Microsoft Azure Administrator Associate Training(AZ-103) Module 5

Agenda

01 Azure Load Balancer

02 Load Balancer Concepts

03 Types of Load Balancers

04 Internal Load Balancer

05 Create Internal Load Balancer

06 Public Load Balancer

07 Create a Public Load Balancer

08 Troubleshooting Load Balancer

09 Why Azure Network Watcher?

10 Azure Network Watcher Features

11 Why VPN Gateways?

12 What is VPN Gateway?

Agenda

13 Set up VPN Gateway Site to Site Connection

14 Why Azure Express Route?

15 What is Azure Express Route

16 Azure Express Route Benefits

17 Azure Express Route Components

18 Express Route Circuits

19 Express Route Peerings

20 Types of Express Route Peering

21 Quiz

Azure Load Balancer

Azure Load Balancer

In Azure, Load Balancers are used to distribute incoming traffic across a pool of resources in order to maintain availability.

Load Balancer Concepts

Load Balancer Concepts

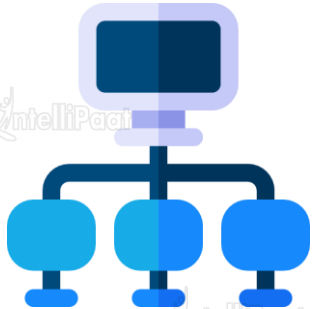
- **Frontend IP Address**
- **Backend Pool**
- **Health Probe**
- **Load Balancing Rule**

A Frontend IP Address is IP Address that is assigned to the load balancer and is used to access the resources being managed by the load balancer.

Load Balancer Concepts

- Frontend IP Address
- **Backend Pool**
- Health Probe
- Load Balancing Rule

A Backend Pool is a pool (group) of resources that are being managed by a load balancer. e.g. VM's.



Load Balancer Concepts

- Frontend IP Address
- Backend Pool
- Health Probe
- Load Balancing Rule

A Health Probe is a special signal that is sent to each resource in the backend pool to check if it's healthy and available.

Load Balancer Concepts

- Frontend IP Address
- Backend Pool
- Health Probe
- Load Balancing Rule

A load balancing rule is used to associate the frontend IP, backend pool and heath probe together.

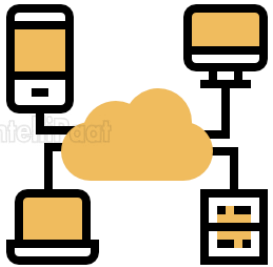
Types of Load Balancers

Types of Load Balancers

There are two types of load balancers in your Azure.

1. Internal Load balancer

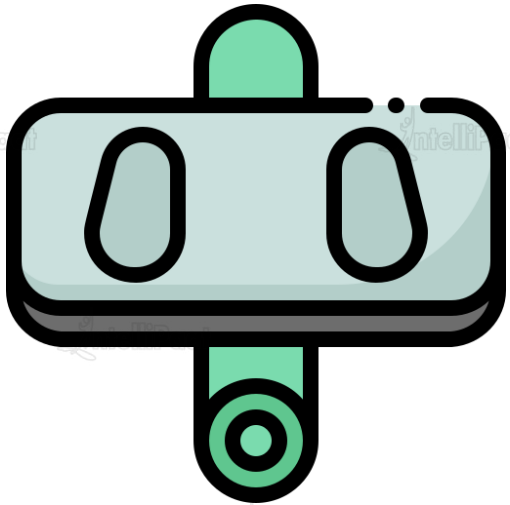
2. Public Load Balancer



Internal Load Balancer

Internal Load Balancer

An Internal Load Balancer is used to direct traffic only between either Azure's internal resources i.e. resources managed by the Azure infrastructure or resources connected to Azure infrastructure using a secure VPN.

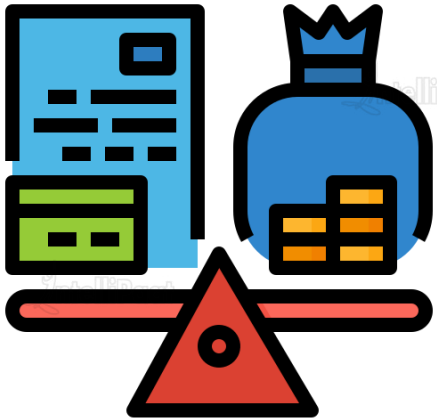


Hands-on : Create an Internal Load Balancer

Public Load Balancer

Public Load Balancer

A Public Load Balancer is used to handle traffic between a public facing IP address of incoming traffic to private IP addresses of Azure resources.



Hands-on: Create a Public Load Balancer

Troubleshooting Load Balancer

Troubleshooting Load Balancer

There are two reason why you might have to troubleshoot a load balancer.

1. VM's are not responding to the health probe.

2. VM's are not responding to the traffic.

VM’s are not responding to the health probe.

