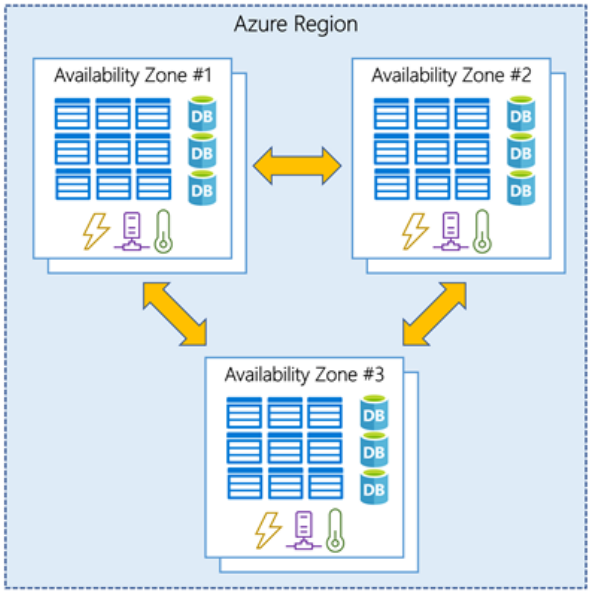
AZ-900 Revision Chapter - 2 : Understand Core Azure Services

Skill 2.1: Understand the core Azure architectural components

Geographies (Countries)
USA, Europe, Asia
Regions (Data Centres)
Central US, East US, UK West, UK East...
Data Centre (Split into Zones with separate power, cooling etc..)
Availability Zone 1, Availability Zone 2...

Azure Geographies/Regions
Boundaries called geographies. Geography boundary can be a country. Countries regulations can dictate this. i.e US Geography, Canada Geography, UK Geography....
Geography is split into 2 or more Regions, typically hundreds of miles apart.
Customers encouraged to replicate data to a region for disaster recovery, data loss.
Region Pairs. Each region is paired with another a few hindred miles away.
Supported Regions
Central US
East US
Region has Availability Zones (within Data Centres)



Data centres have their own Availability zone. Each isolated with own power supply, network, cooling system and water supply. This is for infrastructure.
Currently available are, vms, vm scale sets, managed disks, load balancers, public IP address,
Zone redundant storage, **SQL databases**, **Event hubs**, **Service vpn**, V**PN gateway, Application gateway,**
App Service environments.
Note Availability zones are not Availability Sets. Availability set is different locations for server racks.
Availability zones are zonal services or zonal-redundant services.
Zonal services are for vm's, managed disks and IP addresses. must explicitly deploy in multiple zones.
Zone-redundant services are created on setup. i.e SQL databases. Azure will take care of replicating data once setup.

Azure Resource Manager (ARM)

ARM is a service that allows you to create resources (vm's, Databases, App services...), checks that you're authorised to do so and talks to the resource provider. Controls resources. The command line and Portal interact with ARM using the same API.

Azure portal
Command line
Visual studio
--> Resource Manager API
Azure
--> ARM -->
Resource Povider
Azure
--> Resources (VM's, SQL, a

ARM uses JSON called ARM Templates
ARM allows you to easily deploy multiple Azure resources at once
ARM makes it possible to reproduce any deployment with consistent results at any point in the future
ARM allows you to create declarative templates for deployments instead of requiring you to write and maintain complex deployment scripts
Arm makes it possible to set up dependencies so that your resources are deployed in the right order every time.

Resource groups

Logical container for Azure services.
Resource can only exist in one resource group.
Useful to group all resources for one micro service etc. You can see all costs for the micro service.
Could also be grouped by department. Up to you how you use it.
Note. Subscription is the same as account
TAGS; you can apply one or more tags to a resource. This way, you can group them as in the resource group. Resource tags also appear in billing (exam note).

Skill 2.2: Describe some of the core products available in Azure

Azure Compute Products

There are four common techniques for performing compute in Azure:

- Virtual machines
- Containers
- Azure App Service
- Serverless computing

Azure Virtual Machines. Software-based computer running on a physical machine called the HOST.
Has disk space, memory and CPU power. Host computer runs software caller a **hypervisor** which runs many vm's and these are commonly referred to as GUESTS.
Vm's can run different operating system than the host.
By creating a compute resource (Need to play) you are creating a vm. This is an IaaS offering.
This is now in a rack in the data centre.
VM IS NOW susceptible to DOWNTIME
a) Planned Maintenance. Things like windows updates Will not affect your machine unless the update requires a reboot.
Azure monitors the health of vm's. If one becomes unhealthy, Azure will move data, memory to a new one, so there may be a pause. If the move fails, then you will get unexpected downtime.
TO FIX THIS, you should use Availability Sets. We have **Update Domains** and **Fault**

Domains.

