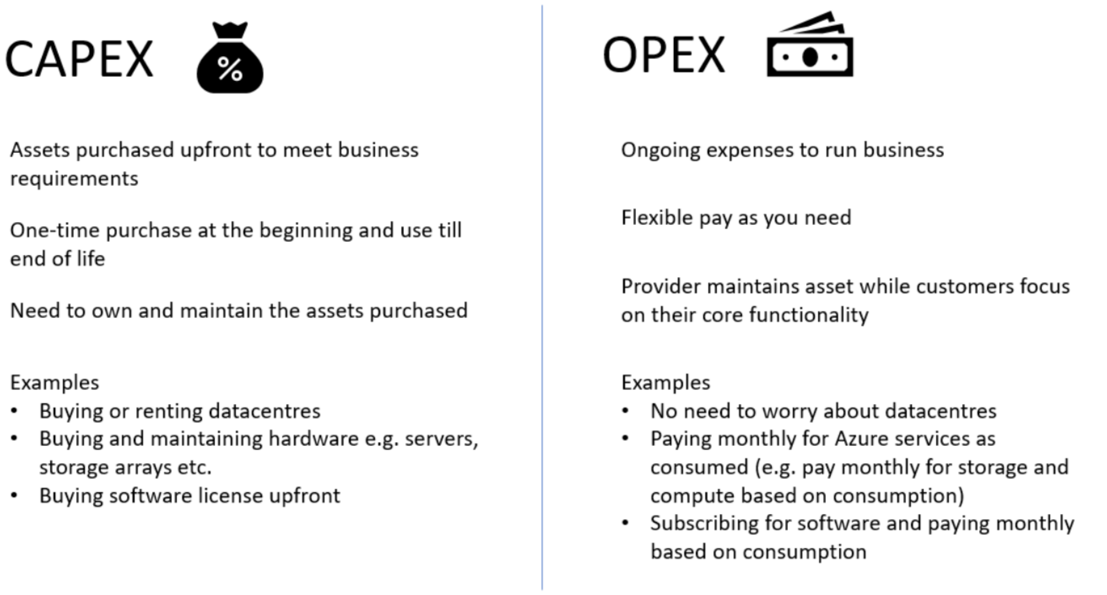
Table of contents

1 Cloud concepts (20-25%)

1.1 Benefits of cloud computing :

- Cost-effective
- Scalable
  - Vertical scaling / scaling up: adding resources (eg. CPU, memory) to an existing server
  - Horizontal scaling / scaling out: adding more servers (eg. have more than 1 server processing request)
- Elastic: automatically adding o removing resource
- Current: able to focus on what matters (Eg. build app)
- Reliable: Offer data backup, disaster recovery and data replication services
- Global: Fully redundant data centers located in various regions
- Secure: offer policies, technologies, controls and expert technical skills
  - Physical security: Cloud providers provide walls, cameras to protect physical assets
  - Digital security : Authorized users or offer tools that help to mitigate security threats

1.2 Differences between capital expenditure and operational expenditure



CAPEX

Assets purchased upfront to meet business requirements

One-time purchase at the beginning and use till end of life

Need to own and maintain the assets purchased

Examples
- Buying or renting datacentres
- Buying and maintaining hardware e.g. servers, storage arrays etc.
- Buying software license upfront

OPEX

Ongoing expenses to run business

Flexible pay as you need

Provider maintains asset while customers focus on their core functionality

Examples
- No need to worry about datacentres
- Paying monthly for Azure services as consumed (e.g. pay monthly for storage and compute based on consumption)
- Subscribing for software and paying monthly based on consumption

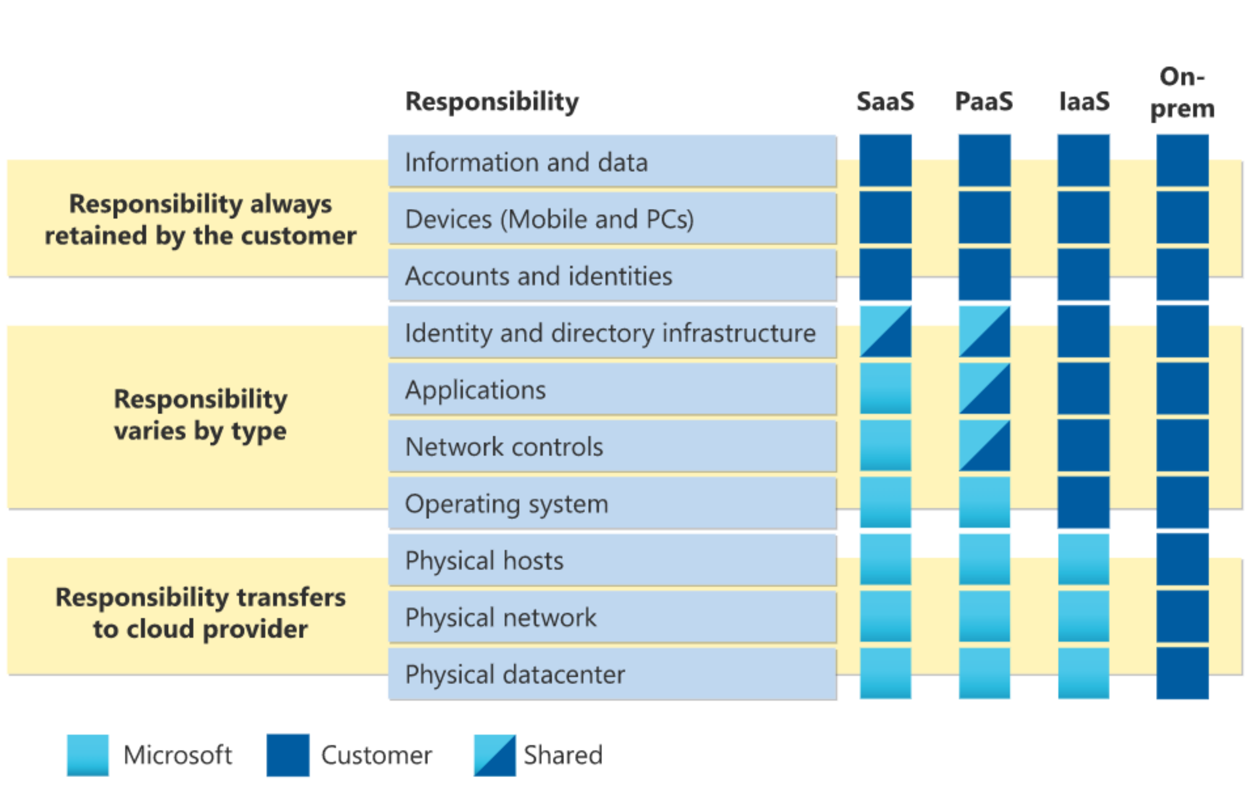
1.3 Consumption-based model

Consumption-based model

- Cloud service provider’s model
- Pay for what is consumed
- No upfront cost
- Stop paying for service no longer required

1.4 Shared responsibility model

- Customers responsible for security of the Azure based on the deployment types, but they are always need to pay responsibility for data, endpoints, account and access management
- Details:



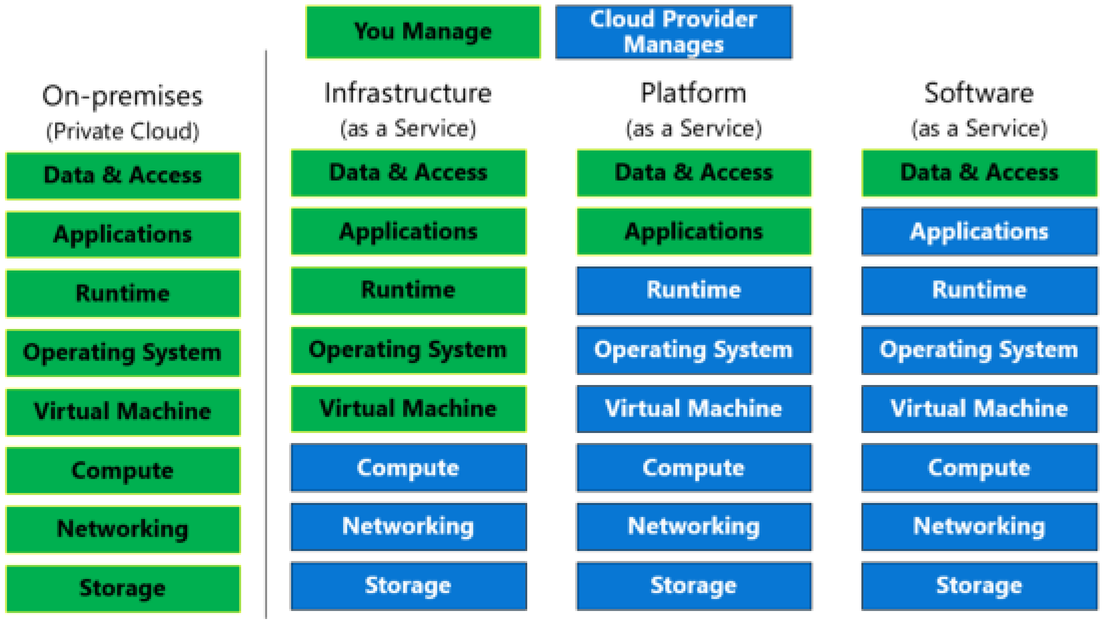
	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◪	◪	■	■
	Applications	□	◪	■	■
	Network controls	□	◪	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◪ Shared

