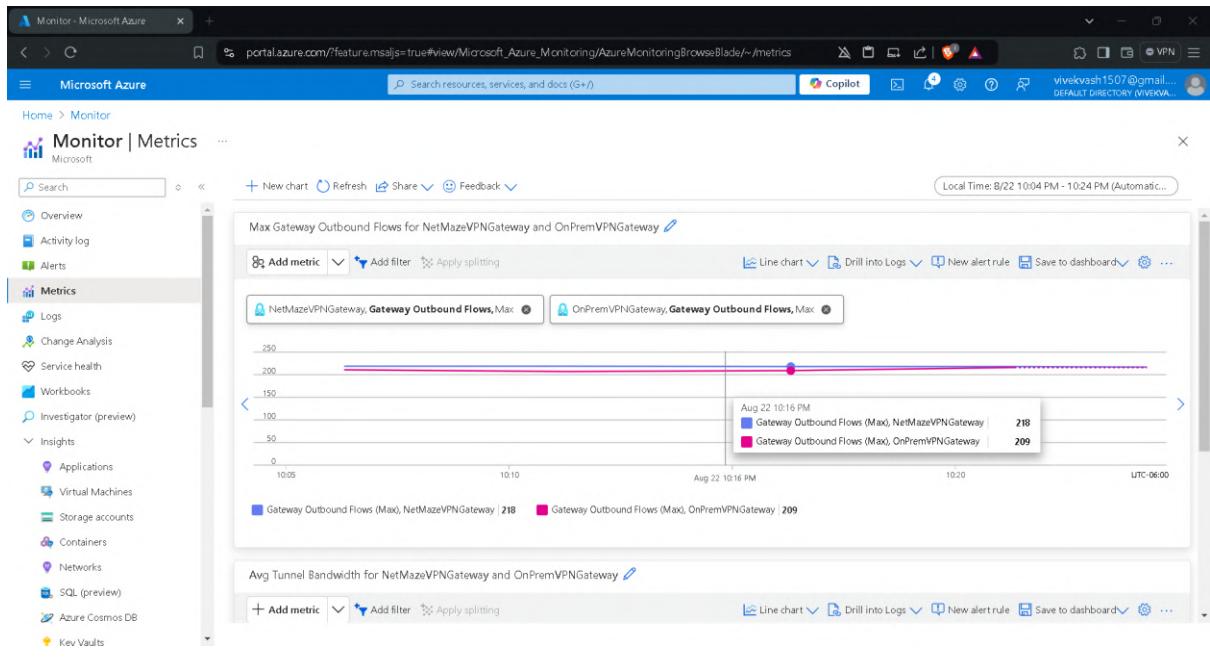
A tooltip message states: "Why can't I select multiple resources? You must select items of the same resource type and location. To select resources of a different resource type or location, please first uncheck your current selection."

