Microsoft Azure

Administrator Associate Training

Implement Advanced Virtual Networking

Agenda

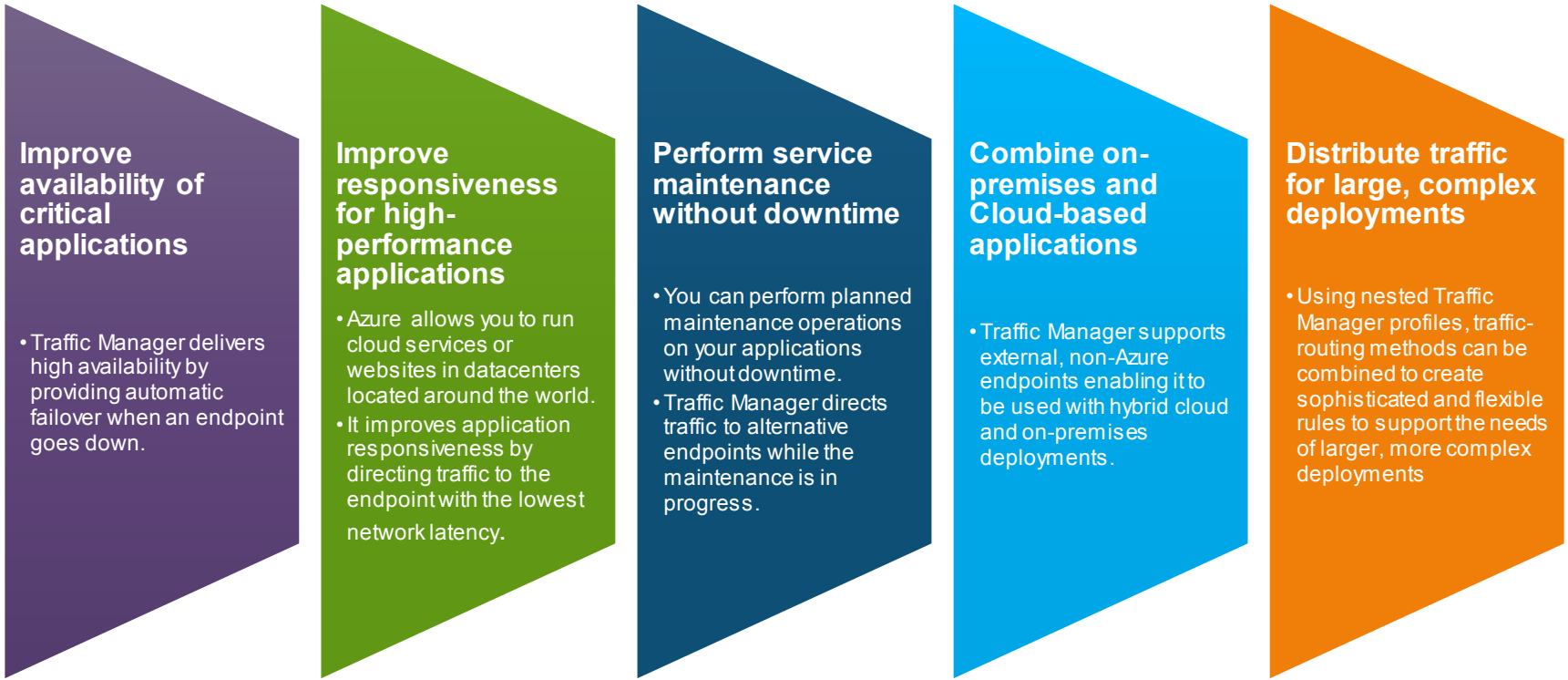
- What is Azure Traffic Manager
- Benefits
- How it works
- Azure Endpoints
- External Endpoints
- Endpoints Monitoring
- Routing Methods
- Priority Traffic-Routing Method
- Weighted Traffic-Routing Method
- Performance Traffic-Routing Method
- Geographic Traffic-Routing Method
- Nested Traffic Manager Profiles
- Traffic View
- What is Azure Load Balancer
- Internet Facing Load Balancer
- Internal Facing Load Balancer
- Probes
- High Availability Ports
- Why use HA Ports
- Multiple VIPs

Azure Traffic Manager

What is Azure Traffic Manager?