1.5 IaaS, PaaS, SaaS

Infrastructure as a Service (IaaS)	**Platform as a Service (PaaS)**	**Software as a Service (SaaS)**

Cloud-based service with pay-as-you-go for mode	Hardware and software tools available over the Internet	Software that's available via a third paty over the internet
Responsible for managing operating system, data and application	Requires less user management and does not provide access to the operating system	Requires the least management, Microsoft handles everything
Characteristic ☐ Highly flexible and highly scalable. ☐ Accessible by multiple users. ☐ Cost-effective.	Characteristic ☐ Accessible by multiple users. ☐ Scalable – you can choose from various tiers of resources to suit the size of your business. ☐ Built on virtualization technology. ☐ Easy to run without extensive system administration knowledge	Characteristic ☐ Available over the internet. ☐ Hosted on a remote server by a third-party provider. ☐ Scalable, with different tiers for small, medium, and enterprise-level businesses. ☐ Inclusive, offering security, compliance, and maintenance as part of the cost
Eg. Azure VM, Azure storage accounts, Digital Ocean, Rackspace	Eg. Azure App Service, Azure SQL databases, Azure Cosmos DB, Azure Synapse Analytics, Heroku, OpenShift	Eg. Outlook email, calendar, Microsoft office 365, Slack, Salesforce, DocuSign



🟩 You Manage 🟦 Cloud Provider Manages

On-premises (Private Cloud)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟩 Data & Access	🟩 Data & Access	🟩 Data & Access	🟩 Data & Access
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Operating System	🟩 Operating System	🟦 Operating System	🟦 Operating System
🟩 Virtual Machine	🟩 Virtual Machine	🟦 Virtual Machine	🟦 Virtual Machine
🟩 Compute	🟦 Compute	🟦 Compute	🟦 Compute
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking
🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage

1.6 Serverless computing

- It is an abstraction of servers, infractures and operating systems.
- To build application faster by eliminating the need for them to manage infrastructure
- It helps teams to have better optimize resources (Automatically allocating or deallocating resources)
- Type of serverless application
  - Serverless functions (Run custom code started by triggers)
  - Serverless Kubernetes
  - Serverless workflow
  - Serverless application environment
  - Serverless API gateway
- Benefits
  - No infrastructure management (No OS)
  - Scalability (Can working under any size)
  - Only pay for what you use

1.7 Definition of cloud computing

Cloud computing is the delivery of computing services (Eg. servers, storage) over the internet to offer faster innovation, flexible of resources and economies of scale)

1.8 Types of cloud computing

Cloud deployment model

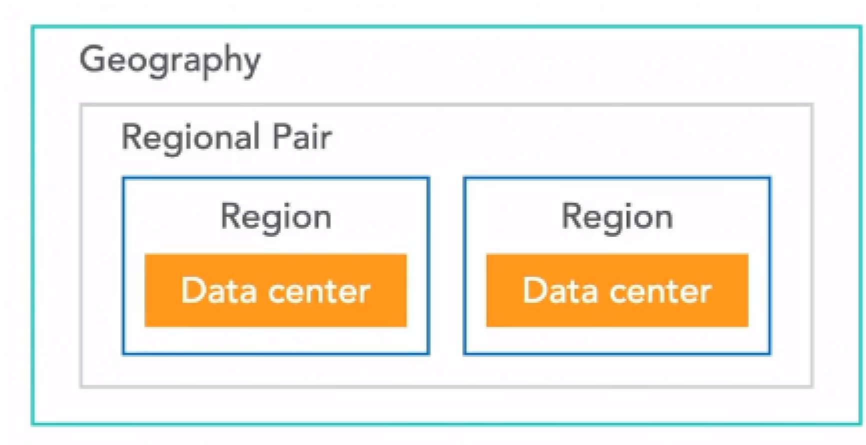
Public cloud	**Private cloud**	**Hybrid cloud**
Most common deployment model	Create a cloud environment in own datacenter	Allow to run applications in the most appropriate location
No local hardware to manage or keep up-to-date everything	Offers a simulation of a public cloud to your users	-
More cheaper	Suitable for the people who are need privacy	Combine public + private (Eg. website in public cloud and db host in private cloud)

2 Core Azure Services (15-20%)

2.1 Core Azure architectural

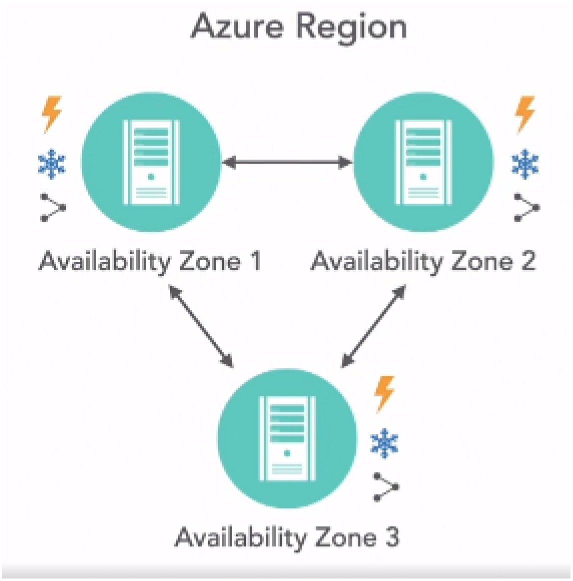
2.1.1 Regions and Region pairs

Region	Region pairs
★ A geographical area on the earth that contains at least one data centers ★ Provides better scalability, redundancy, and preserve data residency for the services ★ Special Azure regions : needed by the Azure customer when build app for regulatory compliance or legal purposes ○ US Dod Central ○ US Gov Virginia ○ US Gov Iowa ○ China East ○ China North	★ Pairing Azure region with another region in the same geographic area ★ Each region must at least 300 miles away ★ Replicate resources to other region with a region pair ★ Whenever there is a regional failure. All the services will automatically fail over to another region in its region pairs. ★ Eg. West US and East US ★ Benefits : ○ Reliable / Data redundancy ○ High availability / Minimize downtime ○ Quick restore



2.1.2 **Availability zones**

- ➔ physically separate locations within each Azure region that are ***tolerant to local failures*** *(achieve through the redundancy and logical isolation of Azure service)*
- ➔ Not every region supports this
- ➔ Those are required to connect by ***high-performance*** network with a round-trip latency of less than 2ms *(because it required to make data stay synchronized and accessible when things go wrong)*
- ➔ Each zone has independent cooling, power and networking
- ➔ 3 zones per region



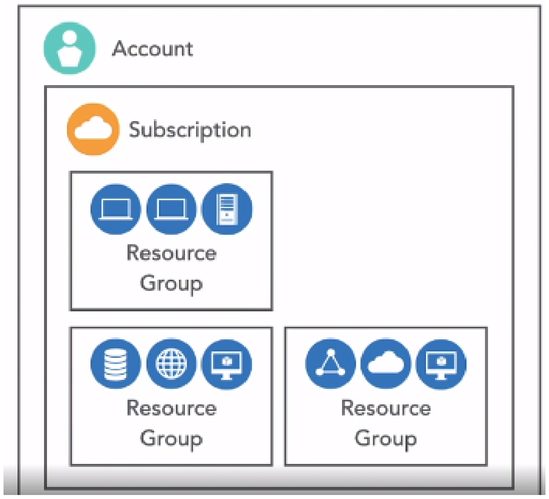
Availability sets

- ➢ It is a logical grouping of 2 or more VMs that helps keep the application available during planned or unplanned maintenance

  - **Planned maintenance** : an event when Azure fabric that hosts VMs is updated, then the availability set allows Azure fabric to update in order when reboot is required
  - **Unplanned maintenance** : an event involves hardware failures in data centers, then the availability set will automatically switch to a functioning server
- A VM is online during maintenance or failure
- Assigned to an update domain and a fault domain
  - **Update domain** : define groups of VMs and underlying physical hardware that can be rebooted simultaneously
  - **Fault domain** : only a server rack is affected when failure occurs
- Only 1 update domain is updated at time
- Fault domains provide physical isolation hardware in the data center

2.1.3 Resource groups

- It is a container that holds related resources for a Azure solution
- It stores the metadata about the resources
- It helps to deploy, manage and monitor resources in a group
- Each resource only able to exist in a resource group, but it can be moved between resource groups
- Resources can be assigned to different regions within the resource group
- Deleting a resource group means that it deletes all the resources in the group



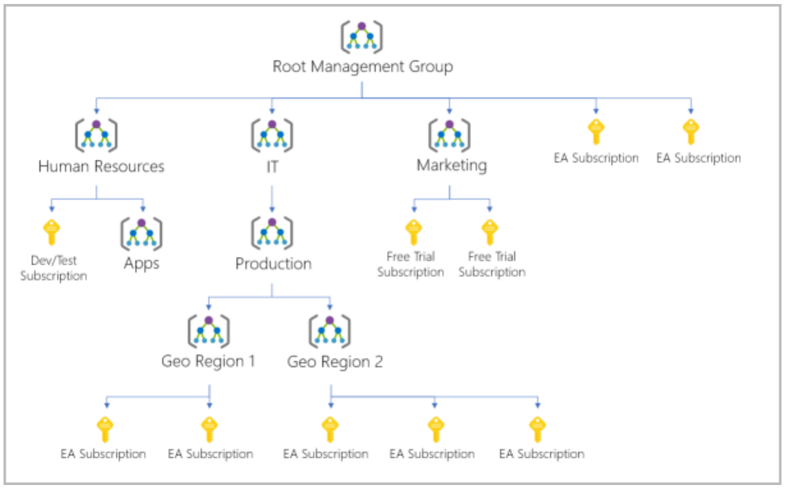
2.1.4 Subscriptions

- Logical container
- Subscription links to Azure Active Directory for authentication and authorization
- Multiple subscriptions can be created by the account holder

