

Azure Load Balancer

Overview

Azure Load Balancer distributes incoming network traffic across a group of backend virtual machines (VMs) or VM scale sets to ensure high availability. It operates at **Layer 4** of the OSI model and acts as a single point of contact for clients.

Azure Load Balancer helps with:

- **High Availability:** If one VM fails, it routes traffic to another.
- **Scalability:** Balances workloads during periods of high demand.
- **Performance:** Optimizes resource utilization.

Types of Azure Load Balancer:

- **Public Load Balancer:** Provides both inbound and outbound connectivity for VMs in your virtual network. It routes internet traffic to your VMs and translates private IPs to public IPs for outbound connections.
- **Internal Load Balancer:** Balances traffic within a private virtual network.

For more insight on Azure Load Balancer visit [Microsoft Learn](#)

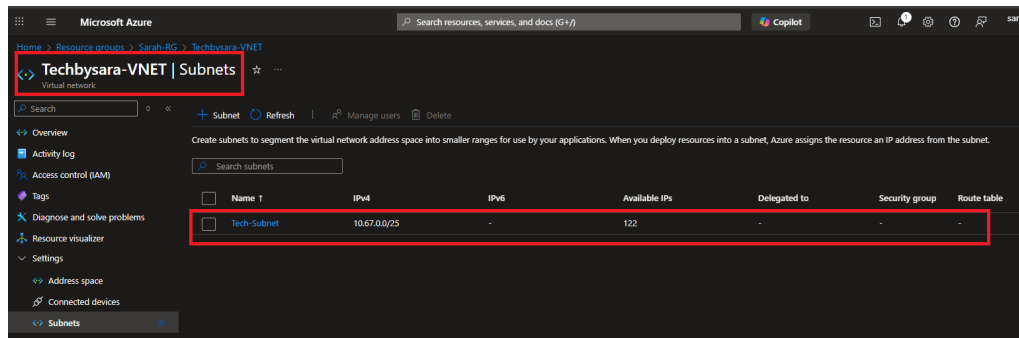
Deploy and Test Azure Load Balancer

Step 1: Prepare the Environment

Ensure the following Azure resources are already in place. These were covered in detail in my previous articles, linked below

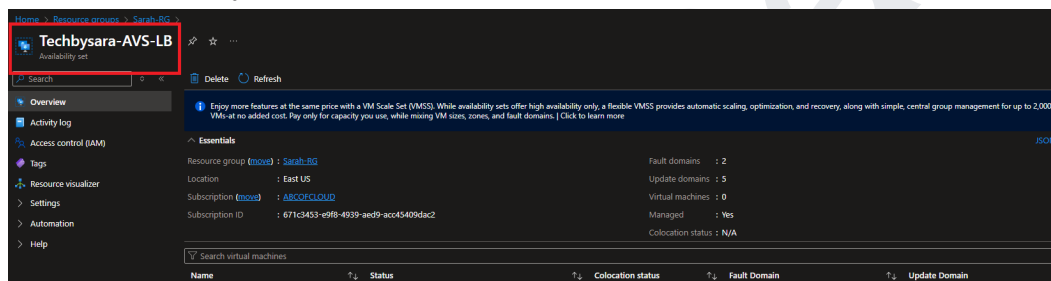
[Creating a VM on Azure](#), [NSG and Public IP Configuration](#), [Availability Sets](#)

- Resource Group: to logically group Azure resources.
- Virtual Network and Subnets.



- Public IP address
- Create a Network Security group (NSG):
 - Allow inbound rules for port **3389** (RDP) from your IP address (low priority).
 - Allow inbound rule for port 80 (HTTP).
 - Associate NSG to the **subnet** shared by both VMs.

