

Availability Zones & Standard Load Balancer

CREATE A STANDARD LOAD BALANCER

1. On the top left-hand side of the screen, click **Create a Resource** and type in **Load Balancer**.
2. Click **+Add**.
3. Place the resources in the resource group you just created for the Azure Backup resources.
4. Use the following inputs to create the load balancer:
 - **stdlb1** – load balancer name.
 - **Region** – Central US (not every region supports Availability Zones).
 - **Public** – for the type of load balancer.
 - **Standard** – for the SKU type.
 - **Create New Public IP Address**
 - **stdlb1-pip** – for the Standard Load Balancer name.
 - **3** – for the Availability Zone.
5. Click **Review + Create** to create the load balancer. You will not be creating tags.

Create load balancer

[Basics](#) [Tags](#) [Review + create](#)

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers use 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

* Type ☐ Internal ☒ Public

* SKU ☐ Basic ☒ Standard

PUBLIC IP ADDRESS

* Public IP address ☒ Create new ☐ Use existing

* Public IP address name

Public IP address SKU

* Assignment ☐ Dynamic ☒ Static

* Availability zone

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

CREATE BACKEND SERVERS VIRTUAL NETWORK

1. On the top left-hand side of the screen click **Create a Resource** and type in **Virtual Network**. Enter these values for the virtual network:
 - *myVnet* - for the name of the virtual network.
 - *10.5.0.0/16* – for the address space.
 - *Choose your Existing Resource Group*.
 - *Central US* – for the location.
 - *myBackendSubnet* - for the subnet name.
 - *10.5.0.0/24* – for the subnet address space.
 - *Leave Service Endpoints and Firewall disabled*.
2. Click **Create** to create the virtual network.

Create virtual network □ ×

* Name
myVnet ✓

* Address space ⓘ
10.5.0.0/16
10.5.0.0 - 10.5.255.255 (65536 addresses)

* Subscription
▼

* Resource group
▼
[Create new](#)

* Location
Central US ▼

Subnet

* Name
myBackendSubnet ✓

* Address range ⓘ
10.5.0.0/24 ✓
10.5.0.0 - 10.5.0.255 (256 addresses)

DDoS protection ⓘ
☒ Basic ☐ Standard

Service endpoints ⓘ
Disabled Enabled

Firewall ⓘ
Disabled Enabled

Create Automation options

CREATE A NETWORK SECURITY GROUP

1. On the top left-hand side of the screen, click **Create a resource**, in the search box type *Network Security Group*, and in the network security group page, click **Create**.
2. In the Create network security group page, enter these values:
 - *myNetworkSecurityGroup* - for the name of the network security group.
 - *Select existing Resource Group*.
 - *Central US* – for the location.

Create network security g... □ ×

* Name

myNetworkSecurityGroup ✓

* Subscription

* Resource group

Create new

* Location

Central US

Create

Automation options

CREATE NETWORK SECURITY GROUP RULES

1. In the Azure portal, click **All resources** in the left-hand menu, and then search and click **myNetworkSecurityGroup** that is located in the existing you have been using resource group.
2. Under **Settings**, click **Inbound security rules**.



3. Click **Add**.

+ Add Default rules						
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

- *Service Tag* - for **Source**.
- *Internet* - for **Source service tag**
- *80* - for **Destination port ranges**
- *TCP* - for **Protocol**
- *Allow* - for **Action**
- *100* for **Priority**
- *myHTTPRule* - for name of the load balancer rule.
- *Allow HTTP* - for description of the load balancer rule.

Add inbound security rule

myNetworkSecurityGroup

Basic

* Source ⓘ

Service Tag

* Source service tag ⓘ

Internet

* Source port ranges ⓘ

*

* Destination ⓘ

Any

* Destination port ranges ⓘ

80

* Protocol

Any TCP UDP

* Action

Allow Deny

* Priority ⓘ

100

* Name


myHTTPRule

Description


Allow HTTP

Add

6. Repeat steps 2 to 4 to create another rule named *myRDPRule* to allow for an inbound RDP connection using port 3389 with the following values:
- *Service Tag* - for **Source**.
 - *Internet* - for **Source service tag**
 - *3389* - for **Destination port ranges**
 - *TCP* - for **Protocol**
 - *Allow* - for **Action**
 - *200* for **Priority**
 - *myRDPRule* for name
 - *Allow RDP* - for description

 Add inbound security rule

myNetworkSecurityGroup

 Basic

* Source ⓘ

Service Tag

* Source service tag ⓘ

Internet

* Source port ranges ⓘ

*

* Destination ⓘ

Any

* Destination port ranges ⓘ

3389

* Protocol

Any TCP UDP

* Action

Allow Deny

* Priority ⓘ

200

* Name

myRDPRule

Description

Allow RDP

Add

+ Add		Default rules				
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	myHTTPRule	80	TCP	Internet	Any	Allow
200	myRDPRule	3389	TCP	Internet	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

CREATE VIRTUAL MACHINES

Create virtual machines in different zones (zone 1, zone 2, and zone 3) for the region that can act as backend servers to the load balancer.

