

Login with **Username & Password** provided by Great Learning lab  
Select **Create a resource**

The screenshot shows the Microsoft Azure home page. At the top, there's a search bar and a 'Copilot' button. Below the header, there's a section titled 'Azure services' with a 'Create a resource' button highlighted with a red box. To the right of this are icons for Quickstart Center, Azure AI services, Kubernetes services, Virtual machines, App Services, Storage accounts, SQL databases, Azure Cosmos DB, and More services. Below this is a 'Resources' section with tabs for 'Recent' and 'Favorite'. A message says 'No resources have been viewed recently' with a 'View all resources' button. Further down are sections for 'Navigate' (Subscriptions, Resource groups, All resources, Dashboard) and 'Tools' (Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, Cost Management).

Enter **Virtual Networks** in search bar

The screenshot shows the 'Create a resource' page in the Microsoft Azure Marketplace. The search bar at the top contains the text 'virtual network'. Below the search bar, there's a 'Get Started' sidebar and a main search results area. The search results for 'virtual network' are listed, with the first result, 'virtual network', also highlighted with a red box. Other results include 'virtual network gateway' and 'virtual networks'. To the right of the search results, there's a section for 'Popular Marketplace products' featuring various cloud services like Windows Server 2019 Datacenter, Ubuntu Server 20.04 LTS, and MongoDB Atlas.

## Select Create

### Select Virtual Network

Showing 1 to 20 of 1115 results for 'virtual network'. [Clear search](#)

Tile view

Resource group, select **rg\_eastus\_262385\_1\_173980496982**

Enter **whizVNet** in Name

Region: **East US**

Basics Security IP addresses Tags Review + create

Subscription \* PAYG-Labs2  
Resource group \* rg\_eastus\_262385\_1\_173980496982  
Create new

Project details

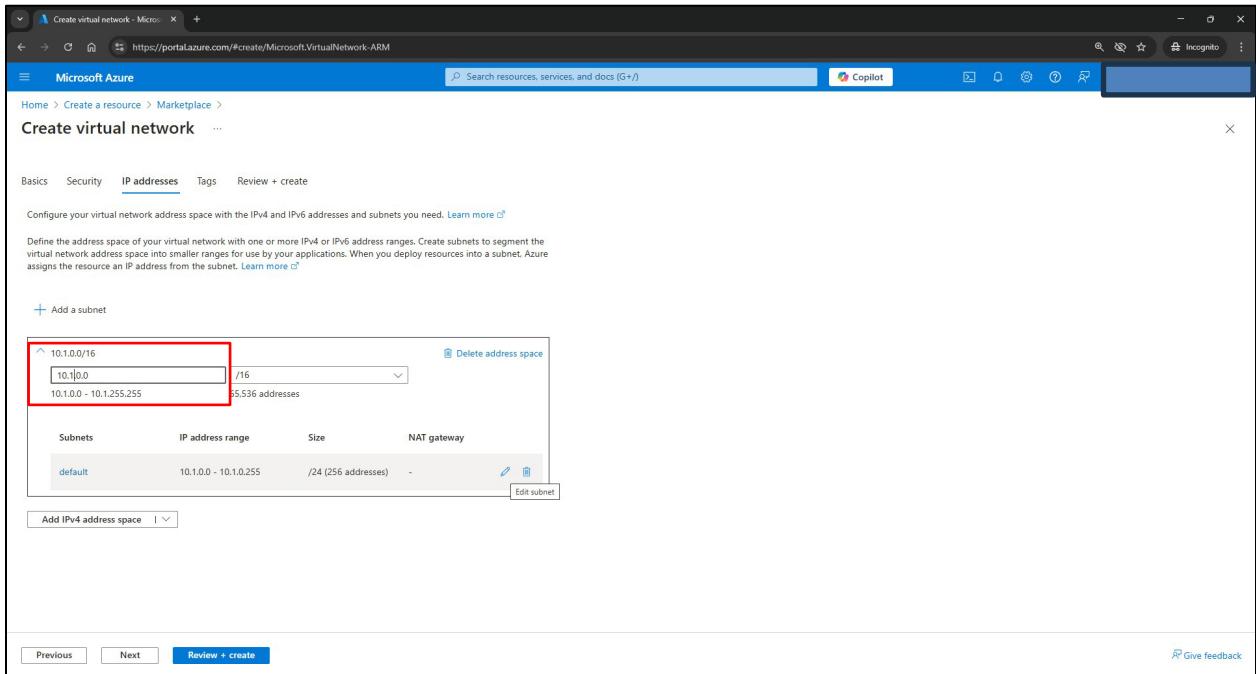
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Virtual network name \* whizVNet

Region \* (US) East US  
Deploy to an Azure Extended Zone

Previous Next Review + create Give feedback

## Enter IP Address of 10.1.0.0



The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The 'IP addresses' tab is selected. In the main area, there's a table for defining subnets. One subnet is listed with the following details:

Subnet	IP address range	Size	NAT gateway
default	10.1.0.0 - 10.1.0.255	/24 (256 addresses)	-

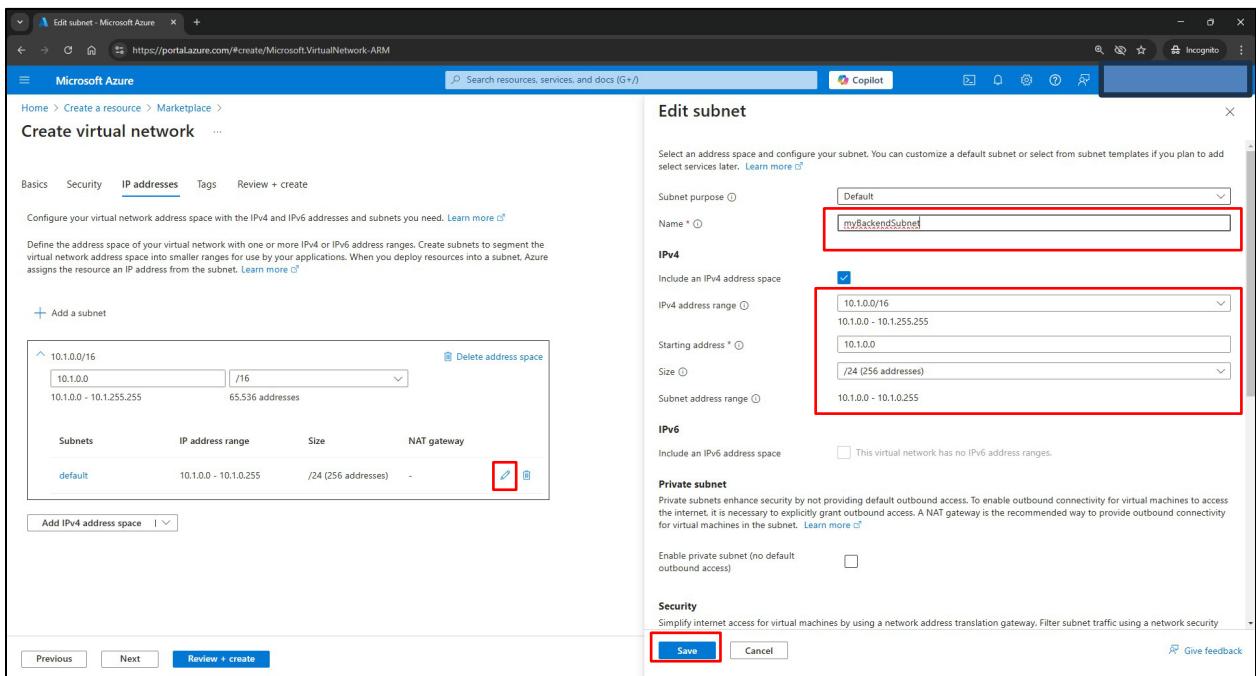
Below the table, there's a button labeled 'Edit subnet'. At the bottom of the page, there are 'Previous', 'Next', and 'Review + create' buttons.

Select Edit

Enter myBackendSubnet

Confirm Subnet address range 10.1.0.0/16, Starting address 10.1.0.0/24

Select Save



The screenshot shows the 'Edit subnet' dialog box. In the 'IPv4' section, the 'Name' field is set to 'myBackendSubnet'. The 'IPv4 address range' is set to '10.1.0.0/16' with 'Starting address' '10.1.0.0' and 'Size' '/24 (256 addresses)'. The 'Save' button at the bottom is highlighted with a red box.

## IP address and Subnet saved

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 a subnet

Subnets	IP address range	Size	NAT gateway
myBackendSubnet	10.1.0.0 - 10.1.0.255	/24 (256 addresses)	-

Add IPv4 address space | ▾

Previous Next Review + create Give feedback

From Security tab, select **Enable Azure Bastion** checkbox

Enter **myBastionIP** under **Azure Bastion host name**

Select **Create a public IP address**

Enhance the security of your virtual network with these additional paid security services. [Learn more](#)

**Virtual network encryption**

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more](#).

Virtual network encryption

**Azure Bastion**

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more](#).

Enable Azure Bastion

Azure Bastion host name myBastionIP

Azure Bastion public IP address \* (New) whiznet-bastion [Create a public IP address](#)

**Azure Firewall**

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. [Learn more](#)

Previous Next Review + create Give feedback

Enter myBastionIP

Select Standard

Select OK

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The current step is 'Add a public IP address'. In the 'Name' input field, the value 'myBastionIP' is entered. The 'SKU' dropdown is set to 'Standard'. The 'OK' button at the bottom of the dialog is highlighted with a red box.

Select Review + Create

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The current step is 'Review + Create'. The 'Review + create' button at the bottom of the page is highlighted with a red box.

## Select Create

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and 'Incognito'. The main page title is 'Create a resource > Marketplace > Create virtual network'. Below the title, there are tabs: 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create'. The 'Review + create' tab is currently active. Under the 'Basics' section, the following details are listed:

- Subscription: PAYG-Labs2
- Resource Group: rg\_eastus\_262385\_1\_17390496982
- Name: whizVNet
- Region: East US

Under the 'Security' section:

- Azure Bastion: Enabled
- Name: (New) myBastionP
- Public IP Address: (New) myBastionIP
- Azure Firewall: Disabled
- Azure DDoS Network Protection: Disabled

Under the 'IP addresses' section:

- Address space: 10.1.0.0/16 (65,536 addresses)
- Subnet: myBackendSubnet (10.1.0.0/24) (256 addresses)
- Subnet: AzureBastionSubnet (10.1.1.0/26) (64 addresses)

Under the 'Tags' section, there are three empty tag fields.

At the bottom of the page, there are 'Previous', 'Next', and 'Create' buttons. The 'Create' button is highlighted with a red box. There is also a 'Give feedback' link at the bottom right.