VM's not responding to the health probe

There may be several reasons for this.

- **VM's in the backend pool are unhealthy.**
- **VM's in the backend pool are not listening on the probe port.**
- **The health probe port is blocked by firewall or NSG.**
- **Misconfiguration in Load Balancer**

VM's not responding to the health probe

There may be several reasons for this.

- **VM's in the backend pool are unhealthy.**
- **VM's in the backend pool are not listening on the probe port.**
- **The health probe port is blocked by firewall or NSG.**
- **Misconfiguration in Load Balancer**

VM's not responding to the health probe

There may be several reasons for this.

- **VM's in the backend pool are unhealthy.**
- **VM's in the backend pool are not listening on the probe port.**
- **The health probe port is blocked by firewall or NSG.**
- **Misconfiguration in Load Balancer**

VM's not responding to the health probe

There may be several reasons for this.

- **VM's in the backend pool are unhealthy.**
- **VM's in the backend pool are not listening on the probe port.**
- **The health probe port is blocked by firewall or NSG.**
- **Misconfiguration in Load Balancer**

VM’s are not responding to the traffic.

VM's not responding to the traffic.

There may be several reasons for this.

- **VM's in backend pool are not listening on the data port**
- **Data port is being blocked by NSG**
- **Accessing the Load Balancer from the same VM and NIC**
- **Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.**

VM's not responding to the traffic.

There may be several reasons for this.

- VM's in backend pool are not listening on the data port
- Data port is being blocked by NSG
- Accessing the Load Balancer from the same VM and NIC
- Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.

VM's not responding to the traffic.

There may be several reasons for this.

- VM's in backend pool are not listening on the data port
- Data port is being blocked by NSG
- Accessing the Load Balancer from the same VM and NIC
- Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.

VM's not responding to the traffic.

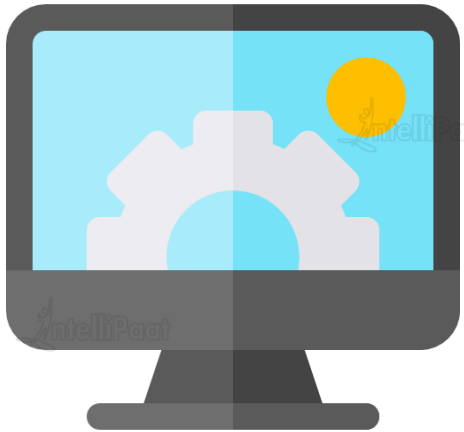
There may be several reasons for this.

- **VM's in backend pool are not listening on the data port**
- **Data port is being blocked by NSG**
- **Accessing the Load Balancer from the same VM and NIC**
- **Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.**

What Is Azure Network Watcher?

What Is Azure Network Watcher?

Azure Network Watcher is a service that contains multiple tools used to diagnose and monitor our Azure Networks.



Azure Network Watcher Features

Azure Network Watcher Features

- **Monitoring**
- **Diagnostics**
- **Metrics**
- **Logs**

Network Watcher allows us to monitor traffic between virtual machines and other endpoints. Such as Virtual Machines, URI's etc.

Azure Network Watcher Features

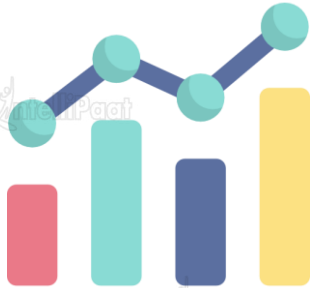
- Monitoring
- Diagnostics
- Metrics
- Logs

Azure Network Watcher allows us to diagnose problems related to filtering, routing, connectivity etc.

Azure Network Watcher Features

- Monitoring
- Diagnostics
- Metrics
- Logs

In Network Watcher we can analyze how many of each network resource we have deployed in a region and what the current limit is.



Azure Network Watcher Features

- Monitoring
- Diagnostics
- Metrics
- Logs

In Network Watcher we analyze log files for our Network Security Groups and diagnostic logs for network resources.

Why VPN Gateways?

Why VPN Gateways

A VPN gateway is used to send private encrypted data from one network to another via the public internet.

What is Azure VPN Gateway?

What is Azure VPN Gateway?

In Azure a VPN Gateway is made up of two or more Virtual Machines

These Virtual Machines are deployed in a special subnet called gateway subnet.

