Load Balancer

1. Introduction to Load Balancer

1.1 Definition

A load balancer is a network device or software solution that evenly distributes incoming network traffic across multiple servers, ensuring optimal utilization and preventing overloading of individual servers. The load balancer acts as an intermediary between clients and the servers, managing the flow of incoming requests.

1.2 Purpose

The primary purpose of a load balancer is to enhance the availability, scalability, and performance of applications or services by ensuring that no single server is overwhelmed with traffic, thus avoiding downtime and slowdowns.

1.3 Benefits

- Improved Scalability: Load balancers allow organizations to scale their infrastructure horizontally by adding more servers to handle increasing traffic loads.
- High Availability: By distributing traffic across multiple servers, load balancers enhance the fault tolerance of the system. If one server fails, the load balancer redirects traffic to healthy servers.
- Optimized Performance: Evenly distributing requests prevents individual servers from becoming overwhelmed, leading to better response times for clients.
- Flexibility: Load balancers can be easily configured and adjusted to suit changing traffic patterns and application requirements.

2. Types of Load Balancers

2.1 Local Load Balancer

A local load balancer operates within a data center or a specific geographical location, distributing traffic among servers located in the same proximity.

2.2 Global Load Balancer

Global load balancers manage traffic across multiple data centers or regions, ensuring that clients are directed to the nearest or best-performing server based on their location.

2.3 Hardware Load Balancer

A hardware load balancer is a physical device specifically designed for load balancing tasks. It often provides high-performance capabilities and is suitable for handling heavy loads.

2.4 Software Load Balancer

A software load balancer is a load balancing solution implemented in software. It is typically deployed on commodity hardware or virtual machines and offers flexibility and cost-effectiveness.

2.5 Application Load Balancer

An application load balancer operates at the application layer (Layer 7) of the OSI model and can make routing decisions based on application-specific data, such as HTTP headers. This allows for more advanced routing and application-aware load balancing.

3. Why Use Load Balancers

3.1 Scalability

Load balancers enable organizations to scale their infrastructure easily by adding or removing servers as traffic demands change. This horizontal scaling approach ensures that resources are efficiently utilized.

3.2 High Availability

Load balancers enhance the availability of applications by distributing traffic across multiple servers. If one server becomes unavailable, the load balancer redirects traffic to healthy servers, minimizing downtime.

3.3 Improved Performance

By evenly distributing incoming requests, load balancers prevent server overload and optimize response times, providing better performance for end-users.

3.4 SSL Termination

Load balancers can handle Secure Sockets Layer (SSL) termination, offloading the resource-intensive SSL decryption and encryption process from the servers, leading to improved server performance.

4. Load Balancer Solutions on Azure

4.1 Azure Load Balancer

Azure Load Balancer is a Layer 4 (Transport Layer) load balancing solution that distributes traffic based on network information such as IP addresses and port numbers. It supports inbound and outbound scenarios, making it suitable for various applications.

4.2 Azure Application Gateway

Azure Application Gateway operates at Layer 7 (Application Layer) and provides advanced application-aware load balancing capabilities. It can route traffic based on URL paths, hostnames, or other application-specific data, making it ideal for web applications.

4.3 Azure Traffic Manager

Azure Traffic Manager is a DNS-based global load balancer that can direct clients to the closest or best-performing endpoint based on configured traffic routing methods, such as performance, geographic, or priority-based routing.

5. Architecture of Load Balancer on Azure

5.1 Components

Azure Load Balancer typically consists of the following components:

- Frontend IP Configuration: Defines the public IP address and port used to receive incoming traffic.
- Backend Pool: Specifies the target virtual machines or instances that will receive the load-balanced traffic.

- Health Probes: Monitors the health of backend instances and determines their availability.
- Load Balancer Rules: Defines how the traffic is distributed based on specified criteria.

5.2 Load Balancing Algorithms

Azure Load Balancer supports several load balancing algorithms, including "Default" (round-robin), "Source IP," and "Source IP Affinity" (session persistence).

5.3 Traffic Distribution Modes

Azure Load Balancer can operate in two distribution modes: "Internet-facing" (public) and "Internal" (private) load balancing.

5.4 Availability Zones

Azure Load Balancer can be deployed across Availability Zones to ensure high availability and fault tolerance.

5.5 Health Probes

Health probes periodically check the health of backend instances, enabling the load balancer to route traffic only to healthy instances.

5.6 Backend Pool

The backend pool consists of the target instances that will receive the load-balanced traffic.

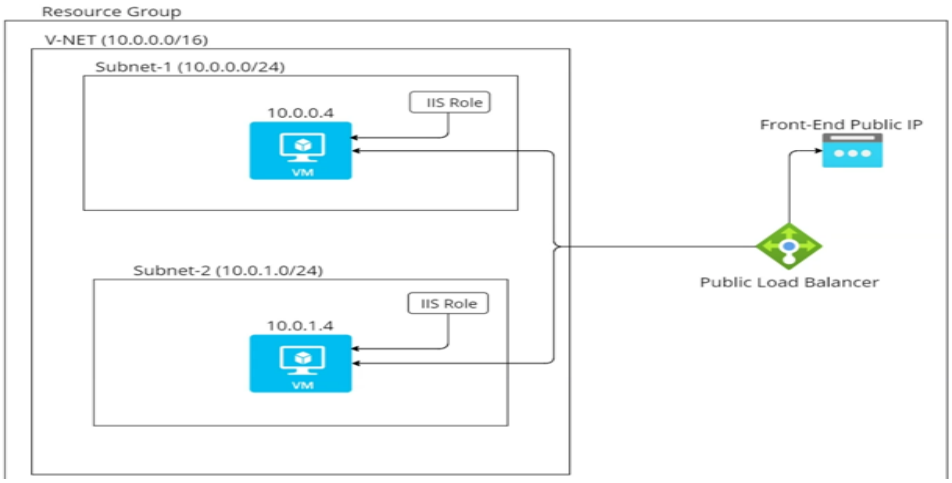
5.7 Frontend IP Configuration

The frontend IP configuration defines the public IP address and port used to receive incoming traffic.

5.8 Load Balancer Rules

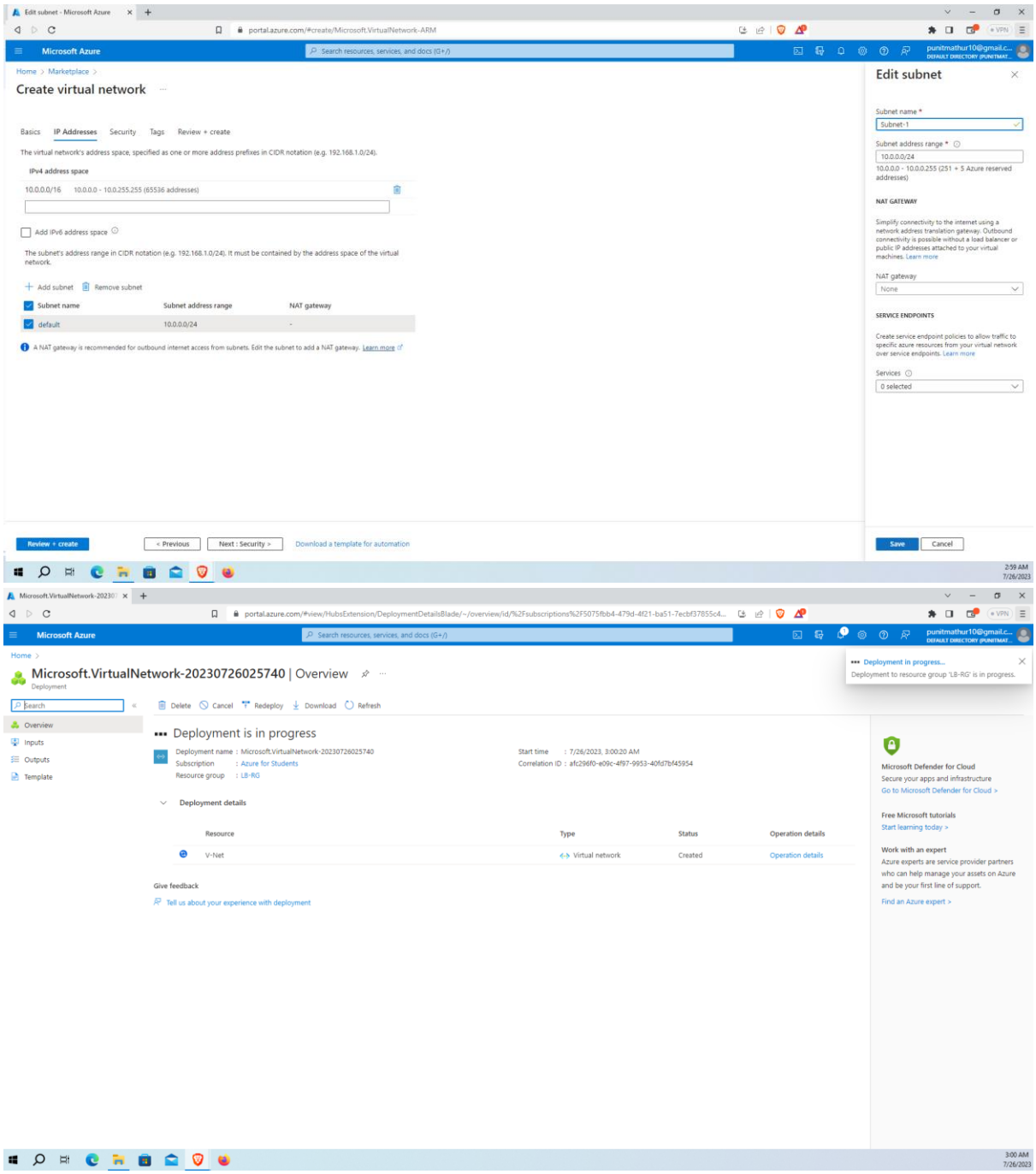
Load balancer rules define how traffic is distributed based on specified criteria, such as port numbers or protocols.

