Microsoft Azure Administrator Associate Training

Implement Workloads and Security

Agenda

- What is Azure Site Recovery
- Azure Migrate
- Prepare Azure resources for disaster recovery of on-premises machines
- Discover and assess on-premises VMware VMs for migration to Azure
- Configuring Serverless Computing
- Azure Traffic Manager
- Azure Load Balancer
- Managing Role-Based Access Control

What Is Azure Site Recovery?

What Is Azure Site Recovery?

Azure Site Recovery is a disaster recovery and business continuity service that provides two types of functionality:

- **Replication:** It handles the synchronization of designated systems betw een a primary site that hosts your production w orkloads and a secondary site that gets activated if a disaster occurs.
- **Orchestration:** It provides orderly failover and failback betw een these tw o locations.

It provides support for the following three disaster recovery scenarios, depending on the location of the primary and secondary sites:

- **Failover and failback between two on-premises sites**
- **Failover and failback between an on-premises site and an Azure region**
- **Failover and failback between two Azure regions**

In addition, you can use Azure Site Recovery to migrate virtual machines to an Azure region by performing failover only.

This capability is available for Linux and Windows operating system instances running in on-premises locations, in Azure, or in the Amazon Web Services environment.

Azure Site Recovery: Benefits

It provides a number of capabilities that help you reach your business continuity goals. These capabilities include:

Storage replication	Orchestration of planned failover and failback	Orchestration of unplanned failover and failback	Orchestration of test failover
• Storage replication maintains the synchronization of disks between your production and DR. • Azure Site Recovery Services offer replication frequency in 30-sec or 15-min or 30-min intervals.	• With planned failover and failback, orchestration delivers an orderly transition process between your production and disaster recovery environments without any data loss.	• Orchestration also allows you to enforce the sequence of individual steps during failover and failback. • However, with unplanned failover and failback, there is a potential for data loss.	• Test failover typically takes place in an isolated network, making it possible to evaluate your disaster recovery approach without affecting the production environment.

Azure Site Recovery: Plan

- To implement orchestrated failover and failback, you need to create a recovery plan.
- A recovery plan identifies protected physical machines and virtual machines and dictates the order in which Site Recovery performs individual steps during failover and failback.
- Recovery plans support Azure Automation scripts and workflows in addition to manual steps.
- This provides a sufficient level of flexibility for more complex disaster recovery scenarios and also helps you achieve your RTO.
- Consider different sets of criteria in each of the following scenarios:

Replicating Hyper-V VMs to Azure

Replicating VMware VMs and physical servers to Azure

Replicating Azure VMs between two Azure regions

Azure Site Recovery:

Capacity Planning

- Microsoft offers the Azure Site Recovery Capacity Planner, which is available at: https://aka.ms/asr-deployment-planner
- This tool evaluates the existing workloads that you intend to protect, and based on this analysis it provides recommendations that are required to implement their protection.
- The tool operates in two modes:

Quick Planner

This mode requires you to provide general statistics representing the current capacity and utilization of your production site.

These statistics could include the total number of virtual machines, average number of disks per virtual machine, average size of a virtual machine disk, average disk utilization, total amount of data that needs replication, and average daily data change rate.

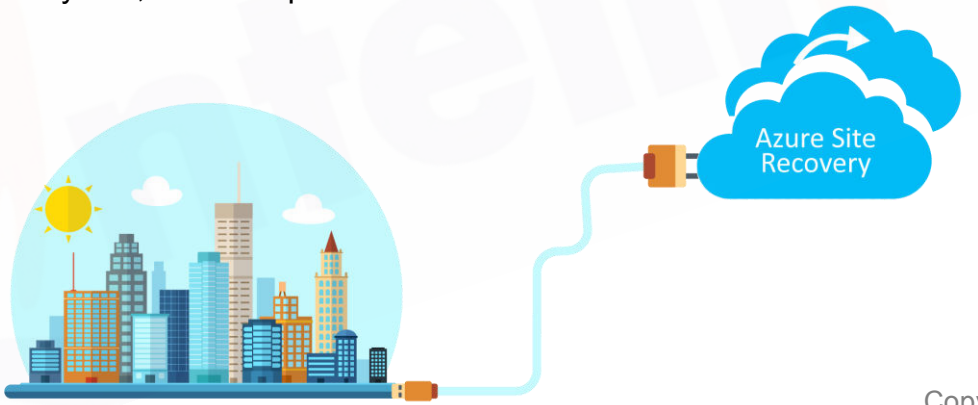
Detailed Planner

This mode requires you to provide capacity and utilization data for each virtual machine that you intend to protect.

This data could include the number of processors, memory allocation, number of network adapters, number of disks, total storage, disk utilization, and the operating system that is running in the virtual machine.