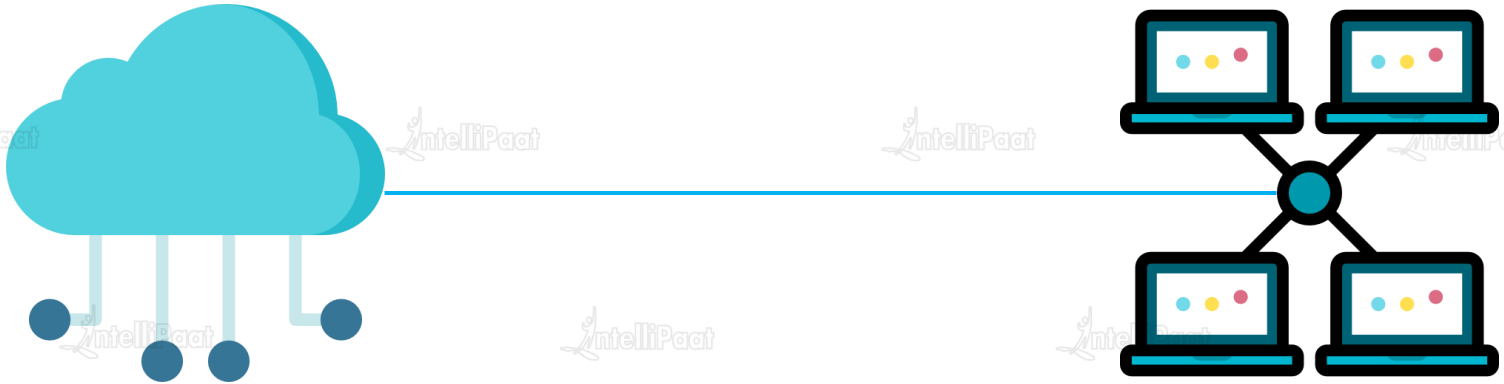
These Virtual Machines are created and configured automatically when we create a VNET Gateway.

Azure Site to Site Connection

Why Site to Site Connection

Why Site to Site Connection

Azure Site to Site Connection is used to connect to your On Premise Network to an Azure Virtual Network over the public internet.



What is Site to Site Connection

What is Azure Site to Site Connection

Azure Site to Site Connection allows us to connect and send traffic between our on premises network and an Azure virtual network.

The traffic is sent over the public internet and is encrypted and sent through a VPN Tunnel.

A Site to Site Connection is an ideal solution for connecting on premise network and an Azure Virtual Network if sending encrypted traffic over public internet is not a concern.

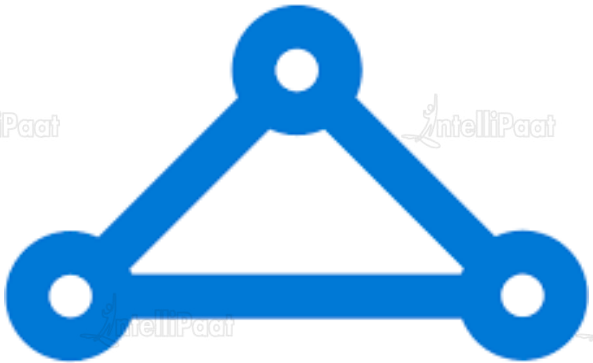
Site Connection require a VPN device to be located in the on premise network with a public IP Address.

Hands-on: Set up VPN Gateway Site to Site Connection

Why Azure Express Route

Why Azure Express Route

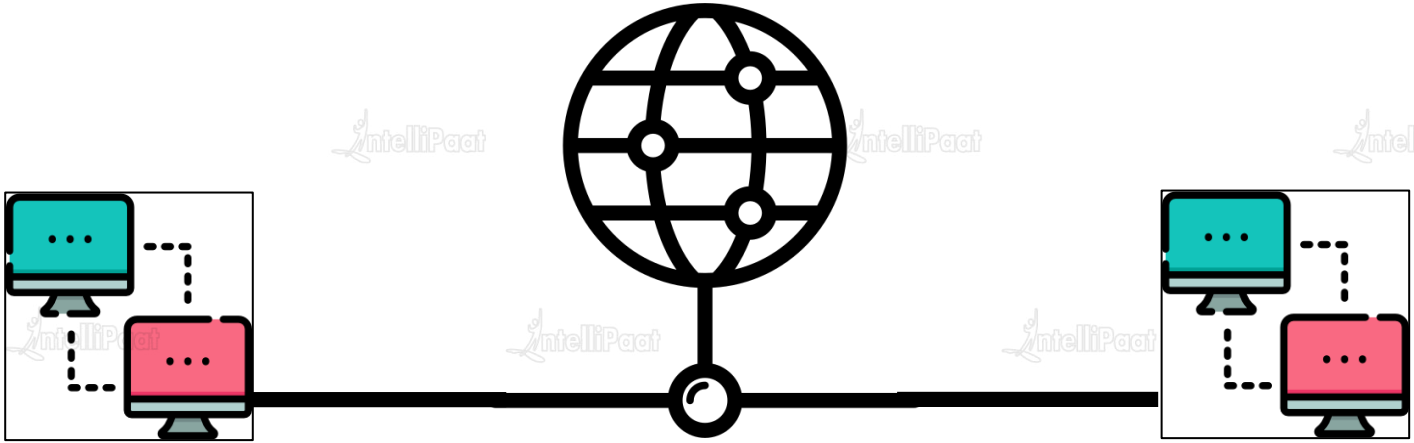
Azure Express Route enables you to connect your on premises network to Azure Cloud privately with low latency.