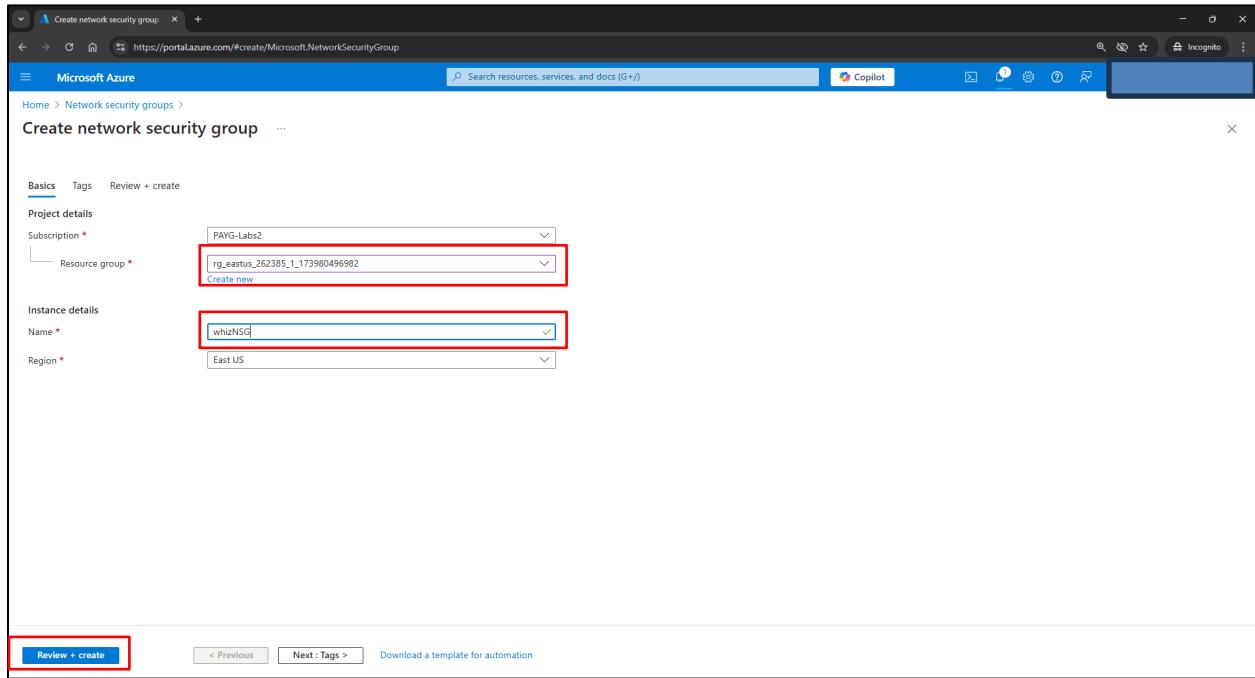
## Navigate to Network Security Groups, select + Create

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and 'Incognito'. The main page title is 'Network security groups'. The 'Network security groups' section is highlighted with a red box. Below it, there are buttons for '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. There are also filter options: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. The results table shows 'Showing 0 to 0 of 0 records'. The columns are: Name ↑, Resource group ↑↓, Location ↑↓, Subscription ↑↓, and Flow log ↑↓. A shield icon is displayed above the table. The message 'No network security groups to display' is shown, along with the text 'Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets.' and a 'Create network security group' button. There is also a 'Learn more' link. At the bottom right, there is a 'Give feedback' link.

Select drop-down for Resource Group rg\_eastus\_262385\_1\_173980496982

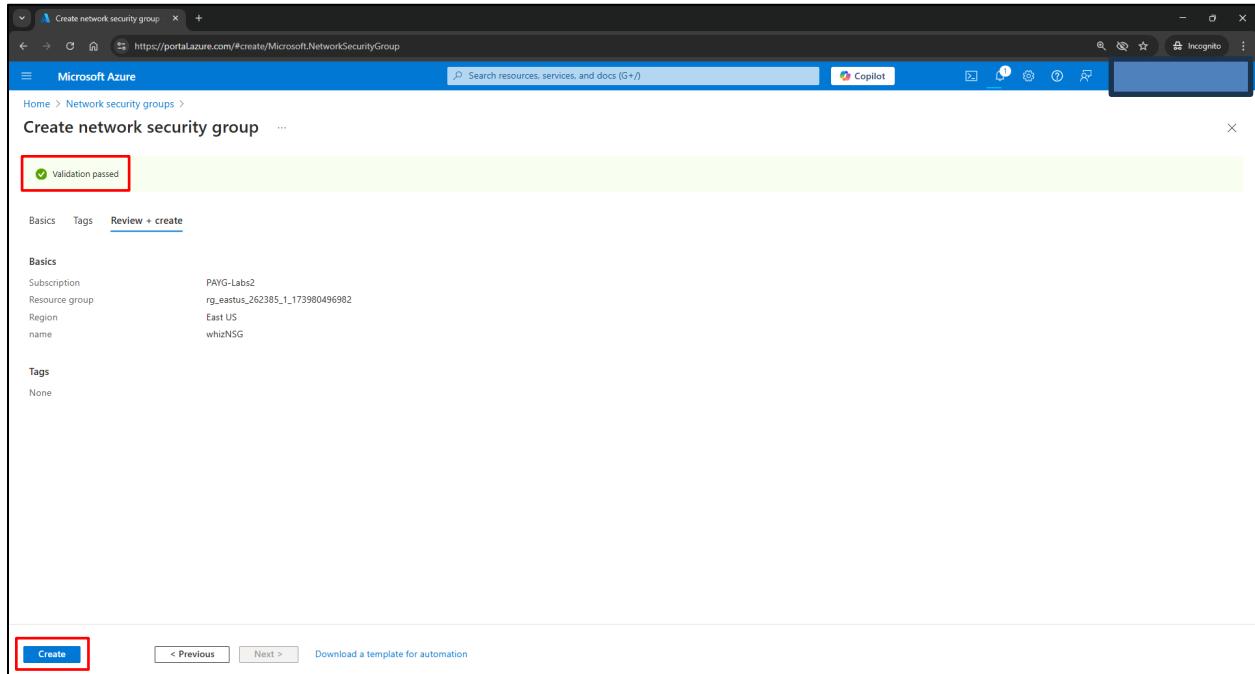
Enter whizNSG in Name

Select Review + Create

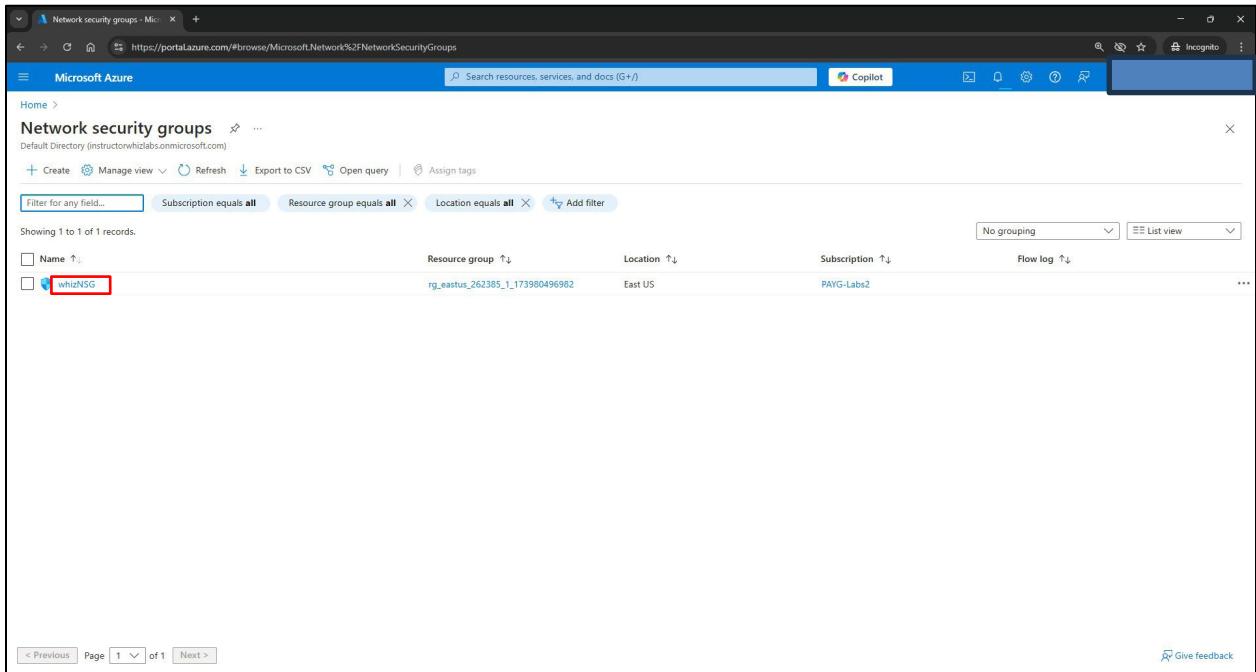


**Validation Passed**

Select Create

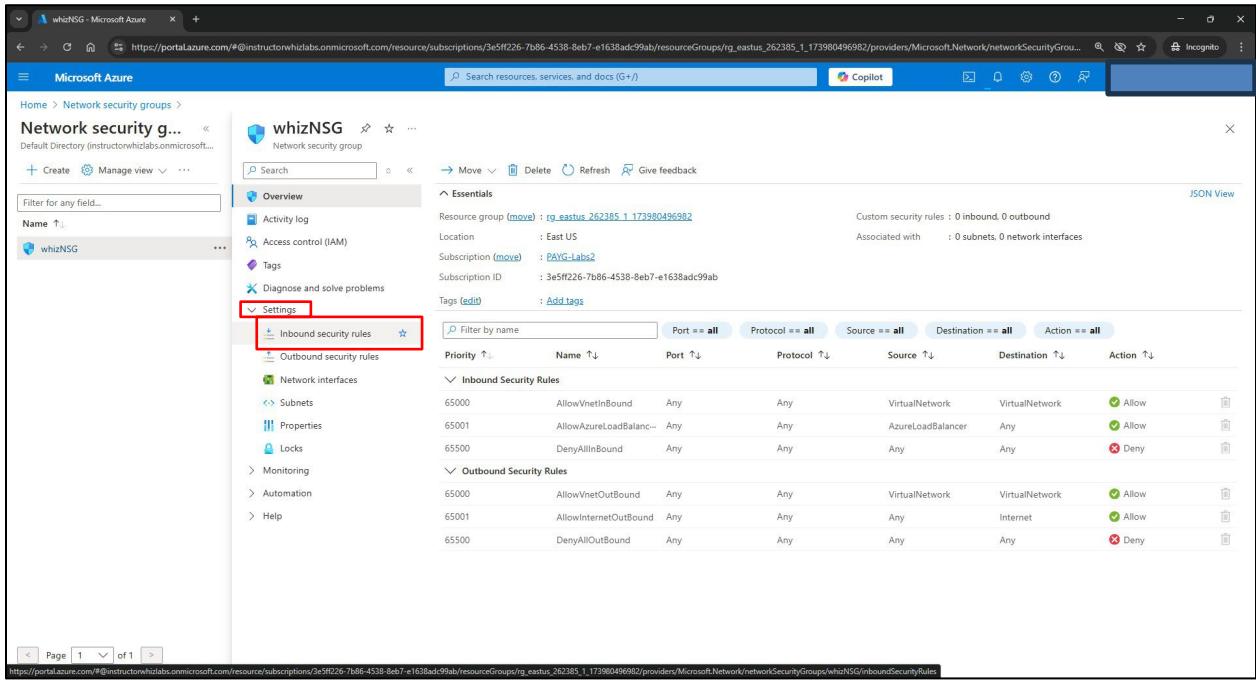


## Select whizNSG



The screenshot shows the Microsoft Azure portal interface. The user is navigating through the 'Network security groups' section. A single item, 'whizNSG', is listed in the table. The 'Name' column shows 'whizNSG'. The 'Resource group' column shows 'rg\_eastus\_262385\_1\_173980496982'. The 'Location' column shows 'East US'. The 'Subscription' column shows 'PAYG-Labs2'. The 'Flow log' column shows 'No grouping'. The 'List view' dropdown is set to 'List view'. At the bottom, there are navigation buttons for 'Page 1 of 1'.