Fault Domains

This denotes a physical rack in the data centre. By default, Azure will provide 2 in an availability set. If one goes down, then the other will still work fine.

Update Domains

This denotes a vm in the rack. By default, Azure will provide 5 vms in an availability set. These are spread around the Fault Domain. Each vm will be updated in turn with a 30 minute pause until it updates the next.

Notes on understanding.

Fault domain is rack number.

Update Domain is the update number on an Fault domain that hold the vm's. Update domain numbers are unique per Fault domain, but can be the same across Fault domains.

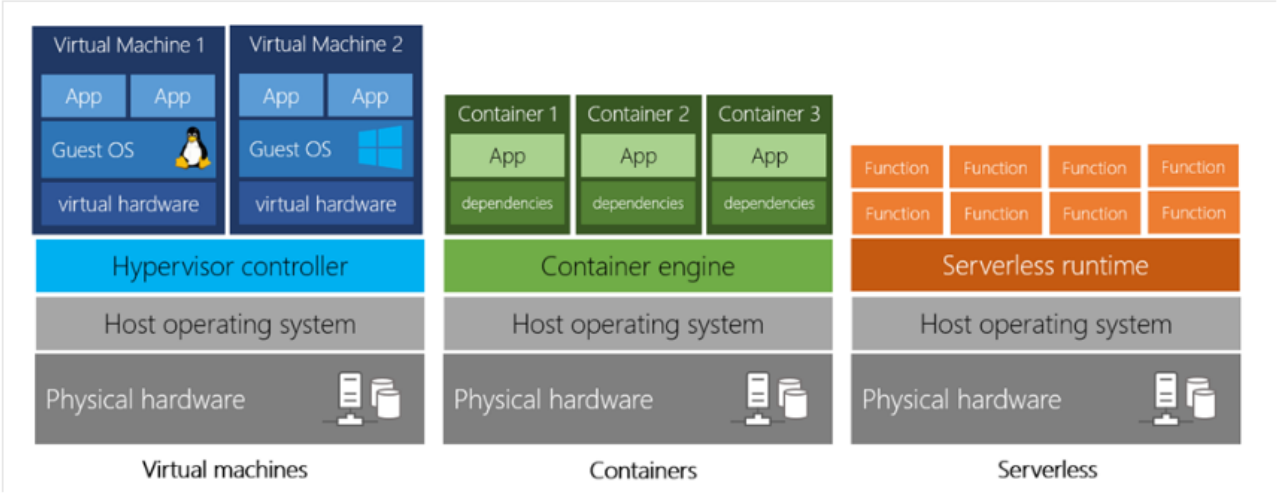
You can see this on the Portal under AvailabilitySets\WebAvailabilitySet\Overview

Issues with Availability sets is cost of increasing and issues with connecting to databases

Scale Sets is the answer to letting Azure increase and decrease vm's depending on usage.

Scale sets are compatible with availability zones. Rules can be used for CPU, disk usage, network usage..

Auto Scale uses elasticity for automatic increase/decrease vm's...



Containers in Azure

A container is created using a zipped version of an application called an image. We have used this for creating ArevTest environments. Computer needs a container runtime installed on it. Most popular is called **Docker**. Each container is isolated so it's secure. Has it's own network, storage etc..

Azure Container Instances is a PaaS service that that has minimal configuration. You pay for memory and CPU, not the vm. Can run multiple containers in ACI. ACI doesn't scale well. Use **Kubernetes** instead. It is a Container Orchestration Service. Kubernetes creates containers in a pod. The computer that Kubernetes pods run on is called a node or a worker. The entire environment of the master and all of it's nodes is called a kubernetes cluster. Azure Kubernetes Cluster. AKS creates the master and all of the nodes for you.

PaaS container hosting has Web App for Containers, a feature of Azure App Service. You pay for Web App Containers as it's running on a VM in App Service. It is part of an **App Service Plan**. App Service allows you to scale. Authentication is easy for PaaS for social media, google etc..