- ★ Subscription option:
  - ○ Pay-as-you-go (billed monthly to a credit card)
  - ○ Free account (12 months, $260 credit per month, over 25 free services)
  - ○ Member offers (using monthly credit)
- ★ Subscription consideration : be aware of the service limit for the subscription option
- ★ Benefits:
  - ○ Subscription billing boundary (eg. subscription is applied to group)
  - ○ Subscription access control boundary (eg. only allow the particular department access the subscription)

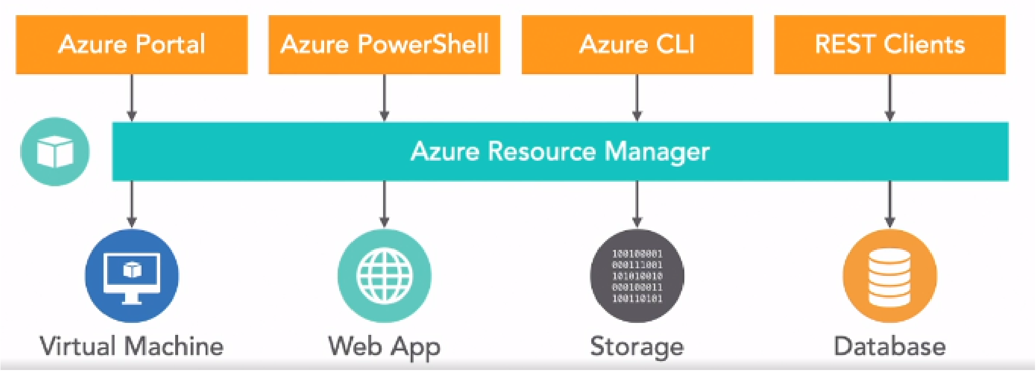
2.1.5 Management groups

- ❖ Group Azure objects in a collections
- ❖ Manage policies, access and compliance for the entire groups



2.1.6 Azure resource manager

- ★ Management level that is used to access and manage the azure resource
- ★ Create, update, delete, organize, control and tag resources in the subscription
- ★ Access through Azure Portal, Azure PowerShell, Azure CLI, REST clients



2.2 Core resource available in Azure

2.2.1 Compute options (Virtual Machines, Azure App Service, Azure Container Instances (ACI), Azure Kubernetes Services (AKS) and Azure Virtual Desktop)

Virtual Machines

- Infrastructure as a service
- Physical computer that is virtualized
- Includes an operating system, visual processor, storage, and networking
- Suitable to used when users need:
  - Total control over the operating system
  - The ability to run custom software
  - To use custom hosting configurations
- Benefits: Availability, Scalability, redundancy

Azure App Service

- Platform as a service
- Build enterprise-grade web, mobile and API apps on any platform
- Run small pieces of code instead of a full app
- Event, timer, message or another trigger-driven event
- Eg. IoT, processing data, and ….

Azure Container Instances (ACI)	Azure Kubernetes Services (AKS)
● Fast and Easy ● Users do not need to manage VMs or configure services ● ACI is a PaaS that supports automatic elastic scale	● It is an orchestration service ● Support automation, manage and interest with multiple container

Azure Virtual Desktop

- ★ A flexible cloud virtual desktop infrastructure (VDI) platform that securely delivers virtual desktops and remote apps with maximum control
- ★ Benefits:
  - Provide the best UX
  - Enhance security

    - ○ Reduce license costs

2.2.2 Virtual Network, VPN Gateway, Virtual Networks peering and ExpressRoute

Virtual network

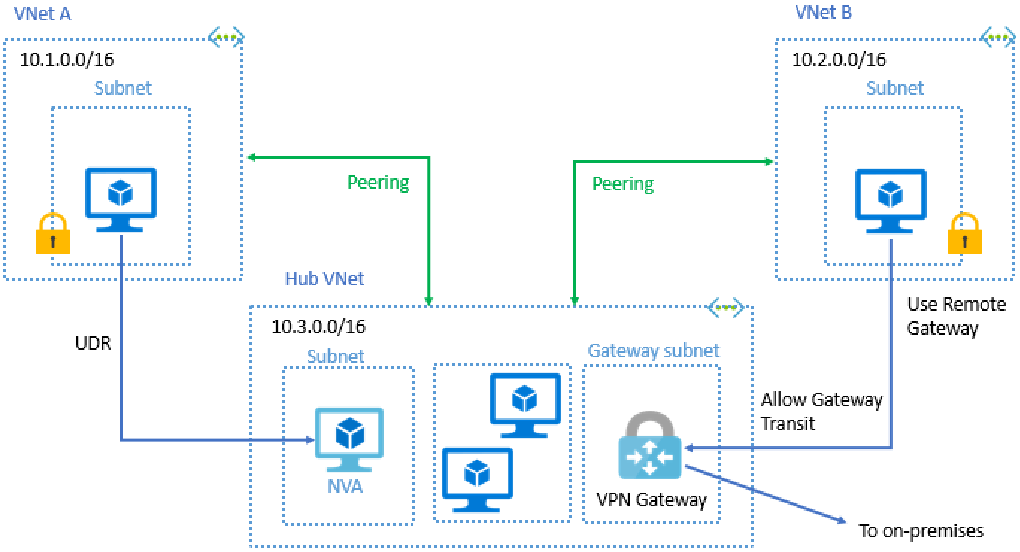
- Logically isolated network
- Ensure secure network communications
- Scope is limited to single region
- Segmented into one or more subnets, that help organize and secure resources
- Each tier has single VM (those are located in different subnets)
- Can be configured through software

VPN gateway

- ★ used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet
- ★ to send encrypted traffic between Azure virtual networks over the Microsoft network
- ★ Each virtual network can have only one VPN gateway
- ★ can create multiple connections to the same VPN gateway, then all VPN tunnels share the available gateway bandwidth

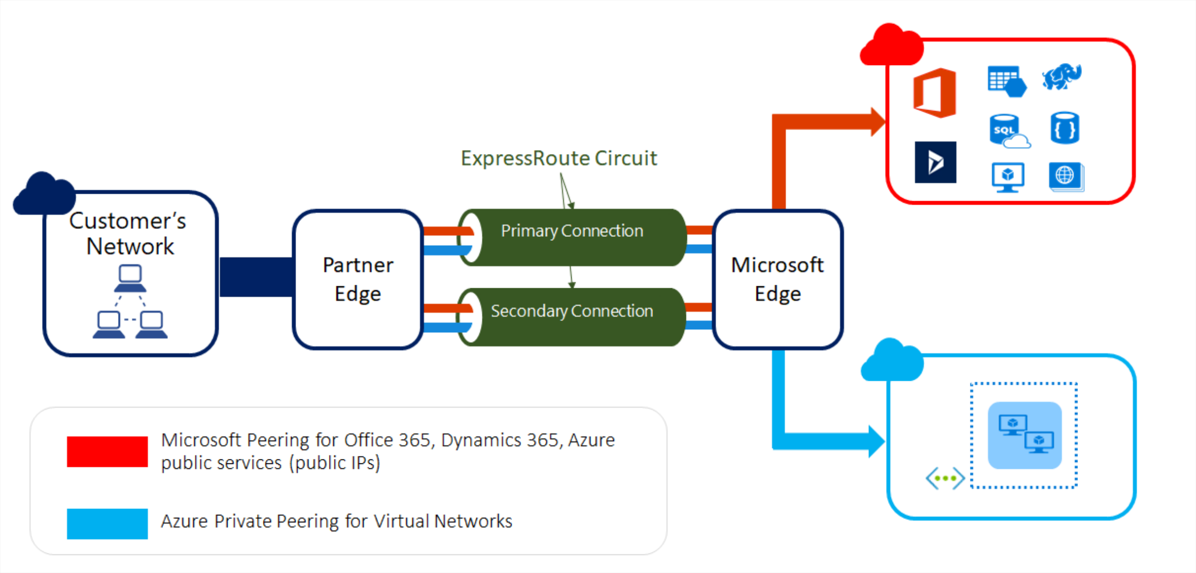
Virtual Networks peering

- ★ to seamlessly connect two or more Virtual Networks in Azure
- ★ 2 types
    - ○ Virtual network peering: Connect virtual networks within the same Azure region.
    - ○ Global virtual network peering: Connecting virtual networks across Azure regions.
- ★ Benefits:
    - A low-latency, high-bandwidth connection between resources in different virtual networks.
    - The ability for resources in one virtual network to communicate with resources in a different virtual network.
    - The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
    - The ability to peer virtual networks created through the Azure Resource Manager.
    - The ability to peer a virtual network created through Resource Manager to one created through the classic deployment model.
    - No downtime to resources in either virtual network when creating the peering, or after the peering is created.