What is Azure Express Route

What is Azure Express Route

Microsoft Azure Express Route allows us to connect our on premises network to Microsoft Cloud services like Azure, Office 365 etc. using a private connection established via a connection provider.



Azure Express Route Benefits

Azure Express Route Benefits

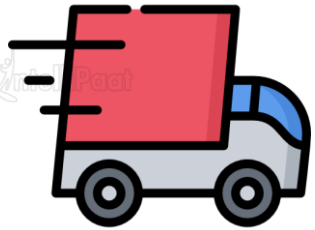
- **Secure**
- **Fast**
- **Cloud Services**
- **Flexible Billing**

Express Route creates a private connections between Microsoft datacenters and infrastructure.

Azure Express Route Benefits

- Secure
- Fast
- Cloud Services
- Flexible Billing

Express Route supports bandwidth up to 10Gbps



Azure Express Route Benefits

- Secure
- Fast
- Cloud Services
- Flexible Billing

Express Route connections can be used to access: Microsoft Azure services, Microsoft Office 365 services, Microsoft Dynamics 365

Azure Express Route Benefits

- Secure
- Fast
- Cloud Services
- Flexible Billing

Express Route supports the following billing system: Unlimited data, Metered Data.

Azure Express Route Components

Azure Express Route Components

Azure Express Route has two major components.

1. Circuits

2. Peering

Express Route Circuits

Express Route Circuits

An Express Route circuit is a logical connection between your on-premises network and Microsoft cloud services through a connectivity provider.

An Express Route circuit is identified and referenced by a unique identifier called a Service Key.

Each circuit has a fixed bandwidth that is shared by all the network peerings.

Express Route Peerings

Express Route Peerings

A Peering is an connection between two separate networks.

Each Express Route Circuit has three types of peering associated with it: Azure Public, Azure Private and Microsoft Peering

Types of Express Route Peering

Types of Express Route Peering

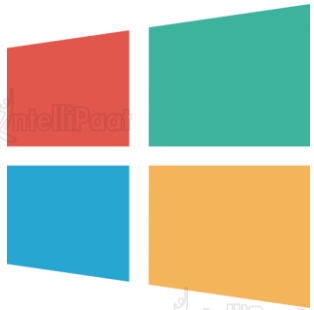
- **Private**
- **Microsoft**
- **Public**

Private peering is used to connect to Azure compute services like virtual machines, cloud services etc. that are deployed in your VNet.

Types of Express Route Peering

- Private
- Microsoft
- Public

Microsoft Peering is used to connect to Microsoft online services like Office 365, Dynamic 365 etc.



Types of Express Route Peering

- Private
- Microsoft
- Public

Public peering is used to connect to service like Azure Storage, SQL databases, Websites etc. Public peering is deprecated for new circuits and it is advised that you use Microsoft peering in its place.

Quiz

Quiz

1. Which of the following is used by load balancer to check if the resources it's managing are healthy or not?

A	Backend pool
B	Frontend IP
C	Load Balancing Rule
D	Health Probe

Quiz

1. Which of the following is used by load balancer to check if the resources it's managing are healthy or not?

A	Backend pool
B	Frontend IP
C	Load Balancing Rule
D	Health Probe

Quiz

2. Which of the following is used to connect on premise network with Azure over public internet?

A	Site to Site Connection
B	ExpressRoute
C	VNET Peering
D	All of the above

Quiz

2. Which of the following is used to connect on premise network with Azure over public internet?

A	Site to Site Connection
B	ExpressRoute
C	VNET Peering
D	All of the above

Quiz

3. Which of the following is used to connect on premise network with Azure using a private connection?

A	Site to Site Connection
B	ExpressRoute
C	VNET Peering
D	All of the above

Quiz

3. Which of the following is used to connect on premise network with Azure using a private connection?

A	Site to Site Connection
B	ExpressRoute
C	VNET Peering
D	All of the above

Quiz

4. Which of the following ExpressRoute peering types is now deprecated?

A	Private Peering
B	Microsoft Peering
C	Public Peering
D	None of the above

Quiz

4. Which of the following ExpressRoute peering types is now deprecated?

A	Private Peering
B	Microsoft Peering
C	Public Peering
D	None of the above

Quiz

5. ExpressRoute supports bandwidth up to 10Gbps. True or False ?

A	True
B	False

Quiz

5. ExpressRoute supports bandwidth up to 10Gbps. True or False ?

A	True
B	False

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24/7 Chat with Our Course Advisor