What is Azure App Service?

Azure App Service is a platform-as-a-service (PaaS) offering in Azure that is designed to host enterprise-grade web-oriented applications. You can meet rigorous performance, scalability, security, and compliance requirements while using a fully managed platform to perform infrastructure maintenance.

Azure Networking Products

Loosely-coupled architecture (micro services)
3 tiers for Websites, Web Tier, Middle(application) Tier and Data Tier. (an N-Tier design)
Web Tier is running Azure App Service (PaaS offering)
Middle Tier is running in an Azure Virtual Machine
Data Tier could be .....
(each of these are running on a separate Azure service, but need to communicate.
Azure Virtual Network is often called a VNet. Contains network interface card (NIC), IP address...
You can break up a VNet into multiple subnets. Default is 10.0.0.0 address range. 256 IP addresses per subnet. (251 is we ignore the reserved ones).
SubNet 1 = Web Tier 10.0.1.0/24, SubNet 2 = Middle Tier 10.0.2.0/24, SubNet 3 = Data Tier 10.0.3.0/24
Remember, you can't use a vm unless you have a network associated with it.
Web Tier has public facing IP address. for PaaS, Azure does it for you. Not for IaaS.
Azure load balancer. If you have 3 IP Addresses for 3 vm's then you can't control who uses which vm.
With a load balancer, there is one IP Address and Azure creates a VNet for the 3vm's and can manage the load for you. (Azure Load Balancer). Load Balancers can also sit within other tiers.
Azure Application Gateway is a load balancer designed for HTTP traffic.
It can, route traffic to specific vm or pool bases on URL
. use cookies to ensure routed to the same vm where vm contains same static info on the user
. display customised error pages with company logos
. handle SSL traffic to stop application tiers from decrypting
You can add Web Application Firewall (WAF) to Application Gateway.
VPN Gateway. This connects your on-premise to a VNet using virtual private network (VPN).
Azure Content Delivery Network. (CDN). Delivers large files or streaming content over the internet.
Stores a cache version of files on a **point-of-presence (POP)** server on edge of network. edge servers.
Time-To-Live (TTL) is how long it keeps it. Default is 7 days.
Azure Trafic Manager is a Domain name system (DNS) -based system. Can configure end-points to make it faster and more reliable. End point can be on-premise or another CSP.
Rules can be Priority, Weighted, Performance, Geographic, Multivalue and SubNet.
As this is DNS based, the traffic does not go through Azure Traffic Manager.

Azure Storage Products.

Azure Blob Storage
Designed for unstructured data. 3 types of Blob
Block Blobs - Used to store files used in an application
Append Blobs - As above but are appended. Normally Log files etc..
Page Blobs - Used to store virtual hard drive (.vhd) files
These tend to be stored in containers. Just like directories/folders.

Hot storage tier - use often. Highest cost of storage, but access cost is low.
Cool storage tier - use rarely. Lower cost of storage, but access cost higher. Keep data for 30 days.
Archive Storage tier - long term storage. Lowest cost, but access is highest. Keep data for 180 days.
. Access is slow. Hot and Cool tier retrieval starts in milliseconds. Archive will start within 15 hours.
Azure Storage used to store data for i.e. On-premise move
Azure Storage Explorer is a free tool for above.
Large amount of data, Microsoft has Data Box. Online service called Data Box Edge.
Encrypt BitLocker.
Data Box Heavy can hold up to 1 petabyte of data.
Azure Queue Storage.
Needs a cloud based message queue. Not guaranteed an instant response.
Applications uses available for languages like, .Net, Java, Node.js, C++, python etc..