Architecture :

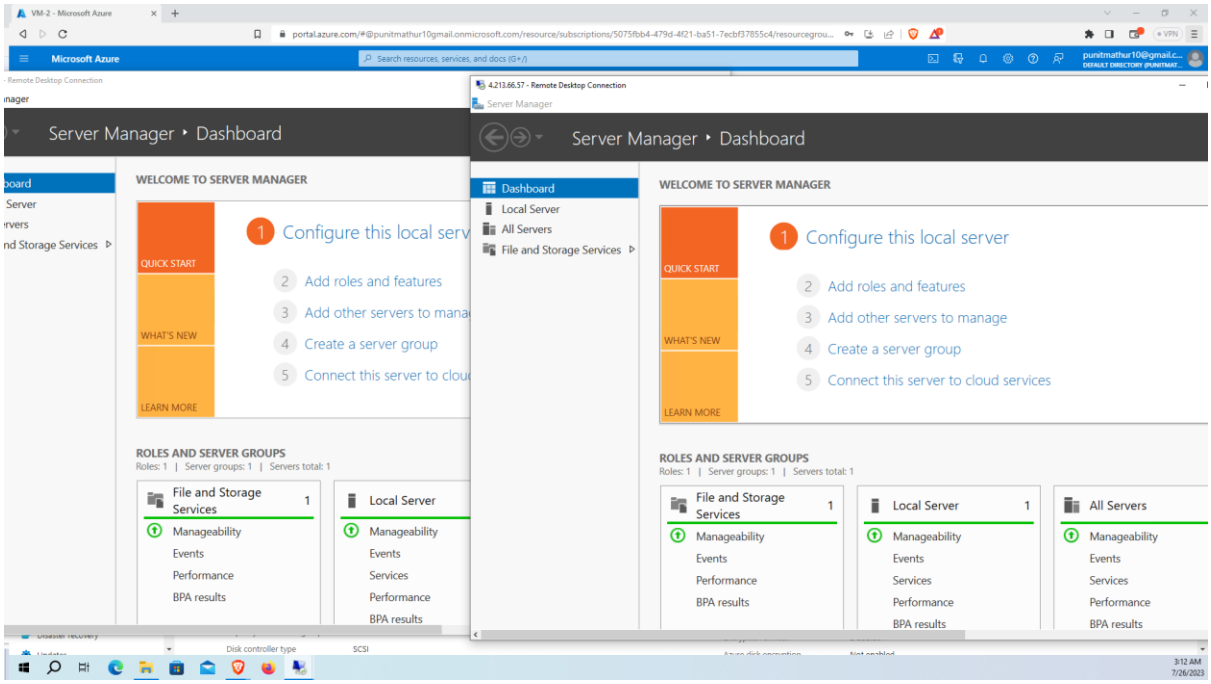


Now we will follow certain steps for making a load balancer.

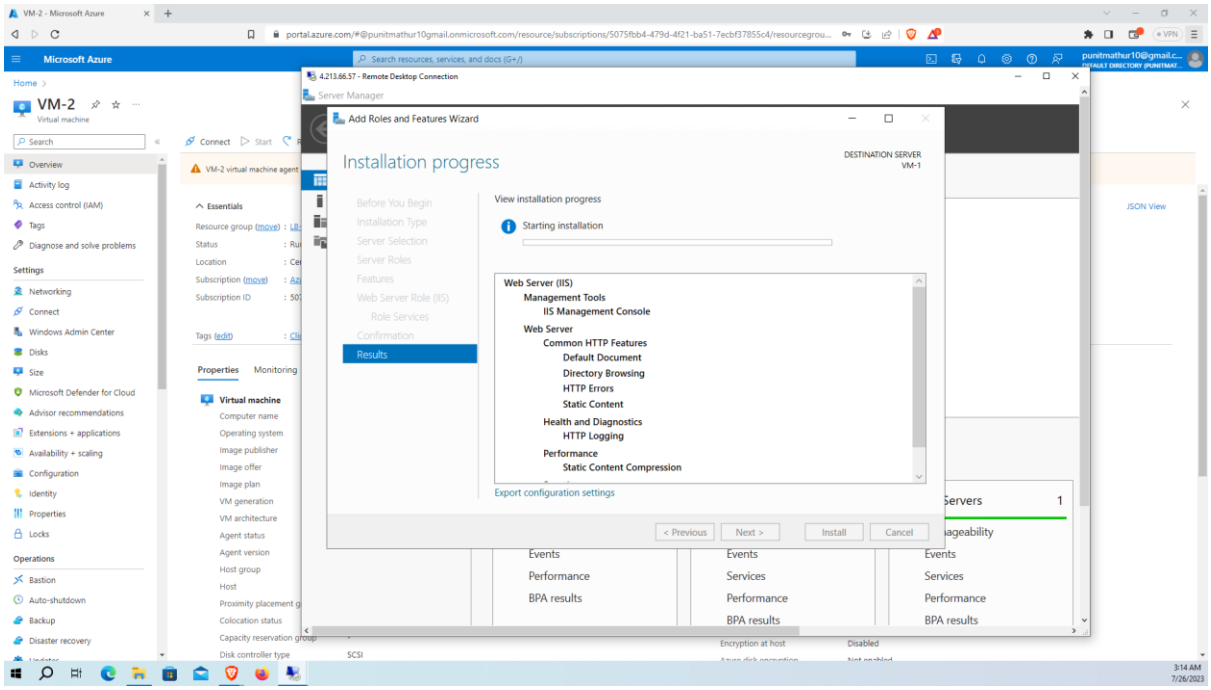
Now create a resource group named LB-RG and then create a virtual network in the same RG. change the name of default subnet as Subnet 1 in this VN.