ExpressRoute

- extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider
- establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365
- ExpressRoute connections don't go over the public Internet
- Benefits:
  - offer more reliability
  - faster speeds
  - consistent latencies
  - higher security than typical connections over the Internet


ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
🟥 Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
🟦 Azure Private Peering for Virtual Networks

2.2.3 Container (blob) storage, disk storage, file storage and storage tiers

Azure Blob storage

- Storage for unstructured data
- High scalable and almost no changes as work with files on disk
- Support variety of file formats
- Stream large video or audio files directly to the user's browser
- Support backup, recovery, archiving

Disk storage

- Provides disks for Azure services
- Data can be stored persistently and accessed from virtual hard disks
- Can be managed by Azure or the users
- Ideal for storing data that is only accessed internally

File storage

- Accessible via Server Message Block (SMB) protocol
- Azure file shares can be mounted concurrently
- File storage sharing can be mounted to access file data

Storage tiers

- Hot storage tiers : storing frequently access data
- Cool storage tiers : storing not frequently accessed data for at least 30 days
- Achieve storage tiers : storing rarely accessed for at least 180 days

2.2.4 Cosmos DB, Azure SQL Database, Azure database for MySql, Azure database for postgreSQL, and Azure SQL Managed instance

Azure Cosmos DB

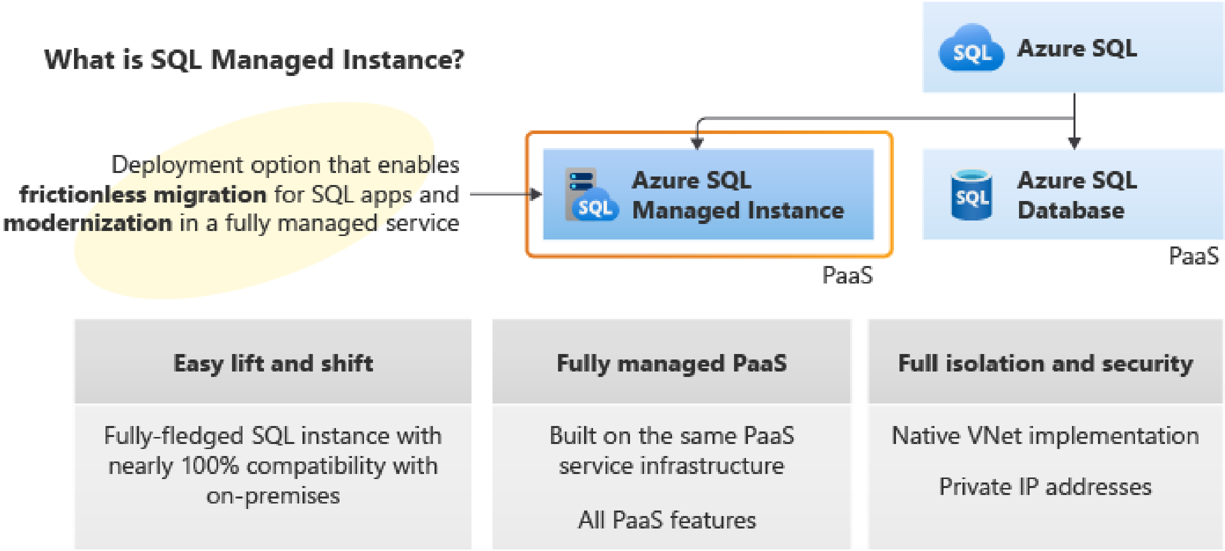
- ➔ Globally distributed database services
- ➔ Support schema-less data
- ➔ Supports highly responsive and always on application

Azure SQL Database

- Relational database as a service (DaaS)
- High performance, reliable, manageable, and secure database
- Supports development of data-driven applications and websites in any language
- Provide guidance to perform migration
- Support migration of existing SQL server database with minimal downtime

Azure SQL Managed instance

★ intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service
★ allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes
★ preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability)
★ designed for customers looking to migrate a large number of apps from an on-premises or IaaS, self-built, or ISV provided environment to a fully managed PaaS cloud environment, with as low a migration effort as possible



What is SQL Managed Instance?

Deployment option that enables **frictionless migration** for SQL apps and **modernization** in a fully managed service

Easy lift and shift	Fully managed PaaS	Full isolation and security
Fully-fledged SQL instance with nearly 100% compatibility with on-premises	Built on the same PaaS service infrastructure All PaaS features	Native VNet implementation Private IP addresses

2.2.5 Azure marketplace

➢ Partners, solution provider and independent software vendors can offer customized solutions
➢ Eg. Wordpress

3 Core solutions & management tools on Azure (10-15%)

3.1 Core solutions available in Azure

3.1.1 Internet of Things (IoT) Hub, IoT Central, and Azure Sphere

Internet of Things (IoT) Hub

- a managed service hosted in the cloud that acts as a central message hub for communication between an IoT application and its attached devices
- connect millions of devices and their backend solutions reliably and securely. Almost any device can be connected to an IoT hub
- scales to millions of simultaneously connected devices and millions of events per second to support your IoT workloads
- Is a managed Platform as a Service (PaaS)

IoT Central

- also a service for communication between IoT apps and the devices it manages
- helps to reduce the challenges of implementing IoT development, operations, and management
- is a fully managed Software as a Service solution (SaaS)
- lowers the bar for entry into the IoT landscape for clients that have limited technical knowledge to manage the IoT stack

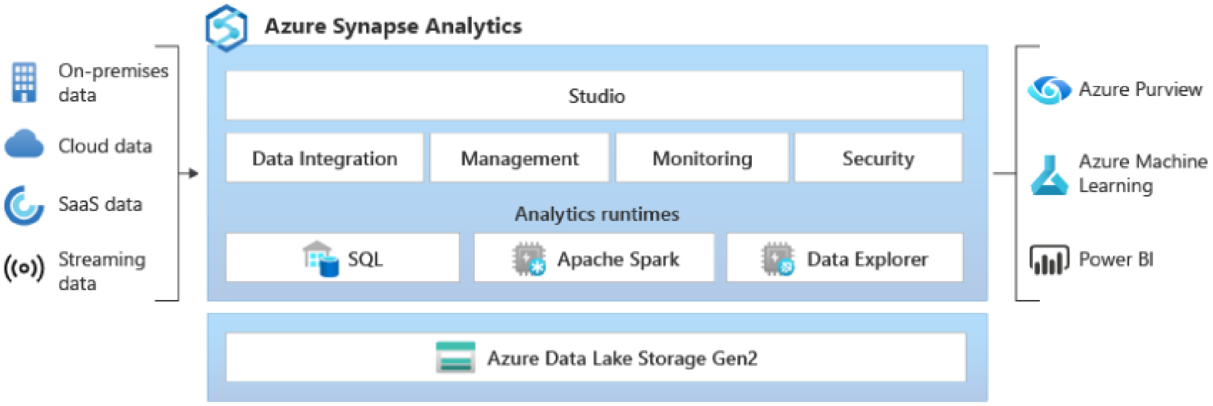
Azure Sphere

- runs an the Sphere certified chip and connects to the Azure Sphere Security Service
- It is essentially a Linux-based operating system with a cloud based security service that enables continues security
- This is a specialized and purpose built OS just for Azure

3.1.2 Azure Synapse Analytics, HDInsight, and Azure databricks

Azure Synapse Analytics

- (formerly SQL Data Warehouse) is a cloud-based enterprise data warehouse that leverages massively parallel processing (MPP) to quickly run complex queries across petabytes of data



HDInsight

- It is a managed, full-spectrum, open-source analytics service in the cloud for enterprises
- can use open-source frameworks such as Hadoop, Apache Spark, Apache Hive, LLAP, Apache Kafka, Apache Storm, R, and more, in your Azure environment

- ➢ Benefits
    - ○ **Cloud native** : create optimized clusters for Hadoop, Spark, Interactive query (LLAP), Kafka, Storm, HBase on Azure & provides an end-to-end SLA on all your production workloads
    - ○ **Low cost** : scale workloads up or down. You can reduce costs by creating clusters on demand and paying only for what you use
    - ○ **Secure and compliant** : to protect your enterprise data assets with Azure Virtual Network, encryption, and integration with Azure Active Directory
    - ○ **Monitoring** : integrates with Azure Monitor logs to provide a single interface with which you can monitor all your clusters
    - ○ **Global availability** : available in more regions than any other big data analytics offering
    - ○ **Productivity** : supports various tools and frameworks
    - ○ **Extensibility** : extend the HDInsight clusters with installed components (Hue, Presto, and so on) by using script actions, by adding edge nodes, or by integrating with other big data certified application

Azure databricks

- It is a data analytics platform optimized for the Microsoft Azure cloud services platform
- offers three environments for developing data intensive applications: Databricks SQL, Databricks Data Science & Engineering, and Databricks Machine Learning

3.1.3 Azure Machine Learning, Cognitive services, and Azure bot services

Azure Machine Learning

- is a cloud service for accelerating and managing the machine learning project lifecycle
- create a model in Azure Machine Learning or use a model built from an open-source platform, such as Pytorch, TensorFlow, or scikit-learn
- MLOps tools help you monitor, retrain, and redeploy models