Azure Disk Storage

Disks on vms. Temporary storage. Lost for maintenance. To stop loss, use images on Azure Storage.
All Azure disks backed by page Blobs in Azure storage.
Unmanaged disks uses Azure Storage account in your Azure Subscription. You have to manage. Can cause issues if there are large volumes.
Managed disks are handled by Microsoft. Using managed disks on a separate scale unit removes single points of failure.
Azure Files
Cannot use Windows 7 or 2008. Needs to access port 445. Can be slow to access. To fix, use Azure File Sync.
Azure Database Products
Azure SQL Database
PaaS offering of SQL Server. 3 deployment options, single database, elastic pool and managed instance.
Single is a basic database that microsoft runs. 2 options, Database Transaction Unit (DTU) and VCore.
VCore is the more flexible, DTU more standard.
Elastic Pool is more than one database all managed by a single SQL Database server. SaaS offerings.
SQL database don't scale horizontally, unless you are using read-only.
Managed instance are database that are copied from on-premise to a private VNet and has a private IP address. Lift-and-shift. Uses Azure Database Migration Service (DMS).
Database on the cloud that are copied to a Azure SQL Database can be synchronised.
Azure Cosmos DB
Unstructured Database. Able to use Key-value, Column, Document and Graph NoSql database systems.
Easy and fast replication
Azure Marketplace and its usage scenarios
Bit like Google Play, Apple Store and Nuget. Click "Dreate a Resource" in Azure Portal.
All templates in Azure Marketplace are ARM templates.

Skill 2.3: Describe some of the solutions available on Azure

IoT (Internet of Things)

Azure IoT Hub. IoT devices can be added to IoT Hub. Iot Hub can send messages (Cloud-to-device) or C2D and back, D2C. You can route the messages to Event Hub, Azure Storage and Service Bus based on message contents. IoT creates a connection string for

authentication. Messages encrypted.
Can also send files for firmware. Each device has a twin in IoT Hub. Can add meta data to assist in batched reboots. Meta data stored as JSON.
For adding a large quantity of devices, IoT Hub Device Provisioning Service, or DPS.
You can route messages using Message Routing.
Standard has more functionality than basic. i.e. Device streams for streaming messages in near real time, C2D messaging, Device management, device twin and module twin and IoT edge for handling IoT Devices at the edge of the network where they reside.
B1 = $10, 400,000: B2 = $50, 6,000,000: B3 = $500, 300,000,000 messages per day.
Free = Free, 8,000: S1 = $25, 400,000: S2 = $250, 6,000,000: S3 = $2,500, 300,000,000.
Azure IoT Central. (Azure Stream Analytics routes messages to Power BI).
IoT Central is a SaaS offering for IoT devices. To create an IoT app, Click New Application and then Create Application. & days free trial, then PAYG. This gives you a Template. You have 3 roles for changing the Template. Application Administrator, full access and add users. Application Builder can edit the pages. And Application operator can just use them.
You can create rules which can in turn create web hooks. These web hooks can trigger tasks.
Device sets allow you to group the devices. Actions on Devie sets are called Jobs. Click on Jobs from the Main Menu to create.
Big Data and Analytics
Big data is defined as more data than you can analyse through convential means within a time frame.
Azure SQL Data Warehouse. Encrypted using Transparent Data Encryption (TDE) AES-256 encryption.
Two scaleable tiers, Gen1 and Gen2. Gen2 uses local disk caching for improved performance.
Azure Data Lake Storage. Data Lake stores any data, but puts related data into containers.
2 common access modes, Object-based (such as Azure Blob Storage) or file-based.
Data Lake Storage Gen2 organises objects into a system of directories and makes object-based and file-based available in the same Data Lake.
Like Azure Blob Storage, Data Lake Storage has Hot, Cool and Archive tiers. Once data is in SQL Data Ware House or Azure Data Lake, you can use Azure HDInsight or Azure data-bricks.
Azure HDInsight. This makes it possible to easily create and manage clusters of computers on a common framework designed to perform distributed processing of big data. Micorsofts version of Hadloop.
Artificial Intelligence.
AI now called Artificial Narrow Intelligence.
Azure Data-Bricks. Data modeling for Machine Learning methods. Data-bricks exists in a Workspace.
Click Launch Workspace and then Daya Bricks. New cluster.
Create Notebook. These are a powerful way to present and interact with data that is related.
Enter queries like SQL stuff. Data bricks creates a job and runs it. uses Serverless computing.
Azure Machine Learning Service. This is a cloud based service for building ML models.
Uses Python.
This can be run on-premise unlike data-bricks. Also uses notebooks. When you train models in Machine Learning Services, a Docker container is created and your model runs inside it.
Azure Machine Learning Studio. Is a SaaS offering. Open using https://studio.azureml.net.
Free and Standard Tiers. (Not going any further on notes unless Questions or Course mentions it).

Serverless Computing.