Azure Site Recovery: Supported Workloads

- Azure Site Recovery can integrate with Windows Server applications (Exchange Server, Database Servers, SharePoint, SQL Server, and Microsoft Dynamics CRM)
- Also, it can integrate with third-party server software from vendors such as Oracle, SAP, IBM, and Red Hat.
- This integration considerably simplifies building recovery plans, which protect the systems that host these products.
- Similarly, you can configure servers that host core infrastructure components, such as AD DS or DNS, to replicate from a primary site to a secondary site, either on-premises or in Azure.



Azure Site Recovery: Migrating

You can deploy Site Recovery to replicate on-premises VMs and physical servers and to migrate them.

When you replicate, you configure on-premises machines to replicate on a regular basis to Azure.

- When an outage occurs, you fail the machines over from the on-premises site to Azure and access them from there.
- When the on-premises site is available again, you fail back from Azure.

When you use Site Recovery for migration, you replicate on-premises machines to Azure.

- Then you fail them over from your on-premises site to Azure and finish up the migration process. There's no failback involved here.

Azure Site Recovery: Migrating

Using Azure Site Recovery, you can:

Migrate on-premises Hyper-V VMs, VMware VMs, and physical servers to Azure.

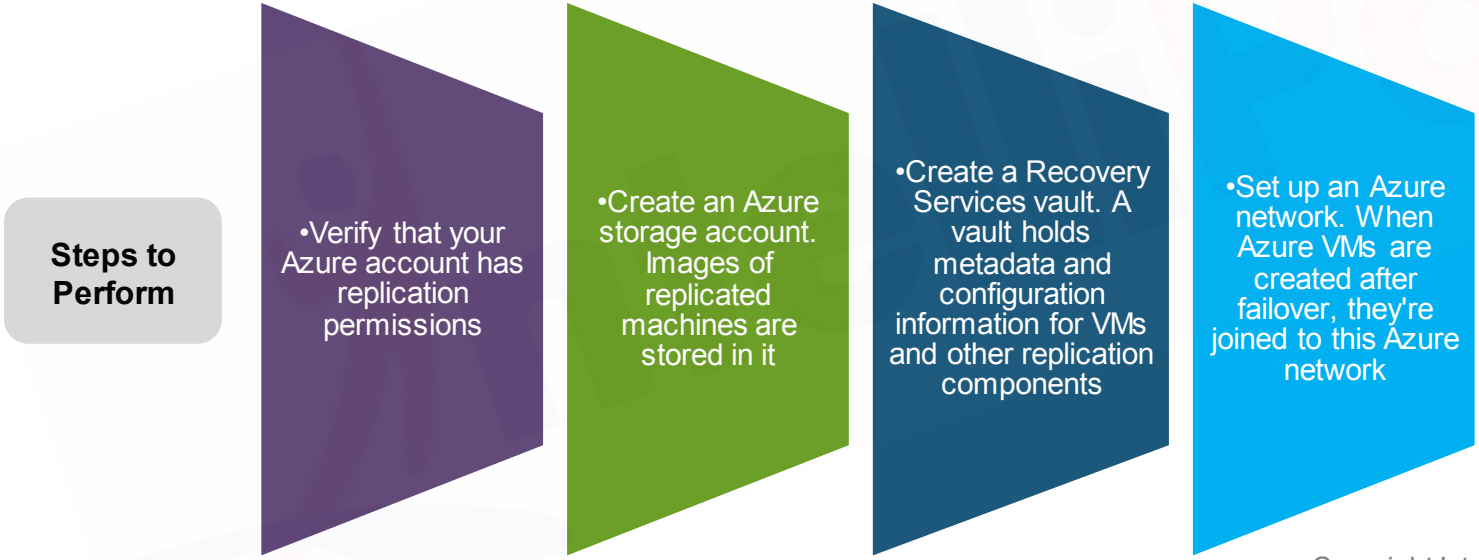
After the migration, workloads running on the on-premises machines will be running on Azure VMs.

Migrate Azure VMs between Azure regions.

Migrate AWS Windows instances to Azure VMs.

Preparing Azure Resources for Disaster Recovery of On-premises Machines

Azure Site Recovery contributes to your **business continuity and disaster recovery (BCDR)** strategy by keeping your business apps up and running during planned and unplanned outages. **Site Recovery** manages and **orchestrates disaster recovery** of on-premises machines and **Azure virtual machines (VMs)**, including **replication**, **failover**, and **recovery**.



Discovering and Assessing On-premises VMware VMs for Migration to A

Azure Migrate services assess on-premises workloads for migration to Azure.

Prerequisites

VMware:

VMs that you plan to migrate must be managed by vCenter Server running versions 5.5, 6.0, or 6.5. Additionally, you need one ESXi host running version 5.5 (or higher) to deploy the collector VM.

vCenter Server account:

You need a read-only account to access the vCenter Server. Azure Migrate uses this account to discover on-premises VMs.