## Select Settings drop down Select Inbound security rules



The screenshot shows the 'Overview' tab for the 'whizNSG' network security group. Under the 'Essentials' section, it shows the resource group, location, subscription, and tags. Below this, the 'Settings' section is expanded, showing the 'Inbound security rules' option, which is highlighted by a red box. The 'Outbound security rules' option is also visible. To the right, a table lists the inbound security rules with columns for Priority, Name, Port, Protocol, Source, Destination, and Action. The first rule is 'AllowVnetInBound' with priority 65000. The second rule is 'AllowAzureLoadBalanc...' with priority 65001. The third rule is 'DenyAllInBound' with priority 65500. The table also includes a header row with filters for Name, Port, Protocol, Source, Destination, and Action.

## Select + Add

The screenshot shows the Microsoft Azure portal interface for managing network security groups. The left sidebar shows the navigation path: Home > Network security groups > whizNSG. The main content area is titled "whizNSG | Inbound security rules". A red box highlights the "+ Add" button at the top center of the rule list. Below the table, there is a pagination control showing "Page 1 of 1".

**Inbound security rules**

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

< Page 1 > of 1 https://go.microsoft.com/fwlink/?linkid=2174617

- Source: Leave the default of **Any**.
- Source port ranges: Leave the default of **\***.
- Destination: Leave the default of **Any**.
- Service: Leave the default of **Custom**.
- Destination port ranges: Enter **\***.
- Protocol: Select **Any**.
- Action: Leave the default of **Allow**.
- Priority: Enter **100**.
- Name: Enter **whizNSGRule-AllowAll-All**

### Select Add

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). On the left, the 'Inbound security rules' list for the 'whizNSG' NSG is displayed, showing three existing rules: 'AllowVnetInBound', 'AllowAzureLoadBalanc...', and 'DenyAllInBound'. On the right, a modal dialog titled 'Add inbound security rule' is open, allowing the creation of a new rule. The 'Name' field is populated with 'whizNSGRule-AllowAll-All'. The 'Source' and 'Destination' dropdowns are set to 'Any'. The 'Protocol' dropdown is set to 'Custom'. The 'Action' dropdown is set to 'Allow'. The 'Priority' input field is set to '100'. The 'Add' button at the bottom left of the dialog is highlighted with a red border.

## Inbound security rule created

The screenshot shows the Microsoft Azure portal interface for managing network security groups. The left sidebar shows the navigation path: Home > Network security groups > whizNSG. The main content area is titled "whizNSG | Inbound security rules". It displays a table of security rules with columns for Priority, Name, Port, Protocol, Source, Destination, and Action. A new rule has been added with a priority of 100, named "whizNSGRule-AllowInBound", which allows traffic from any source port to any destination port. This row is highlighted with a red box. Other default rules are listed below it.

Priority ↑	Name ↑	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	whizNSGRule-AllowInBound	Any	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

## Under Settings, select Outbound security rules

Select + Add

The screenshot shows the Microsoft Azure portal interface for managing network security groups. The left sidebar shows the navigation path: Home > Network security groups > whizNSG. The main content area is titled "whizNSG | Outbound security rules". It displays a table of security rules with columns for Priority, Name, Port, Protocol, Source, Destination, and Action. A new rule has been added with a priority of 65500, named "DenyAllOutBound", which denies all outbound traffic. This row is highlighted with a red box. Other default rules are listed below it.

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

- Source: Leave the default of **Any**.
- Source port ranges: Leave the default of **\***.
- Destination: Leave the default of **Any**.
- Service: Leave the default of **Custom**.
- Destination port ranges: Enter **\***.
- Protocol: Select **TCP**.
- Action: Leave the default of **Allow**.
- Priority: Enter **100**.
- Name: Enter **whizNSGRule-AllowAll-TCP-Out**

### Select Add

The screenshot shows the Microsoft Azure portal interface for creating an outbound security rule. The left sidebar shows the navigation path: Home > Network security groups > whizNSG. The main area displays the 'Outbound security rules' section, listing three existing rules: 'AllowVnetOutBound', 'AllowInternetOutBound', and 'DenyAllOutBound'. A red box highlights the configuration fields for the new rule being added:

- Source:** Any
- Source port ranges:** \*
- Destination:** Any
- Service:** Custom
- Destination port ranges:** \*
- Protocol:** TCP (selected)
- Action:** Allow (selected)
- Priority:** 100
- Name:** whizNSGRule-AllowAll-TCP-Out

The 'Add' button at the bottom of the dialog is highlighted with a red box.

## Outbound security rule added

The screenshot shows the Microsoft Azure portal interface for managing network security groups. The left sidebar shows the navigation path: Home > Network security groups > whizNSG. The main content area is titled "whizNSG | Outbound security rules". It displays a table of security rules:

Priority	Name	Port	Protocol	Source	Destination	Action
100	whizNSGRule-AllowAll... Any	Any	TCP	Any	Any	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

A red box highlights the first rule, "whizNSGRule-AllowAll... Any".

## Navigate to Load balancer

### Select Create

The screenshot shows the Microsoft Azure portal interface for managing load balancers. The left sidebar shows the navigation path: Home > Load balancing. The main content area is titled "Load balancing | Load Balancer". A red box highlights the "+ Create" button.

The page displays a table with columns: Name, SKU, Resource group, Location, and Subscription. A large diamond icon is centered on the page, and the text "No load balancers to display" is shown below it.

A note at the bottom states: "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."

Select Resource group drop down, select **rg\_eastus\_262385\_1\_173980496982**

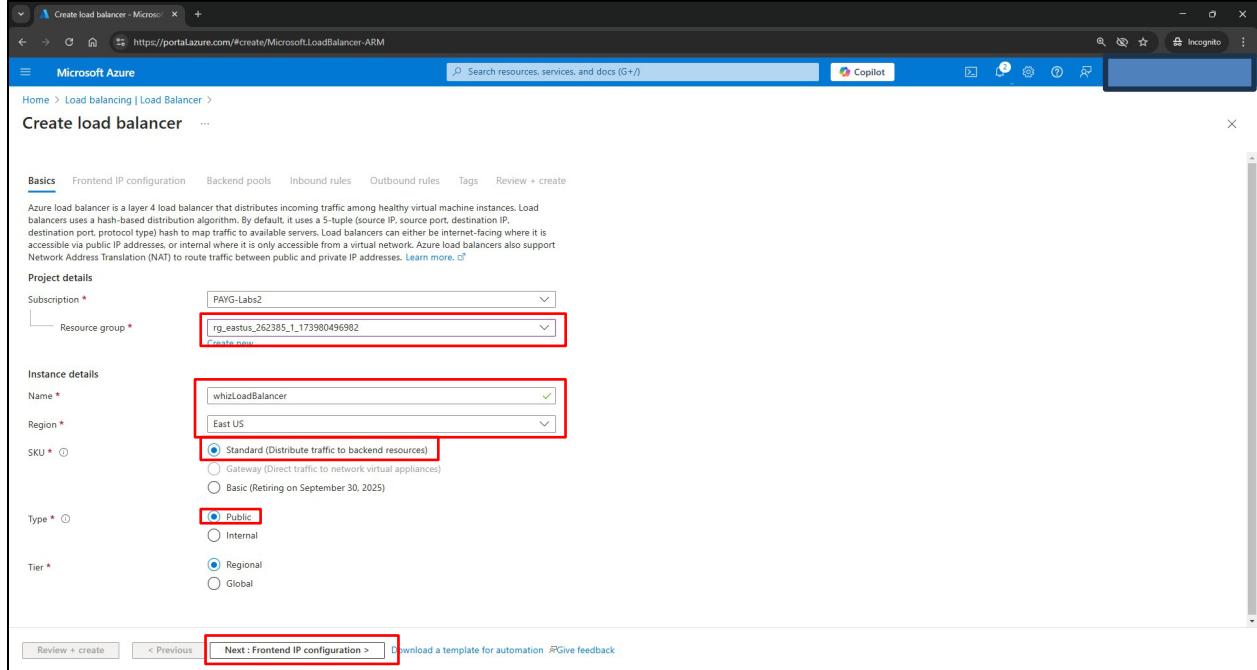
Enter name **whizLoadBalancer**

Region: **East US**

Select **Standard**

Select **Public**

Select **Next: Frontend IP configuration**



Enter **myFrontEndIP** under Name

IP version: **IPv4**

IP type: **IP address**

Select **Create new** under Public IP address

The screenshot shows the 'Add frontend IP configuration' dialog in the Azure portal. The 'Name' field is filled with 'myFrontEndIP'. Under 'IP version', 'IPv4' is selected. Under 'IP type', 'IP address' is selected. In the 'Public IP address' dropdown, 'Create new' is selected, which is highlighted with a red box. The 'Save' button at the bottom is also highlighted with a red box.

Under Add a public IP address, enter **loadbalancerip** under Name

Select **Save**

The screenshot shows the 'Add a public IP address' dialog in the Azure portal. The 'Name' field is filled with 'loadbalancerip'. Under 'SKU', 'Standard' is selected. Under 'Tier', 'Regional' is selected. The 'Save' button at the bottom is highlighted with a red box.

Gateway Load balancer: **None**

Select **Save**

The screenshot shows the 'Add frontend IP configuration' dialog in the Microsoft Azure portal. The 'Name' field is set to 'myFrontEndip'. The 'IP version' is set to 'IPv4'. The 'IP type' is set to 'IP address'. The 'Public IP address' dropdown is set to '(new) loadbalancerip'. The 'Gateway Load balancer' dropdown is set to 'None' and is highlighted with a red box. The 'Save' button at the bottom right is also highlighted with a red box.

Frontend IP configuration created

Select **Review + Create**

The screenshot shows the 'Create load balancer' dialog in the Microsoft Azure portal. The 'Name' field is set to 'myFrontEndip'. The 'IP address' dropdown is set to '(new) loadbalancerip (To be created)' and is highlighted with a red box. The 'Review + create' button at the bottom left is highlighted with a red box.

## Validation Passed

### Select Create

The screenshot shows the 'Create load balancer' wizard in the Microsoft Azure portal. A red box highlights the 'Validation passed' message at the top. Another red box highlights the 'Create' button at the bottom.

**Validation passed**

**Create**

### From Load Balancer page, select + Create

The screenshot shows the 'Load balancing | Load Balancer' list page in the Microsoft Azure portal. A red box highlights the '+ Create' button at the top left of the search bar.