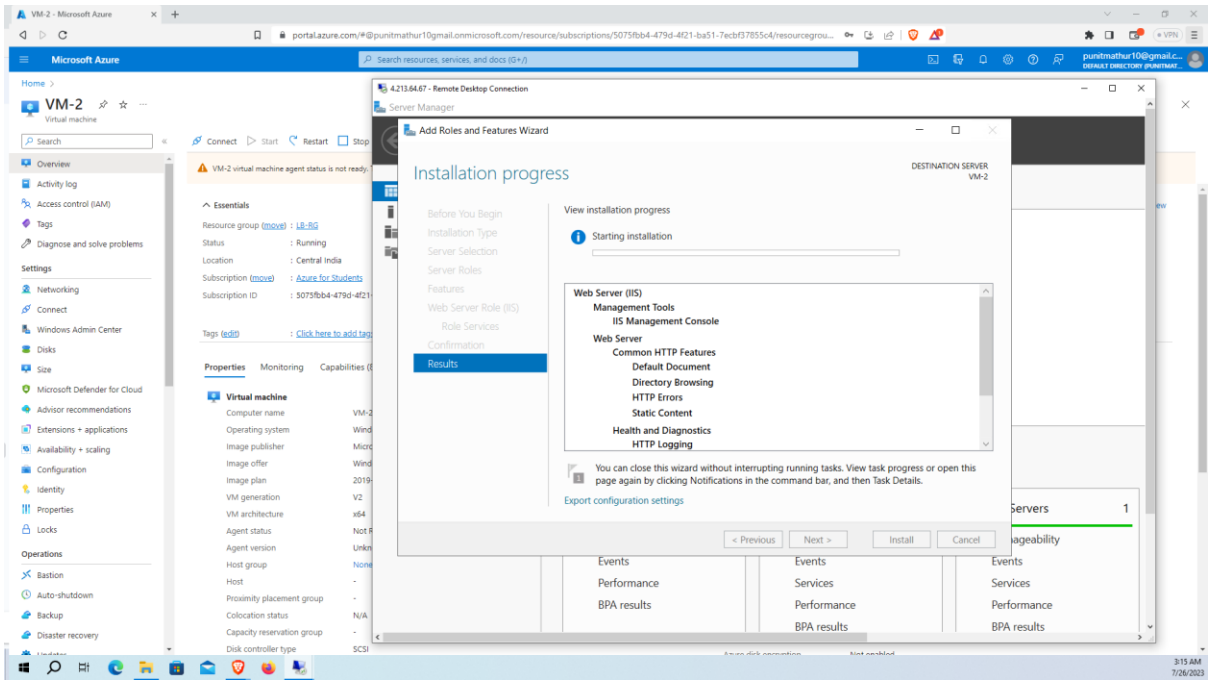


Now create 2 VM named VM1 and VM2 using window server 2019 as image and size as Standard_D2s_v3.in VM1 select virtual network as V-Net and subnet as Subnet 1 and in VM2 select virtual network as V-Net and subnet as Subnet 2 Now open them using RDP.

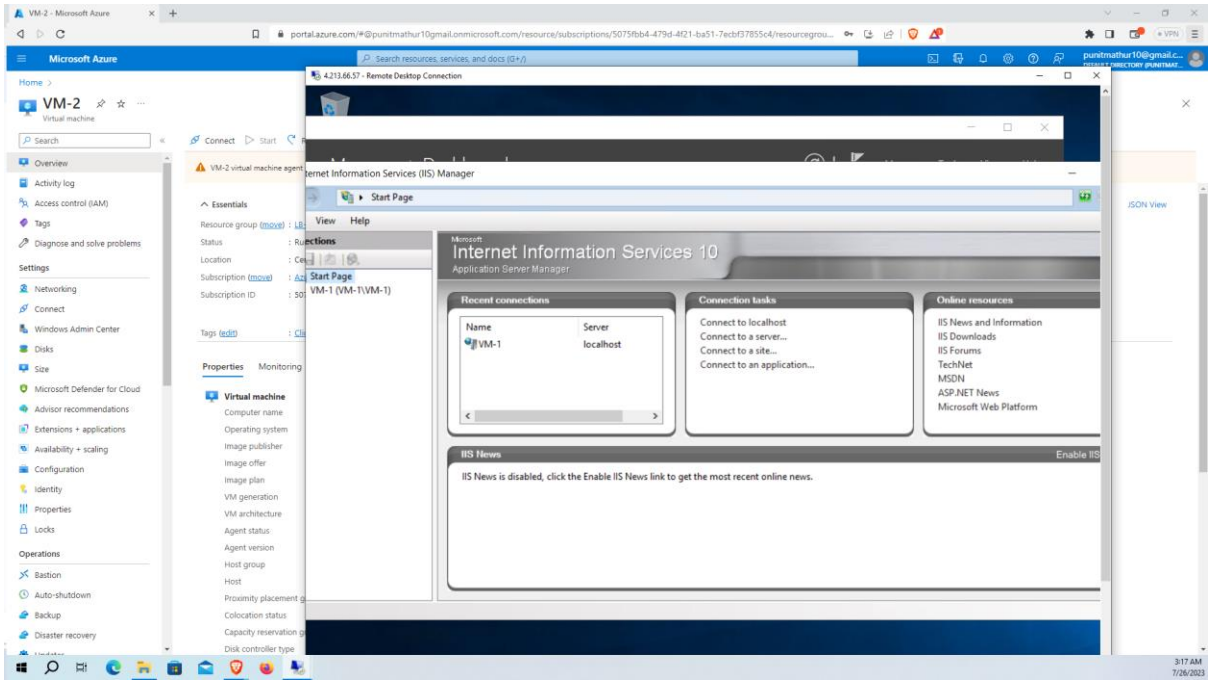


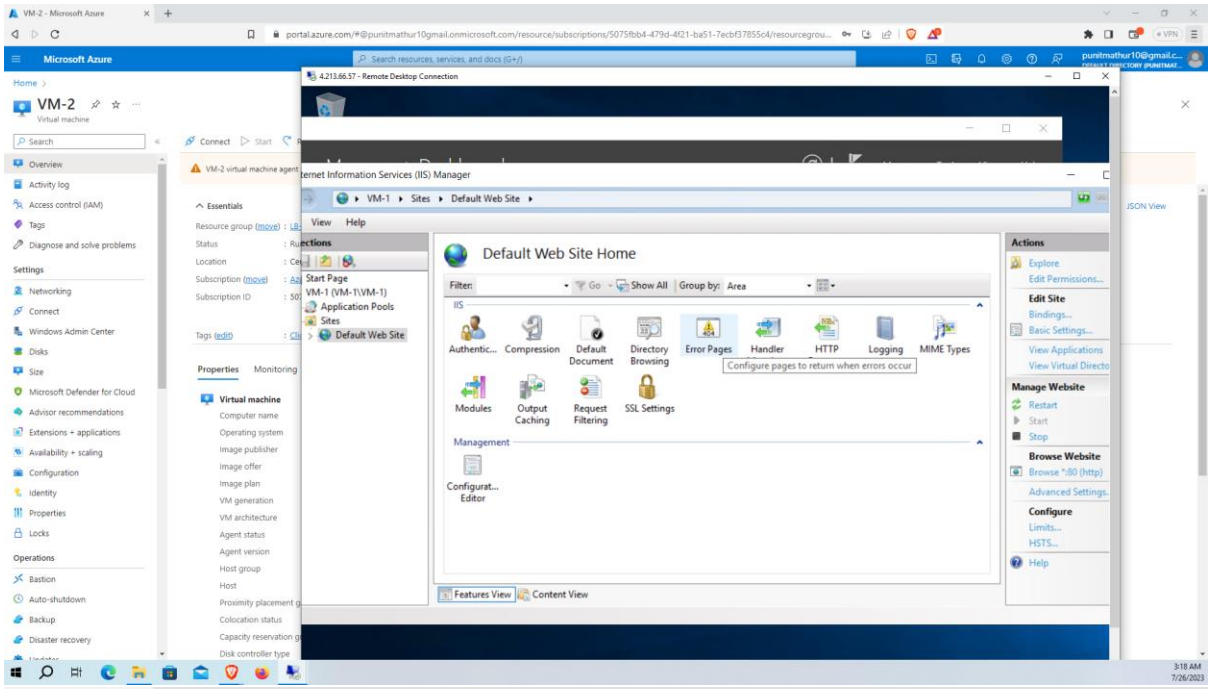
Now install IIS Server on both of them.

