AZ 900 Orientation

The Azure Roadmap

Fundamentals

AZ-900
Fundamentals

Associate

Administrator
- AZ-103

Developer
- AZ-203

AI Engineer
- A1-100

Data Scientist
DP-100

Data Engineer
- DP-200
- DP-201

Security
- AZ-500

Expert

Solutions Architect Expert
- AZ-300
- AZ-301

DevOps Engineer Expert
- AZ-400

Specialty

Azure for SAP Workloads
- AZ-120

IoT Developer
- AZ-220

About the Exam

Topic	Link
MS Learn	https://learn.microsoft.com/en-us/certifications/exams/az-900
Study Guide	Study Guide
Last Update	October 28, 2022
Passing score	700 / 1000
Negative Marking	No
Exam Duration	45 Minutes
Questions	40 – 50
Exam	* Proctored (Can be taken from home using personal laptop, since need to install a software, camera access and good stable internet * Prometric centers
Udemy Learning	https://cognizant.udemy.com/course/az900-azure/
Udemy Practice Test	https://cognizant.udemy.com/course/az900-azure-tests/learn/quiz/4700490#overview
ESI Practice Test	https://esi.microsoft.com/getcertification

Modules

- **Cloud concepts** :
  - Cloud computing
  - Benefits of using cloud services
  - cloud service types
- **Azure architecture and services**
  - Core architectural components of Azure
  - Azure compute and networking services
  - Azure storage services
  - Azure identity, access, and security
- **Azure management and governance**
  - Cost management in Azure
  - Features and tools in Azure for governance and compliance
  - Features and tools for managing and deploying Azure resources
  - Monitoring tools in Azure

Part 1: Cloud Concepts

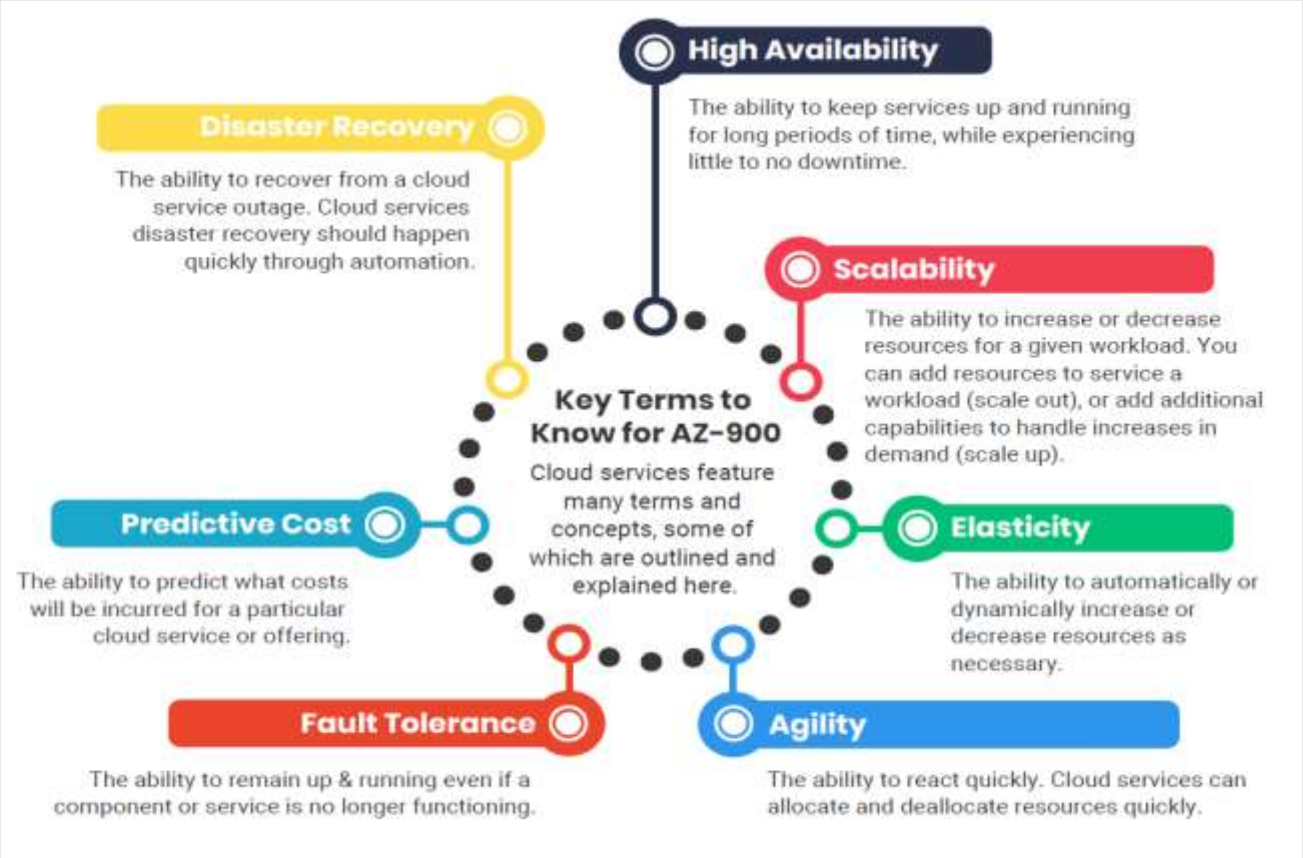
What is cloud computing?

- Delivery of computing services over the internet
- These services include servers, storage, databases, networking, software, analytics, and intelligence.
- Cloud computing offers faster innovation, flexible resources, and economies of scale.

Why is cloud computing typically cheaper to use?