**+ Create**

Enter Resource group **rg\_eastus\_262385\_1\_173980496982**

Name: **whizLoadBalancer-gw**

SKU: **Gateway**

Type: **Internal**

Select **Next: Frontend IP configuration**

Project details

- Subscription: PAYG-Labs2
- Resource group: rg\_eastus\_262385\_1\_173980496982
- Name: whizLoadBalancer-gw
- Region: East US
- SKU: Gateway
- Type: Internal
- Tier: Regional

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

Next : Frontend IP configuration >

Select + Add a frontend IP configuration

+ Add a frontend IP configuration

Name	IP address	Virtual network	Subnet
Add a frontend IP to get started			

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

Next : Backend pools >

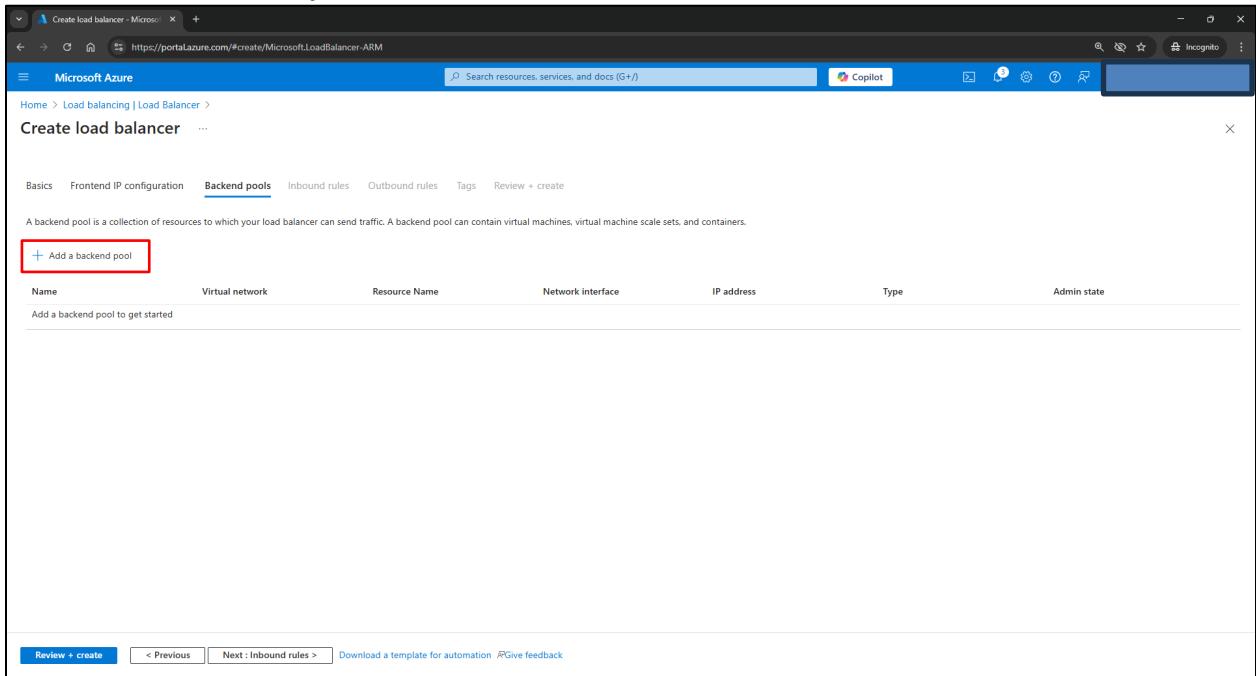
Name: **whizFrontEnd**  
Subnet, select **myBackendSubnet**  
Select **Save**

The screenshot shows the 'Add frontend IP configuration' dialog in the Azure portal. The 'Name' field is set to 'whizFrontEnd'. The 'Virtual network' is 'whizVNet' and the 'Subnet' is 'myBackendSubnet (10.1.0.0/24)'. The 'Save' button is highlighted with a red box.

Select Next: Backend pools

The screenshot shows the 'Create load balancer' wizard at the 'Frontend IP configuration' step. The 'Name' is 'whizFrontEnd', 'IP address' is 'Dynamic', 'Virtual network' is 'whizVNet', and 'Subnet' is 'myBackendSubnet'. The 'Next : Backend pools >' button is highlighted with a red box.

## Select + Add a backend pool



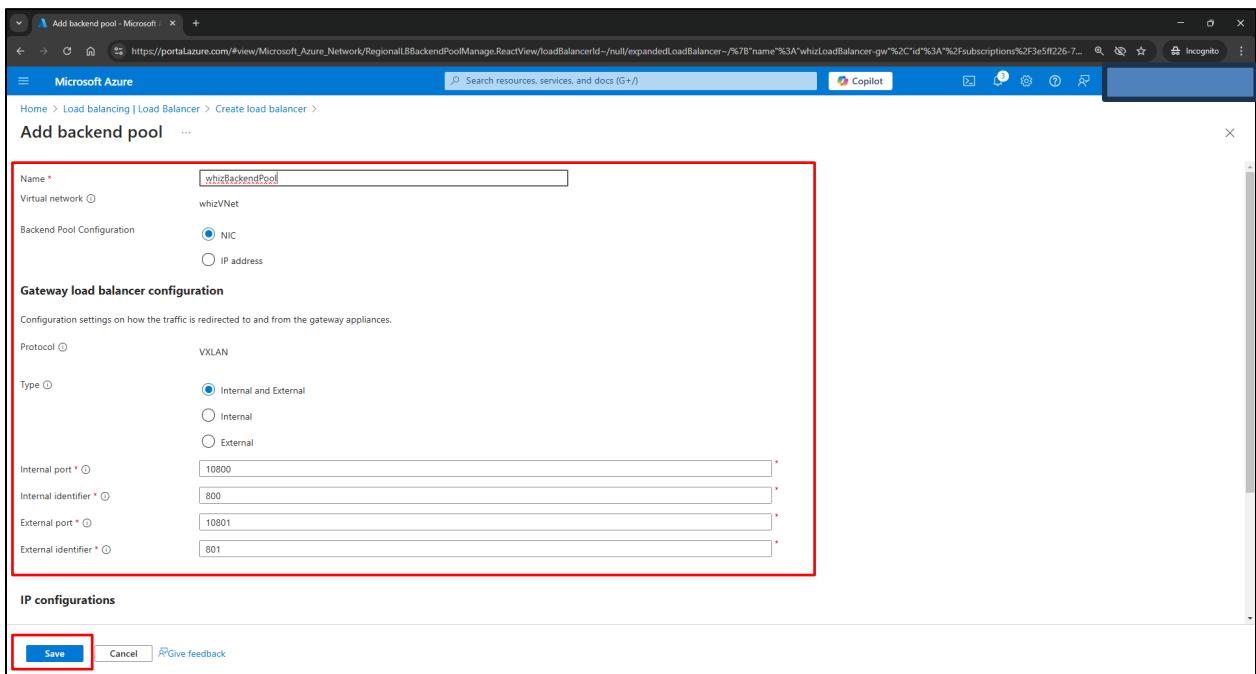
The screenshot shows the Microsoft Azure portal interface for creating a load balancer. The current step is 'Backend pools'. A red box highlights the '+ Add a backend pool' button. Below it, there's a table with columns: Name, Virtual network, Resource Name, Network interface, IP address, Type, and Admin state. A note says 'Add a backend pool to get started'. At the bottom, there are 'Review + create' and 'Next : Inbound rules >' buttons.

Enter **whizBackendPool**

Under **Gateway load balancer configuration**

- Type: Select **Internal and External**
- Internal port: Leave the default of **10800**
- Internal identifier: Leave the default of **800**
- External port: Leave the default of **10801**
- External identifier: Leave the default of **801**

Select **Save**



The screenshot shows the 'Add backend pool' configuration page. A large red box highlights the 'Gateway load balancer configuration' section, which includes fields for Protocol (VLAN), Type (Internal and External selected), and port/identifier settings (Internal port: 10800, Internal identifier: 800, External port: 10801, External identifier: 801). Another red box highlights the 'Save' button at the bottom left.

## Backend pool created Select Next: Inbound rules

The screenshot shows the Microsoft Azure portal interface for creating a load balancer. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and 'Incognito'. The main title is 'Create load balancer'. Below it, the breadcrumb navigation shows 'Home > Load balancing | Load Balancer > Create load balancer'. The current step is 'Backend pools', indicated by a blue underline. Other tabs include 'Basics', 'Frontend IP configuration', 'Inbound rules', 'Outbound rules', 'Tags', and 'Review + create'. A sub-section titled '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.' is displayed. A table lists existing backend pools: 'whizBackendPool' (selected, highlighted in blue). The table columns are 'Name', 'Virtual network', 'Resource Name', 'Network interface', 'IP address', 'Type', and 'Admin state'. The 'Type' column for 'whizBackendPool' shows 'Internal and External'. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Inbound rules >', 'Download a template for automation', and 'Give feedback'.

## Select + Add a load balancing rule

The screenshot shows the Microsoft Azure portal interface for creating a load balancer. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and 'Incognito'. The main title is 'Create load balancer'. Below it, the breadcrumb navigation shows 'Home > Load balancing | Load Balancer > Create load balancer'. The current step is 'Inbound rules', indicated by a blue underline. Other tabs include 'Basics', 'Frontend IP configuration', 'Backend pools', 'Outbound rules', 'Tags', and 'Review + create'. A sub-section titled 'Load balancing rule' is displayed, stating that it distributes incoming traffic to a selected IP address and port combination across a group of backend pool instances. A table lists existing load balancing rules: '+ Add a load balancing rule' (highlighted with a red box). The table columns are 'Name ↑↓', 'Frontend IP configuration ↑↓', 'Backend pool ↑↓', 'Health probe ↑↓', 'Frontend Port ↑↓', and 'Backend port ↑↓'. Below the table, there is a section for 'Inbound NAT rule', with a note that it forwards incoming traffic to a specific virtual machine. A button '+ Add an inbound nat rule' is shown. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Outbound rule >', 'Download a template for automation', and 'Give feedback'.

Under **Add load balancing rule**, enter:

- Name: Enter **whizLBRule**
- IP Version: Select **IPv4 or IPv6** depending on your requirements.
- Frontend IP address: Select **whizFrontEnd**
- Backend pool: Select **whizBackendPool**
- Health probe: Select **Create new**

**Add load balancing rule**

whizLoadBalancer-gw  
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 health of the backend instances. Only backend instances that the health probe considers healthy receive new traffic. [Learn more.](#)

**Name \*** whizLBRule

**IP version \***  IPv4  IPv6

**Frontend IP address \*** whizFrontEnd (Dynamic)

**Backend pool \*** whizBackendPool

**High availability ports** Enabled

**Health probe \*** (new) whizHealthProbe (TCP:80) [Create new](#)

**Session persistence** None

**Idle timeout (minutes)** 4

**Enable TCP Reset**

**Enable Floating IP**

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

- Name: enter **whizHealthProbe**
- Select **TCP** in Protocol.
- Leave the rest of the defaults, and select **Save**.

**Add load balancing rule**

whizLoadBalancer-gw  
Health probes are used to check the status of a backend pool instance. If the health probe fails to get a response from a backend instance then no new connections will be sent to that backend instance until the health probe succeeds again.

