AZ-900: Microsoft Azure Fundamentals

Exam Cram Notes

Fourth Edition

Chapter 01: Introduction to Azure

Introduction

Microsoft's Cloud Platform, like Google and Amazon's Cloud Platforms, is Azure. It is usually a platform that lets us use Microsoft software. It simplifies our work by providing virtual machines, rapid data processing, analytical tools, and monitoring sensors. Azure pricing is also more straightforward and less expensive. It is known as "Pay as You Go," which means you only pay for the services when you use them.

What is Cloud Computing?

Cloud computing is the process of storing data and gaining access to machines via the internet. It is the internet-based delivery of various computer services such as servers, software, analytics, databases, and storage.

Benefits of Cloud Computing

We are all aware that Cloud Computing has significantly shifted traditional company thinking about IT resources. There are numerous advantages of using cloud computing. Here are a few examples:

- Cost
- Scalability
- Increase Speed and Agility
- Reliability
- Security

The Economy of Cloud Computing

The PAY AS YOU GO technique is the economic foundation of cloud computing. Users/Customers should only be required to pay for how they use cloud services. The users will undoubtedly benefit from it. Thus, everyone can benefit greatly economically from the Cloud. The removal of some indirect costs associated with assets like software licenses and support is another benefit. Users can access software applications in the cloud on a subscription basis for free because the cloud provider still owns the rights to the software-providing service.

Consumption-based Model

Two sorts of costs should be considered when contrasting IT infrastructure options. Operations Expenditures (OpEx) and Capital Expenditures (CapEx)

CapEx often involves a one-time, upfront expense to acquire or secure tangible resources. It includes constructing a new building, repaving the parking lot, constructing a data center, or purchasing a corporate vehicle.

OpEx, on the other hand, involves a one-time purchase of goods or services. It can be used to pay for convention center rentals, company car leases, and cloud service contracts.

Technical Terms

To comprehend Cloud Computing, you must first comprehend a few technical phrases.

- **High Availability (HA)** - You can achieve high availability for your servers by replacing a failed server with a new one as soon as possible. The number of VMs you set up to eventually cover in case one goes down determines how well HA works.
- **Fault Tolerance** - Fault tolerance refers to the fact that if there is a fault on the Azure side, it is promptly addressed by Azure with no downtime.
- **Disaster Recovery (DR)** - In the event of a catastrophic event, such as a cyber-attack. If something goes wrong with these important systems, you have a plan in place in DR to get your business back up and running.
- **Scalability** - Scalability in cloud computing refers to the capacity to easily and quickly add or remove resources in response to demand.
- **Elasticity** - Elasticity refers to the ability to dynamically expand or contract network resources in order to adapt to autonomous

working load changes and maximize resource utilization.

- **Agility** - The ability to react rapidly and efficiently to changes in the business environment is known as agility. The capacity to quickly design, test, and deploy business-driven software applications is often called agility.

Manageability in the Cloud

The alternatives for management are a key advantage of cloud computing. In this section, you will learn about two different types of manageability for cloud computing, both of which have great advantages.

Management of the Cloud

You may manage your cloud resources by managing the cloud. Within the cloud, you can:

- Deploy resources at the appropriate scale automatically as needed
- Remove the need for manual configuration by deploying resources based on a template that has already been configured
- Resources' conditions will be tracked, and failing ones will be replaced automatically
- To be informed about performance in real-time, receive automatic alerts based on preset metrics

Management in the Cloud

How you can manage your cloud environment and resources is referred to as management in the cloud. These are manageable:

- Using web portal
- Using command-line interface
- Using API
- Using PowerShell

Types of Cloud computing

Cloud computing is a broad word that refers to a set of services that provide organizations with a low-cost way to expand their IT capacity and usefulness.

Businesses can choose where, when, and how they employ cloud computing to ensure an efficient and dependable IT solution based on their individual needs.

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three basic cloud computing service models (SaaS). Although there are evident distinctions between the three and what they can offer a business in terms of storage and resource sharing, they can also interact to build a single cloud computing paradigm.

Software as a Service

Cloud providers take over both servers and code. Cloud providers host and maintain the applications and underlying infrastructure for SaaS and handle updates such as software upgrades and security patches. Users link the app over the internet, usually through their phone, tablet, or PC through their web browser.

This first service is Software as a Service (SaaS) and is considered the largest and most popular use of cloud computing today. It is continuing to grow as it replaces traditional on-device software with web-based alternatives. Rapidly moving programs to the cloud, often using a subscription-based model, and making the software browser-accessible, eliminates the need to install client software and, in many cases, makes it cross-platform and accessible on the broad set of devices that we use today. Some examples include Gmail, Google Drive, Power BI, Microsoft Office 365, etc.

Platform as a Service

Cloud computing platforms that provide an on-demand environment to build, test, deliver and manage software applications are called Platform as a Service. PaaS is designed to facilitate the fast development of web or mobile apps for developers without setting or maintaining the underlying server, storage, network, and database infrastructure needed for development.

Platform as a Service (PaaS) is a platform, which runs on a single VM and is designed to support the complete application life cycle, typically for website building, testing, deploying, managing, and updating. This service allows you to avoid the expense and complexity of buying, installing, and managing software licenses. Instead, you manage the applications and services you deploy, and the cloud service provider typically manages everything else. One example of such a service is the Azure App Service platform for hosting web apps and services, and the other is SQL in Azure, which provides an enterprise-grade cloud-based version of SQL Server in

the cloud. It includes Google, Microsoft Azure, Amazon Web Service (AWS), etc.

Infrastructure as a Service

An Infrastructure as a Service (IaaS) enables a server in the cloud or Virtual Machine (VM) instance that you would have complete control over. This offering is closer to an on-premises VM. IaaS requires you to manage the operating system and the virtual machine's disk and networking attributes. Hardware management is taken care of, and a remote desktop is utilized to manage the VM. IaaS is a great solution where multiple applications running on a single VM are needed to fulfill the needs of third-party software.

Serverless

Overlapping PaaS, serverless computing concentrates on creating application functionality without continually spending time maintaining the required server and infrastructure. The cloud provider is responsible for configuration, capacity planning, and server governance. The highly scalable and event-based serverless architectures only use resources when a particular task or trigger takes place.

Shared Responsibility Model

Understanding the shared responsibility model, which security tasks are handled by you, and which tasks are handled by the cloud provider is crucial as you investigate and assess public cloud services. Depending on whether the workload is hosted on software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), or in an on-premises datacenter, the workload responsibilities change.

Cloud Computing Deployments Models

There are three different types of Cloud Computing: Public, Private and Hybrid.

- Third-party computer services providers such as storage, software, and other services own and run the public cloud.
- A private cloud is a model that runs cloud resources within its own data center using the same legacy IT architecture.
- Hybrid clouds combine public and private clouds and technology to allow data and applications to be shared. The hybrid cloud provides greater versatility and allows further deployment
- The community cloud model allows the user to access the group of organizations for its services. It can provide a sharing mechanism, but its security is higher than a public cloud and lower than a private cloud.

What is Azure?

Microsoft Azure is a Public Cloud that is also known as Windows Azure. You can freely design, manage, and deploy applications in a massive, worldwide network using your favorite tools and frames. Azure is regarded as a provider of both IaaS and PaaS. Azure has approximately 100 services, ranging from virtual machine execution to developing new computing paradigms such as smart bots and mixed reality.

To utilize Azure, you must first create an account through “Azure.com” or with the assistance of a salesperson. Sign up for a free Azure account to get a free USD 200 credit and access to more than 25 free services.

Azure Market Place

Microsoft and its partners offer technical solutions and services in the Azure marketplace to help you build and extend Azure products and services. It has various services and applications like VMs, Templates, apps, Azure managed services, etc.

Physical Infrastructure

Data centers are the first component of Azure's physical infrastructure. The data centers are conceptually equivalent to huge corporate data centers. They are buildings with racks of resources and specialized power, cooling, and networking equipment.

Azure has data centers worldwide because it is a worldwide cloud service. These particular data centers, however, are not immediately reachable. To help you achieve resilience and dependability for your business-critical workloads, data centers are organized into Azure Regions or Azure Availability Zones.

You can interactively explore the underlying Azure architecture on the Global Infrastructure webpage.

Azure Data center

Suppose you purchased services in Azure such as SQL database, web hosting virtual machine, or one of the many services offered by Azure. All these services run on a physical infrastructure underneath some services. A physical facility that hosts these services is called a data center. It is used to host a group of network servers, and a typical data center has its power pooling and networking infrastructure.

Geography

Azure divides the world into geographies defined by geopolitical boundaries or country borders. Azure geography is a discrete market typically containing two or more regions that preserve data residency and compliance boundaries.

Global Footprint

Azure has more global regions than any other cloud provider, allowing it to scale to bring consumers worldwide closer to applications. Azure is offered in 58 different areas worldwide, with 140 of them in 140 different nations.

Regions

Azure resources are deployed through regions, which are geographical areas where Azure is available. It is a collection of data centers connected by a dedicated regional low-latency network with a latency-defined border.

How to Choose a Region?

When choosing a region, you need to think about three things mainly:

- **Location**- To reduce the latency, choose a region closest to the user
- **Features**- All features are not available in all regions, so select a region where your specific feature is available
- **Price**- Service prices in Azure vary from region to region

Why are regions important?

No other cloud service has as many international regions as Azure. You have the freedom to deliver applications near your users wherever they may be due to these zones. Global regions offer greater scalability and redundancy. They maintain data residency for your services as well.

Special Regions

When building out your apps for compliance or legal requirements, you may want to use one of the specialized Azure regions. Here are a few examples:

- **US regions** - These Azure regions offer physically and logically network-isolated instances for U.S. government agencies and partners, including US DoD Central, US Gov Virginia, US Gov Iowa, and more. These data centers have additional compliance certifications and are run by screened U.S. employees.
- **China North, China East, and other areas** - Through a special collaboration between Microsoft and 21Vianet, in which Microsoft does not directly administer the data centers, these regions are now accessible.

Sovereign Regions

Azure has both ordinary regions and sovereign regions. The Azure instances, known as sovereign regions, are separate from the main Azure instance. You might need to use a sovereign region for compliance or legal reasons.

These Azure sovereign regions:

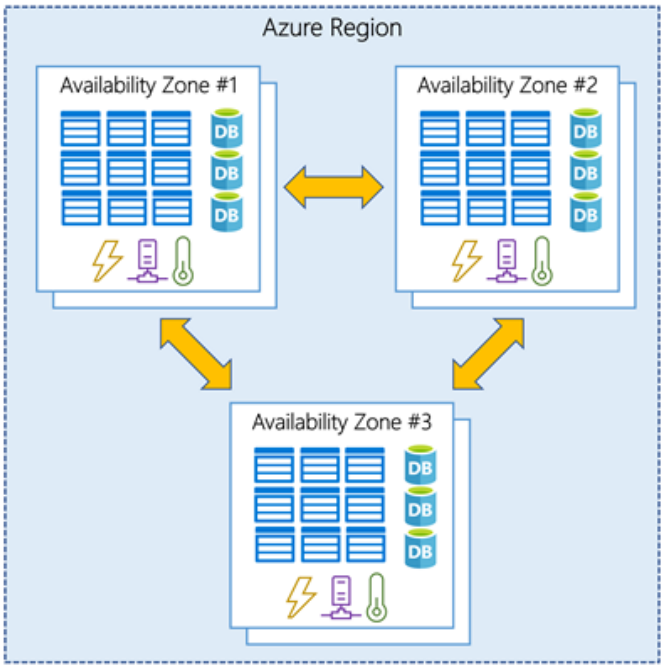
- Instances of Azure that are physically and logically network-isolated for use by US government organizations and partners include US DoD Central, US Gov Virginia, US Gov Iowa, and more. These data centers have additional compliance certifications and are run by US employees who have been thoroughly vetted
- Through an innovative collaboration between Microsoft and 21Vianet, whereby Microsoft does not directly run the data centers, several regions—including China East, China North, and others—are made available

Availability Set

An Availability Set is a logical grouping mechanism for separating VM resources from one another.

Availability Zone

Availability Zones (AZ) are physically distinct locations within an Azure region. One or more independently running power and network data centers make up an availability zone. A minimum of three zones exists in each region.



Management Infrastructure

Azure resources and resource groups, subscriptions, and accounts make up the management infrastructure. Planning your projects and products within Azure will be easier if you understand the hierarchical structure.

Azure Resource Manager (ARM)

Azure Resource Manager gives you the tools you need to organize and secure your resources. It is a fundamental service that is used to install and manage Azure resources. It comes with a management layer that enables you to create, upgrade, and delete Azure subscription tools. After deployment, you use management tools like access control, locks, and tags to keep your resources safe and organized.

Resource

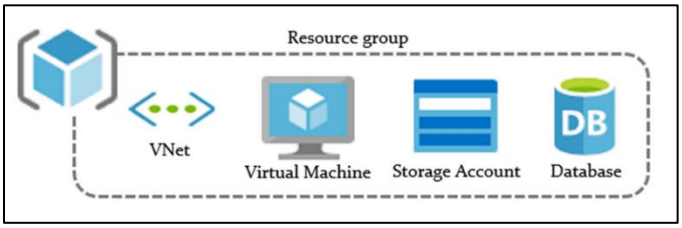
A Resource is a manageable item that is available in Azure, like VM, storage, databases, etc. Each resource can reside only in one resource group.

Resource Groups

Resource Groups are the place where you deploy your resources. Here, you need to identify which resource group you want to deploy a resource to. It is like a container where all a solution's resources or the resources you want to manage in a group reside. The resource from the resource group can be added or removed at any time. You can move your resources from one group to another, and the resource from multiple regions can also be in one resource group. With the resource group, you have access control to the resource. The resources in different resource groups can interact with each other.

Logical Groups

Resource groups are used to organize and manage Azure resources. You can add order and organization to your Azure resources by grouping similar usage, type, or location resources. Because materials are often so disorganized, logical grouping is the component that you might be the most interested in.



Lifecycle

When you delete a resource group, it also deletes all of the resources included within it. Organizing resources by life cycle can be advantageous in non-production contexts where you might test an experiment and then discard it. It is simple to remove a collection of resources at once using resource groups.

Authorization

Role-Based Access Control (RBAC) permissions allow you to grant users the specific rights they need to perform their jobs. RBAC permission can also be applied to resource groups. You may simplify administration and limit access to only what is required by applying RBAC rights to a resource group.

Resource Provider

Resource Provider is a service that supplies the resources that you can deploy for a manageable resource for the resource manager.

Resource Manager Template

Resource Manager Template is a JavaScript Object Notation (JSON) file that defines the resources deployed in the resource group. It also defines the dependencies between the deployed resources. With this template, resources can be deployed in a consistent and repeatable way.

ARM Benefits

- You have group resource handling like deploying, management, and monitoring
- You get consistency; For example, when you deploy resources, it will happen in the same way as every time
- Dependencies of each resource so no other will get into the resource
- Access Control, which is built-in to assign access to the users
- Tagging, which makes it easier to identify the resource in the future
- For billing, you can use tagging to stay on top

Azure Resource Manager has several features that you can use to organize resources, enforce standards, and protect your critical Azure resources from accidental deletion. The resource groups are just like a container for resources deployed on Azure. By placing resources of similar usage, type, or location in the same resource group. You can provide some order and organization to your Azure resources.

Tags

Tags allow you to improve the organization of your resources even further. You can use tags to associate custom details with a resource or resource groups such as a cost center or billing department.

Resource groups and tags are great for helping you organize existing resources or groups.

Policies

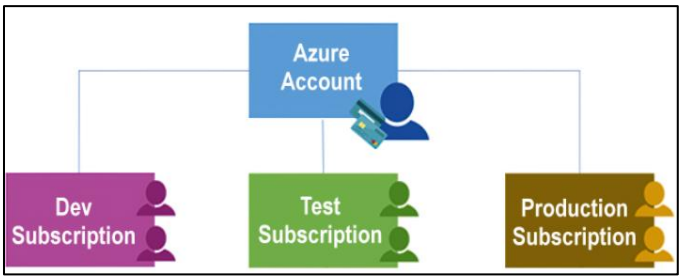
Azure policies are used to ensure that the new resource uses the same rules. The policies defined by Azure ensure that new resources use the same tags as an existing resource.

Azure Subscriptions

You can get authenticated and authorized access to Azure services with an Azure subscription. It also enables you to allocate resources. An Azure subscription is a logical unit of Azure services linked to an Azure account, which is an Azure Active Directory (Azure AD) or a directory that Azure AD trusts identity in.

A single subscription or many subscriptions with different charging models and access-management rules can be added to an account. Azure subscriptions can be used to set limits on Azure products, services, and resources. You can utilize one of two types of subscription boundaries:

- Billing Boundary
- Access Control Boundary



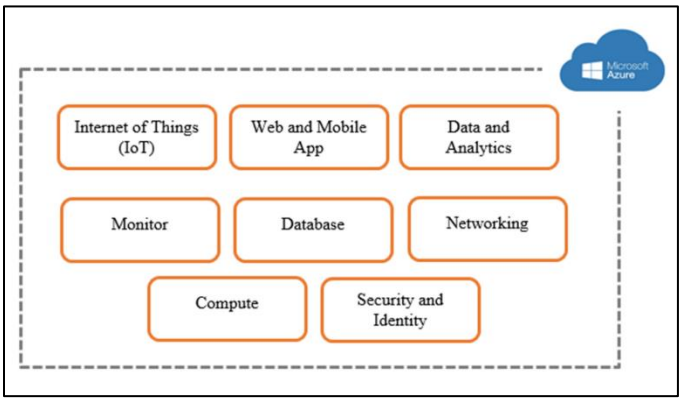
Azure Management Groups

If your company has a lot of subscriptions, you will need a way to keep track of access, regulations, and compliance for all of them. Over and above subscriptions, Azure management groups provide a level of scope. Subscriptions are organized into containers called management groups, and the management groups are subject to your governance rules. All subscribers within a management group automatically inherit the management group's conditions.