Only pay when the code is running on the vm. Serverless services include Azure Databricks and Azure Machine Learning Services. Azure Functions are serverless compute, Azure Logic Apps are serverless workflows and Azure Event Grid are serverless event routing.
Azure Functions. Create programs to run without deploying. Can create Function App in Microsoft Visual Studio, Microsoft Visual Studio Code, Maven for Java, Python Command Line, Azure Command Line Interface (CLI) and Azure Portal. Functions are run by a trigger. After run has finished, you choose what happens next called an Output Binding.
Azure Logic Apps. Similar to Azure Functions in the they are kicked off by a trigger. Do not need to write code. Connectors, triggers and actions. Created in Azure Portal. Connect, select the trigger and then the corresponding action(s).
Azure Event Grid. Logic app is like Arev pooling. The Azure event is live a eventhandler. An action can be called for an event.

Skill 2.4: Understand Azure management tools

Azure Portal. This portal has ARM in the back-end. Dashboard is full customizable. Basically, try it.

- **Azure portal** for interacting with Azure via a Graphical User Interface (GUI)
- **Azure PowerShell** and **Azure Command-Line Interface** (CLI) for command line and automation-based interactions with Azure. PowerShell Core and CLI can run on Linux, Macs and Windows.
- **Azure Cloud Shell** for a web-based command-line interface
- **Azure mobile app** for monitoring and managing your resources from your mobile device. iOS or Android phone or tablet. (Not create)

Azure and **PowerShell.** PowerShell uses az commands. PowerShell is cross platform. Can use Linux, Mac as well as Windoes. Need to install first. Runs as Administrator in Windows, Superuser elsewhere.
Good for scripting.
Azure CLI (Command Line Interface). Can be programmed in Python, Ruby... Cross platform like powershell. Has interactive mode. Simply type in "az interactive".
Azure Advisor. (Offers advice on availability, security, performance and cost. Available for Azure vms, availability sets, application gateways, App Service applications, SQL server and Azure Redis Cache and many more..)

STORAGE

Compare on-premises storage to Azure data storage

The following table describes the differences between on-premises storage and Azure data storage.

COMPARE ON-PREMISES STORAGE TO AZURE DATA STORAGE

Needs	On-premises	Azure data storage
Compliance and security	Dedicated servers required for privacy and security	Client-side encryption and encryption at rest
Store structured and unstructured data	Additional IT resources with dedicated servers required	Azure Data Lake and portal analyzes and manages all types of data
Replication and high	More resources, licensing, and	Built-in replication and redundancy

Needs	On-premises	Azure data storage
availability	servers required	features available
Application sharing and access to shared resources	File sharing requires additional administration resources	File sharing options available without additional license
Relational data storage	Needs a database server with database admin role	Offers database-as-a-service options
Distributed storage and data access	Expensive storage, networking, and compute resources needed	Azure Cosmos DB provides distributed access
Messaging and load balancing	Hardware redundancy impacts budget and resources	Azure Queue provides effective load balancing
Tiered storage	Management of tiered storage needs technology and labor skill set	Azure offers automated tiered storage of data

NETWORKING

Let's break this down.

What's an Azure region?
A *region* is one or more Azure data centers within a specific geographic location. East US, West US, and North Europe are examples of regions. In this instance, you see that the application is running in the East US region.

What's a virtual network?
A *virtual network* is a logically isolated network on Azure. Azure virtual networks will be familiar to you if you've set up networks on Hyper-V, VMware, or even on other public clouds. A virtual network allows Azure resources to securely communicate with each other, the internet, and on-premises networks. A virtual network is scoped to a single region; however, multiple virtual networks from different regions can be connected together using virtual network peering.
Virtual networks can be segmented into one or more *subnets*. Subnets help you organize and secure your resources in discrete sections. The web, application, and data tiers each have a single VM. All three VMs are in the same virtual network but are in separate subnets.
Users interact with the web tier directly, so that VM has a public IP address along with a private IP address. Users don't interact with the application or data tiers, so these VMs each have a private IP address only.
You can also keep your service or data tiers in your on-premises network, placing your web tier into the cloud, but keeping tight control over other aspects of your application. A *VPN gateway* (or virtual network gateway), enables this scenario. It can provide a secure connection between an Azure Virtual Network and an on-premises location over the internet.
Azure manages the physical hardware for you. You configure virtual networks and gateways through software, which enables you to treat a virtual network just like your own network. You

choose which networks your virtual network can reach, whether that's the public internet or other networks in the private IP address space.