**Name \*** whizHealthProbe

**Protocol \*** TCP

**Port \*** 80

**Interval (seconds) \*** 5

**Used by** Not used [Save](#) [Cancel](#)

**Session persistence** None

**Idle timeout (minutes)** 4

**Enable TCP Reset**

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

## Session persistence: Select **None**

Select **Save**

The screenshot shows the 'Add load balancing rule' page in the Microsoft Azure portal. The 'Inbound rules' tab is selected. On the right, under 'Session persistence', the dropdown menu is open with 'None' selected. A tooltip explains that session persistence is disabled. The 'Save' button at the bottom right is highlighted with a red box.

## Select **Review + Create**

The screenshot shows the 'Create load balancer' review step. The 'Review + create' button at the bottom left is highlighted with a red box. Other buttons like 'Previous' and 'Next' are also visible.

## Validation passed

### Select Create

Validation passed

Create load balancer

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

**Basics**

Subscription	PAYG-Labs2
Resource group	rg_eastus_262385_1_173980496982
Name	whizLoadBalancer-gw
Region	East US
SKU	Gateway
Tier	Regional
Type	Internal

**Frontend IP configuration**

Frontend IP configuration name	whizFrontEnd
Frontend IP configuration IP address	Dynamic

**Backend pools**

Backend pool name	whizBackendPool
Internal port	10800
Internal identifier	800
External port	10801
External identifier	801

**Inbound rules**

**Create**

< Previous Next > Download a template for automation Give feedback

## Navigate to Virtual Machines

### Select + Create

Virtual machines

+ Create

No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

+ Create

Learn more about Windows virtual machines

Learn more about Linux virtual machines

Give feedback

Virtual machine name: **whizNVA**

Region: **East US**

Security type: **Standard**

Image: **Windows Server 2019 Datacenter – x64 Gen 2**

Scroll down

The screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. The 'Instance details' section is highlighted with a red box. It includes fields for Virtual machine name (whizNVA), Region (US East US), Availability options (Availability zone), Zone options (Self-selected zone), Security type (Standard), and Image (Windows Server 2019 Datacenter - x64 Gen 2). Below the security type, there is a note about Trusted launch.

**Instance details**

- Virtual machine name \* whizNVA
- Region \* (US) East US
- Availability options (Availability zone)
- Zone options (Self-selected zone)
  - Choose up to 3 availability zones, one VM per zone
  - Azure-selected zone (Preview)
    - Let Azure assign the best zone for your needs
- Using an Azure-selected zone is not supported in region 'East US.'
- Availability zone \* Zone 1
- You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)
- Security type \* Standard
- Trusted launch virtual machine is required when using IP Gallery images.
- Image \* Windows Server 2019 Datacenter - x64 Gen 2

This image is compatible with additional security features. [Click here to swap to the Trusted launch security type.](#)

< Previous Next : Disks > Review + create Give feedback

Size: **Standard\_B2**

Username: **localadmin**

Password: **Password12345**

Select Disks

The screenshot shows the 'Create a virtual machine' wizard on the Microsoft Azure portal. The 'Administrator account' section is highlighted with a red box. It includes fields for Username (localadmin), Password, and Confirm password. Below the account section, there are sections for Inbound port rules and Public inbound ports.

**Administrator account**

- Username \* localadmin
- Password \*
- Confirm password \*

**Inbound port rules**  
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

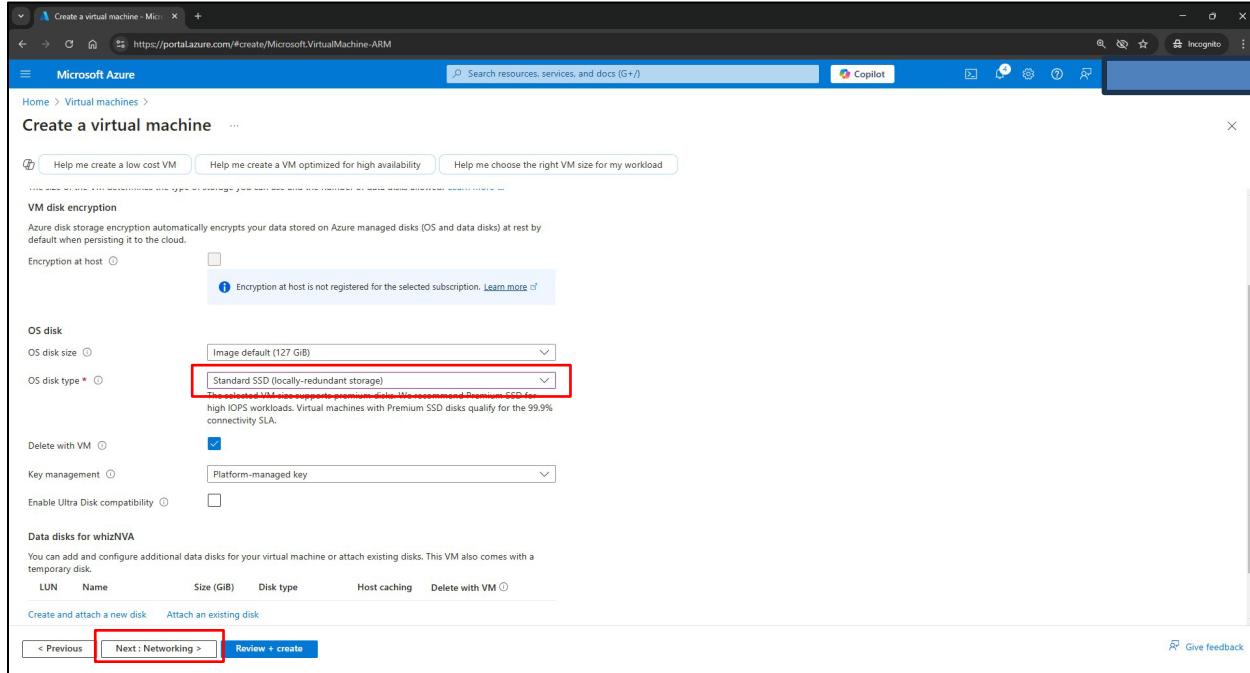
Public inbound ports \*  None  Allow selected ports

Select inbound ports \* RDP (3389)

< Previous Next : Disks > Review + create Give feedback

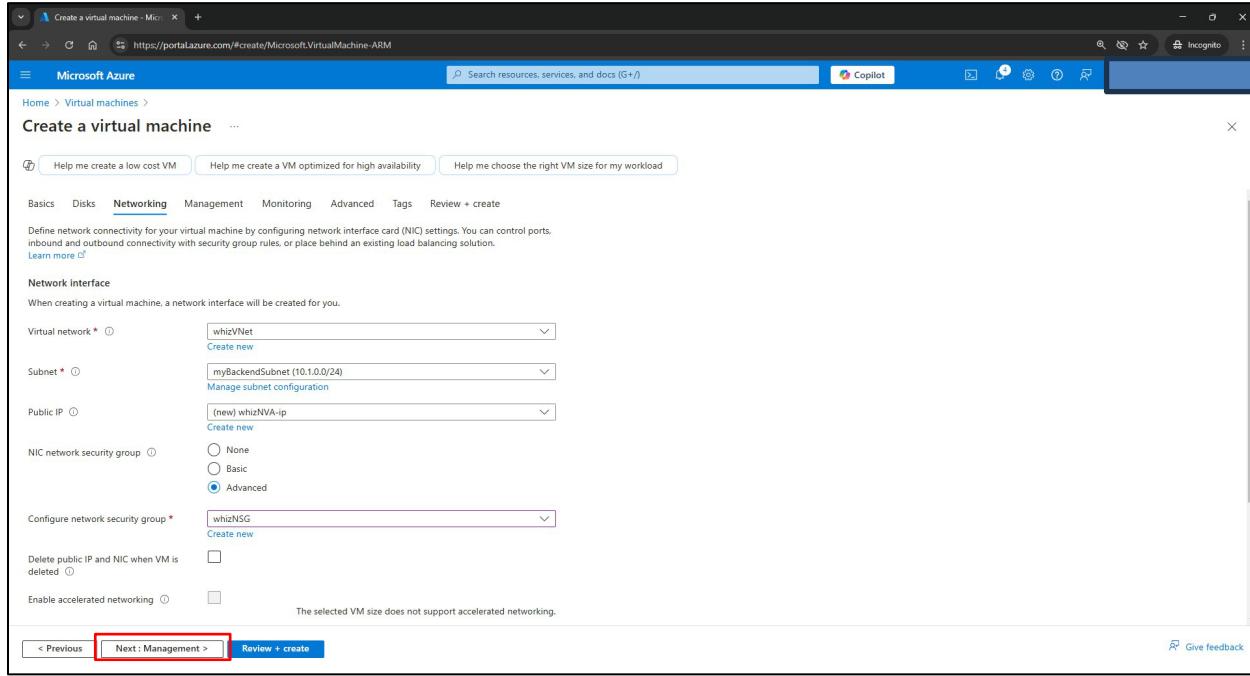
## OS disk type: Standard SSD

### Select Networking



The screenshot shows the Azure portal interface for creating a virtual machine. The page title is "Create a virtual machine". The "Networking" tab is selected. In the "OS disk" section, the "OS disk type" dropdown is highlighted with a red box, showing "Standard SSD (locally-redundant storage)" selected. Below the dropdown, there is a note: "The selected VM disk type supports FIPS, WORM, and Premium FDD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA." At the bottom of the screen, there are navigation buttons: "< Previous", "Next: Networking >" (which is highlighted with a red box), and "Review + create".

### Select Next: Management



The screenshot shows the Azure portal interface for creating a virtual machine. The "Management" tab is selected. In the "Network interface" section, the "Virtual network" dropdown is highlighted with a red box, showing "whizVNet" selected. Other network settings include "Subnet" set to "myBackendSubnet (10.1.0.0/24)", "Public IP" set to "(new) whizNVA-ip", and "NIC network security group" set to "whizNSG". At the bottom of the screen, there are navigation buttons: "< Previous", "Next: Management >" (which is highlighted with a red box), and "Review + create".

## Diagnostics, Boot Diagnostics, select **Disable** Select **Review + Create**

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The current step is 'Monitoring'. In the 'Diagnostics' section, there is a dropdown for 'Boot diagnostics' with three options: 'Enable with managed storage account (recommended)', 'Enable with custom storage account', and 'Disable'. The 'Disable' option is selected and highlighted with a red box. At the bottom of the page, the 'Review + create' button is also highlighted with a red box.

## Validation Passed

### Select **Create**

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The current step is 'Review + create'. A green bar at the top indicates 'Validation passed'. At the bottom of the page, the 'Create' button is highlighted with a red box.

From Load Balancer page, select **whizLoadBalancer-gw**

The screenshot shows the Microsoft Azure portal interface for the Load Balancer service. The left sidebar navigation includes Home, Load balancing, Overview, Load Balancing Services (Application Gateway, Front Door and CDN profiles, Load Balancer), and Traffic Manager. The main content area displays a table of load balancers. A red box highlights the entry for 'whizLoadBalancer-gw'. The table columns are Name, SKU, Resource group, Location, and Subscription. The 'whizLoadBalancer-gw' row shows Standard SKU, rg\_eastus\_262385\_1\_173980496982 resource group, East US location, and PAYG-Labs2 subscription.