Azure Services

In Azure, there are a variety of services and capabilities to choose from. The following are the most often-used categories:

- Compute
- Networking
- Storage
- Data and Analytics
- Databases
- Web and Mobile
- Security and Identity
- Monitoring and Management
- Internet of Things



Compute

There are various alternatives for hosting applications and services in Azure. Azure Compute provides you with a platform on which to run your apps.

Networking

The relationship between computational resources and application access is a critical function of Azure networking. Azure offers several networking services that can be utilized separately or in combination. In comparison to any other Cloud Platform, Azure networking delivers the best safe environment for your data.

Storage

Azure Storage is a Microsoft cloud storage system for storing up-to-date content. Azure Storage includes a data object store that is extremely scalable, a cloud file system service, a dependable messaging store, and a NoSQL store. Azure Storage is safe, dependable, long-lasting, scalable, manageable, and accessible.

Data and Analytics

Data comes in a variety of sizes and forms. When people talk about Big Data, they are referring to massive amounts of data. It is frequently so vast that typical processing and analysis methods are no longer appropriate.

Open Source cluster technologies have been created to deal with these enormous data collections. Microsoft Azure provides a comprehensive set of Big Data and analytics tools and services.

Databases

The Azure Database service is fully managed. It combines business-grade efficiency with built-in high availability, allowing you to effortlessly scale and reach global distribution without worrying about costly downtime.

Web and Mobile

In today's corporate world, a great web experience is critical. For the construction and management of web applications and HTTP-based web services, Azure offers premium support. Azure creates engaging cross-platform Android, iOS, and Windows apps that meet your business needs and reach your consumers wherever they are.

Security and Identity

We all know that security is critical in the cloud, and having accurate and up-to-date Azure Security information is crucial. Azure offers a variety of security tools and features, making it the best choice for your apps and services. You can secure Azure identity and access management solutions on the front door for your applications and data.

Monitoring and Management

System managers and developers may use Azure management and governance tools to keep their resources secure and compliant, whether on-premises or in the cloud. Throughout the IT cycle, it keeps track of infrastructure, software, system provisioning and setup, app updates, vulnerability detection, backup resources, disaster recovery, policy execution, process automation, and even cost management.

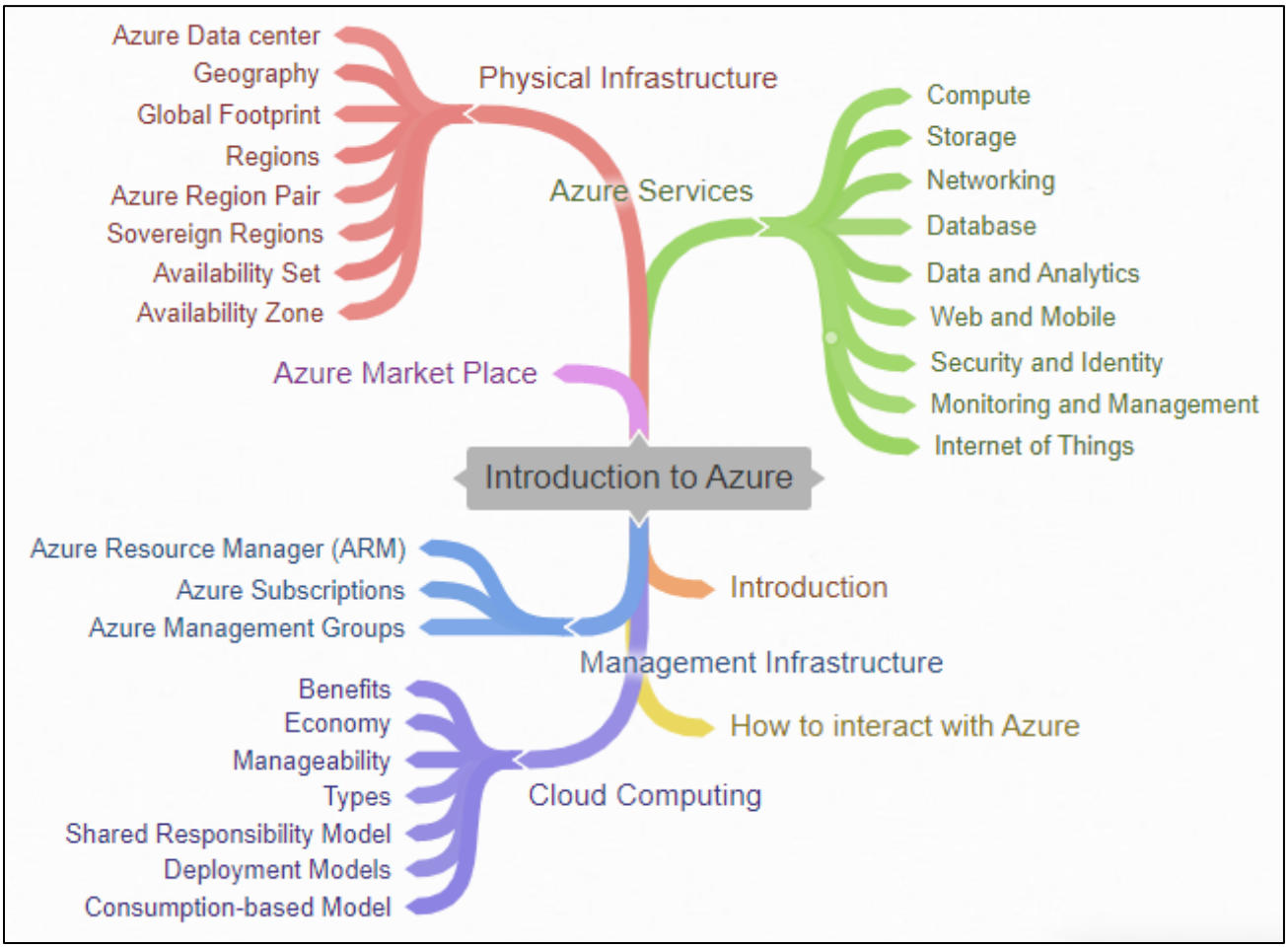
Internet of Things

The Internet of Things (IoT) is a network of internet-connected gadgets that communicate with one another (send and/or receive data) via embedded sensors in the cloud. Azure IoT, or Azure Internet of Things, is a suite of Microsoft-managed cloud services that connect, monitor, and govern many IoT assets.

How to Interact with Azure

- Azure Portal
- Azure CLI
- Azure PowerShell
- Azure Cloud Shell

Mind Map


Introduction to Azure
Physical Infrastructure
Azure Data center
Geography
Global Footprint
Regions
Azure Region Pair
Sovereign Regions
Availability Set
Availability Zone
Azure Services
Compute
Storage
Networking
Database
Data and Analytics
Web and Mobile
Security and Identity
Monitoring and Management
Internet of Things
Azure Market Place
Introduction
Management Infrastructure
Azure Resource Manager (ARM)
Azure Subscriptions
Azure Management Groups
How to interact with Azure
Cloud Computing
Benefits
Economy
Manageability
Types
Shared Responsibility Model
Deployment Models
Consumption-based Model

Chapter 02: Compute

Virtual Machines (VMs)

A virtual machine is a server or computer that runs on top of another computer and acts like one. It runs on Windows PCs just like any other program, giving users an identical experience as if they were using the operating system. Virtual hardware includes CPUs, RAM, hard drives, network ports, and other devices for each virtual computer.

Features

Azure offers the following features for the self-deployment of virtual machines:

- Infrastructure as a Service
- Tools
- Compliance
- Recommendations
- Choice

Pricing

Azure charges for Virtual Machines on an hourly basis and the resources you use. In other words, the more CPUs and RAM you utilize on your virtual machines, the more you will have to spend every hour.

Use Cases

Before you create, you have all of the necessary information about the VM, including its advantages and disadvantages.

Pros

- Control
- Application
- Existing Infrastructure

Cons

- Not for Everything
- Maintenance

Scale Sets

You may use Azure virtual machine scale sets to construct and manage a collection of load-balanced, identical VMs. Scale sets make your applications more accessible and allow you to manage, configure, and upgrade a large number of virtual machines from a single location.

Benefits

The scale sets offer the following key benefits:

- Easy to create and manage multiple VMs
- Allows your application to scale as resource demand changes automatically
- Works at large-scale

Application Hosting Options

The first option you might consider if you need to host your application on Azure is a virtual machine (VM) or a container. Both VMs and containers offer excellent hosting solutions. With VMs, you have complete control over the hosting environment and may set it up in anyway you choose. If you are new to the cloud, VMs might also be your most familiar hosting option. Containers can also be a strong and appealing option because they can isolate and control various components of the hosting solution separately.

Azure App Service is one additional hosting service you may use with Azure.

App Services

Azure App Service is a fully managed Platform as a Service (PaaS), which means Azure manages and controls servers, networks, storage, and other core infrastructures, leaving you to focus on business objectives and logic. Azure App Service is an HTTP-based service that allows you to host web applications, REST APIs, and mobile backends.

Features

Some key features of App Service are outlined here:

- Multiple Languages and Frameworks
- DevOps Optimization
- Global Scale with High Availability
- Connections to SaaS Platforms and On-premises Data
- Security and Compliance

- Application Templates
- Visual Studio Integration
- API and Mobile Features
- Serverless Code

App Services Categories

Azure App services are divided into three main categories:

- Web Apps
- Web Apps for Containers
- API Apps
- WebJobs
- Mobile Apps

Pricing Tier of an App Service Plan

Azure offers a series of App Service plan pricing tiers. Each tier has several well-defined features like CPU, storage, size, and scale. You can choose the tier according to your requirement and the cost you must pay.

Azure Container Instances

Containers have become the preferred way for cloud applications to be packaged, deployed, and managed. Azure Container Instances is the simplest and fastest way to run a container in Azure without managing any virtual machines without having to follow a higher-level service.

ACI Features

- Manage Application Dependencies
- Less Overhead
- Increased Portability
- Efficiency
- Consistency

Container in Azure Workflow

The workflow for using a Container in Azure is following:

- Software Development Cycle
- Application Placed in Container
- Azure Container Instances

Benefits of ACI

Azure Container Instances (ACI) has the following benefits:

- Run containers without managing servers
- Increase agility with containers on demand
- Secure applications with hypervisor isolation
- Works with your favorite tools

Azure Kubernetes Service

Kubernetes

Kubernetes is an open-source container orchestration system that automates applications' deployment, administration, and scaling.

Azure Kubernetes Service

The Azure Kubernetes Service (AKS) makes it easy to set up a managed Kubernetes cluster in the cloud. By transferring several duties to Azure, AKS reduces the complexity and operational overheads of Kubernetes management. Azure is in charge of the Kubernetes masters. You are the only one that manages and maintains the agent nodes. AKS is a free managed Kubernetes service; you only pay for the agent nodes within your clusters, not for the masters.

Azure Container Registry

ACR is a service that maintains a list of all currently valid container images. For containers, it maintains files and artifacts. The pictures come from ACR when your Azure container instances and Kubernetes service need to generate a new container.

AKS Cluster Architecture

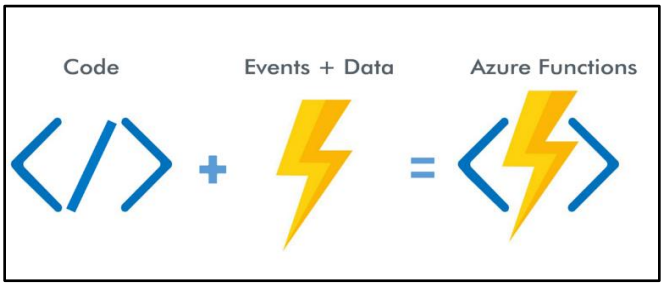
The following are the primary components that make up the Azure Kubernetes Service cluster architecture:

- Node
- Node Pools
- Pods

Azure Functions

The smallest computing on Azure is Azure Function. It is a single function that simplifies running little bits of code or "functions" in the cloud.

Functions can speed up development and allow you to use your preferred programming languages, such as C#, Java, JavaScript, PowerShell, and Python. Azure Functions is a serverless computing solution hosted on Microsoft Azure's public cloud.



Features

Here are some key features of Functions:

- Choice of your language
- Pricing Model for Pay-per-use
- Integrated Security
- Simplified Integration
- Open-source

Azure Virtual Desktop

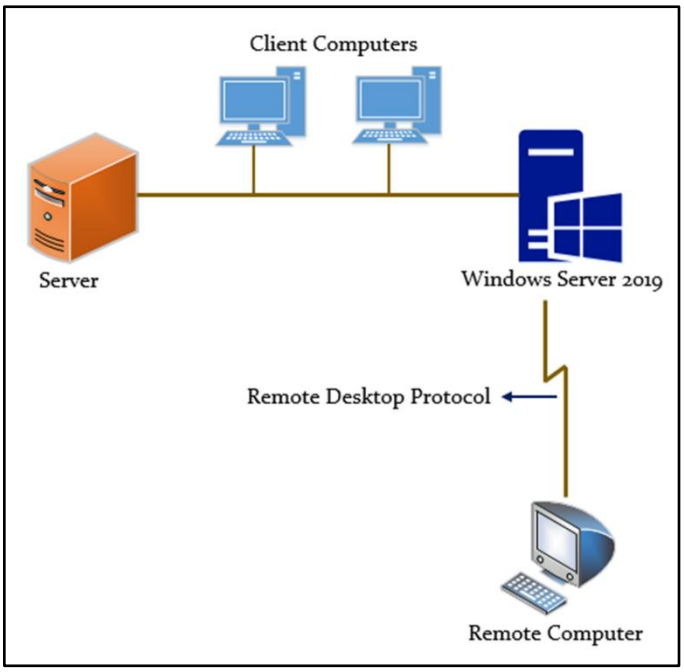
Azure Virtual Desktop is a cloud-based desktop and application virtualization service. It allows your users to access a cloud-hosted version of Windows from anywhere. It is compatible with apps that let you access distant desktops and apps. Windows, Mac, iOS, Android, and Linux are all supported by Azure Virtual Desktop. Most recent browsers can also be used to access Azure Virtual Desktop-hosted experiences.

Key Features

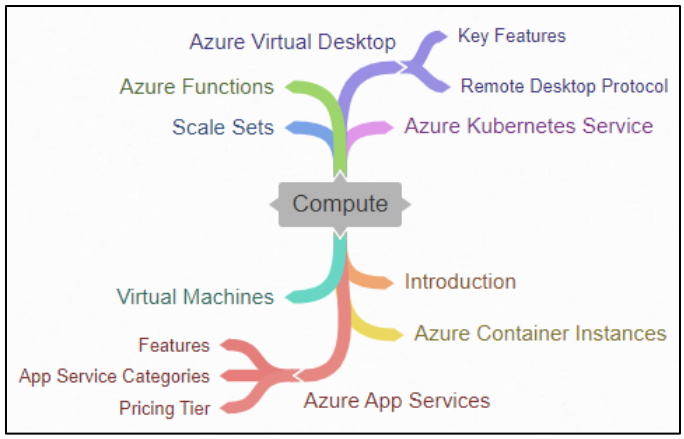
- Simplified Management
- Performance Management
- Multi-Session Windows 10 Deployment

Remote Desktop Protocol (RDP)

Remote Desktop Protocol is the graphical terminal or terminal server that is used to connect to another computer through a network connection. It listens for TCP on port 3389. RDP allows the client to protect the server from the software interface connection. It can run an application mode that loads the shortcut from the user's desktop and appears as if it is the standard application.



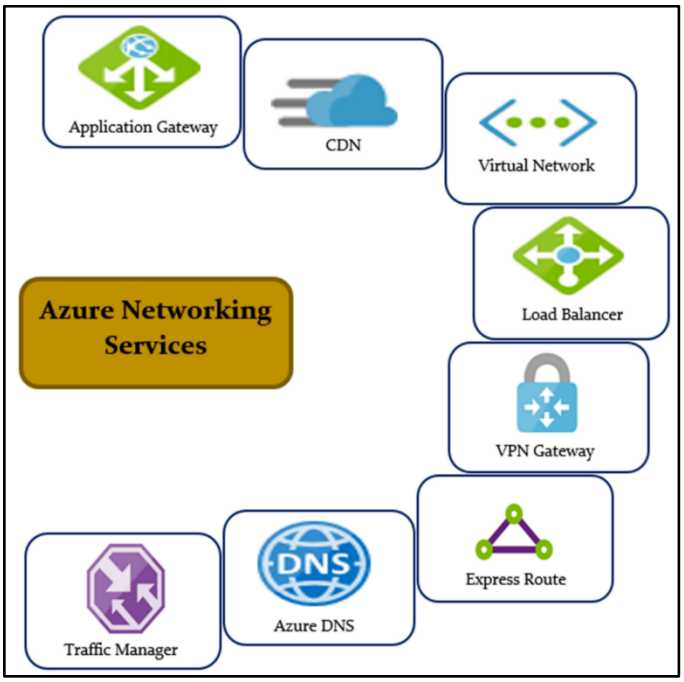
Mind Map



Chapter 03: Networking

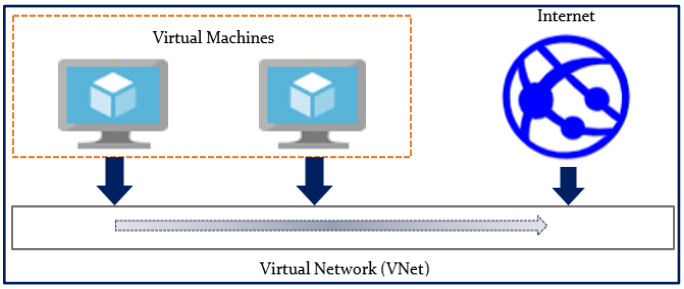
Introduction

Azure networking is a critical component in constructing a successful public cloud in Microsoft Azure and a core feature of the platform. Microsoft Azure's networking service provides connectivity to consumers and provides connectivity between service pieces.