Cognitive services

- brings AI within reach of every developer and data scientist
- Enable developers and data scientists of all skill levels to easily add AI capabilities to their apps
- All it takes is an API call to embed the ability to see, hear, speak, search, understand, and accelerate advanced decision-making into your apps
- Benefits:
    - ○ Use customizable, pretrained models built with breakthrough AI research
    - ○ Deploy Cognitive Services anywhere from the cloud to the edge with containers
    - ○ Empower responsible use with industry-leading tools and guidelines
- Services : Speech, language, vision, decision, OpenAI

Azure bot services

- A comprehensive development environment for designing and building enterprise-grade conversational AI

3.1.4 Serverless computing solutions that include Azure functions and Logic Apps

Azure function	Logic apps
Usually stateless, except Durable functions	Stateful
Code-first (imperative)	Designer-first (declarative)
About a dozen build-in binding types. Write code for custom bindings	Large collection of connectors
Each activity is an Azure function, write code for activity functions	Large collection of ready-made actions
Monitor through Azure Application Insights	Monitor through Azure portal, Log analytics
Management through REST API, Visual Studio	Management through Azure Portal, REST API, Powershell, Visual Studio
Run locally or in the cloud	Runs only in the cloud

3.1.5 Azure DevOps, GitHub actions, and Azure DevTest Labs

Azure DevOps

- provides developer services for allowing teams to plan work, collaborate on code development, and build and deploy applications
- supports a collaborative culture and set of processes that bring together developers, project managers, and contributors to develop software
- allows organizations to create and improve products at a faster pace than they can with traditional software development approaches
- Standalone services:
    - Azure Repos
    - Azure Pipeline
    - Azure Board
    - Azure Test Plan
    - Azure artifacts

- Usage
    - Quick set-up
    - Maintenance-free operations
    - Easy collaboration across domains
    - Elastic scale
    - Rock-solid security

Github actions

- automate your software development workflows from within GitHub
- deploy workflows in the same place where you store code and collaborate on pull requests and issues
- GitHub Actions also include support for utilities, including Azure Resource Manager templates, Azure CLI, and Azure Policy.

Azure DevTest labs

- a service for easily creating, using, and managing infrastructure-as-a-service (IaaS) virtual machines (VMs) and platform-as-a-service (PaaS) environments in labs
- offer preconfigured bases and artifacts for creating VMs, and Azure Resource Manager (ARM) templates for creating environments like Azure Web Apps or SharePoint farms
- Role
  - **Lab owners** can create pre configured VMs that have tools and software lab users need.
  - **Lab users** can claim pre configured VMs, or create and configure their own VMs and environments.

3.2 Azure management tools

3.2.1 Azure Portal, Azure PowerShell, Azure CLI, Cloud shell, and Azure mobile app

Azure portal

- is a web-based, unified console that provides an alternative to command-line tools
- manage your Azure subscription using a graphical user interface
- build, manage, and monitor everything from simple web apps to complex cloud deployments
- Create custom dashboard
- designed for resiliency and continuous availability

Azure Powershell

- a set of cmdlets for managing Azure resources directly from PowerShell.
- is designed to make it easy to learn and get started with, but provides powerful features for automation
- Usage
  - Create a storage account
  - Transfer objects to/from Azure Blob storage
  - Create and retrieve secrets from Azure Key Vault
  - Create an Azure SQL database and firewall
  - Run a container in Azure Container Instances
  - Create a Virtual Machine Scale Set

    - Create a standard load balancer

Azure CLI

- is a set of commands used to create and manage Azure resources
- allows the execution of commands through a terminal using interactive command-line prompts or a script

Cloud shell

- is an interactive, authenticated, browser-accessible shell for managing Azure resources
- provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell

Azure mobile app

- a fully managed platform as a service (PaaS) offering for professional developers
- brings a rich set of capabilities to web, mobile, and integration scenarios
- gives enterprise developers and system integrators a mobile-application development platform that's highly scalable and globally available
- With mobile app SDK:
    - **Build native and cross-platform apps**: Build cloud-enabled apps for Android, iOS, or Windows using native SDKs.
    - **Connect to your enterprise systems**: Authenticate your users with Azure Active Directory, and connect to enterprise data stores.
    - **Build offline-ready apps with data sync**: Make your mobile workforce more productive by building apps that work offline. Use Azure Mobile Apps to sync data in the background.
- Features:
    - **Authentication and authorization**: Use Azure Mobile Apps to sign-in users using social and enterprise provides. Azure App Service supports Azure Active Directory, Facebook, Google, Microsoft, Twitter, and OpenID Connect.
    - **Data access**: Mobile Apps provides a mobile-friendly OData v3 data source that's linked to Azure SQL Database or an on-premises SQL server.
    - **Offline sync**: Build robust and responsive mobile applications that operate with an offline dataset. You can sync this dataset automatically with service, and handle conflicts with ease.
    - **Client SDKs**: There is a complete set of client SDKs that cover cross-platform development (.NET, and Apache Cordova). Each client SDK is available with an MIT license and is open-source.

3.2.2 Azure Advisor

- a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments
- analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve

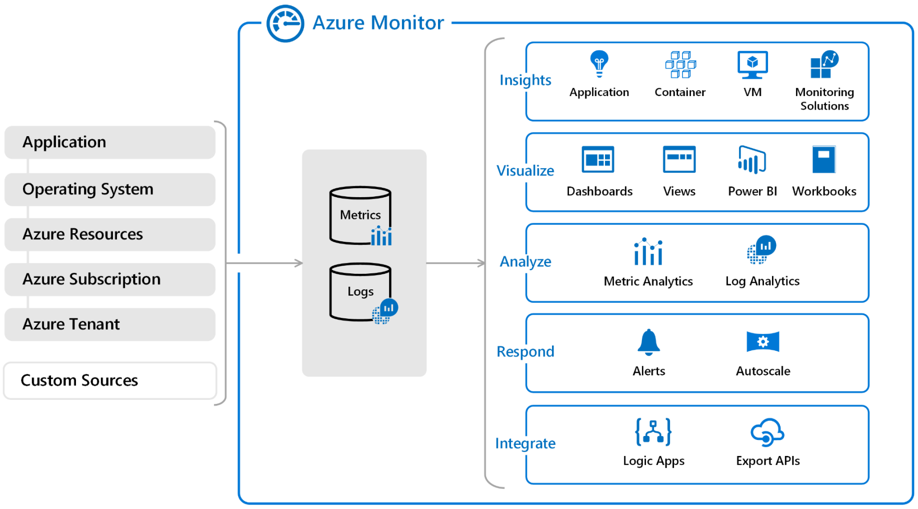
    - the cost effectiveness
    - Performance
    - Reliability (formerly called High availability)
    - Operational experience
    - and security of your Azure resources
- Usage
    - Get proactive, actionable, and personalized best practices recommendations.
    - Improve the performance, security, and reliability of your resources, as you identify opportunities to reduce your overall Azure spend.
    - Get recommendations with proposed actions inline.

3.2.3 Azure Resource Manager (ARM) template

- The template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project.
- The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it
- In the template, you specify the resources to deploy and the properties for those resources
- https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/overview

3.2.4 Azure Monitor

- maximize the availability and performance of your applications and services
- delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments
- helps you understand how your applications are performing and proactively identify issues affecting them and the resources they depend on
- Usage
    - Detects and diagnoses issues across applications and dependencies with **Application Insights**.
    - Correlate infrastructure issues with **VM insights and Container insights**.
    - Drill into your monitoring data with **Log Analytics** for troubleshooting and deep diagnostics.
    - Support operations at scale with **smart alerts and automated actions**.
    - Create visualizations with **Azure dashboards and workbooks**.
    - Collect data from monitored resources using **Azure Monitor Metrics**.



3.2.5 Azure Service Health

★ It is a suite of experiences that provide personalized guidance and support when issues in Azure services are or may affect you in the future

★ It is a combination of three separate smaller services
  - **Azure status** informs you of service outages in Azure
  - **Service health** provides a personalized view of the health of the Azure services and regions you're using
  - **Resource health** provides information about the health of your individual cloud resources such as a specific virtual machine instance

4 General security & network security features (10-15%)

4.1 Azure security features

4.1.1 Basic features of Azure security center, including policy compliance, security alerts, secure score and resource hygiene

Azure security center

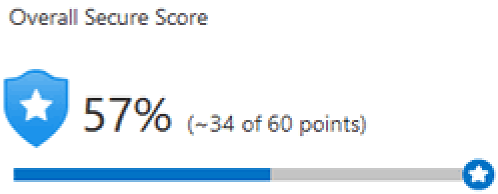
❖ Provides threat protection across all services both in Azure and on-premises

❖ gives you control over the security of your Azure subscriptions and other machines that you connected to it outside of Azure.