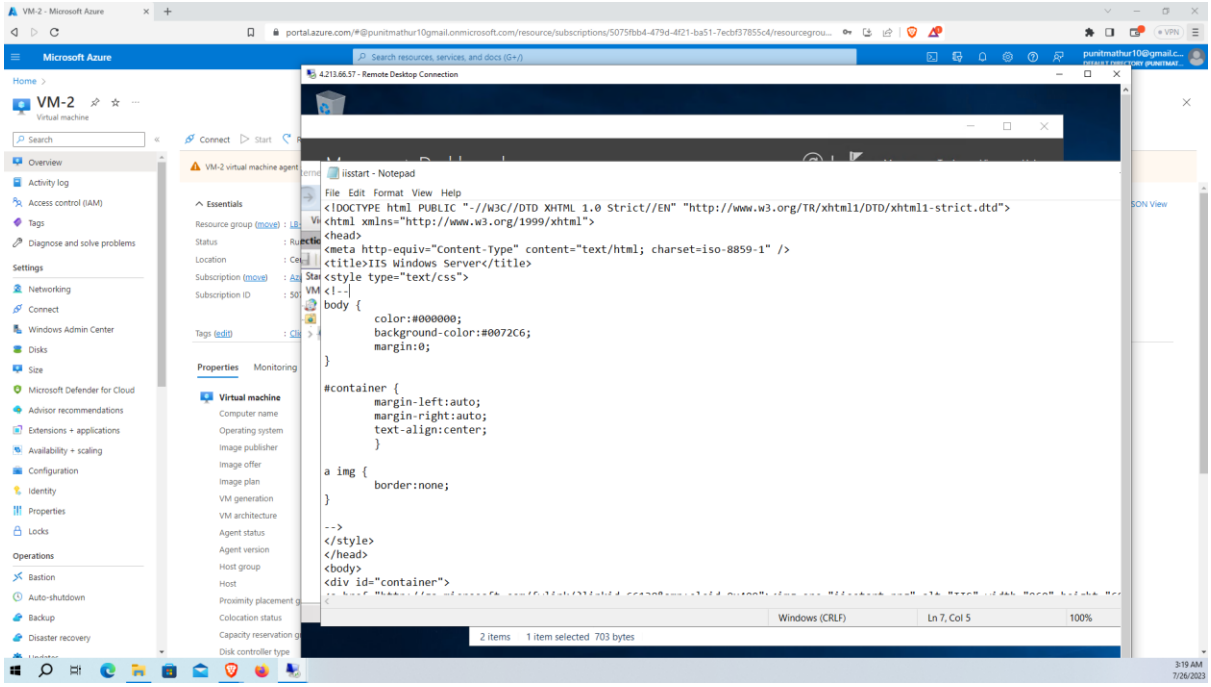




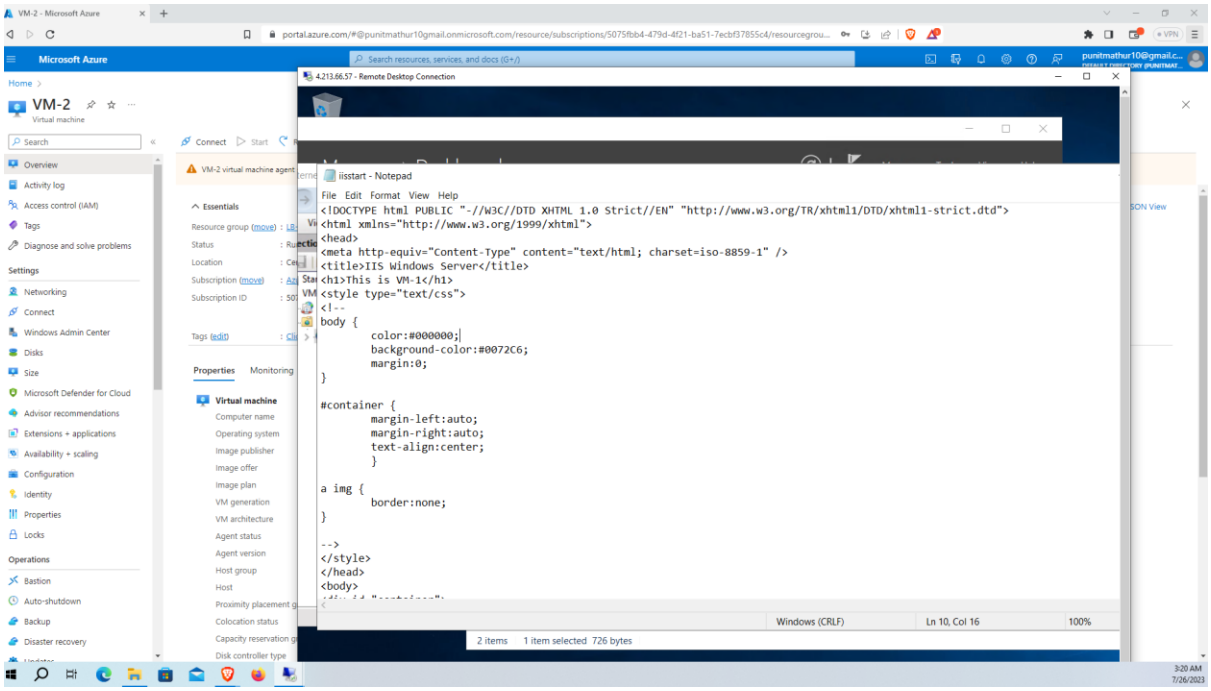
Now go to the Tools and then open the IIS Manager. Now go to the IIS Manager then expand the VM and then Sites and click on Default Web Site.Now go to C drive and then inetpub -> wwwroot and then open the iisstart html file on notepad.Now edit this html file so that we can recognize that the load balancer is sending traffic to which machine.As you can see in the below screenshot that our changes are reflected on the website too.

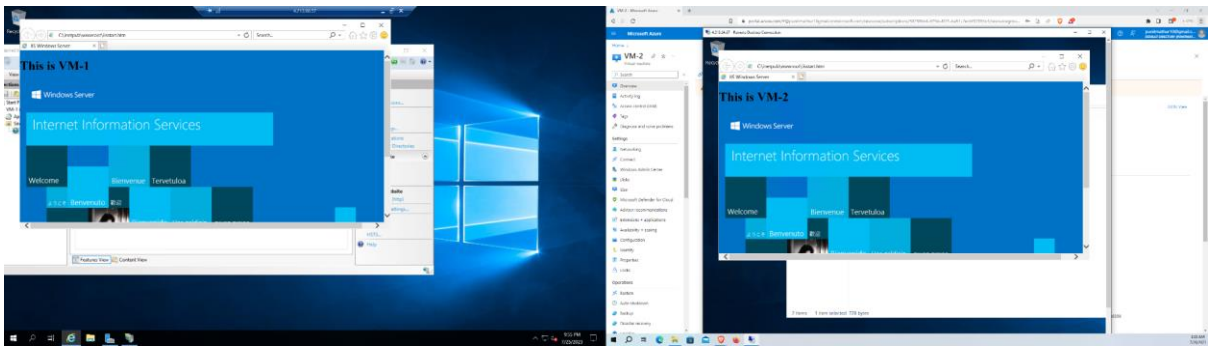



VM-2 - Microsoft Azure
Microsoft Azure
VM-2
Virtual machine
4.213.66.57 - Remote Desktop Connection
Internet Information Services (IIS) Manager
VM-1 ▸ Sites ▸ Default Web Site ▸
Default Web Site Home
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler
HTTP
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Configurat... Editor
Features View
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Limits...
HSTS...
Help