➤ Availability Sets

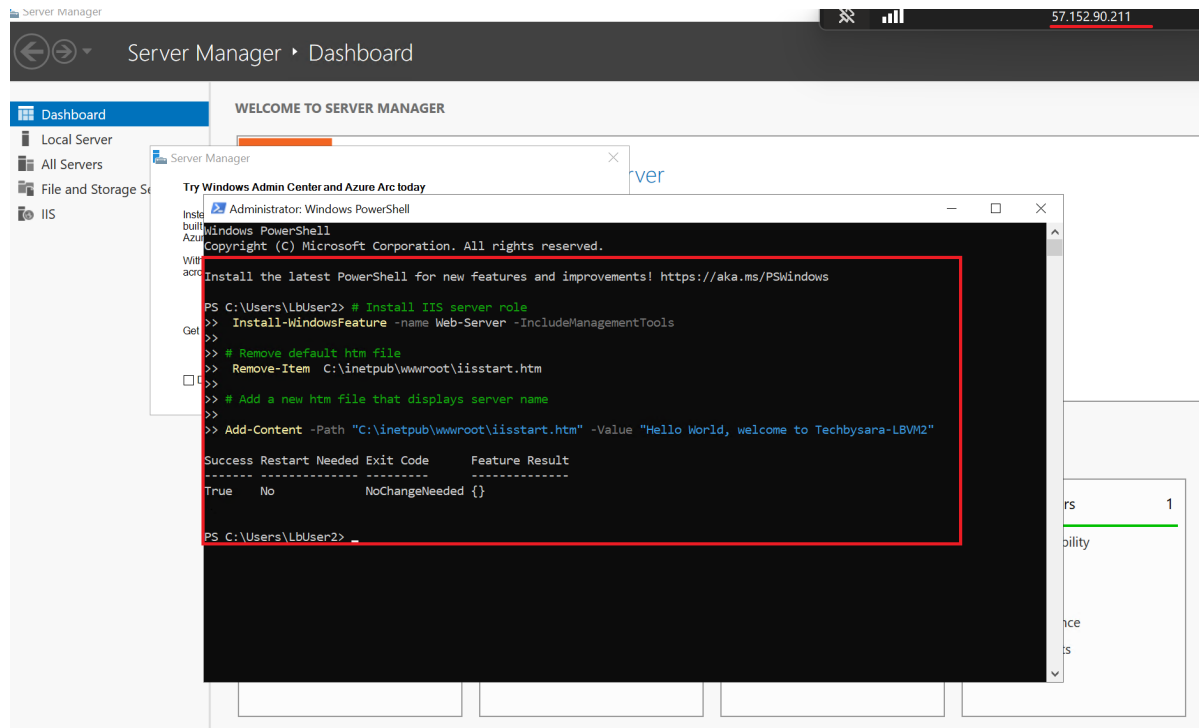


- Two Virtual Machines: ensure both are added to the same Availability Set (for fault domain separation).

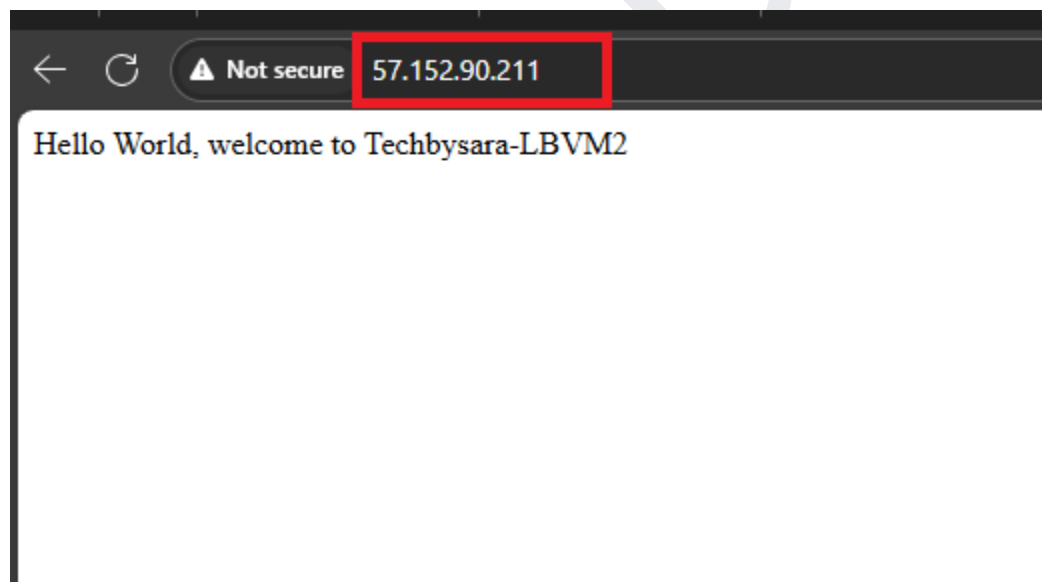
Configure VM:

Note: Exposing RDP (port 3389) to the internet is not recommended in production environments. Use VPN or **Azure Bastion** instead. This setup is for testing purposes only.

- On the VMs overview page > Select Connect > Download RDP file.
- Establish connection using the VMs public IP address > Enter credentials > Click OK.
- Install IIS using PowerShell.
 - On the VM search bar > Windows PowerShell > Open.
 - Install the ISS server.
 - Replace default iisstart.htm with a custom file displaying the VMs name.