- Microsoft Azure Traffic Manager allows you to control the distribution of user traffic for service endpoints in different datacenters.
- Service endpoints supported by Traffic Manager include Azure VMs, Web Apps, and cloud services.
- You can also use Traffic Manager with external, non-Azure endpoints.
- Traffic Manager uses the Domain Name System (DNS) to direct client requests to the most appropriate endpoint based on a traffic-routing method and the health of the endpoints.
- Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models.
- Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Azure Traffic Manager: Benefits



Azure Traffic Manager: How it works?

Azure Traffic Manager enables you to control the distribution of traffic across your application endpoints.

An endpoint is any Internet-facing service hosted inside or outside of Azure.

Traffic Manager provides two key benefits:

- Distribution of traffic according to one of several traffic-routing methods
- Continuous monitoring of endpoint health and automatic failover when endpoints fail

When a client attempts to connect to a service, it must first resolve the DNS name of the service to an IP address.

The client then connects to that IP address to access the service.

The most important point to understand is that Traffic Manager works at the DNS level.

Traffic Manager uses DNS to direct clients to specific service endpoints based on the rules of the traffic-routing method.

Clients connect to the selected endpoint directly.

Azure Traffic Manager:
Azure Endpoints

- Azure endpoints are used for Azure-based services in Traffic Manager.
- The following Azure resource types are supported:

Web Apps

PublicIPAddress Resources

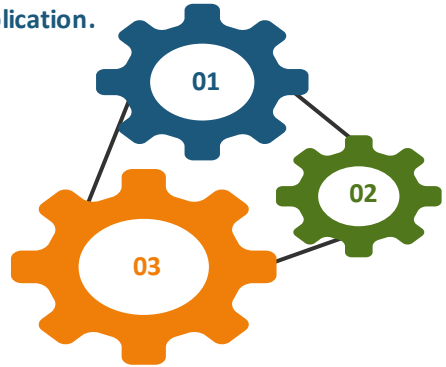
The publicIpAddress must have a DNS name assigned to be used in a Traffic Manager profile.

- When the underlying service is stopped, Traffic Manager does not perform endpoint health checks or direct traffic to the endpoint.
- This detection does not apply to PublicIpAddress endpoints.

Azure Traffic Manager: External Endpoints

- External endpoints are used for services outside of Azure.
- External endpoints can be used individually or combined with Azure Endpoints.
- Combining Azure endpoints with external endpoints enables various scenarios:

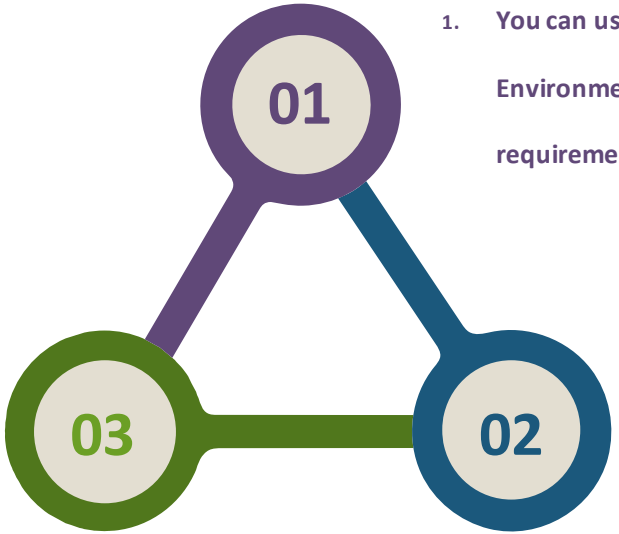
1. In either an active-active or active-passive failover model, use Azure to provide increased redundancy for an existing on-premises application.