Virtual Network

A Virtual Network (or VNet) is a networking service used by Microsoft Azure to host infrastructure resources. It is the most important component of the Azure network. It is a logical separation of the Azure cloud for your subscription. VNets are used in Azure to provision and maintain virtual private networks (VPNs).



IP Address

Each traffic has its IP address, ensuring that traffic delivers to the right destination (server). An IP address serves two main functions: network interface and address.

Address Space

The range of IP addresses is referred to as an address space.

Subnets

A subnet is a feature that allows you to segment your network.

Subnet Regions

Within Azure, each virtual network is assigned to a certain area.

Subscription

There is only one subscription per virtual network, and each subscription has many virtual networks.

Cloud Advantages

- Scaling
- Isolation
- Security
- High Availability

Load Balancer

A load balancer is employed in front of two VMs to access the data before it reaches the target. As a result, several users can more efficiently utilize the service at the same time.

Generally, a load balancer is used to distribute traffic from the front end to the backend pool according to rules and health conditions.

Public and internal load balancers are the two types of load balancers. The public load balancer changes the VM's private IP address to a public IP address for outbound access and internet-facing. On the other hand,

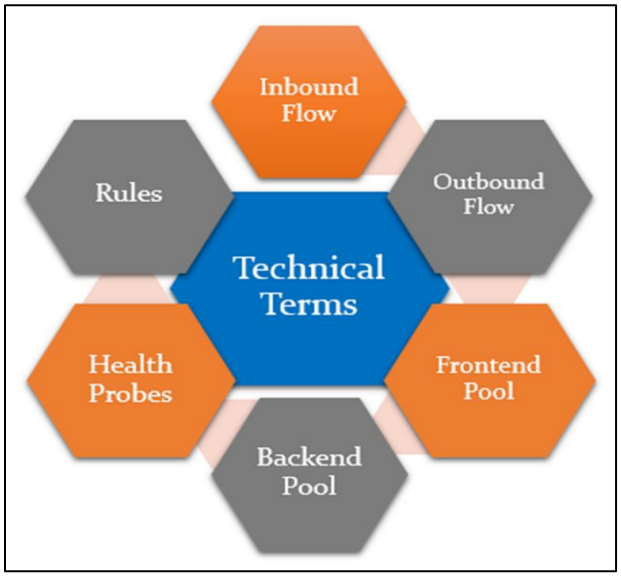
the internal load balancer is capable of handling traffic within the VNet.

Benefits of Load Balancer

- Internet Traffic
- Internal Network
- Port Forwarding
- Outbound Traffic

Technical Terms of Load Balancer

- **Inbound Flow:** Inbound flow is traffic that comes from either the internet or the local network. The load balancer then receives this traffic
- **Outbound Flow:** Outbound flow is used for establishing the connection between the public frontend and virtual machine backend
- **Frontend Pool:** Frontend pool connects clients to the load balancer via IP addresses. It manages traffic to the VM. All the traffic arrives here first
- **Backend Pool:** Backend pool allows VM to receive the traffic from a load balancer
- **Rules and Health Probes:** Rules refer to the load balancer rule for directing the traffic, and health probes ensure that VM is ready to receive traffic before the load sends any, as the load balancer always sends traffic to the healthy VM. Health probes can be HTTP, HTTPS, or TCP



VPN Gateway

A VPN gateway is useful for establishing a secure private connection between Azure resources and an on-premises environment, offices, the cloud, or other premises inside the cloud. VPN stands for Virtual Private Network. The VPN gateway in Microsoft Azure manages the cloud's managed services.

Virtual Network Gateway

A virtual network gateway (VPN gateway) is a specific sort of virtual network gateway. A virtual network gateway comprises multiple virtual machines (VMs) that are part of the Gateway Subnet.

Gateway Type

- Network-to-Network Connection
- Site-to-Site Connection
- Point-to-Site Connection

Create a VPN Gateway

There are two possible options for creating the VPN gateway.

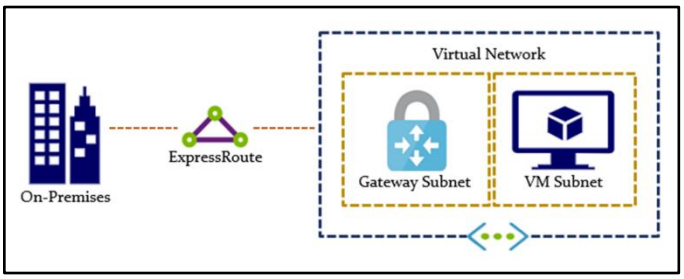
Route-based – Route-based VPN works on a route tunnel interface in the virtual network. This device allows the routing table to direct the traffic to different IPsec tunnels. It routes traffic dynamically over the tunnel interface. This VPN option is commonly used to avoid overlapping subnets and plays a vital role in accessing multiple subnets.

Policy-based –Policy-based VPN restricts traffic flow to certain network subnets according to the configured policy. It is built on a firewall device and defines the policy of how to encrypt or decrypt the network traffic through an IPsec tunnel. This VPN option is commonly used to access only one subnet or network at the remote site.

Azure ExpressRoute

Azure ExpressRoute allows you to have a dedicated private connection from your on-premises network into the Microsoft cloud. With the help of ExpressRoute, you can easily connect to your data center and a Microsoft cloud provider like Azure.

ExpressRoute also provides layer 2 and layer 3 connectivity to allow private, secure access to the resources deployed in the Azure virtual network.



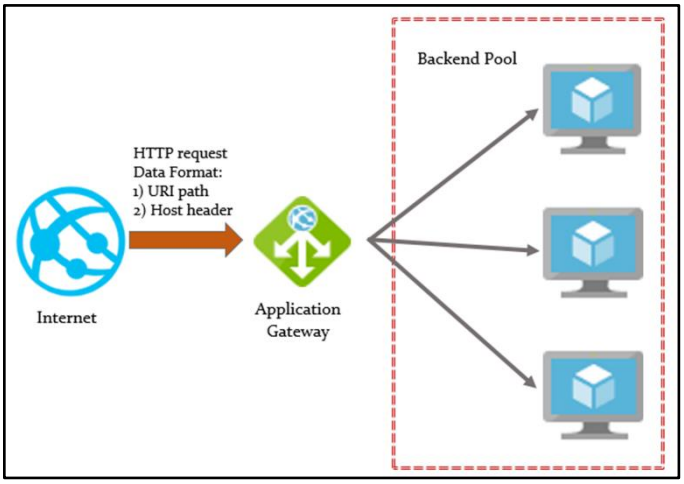
ExpressRoute Connectivity Model

There are three ways to connect ExpressRoute:

1. Any-to-Any (IPVPN) Networks
2. Virtual cross-connection through an Ethernet Exchange
3. Point-to-Point Ethernet connection

Application Gateway

The application gateway is one sort of VPN gateway. It is the most advanced load balancer, allowing online traffic to be balanced and web applications managed using HTTP requests. The gateway is known as the layer 7 load balancer within Microsoft Azure because of its services.



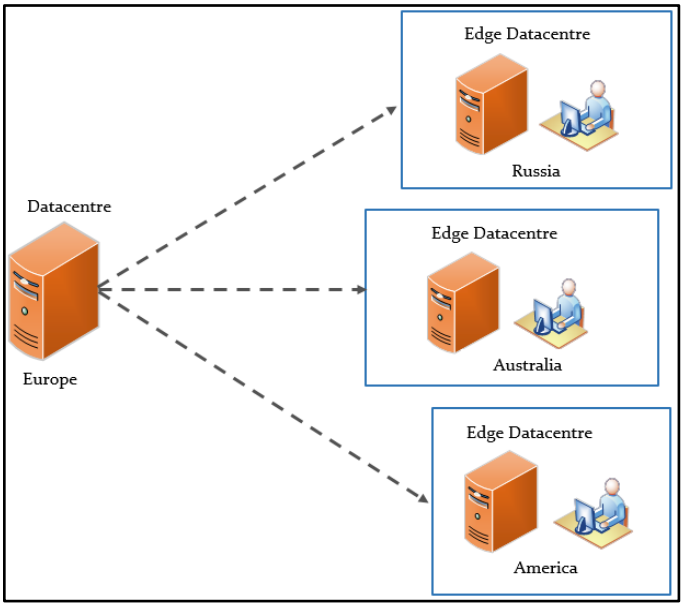
Benefits of Application Gateway

- Scaling
- High Availability
- Encryption
- Zone Redundancy
- SSL Offload
- Multi-Site hosting
- Cost-effective
- Session affinity
- Web Socket Support
- Web Application Firewall

Content Delivery Network

It is a distributed network of servers that can provide online content to users in their immediate vicinity. Within Azure, CDN relocates duplicate data to a data center that is closer to the user, allowing users to access the application quickly.

A Content Delivery Network (CDN)'s primary goal is to provide users with the shortest possible latency by delivering data from edge nodes.



Benefits of CDN

- Global Coverage
- Better Performance
- Scaling
- Distribution

Express Route

Within Microsoft Azure, the Express route is a private connection that can be used in on-premises data centers. It can give a dedicated connection of up to 10 Gigabits per second. This sort of routing is useful when connecting two or more Azure regions, and it eliminates the need for VPN and VNet peering.

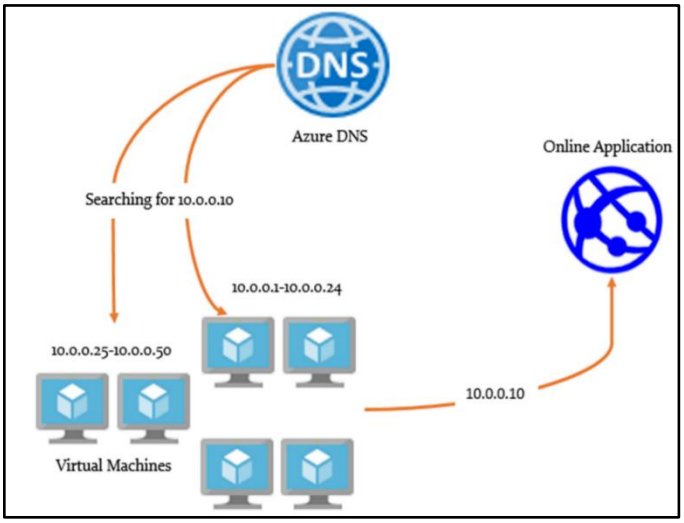
Traffic Manager

The traffic manager is in charge of managing and monitoring all routing traffic within the Azure

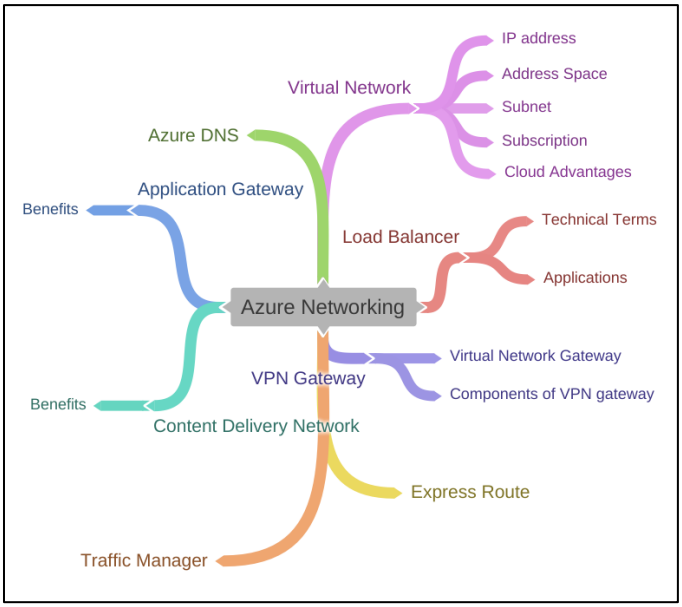
infrastructure globally. Azure DNS is required to choose the best potential endpoint (internal or external) for traffic routing. Due to different web apps across the region, the traffic manager distributes the load across multiple regions.

Azure DNS

Domain Name System (DNS) is a Microsoft Azure feature that allows you to host a domain within Azure. The main benefit of DNS is that it eliminates the requirement to host within both DNS providers and Azure. Azure DNS allows you to monitor DNS records with the same authorization as other Azure services. Azure DNS is also in charge of managing domain and DNS server interactions quickly.



Mind Map



Chapter 04: Storage

Introduction

It is a known fact that to perform any type of compute; we need some form of storage. We need storage for transient data, data used for a single session, user details, customer data, orders, and everything else. This chapter will discuss four ways to create Storage on Azure. These include Blob, which is used in many different scenarios and is incredibly flexible; Disk Storage, which is like a disk for storing data; File Storage, which is a fully managed file storage in the cloud used to the extent your on-premises storage. One is Archive Storage, a cheap way to store massive amounts of archived data. It would help if you made the right decision in storage, as it makes your application sufficient. Choosing the right storage option for your required job is one of the most critical steps. Storage is scaling up constantly, and we need modern solutions. Therefore, Microsoft introduced Azure Storage, which provides us with the best solution.

Storing data in the cloud omits the need for any hardware or physical space and makes scaling of storage as per requirement very easy. By storing data in the cloud, you can also increase the availability of data.

Storage Account

A Storage Account is similar to an Azure Storage access point. An Azure storage account holds all of your Azure Storage Data Objects, such as blobs, files, queues, tables, and disks. Your Azure Storage data is accessible through HTTP or HTTPS from anywhere in the globe, with the storage account's unique namespace.

It is written in the format: “https://<Storage-Account-Name>.<Storage-type>.core.windows.net”.

There are two sorts of storage accounts. The "Standard" storage account gives users access to Blob Storage, Table Storage, Queue Storage, and File Storage. A "Premium" account, which is a new option that allows customers to save data on SSD drives to increase IO capacity, is an alternative.

There are five main sorts of storage accounts, each with its own set of features and costs.

- General-purpose v2 accounts
- General-purpose v1 accounts
- BlockBlobStorage accounts
- FileStorage accounts
- BlobStorage accounts

Azure Storage Redundancy

Your data is always stored in several copies by Azure Storage to safeguard it against both planned and unforeseen occurrences, such as temporary hardware failures, network outages, power outages, and natural disasters. Despite failures, redundancy makes sure that your storage account reaches its availability and durability goals.

Redundancy in a Primary Region

In the primary region, data in an Azure Storage account is always duplicated three times. In the primary region, Azure Storage provides two choices for data replication: locally redundant storage (LRS) and zone-redundant storage (ZRS).

Locally Redundant Storage (LRS)

Your data is replicated three times within a single data center in the primary region with locally redundant storage (LRS). Over a given year, LRS guarantees at least 11 nines of object durability (99.999999999%).

Zone-Redundant Storage

Zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region for Availability Zone-enabled Regions. For data objects stored in Azure Storage, ZRS offers the durability of at least 12 nines (99.9999999999%) over a specific year.

Redundancy in a Secondary Region

For applications that demand exceptional durability, you can also opt to replicate the data in your storage account to a secondary region that is hundreds of miles away from the original region. In the event of a catastrophic failure that prohibits the recovery of the data in the primary region, if the data in your storage account is transferred to a backup region, your data will still be available.

Geo-Redundant Storage

Using LRS, GRS replicates your data three times synchronously within a single physical location in the primary region. The data is then asynchronously copied via LRS to a single physical place in the secondary region (the region pair). For data objects stored in Azure Storage, GRS offers the durability of at least 16 nines (99.99999999999%) over a specific year.

Geo-Zone-Redundant Storage

Geo-replication and availability zone redundancy work together to give GZRS with both high availability and protection from regional failures. In a GZRS storage account, data is replicated to a secondary geographic region using LRS for protection against local disasters, and it is copied across three Azure availability zones in the primary region (equivalent to ZRS). Microsoft suggests using GZRS for applications that call for the highest levels of consistency, durability, and availability, as well as good performance and resilience for disaster recovery.

Azure Storage

Azure Storage is a data storage service provided by Microsoft. It is a highly scalable object store as well as a messaging message store. It also provides access to a file system. It is a NoSQL database that offers several advantages, including:

- Durability
- High Availability
- Security
- Accessibility
- Scalability

Blob Storage

Blob stands for Binary Large Object, and it is a storage format for binary or text data. It is used to store enormous volumes of data.

Three types of Blobs are supported in Azure:

- Block blobs can hold up to 4.7TB of text and binary data.
- Log data is stored in append blobs, which can be up to 195GB in size.
- For frequent read and write operations on data, page blobs are utilized. It can hold up to 8TB of data.

You must choose the sort of storage account you want during the creation process based on several price options.

- Hot Tier
- Cold Tier
- Archive Tier

The archive tier can be set to blob only while the Hot/Cool tier is enabled at the storage account level or blob level. All three levels of storage access can be found in the same storage account, and a blob default level is inherited from the account level setting. However, a blob-level tier can be used to set the level of the object.

The various access tiers should be taken into account:

- Only the hot and cool access tiers are programmable at the account level. At the account level, the archive access tier is not accessible.
- Tier settings for hot, cool, and archives can be made at the blob level before or after upload.
- Although the availability of data in the cold access tier can be significantly lower, it still needs to have good durability, short retrieval time, and high throughput. Compared to hot data, cold data offers an acceptable trade-off between cheaper storage costs, a somewhat poorer availability service-level agreement (SLA), and higher access prices.
- The least expensive form of data storage is archive storage, which also has the greatest access and rehydration fees.

Disk Storage

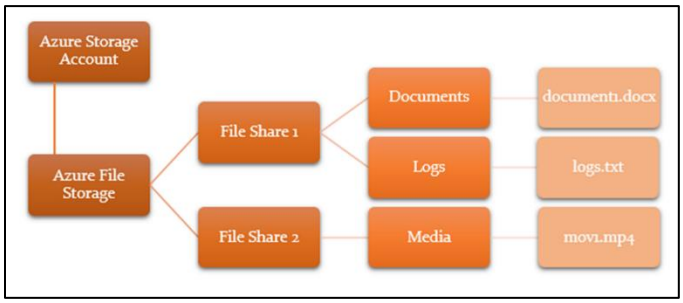
It is a disk where you can save your files. The disk associated with your VM is known as a managed disk. Managed means that Azure will take care of this disk for you, including managing uptime and backups. Disks come in four basic varieties.