Permissions:

On the vCenter Server, you need permissions to create a VM by importing a file in .OVA format.

Discovering and Assessing On-premises VMware VMs for Migration to A

Azure Migrate services assess on-premises workloads for migration to Azure.

Steps to Perform

Create an account for VM discovery.

Sign in to the Azure portal.

Create a project.

Download the collector appliance.

Create the collector VM.

Run the collector to discover VMs.

Create and view an assessment

Hands-on

Hands-on

- Create Site Recovery Services
- Enable replication between two regions for the VM
- Perform failover and failback

Configuring Serverless Computing

Routing Custom Events to Web Endpoint with the Azure Portal and Event Grid

Azure Event Grid is an event service for the cloud.

Perform these steps:

Managing a Function App in the Azure Portal

In Azure Functions, a function app provides the execution context for your individual functions. Function app behaviors apply to all functions hosted by a given function app.

Perform these steps:

In the search bar at the top of the portal, type the name of your function app and select it from the list.

Favorite Functions in the portal

- Log in to the Azure portal
- Click on the arrow at the bottom left to expand all services, type Functions in the Filter field, and then click on the star next to Function Apps
- Close the menu, scroll down to the bottom to see the Functions icon, and click on it to see a list of all your function apps. Click on your function app to work with functions in this app

Function Apps settings tab

- The Settings tab is where you can update the Functions runtime version used by your function app. It is also where you manage the host keys used to restrict HTTP access to all functions hosted by the function app

Platform features tab

- Function apps are run, and are maintained, by the Azure App Service platform. As such, your function apps have access to most of the features of Azure's core web hosting platform. The Platform features tab is where you access many features of the App Service platform that you can use in your function apps

Managing a Function App in the Azure Portal

Further, we can focuses on the following App Service features in the Azure portal that are useful for functions:

App Service editor (to modify)

Application settings (to configure and manage framework versions, remote debugging, app settings, etc.)

Console (In-portal console is an ideal developer tool to interact with function app from the command line)

Advanced tools (Advanced tools for App Service called Kudu provide access to advanced administrative features of your function app)

Deployment options (Functions lets you develop your function code on your local machine)

Cross-origin Resource Sharing (CORS) (to prevent malicious code execution in your services; App Service blocks call to your function apps from external sources)

Authentication (App Service supports Azure Active Directory authentication and signs in with social providers, such as Facebook, Microsoft, and Twitter)

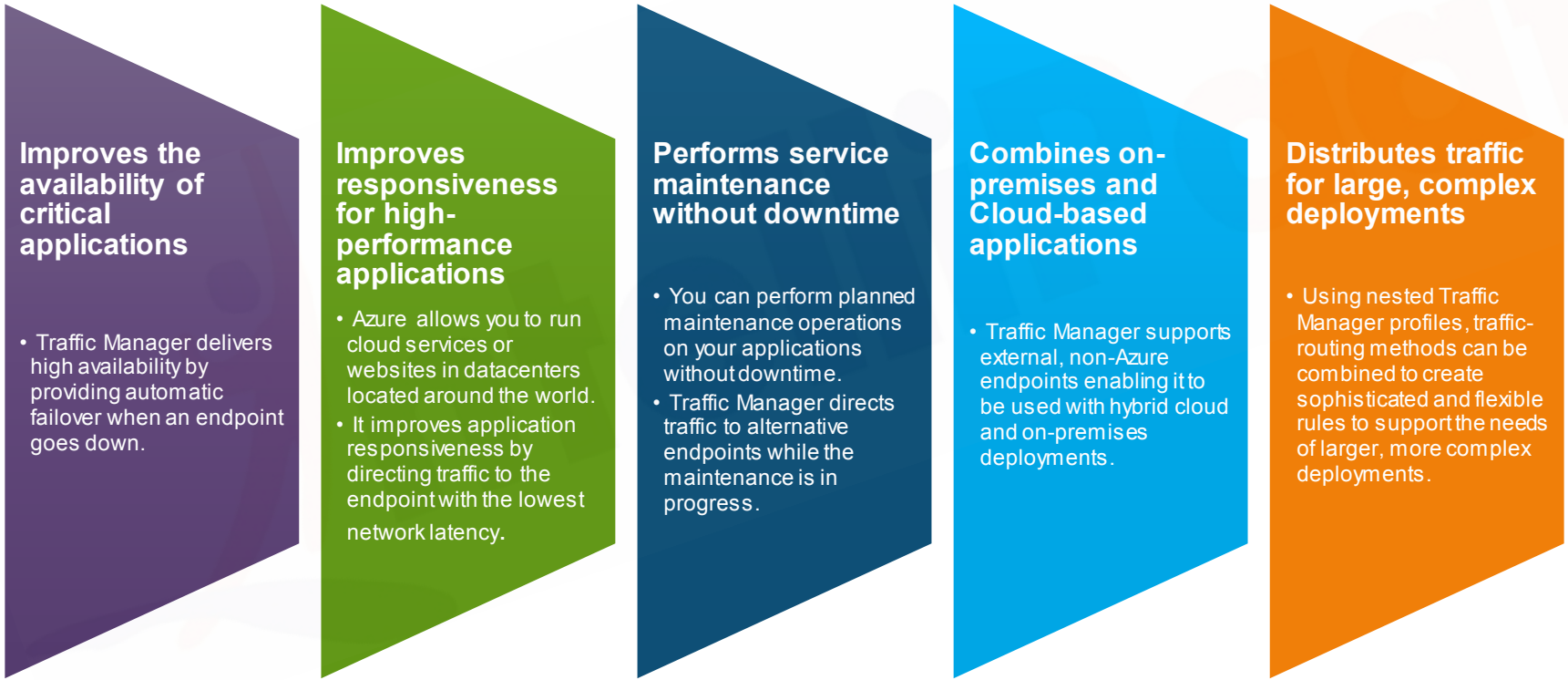
API definition (API definition lets you configure and describe our API)