2. To reduce application latency for users around the world, extend an existing on-premises application to additional geographic locations in Azure.

3. Use Azure to provide additional capacity for an existing on-premises application, either continuously or as a 'burst-to-cloud' solution to meet a spike in demand.

Azure App Service Environment

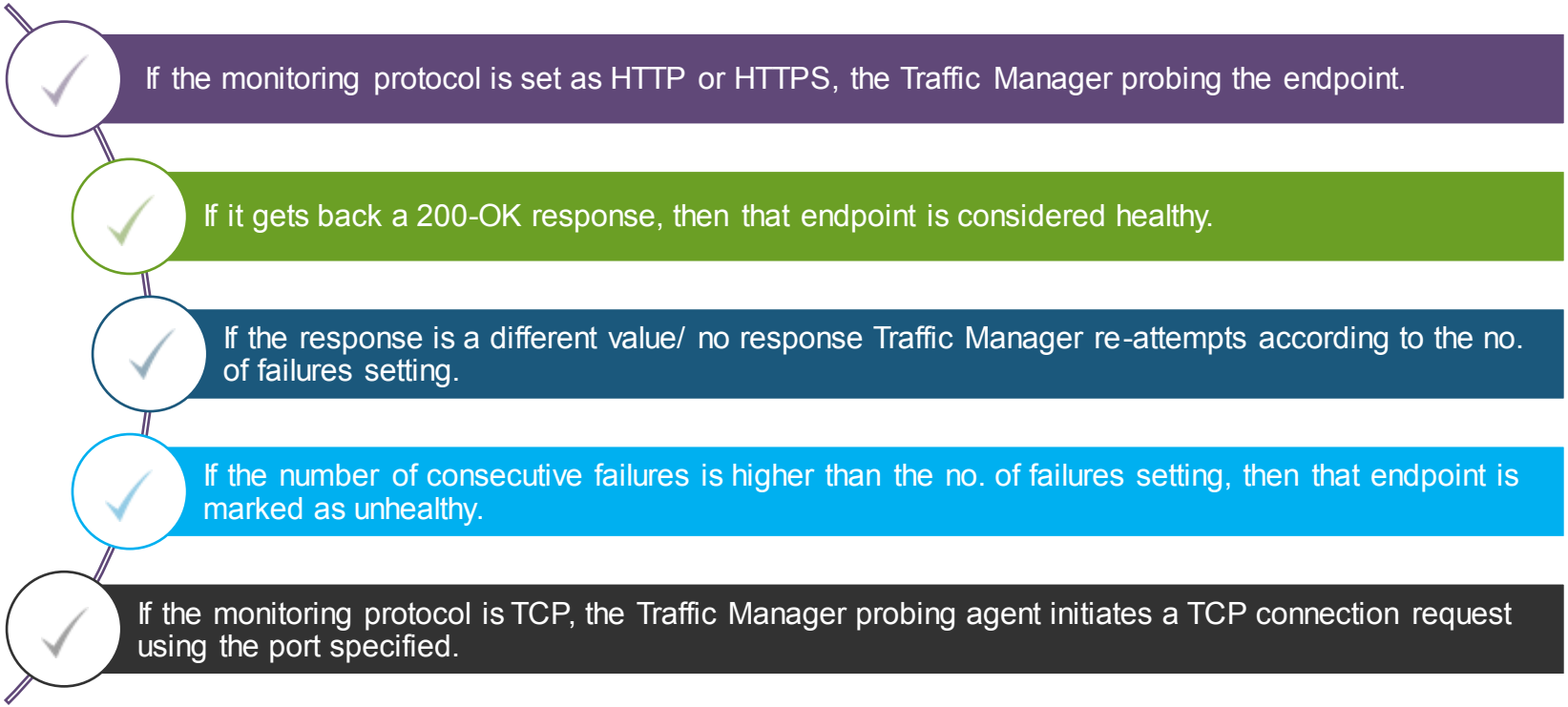


1. You can use the App Service Environment to accommodate this requirement.

2. Business-critical apps often require highly scalable, isolated, and dedicated environments.

3. You can use the App Service Environment to host web apps, mobile apps, and API apps that require highly scalable compute resources, isolation, and direct virtual network connectivity.