- On the top left-hand side of the screen, click **Create a resource > Compute > Windows Server 2016 Datacenter** and enter these values for the virtual machine:
 - myVM1* - for the name of the virtual machine.
 - azureuser* - for the administrator user name.
 - Select existing Resource Group*.
- Click **OK**.
- Select **DS1_V2** for the size of the virtual machine and click **Select**.
- Enter these values for the VM settings:
 - zone 1* - for the zone where you place the VM.
 - myVNet* - ensure it is selected as the virtual network.
 - myBackendSubnet* - ensure it is selected as the subnet.
 - myNetworkSecurityGroup* - for the name of network security group (firewall).
- Click **Disabled** to disable boot diagnostics.
- Click **OK**, review the settings on the summary page, and then click **Create**.

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Guest config](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? [Create VM from Azure Marketplace](#)

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

* Virtual machine name ⓘ

* Region ⓘ

Availability options ⓘ

* Availability zone ⓘ

* Image ⓘ

[Browse all images and disks](#)

* Size ⓘ **Standard DS1 v2**
1 vcpu, 3.5 GB memory
[Change size](#)

ADMINISTRATOR ACCOUNT

* Username ⓘ

* Password ⓘ

* Confirm password ⓘ

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Guest config](#) [Tags](#) [Review + create](#)

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network ⓘ

[Create new](#)

* Subnet ⓘ

[Manage subnet configuration](#)


Public IP ⓘ

[Create new](#)

NIC network security group ⓘ ☐ None ☒ Basic ☐ Advanced

* Public inbound ports ⓘ ☐ None ☒ Allow selected ports

* Select inbound ports

 These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

Accelerated networking ⓘ ☐ On ☒ Off

The selected VM size does not support accelerated networking.

LOAD BALANCING

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐ Yes ☒ No

7. Create a second VM, named, *VM2* in Zone 2, and third VM in Zone 3, and with *myVnet* as the virtual network, *myBackendSubnet* as the subnet, and **myNetworkSecurityGroup* as the network security group using steps 1-6.

INSTALL IIS ON VMs

1. Click **All resources** in the left-hand menu, and then from the resources list click **myVM1** that is located in the *myResourceGroupLBAZ* resource group.
2. On the **Overview** page, click **Connect** to RDP into the VM.
3. Log into the VM with username *azureuser*.
4. On the server desktop, navigate to **Windows Administrative Tools>Windows PowerShell**.
5. In the PowerShell Window, run the following commands to install the IIS server, remove the default iisstart.htm file, and then add a new iisstart.htm file that displays the name of the VM:

```
# Install IIS server role
Install-WindowsFeature -name Web-Server -IncludeManagementTools
# Remove default htm file
Remove-Item C:\inetpub\wwwroot\iisstart.htm
# Add a new htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from " +
$env:computername)
```

6. Close the RDP session with *myVM1*.
7. Repeat steps 1 to 6 to install IIS and the updated iisstart.htm file on *myVM2* and *myVM3*.

CREATE A BACKEND ADDRESS POOL

To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual (NICs) connected to the load balancer. Create the backend address pool *myBackendPool* to include *VM1*, *VM2*, and *VM3*.

1. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
2. Under **Settings**, click **Backend pools**, then click **Add**.
3. On the **Add a backend pool** page, do the following:
 - For name, type *myBackEndPool*, as the name for your backend pool.
 - For **Virtual network**, in the drop-down menu, click **myVNet**
 - For **Virtual machine**, in the drop-down menu, click, **myVM1**.
 - For **IP address**, in the drop-down menu, click the IP address of myVM1.
4. Click **Add new backend resource** to add each virtual machine (*myVM2* and *myVM3*) to add to the backend pool of the load balancer.
5. Click **Add**.

Add backend pool

Name
myBackendPool

IP version
IPv4

Virtual network
myvnet (3 VM)

☒ VIRTUAL MACHINE

myvm1

ipconfig1

...

myvm2

ipconfig1

...

myvm3

ipconfig1 (10.5.0.6)

...

Add

- Check to make sure your load balancer backend pool setting displays all the three VMs - **myVM1**, **myVM2** and **myVM3**.