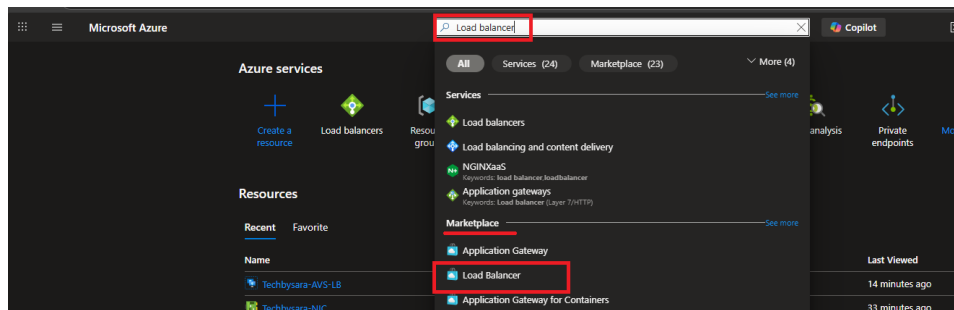
- Confirm the new HTML page reflects the VM name.



Once completed, disassociate the public IPs from both VMs. The Load Balancer will route traffic.

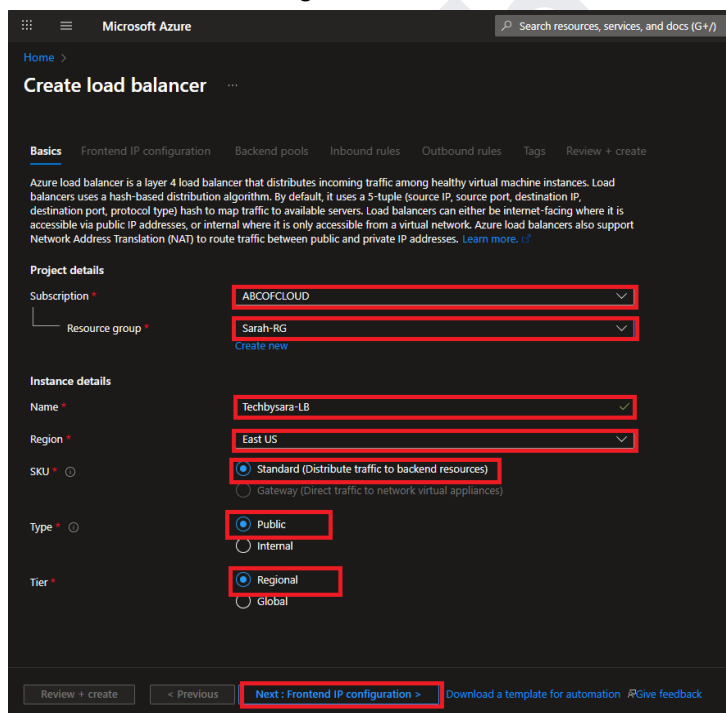
Step 2: Create the Load Balancer

1. On Azure portal search > “**Load Balancer**” under Market place and select it.



2. Fill in the basic settings:

- **Subscription:** Select your active subscription under which you want to create this Load balancer.
- **Resource group:** Select your existing resource group.
- **Name:** Enter your preferred name (eg., Sarah-RG).
- **Region:** Select the same region as your VMs (e.g., East US).
- **SKU:** Select Standard ideal for workloads that require high performance and low latency.
- **Type:** Select Public load balancer (This would enable access from the public IP of the load balancer).
- **Tier:** Select Regional



Select > Next: Frontend IP Configuration:

- In Frontend IP configuration, select + Add a frontend IP configuration.
- Name: Select your preferred name (e.g., Techbysara_FrontendIP).
- IP version: IPv4
- IP type: IP address.
- Public IP address: Select your public IP or create new.
- Click Save

Microsoft Azure

Search resources, services, and docs (G+/I)

Home >

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 ↑↓
Techbysara_FrontendIP	Techbysara-PIP (52.226.176.70)

Review + create < Previous **Next: Backend pools >** Download a template for automation Give feedback

Select Next: Backend pools:

- Name: Enter your preferred backend pool name (e.g., Techbysara-BackendPool).
- Virtual Network: Select your VNet (e.g., Techbysara-VNET).
- Backend pool Configuration: Select NIC.
- + Add: Choose the two VMs.

Note: All IP configurations must be in the same region and VNet as the Load Balance.

Microsoft Azure

Search resources, services, and docs (G+/I)

Home >

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
▼ Techbysara_BackendPool						
Techbysara_BackendPool	Techbysara-VNET	Techbysara-LBVM1	techbysara-lbvm1838	10.67.0.5	-	None
Techbysara_BackendPool	Techbysara-VNET	Techbysara-LBVM2	techbysara-lbvm2885	10.67.0.6	-	None

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

Select Next: Inbound rules:

Under Inbound rules > Select + Add a load balancing rule.