Select **Settings** drop down

Select **Backend pools**

The screenshot shows the 'whizLoadBalancer-gw' Load Balancer settings page. The left sidebar shows Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (highlighted with a red box), Frontend IP configuration, and Backend pools (highlighted with a red box). The main content area includes sections for Essentials (Resource group, Location, Subscription, SKU, and Tags), Configure high availability and scalability for your applications (Balance IPv4 and IPv6 addresses, Build highly reliable applications), and links for View frontend IP configuration, View health probes, and View load balancing rules.

## Select Backend pool whizBackendPool(1)

The screenshot shows the Microsoft Azure portal interface for managing a load balancer. On the left, the navigation pane is visible with options like Overview, Load Balancing Services, Application Gateway, Front Door and CDN profiles, Load Balancer, and Traffic Manager. The main content area is titled "whizLoadBalancer-gw | Backend pools". It displays a table of backend pools, with one entry highlighted: "whizBackendPool(1)". A red box surrounds this entry. The table columns include Backend pool, Resource Name, IP address, Network inter..., Type, Rules count, Resource Sta..., and Admin sta... . Below the table, there are sections for Health probes, Load balancing rules, Properties, Locks, Monitoring, Automation, and Help.

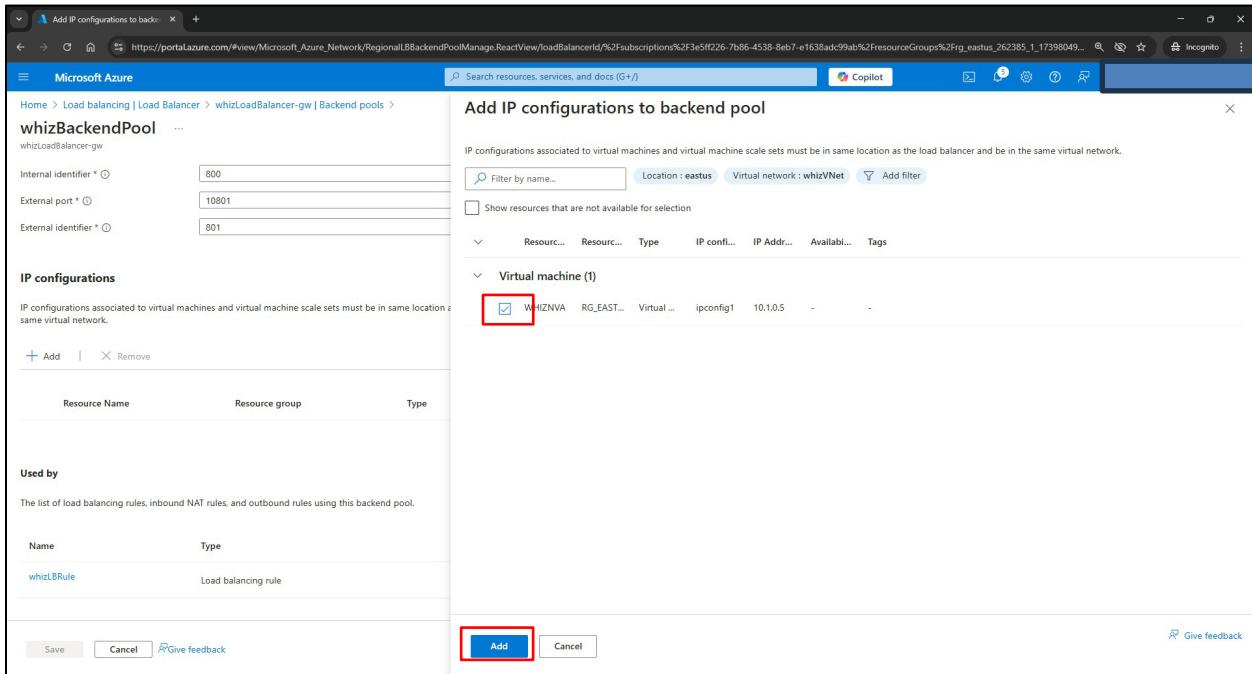
Scroll down

Under IP configuration, select + Add

The screenshot shows the Microsoft Azure portal interface for managing a specific backend pool named "whizBackendPool". The page title is "whizBackendPool - Microsoft Azure". The "IP configurations" section is visible, featuring fields for Internal identifier (set to 800), External port (set to 10801), and External identifier (set to 801). A red box highlights the "+ Add" button. Below this, a table lists IP configurations with columns: Resource Name, Resource group, Type, IP configuration, IP Address, and Availability set. The table currently has one row: "whizLBRule" under "Type". The "Used by" section shows a list of load balancing rules, including "whizLBRule". At the bottom of the page are "Save", "Cancel", and "Give feedback" buttons.

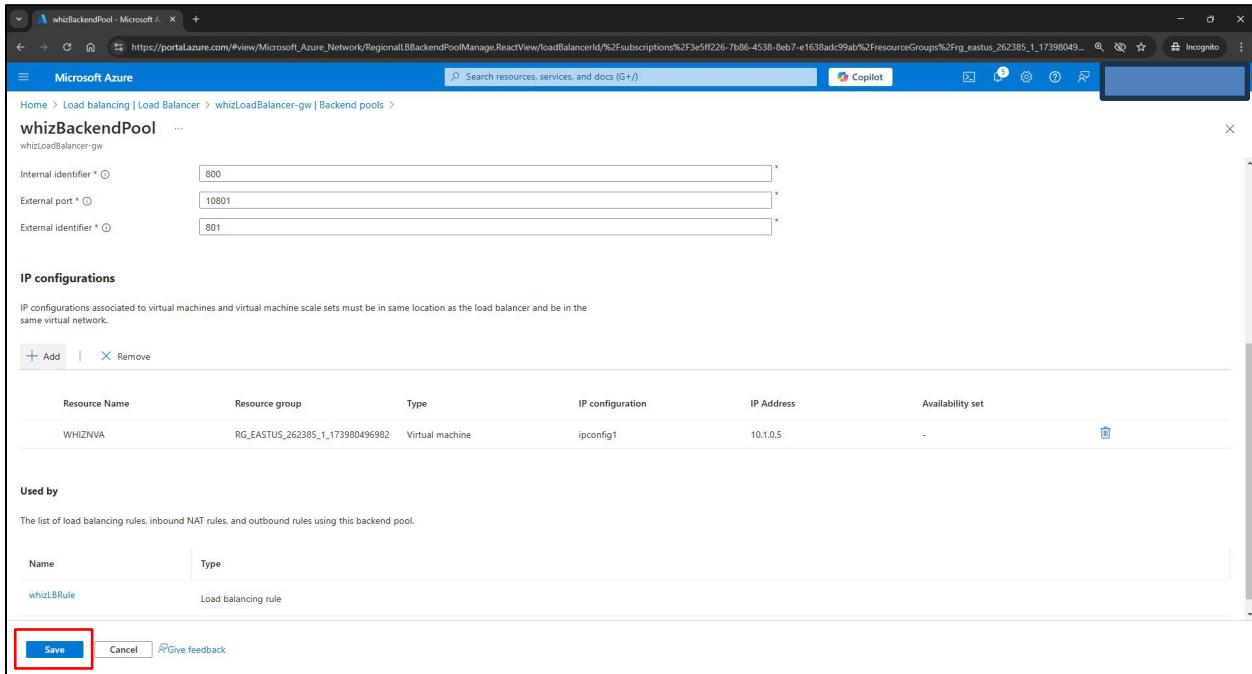
Select checkbox next to WHIZNVA

Select Add



The screenshot shows the 'Add IP configurations to backend pool' dialog in the Azure portal. On the left, there are fields for Internal identifier (800), External port (10801), and External identifier (801). The 'IP configurations' section lists a single item: 'WHIZNVA' (Type: Virtual machine, IP configuration: ipconfig1, IP Address: 10.1.0.5). The 'Used by' section shows a load balancing rule named 'whizLBRule'. At the bottom, there are 'Save', 'Cancel', and 'Give feedback' buttons, with the 'Add' button highlighted with a red box.

Select Save



The screenshot shows the 'whizBackendPool' configuration page in the Azure portal. It displays the same settings as the previous dialog: Internal identifier (800), External port (10801), and External identifier (801). The 'IP configurations' section now shows the added entry for 'WHIZNVA'. The 'Used by' section remains the same. At the bottom, the 'Save' button is highlighted with a red box.

## Added to the whizBackendPool

The screenshot shows the Microsoft Azure portal interface for managing load balancers. The left sidebar navigation includes Home, Load balancing, Load Balancer, Application Gateway, Front Door and CDN profiles, Load Balancer (selected), and Traffic Manager. The main content area is titled "whizLoadBalancer-gw | Backend pools". It displays a table of backend pools:

Backend pool	Resource Name	IP address	Network interface	Type	Rules count	Resource Status	Admin status
whizBackendPool (1)	whizNVA	10.1.0.5	whiznva428_z1	Internal and External	1	Running	None

A red box highlights the first row of the table.

## Select whizLoadBalancer

The screenshot shows the Microsoft Azure portal interface for managing load balancers. The left sidebar navigation includes Home, Load balancing (selected), Application Gateway, Front Door and CDN profiles, Load Balancer (selected), and Traffic Manager. The main content area is titled "Load balancing | Load Balancer". It displays a table of load balancers:

Name	SKU	Resource group	Location	Subscription
whizLoadBalancer	Standard	rg_eastus_262385_1_173980496982	East US	PAYG-Labs2
whizLoadBalancer-gw	Gateway	rg_eastus_262385_1_173980496982	East US	PAYG-Labs2

A red box highlights the "whizLoadBalancer" row.

## Under Settings, select Frontend IP configuration

The screenshot shows the Microsoft Azure portal interface for managing a load balancer. The left sidebar navigation shows 'Load balancing | Load Balancer'. The main content area is titled 'whizLoadBalancer' and displays its 'Overview' settings. A red box highlights the 'Frontend IP configuration' link under the 'Settings' section. The right side of the screen contains promotional banners for high availability and scalability, and a 'View frontend IP configuration' button.