Azure Traffic Manager: Endpoints Monitoring



Azure Traffic Manager:
Routing Methods

Performance

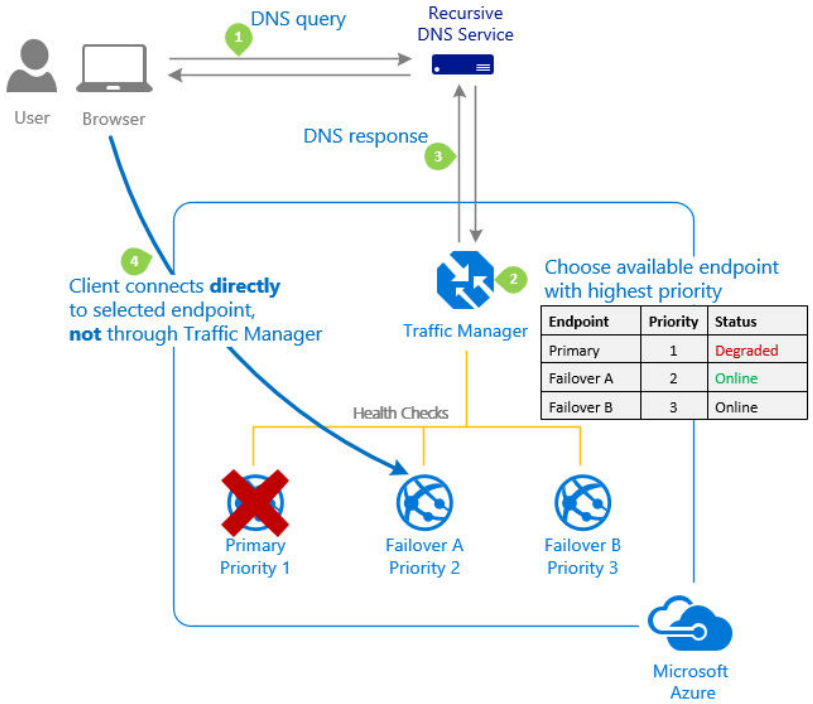
Priority/ Failover

Weighted

Geographic

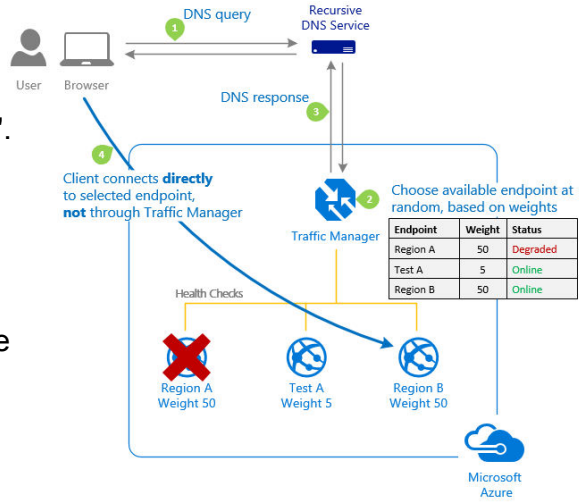
Azure Traffic Manager:
Priority Traffic-Routing Method

- The 'Priority' traffic-routing method allows to implement the failover pattern.
- By default, Traffic Manager sends all traffic to the primary (highest-priority) endpoint.
- If the primary endpoint is not available, Traffic Manager routes the traffic to the second endpoint.
- If both the primary and secondary endpoints are not available, the traffic goes to the third, and so on.