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 the Traffic Manager include Azure VMs, Web Apps, and cloud services.
- You can also use the 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 Does It Work?

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 endpoints directly.

Azure Traffic Manager:
Azure Endpoints

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

Web Apps

PublicIPAddress Resources

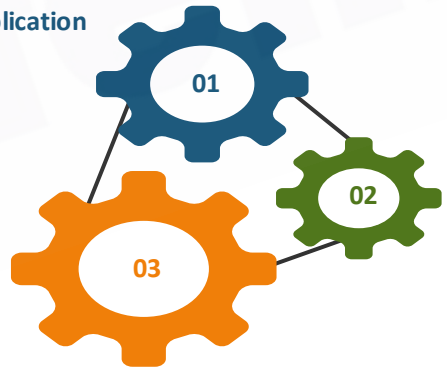
The PublicIPAddress must have a DNS name assigned to be used in a Traffic Manager profile.

- 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:

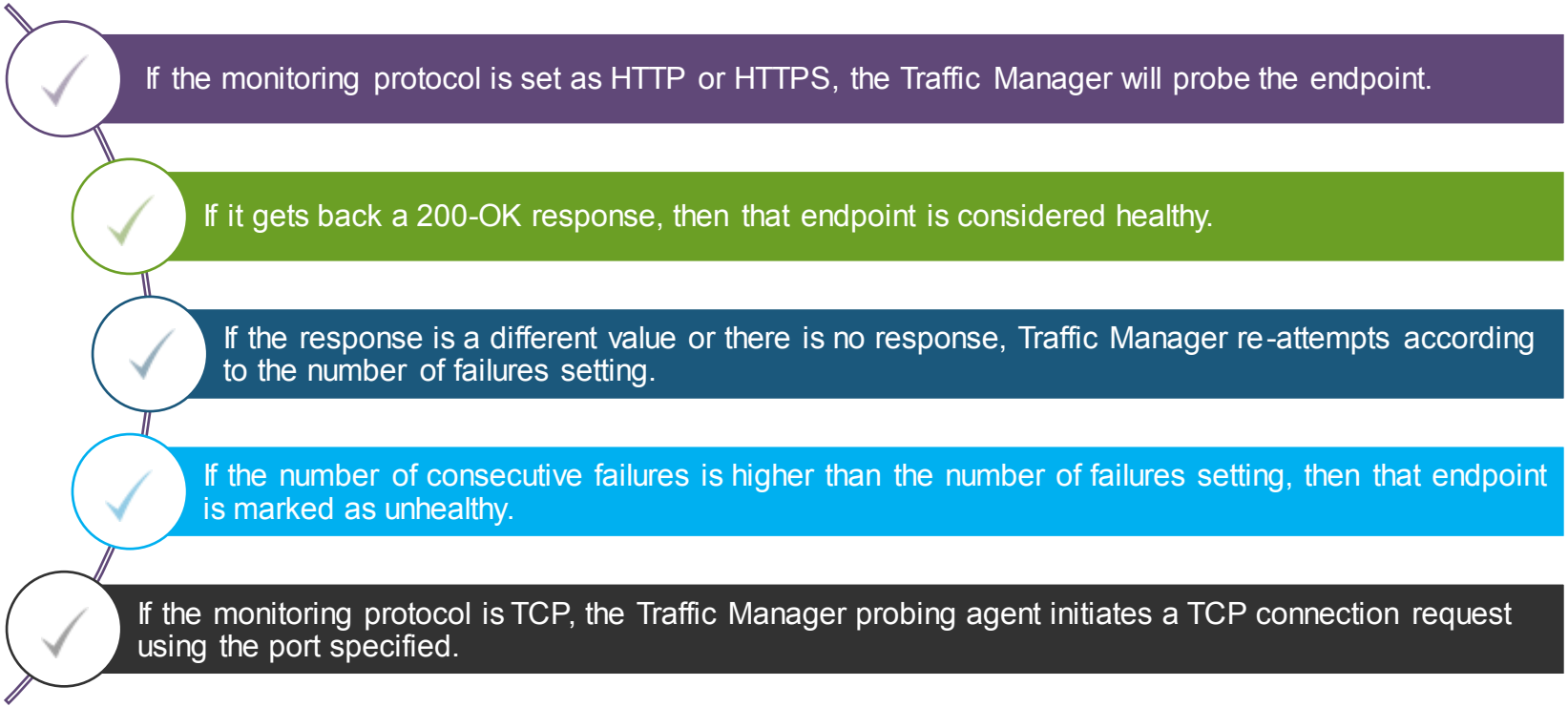
1. In either an active–active or active–passive failover model, use Azure to provide increased redundancy for an existing on-premises application