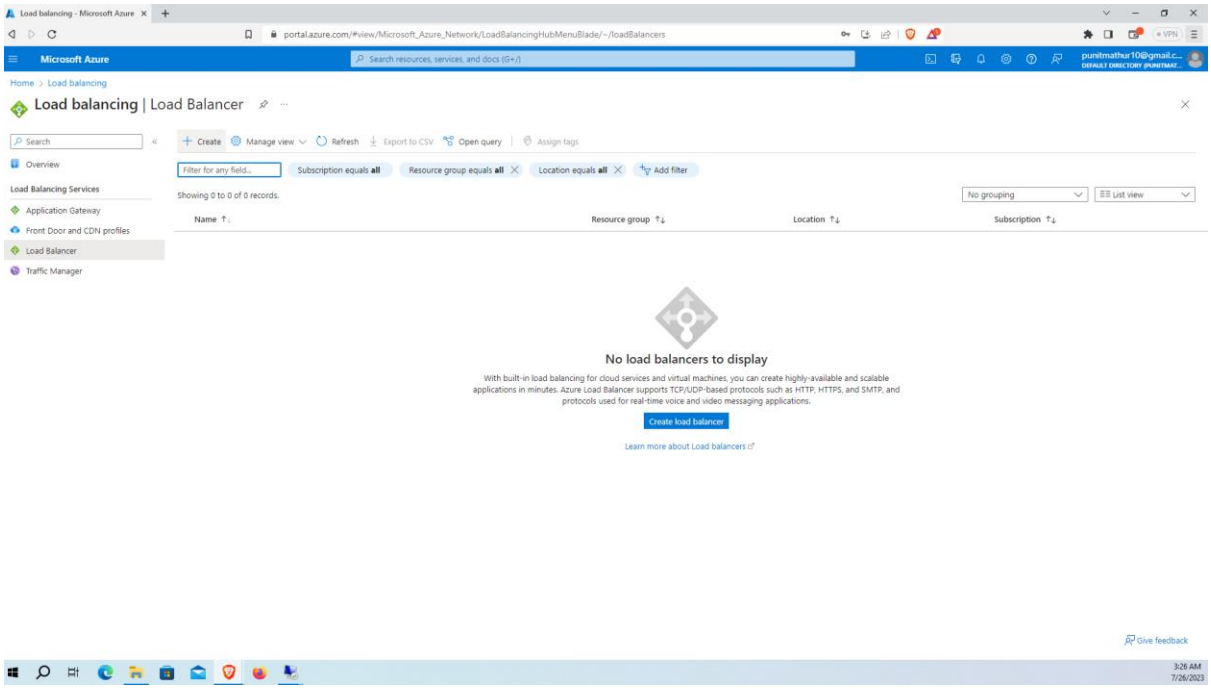

VM-2 - Microsoft Azure
Microsoft Azure
VM-2
Virtual machine
4.213.66.57 - Remote Desktop Connection
iisstart - Notepad
File Edit Format View Help
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
color:#000000;
background-color:#0072C6;
margin:0;
}
#container {
margin-left:auto;
margin-right:auto;
text-align:center;
}
a img {
border:none;
}
-->
</style>
</head>
<body>

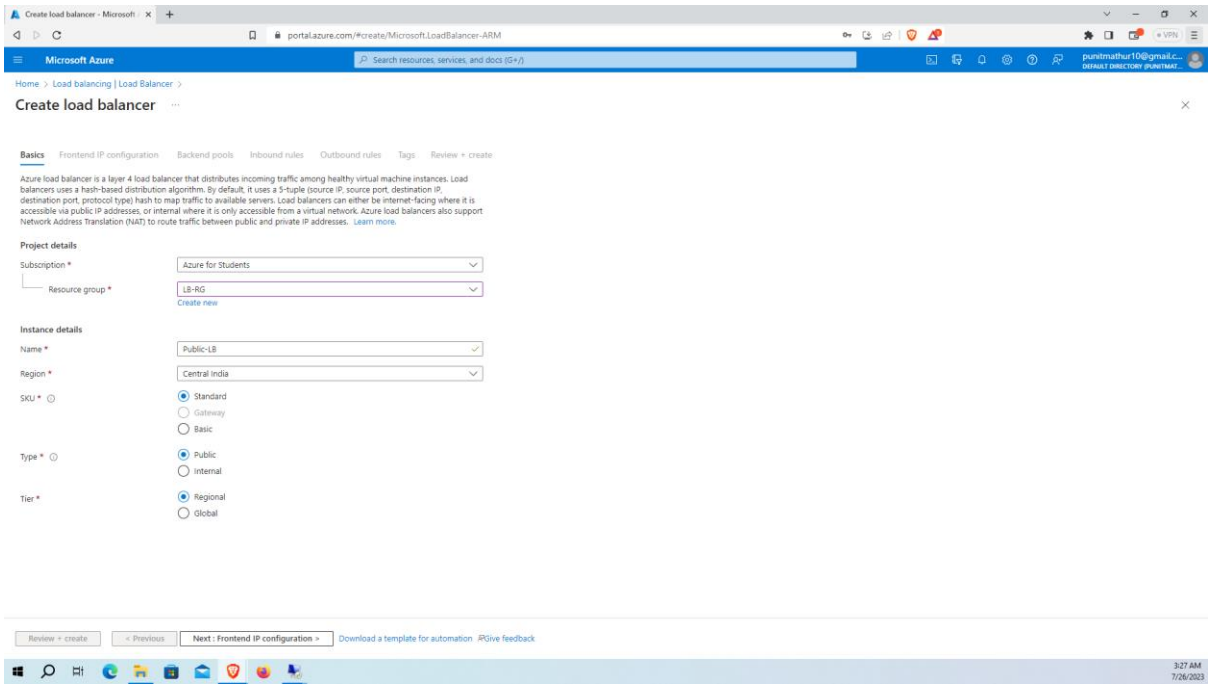
Windows (CRLF)
Ln 7, Col 5
100%
2 items
1 item selected 703 bytes

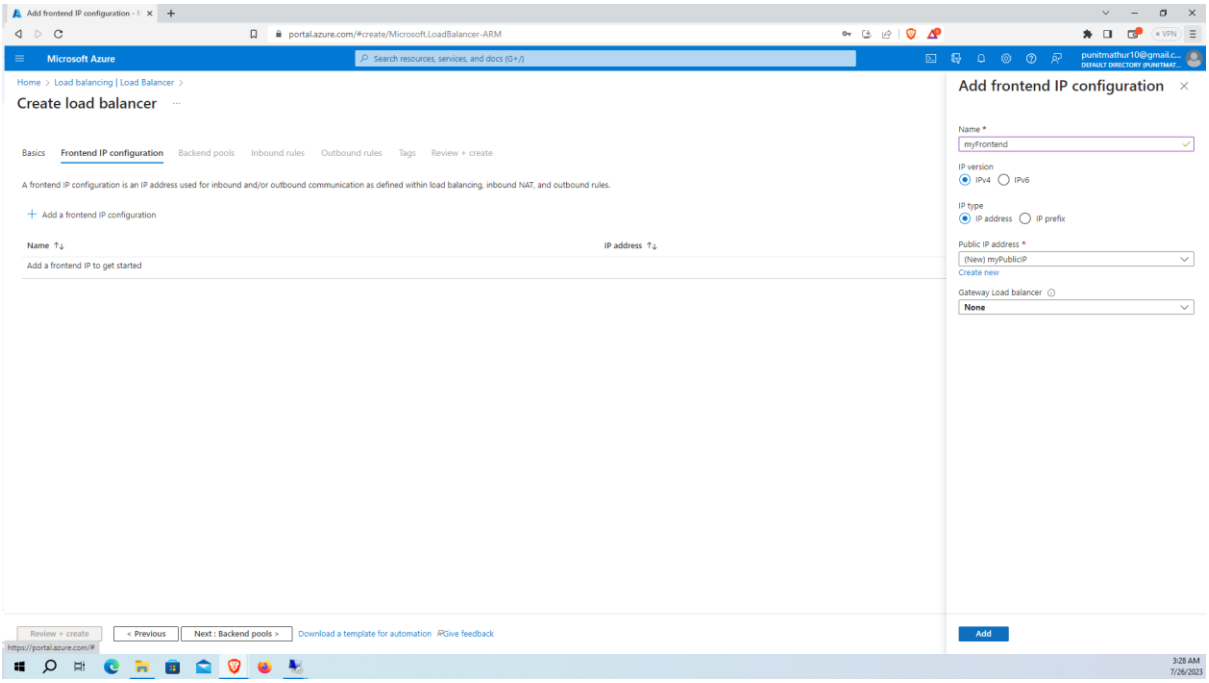

VM-2 - Microsoft Azure
Microsoft Azure
Home
VM-2
Virtual machine
4.213.66.57 - Remote Desktop Connection
iisstart - Notepad
File Edit Format View Help
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<h1>This is VM-1</h1>
<style type="text/css">
<!--
body {
color:#000000;
background-color:#0072C6;
margin:0;
}
#container {
margin-left:auto;
margin-right:auto;
text-align:center;
}
a img {
border:none;
}
-->
</style>
</head>
<body>
Windows (CRLF)
Ln 10, Col 16
100%
2 items
1 item selected 726 bytes