- HDD
- Standard SSD
- Premium SSD
- Ultra Disk

File Storage

You get the following advantages with File Storage:

- It is fully managed, so you do not have to worry about OS or hardware.
- You may share files across many Azure computers and connect to your on-premises infrastructure.
- Extremely reliable, even in the face of outages
- It comes with built-in redundancy.



Archive

Generally, Azure Archive Storage is generally used for archiving data while paying less. The majority of the company's rules, legislations, and recovery scenarios necessitate the storage of a substantial volume of archive data. Therefore, the Azure archive service can come in handy. It is one of Azure's most affordable storage options, allowing you to store gigabytes of data for as little as a few dollars per month.

Identify Azure Data Migration Options

It is crucial to comprehend how to enter data and information into Azure. Azure enables asynchronous data movement using Azure Data Box and real-time data migration using Azure Migrate for infrastructure, apps, and data.

Azure Migrate

You can move from an on-premises environment to the cloud using the Azure Migrate service. Your on-premises data center's assessment and migration to Azure can be managed with the aid of Azure Migrate, which serves as a hub.

Azure Data Box

Large amounts of data may be moved quickly, affordably, and reliably with the help of Azure Data Box, a physical migration service. Your exclusive Data Box storage device, which has a maximum usable storage capacity of 80 terabytes, is shipped to you to speed up secure data transmission. A local carrier ship the Data Box to and from your data center. A tough casing shields the Data Box and keeps it safe during transit.

You can order the Data Box device through the Azure interface to import or export data from Azure. After receiving the device, you can simply configure it through the local web UI and link it to your network. Simply return the Data Box after transferring the data (into or out of Azure). Once Microsoft receives the Data Box back, the data is immediately uploaded if you transfer data into Azure. The Data Box service in the Azure interface keeps track of the procedure from beginning to conclusion.

Identify File Movement Options

Azure includes tools that enable you to migrate or interact with single files or small file groups in addition to big-scale migration using services like Azure Migrate and Azure Data Box. AzCopy, Azure Storage Explorer, and Azure File Sync are a few of these utilities.

AzCopy

You can copy blobs or files to or from your storage account using the command-line tool AzCopy. You can synchronize files and upload, download, and copy them between storage accounts with AzCopy. AzCopy can also be set up to cooperate with other cloud service providers to facilitate file transfer between clouds.

Storage Explorer

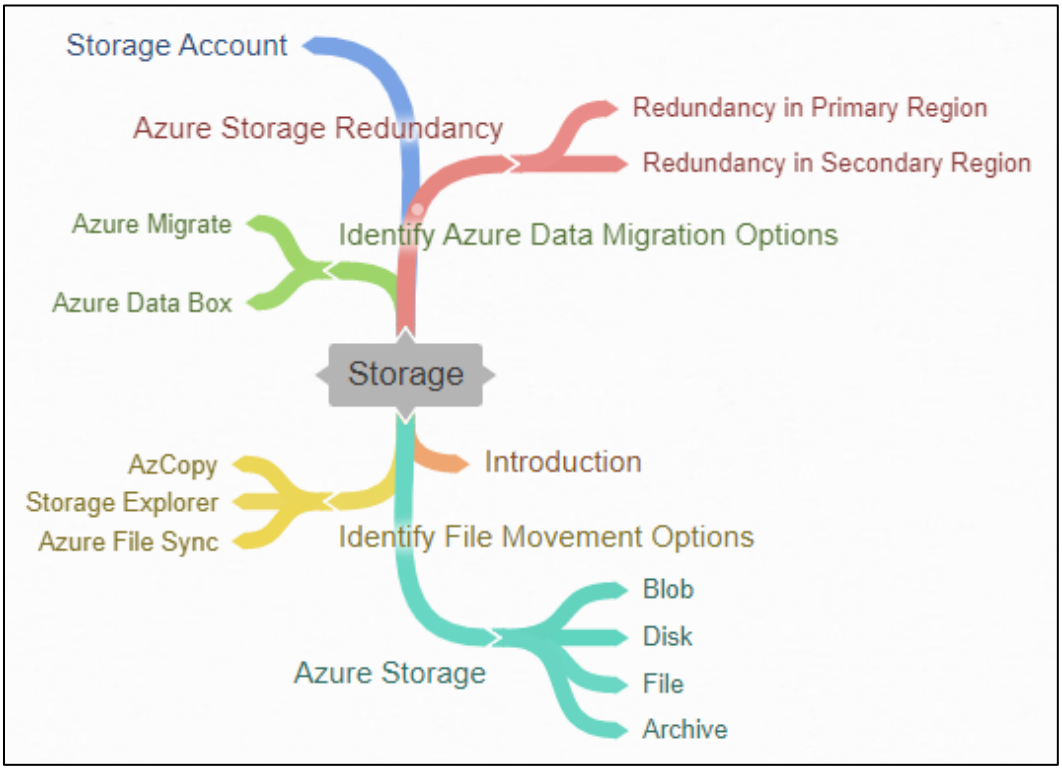
A standalone software called Azure Storage Explorer offers a graphical interface for managing the files and blobs in your Azure Storage Account. AzCopy handles all file and blob management functions on the backend and

is compatible with Windows, macOS, and Linux operating systems. You can upload to Azure, download from Azure, or switch between storage accounts using Storage Explorer.

Azure File Sync

By using Azure File Sync, you can consolidate your file shares in Azure Files while maintaining the adaptability, speed, and compatibility of a Windows file server. It is like creating a small content delivery network on your Windows file server. As soon as you install Azure File Sync on your local Windows server, your files in Azure will automatically remain in bi-directional sync.

Mind Map



Chapter 05: Databases

Introduction

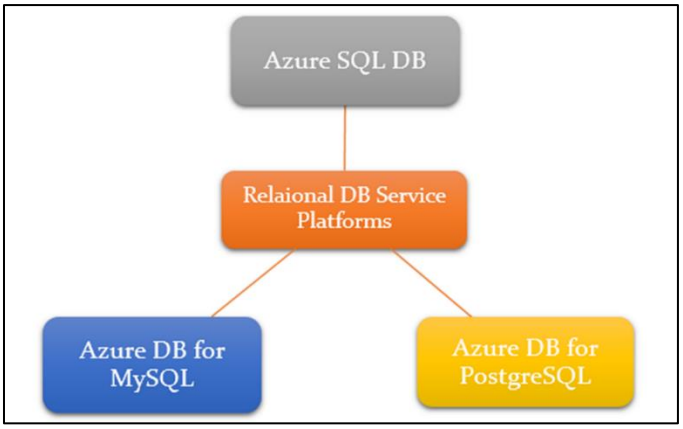
In modern business, managing data is much more important as a huge amount of data is collected from various sources, and you want this data stored safely in a database. Azure has a service known as Azure Databases that fulfills your business requirement. This chapter will discuss some keys that Azure databases offer, which are important from the exam perspective. We will discuss Cosmo DB, which scales globally and is a fully managed database service. It has a fast read and write capability. Azure SQL is managed database that will also be discussed in this chapter. We also learn about the MySQL database, which is one of the most popular community databases. We will discuss PostgreSQL, an open-source database with some unique features.

Furthermore, we will learn about the migration of databases to Azure by using Database Migration Services. With the database, your data will be organized to get exactly the data you want within no time at all.

Databases

Microsoft Azure helps you unlock your potential wherever you have your data. You can support quick growth and save innovation time by supporting open-source database engines with a secure, corporate-grade, fully managed database service. Azure provides a variety of data types and volume storage facilities. In addition, this data is available to users immediately via global connectivity. Azure helps you get it to the market quickly, distribute it widely, and handle it with ease and confidentiality no matter what you create. There are multiple Azure Database Services provided by Azure, which include:

- Cosmos DB
- Azure SQL
- Azure Database for MySQL
- Azure Database for Postgre SQL



Cosmos DB

From its inception, Cosmos DB has been a global service. You may put the data nearest to the user with Cosmos DB. This is a critical feature that also provides a wonderful user experience. It might be tough to synchronize databases spread across several locations, but with Cosmos DB, Azure takes care of this for you. All the data stored in Cosmos DB are encrypted at rest or in motion.

Latency

Latency, as we all know, is the time it takes for data to transit.

Scalability

When the need for resources increases, Cosmos DB allows you to scale your database to infinity automatically.

Connectivity

You can work with Cosmos DB in a variety of ways, such as using one of the built-in ways to connect to the database, such as SDKs or APIs. Different languages, such as C#, Java, and Node.js, can also be used.

Azure SQL

It is a managed Database as a Service, with hardware and IaaS handled by another Azure service. The Microsoft Azure SQL Database includes a cloud-based Database Management System (DBMS). You can effortlessly move your on-premises SQL database to Azure SQL and benefit

from it using Azure SQL. You can store 100TB of data in a minute with Azure SQL.

Integrated with ML

You can also use Azure SQL to access integrated Machine Learning technologies

Scalability

Because it is a cloud-based service, it provides outstanding scalability and high availability. It also guarantees 99.995% availability.

Security

Security is a built-in component of Azure Cloud Platform, providing you with benefits in terms of data security.

Azure Database for MySQL

Azure Database for MySQL is a community-built database, whereas Azure SQL is a Microsoft offering. The Azure MySQL platform offers a fully managed and ready-to-use MySQL cloud database. Azure Server for MySQL was created to deliver high availability with a 99.99 percent SLA while requiring no additional setup, replica features, or fees to ensure that your programs perform as they should. It offers batching and backup automation, as well as monitoring. All of this is provided free of charge. Microsoft manages Azure Database for MySQL, which is a PaaS.

Azure Database for Postgre SQL

It is a relational database that is open-source and similar to MySQL. It is a MacOS default database. It provides predictable performance, security, high availability, and dynamic scalability for mission-critical workloads.

Features

- You can use this database with a variety of extensions, including JSONB (a binary form of JSON) and Ruby, Python, and other programming languages.
- You can use this to accomplish horizontal scaling.
- It contains a feature that identifies disruptive events that have an impact on performance and allows you to take action.
- It provides completely managed database services, such as automatic patching, automatic backups, and built-in monitoring, similar to Azure Database for MySQL.

Database Migration Service

You can migrate databases from on-premises to Azure using a specific tool in Azure. You can migrate your existing SQL server with only one tool; there is no need to use several programs.

The Azure Server Migration Service is a fully managed program that allows service providers to migrate to Azure Data platforms with minimal downtime.

The service is currently available to the general public, with continuous initiatives to expand the service focusing on:

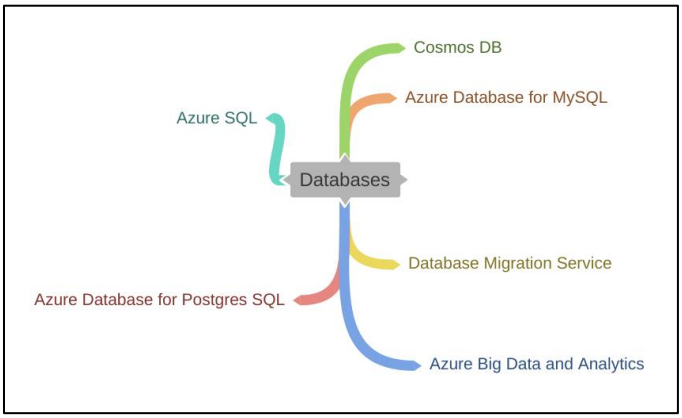
- Reliability and performance
- Addition on source/target pairs
- For friction, free migration is used for continuous investment

Azure Big Data and Analytics

Big data is a technical discipline that aids in extracting, processing, and analyzing data that is too massive or complicated for typical software to handle. As a result, Azure offers diverse technologies and services for dealing with massive and complicated datasets. The most commonly used services are:

- Azure Data Lake Analytics
- Azure Databricks
- Azure Synapse Analytics
- Azure HDInsights

Mind Map



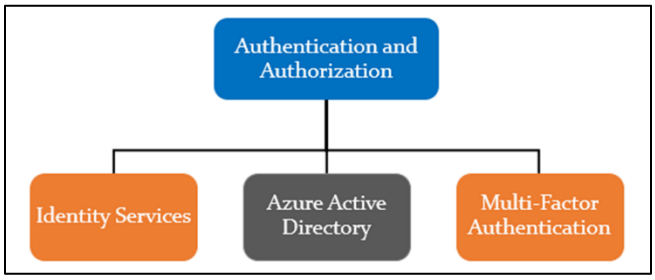
Chapter 06: Authentication and Authorization

Introduction

Any technology service with IT applications that control data access from illegal users is very important to provide a secure environment. In addition, it is also very critical to find which user access which part of the infrastructure. This chapter will discuss the fundamentals of authentication and authorization of users in Azure. Both of them are two major steps for ensuring network security. Authentication is a way of finding out whether the user exists in the database or not. Once the user is found from the database user ID and password, the next step is to ensure the user can access how many services.

Authentication and Authorization in Azure includes:

- **Identity Services:** Identity services identify the platform for the user and ensure user validations for the application
- **Azure Active Directory:** This directory service can provide access and control of access to users with different directory services
- **Multi-Factor Authentication:** Provides security features by getting multiple information about the user for authentication



Identity Services

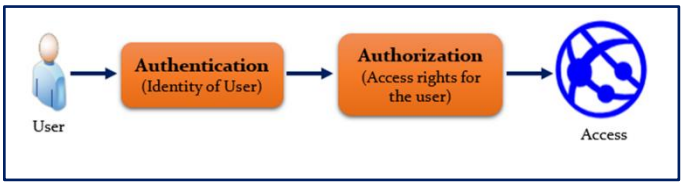
When a user accesses an online service that requires a username (also known as a User ID) and password, the user must first create a username (also known as a User ID). Authentication, authorization, and access management policies are all part of identity services.

Authentication

Authentication is the process of identifying a user using a user ID and password from a database.

Authorization

After authentication, the process of authorization is carried out. It determines what sort of data access the authenticated user has.



Access Management

Access management is an important aspect of any cloud architecture since it ensures that other user's access to services is restricted. It ensures privacy, integrity, and accessibility.

Access management policies should also cover the following:

- Authentication and Authorization
- Faraway from Unauthorized Users

Azure Active Directory

The main tool for managing and monitoring the dedicated users' information in Microsoft Azure is Azure Active Directory (AAD).

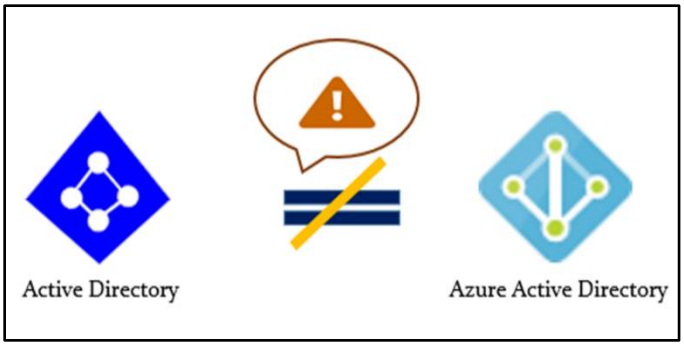
Active Directory

Active Directory (AD) is a directory service created by Microsoft for storing information about users, resources, and other networked objects. Offices, educational institutions, and management departments all employ AD.

Azure Active Directory

The Azure Active Directory (AAD) is not the same as the Active Directory (AD) (AD). AD makes its directory service available to the firms that created it. Azure Active Directory services, on the other hand, are available for

everything on Azure. It is the first service a person gets when they sign up for an Azure account.



AAD Services

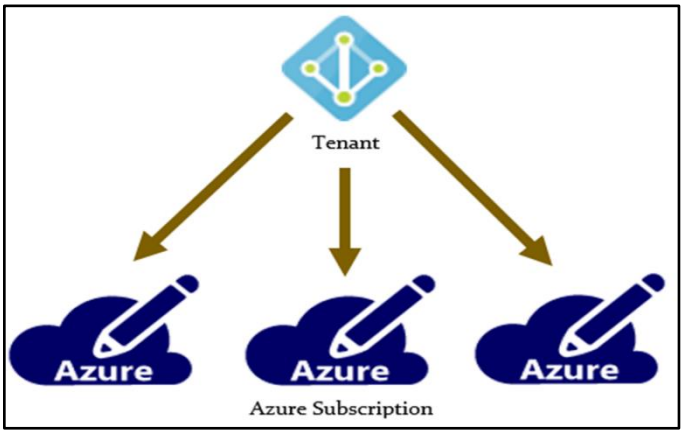
- **Mandatory Service:** Without AAD services, Microsoft Azure users cannot create an account.
- **First User:** The first user and owner are assigned to every Azure account. An AAD service is required to become an Azure user.

Tenant

In Azure, a tenant is a representation of an organization. A dedicated instance of the AAD service is referred to as a tenant. When a user establishes an Azure account, it is the first ADD service that appears.

Subscription

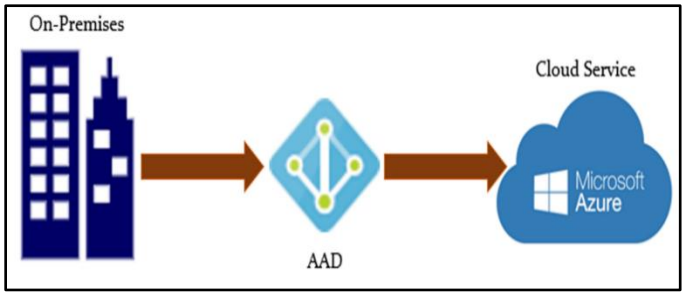
To use Azure resources and services, you will need to sign up for a subscription.