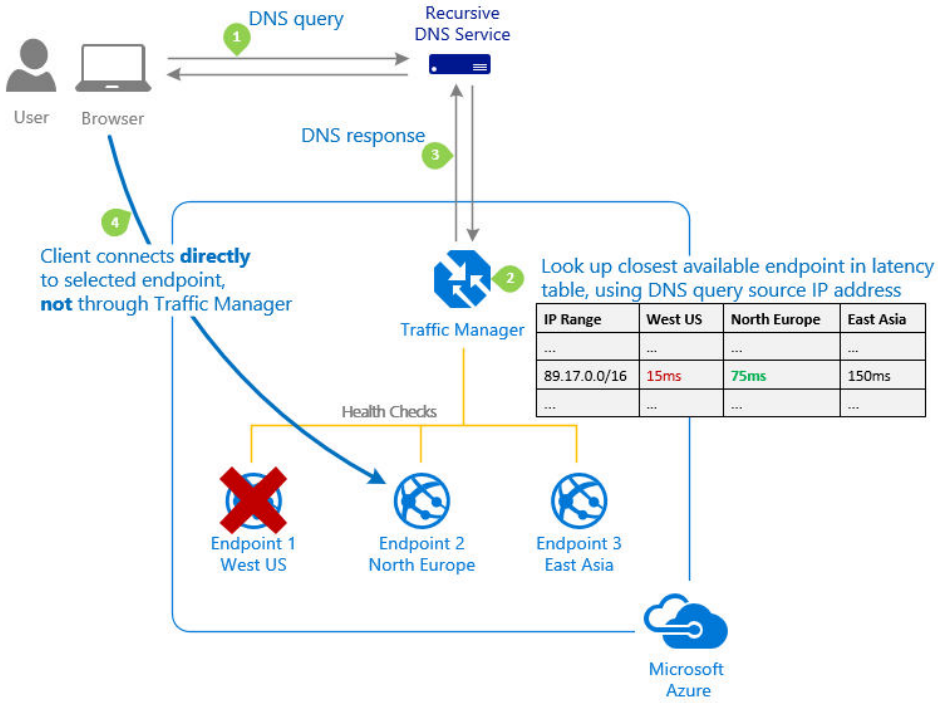
Azure Traffic Manager: Weighted Traffic-Routing Method

- The 'Weighted' traffic-routing method allows you to distribute traffic evenly or to use a pre-defined weighting.
- In the Weighted traffic-routing method, you assign a weight to each endpoint.
- The weight is an integer from 1 to 1000. Traffic Managers uses a default weight of '1'. This parameter is optional.
- For each DNS query received, Traffic Manager randomly chooses an available endpoint.
- The probability of choosing an endpoint is based on the weights assigned to all available endpoints.
- Using the same weight across all endpoints results in an even traffic distribution.
- Using higher or lower weights on specific endpoints causes those endpoints to be returned more or less frequently in the DNS responses.



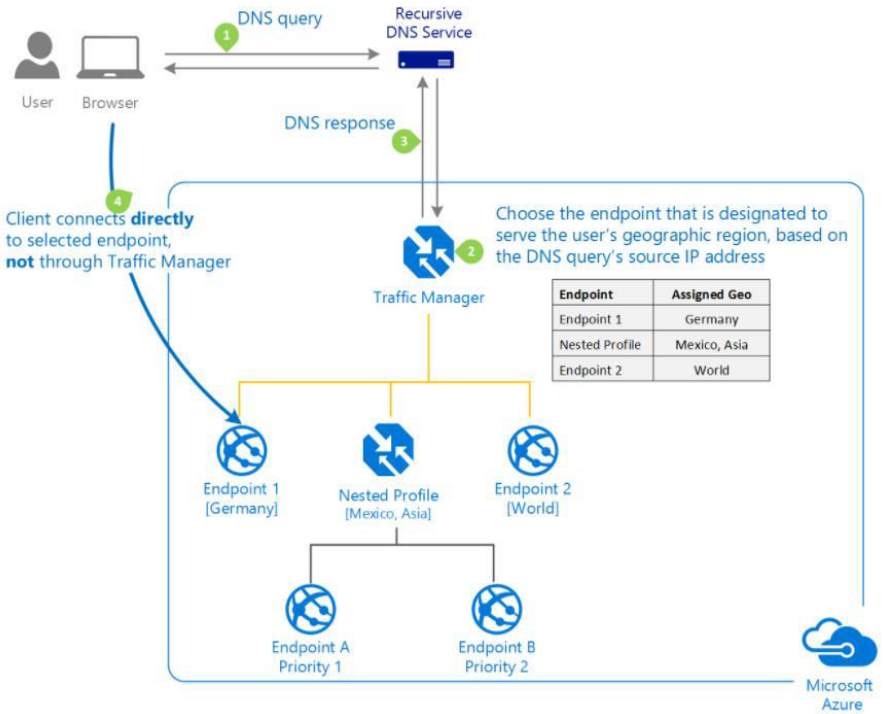
Azure Traffic Manager:
Performance Traffic-Routing Method