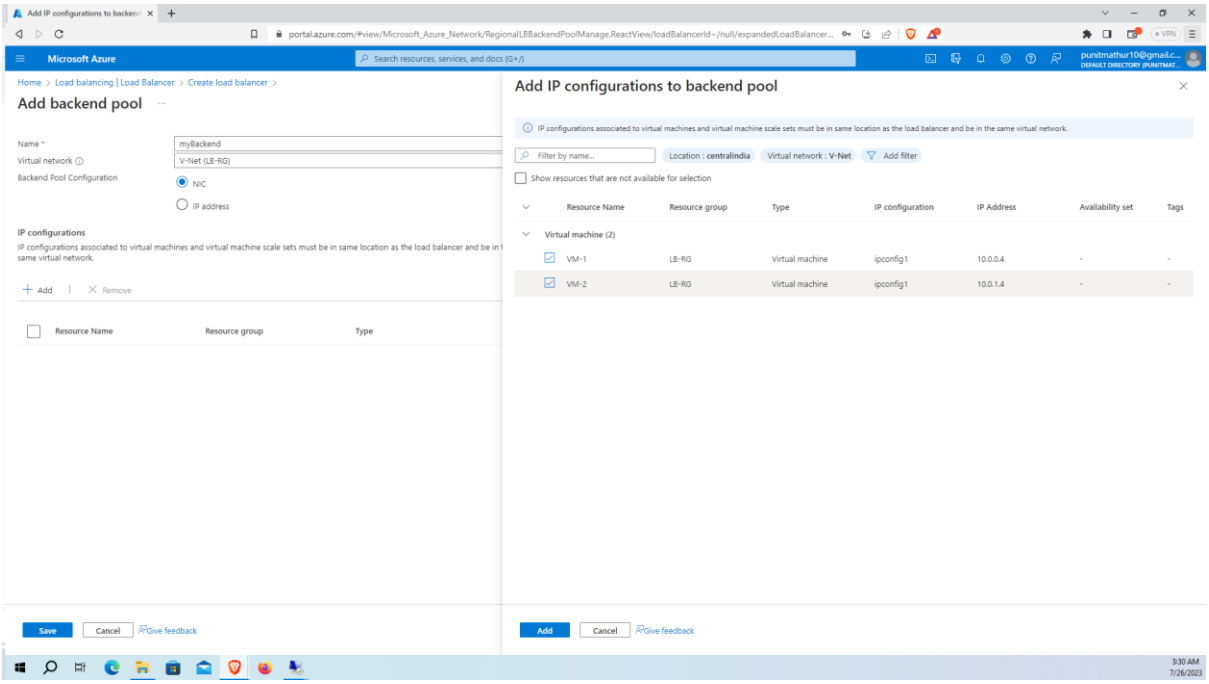

This is VM-1
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
This is VM-2
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa

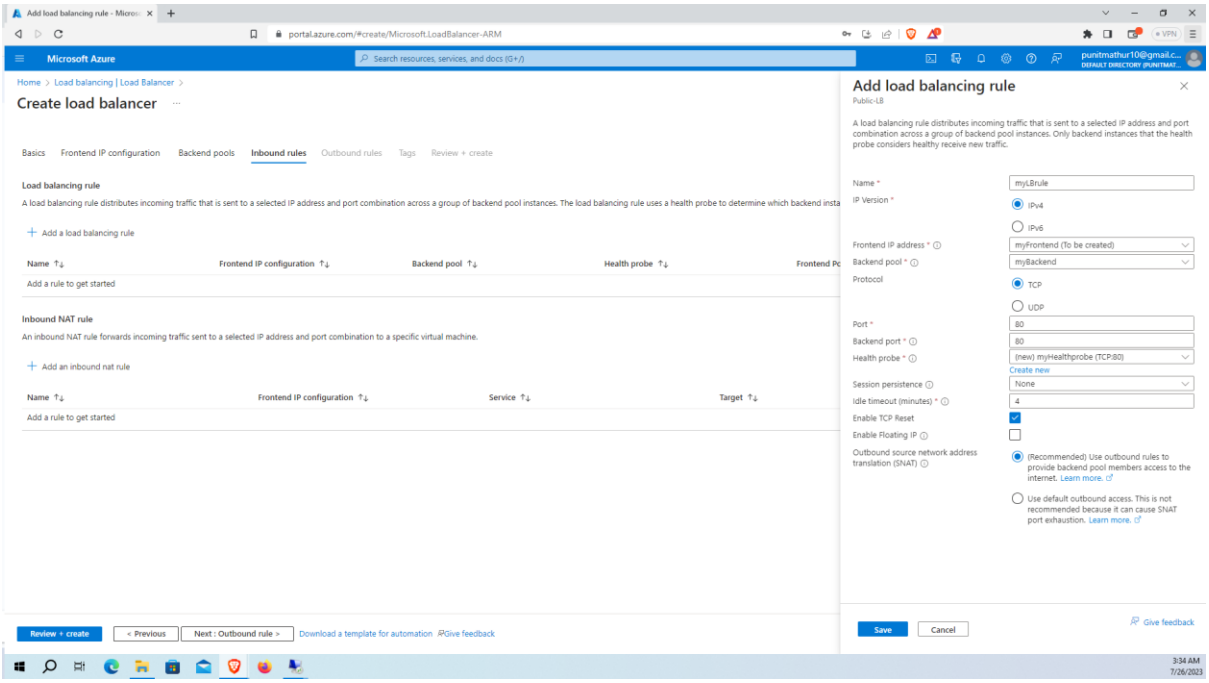
Now we will Create a Public Load Balancer following the steps mentioned below in the screenshots : -