Hybrid Cloud Architecture

Some services are hosted on-premises, and others are hosted in the cloud in a hybrid cloud architecture. The AAD instance can be utilized in hybrid cloud architecture when a user wishes to set up a hybrid cloud infrastructure.

There are several services that AAD uses on Azure for management purposes.



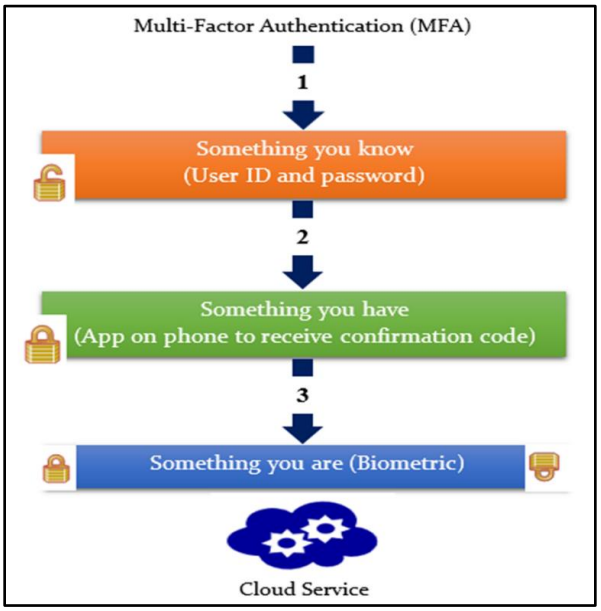
Azure External Identities

A person, thing, service, etc., external to your business is known as an external identity. All the secure communication channels you can utilize with users outside your business are Azure AD External Identities. You can share your resources and specify how internal users can access other businesses if you wish to work with partners, distributors, suppliers, or vendors. Developers who make consumer-facing apps have control over their users' identity experiences.

Single sign-on may sound similar to external identities. External users can "bring their own identities" with the help of External Identities. They can sign in using their credentials regardless of whether they have a digital identity granted by a company, the government, or an unmanaged social identity like Google or Facebook. To safeguard your resources, the external user's identity provider handles their identity while you control access to your apps using Azure AD or Azure AD B2C.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) provides a layer-based authentication using more than one form of authentication. MFA is recommended as a default. It is a part of AAD that enables other ways to authenticate users.



How MFA Works

MFA (Multi-Factor Authentication) is a user authentication method involving several steps. The first step is to confirm the user's identity using their user ID and password. The user's phone will be sent a code for further verification in the second step. Biometric verification is the third step. This is an optional step.

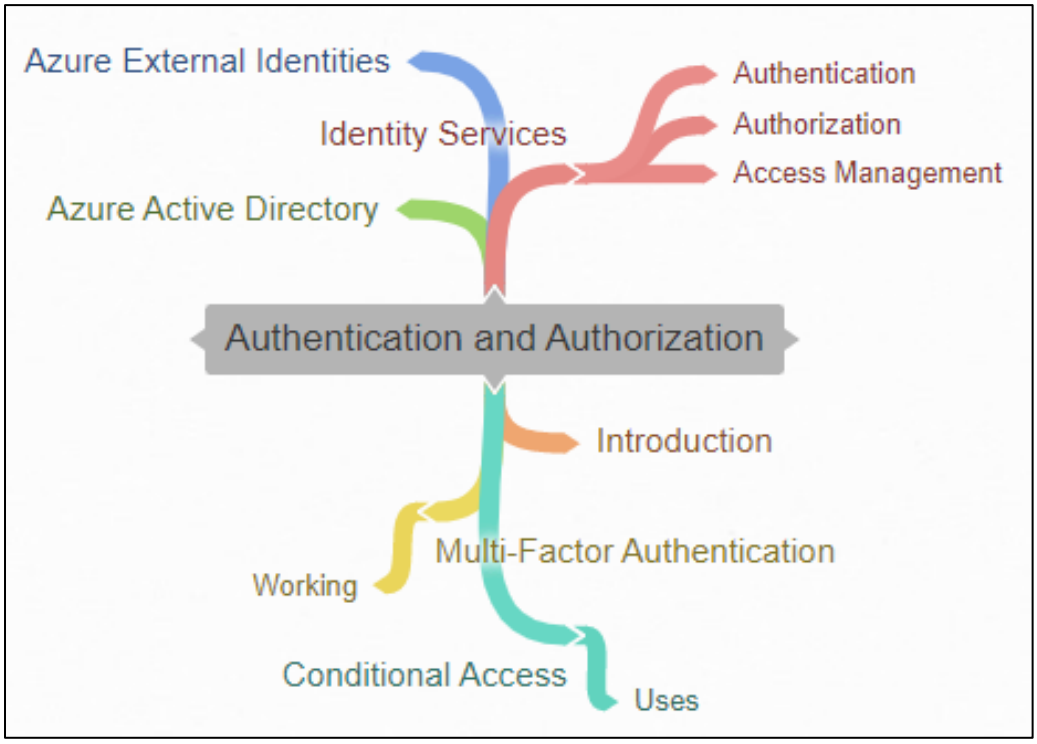
Conditional Access

Azure Active Directory employs Conditional Access to enable (or restrict) access to resources based on identification signals. These signals include the user's identity, the user's location, and the device from which the user is seeking access.

IT administrators benefit from Conditional Access in the following ways:

- Allow users to be productive wherever and at any time.
- Safeguard the company's assets.
- Users can also enjoy a more granular multifactor authentication experience with Conditional Access. For example, if a user is at a known location, they may not be asked for a second authentication factor. If their sign-in signals are uncommon or they are at an exceptional location, they may be asked for a second authentication factor.

Mind Map



Chapter 07: Azure Solutions

Introduction

Microsoft Azure, often known as Windows Azure, is the company's public cloud computing platform. It offers a wide range of cloud services, such as computing, analytics, storage, and networking. Users can use these services to construct and grow new apps in the public cloud or to run existing ones. Microsoft Azure provides both a Platform as a Service (PaaS) and an Infrastructure as a Service (IaaS) model.

There are several products, features, and services available in Azure. This session will look at some of Azure's basic products. You will learn about the Internet of Things (IoT), Big Data, Artificial Intelligence (AI), Azure serverless computing, and DevOps, among other cutting-edge technologies available today in Azure. All of these are Azure's solutions to its client's problems.

Choosing the Best Azure IoT Service for Your Application

Internet of Things

The Internet of Things (IoT) is a linked network of computing devices, mechanical and digital equipment, items, and people. They are all outfitted with Unique Identifiers (UIDs) and the ability to send data over a network without the need for human interaction.

Microsoft's Azure Internet of Things (IoT) is a suite of cloud services that connects, monitors, and controls billions of IoT assets. Simply said, an IoT solution consists of one or more IoT devices and one or more cloud-based back-end services that connect each other.

Identify the product options

IoT enables devices to collect and then transmit data for analysis. Sensors are built into smart gadgets to collect data. The following are a few examples of common sensors that measure physical attributes:

- Sensors that measure temperature and humidity levels in the environment
- Barcode, QR code, or Optical Character Recognition (OCR) scanners
- Geo-location and proximity sensors
- Light, color, and infrared sensors
- Sound and ultrasonic sensors
- Motion and touch sensors
- Accelerometer and tilt sensors
- Smoke, gas, and alcohol sensors
- Error sensors to identify when there is a problem with the device
- Mechanical sensors that detect anomalies or deformations
- Flow, level, and pressure sensors for measuring gasses and liquids

IoT Services

Azure provides several IoT-related services to assist you. Here are two of the most important IoT services.

IoT Hub

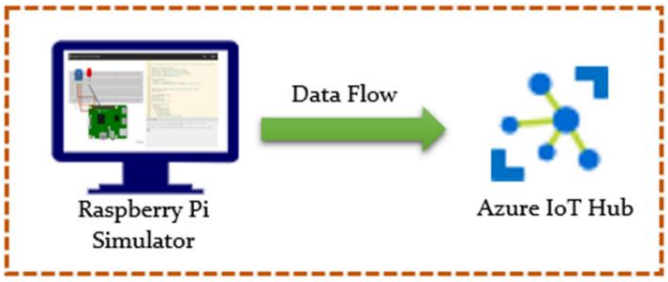
IoT Hub is a cloud-based, managed service that operates as a central hub for all connected devices' data streams. It facilitates bi-directional communication between your IoT app and the devices it manages.

IoT Hub Features

- Scaling
- Securing
- PaaS
- Integrating
- Ease of Deployment

Microsoft Raspberry Pi Simulator

Microsoft has launched a Raspberry Pi Azure IoT online simulator to connect the devices to the Azure IoT Hub.



This online simulator is a core tool with three main areas. These are:

- Assembly Area
- Coding Area
- Integrated Console Window

Azure IoT Edge

Azure IoT Edge is the cloud-based computing service used to manage and ensure the smooth running of workflow on the edge device. It enables moving cloud analytics and custom business logic to IoT devices. The device can easily process logic directly without pushing data to the cloud.

Functions of Azure IoT Edge

There are several functions of Azure IoT Edge that enable us to:

Fast Communication – As the Azure IoT Edge can connect the IoT Hub to the edge device by running the functionality built at the edge. The device will take less time to communicate with the edge device and ensure low latency and response time.

Monitor Edge Devices – Azure IoT Edge has a cloud interface and a runtime workflow that lets you control and monitor remotely and easily deliver computing workloads to the edge device through IoT Hub.

Distribute AI and Analytics Workloads – IoT Edge provides an ease to deploy runtime modules by using Artificial Intelligence and machine learning to run them on the edge devices.

Reduce Costs – IoT Edge controls and minimizes the cost by using the filtered data for future analysis. This approach reduces response time and storage costs as well.

Supports Multiple Languages – IoT Edge allows the use of existing developer`s skillset and offers multiple programming languages like C, C#, Node.js, Java, etc, to run the modules on the edge devices.

Provide an Extra Level of Security – IoT Edge uses various security modules to implement secure and sensitive computing and also makes use of Microsoft Defender for Cloud to ensure the threat protection of end devices.

Operate in Offline Mode – IoT Edge also enables intermittent and offline connectivity between the cloud and edge device and provides functionalities to deliver computing workloads reliably.

Function as a Gateway – The main advantage of the IoT Edge is that it can efficiently work as a protocol gateway that enables the custom and cloud logic on the edge device.

Working of IoT Edge

The structure of Azure IoT Edge consists of three components. These are:

- IoT Edge Modules
- IoT Edge Runtime
- IoT Edge cloud Interface

IoT Central

Azure IoT Central is a fully managed, highly scalable IoT SaaS solution that reduces the complexity and costs of developing, managing, and maintaining IoT solutions of an enterprise-grade nature.

Its user-friendly interface makes it simple to keep track of device needs, create rules, and manage millions of devices and their data throughout their lives.

Azure Sphere

For customers, Azure Sphere creates an end-to-end, exceptionally secure IoT solution that includes everything from the device's hardware and operating system to the dependable process of sending messages from the device to the message hub. For internet-connected devices, Azure Sphere provides built-in communication and security features.

Big Data

Big Data is a word that refers to a vast collection of data that continues to increase exponentially over time. In

terms of business value, big data provides better service, products, and increased profitability.

There are numerous services and technologies in Azure that deal with Big Data, some of which are listed below:

Azure Data Lake Analytics

Azure Data Lake Analytics is a job analytics solution that simplifies huge data and is available on demand. Parallel processing is used in Data Lake Analytics, which implies two or more processors handle the same data at the same time.

HDInsight

Azure HDInsight is a cloud-based big data analytics service from Microsoft that assists businesses in processing large amounts of streaming or historical data. Azure HDInsight makes storing large amounts of data simple, efficient, and cost-effective.

Azure Databricks

Azure Databricks is an analytics platform built on Apache Spark, an open-source cluster computing framework designed to complement Microsoft Azure. Databricks distribute and process a dataset across multiple machines at the same time. You do not need a lot of computers or upkeep when you use Databricks.

Big Data Outcomes

Collectively, big data services can bring the following outcomes for you.

- Speed
- Cost Reduction
- Better Decision Making
- New Products and Services
- Artificial Intelligence

Artificial intelligence (AI) refers to a machine's ability to mimic intelligent human behavior. Although AI and Machine learning are sometimes lumped together in Microsoft, AI is often referred to as Machine Learning or AI, a sub-category of Machine Learning.

According to Microsoft, how machine learning may be employed on the cloud platform is broken down into three pieces.

- Models
- Knowledge Mining
- Built-in Apps

Azure Cognitive Services

Cognitive services make AI accessible to all developers without needing machine learning skills. All you need is one API call to embed the feature to see, hear, speak, search, comprehend, and expedite the decision-making in your apps. Azure Cognitive Services may be used to tackle challenges like assessing text for emotional sentiment or analyzing photos to identify items or faces. You do not need any special machine learning or data science experience to use these services. Developers can use APIs to access Azure Cognitive Services and easily incorporate these features with only a few lines of code.

Azure Machine Learning Studio

The Azure Machine Learning Studio is the machine learning service's top-level tool. It is a visual tool for managing all of your machine learning requirements. It gives data scientists and developers a centralized area to work with all of the artifacts for designing, training, and deploying machine learning models.

Machine Learning Services

- End-to-End Service
- Tooling
- Automation

Azure Bot Service

Bot Framework and Azure Bot Service are tools for creating virtual agents that understand and answer inquiries like humans do. In comparison to Azure Machine Learning and Azure Cognitive Services, Azure Bot Service offers a distinct use case. It does this by forming a virtual agent that can converse intelligently with humans. Behind the scenes, the bot you make applies other Azure services, such as Azure Cognitive Services, to learn what their human counterparts are asking for.

Serverless

Serverless computing is a critical component of current cloud computing. By removing the requirement for developers to manage infrastructure, the serverless architecture allows them to build applications faster. It is a PaaS at its most extreme. The infrastructure required for running code with serverless apps is automatically offered, scaled, and managed by the cloud service provider.

Benefits of Serverless Model

- No Infrastructure Management
- Dynamic Scalability
- Faster Time to Market
- More Efficient Use of Resources

Azure Functions

Azure Functions is the computational component of Azure's serverless services. It is called a function since it just has one task to complete each time. That is, you can use Functions to write code without having to worry about deploying it or setting up virtual machines to run it on.

Azure Logic Apps

Azure Logic Apps is a cloud service that connects systems inside and outside the Azure Platform; you may integrate apps, data, and services across enterprises or even an entire system. Using this software, you may automate and orchestrate business processes, tasks, activities, and workflows.

Azure Event Grid

An event is an activity or occurrence that can be identified by a computer and has importance for system application in the computing world. Azure Event Grid makes it simple to create apps based on event-driven architectures. Events from Azure services, such as storage blobs and resource groups, have built-in support in Event Grid.

Data sources and event handlers are linked together by Event Grid. When photos are added to a blob storage container, you can use Event Grid to trigger a serverless function that analyzes them.

DevOps

DevOps is a word that combines the development and operations of the term to describe a joint or cooperative approach to the activities performed by an organization's application development departments and IT operations.

Azure DevOps

Azure DevOps provides developer tools to aid teams in project planning, application development, and product design and deployment.

You may use one or more of the following services, depending on your business needs:

- Azure Boards
- Azure Pipelines
- Azure Repos
- Azure Test Plans
- Azure Artifacts

Azure DevTest Labs

Azure DevTest Labs enables team developers to successfully manage Virtual Machines (VMs) and PaaS technologies without the need for permissions. It is primarily concerned with environmental management. Developers and engineers can use this to set up a testing and development environment.

Monitoring

Azure Advisor

Azure Advisor evaluates your Azure resources and makes recommendations to improve their dependability, security, and performance and achieve operational excellence and lower expenses. The advisor is designed to save you time when it comes to cloud optimization. The recommendation service includes actions you can take immediately, postpone, or dismiss.

Azure Monitor

Azure Monitor is a platform for aggregating, evaluating, visualizing, and potentially acting on metrics and recording data from your entire Azure and on-premises environment.

Azure Service Health

Azure Service Health shows you a customized view of the health of the Azure services, regions, and resources you use.

Set up Azure Environment

Microsoft provides a variety of tools and services to help you manage your cloud environment, each tailored to certain situations and users.

The Azure Portal

You may get almost all of Azure's features by using the Azure portal, a web-based user interface. The Azure portal has a nice graphical user interface that lets you see all the services you are using, create new ones, modify them, and read reports. The Azure portal is how most

users first experience Azure. But, as your Azure usage grows, you will possibly prefer a more repeatable code-centric way to manage your Azure resources.

The Azure Mobile App

When you are not at your computer, the Azure mobile app allows you access to your Azure resources. You can accomplish the following with it:

- Keep track of your Azure resource's health and condition.
- Check for notifications, identify and repair problems quickly, and restart a web app or virtual machine.
- Run the Azure CLI or Azure PowerShell commands to handle your Azure resources.

Azure PowerShell

Azure PowerShell is a shell with which developers, DevOps, and IT professionals can perform commands called cmdlets. These commands call the Azure Rest API to deliver every conceivable management job in Azure.