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.

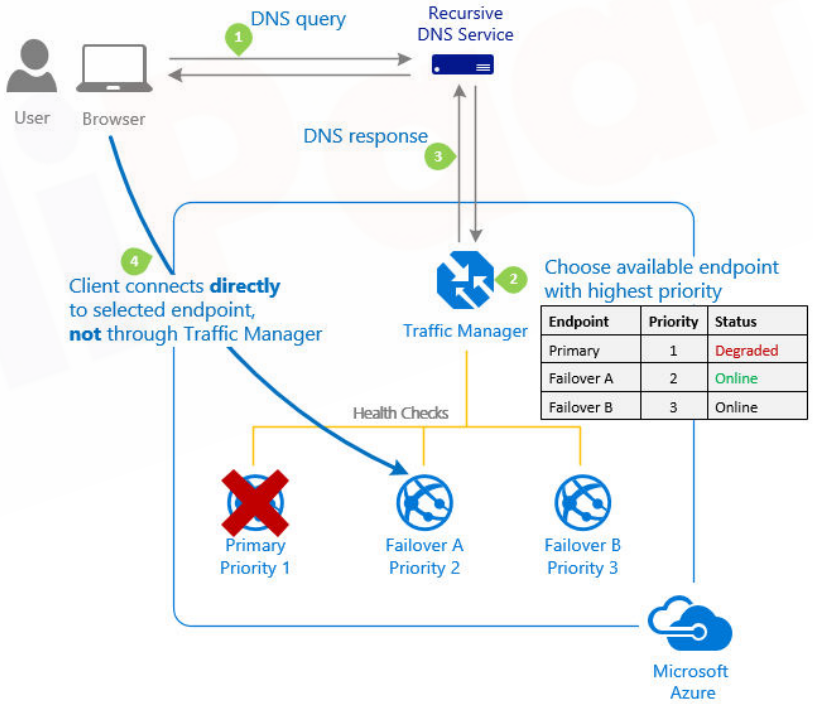
Azure Traffic Manager: Endpoints Monitoring



Azure Traffic Manager:
Routing Methods

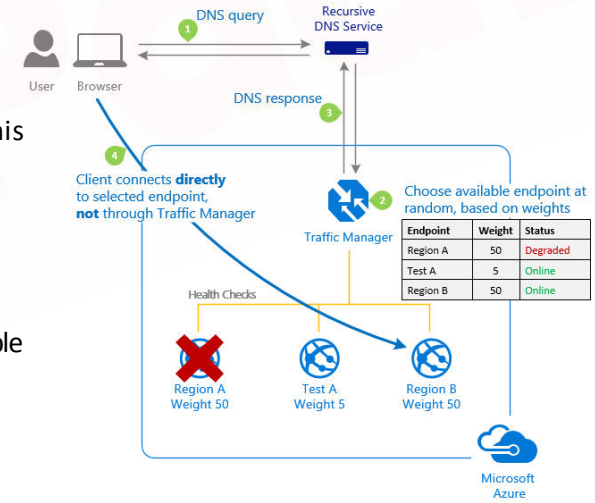
Azure Traffic Manager:
Priority Traffic-routing Method