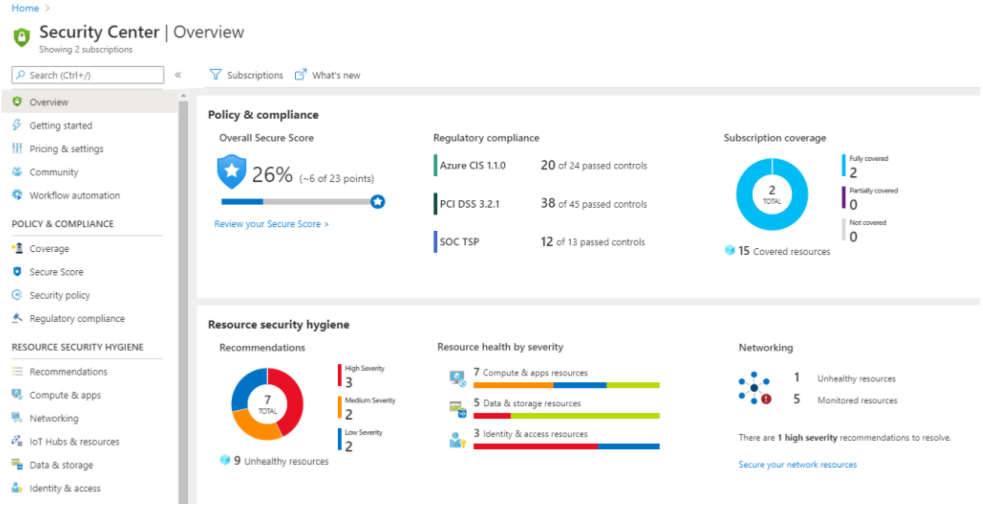
❖ It has 2 tiers which are free and standard

❖ Scenarios:
  - ➢ For incident response
  - ➢ Enhance security

- Basic features:
  - **Policy configuration** -- allows admins to establish a set of security-related controls for a specific Azure subscription or resource group. An Azure resource group refers to the collection of Azure resources, such as a VM, storage, database or virtual network, required to run an application.
  - **Alerts** -- issues an alert when potential security threats, such as compromised VMs or malware, are detected. Azure Security Center automatically collects and integrates log data about Azure resources to produce alerts.
  - **Secure scores** - Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.



  - Resource hygiene : It is like your one-stop solution to finding out any issues very quickly



There are **1 high severity** recommendations to resolve.

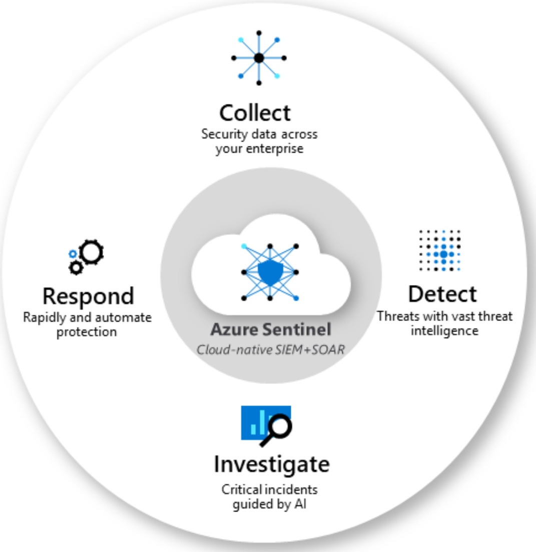
4.1.2 Azure key vault

- Is a centralized cloud service used in Azure to protect customers' secrets
- Usage
  - Secrets management
  - Key management
  - Certificate management
  - Store secrets backed by hardware security modules (HSMs)

★ Benefits
  - ○ Centralized application secret
  - ○ Securely stored secrets and keys
  - ○ Monitor access and use
  - ○ Simplified administration of application secrets
  - ○ Integrate with other Azure service

4.1.3 Azure sentinel

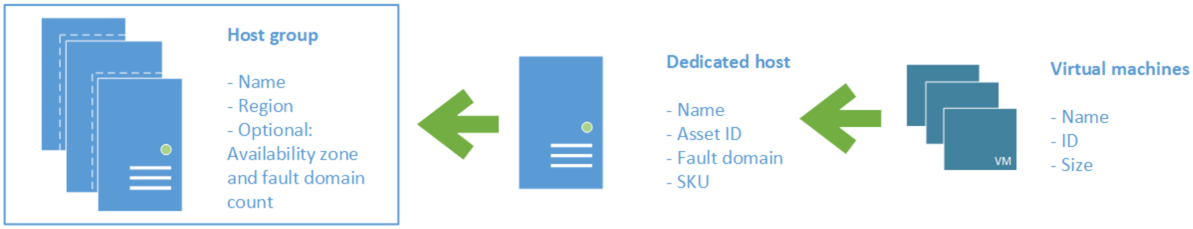
- ☐ a scalable, cloud-native, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution
- ☐ delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response


Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Azure Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

4.1.4 Azure dedicated hosts

- a service that provides physical servers - able to host one or more virtual machines - dedicated to one Azure subscription
- Dedicated hosts are the same physical servers used in our data centers, provided as a resource
- Benefits:
  - ○ **Hardware isolation at the physical server level**. No other VMs will be placed on your hosts. Dedicated hosts are deployed in the same data centers and share the same network and underlying storage infrastructure as other, non-isolated hosts.

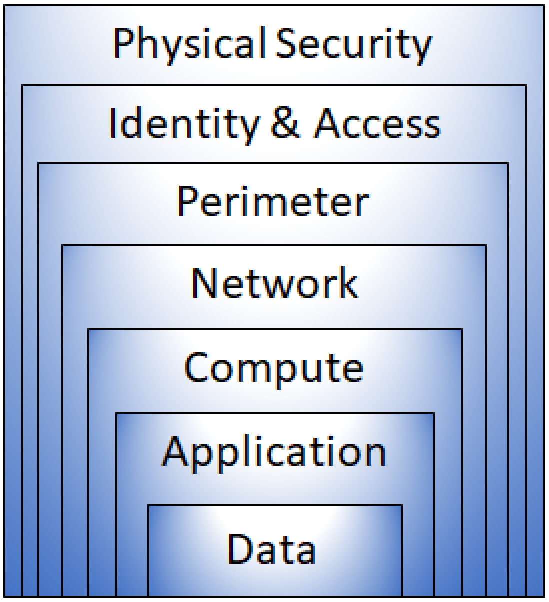
- **Control over maintenance events** initiated by the Azure platform. While the majority of maintenance events have little to no impact on your virtual machines, there are some sensitive workloads where each second of pause can have an impact. With dedicated hosts, you can opt-in to a maintenance window to reduce the impact to your service.
- With the **Azure hybrid** benefit, you can bring your own licenses for Windows and SQL to Azure. Using the hybrid benefits provides you with additional benefits. For more information, see Azure Hybrid Benefit.



4.2 Azure network security

4.2.1 Defense in depth

- to protect information and prevent it from being stolen by those who aren't authorized to access it
- uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data
- Layers
    - The **physical security layer** is the first line of defense to protect computing hardware in the datacenter.
    - The **identity and access layer** controls access to infrastructure and change control.
    - The **perimeter layer** uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
    - The **network layer** limits communication between resources through segmentation and access controls.
    - The **compute layer** secures access to virtual machines.
    - The **application layer** helps ensure that applications are secure and free of security vulnerabilities.
    - The **data layer** controls access to business and customer data that you need to protect.



4.2.2 Network security group (NSG)

- Critical in restricting unnecessary communication between virtual machines
- It is capable of filtering network traffic to and from the Azure resources in an Azure Virtual Network

4.2.3 Azure firewall

- A network security services that protects the Azure Virtual Network resources
- It provides inbound protection for non-HTTP/S protocols
- It provides outbound protection for all ports and protocols and application-level protection for outbound HTTP/S

4.2.4 Azure DDoS protection

- It able to protect Azure application from DDoS attacks
- When an attempt to overwhelm the network, Azure DDoS protection will blocks the traffic
- There are 2 tiers : basic and standard

5 Identity, governance, privacy & compliance features (15-20%)

5.1 Core Azure identity services

5.1.1 Difference between authentication and authorization

Authentication	Authorization
The process of establishing the identity of a person or service that is looking to access a resource	The process of establishing the level of access that an authenticated person or service has towards a resource

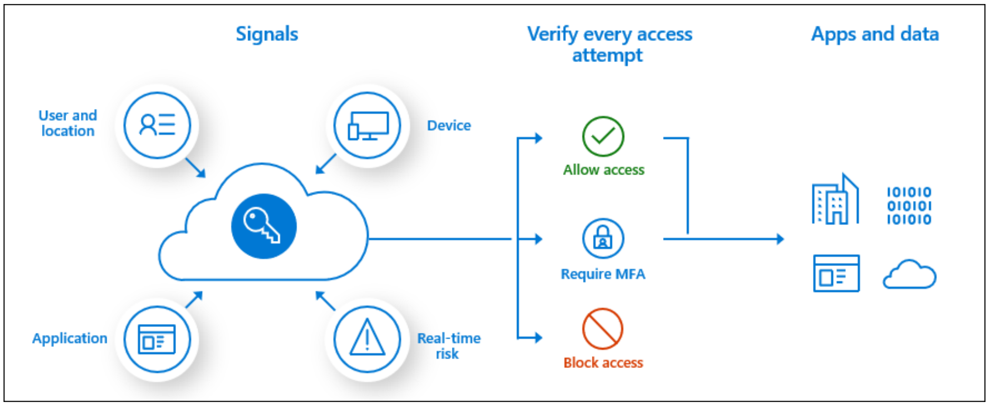
5.1.2 Azure Active Directory

- A cloud-based identity services
- Support synchronizing with existing on-premises Active Directory or can be used stand-alone
- Services
  - Authentication
  - Single-sign-on
  - Application management
  - Business to business (B2B) identify services
  - Business to customer (B2C) identify services
  - Device management

5.1.3 Conditional Access, Multi Factor authentication, and Single sign-on (SSO)

Conditional access

- It is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals
- brings signals together, to make decisions, and enforce organizational policies
- Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action
- Usage:
  - Require multi factor authentication to access an application
  - Require access to services only through approved client applications.
  - Require users to access your application only from managed devices
  - Block access from untrusted sources, such as access from unknown or unexpected locations
- Example : A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it

    - 

Single sign-on

- Users only need to remember a single ID and password to access multiple applications
- Reduces the effort required to modify or disable accounts

Multi factor authentication (MFA)

- Further enhance the security for identifies by requiring additional element for authentication
- Categories of elements
    - Something the user knows (email address and password)
    - Something the user has (code that's sent to the user's mobile phone)
    - Something the user is (some sort of biometric property, such as a fingerprint or face scan that's used on many mobile devices)

5.2 Azure governance features

5.2.1 Role-based authentication

- Role determine the users access to an Azure service instance
- Eg. read-only or contributor
- Identities can be either mapped to roles directly or through group memberships

5.2.2 Resource locks

- prevents resources from being accidentally deleted or changed
- manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template
- 2 levels
    - **CanNotDelete** means authorized people can still read and modify a resource, but they can't delete the resource without first removing the lock.