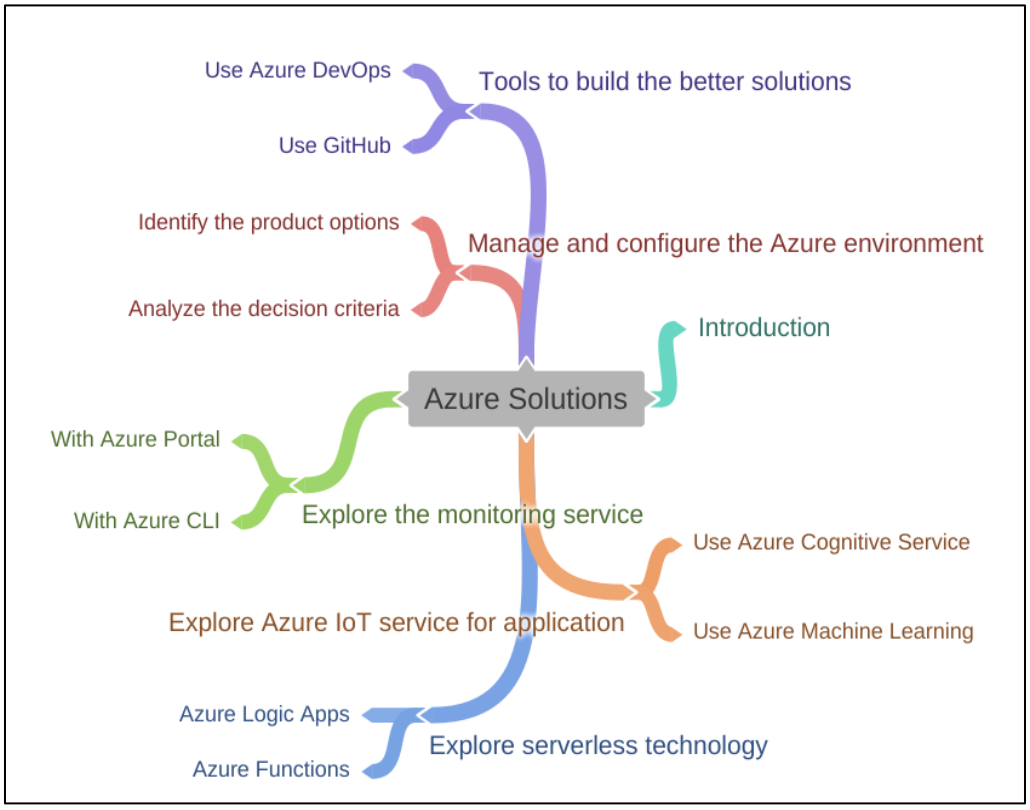
The Azure CLI

The Azure CLI command-line interface is an executable program that allows a developer, DevOps specialist, or IT specialist to run Bash commands. The instructions use the Azure Rest API to do all of Azure's management tasks. You can run the commands individually or merge them into a script and execute them together for the routine setup, teardown, and maintenance of a single resource or an entire environment.

ARM templates

You can declare the resources you want to use in a declarative JSON language using Azure Resource Manager templates (ARM templates). The benefit is that the entire ARM template is validated before any code is executed to ensure that the resources are built and connected correctly. The template then coordinates the parallel generation of those resources. If you need 50 instances of the same resource, all 50 instances are created at the same time.

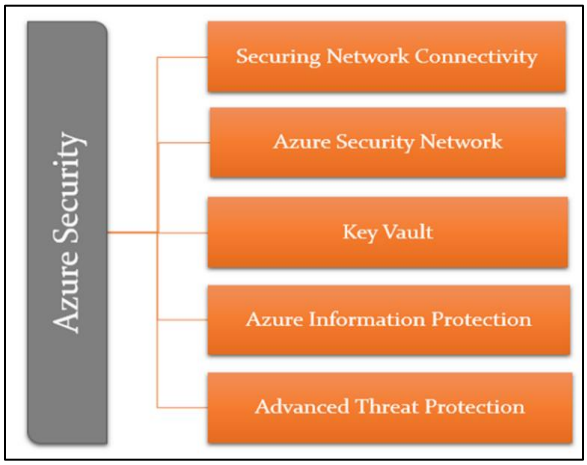
Mind Map



Chapter 08: Security

Why Security is Important?

Security refers to a collection of policies or regulations that allow traffic to be sent to the network efficiently. The network's security is critical, especially when infrastructure communication is done over the internet.



Zero Trust Model

A security concept known as "Zero Trust" guards resources by preparing for the worst-case situation. Zero Trust checks each request as though it came from an uncontrolled network at first, assuming there has been a breach.

Organizations now require a new security paradigm that adapts to the complexity of the contemporary environment, embraces the mobile workforce, and safeguards people, devices, apps, and data no matter where they are.

Microsoft strongly advises the Zero Trust security architecture, which is founded on the following tenets, to address this new computing world:

Verify explicitly - Authenticate and authorize consistently depending on all accessible data points.

Use least privilege access - Use Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive rules, and data protection to restrict user access.

Assume breaches - Consider a breach; reduce blast radius and segment access. Make sure the encryption is end-to-end. Use analytics to get visibility, support threat identification, and strengthen defenses.

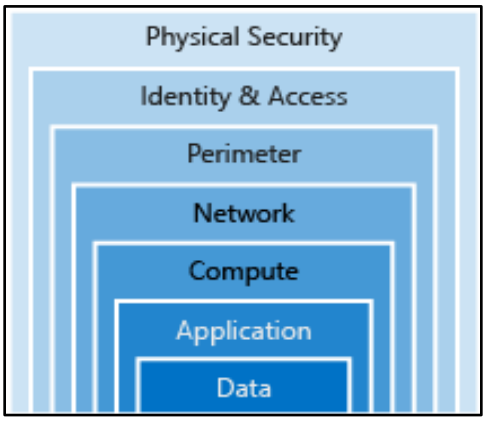
Defense in Depth

The following are some significant points from Defense in Depth:

- A strategy to stifle any attempt to gain unauthorized access to information.
- Layered approach: Each layer protects the others, so if one is compromised, the others prevent further exposure.
- Microsoft uses it in both physical data centers and Azure services.

In cloud computing, there are seven general layers of security, and Azure is no exception:

- Physical
- Identity and Access
- Perimeter
- Network
- Compute
- Application
- Data

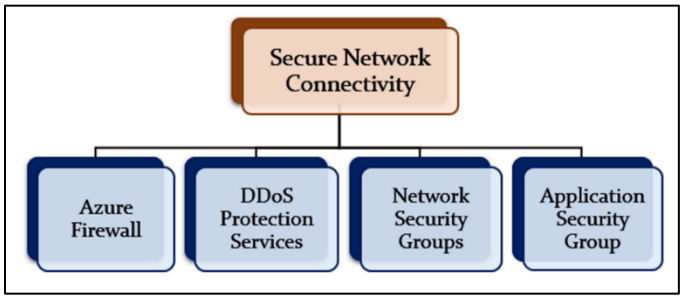


Securing Network Connectivity

Users have access to everything through Azure networks. Microsoft Azure's resources and services are all

connected to a network to allow users, processes, and other services to communicate with one another.

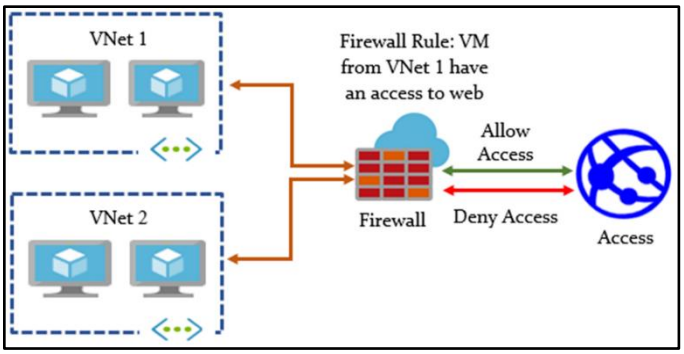
Secure network connectivity is critical for achieving optimal network performance.



Azure Firewall

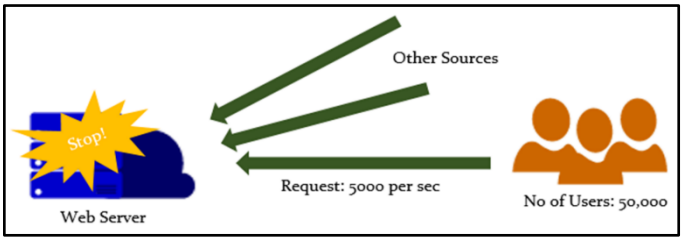
A firewall in Azure is a critical service that protects the network from unauthorized traffic.

- Rules
- Variation
- Compulsory Bit



Distributed Denial of Service Attacks (DDoS)

The most prevalent attack on internet-connected systems is Distributed Denial of Service (DDoS). It occurs when a large number of requests arrive from different sources, causing the server's usual operation to be disrupted.



DDoS Protection Service

- **Target a Website:** A large number of servers are directed at the same website or machine to disable it. GitHub, for example, was a target with 127 megabyte requests per second.
- **Azure Protection Service:** DDoS protection is available with Microsoft Azure. Depending on the application's user needs, this service offers varying levels of protection. The Azure protection service detects and mitigates DDoS attacks.
- **No Halt:** Due to Azure's global presence, the Azure Protection service would not disrupt the normal operation of other services on the website.

Network Security Groups

The network's security group provides a secure management environment. The configuration of a Virtual Network (VNet) where multiple Virtual Machines (VMs) within the subnet are connected requires the use of a Network Security Group (NSG).

Application Security Group

The application running on that particular VM or subnet in the network is protected by the Application Security Group (ASG). ASG ensures application security, while NSG ensures traffic flow security.

Microsoft Defender for Cloud

Users can monitor security features for Azure resources as well as on-premises resources using Azure Microsoft Defender for Cloud. Microsoft Defender for Cloud is a portal within the Azure portal dedicated to Azure Security. The Microsoft Defender for Cloud displays a danger alert that Azure detects and mitigates for its users. Microsoft Defender for Cloud can also be used in a hybrid cloud environment.

Sections in Azure Microsoft Defender for Cloud

Each Microsoft Defender for Cloud interface area displays a graphical depiction of the unique performance behavior of security capabilities.

- Policy, Compliance, and Subscription Coverage
- Integrate with Other Cloud Providers
- Alerts for Resources Security
- Networking

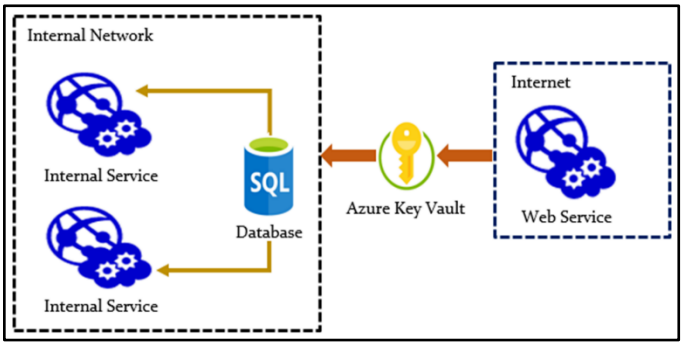
How to use Microsoft Defender for Cloud?

Azure users must perform these three steps to take advantage of the Microsoft Defender for Cloud infrastructure security.

- Define Policies
- Resource Protection
- Response

Key Vault

Microsoft provides Azure Key Vault as a service to hide the key password and other information. It is the greatest way to keep your keys safe. You can share your secrets with others using Azure Key Vault without revealing the real secrets. Azure Key Vault is installed in the VM's storage account.



Features of Key Vault

Azure Key Vault has several key features, some of which are:

- Secure Hardware
- Application Isolation
- Global Scaling

Azure Information Protection

Azure Information Protection (AIP) allows you to share resources securely. Azure Information Protection allows you to share files, documents, and sensitive data inside and outside while maintaining complete control over it. The Azure Information Protection service is fully utilized by Microsoft 365.

Advanced Threat Protection (ATP)

Advanced Threat Protection (ATP) is the advanced and secure option for providing link security compared to the standard option. It adds an extra layer of security and user control to make the system more secure and protected.

Features of Advanced Threat Protection (ATP)

Several Azure Advanced Threat Protection (ATP) components ensure the safety of links and assess security risks.

- Monitor Users
- Supervised User's Behavior
- Propose Changes

Cyber-Attack Kill-Chain

The kill chain for a cyber-attack is a series of steps that define how the attack is planned and executed. This deployed approach provides for the detection and response to an attack. The model reveals seven stages in which cyber-attack reaction and detection are possible.

Azure Sentinel

Sentinel is a security information and event management (S-I-E-M) or SIEM (Security Information and Event Management) solution. For any cloud infrastructure, this is a regularly used tool.

Azure Dedicated Host

Virtual machines (VMs) in Azure run on centralized hardware that Microsoft controls. Your VM workloads are separated from workloads other Azure users run, even though the underlying hardware is shared.

Some businesses must adhere to regulatory compliance, which necessitates that they are the sole users of the actual machine hosting their virtual machines. Azure Dedicated Host hosts your Azure VMs for Windows and Linux on dedicated physical servers.

VM relationships with dedicated hosts and host groups are depicted in the following diagram. A physical server in an Azure data center is associated with a dedicated host. A group of devoted hosts is known as a host group.

There are lots of advantages of cloud computing benefits, like:

- Availability Zones
- Fault Isolation
- High Availability
- Scale Sets

You can use Windows, Linux, or SQL Server as your VM image. Save some coins by using existing software licenses that you might have, for example, Windows

Server or SQL Server. A Dedicated Host is a good alternative for the hardware-conscious cloud user, but it can also get expensive. Use it wisely.

Benefits

Dedicated Azure Host:

- Gives you access to and control over the server infrastructure that hosts your Azure virtual machines.
- By placing your workloads on an isolated server, assists in meeting compliance standards.
- Allows for the customization of the host's processor count, server capabilities, VM series, and VM size.

Availability Considerations for Dedicated Host

The actual server in Microsoft's cloud data center receives the dedicated host after Azure has provisioned it.

You can set up several hosts in a host group for high availability and distribute your virtual machines across them. A benefit of maintenance control is that VMs can use it on dedicated hosts. With the use of this function, you can choose a 35-day rolling window for when routine maintenance upgrades take place.

Pricing

No matter how many VMs you deploy to a dedicated server, you will only be charged for that one. The VM family, kind (hardware size), and region all affect the hosting price.

The host and virtual machines (VMs) are invoiced independently from software licensing, storage, and network consumption. See Azure Dedicated Host price for further details.

Combine Azure services to create a complete Network Security solution

Secure the perimeter layer

The perimeter layer is responsible for defending your company's resources against network-based threats. It is critical to recognize these attacks, notify the proper security teams, and eliminate their impact to keep your network secure. To do so, follow these steps:

- Filter large-scale attacks with Azure DDoS Protection before they may cause a denial of service for consumers.
- With Azure Firewall, you can use perimeter firewalls to detect and notify of dangerous threats on your network.

Secure the network layer

At this layer, the goal is to limit network connectivity across all of your resources to only what is necessary. Limit communication to only what is required by segmenting your resources and using network-level rules.

You can limit the possibility of lateral migration across your network by blocking connectivity. Create rules that define allowed incoming and outbound communication at this tier using network security groups. Here are some best practices to follow:

- By segmenting your network and implementing access rules, you can limit communication between resources.
- By default, deny.
- Limit inbound internet access and outgoing internet access as needed.
- Implement a secure network to an on-premises network

Combine Services

You may mix Azure networking and security services to manage your network security and give more layered protection. You can integrate services in two ways:

Network Security Groups and Azure Firewall

The Azure Firewall adds to the capabilities of network security groups. They give superior defense-in-depth network security when used together.

Network security groups enable distributed network-layer traffic filtering to limit traffic to resources within virtual networks in each subscription.

Azure Firewall is a centralized network firewall as a service that is fully stateful. It protects networks and applications at the network and application levels across many subscriptions and virtual networks.

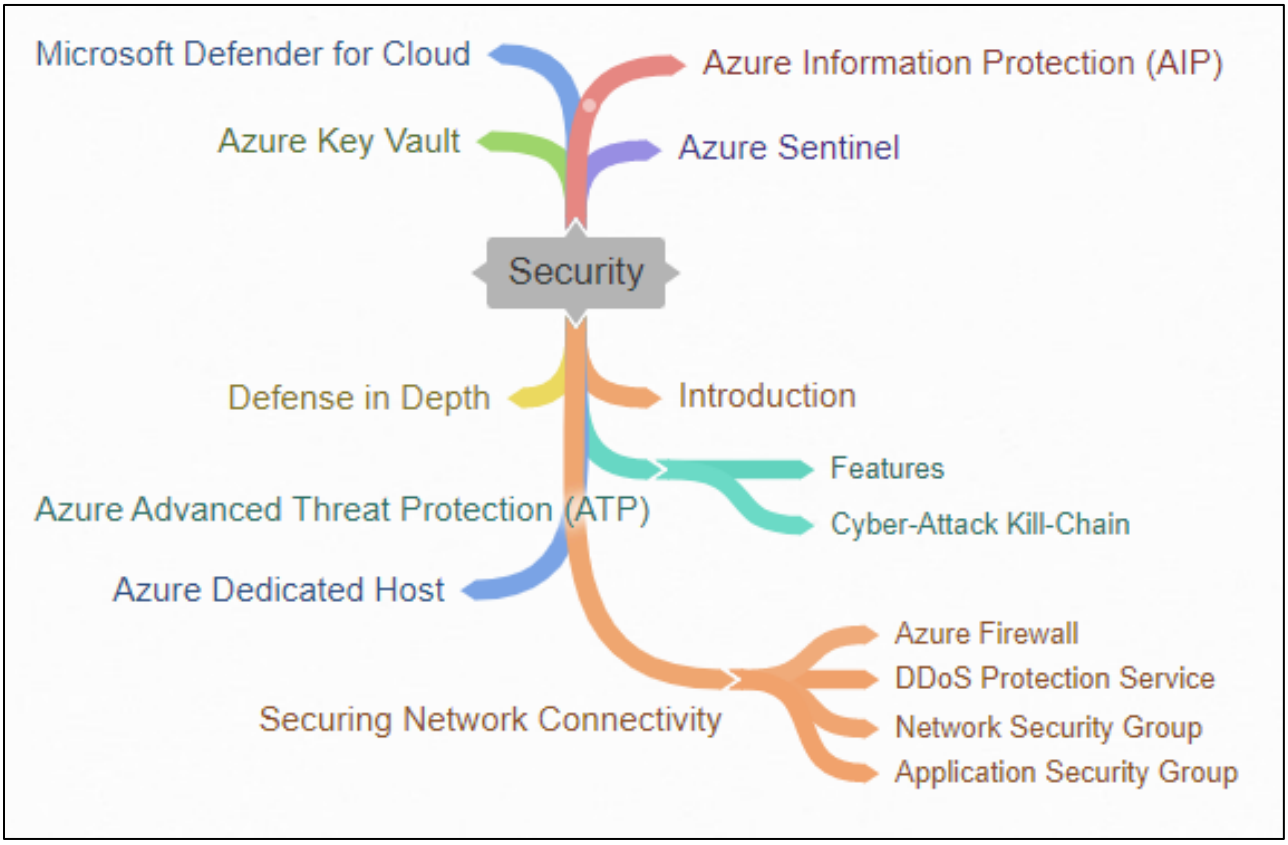
Azure Application Gateway Web Application Firewall and Azure Firewall

Web application firewall (WAF) is an Azure Application Gateway feature that provides centralized, inbound security against common exploits and vulnerabilities for your web applications.