- Deploying endpoints in two or more locations across the globe, to rout the traffic to the location that is 'closest'.
- The 'Performance' traffic-routing method determines the closest endpoint by measuring network latency.
- Traffic Manager chooses an available endpoint in the Azure datacenter that has the lowest latency, then returns that endpoint in the DNS response.



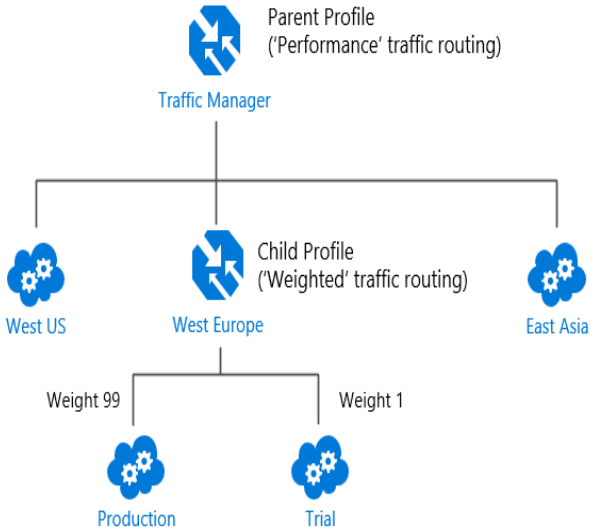
Azure Traffic Manager: Geographic Traffic-Routing Method

- Using Geographic routing, users are directed to specific endpoints based on which geographic location their DNS query originates from.
- Examples include:
  - Complying with data sovereignty.
  - Localization of content.
  - User experience and measuring traffic from different regions.
- When a region or a set of regions is assigned to an endpoint, any requests from those regions gets routed only to that endpoint.



Azure Traffic Manager:
Nested Traffic Manager Profiles

- Each Traffic Manager profile specifies a single traffic-routing method.
- You can nest Traffic Manager profiles to combine the benefits of more than one traffic-routing method.
- Nested profiles allow you to override the default Traffic Manager behavior to support larger and more complex application deployment.
- Example:
  - Suppose you wish to test an update to your service before rolling it out more widely.
  - You want to use the 'weighted' traffic-routing method to direct a small percentage of traffic to your test deployment.
  - You set up the test deployment alongside the existing production deployment in West Europe.



Azure Traffic Manager: Traffic View

- Traffic Manager provides you with DNS level routing so that your end users are directed to healthy endpoints based on the routing method.
- By using Traffic View, you can:

Understand where your user bases are located.	View the volume of traffic originating from these regions.	Get insights into what is the representative latency experienced by these users.

- For example, you can use Traffic View to understand which regions have a large number of traffic but suffer from higher latencies.
- Next, you can use this information to plan your footprint expansion to new Azure regions so that these users can have a lower latency experience.