    - **ReadOnly** means authorized people can read a resource, but they can't delete or change the resource. Applying this lock is like restricting all authorized users to the permissions granted by the Reader role in Azure (RBAC).

5.2.3 Tags

- another way to organize resources
- provide extra information, or metadata, about your resources
- Those information help to
    - **Resource management** Tags enable you to locate and act on resources that are associated with specific workloads, environments, business units, and owners.
    - **Cost management and optimization** Tags enable you to group resources so that you can report on costs, allocate internal cost centers, track budgets, and forecast estimated cost.
    - **Operations management** Tags enable you to group resources according to how critical their availability is to your business. This grouping helps you formulate service-level agreements (SLAs). An SLA is an uptime or performance guarantee between you and your users.
    - **Security Tags** enable you to classify data by its security level, such as public or confidential.
    - **Governance and regulatory compliance** Tags enable you to identify resources that align with governance or regulatory compliance requirements, such as ISO 27001. Tags can also be part of your standards enforcement efforts. For example, you might require that all resources be tagged with an owner or department name.
    - **Workload optimization and automation** Tags can help you visualize all of the resources that participate in complex deployments. For example, you might tag a resource with its associated workload or application name and use software such as Azure DevOps to perform automated tasks on those resources.

5.2.4 Azure policy

- For creating, assigning and managing policies
- The policies enforce different rules upon the resources to ensure those resources stay compliant with the corporate standards and service level agreements
- It evaluates resources for noncompliance with assigned policies

5.2.5 Azure blueprints

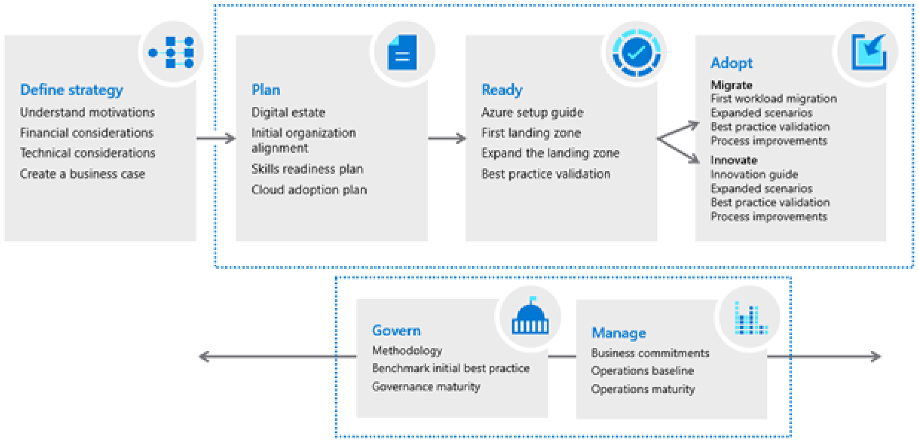
- Enable cloud architects and central IT groups to define a set of Azure resources that are repeatable

- Can resources be implemented with compliance to an organization’s standards, patterns and requirements
- A declarative way to coordinate the deployment of discrete resource templates and other artifacts
- Can combine with the resource locks, therefore the locks could be replace even if someone accidentally delete the lock

5.2.6 Cloud adoption framework for Azure

- create and implement the business and technology strategies needed to succeed in the cloud
- consists of tools, documentation, and proven practices

Microsoft Cloud Adoption Framework for Azure



5.3 Privacy and compliance resources

5.3.1 Microsoft core tenets of Security, Privacy, and compliance

Security	Privacy	Compliance
• Security Development lifecycle • Build-in product security • Data privacy • Azure Active Directory • Data encryption • Cyber defense operations center	• Control • Transparency • Security • Legal protections • No content-based targeting	• Industry verified global standards • Most comprehensive offering of any cloud offering • All compliance offerings are available • Azure Security and Compliance blueprints, Azure security center, Azure policy

5.3.2 Purpose of the Microsoft privacy statement, Online Service Terms (OST) and Data protection Addendum (DPA)

Microsoft privacy statement

- covers all of Microsoft's services, websites, apps, software, servers, and devices
- provides information that's relevant to specific products such as Windows and Xbox

Online service terms (OST)

- a legal agreement between Microsoft and the customer
- details the obligations by both parties with respect to the processing and security of customer data and personal data
- applies specifically to Microsoft's online services that you license through a subscription, including Azure, Dynamics 365, Office 365, and Bing Maps

Data protection Addendum (DPA)

- defines the data processing and security terms for online services
- Terms
  - Compliance with laws.
  - Disclosure of processed data.
  - Data Security, which includes security practices and policies, data encryption, data access, customer responsibilities, and compliance with auditing.
  - Data transfer, retention, and deletion.

5.3.3 Trust Center

- an important part of the Microsoft Trusted Cloud Initiative and provides support and resources for the legal and compliance community
- Function
  - In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products
  - Additional resources for each topic
  - Links to the security, privacy, and compliance blogs and upcoming events.

5.3.4 Azure compliance documentation

- provides you with detailed documentation about legal and regulatory standards and compliance on Azure
- Compliances include
  - Global
  - US government
  - Financial services
  - Health
  - Media and manufacturing

    - Regional

5.3.5 Azure Sovereign regions (Azure Government cloud services and Azure China cloud services)

Azure Government cloud services

- To provide the highest level of security and compliance, Azure Government uses physically isolated datacenters and networks located only in the US. Azure Government customers, such as the US federal, state, and local government or their partners, are subject to validation of eligibility.
- Azure Government provides the broadest compliance and Level 5 DoD approval. Azure Government is available in eight geographies and offers the most compliance certifications of any cloud provider

Azure China cloud services

- According to the China Telecommunication Regulation, providers of cloud services, infrastructure as a service (IaaS) and platform as a service (PaaS), must have value-added telecom permits.
- Only locally registered companies with less than 50 percent foreign investment qualify for these permits. To comply with this regulation, the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft
- Azure China 21Vianet supports most of the same services that global Azure has, such as geosynchronous data replication and autoscaling

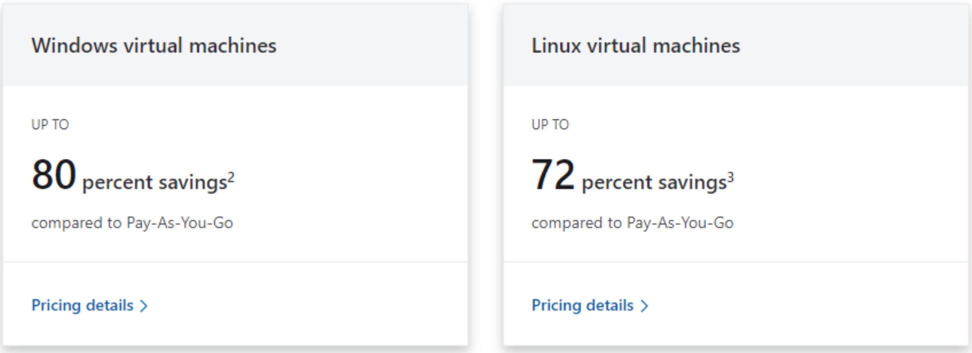
6 Azure cost management and Service level agreements (10-15%)

6.1 Factors that can affects costs

(a) Resource types : storage account you specify a type (such as block blob storage or table storage)
(b) Services : services from third-party vendors through Azure Marketplace
(c) Location : Different regions can have different associated prices. Because geographic regions can impact where your network traffic flows, network traffic is a cost influence to consider as well
(d) ingress (incoming request in network traffic)
(e) Egress traffic (outcoming request in network traffic)

6.2 Factors that can reduce costs

(a) Reserved instance (Combine Windows and Linux reserved VM instances savings with pay-as-you-go pricing to manage costs across predictable and variable workloads)