Azure Firewall offers the following features:

- Non-HTTP/S protocols are protected from inbound traffic (for example, RDP, SSH, and FTP).
- All ports and protocols are protected at the network level for outbound traffic.
- Outbound HTTP/S protection at the application level.

Mind Map



Chapter 09: Privacy, Compliance, and Trust

Build a cloud governance strategy on Azure

Governance

We all know that most businesses use the Azure platform because of its flexibility in allowing developers to build, manage, update, and delete resources as needed. Unwanted access to the resource, on the other hand, can result in unintended costs. To overcome this, Azure provides a resource access governance solution, which is managing, monitoring, and auditing resource usage to meet goals and requirements.

Azure Policy

Azure Policy is a tool for creating policies in the cloud. You can manage and assign policies to resources with numerous rules using Azure Policy, ensuring that individual resources comply with your business standards and SLAs. Azure Policy is a system that allows you to accept or refuse things by default.

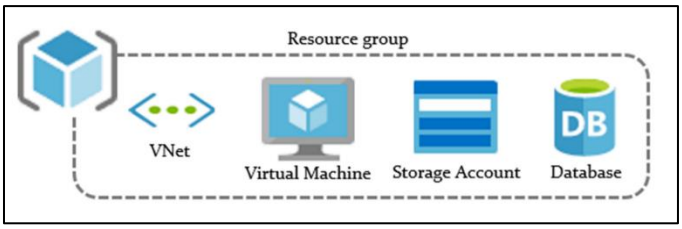
Concept of resource groups

You may use Azure Resource Manager (ARM) to organize your resources, enforce standards, and safeguard your key Azure resources from being accidentally deleted. The containers for Azure resources are called resource groups. You may give your Azure resources some order and organization by grouping resources similar to consumption, type, or location.

Tags enable you to improve the arrangement of your resources further. Tags can be used to link custom details to a resource or collection of resources, such as the cost center or billing department. Tags and resource groups are excellent for organizing existing resources and resource groups.

Resource Groups

The resource group is like a bucket that stores all of the components you will need to manage from start to finish, from initiation to retirement. For example, deleting a resource group and all the items it contains is much quicker than deleting the VM, which counts the virtual network and all objects separately.



Tagging

In Azure, tagging is a label with key-value pairs that may be provided to resources to make them more easily identifiable. The name ad value contains some specific number, as indicated by the key.

Secure resources with RBAC

A role in Microsoft Azure is a set of tasks that you can or cannot perform. With your role definition, you might be able to construct and administer virtual machines. It, on the other hand, stops you from removing them.

- **Owner –** Gives you complete access to Azure resources, which you can delegate to other users.
- **Contributor –** This job is similar to that of an owner in that it grants full access to Azure resources. Control, on the other hand, cannot be delegated. Only the resources are shown to the reader.
- **User Access Administrator** - It can govern Azure resource access.

Secure Azure resources with RBAC

Introduction

Azure resource protection, such as virtual networks, websites, virtual machines, storage, and so on, is extremely challenging for any company or organization, particularly when using the cloud. Azure-based resources and services are being used by businesses and organizations to develop their solutions. Furthermore, they wish to secure and preserve their resource from unintended consequences, such as data loss, hacking, etc. Companies can also grant resource access to their employees so they can easily perform their duties.

Role Based Access Control (RBAC) is used to manage and safeguard Azure resources and grant use to various employees and allow them to access the resource from a certain location. RBAC is an authorization system that secures and protects your Azure resources while also granting access to employees and managing who has access to them and where they can access them (location).

Azure Subscription

Azure Active Directory (Azure AD) is also utilized for identity and access control when dealing with RBAC. You must use an Azure subscription when you begin working with Azure. A single Azure Active Directory is tied to a single Azure subscription. The Azure resources in the Azure subscription can be managed and controlled by users, groups, and many applications in that directory. For sign-on (SSO) and access control, each Azure subscription uses a single Azure AD directory. You may extend your on-premises AD directory to the cloud using the Azure feature Azure AD Connect. This capability allows us to manage and monitor our Azure subscriptions using our existing work IDs.

Role-Based Access Control (RBAC)

Role-based access control is one of the most important aspects of the governance of uses and access to Azure resources. You can define fine-grained access management to resources using RBAC. You can also establish particular user access to an individual resource, such as what they can do with it and what areas of the resource they have access to.

RBAC works by assigning roles to users, and this role assignment is based on three elements, which are:

- Security Principal
- Role Definition
- Scope

Role Assignment

The process of integrating all of these to allow appropriate action to Azure resources is known as role assignment. The creation of a role assignment grants access and the deletion of that role assignment removes it.

Resource Locks

Resource locks are an option in Azure that can be used to prevent users from making needless changes or deletions. There are two modes for these locks. One is for deleting, while the other is for reading only. You can make any changes to that resource except delete it if you use delete lock. You can view the resource without altering, modifying, or deleting it if you have read-only access. Resource locks can be applied to subscriptions, resource groups, or any resource present in the resource group.

Azure Blueprint

It is an Azure resource creation template. The blueprint defines everything you will need to deploy in Azure's standard cloud infrastructure.

Azure Advisor for Security Assistance

Security Assistance is a part of the Microsoft Defender for Cloud and is available through Azure Advisor, which is a separate site within Azure.

Subscription Governance Strategy

You identify a cloud organization structure that suits your company's needs at the start of any cloud governance project. Typically, this phase entails building a cloud center of excellence team (also called a cloud enablement team or a cloud custodian team). This group has the authority to establish governance policies for the entire organization from a centralized place.

The subscription level is frequently where teams begin their Azure governance plan. When it comes to creating and managing subscriptions, there are three primary factors to consider:

- Billing
- Access Control
- Subscription Restrictions.

Azure Monitor

Azure Monitor uses telemetry data to improve your Azure experience. Azure Monitor provides a comprehensive solution for capturing, monitoring, and using cloud and on-site telemetry, maximizing flexibility and application efficiency. It assists you in understanding how your apps work and proactively detecting problems and the resources on which they rely.

Outcomes

The outcome of using Azure Monitor:

- Maximize performance
- Maximize availability
- Identify issue

Azure Service Health

With Azure Service Health, you will be notified whenever a planned maintenance or service incident occurs. You will be notified about platform maintenance, whether it is planned or unplanned, with Azure Service Health. It possesses the following characteristics:

- Dashboard
- Custom Alerts
- Real-time Tracking
- Free Service

Compliance

The general principle that cloud services deliver must adhere to the requirements faced by cloud customers is strongly compliant. This is a very important issue with new cloud computing services, and many IT professionals are thoroughly looking at it. If any company in the EU does not take compliance seriously, they then have to pay a massive fine. For example, suppose any company is dealing with paying customers and does not comply with privacy and regulations about personal data. In that case, the company could be fined 4% of the annual global turnover. Below are some different standards and regulations cloud customers need to comply with.

Available Compliance Category on Azure

The image below displays a few of the more well-known compliance products offered on Azure; however, there are many more. These products are divided into four categories: international, US government, business, and regional.

A sample shows some Azure compliance services organized across global, US government, industry, and regional categories.

Let's take a deeper look at a couple of them to get an idea of the breadth of compliance services that are offered on Azure.

Criminal Justice Information Service

The Criminal Justice Information Services (CJIS) Security Policy must be followed by any US state or local organization that wishes to use the FBI's Criminal Justice Information Services database.

The CJIS Security Policy is only formally committed to compliance by one major cloud provider, Azure. Microsoft complies with the same standards as public safety and law enforcement agencies.

Cloud Security Alliance STAR Certification

Cloud Security Alliance (CSA) STAR Certification, which entails a thorough independent third-party examination of a cloud provider's security posture, has been earned by Azure, Intune, and Microsoft Power BI.

The International Organization of Standards/International Electrotechnical Commission (ISO/IEC) 27001 certification and fulfillment of the Cloud Controls Matrix criteria are prerequisites for STAR Certification (CCM). With the use of this accreditation, a cloud service provider can:

- Meets the relevant ISO/IEC 27001 criteria.
- Has addressed the CCM's list of issues that are essential to cloud security.
- Has been evaluated for the management of activities in CCM control areas against the STAR Capability Maturity Model.

European Union Model Clauses

Microsoft provides standard contractual clauses for the European Union (EU) that offer legal protections for the transfer of personal data outside of the EU.

Microsoft is the first company to have its contractual privacy protections for its enterprise cloud clients, Azure, jointly approved by the EU's Article 29 Working Party as compliant with current EU criteria for cross-border data transfers. By complying with this standard, Azure users can utilize Microsoft services to freely transfer data from Europe to the rest of the globe using Microsoft's cloud.

Health Insurance Portability and Accountability Act

A US federal statute known as the Health Insurance Portability and Accountability Act (HIPAA) governs patient Protected Health Information (PHI).

Azure gives clients a Business Associate Agreement (BAA) in accordance with HIPAA and the HITECH Act, which outlines adherence to specific security and privacy rules. Microsoft provides a BAA as a contract amendment to Azure customers to support customers in their compliance activities.

National Institute of Standards and Technology Cybersecurity Framework

The Cybersecurity Framework (CSF) of the National Institute of Standards and Technology (NIST) is a voluntary framework including standards, recommendations, and best practices for handling cybersecurity-related risks.

Independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits have been performed on Microsoft cloud services. FedRAMP-certified Microsoft cloud services are available.

Office 365 is additionally accredited to the goals outlined in the NIST CSF with a verified assessment carried out by the Health Information Trust Alliance (HITRUST), a prominent organization for developing and accreditation security and privacy standards.

UK Government G-Cloud

A cloud computing certification for services used by British government agencies is called the United Kingdom (UK) Government G-Cloud. The UK government has granted Azure official recognition.

Industry Compliance

This refers to the legislation and rules the industry generally has to comply with. The most common three legislations and rules are:

- **General Data Protection Regulation (GDPR)** - Its main objective is to protect individuals and the processing of their data. With this, you get personal data back to an individual rather than a company that owns it. To protect consumer's data, forces companies to implement a lot of tools.
- **ISO Standards** - ISO is the International Standardization Organization, and they have a huge number of compliance categories. Generally, it is compliant with quality and customer satisfaction, which is ISO 9001:2008
- **NIST** – NIST is the National Institute of Standards and Technology and focuses purely on the technology industry. NIST guidelines are designed in such a way that compliance with NIST also means compliance with multiple Federal US regulations. CyberSecurity Framework is one of the most famous frameworks there is

Azure Compliance Manager

For Compliance, Azure provides you the Azure Compliance Manager because the company knows about compliance and as it knows about your resources, so it can easily combine the tools and give you a recommendation as per that. There are many benefits of using Compliance Manager in Azure, some of which are:

- It gives you a recommendation on ensuring compliance with GDPR, NIST, ISO, or others
- It assigns tasks to your team and tracks the progress of the task; each member is responsible for a certain compliance area
- With that, you have a compliance score to chase perfect compliance
- It gives you secure storage for uploading the compliance documents to prove compliance
- It gives you a report on compliance of data so that you can give that report to your managers and auditors

Microsoft Privacy Statement

The Microsoft Privacy Statement details the types of personal information that Microsoft gathers, how it uses it, and why.

The privacy statement covers all of Microsoft's services, websites, applications, software, servers, and gadgets. This list includes items like enterprise and server solutions, home-use gadgets, and educational software for students.

The privacy statement from Microsoft also includes details pertinent to particular goods like Windows and Xbox.

Online Service Terms

The terms of the contract between Microsoft and the consumer are known as the Online Services Terms (OST). The OST outlines each party's responsibilities for the processing and security of customer and personal data. The OST especially applies to Microsoft's subscription-based online services, such as Azure, Dynamics 365, Office 365, and Bing Maps.

Data Protection Addendum

The conditions for data processing and security for online services are further defined in the Data Protection Addendum (DPA). These words comprise:

- Adherence to the law.
- Revealing processed data.
- Data Security covers security procedures and guidelines, data encryption, data access, client obligations, and audits compliance.
- Transfer, storage, and destruction of data.

How to use the DPA:

- Visit the Documentation and Licensing Terms page.
- Enter DPA in the search box.
- Find the link to the DPA in your chosen language in the search results. As an alternative, you can filter the results by typing your chosen language in the search field that appears. Here is an example that obtains the DPA in English.

Transparency is crucial when it comes to how a cloud provider explains its privacy rules and handles your data. Microsoft's commitment to protecting data and privacy in the cloud is outlined in the Microsoft Privacy Statement, the OST, and the DPA.

Azure Government Cloud

In order to know what compliance is, who makes guidelines, bodies, and framework, and how Azure manages it all, you have two regions and offerings that are unique when there is compliance.

First is Azure Government Cloud; if you are a US government body or are contracted for one, you can access Azure resources in Azure Government Cloud regions. They are separate dedicated data centers. With these dedicated data centers, you get guaranteed that only US federal, state, and local governments have access to this dedicated instance with operations controlled by Screened US citizens.

It ensures compliance with required US government agencies and level 5 Department of Defense approval. With this, you can get all the benefits of Azure like HA, scalability, and managed resources.

China Region

It is the second specific region when it comes to compliance. As a country, China has very specific and strict requirements when there is data, internet, or online entities, so when you need to provide cloud services here, you have to use the China region in Azure. This means that Azure has physically separated data centers located in China without any connection to the other regions of Azure. All data is stored in China at all times. For example, if China is included in the region for DynamoDB, it will not work globally. Within that, you are completely compliant with all Chinese regulations. All of these physically separated locations are managed by Chinese companies.

Azure China 21Vianet

21Vianet operates Azure China 21Vianet. It is a geographically segregated instance of cloud services in China. Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly-owned subsidiary of Beijing 21Vianet Broadband DataCenter Co., Ltd., operates and transacts Azure China 21Vianet independently.

According to the China Telecommunication Regulation, cloud service providers, infrastructure as a service (IaaS), and platform as a service (PaaS) providers must have value-added telecom permits. These permits are only available to locally registered businesses with less than 50% foreign participation. To comply with this regulation, 21Vianet operates the Azure service in China based on Microsoft-licensed technologies.

Azure products and services available in China

The Azure services have similar service standards and are built on the same Azure, Office 365, and Power BI technologies that make up the Microsoft global cloud service. Where applicable, customers and 21Vianet execute Azure agreements and contracts in China.

The fundamental elements of IaaS, PaaS, and software as a service are all present in Azure (SaaS). Network, storage, data management, identity management, and numerous other services are among these elements.

The majority of the capabilities offered by worldwide Azure, including geosynchronous data replication and autoscaling, are supported by Azure China 21Vianet. Even if you already use global Azure services, you may need to rehost or modify any or all of your apps or services to run in China.

Privacy

Compliances are an extension of privacy. Because privacy is a key feature of Azure, there is no one service or location for it.

Trust

In Azure, there are two services in terms of Trust. One is Trust Center, and the other is Service Trust Portal.

Trust Center

Trust Center is a shortcut to knowing all the things that Microsoft does to make sure that you do not lose trust in Azure and other services. With this, you have a link to learn about security, privacy, GDPR, the location of your data, compliance, and more. This link lets you know more about security implementations, privacy implementations, etc.

The Trust Center demonstrates how Microsoft implements and supports security, privacy, compliance, and transparency in all of its cloud products and services and the company's guiding principles for preserving data integrity in the cloud. The Microsoft Trusted Cloud Initiative's Trust Center is a key component that offers materials and assistance to the legal and compliance sector.

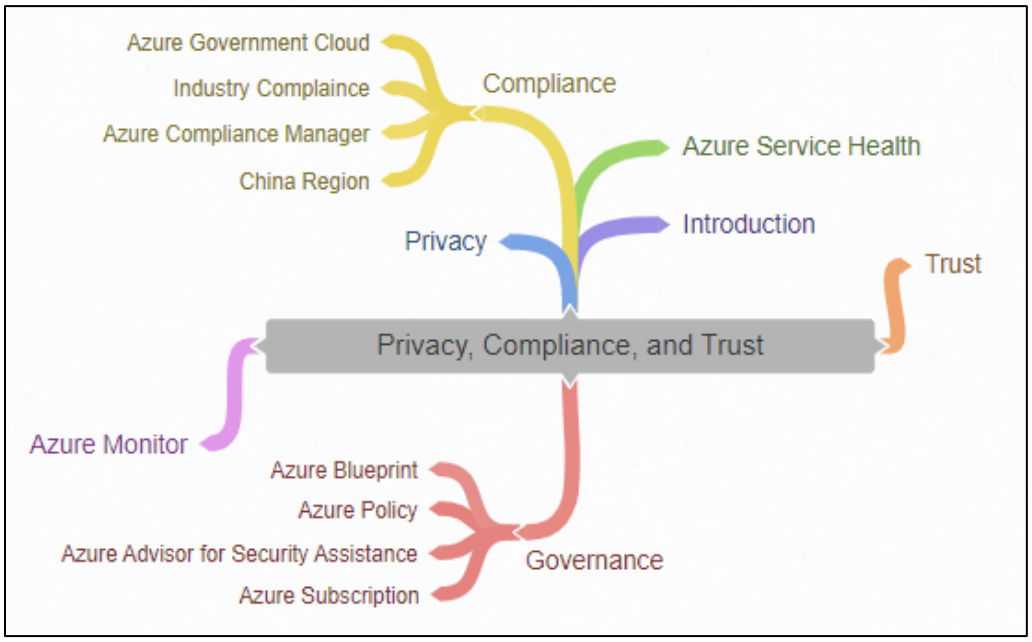
The Trust Center gives you:

- Comprehensive details on the capabilities, offerings, rules, and practices used by Microsoft cloud solutions in terms of security, privacy, and compliance.
- Additional sources for every subject.
- Links to forthcoming events as well as the security, privacy, and compliance blogs.
- For additional employees in your company who might be involved in compliance, security, and privacy, the Trust Center is a valuable resource. These individuals consist of business managers, privacy and risk officers, and legal compliance teams.