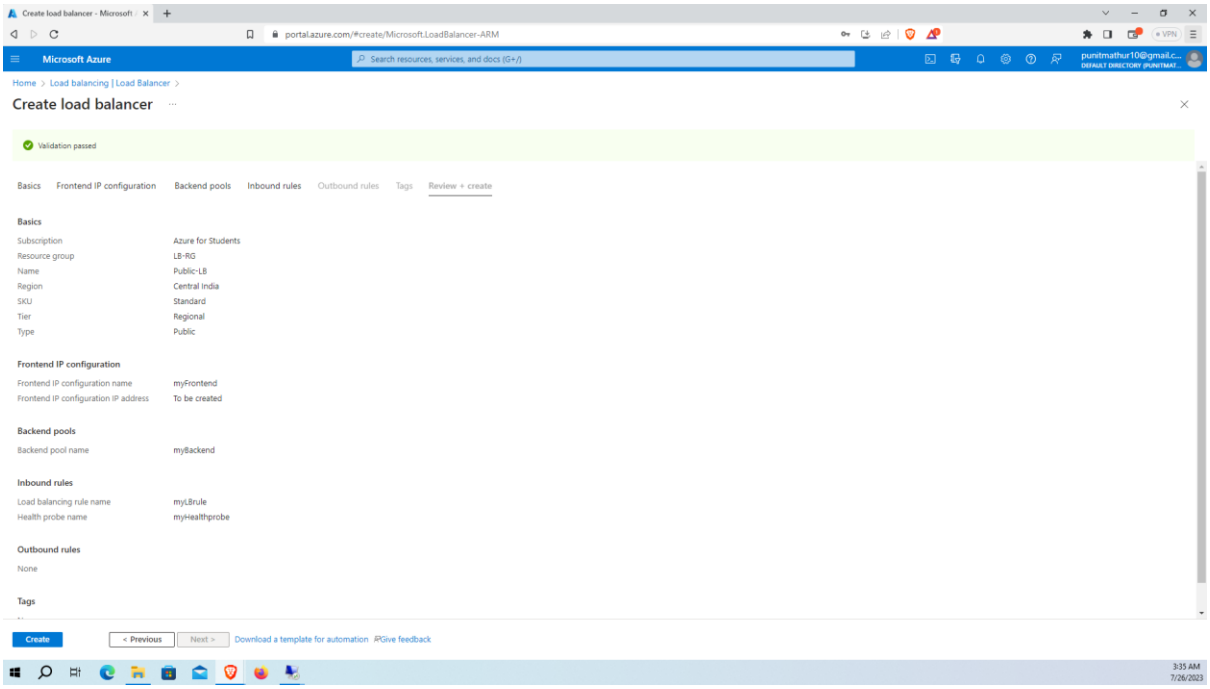


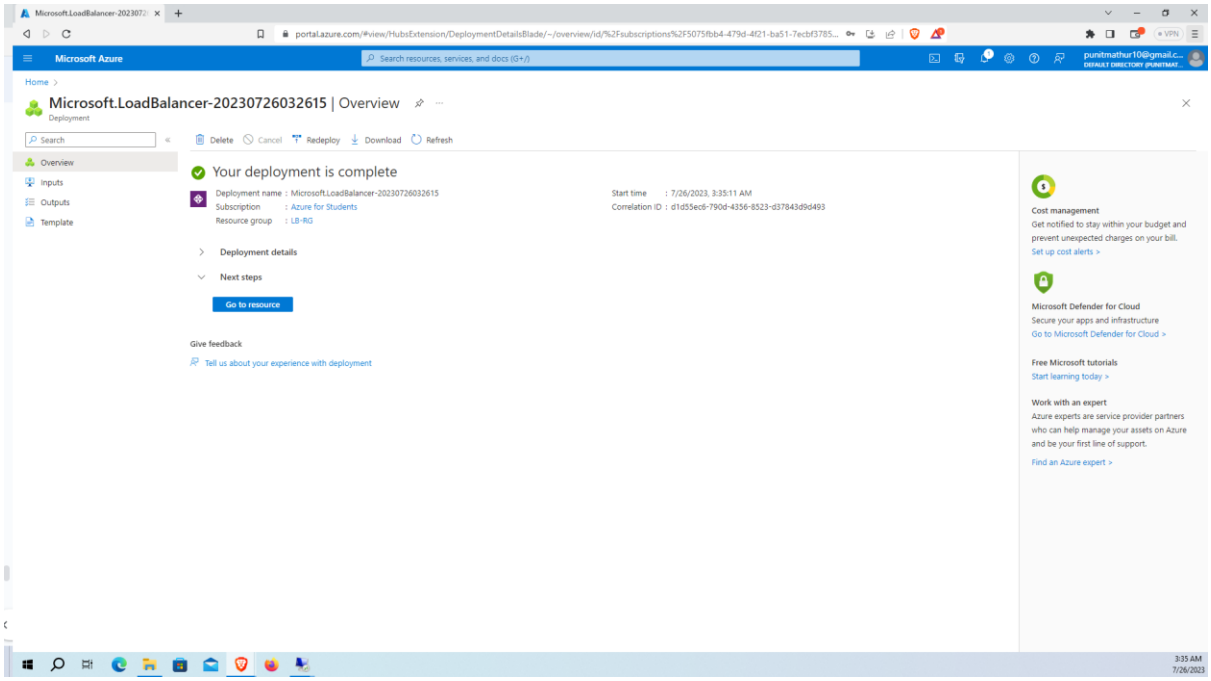


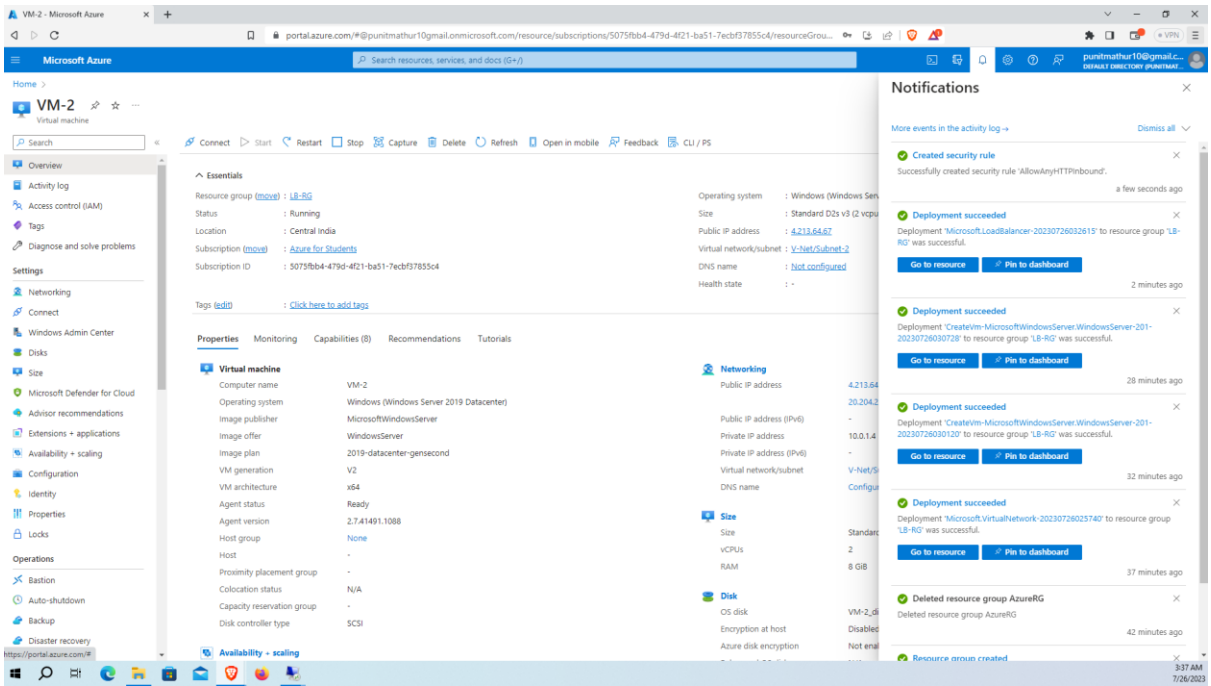

Add frontend IP configuration
portal.azure.com/#create/Microsoft.LoadBalancer-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancing | Load Balancer >
Create load balancer
Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create
A 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
Add a frontend IP to get started
Review + create
< Previous
Next : Backend pools >
Download a template for automation
Give feedback
Add frontend IP configuration
Name *
myFrontend
IP version
IPv4
IPv6
IP type
IP address
IP prefix
Public IP address *
(New) myPublicIP
Create new
Gateway Load balancer
None
Add
3:28 AM
7/26/2023