What's a network security group?
A *network security group*, or NSG, allows or denies inbound network traffic to your Azure resources. Think of a network security group as a cloud-level firewall for your network.
For example, notice that the VM in the web tier allows inbound traffic on ports 22 (SSH) and 80 (HTTP). This VM's network security group allows inbound traffic over these ports from all sources. You can configure a network security group to accept traffic only from known sources, such as IP addresses that you trust.

Resiliency refers to a system's ability to stay operational during abnormal conditions.

These conditions include:

- Natural disasters
- System maintenance, both planned and unplanned, including software updates and security patches.
- Spikes in traffic to your site
- **Threats made by malicious parties, such as distributed denial of service, or DDoS, attacks**

A *load balancer* distributes traffic evenly among each system in a pool. A load balancer can help you achieve both high availability and resiliency.
Say you start by adding additional VMs, each configured identically, to each tier. The idea is to have additional systems ready, in case one goes down, or is serving too many users at the same time.
The problem here is that each VM would have its own IP address. Plus, you don't have a way to distribute traffic in case one system goes down or is busy. How do you connect your VMs so that they appear to the user as one system?
The answer is to use a load balancer to distribute traffic. The load balancer becomes the entry point to the user. The user doesn't know (or need to know) which system the load balancer chooses to receive the request.

What is Azure Load Balancer?

Azure Load Balancer is a load balancer service that Microsoft provides that helps take care of the maintenance for you. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) applications. You can use Load Balancer with incoming internet traffic, internal traffic across Azure services, port forwarding for specific traffic, or outbound connectivity for VMs in your virtual network.
there's no infrastructure or software for you to maintain. You define the forwarding rules based on the source IP and port to a set of destination IP/ports.

Azure Application Gateway

If all your traffic is HTTP, a potentially better option is to use Azure Application Gateway. Application Gateway is a load balancer designed for web applications. It uses Azure Load Balancer at the transport level (TCP) and applies sophisticated URL-based routing rules to support several advanced scenarios.

This type of routing is known as application layer (OSI layer 7) load balancing since it understands the structure of the HTTP message.

Here are some of the benefits of using Azure Application Gateway over a simple load balancer:

- **Cookie affinity**. Useful when you want to keep a user session on the same backend server.
- **SSL termination**. Application Gateway can manage your SSL certificates and pass unencrypted traffic to the backend servers to avoid encryption/decryption overhead. It also supports full end-to-end encryption for applications that require that.
- **Web application firewall**. Application gateway supports a sophisticated firewall (WAF) with detailed monitoring and logging to detect malicious attacks against your network infrastructure.
- **URL rule-based routes**. Application Gateway allows you to route traffic based on URL patterns, source IP address and port to destination IP address and port. This is helpful when setting up a content delivery network.
- **Rewrite HTTP headers**. You can add or remove information from the inbound and outbound HTTP headers of each request to enable important security scenarios, or scrub sensitive information such as server names.

What is a Content Delivery Network?

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. It is a way to get content to users in their local region to minimize latency. CDN can be hosted in Azure or any other location. You can cache content at strategically placed physical nodes across the world and provide better performance to end users. Typical usage scenarios include web applications containing multimedia content, a product launch event in a particular region, or any event where you expect a high-bandwidth requirement in a region.

What is network latency?

Latency refers to the time it takes for data to travel over the network. Latency is typically measured in milliseconds.
Compare latency to bandwidth. Bandwidth refers to the amount of data that can fit on the connection. Latency refers to the time it takes for that data to reach its destination.

Use Traffic Manager to route users to the closest

endpoint

One answer is **Azure Traffic Manager**. Traffic Manager uses the DNS server that's closest to the user to direct user traffic to a globally distributed endpoint.

Compare Load Balancer to Traffic Manager

Azure Load Balancer distributes traffic within the same region to make your services more highly available and resilient. Traffic Manager works at the DNS level, and directs the client to a preferred endpoint. This endpoint can be to the region that's closest to your user.
Load Balancer and Traffic Manager both help make your services more resilient, but in slightly different ways. When Load Balancer detects an unresponsive VM, it directs traffic to other VMs in the pool. Traffic Manager monitors the health of your endpoints. When Traffic Manager finds an unresponsive endpoint, it directs traffic to the next closest endpoint that is responsive.