Windows virtual machines

UP TO

80 percent savings[2]

compared to Pay-As-You-Go

Pricing details >

Linux virtual machines

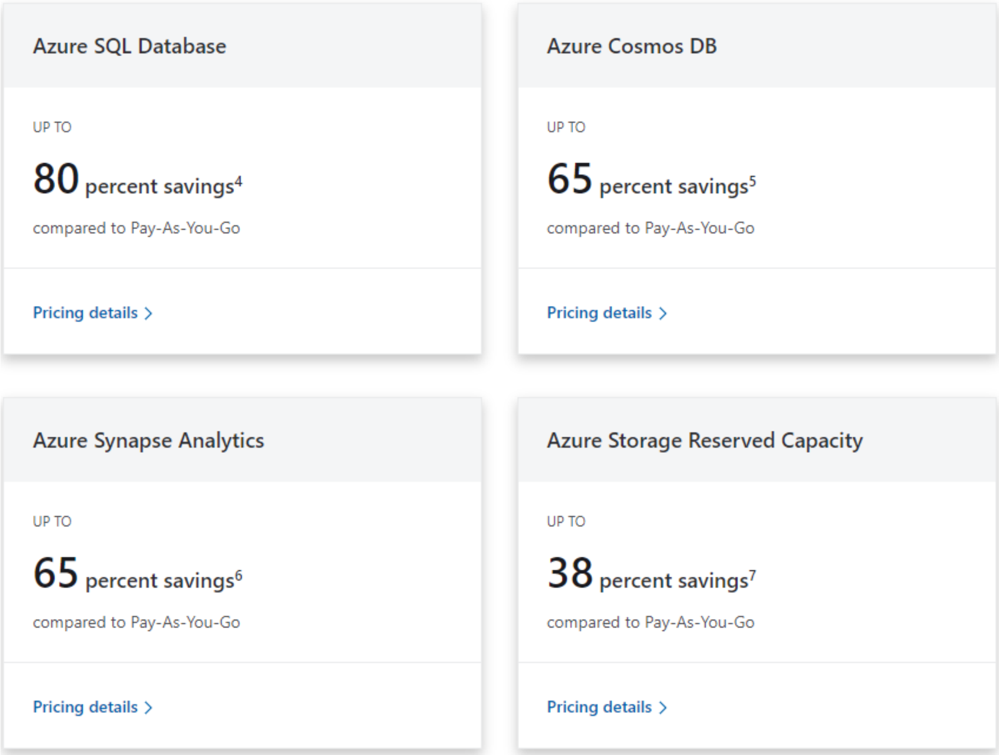
UP TO

72 percent savings[3]

compared to Pay-As-You-Go

Pricing details >

(b) Reserved capacity (Reduce your spend by pre-committing to fully managed Azure data services. Pay upfront or pay on a monthly basis at no additional cost.)



Azure SQL Database

UP TO

80 percent savings[4]

compared to Pay-As-You-Go

Pricing details >

Azure Cosmos DB

UP TO

65 percent savings[5]

compared to Pay-As-You-Go

Pricing details >

Azure Synapse Analytics

UP TO

65 percent savings[6]

compared to Pay-As-You-Go

Pricing details >

Azure Storage Reserved Capacity

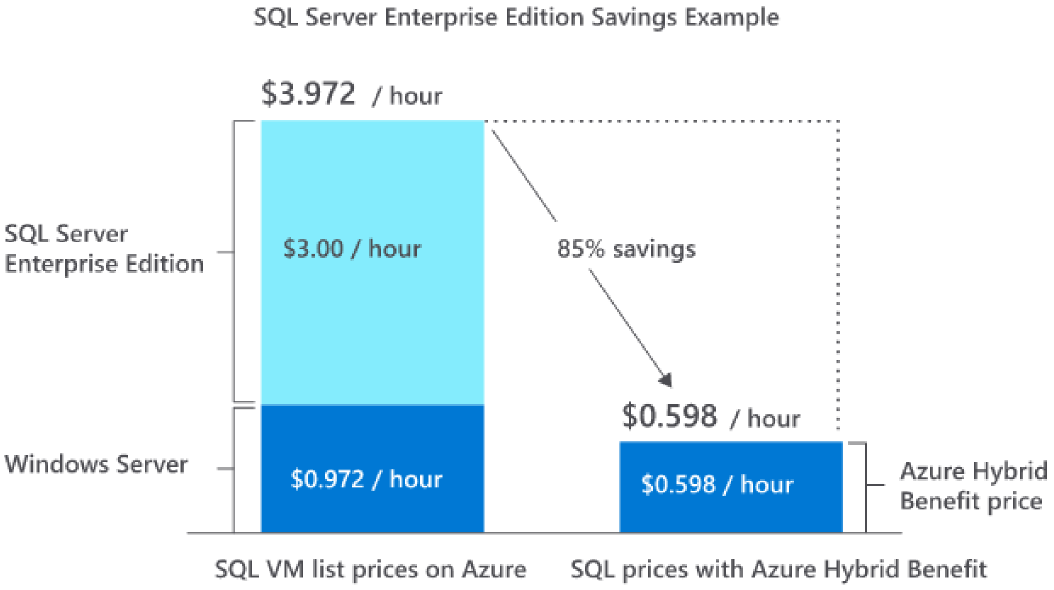
UP TO

38 percent savings[7]

compared to Pay-As-You-Go

Pricing details >

(c) Hybrid use benefit (AWS is five times more expensive than Azure for Windows and SQL Server. Save big when you migrate your on-premises workloads to Azure)



(d) Spot pricing

6.3 Pricing calculator and total cost of Ownership (TCO) calculator

Pricing calculator	Total cost of Ownership (TCO) calculator
● It displays Azure products in categories. ● You add these categories to your estimate and configure according to your specific requirements. ● You then receive a consolidated estimated price, with a detailed breakdown of the costs associated with each resource you added to your solution. ● You can **export or share** that estimate or save it for later. You can load a saved estimate and modify it to match updated requirements. You also can access pricing details, product details, and documentation for each product from within the Pricing calculator.	estimate the cost savings of operating your solution on Azure over time
	Steps: 1. Define your workloads.

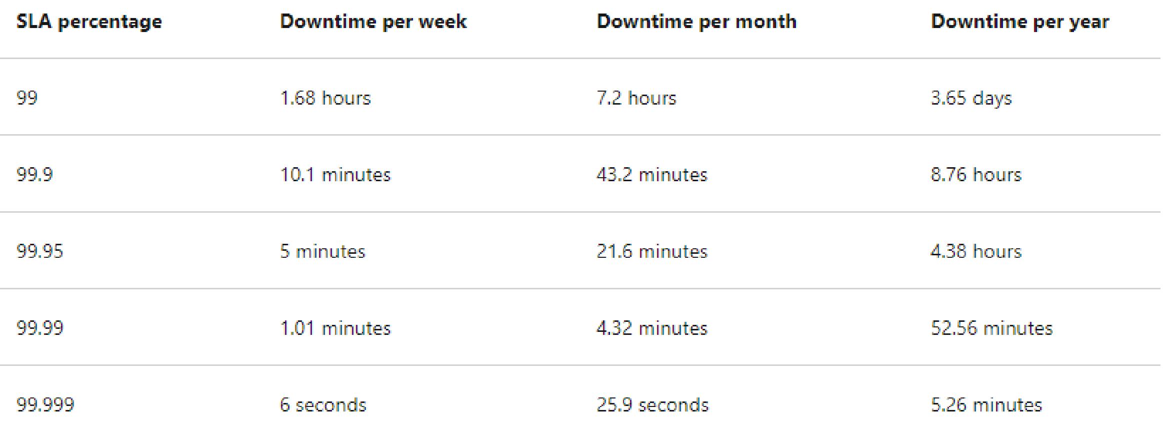
	2. Adjust assumptions. 3. View the report.

6.4 Azure cost management

- shows organizational cost and usage patterns with advanced analytics
- Reports in Cost Management show the usage-based costs consumed by Azure services and third-party Marketplace offerings
- Automated billing data export and scheduled reports are available
- uses Azure management groups, budgets, and recommendations to show clearly how your expenses are organized and how you might reduce costs
- use the Azure portal or various APIs for export automation to integrate cost data with external systems and processes

6.5 Azure Service Level agreement (SLA)

- defines the performance standards that Microsoft commits to for you, the customer
- Free products typically don't have an SLA
- Each Azure service defines its own SLA



SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99	1.01 minutes	4.32 minutes	52.56 minutes
99.999	6 seconds	25.9 seconds	5.26 minutes

6.6 Actions that can impact on SLA

- Choose customization options that fit your required SLA
  - Disks (Eg. Standard HDD Managed Disk)
  - Tiers (Eg. free tier product and as a standard paid service)
- Availability zones
  - to improve the availability of the application, avoid having any single points of failure. So instead of adding more virtual machines, you can deploy one or more extra instances of the same virtual machine across the **different availability zones** in the same Azure region
  - Each zone is made up of one or more data centers equipped with independent power, cooling, and networking. These zones use different schedules for maintenance, so if one zone is affected, your virtual machine instance in the other zone is unaffected.

- Included redundancy to increase availability
    - have duplicate components across several regions

6.7 Service lifecycle in Azure

- defines how every Azure service is released for public use
- Steps
    - **development phase**. In this phase, the Azure team collects and defines its requirements, and begins to build the service.
    - released to the **public preview** phase. During this phase, the public can access and experiment with it and provide real-world feedback. Your feedback helps Microsoft improve services. More importantly, providing feedback gives you the opportunity to request new or different capabilities so that services better meet your needs.
    - After a new Azure service has been validated and tested, it's released to all customers as a production-ready service. This is known as **general availability (GA)**.