## Select myFrontEndip

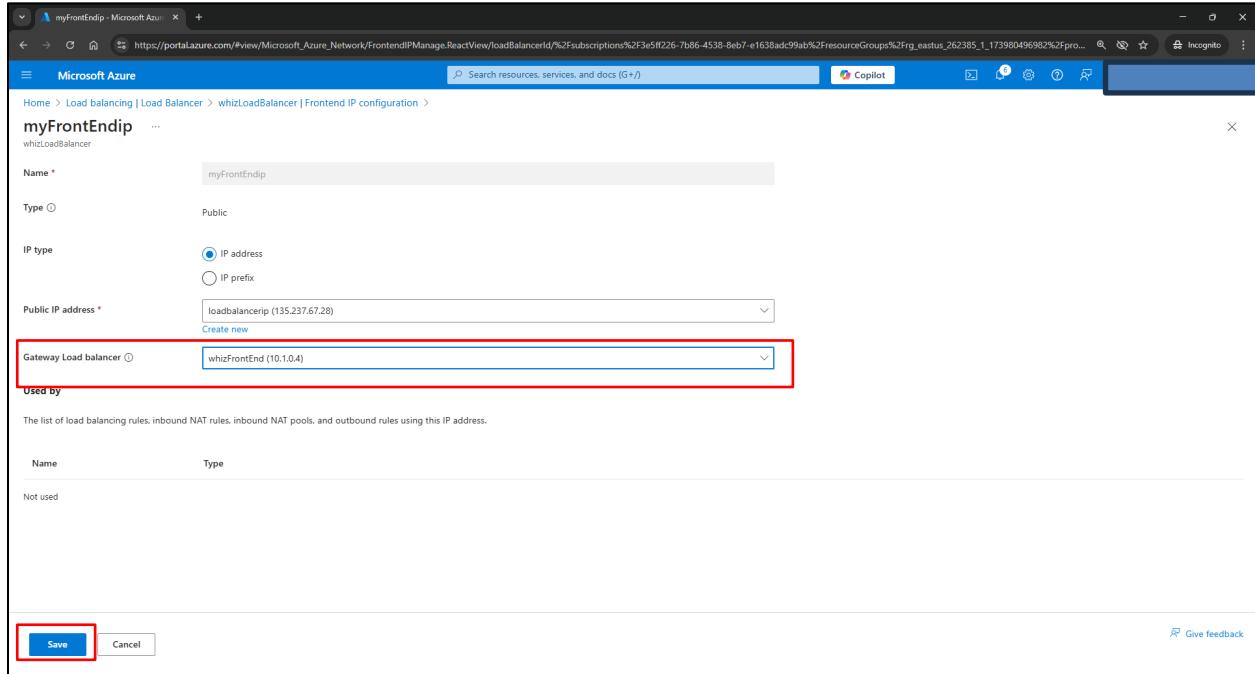
This screenshot continues from the previous one, showing the 'Frontend IP configuration' page for the 'whizLoadBalancer'. The 'myFrontEndip' entry is highlighted with a red box. The table lists the frontend IP configuration details: Name (myFrontEndip), IP address (135.237.67.28 (loadbalancerip)), and Rules count (0).

Name	IP address	Rules count
myFrontEndip	135.237.67.28 (loadbalancerip)	0

Select drop down next to **Gateway Load balancer**

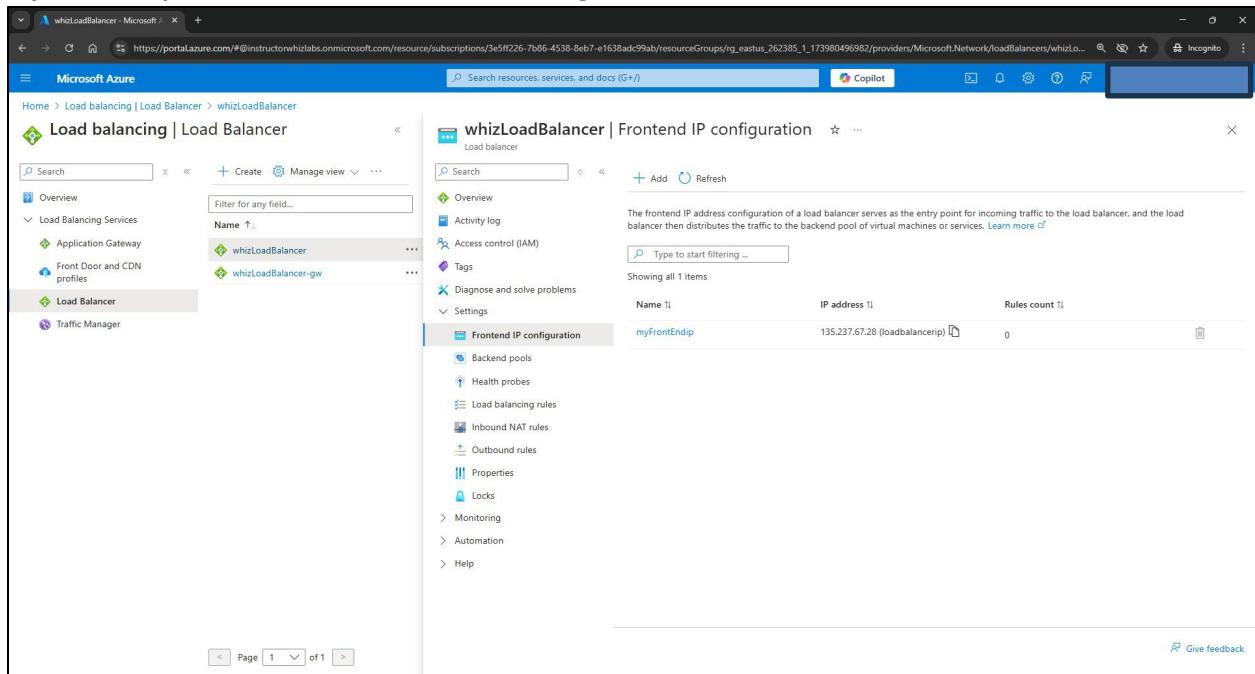
Select **whizFrontEnd (10.1.0.4)**

Select **Save**



The screenshot shows the Microsoft Azure portal interface for managing a load balancer. The URL in the address bar is [https://portal.azure.com/#view/Microsoft\\_Azure\\_Network/FrontendIPManage.ReactView/loadBalancerId/%2Fsubscriptions%23e5ff226-7b86-4538-8eb7-e1638adc99ab%2FresourceGroups%2Frq\\_eastus\\_262385\\_1\\_173980496982%2Fpro...](https://portal.azure.com/#view/Microsoft_Azure_Network/FrontendIPManage.ReactView/loadBalancerId/%2Fsubscriptions%23e5ff226-7b86-4538-8eb7-e1638adc99ab%2FresourceGroups%2Frq_eastus_262385_1_173980496982%2Fpro...). The page title is "myFrontEndip - Microsoft Azure". The main content area shows the configuration for a "myFrontEndip" frontend IP configuration. The "Name" field is set to "myFrontEndip". The "Type" is "Public". The "IP type" is "IP address", with "loadbalancerip (135.237.67.28)" selected. The "Gateway Load balancer" dropdown is highlighted with a red box, showing "whizFrontEnd (10.1.0.4)". Below the form, a section titled "Used by" lists load balancing rules, inbound NAT rules, inbound NAT pools, and outbound rules using this IP address. At the bottom, there are "Save" and "Cancel" buttons, with the "Save" button highlighted with a red box.

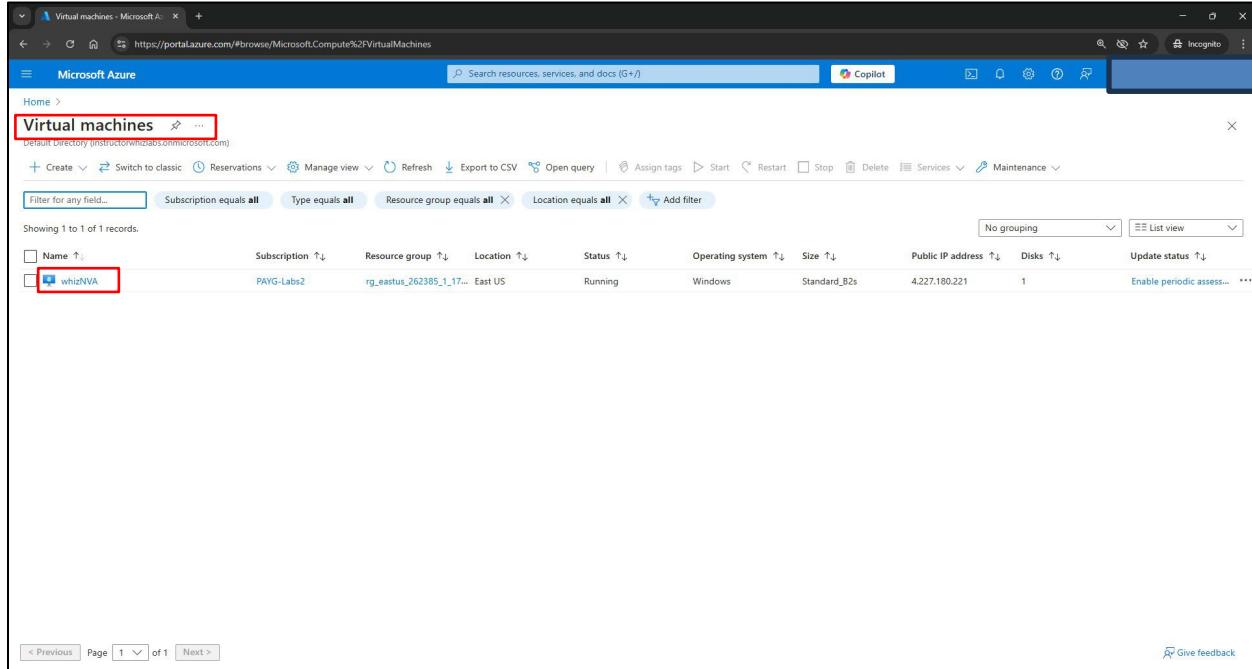
**myFrontEndip added to the Frontend IP configuration**



The screenshot shows the Microsoft Azure portal interface for managing a load balancer. The URL in the address bar is [https://portal.azure.com/#/instructorwhizlabs.onmicrosoft.com/resource/subscriptions/3e5ff226-7b86-4538-8eb7-e1638adc99ab/resourceGroups/rq\\_eastus\\_262385\\_1\\_173980496982/providers/Microsoft.Network/loadBalancers/whizLoadBalancer](https://portal.azure.com/#/instructorwhizlabs.onmicrosoft.com/resource/subscriptions/3e5ff226-7b86-4538-8eb7-e1638adc99ab/resourceGroups/rq_eastus_262385_1_173980496982/providers/Microsoft.Network/loadBalancers/whizLoadBalancer). The page title is "whizLoadBalancer | Load Balancer". The left sidebar shows "Load Balancing Services" with "Application Gateway" and "Load Balancer" selected. The main content area shows the "whizLoadBalancer | Frontend IP configuration" page. It has a search bar and a table with one row: "Name": "myFrontEndip", "IP address": "135.237.67.28 (loadbalancerip)", and "Rules count": "0". The table has columns for Name, IP address, and Rules count. The "Frontend IP configuration" section is expanded, showing options like Backend pools, Health probes, Load balancing rules, Inbound NAT rules, Outbound rules, Properties, Locks, Monitoring, Automation, and Help. At the bottom, there is a "Page 1 of 1" navigation bar and a "Save" button highlighted with a red box.