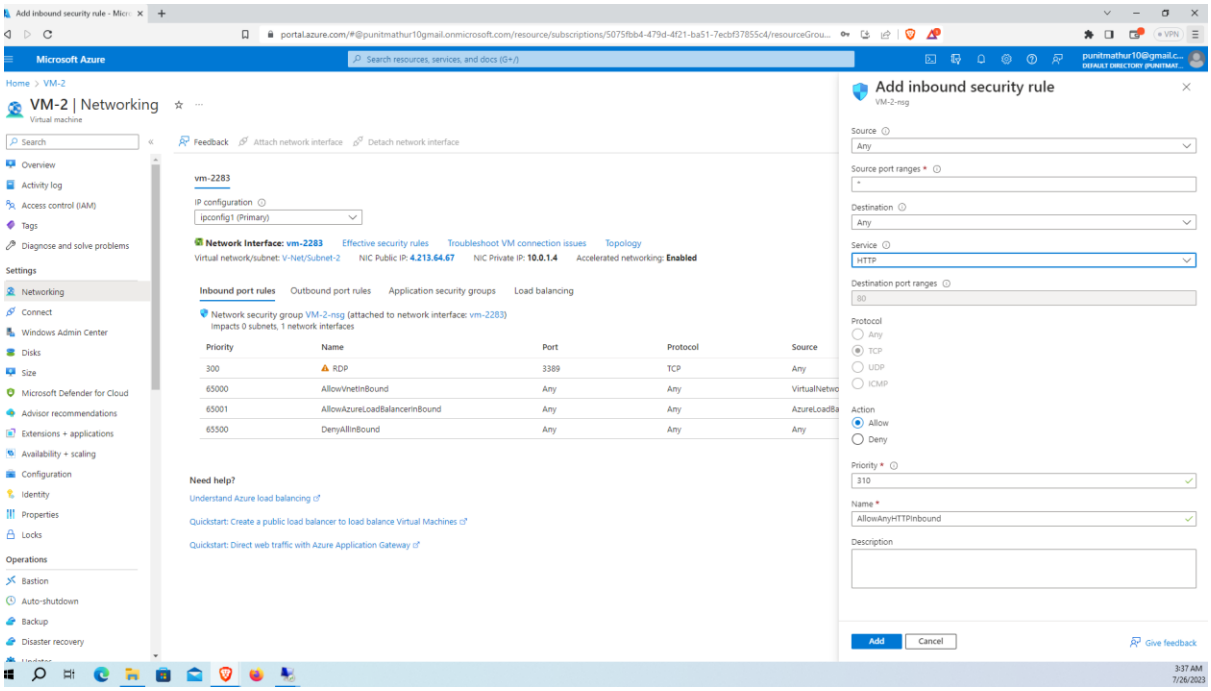

Add IP configurations to backend
portal.azure.com/#view/Microsoft_Azure_Network/RegionalLBBackendPoolManage.ReactView/loadBalancerId~/null/expandedLoadBalancer...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancing | Load Balancer > Create load balancer >
Add backend pool
Name *
myBackend
Virtual network
V-Net (LB-RG)
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
Save
Cancel
Give feedback
Add IP configurations to backend pool
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.
Filter by name...
Location : centralindia
Virtual network : V-Net
Add filter
Show resources that are not available for selection
Resource Name
Resource group
Type
IP configuration
IP Address
Availability set
Tags
Virtual machine (2)
VM-1
LB-RG
Virtual machine
ipconfig1
10.0.0.4
VM-2
LB-RG
Virtual machine
ipconfig1
10.0.1.4
Add
Cancel
Give feedback
3:30 AM
7/26/2023


Add load balancing rule - Micros
portal.azure.com/#create/Microsoft.LoadBalancer-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
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 determine which backend insta
Add a load balancing rule
Name
Frontend IP configuration
Backend pool
Health probe
Frontend Pc
Add a rule to get started
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
Review + create
< Previous
Next : Outbound rule >
Download a template for automation
Give feedback
Add load balancing rule
Public-LB
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. Only backend instances that the health probe considers healthy receive new traffic.
Name *
myLBrule
IP Version *
IPv4
IPv6
Frontend IP address *
myFrontend (To be created)
Backend pool *
myBackend
Protocol
TCP
UDP
Port *
80
Backend port *
80
Health probe *
(new) myHealthprobe (TCP:80)
Create new
Session persistence
None
Idle timeout (minutes) *
4
Enable TCP Reset
Enable Floating IP
Outbound source network address translation (SNAT)
(Recommended) Use outbound rules to provide backend pool members access to the internet. Learn more.
Use default outbound access. This is not recommended because it can cause SNAT port exhaustion. Learn more.
Save
Cancel
Give feedback
3:34 AM
7/26/2023


Create load balancer - Microsoft
portal.azure.com/#create/Microsoft.LoadBalancer-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home > Load balancing | Load Balancer >
Create load balancer
Validation passed
Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create
Basics
Subscription
Azure for Students
Resource group
LB-RG
Name
Public-LB
Region
Central India
SKU
Standard
Tier
Regional
Type
Public
Frontend IP configuration
Frontend IP configuration name
myFrontend
Frontend IP configuration IP address
To be created
Backend pools
Backend pool name
myBackend
Inbound rules
Load balancing rule name
myLBrule
Health probe name
myHealthprobe
Outbound rules
None
Tags
Create
< Previous
Next >
Download a template for automation
Give feedback
3:35 AM
7/26/2023


Microsoft Azure
Search resources, services, and docs (G+/)
Home
Microsoft.LoadBalancer-20230726032615 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : Microsoft.LoadBalancer-20230726032615
Subscription : Azure for Students
Resource group : LB-RG
Start time : 7/26/2023, 3:35:11 AM
Correlation ID : d1d55ec6-790d-4356-8523-d37843d9d493
Deployment details
Next steps
Go to resource
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 >
3:35 AM
7/26/2023


VM-2 - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Home
VM-2
Virtual machine
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Availability + scaling
Configuration
Identity
Properties
Locks
Operations
Bastion
Auto-shutdown
Backup
Disaster recovery
Essentials
Resource group (move) : LB-RG
Status : Running
Location : Central India
Subscription (move) : Azure for Students
Subscription ID : 5075fbb4-479d-4f21-ba51-7ecbf37855c4
Tags (edit) : Click here to add tags
Operating system : Windows (Windows Ser
Size : Standard D2s v3 (2 vcpu
Public IP address : 4.213.64.67
Virtual network/subnet : V-Net/Subnet-2
DNS name : Not configured
Health state : -
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name VM-2
Operating system Windows (Windows Server 2019 Datacenter)
Image publisher MicrosoftWindowsServer
Image offer WindowsServer
Image plan 2019-datacenter-gensecond
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.41491.1088
Host group None
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI
Networking
Public IP address 4.213.64
Public IP address (IPv6) -
Private IP address 10.0.1.4
Private IP address (IPv6) -
Virtual network/subnet V-Net/S
DNS name Configur
Size
Size Standard
vCPUs 2
RAM 8 GiB
Disk
OS disk VM-2_di
Encryption at host Disabled
Azure disk encryption Not enal
Availability + scaling
Notifications
More events in the activity log →
Dismiss all
Created security rule
Successfully created security rule 'AllowAnyHTTPInbound'.
a few seconds ago
Deployment succeeded
Deployment 'Microsoft.LoadBalancer-20230726032615' to resource group 'LB-RG' was successful.
Go to resource
Pin to dashboard
2 minutes ago
Deployment succeeded
Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230726030728' to resource group 'LB-RG' was successful.
Go to resource
Pin to dashboard
28 minutes ago
Deployment succeeded
Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230726030120' to resource group 'LB-RG' was successful.
Go to resource
Pin to dashboard
32 minutes ago
Deployment succeeded
Deployment 'Microsoft.VirtualNetwork-20230726025740' to resource group 'LB-RG' was successful.
Go to resource
Pin to dashboard
37 minutes ago
Deleted resource group AzureRG
Deleted resource group AzureRG
42 minutes ago
Resource group created
3:37 AM
7/26/2023


Add inbound security rule - Micr
portal.azure.com/#@punitmathur10gmail.onmicrosoft.com/resource/subscriptions/5075fbb4-479d-4f21-ba51-7ecbf37855c4/resourceGrou...
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home > VM-2
VM-2 | Networking
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Availability + scaling
Configuration
Identity
Properties
Locks
Operations
Bastion
Auto-shutdown
Backup
Disaster recovery
Feedback
Attach network interface
Detach network interface
vm-2283
IP configuration
ipconfig1 (Primary)
Network Interface: vm-2283
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: V-Net/Subnet-2
NIC Public IP: 4.213.64.67
NIC Private IP: 10.0.1.4
Accelerated networking: Enabled
Inbound port rules
Outbound port rules
Application security groups
Load balancing
Network security group VM-2-nsg (attached to network interface: vm-2283)
Impacts 0 subnets, 1 network interfaces
Priority
Name
Port
Protocol
Source
300
RDP
3389
TCP
Any
65000
AllowVnetInBound
Any
Any
VirtualNetwo
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBa
65500
DenyAllInBound
Any
Any
Any
Need help?
Understand Azure load balancing
Quickstart: Create a public load balancer to load balance Virtual Machines
Quickstart: Direct web traffic with Azure Application Gateway
Add inbound security rule
VM-2-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
HTTP
Destination port ranges
80
Protocol
Any
TCP
UDP
ICMP
Action
Allow
Deny
Priority *
310
Name *
AllowAnyHTTPInbound
Description
Add
Cancel
Give feedback
3:37 AM
7/26/2023