Hands-On

Hands-On

- Configure Traffic Manager using Priority Routing method.
- Configure 2 Web Server using Priority Routing method.
- Failover the traffic from Primary to Secondary web server.

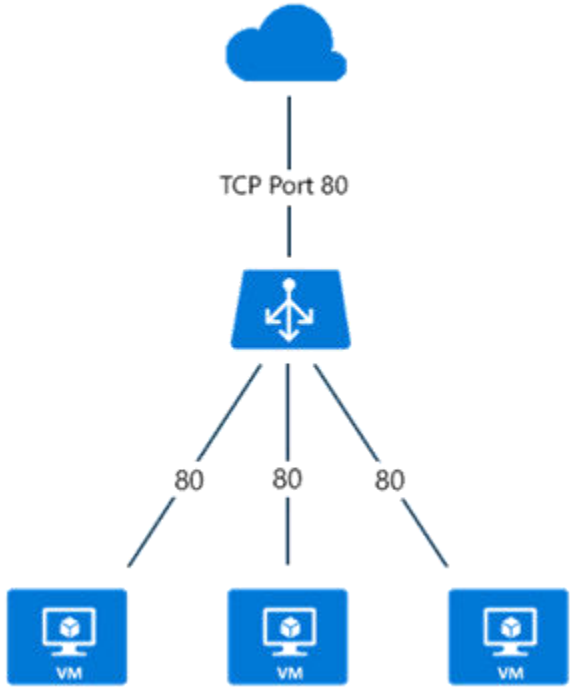
Azure Load Balancer

What is Azure Load Balancer?

- Azure Load Balancer delivers high availability and network performance to your applications.
- It is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic.
- Azure Load Balancer can be configured to Load balance incoming Internet traffic to virtual machines
- All resources in the cloud need a public IP address to be reachable from the Internet.

Azure Load Balancer:
Internet Facing Load Balancer

- Azure load balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the virtual machine and vice versa for the response traffic from the virtual machine.
- Load balancing rules allow you to distribute specific types of traffic between multiple virtual machines or services.
- For example, you can spread the load of web request traffic across multiple web servers.
- The following figure shows a load-balanced endpoint for web traffic that is shared among three virtual machines for the public and private TCP port of 80. These three virtual machines are in a load-balanced set.
- When Internet clients send web page requests to the public IP address of the cloud service on TCP port 80, the Azure Load Balancer distributes the requests between the three virtual machines in the load-balanced set.
- You can also configure session affinity.



Azure Load Balancer:
Internal Facing Load Balancer

- Azure Internal Load Balancer (ILB) only directs traffic to resources that are inside a cloud service or that use a VPN to access Azure infrastructure.
- The load-balanced virtual IP (VIP) addresses are never directly exposed to an internet endpoint.
- ILB enables the following types of load balancing:

▪Within a cloud service	Within a virtual network	For a cross-premises virtual network
• Load balancing from VMs that reside within the same cloud service.	• Load balancing from VMs in the virtual network that reside within the same virtual network.	• Load balancing from on-premises computers to a set of VMs that reside within the same virtual network.

Azure Load Balancer: Probes

- Azure Load Balancer offers the capability to monitor the health of server instances by using probes.
- When a probe fails to respond, Load Balancer stops sending new connections to the unhealthy instance.
- The existing connections are not affected, and new connections are sent to healthy instances.
- TCP or HTTP custom probes must be configured when you use VMs behind Load Balancer.
- Probe behavior depends on:

The number of successful probes that allow an instance to be labeled as up.	The number of failed probes that cause an instance to be labeled as down.

- The timeout and frequency values set in SuccessFailCount determine whether an instance is confirmed to be running or not running.