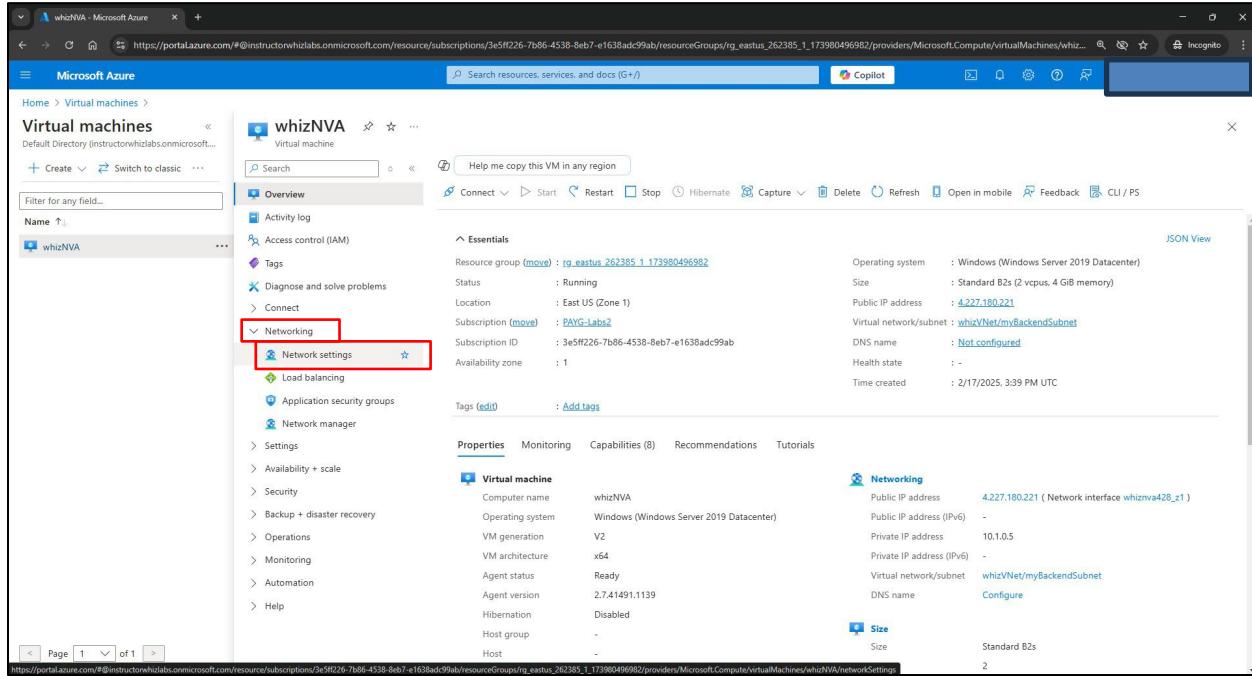
## Navigate to Virtual Machines

### Select whizNVA



The screenshot shows the Microsoft Azure portal interface. In the top left, there's a breadcrumb trail: Home > Virtual machines. The 'Virtual machines' link is highlighted with a red box. Below the navigation bar, there are several filter options: 'Subscription equals all', 'Type equals all', 'Resource group equals all', 'Location equals all', and a 'Filter for any field...' dropdown. The main table lists one record: 'whizNVA'. The columns include Name, Subscription, Resource group, Location, Status, Operating system, Size, Public IP address, Disks, and Update status. The 'whizNVA' row is also highlighted with a red box. At the bottom of the table, there are navigation buttons for '< Previous', 'Page 1 of 1', and 'Next >'. On the right side of the table, there are grouping and view mode buttons.

### Under Networking tab, select Network settings



The screenshot shows the detailed view of the 'whizNVA' virtual machine. The left sidebar has a tree view with 'Overview' selected, and 'Networking' is expanded, with 'Network settings' highlighted with a red box. Other options in the sidebar include Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Load balancing, Application security groups, Network manager, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, and Help. The main content area shows the 'Essentials' tab with basic information like Resource group, Status, Location, Subscription, and Availability zone. The 'Properties' tab shows details about the VM itself. The 'Networking' tab is active, displaying network interface information such as Public IP address (4.227.180.221), Private IP address (10.1.0.5), and DNS name (Not configured). There are also sections for Size (Standard B2s) and a 'Configure' button. The URL in the browser is https://portal.azure.com/#@instructorwhizlabs.onmicrosoft.com/resource/subscriptions/3e5ff226-7b86-4538-8eb7-e1638ad99ab/resourceGroups/rg\_eastus\_262385\_1\_173980496982/providers/Microsoft.Compute/virtualMachines/whizNVA/networkSettings.

## Select NIC whiznva428\_z1

This screenshot shows the Microsoft Azure portal interface for a virtual machine named 'whizNVA'. The user has navigated to the 'Network settings' section. In the top navigation bar, there is a search bar and a Copilot button. Below the search bar, there are tabs for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Network settings (which is currently selected), Load balancing, Application security groups, Network manager, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, and Help. The 'Networking' section displays details about the network interface: Network interface is 'whiznva428\_z1', Virtual network / subnet is 'whizVNet / myBackendSubnet', Public IP address is '4.227.180.221', Private IP address is '10.1.0.5', Admin security rules is '0 (Configure)', Load balancers is '1', Application security group is 'whizNSG', Network security group is 'whizNSG', Accelerated networking is 'Disabled', and Effective security rules is '0'. Below this, the 'Rules' section shows a single rule: 'Network security group whizNSG (attached to networkinterface: whiznva428\_z1)' with 'Impacts 0 subnets, 1 network interfaces'. There is also a 'Create port rule' button. At the bottom of the page, there is a table for 'Inbound port rules (4)'.

Under **Settings** drop down, select **IP configuration**

Under **Gateway load balancer**, select drop down for **whizLoadBalancer-gw/whizFrontEnd**

Select **Apply**

This screenshot shows the 'IP configurations' section for the 'whiznva428\_z1' virtual machine. The left sidebar includes options for Overview, Activity log, Access control (IAM), Tags, Settings (which is selected), IP configurations (highlighted with a red box), DNS servers, Properties, Locks, Monitoring, Automation, and Help. The main area shows 'IP Settings' with 'Enable IP forwarding' checked and 'Virtual network' set to 'whizVNet'. The 'IP configurations' table lists one entry: 'ipconfig1' (Type: IPv4, Primary, Private IP Address: 10.1.0.5 (Dynamic), Public IP Address: 4.227.180.221 (whizNVA-ip)). The 'Gateway load balancer' dropdown is set to 'whizLoadBalancer-gw/whizFrontEnd (10.1.0.4)'. Below the table, a note states: 'Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article.' At the bottom of the page, there are 'Apply' and 'Discard changes' buttons, with 'Apply' highlighted by a red box.

## Navigate to Lab Validation tab

### Select Validation

#### Select Validate My Lab

The screenshot shows the 'Lab Validation' tab selected in the navigation bar. A red box highlights the 'Validate My Lab' button. The main area displays the 'Check your Validation' section, which includes a summary of the lab's overall status (Passed) and five specific resource checks: Virtual Network, Network security group, Azure Load Balancer, and Virtual Machine, all marked as successful. On the right side, there is a sidebar with a timer showing '0h 20m 59s left', and a green 'Validation' button is highlighted with a red box. The sidebar also contains sections for 'Lab Credentials' (User Name: labuser\_262385\_173980496982, Password: P@#MeZBx056%, Resource Group: rg\_eastus\_262385\_1\_173980496982), a 'Submit Feedback' button, and a 'Share' link.

## Navigate to Resource Groups

### Select Resource group rg\_eastus\_262385\_1\_1739804496982

#### Select Delete resource group

The screenshot shows the 'Resource groups' blade in the Microsoft Azure portal. A red box highlights the 'rg\_eastus\_262385\_1\_173980496982' resource group in the list. Another red box highlights the 'Delete resource group' button in the top right corner of the resource group details panel. The details panel shows the resource group's name, subscription information, and location. Below it, the 'Resources' section lists various Azure resources, including a load balancer, bastion IP, and network security group, all located in East US.

Copy / past Resource Group name in **Enter resource group name to confirm deletion** box  
Select checkbox next to **Apply force delete for selected Virtual machines and Virtual machine scale sets**

## Select Delete

The following resource group and all its dependent resources will be permanently deleted.

**Resource group to be deleted**

[Icon] rg_eastus_262385_1_173980496982	[Delete]
--	----------

**Dependent resources to be deleted (11)**  
All dependent resources, including hidden types, are shown

Name	Resource type
loadbalancerip	Public IP address
myBastionIP	Public IP address
myBastionIP	Bastion
whizLoadBalancer	Load balancer
whizLoadBalancer-gw	Load balancer
whizNSG	Network security group
whizNVA	Virtual machine
whizNVA-ip	Public IP address
whiznva428_z1	Network interface
whizNVA_ODisk_1_e1e9d1b5b213472da4f5f9f	Disk
whizVNet	Virtual network

Apply force delete for selected Virtual machines and Virtual machine scale sets

Enter resource group name to confirm deletion : **rg\_eastus\_262385\_1\_173980496982**

**Delete** **Cancel**

## Select Delete

The following resource group and all its dependent resources will be permanently deleted.

**Resource group to be deleted**

[Icon] rg_eastus_262385_1_173980496982	[Delete]
--	----------

**Dependent resources to be deleted (11)**  
All dependent resources, including hidden types, are shown

Name	Resource type
loadbalancerip	Public IP address
myBastionIP	Public IP address
myBastionIP	Bastion
whizLoadBalancer	Load balancer
whizLoadBalancer-gw	Load balancer
whizNSG	Network security group
whizNVA	Virtual machine
whizNVA-ip	Public IP address
whiznva428_z1	Network interface
whizNVA_ODisk_1_e1e9d1b5b213472da4f5f9f	Disk
whizVNet	Virtual network

Apply force delete for selected Virtual machines and Virtual machine scale sets

Enter resource group name to confirm deletion : **rg\_eastus\_262385\_1\_173980496982**

**Delete** **Go back**

Normally, would delete everything, but Business WhizLabs does not allow us to delete Resource Groups

The screenshot shows the Microsoft Azure portal's Resource Groups overview page. The URL in the address bar is [https://portal.azure.com/#@instructorwhizlabs.onmicrosoft.com/resource/subscriptions/3e5f226-7b86-4538-8eb7-e1638adc99ab/resourceGroups/rg\\_eastus\\_262385\\_1\\_173980496982/overview](https://portal.azure.com/#@instructorwhizlabs.onmicrosoft.com/resource/subscriptions/3e5f226-7b86-4538-8eb7-e1638adc99ab/resourceGroups/rg_eastus_262385_1_173980496982/overview).

**Resource groups** > rg\_eastus\_262385\_1\_173980496982

**Overview**

**Essentials**

- Subscription (move) : PAYG-Labs
- Subscription ID : 3e5f226-7b86-4538-8eb7-e1638adc99ab
- Location : East US
- Tags (edit) : CreationTime : 1739804969

**Resources**

Name	Type	Location
loadbalancerip	Public IP address	East US
myBastionIP	Bastion	East US
myBastionIP	Public IP address	East US
whizLoadBalancer	Load balancer	East US
whizLoadBalancer-gw	Load balancer	East US
whizNSG	Network security group	East US
whizNVA	Virtual machine	East US
whizNVA-ip	Public IP address	East US

**Error Message:** Delete resource group rg\_eastus\_262385\_1\_173980496982 failed  
Failed to delete resource group rg\_eastus\_262385\_1\_173980496982: The client 'labuser\_262385\_1739804966591@instructorwhizlabs.onmicrosoft.com' with object id '8abb25d7-131c-4741-84fd-001b1f15524' does not have authorization to perform action 'Microsoft.Resources/subscriptions/resourceGroups/delete'. If the scope '/subscriptions/3e5f226-7b86-4538-8eb7-e1638adc99ab/resourceGroups/rg\_eastus\_262385\_1\_173980496982' or the scope is invalid, if access was recently granted, please refresh your credentials. (Code: AuthorizationFailed)