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



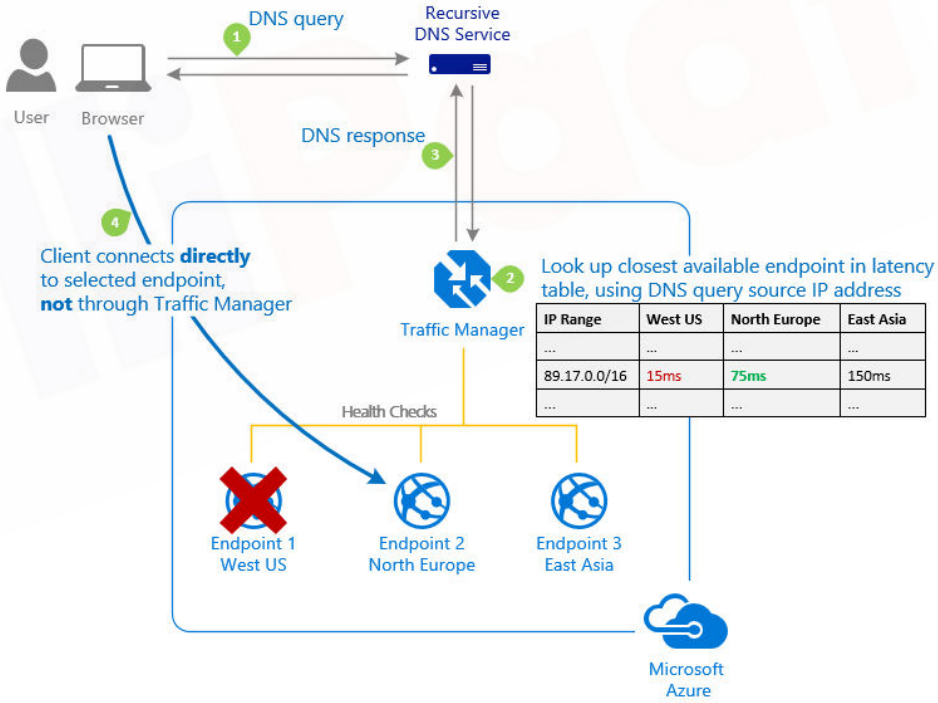
Azure Traffic Manager: Weighted Traffic-routing Method

- 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. the Traffic Managers uses a default weight of '1'. This parameter is optional.
- For each DNS query received, the 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

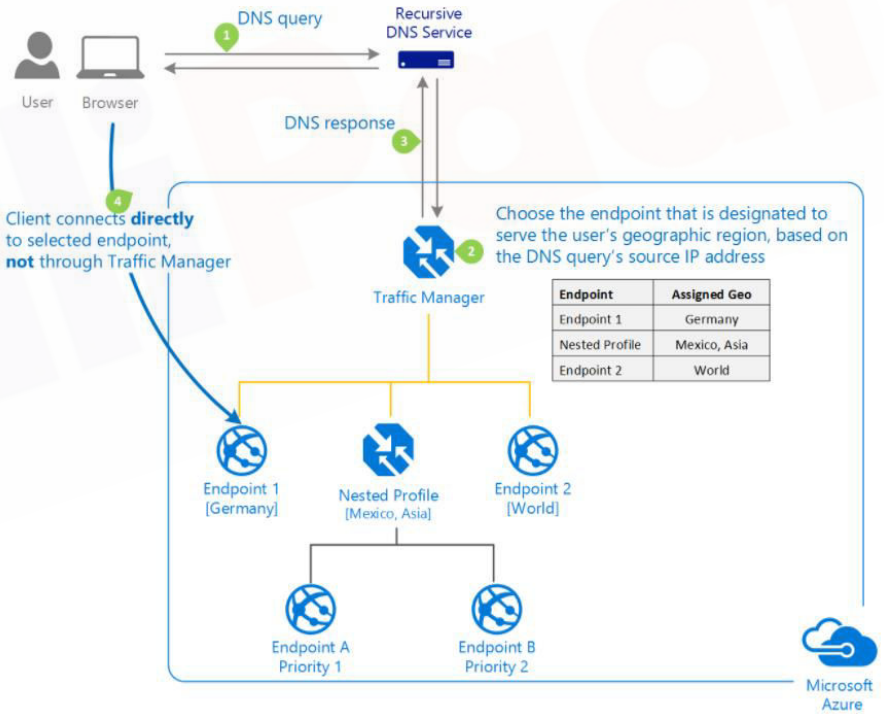
- Deploying endpoints in two or more locations across the globe, to route the traffic to the location that is the 'closest.'
- The ‘performance' traffic-routing method determines the closest endpoint by measuring network latency.
- Traffic Manager chooses an available endpoint in the Azure datacenter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



Azure Traffic Manager: Geographic Traffic-routing Method

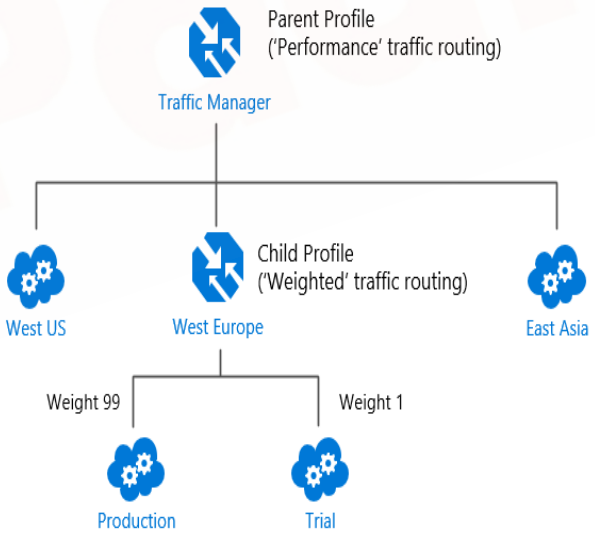
- Using geographic traffic-routing method, users are directed to specific endpoints based on which geographic location their DNS query originates from.
- Examples include:
  - Complying with data sovereignty
  - Localization of content
  - User experience and measuring traffic from different regions