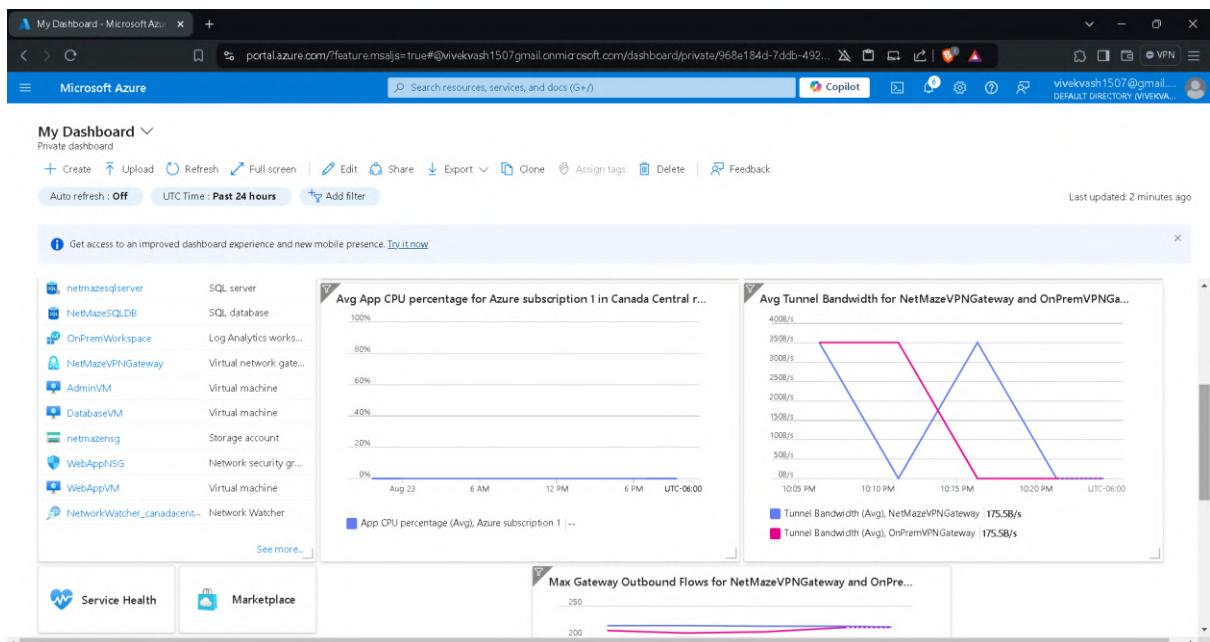
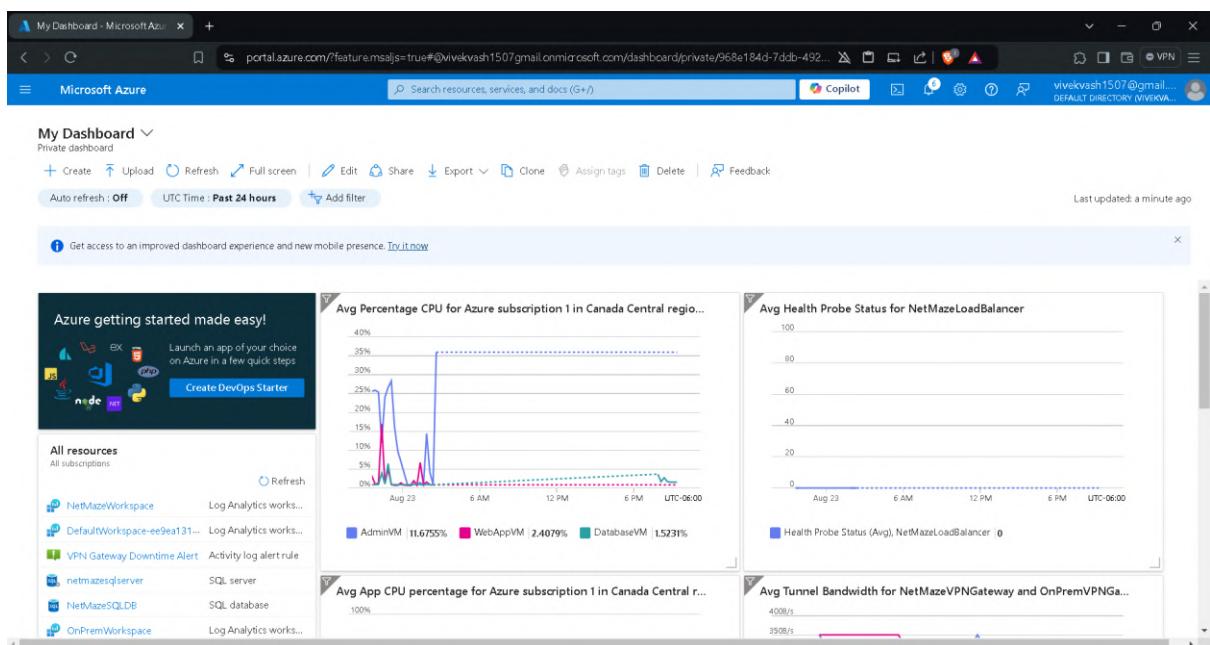
Selected scopes: 2 SQL databases

Resource type	Location
SQL database	Canada Central
SQL database	Canada Central

Buttons: Apply, Cancel, Clear all selections.







My Dashboard - Microsoft Azure

portal.azure.com/?feature.msaljs=true#vivekvash1507@gmail.onmicrosoft.com/dashboard/private/968e184d-7dbb-492...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

vivekvash1507@gmail...

DEFAULT DIRECTORY (vivekvash1507@gmail.com)

Last updated: 2 minutes ago

My Dashboard

Private dashboard

+ Create | Upload | Refresh | Full screen | Edit | Share | Export | Clone | Assign tags | Delete | Feedback

Auto refresh: Off | UTC Time: Past 24 hours | Add filter

Get access to an improved dashboard experience and new mobile presence. Try it now!

Service Health | Marketplace | See more...

Quickstarts + tutorials

Windows Virtual Machines | Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines | Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service | Create Web Apps using .NET, Java, Node.js, Python, PHP

App CPU percentage (Avg), Azure subscription 1

Tunnel Bandwidth (Avg), OnPremVPNGateway 0B/s

Max Gateway Outbound Flows for NetMazeVPNGateway and OnPremVPNGateway

Aug 22 10:16 PM UTC-06:00

250  
200  
150  
100  
50  
0

10:05 PM 10:10 PM 10:20 PM

Gateway Outbound Flows (Max), NetMazeVPNGateway 21B  
Gateway Outbound Flows (Max), OnPremVPNGateway 209