+ Add
Refresh

Search backend address pools

VIRTUAL MACHINE	VIRTUAL MACHINE STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS
myBackendPool (3 virtual machines)			...
myVM1	Running	myvm1937	10.5.0.4
myVM2	Running	myvm2965	10.5.0.5
myVM3	Running	myvm3752	10.5.0.6

CREATE A HEALTH PROBE

To allow the load balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. Create a health probe *myHealthProbe* to monitor the health of the VMs.

- Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
- Under **Settings**, click **Health probes**, then click **Add**.
- Use these values to create the health probe:
 - myHealthProbe* - for the name of the health probe.
 - HTTP** - for the protocol type.
 - 80** - for the port number.
 - 15** - for number of **Interval** in seconds between probe attempts.
 - 2** - for number of **Unhealthy threshold** or consecutive probe failures that must occur before a VM is considered unhealthy.
- Click **OK**.

myHealthProbe
stdlib1

Save Discard Delete

* Name
myHealthProbe

IP version
IPv4

Protocol ⓘ
TCP

* Port ⓘ
80

* Interval ⓘ
15
seconds

* Unhealthy threshold ⓘ
2
consecutive failures

Used by ⓘ
Not used

CREATE A LOAD BALANCER RULE

1. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
2. Under **Settings**, click **Load balancing rules**, then click **Add**.
3. Use these values to configure the load balancing rule:
 - *myHTTPRule* - for the name of the load balancing rule.
 - **TCP** - for the protocol type.
 - *80* - for the port number.
 - *80* - for the backend port.
 - *myBackendPool* - for the name of the backend pool.
 - *myHealthProbe* - for the name of the health probe.
4. Click **OK**.

Add load balancing rule

stdlb1

Name

myHTTPRule

IP Version

☒ IPv4 ☐ IPv6

Frontend IP address ⓘ

40.67.171.59 (LoadBalancerFrontEnd)

Protocol

☒ TCP ☐ UDP

Port

80

Backend port ⓘ

80

Backend pool ⓘ

myBackendPool (3 virtual machines)

Health probe ⓘ

myHealthProbe (TCP:80)

Session persistence ⓘ

None

Idle timeout (minutes) ⓘ

4

Floating IP (direct server return) ⓘ

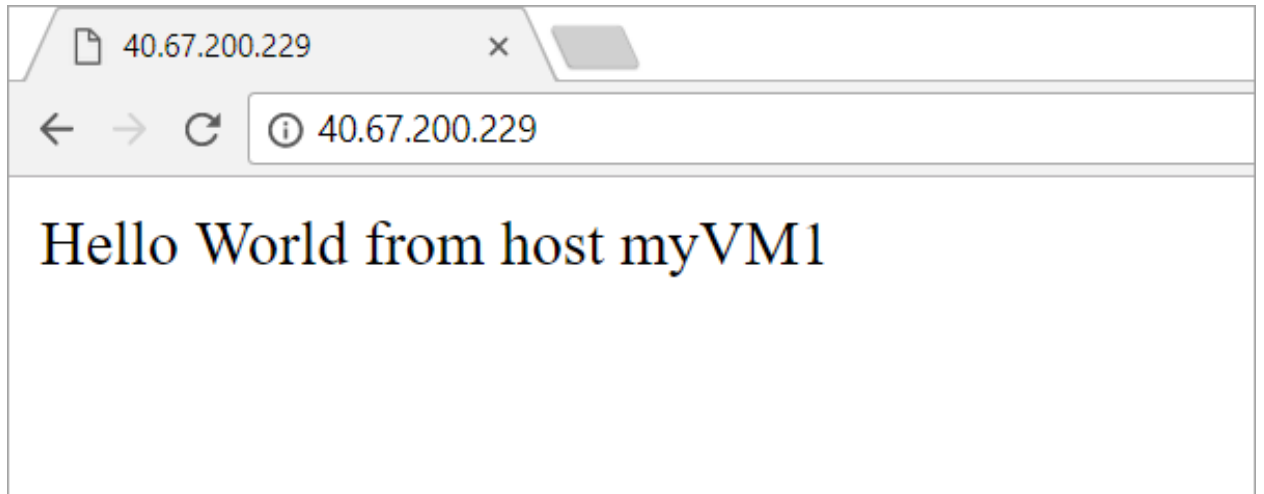
Disabled

Enabled

OK

TEST THE LOAD BALANCER

1. Find the public IP address for the Load Balancer on the **Overview** screen. Click **All resources** and then click **myPublicIP**.
2. Copy the public IP address, and then paste it into the address bar of your browser. The default page of IIS Web server is displayed on the browser.



To see the load balancer distribute traffic across the VMs distributed across the zone you can force-refresh your web browser. If you do not see web traffic disperse between the VMs, simply power off each VM and note the change that happens automatically (without downtime).