Service Trust Portal

Service Trust Portal is a location to review all the independent reports about Azure. It is a portal of proof that they are compliant with many millions of different standards and certifications. It is crucial to know that Azure complies with the various quality and security standards more than any other cloud provider. In short, we can say that it is a one-stop-shop for security related to Azure Cloud.

Mind Map


Azure Government Cloud
Industry Complaince
Azure Compliance Manager
China Region
Compliance
Azure Service Health
Introduction
Privacy
Trust
Privacy, Compliance, and Trust
Azure Monitor
Azure Blueprint
Azure Policy
Azure Advisor for Security Assistance
Azure Subscription
Governance

Chapter 10: Pricing

Azure Pricing Structure

The following factors determine the Azure price structure:

- Pay for the resources you access
- Pay for the number of hours you use
- Pay depending on the size of the resource
- Service payment is tiered
- Pricing as per the location of service

Subscriptions

Microsoft Azure's price is based on a subscription fee that is tied to the amount of time you spend using the Azure infrastructure. The subscription contains all Azure resources; you will not be able to access any resources until you have subscribed. When you join Azure, you get an Azure subscription, and all of the services you create are included.

Subscription in Azure can be defined as:

- Multiple Subscriptions
- Billing Admin
- Billing Cycle

Offer Types

Azure has a large number of active offers kinds at any given time. Depending on your subscription type, you may be eligible for the deal.

Management Groups

When it comes to subscriptions, Azure's Management Groups feature is beneficial. Management groups may mention the following items:

- Group Subscriptions
- Organize
- Billing Logic

Cost Management

We understand that cost control can be costly when resources and services are in use. When you use Azure resources or services, you must first purchase them; otherwise, you will be unable to use them. Because tracking every single expenditure is so laborious, you will need a service that automates cost management. Cost management in Azure can be done in a variety of ways, some of which are listed below.

Azure Free Account

You are eligible for a free Azure account if you have never had a free Azure trial and have never been a paying Azure subscriber.

Azure Cost Management

Azure Cost Management is a useful tool in Azure that allows you to examine your costs in detail. You may use cost management to define a budget for your Azure spending, set up configurable alarms to alert you when you reach a budgeted limit, and analyze your costs in detail.

Pricing Factors

Cloud computing pricing is difficult to predict and calculate. Networks, connections, virtual machines, firewalls, storage accounts, functionalities, and so on are all available in an Azure account.

The key elements that influence expenses are the number of resources, kind of resource, Azure regions used, and bandwidth.

Pricing Calculator

The Azure pricing calculator can help you estimate expenses based on the products you want to use, where those products will be deployed and other factors.

Total Cost of Ownership (TCO) Calculator

The pricing calculator can help you estimate your costs for new Azure applications, but the TCO calculator is a better option if you have on-premises applications that you want to migrate to Azure and want an estimate of how much you can save.

Best Practices for Minimizing Azure Costs

To implement cost control effectively and reduce costs, you need to:

- Be equipped with the right tools for performance
- Be responsible for costs
- Take appropriate action to reduce expenses

Spending Limits

Azure spending limits are advised to keep you from going over your credit limit and to keep track of the entire cost of your Azure subscription.

Default Limit: Default spending limits will apply to some Azure customers with monthly credits. This might be anything between 0 and 150 dollars for a free account and 150 dollars for a Microsoft membership account. When the credits are depleted, the limit is reached.

No Increase: When the credits are depleted, either eliminate the spending limit or keep it in place.

No Spending Limit: Pay-as-you-go subscription has no spending limit functionality.

Quotas

A quota is a limit on certain properties of an Azure service.

Tags

Tags are non-functional labels assigned to resources or resource groups to keep track of their costs. You can add as many as you like to each resource.

The following are some common tag-recommended practices:

- Identify Roles
- Related Resources
- Filter
- Unambiguous

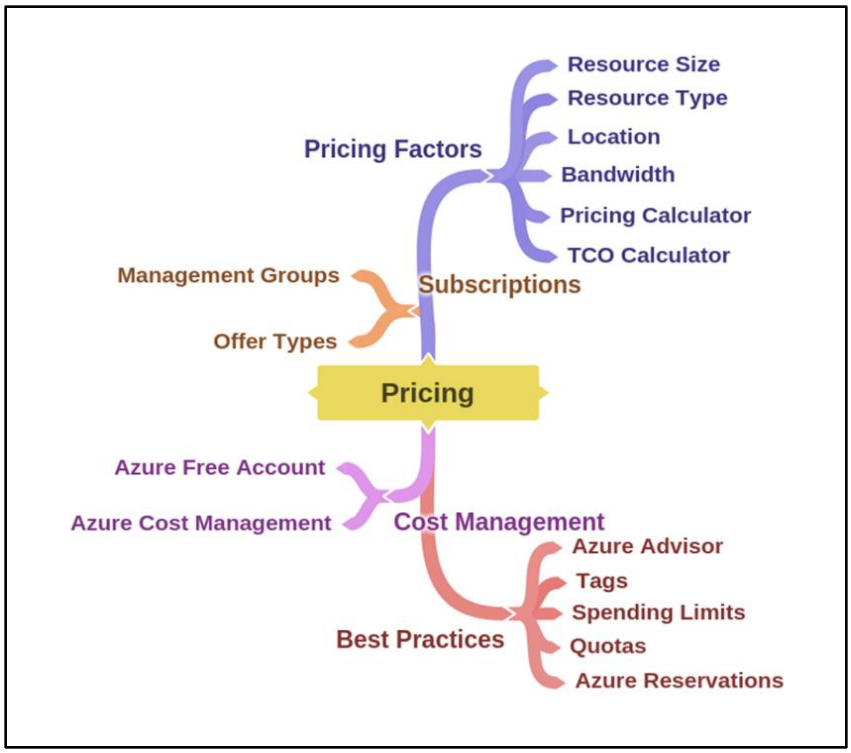
Reserved Instances

With Reserved Instance, you can prepay for a virtual machine or SQL Database compute capacity for one or three years.

Azure Advisor

Azure Advisor is a tool that discovers virtual machines that are underutilized in terms of CPU or network costs. Based on expected expenditures, you can then either shut down or resize the system to keep the machines functioning.

Mind Map



Chapter 11: Managing and Deploying Azure Resources

Introduction

The key architectural components of Azure, such as Resource Groups, Resource Manager Template, Geography, and Azure App Service, are covered in this chapter. The ARM template is a JavaScript Object Notation (JSON) file that serves as a deployment code for the resources in resource groups.

Azure Resource Groups

Azure Resource Groups differ in the number of Azure resources they contain. Azure Resource Groups assist with resource monitoring, management, and access control. All resources within a resource group can span several Azure regions using the resource group.

Azure Resource Groups allow you to manage a collection of Azure resources such as Virtual Machines, SQL Databases, and Storage Accounts. Resource groups make adding and removing resources simple while also allowing you to apply role-based access controls. Depending on the company's needs, the same sort of resources is generated within a resource group. There is no additional cost associated with the production of the resource group.

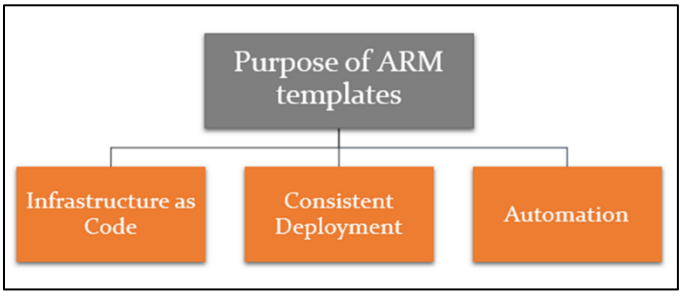
Azure Resource Manager

After deployment, Azure Resource Manager allows us to arrange and monitor all of the resources. The deployment parameters, variables, resource list, and output are specified using the Azure Resource Manager (ARM) template. It also includes the JSON file, which can be used to deploy resources more quickly

Purpose of ARM Templates

The main purpose of ARM templates includes:

- Infrastructure as Code
- Consistent Deployment
- Automation



Structure of ARM Templates

Azure Resource Manager Template is a simple template that contains:

- $schema,
- contentVersion
- Parameters
- variables
- functions
- resources
- outputs

Working with ARM Templates

After understanding the ARM template's concept and what is inside it, in this section, we will learn how to retrieve ARM templates, export the ARM template, and deploy resources using Cloud Shell.

When using the ARM template, you should perform the following deployments.

Deploy to a Resource Group

To represent the resources inside a single resource group, ARM templates are typically utilized. The deployment specifies which resources are available and which resource group configurations are available.

If you have numerous resource groups, you may also use an ARM template to deploy them. On the other hand, deploying various resource groups has become sophisticated and difficult. In such circumstances, you can make use of linked data.

Deployment Modes

If you have used the ARM templates before and wish to deploy the resource in the resource group, you will need to deploy several resources within the same resource. There are two options for accomplishing this.

- **Complete Mode –** The ARM template will erase all resources that are not in the template or are not in use.
- **Incremental Mode -** Nothing will be deleted during this deployment. Only the properties of the resources in the resource group will be updated. This is the default setting.

Deployment Tools

You have several alternatives when working with the Azure Resource Manager (ARM) template. Azure Portal, Visual Studio Code, Azure PowerShell, Azure CLI, and other tools are available. Advanced integration is possible with tools such as Visual Studio Code, CI/CD, and Azure pipelines.

Azure Marketplace

Azure Marketplace is a web marketplace with thousands of virtual machines, developer services, and applications. Azure Marketplace allows cloud-based products to be easily sold to others. It also facilitates application development by allowing users to seek assistance and use Azure Marketplace resources.

Azure Datacenter

Suppose you acquire Azure services, whether it is a SQL database, a web hosting virtual machine, or another of Azure's many services. All of these run on a physical infrastructure beneath some form of service, and a data center is a physical location that hosts these services. A typical data center has its power pooling and networking infrastructure, and it is used to house a group of network servers.

Geography

Azure divides the globe into regions based on geopolitical borders or country borders. Azure geography is a distinct market of two or more regions that keep data residency and compliance boundaries intact.

This division has several benefits.

- Customers with unique data residency and compliance requirements can keep their data and apps close by using geographies.
- Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are met within geographical bounds.
- Their link to dedicated high-capacity networking infrastructure makes geographies fault-tolerant enough to withstand entire region failure.

Azure Regions

The data centers are the foundation of Azure's worldwide infrastructure; a region is a collection of data centers connected by high-speed internet access.

Availability Zones

Within Azure regions, there are Availability Zones. These zones provide secure environments in which to run applications and data.

Availability Sets

Availability sets are logical combinations of VMs that give the highest level of application availability. For availability sets, there is no charge. For service within the availability set, Azure provides a 99.95 percent SLA.

Azure Arc

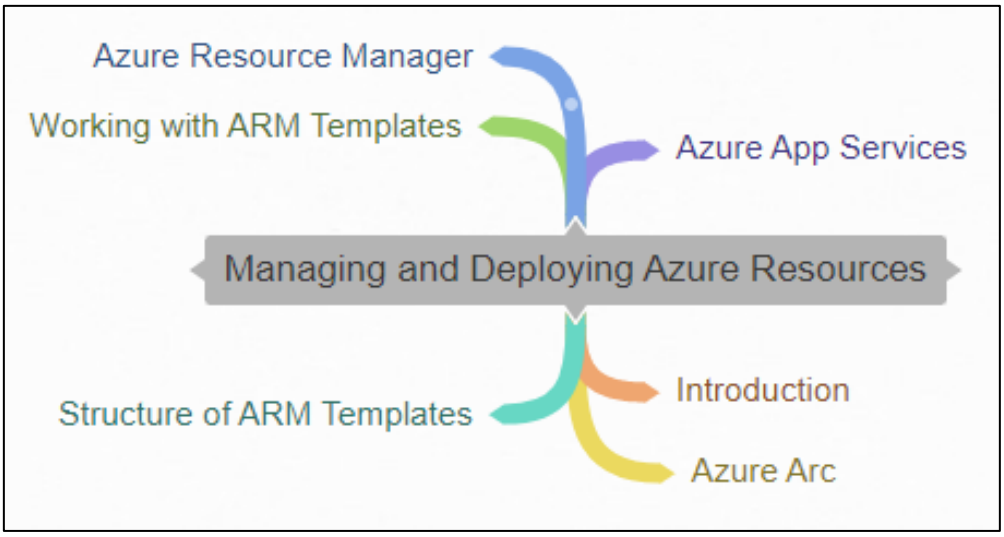
The management of hybrid and multi-cloud settings can become very challenging. Various tools are available to provision, configure, and monitor Azure resources. What about cloud resources in a multi-cloud configuration or on-premises resources in a hybrid configuration?

Arc enables you to expand Azure compliance and monitoring to your hybrid and multi-cloud settings using Azure Resource Manager (ARM). Azure Arc simplifies governance and management by providing a unified multi-cloud and on-premises management platform.

Azure App Service

Azure App Services are typically utilized in Microsoft Azure to provide a hosting environment for web applications. The load balancer spreads the incoming traffic request across all available VM instances of the web application, and Azure App Service maintains multiple instances to handle the traffic.

Mind Map


Azure Resource Manager
Working with ARM Templates
Azure App Services
Managing and Deploying Azure Resources
Introduction
Structure of ARM Templates
Azure Arc

Chapter 12: Support

Plans

Microsoft offers a variety of Azure support options to help you select the proper degree of assistance for your business. Basic, Developer, Standard, Professional Direct, and Premier are the five support options available in Azure. Choosing the correct plan requires balancing how much aid and support you require and how much you are ready to spend.

The things which are included in all support plans are:

- 24/7 Access
- Online Self-Help
- Forums
- Azure Advisor
- Service Health

Tickets

There is a media called "Tickets" that can be used to contact assistance. Tickets provide support as a result of the inquiry issue. A ticket is usually a number that is used to identify your request.

Channels

Azure provides many free channels via which you can get further help, Azure. Support is available through the following channels:

- Azure Documentation
- Forums
- Social Media

Knowledge Center

The knowledge center is where all Azure knowledge can be found. Basic questions common to all new Azure users can be found in the knowledge center and are referred to as common questions.

Service Level Agreement

When you are using Azure Services, you need some form of guarantee that the service will be running stably. This is called Service Level Agreement, which helps ensure the services you are subscribed to are available to you as mentioned in the agreement.

Properties

Some properties of SLAs are:

- Confidence
- Contract
- Multiple SLAs
- Complex
- Mandatory

Service Life Cycle

The Service Lifecycle is the lifecycle of every product and service in Azure. Azure is a dynamic ecosystem where new services are added regularly.

It is critical to comprehend the Azure service lifecycle, how to keep up with changes, and how the lifecycle of service may affect your support and SLA.

Gathering Customers Data

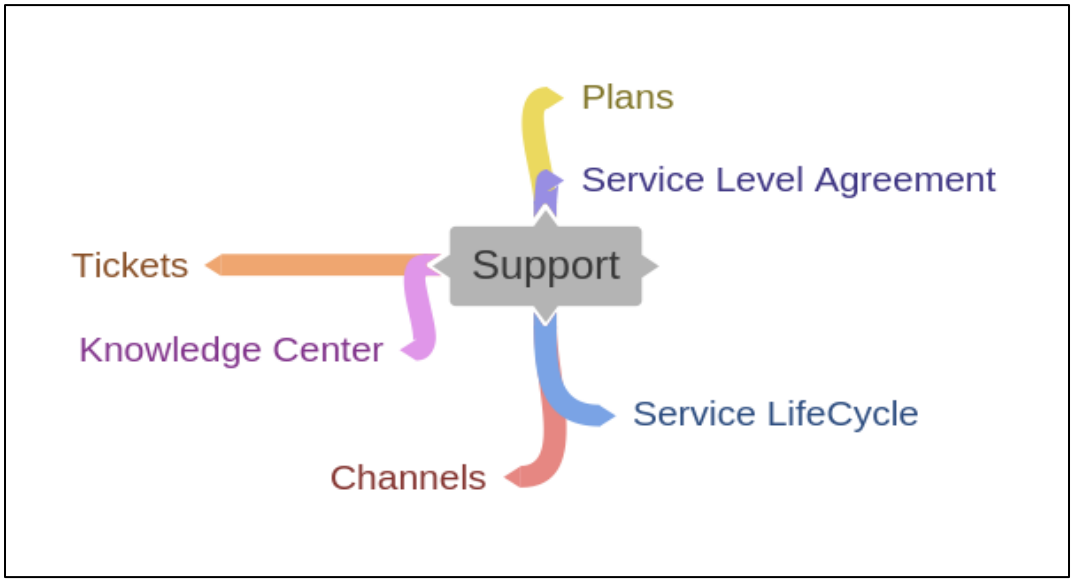
When Microsoft develops services for the Azure platform, it is vital to ask customers questions about the new features before implementing them. If the services fail, this step can save a lot of money.

Stages

There are two main stages in Service Life Cycle:

- Preview
  - *Private Preview*
  - *Public Preview*
- General Availability

Mind Map


Plans
Service Level Agreement
Tickets
Support
Knowledge Center
Service LifeCycle
Channels