  When a region or a set of regions is assigned to an endpoint, any requests from those regions get 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 the 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 the Traffic Manager using the priority traffic-routing method.
- Configure two Web Servers using the priority traffic-routing method.
- Failover the traffic from primary to secondary web servers.

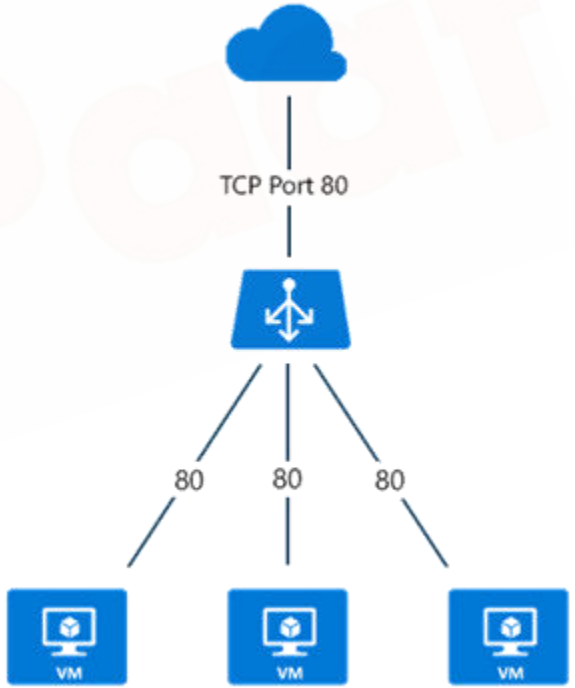
Azure Load Balancer

What Is Azure Load Balancer?

- Azure Load Balancer delivers high availability and network performance to your applications.
- It is a layer 4 (TCP and 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 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.
- 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

- 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.
- The load balancing decision is made per flow, based on the:

Source and Destination IP Addresses	Source and Destination Ports	Protocol

- HA ports help 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.
- 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 the port number.

Azure Load Balancer:
Why Use HA Ports?

- You can use 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, frontend and backend configurations 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

- Connect an on-premises network to a Microsoft Azure virtual network
  - Prepare your on-premises network
  - Create the cross-premises virtual network in Azure
  - Run PowerShell
  - Configure your on-premises VPN device to connect to the Azure VPN gateway.

Hands-on

Hands-on

- Configure an availability set with two fault domains
- Launch two web servers in the availability set
- Configure Load Balancer
- Access web servers using Load Balancer

Managing Role-based Access Control (RBAC)

Managing Role-based Access Control (RBAC)