The screenshot shows the Microsoft Azure My Dashboard. The top navigation bar includes 'Create', 'Upload', 'Refresh', 'Full screen', 'Edit', 'Share', 'Export', 'Clone', 'Assign tags', 'Delete', and 'Feedback'. Below this is a search bar and a Copilot button. The dashboard header shows the user's email 'vivekvash1507@gmail.com' and the last update time '2 minutes ago'. On the left, there are sections for 'Service Health' and 'Marketplace', along with 'Quickstarts + tutorials' for 'Windows Virtual Machines', 'Linux Virtual Machines', and 'App Service'. A prominent chart on the right titled 'Max Gateway Outbound Flows' compares 'NetMazeVPNGateway' and 'OnPremVPNGateway' over the past hour. The chart shows values of approximately 21B and 209 respectively. The x-axis spans from 10:05 PM to 10:20 PM on Aug 22, and the y-axis ranges from 0 to 250.

# Conclusion

## Summary of Steps

- **Set Up Virtual Networks:** Deployed Azure Virtual Networks (VNet) for both main Azure (NetMazeVNet) and simulated on-premises (OnPremVNet) environments, including configuring subnets and gateway subnets for future site-to-site VPN connections.
- **Establish Secure Connectivity:** Implemented Azure VPN Gateway to create a site-to-site VPN connection between OnPremVNet and NetMazeVNet, ensuring secure communication between the simulated on-premises environment and Azure.
- **Resource Deployment:** Deployed virtual machines in each subnet of NetMazeVNet, including a web server in the WebAppSubnet, a MySQL database in the DatabaseSubnet, and an administrative machine in the AdminSubnet.
- **Network Access Control:** Configured Network Security Groups (NSGs) to manage inbound and outbound traffic for each subnet, ensuring only authorized traffic was allowed based on specific rules.
- **Secure Administrative Access:** Implemented Azure Bastion to securely manage RDP and SSH access to virtual machines without exposing them to the public internet.
- **Private Access to Azure PaaS Services:** Configured Azure Private Link to securely connect to Azure SQL Database within the VNet, ensuring data transfer over private endpoints.
- **DNS and Load Balancing:** Set up Azure DNS for custom domain names and implemented Azure Load Balancer to distribute traffic across the VMs in the WebApp Subnet.

- **Access Control Finalization:** Updated and finalized NSG rules to reflect the project's security posture after resource deployment, ensuring proper access control was in place.
- **Performance and Security Testing:** Simulated various network scenarios to test performance and security, including data transition between on-premises and Azure, and validating security configurations through different tests.
- **Monitoring and Auditing:** Enabled diagnostics and monitoring for VPN Gateways, NSGs, SQL Databases, and Load Balancer; set up alerts for suspicious activities, and reviewed logs and metrics for network operations.

## Lessons Learned

- **Importance of Secure Network Architecture:** Learned how critical it is to design and implement a secure and robust networking architecture in cloud environments.
- **Effective Use of Azure Networking Services:** Gained hands-on experience with Azure services such as VPN Gateway, NSGs, Load Balancer, and Private Link, understanding their role in securing and optimizing cloud infrastructure.
- **Significance of Monitoring and Auditing:** Understood the necessity of continuous monitoring and auditing for maintaining the health, performance, and security of cloud resources.

## **Skills Demonstrated**

Through the NetMaze Explorer project, the following skills were demonstrated:

1. **Network Architecture Design:**
  - Proficient in designing a hybrid networking environment using Azure Virtual Networks, subnets, and VPN Gateways.
  - Demonstrated ability to establish secure site-to-site VPN connections and manage cross-network communication.
2. **Resource Deployment and Management:**
  - Experienced in deploying and managing Azure resources, including virtual machines, NSGs, and Load Balancers.
  - Skilled in configuring and securing network resources for optimized performance and security.
3. **Secure Access Implementation:**
  - Implemented Azure Bastion for secure RDP and SSH access to VMs, reducing the exposure of VMs to public internet threats.
  - Configured Azure Private Link to ensure private and secure access to Azure SQL Database.
4. **Monitoring and Diagnostics:**
  - Enabled and configured monitoring tools and diagnostics across key Azure resources.

- Set up custom alerts to detect and respond to suspicious activities or resource downtime.

**5. Performance Testing and Validation:**

- Conducted thorough performance and security testing of network configurations, including load balancer functionality and data transfer validation.
- Validated security setups through targeted access tests, ensuring the integrity of security controls.

**6. Cost Management and Resource Cleanup:**

- Demonstrated awareness of resource management by cleaning up unnecessary resources after testing, ensuring cost-effective operations.

And Strong **Hands-on** Capabilities in the

(Implement and manage virtual networking)

Scope of **Microsoft Certified: Azure Administrator Associate (AZ-104)**

**Skills measured**

- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- **Implement and manage virtual networking**
- Monitor and maintain Azure resources