Azure Load Balancer:
High Availability Ports

- Azure Load Balancer helps you load balance TCP and UDP, when you are using an internal Load Balancer.
- You can simplify your use of Load Balancer by providing a single rule to load balance all TCP and UDP.
- Load balancing decision is made per flow, based on the:

Source & Destination IP Address	Source & Destination Port	Protocol

- The HA ports helps, in providing high availability for network virtual appliances (NVA) inside virtual networks.
- It can also help when a large number of ports must be load balanced.
- The HA ports feature is configured when you set the front-end and back-end ports to **0**, and the protocol to **All**.
- The internal Load Balancer resource then balances all TCP and UDP flows, regardless of port number.

Azure Load Balancer: Why use HA Ports?

- You can use Network virtual appliance (NVAs) for securing your Azure workload from multiple types of security threats.
- When NVAs are used in these scenarios, they must be reliable and highly available, and they must scale out for demand.
- You can achieve these goals simply by adding NVA instances to the back-end pool of the Azure internal Load Balancer, and configuring an HA ports Load Balancer rule.
- HA ports provide several advantages for NVA HA scenarios:

Fast failover to healthy instances, with per-instance health probes.

Higher performance with scale-out to *n*-active instances

N-active and active-passive scenarios.

Azure Load Balancer: Multiple VIPs

- Azure Load Balancer allows you to load balance services on multiple ports, multiple IP addresses, or both.
- You can use public and internal load balancer definitions to load balance flows across a set of VMs.
- When you define an Azure Load Balancer, a frontend and a backend configuration are connected with rules.
- The health probe referenced by the rule is used to determine how new flows are sent to a node in the backend pool.
- The frontend is defined by a Virtual IP (VIP), which is comprised of an IP address (public or internal), a transport protocol (UDP or TCP) and a port number.

Hands-On

Hands-On

- Configure Availability Set with 2 fault domains
- Launch 2 Web server in Availability Set
- Configure Load Balancer
- Access Web Server using Load Balancer

QUIZ

Quiz 1

Azure Traffic Manager ?

A	helps to create traffic for your website
B	helps to reduce the traffic on your website
C	helps to increase the traffic on your website
D	helps in controlling the distribution of traffic

Answer 1

Azure Traffic Manager ?

A	helps to create traffic for your website
B	helps to reduce the traffic on your website
C	helps to increase the traffic on your website
D	helps in controlling the distribution of traffic

Quiz 2

What does traffic manager uses?

A Domain Name System

B Vnet Peering

C Azure VM

D Network Security Groups

Answer 2

IntelliPaat

What does traffic manager uses?

A	Domain Name System
B	Vnet Peering
C	Azure VM
D	Network Security Groups

Quiz 3

Does Azure uses endpoints for Azure-based services in Traffic manager?

A	Yes
B	No

Answer 3

Does Azure uses endpoints for Azure-based services in Traffic manager?

A	Yes
B	No

Quiz 4

Which option is correct about External Endpoints?

A	External endpoints are used for enabling the third party endpoints for your instance
B	External endpoints are used for services outside of Azure
C	External endpoints enables you to use the third party cloud services
D	All of the above

Answer 4

Which option is correct about External Endpoints?

A	External endpoints are used for enabling the third party endpoints for your instance
B	External endpoints are used for services outside of Azure
C	External endpoints enables you to use the third party cloud services
D	All of the above

Quiz 5

At which response the endpoint is considered as healthy?

A	500-OK response
B	300-OK response
C	200-OK response
D	100-OK response

Answer 5

At which response the endpoint is considered as healthy?

A	500-OK response
B	300-OK response
C	200-OK response
D	100-OK response

Quiz 6

At what point the endpoint is considered as unhealthy?

A	If the number of failures are lower than the no. of failure settings
B	If the number of failures are higher than the no. of failure settings
C	If the number of failures are equivalent to the no. of failure settings
D	None of the above

Answer 6

At what point the endpoint is considered as unhealthy?

A	If the number of failures are lower than the no. of failure settings
B	If the number of failures are higher than the no. of failure settings
C	If the number of failures are equivalent to the no. of failure settings
D	None of the above

India : +91-7847955955

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

sales@intellipaat.com

24X7 Chat with our Course Advisor