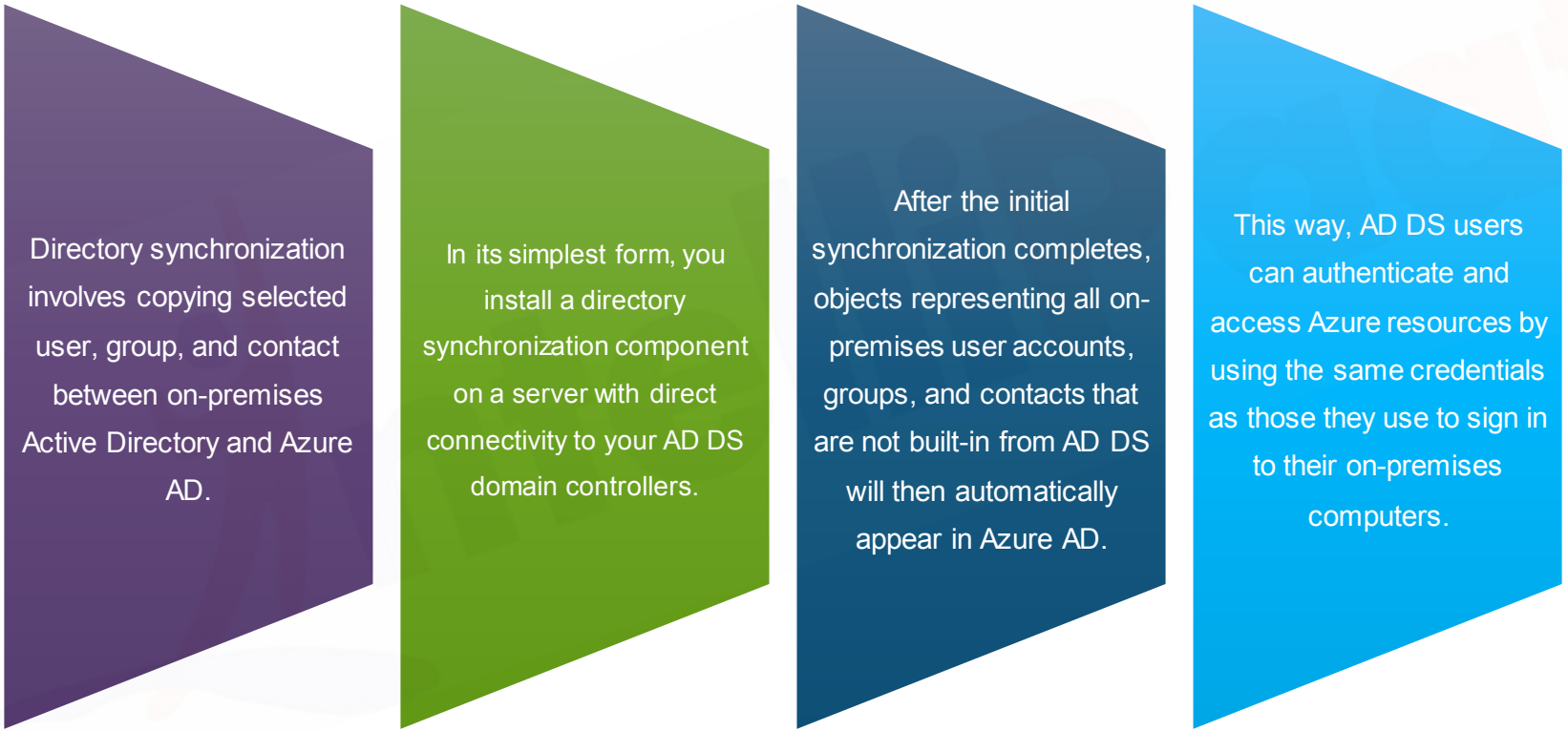
- RBAC enables fine-grained access management for resources that exist in an Azure subscription.
- By using RBAC, you can implement delegated management of cloud resources.
- For example, you can allow your development team to create their own virtual machines, but limit virtual networks to which those machines can be connected.
- RBAC has three basic built-in roles that apply to all resource types:

Multi-factor Authentication

- Azure Multi-Factor Authentication (MFA) adds an additional security layer in the authentication process by requiring more than one method of authentication to identify the user identity.
- Usernames and passwords are still required to sign in to access data and applications, but an additional access method can be added as a second factor of authentication.
- Multi-factor authentication combines such as a password or a PIN.

- You can authenticate via a phone call.
- You can authenticate via a text message.
- You can authenticate using a third-party OAuth token.

Directory Synchronization



Hands-on

Hands-on

- Configure Azure AD
- Create a user in Azure AD
- Login via Azure AD
- Enable MFA

QUIZ

Quiz 1

Azure site recovery is_____?

A	a disaster recovery and business continuity service that provides replication and orchestration
B	a site recovery service which provides automation in your service
C	a service which helps only in fault tolerance of your service
D	a service used only to recover from the disaster

Answer 1

Azure site recovery is_____?

A	a disaster recovery and business continuity service that provides replication and orchestration
B	a site recovery service which provides automation in your service
C	a service which helps only in fault tolerance of your service
D	a service used only to recover from the disaster

Quiz 2

Does Site Recovery encrypt replication?

A	Yes
B	No

Answer 2

Does Site Recovery encrypt replication?

A	Yes
B	No

Quiz 3

Capacity Planner helps in _____?

A	evaluating the capacity of your cloud storage and provide you stats and prediction based on your usage.
B	evaluating your server usage and do the fault tolerance
C	evaluating the existing workloads that you intend to protect, and based on this analysis, it provides recommendations that are required to implement the protection.
D	evaluating the amount of workload and allot the storage according to the required need.

Answer 3

Capacity Planner helps in _____?

A	evaluating the capacity of your cloud storage and provide you stats and prediction based on your usage.
B	evaluating your server usage and do the fault tolerance
C	evaluating the existing workloads that you intend to protect, and based on this analysis, it provides recommendations that are required to implement the protection.
D	evaluating the amount of workload and allot the storage according to the required need.

Quiz 4

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 4

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 5

IntelliPaat

What does traffic manager uses?

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

Answer 5

IntelliPaat

What does traffic manager uses?

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

Quiz 6

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

A	Yes
B	No

Answer 6

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

A	Yes
B	No

Quiz 7

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 7

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 8

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 8

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 9

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 9

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

24/7 Chat with Our Course Advisor