- Name: Enter your preferred LB rule name (e.g., Techbysara-LBRule)..
- IP version: IPv4

- Frontend IP address: Select your configured frontend IP from the drop down menu.
- Backend pool: Select your backend pool from the drop down menu.
- Protocol: Select TCP
- Port: 80
- Backend port: 80
- **Health probe:** Create new.
 - Enter your preferred name.
 - Protocol: TCP.
 - Port: 80
 - Interval (seconds) Leave the default.
 - Save
- Session persistence: Select > None.
- Idle timeout (minute): Leave the default.
- Leave other options as default.

Home >

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 instances are eligible to receive traffic.

[+ Add a load balancing rule](#)

Name ↑↓	Frontend IP configuration ↑↓	Backend pool ↑↓	Health probe ↑↓	Frontend Port ↑↓	Backend port ↑↓
Techbysara-LBRule	Techbysara_FrontendPool	Techbysara_BackendPool	Techbysara-HealthProbe	80	80

Select + Add an Inbound NAT Rule:

An **Inbound NAT rule** maps a port on the Load Balancer's public IP to a specific port on a **single VM**, enabling direct access to it

- Name: Enter your preferred name(e.g., LBVM1-NAT).
- Type: Select VM.
- Target virtual machine: Select your target VM from the dropdown menu.
- Network IP configuration: Select the VM private IP.
- Frontend IP address: Select the frontendpool from the dropdown.
- Frontend port: 2000
- Service Tag: Custom
- Backend port: 3389
- Protocol: Select TCP
- Enable TCP Reset: Leave unchecked.
- Idle timeout minute: Leave the default.
- Enable Floating IP: Leave unchecked.
- Select Save.

Add inbound NAT rule

Techbysara-LB

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

⚠ Inbound NAT rule v1 will be retired on 30, September 2027. It is highly recommended to start new creations on V2 of Inbound NAT rules to avoid future migrations and benefit from all the new and significant improvements. [Learn more.](#)

Name * LBVM1-NAT

Type ☒ Azure virtual machine ☐ Backend pool

Target virtual machine TECHBYSARA-LBVM1

Network IP configuration * ipconfig1 (10.67.0.5)

Frontend IP address * Techbysara_FrontendIP (52.226.176.70)

Frontend Port * 2000

Service Tag * Custom

Backend port * 3389

Protocol ☒ TCP ☐ UDP

Enable TCP Reset ☐

Idle timeout (minutes) * 4

Enable Floating IP ☐

Save **Cancel** [Give feedback](#)

➤ Repeat for the second VM.

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 instances are eligible to receive traffic.

+ Add a load balancing rule

Name ↑↓	Frontend IP configuration ↑↓	Backend pool ↑↓	Health probe ↑↓	Frontend Port ↑↓	Backend port ↑↓
Techbysara-LBRule	Techbysara_FrontendIP	Techbysara_BackendPool	Techbysara-HealthProbe	80	80

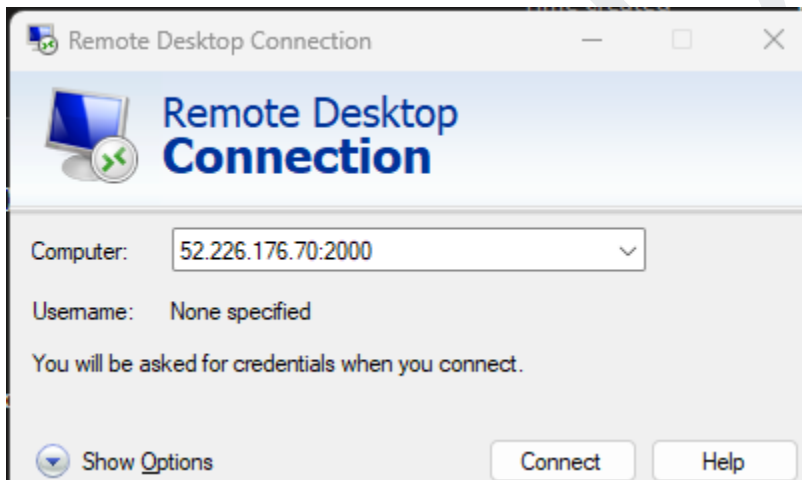
Inbound NAT rule

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 ↑↓	Frontend Port ↑↓
LBVM1-NAT	Techbysara_FrontendIP	Custom	TECHBYSARA-LBVM1	2000
LBVM2	Techbysara_FrontendIP	Custom	TECHBYSARA-LBVM2	3004

- Proceed to Next: Review + create > Create.
- After deployment, establish RDP connections using:
 - Load balancer Public IP.
 - Frontend NATports (e.g., 2000 and 3004).



Successfully connected to both VMs via the Load Balancer and test web access on port 80.