- Uses pay-as-you-go pricing model, typically pay only for the cloud services you use, which helps you:
  - Lower your operating costs.
  - Run your infrastructure more efficiently.
  - Scale as your business needs change.
- Instead of maintaining CPUs and storage in your datacenter, you rent them for the time that you need them.
- The cloud provider takes care of maintaining the underlying infrastructure for you.

Why should I move to the cloud?



High Availability

The ability to keep services up and running for long periods of time, while experiencing little to no downtime.

Disaster Recovery

The ability to recover from a cloud service outage. Cloud services disaster recovery should happen quickly through automation.

Scalability

The ability to increase or decrease resources for a given workload. You can add resources to service a workload (scale out), or add additional capabilities to handle increases in demand (scale up).

Key Terms to Know for AZ-900

Cloud services feature many terms and concepts, some of which are outlined and explained here.

Predictive Cost

The ability to predict what costs will be incurred for a particular cloud service or offering.

Elasticity

The ability to automatically or dynamically increase or decrease resources as necessary.

Fault Tolerance

The ability to remain up & running even if a component or service is no longer functioning.

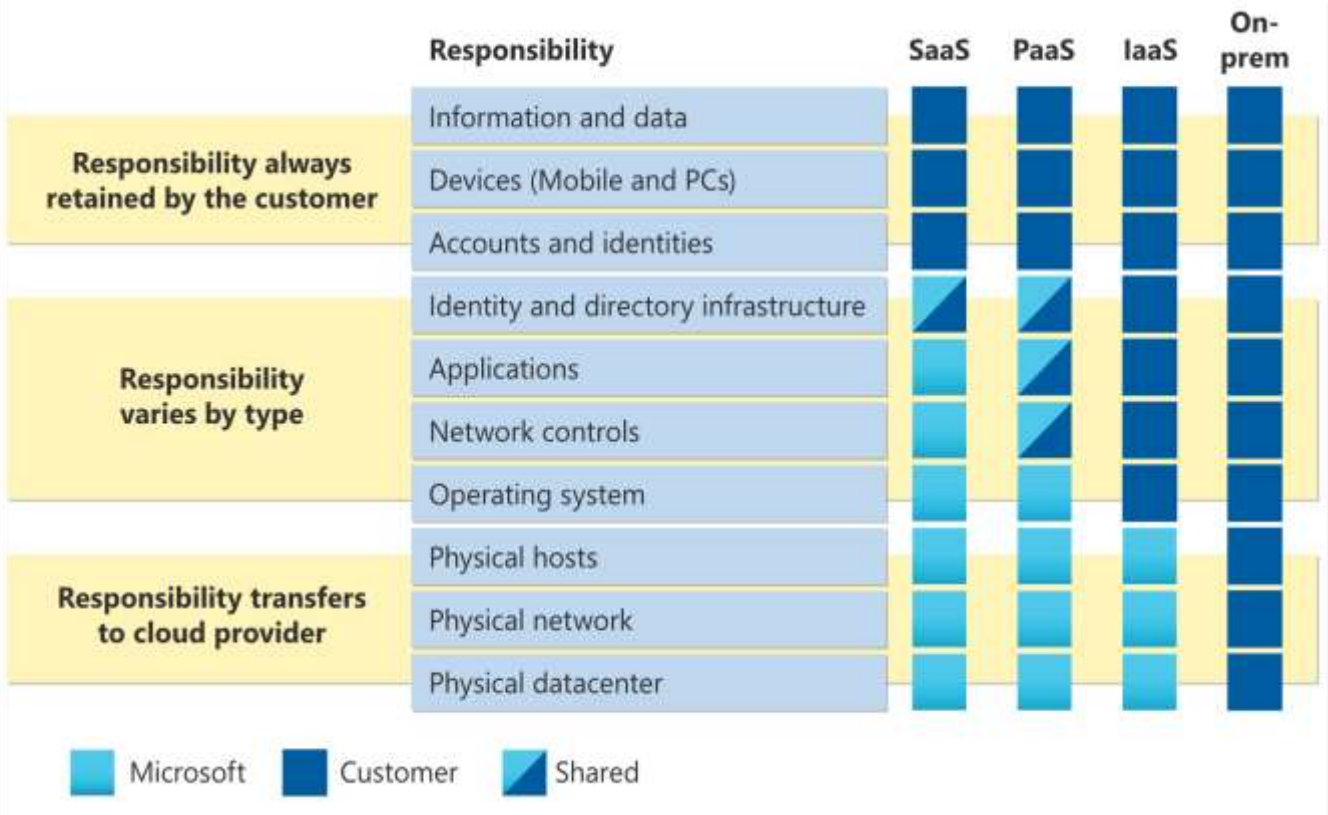
Agility

The ability to react quickly. Cloud services can allocate and deallocate resources quickly.

- **High availability**: Depending on the service-level agreement (SLA) that you choose, your cloud-based apps can provide a continuous user experience with no apparent downtime, even when things go wrong.
- **Scalability**: Apps in the cloud can scale vertically and horizontally:
  - Scale vertically to increase compute capacity by adding RAM or CPUs to a virtual machine.
  - Scaling horizontally increases compute capacity by adding instances of resources, such as adding VMs to the configuration.
- **Elasticity**: You can configure cloud-based apps to take advantage of autoscaling, so your apps always have the resources they need.
- **Agility**: Deploy and configure cloud-based resources quickly as your app requirements change.
- **Geo-distribution:** You can deploy apps and data to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region.
- **Disaster recovery**: By taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your apps with the confidence that comes from knowing that your data is safe in the event of disaster.

Shared Responsibility Model

With the shared responsibility model, these responsibilities get shared between the cloud provider and the consumer.



	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

Discuss different types of cloud models

- **Public cloud:** Services are offered over the public internet and available to anyone who wants to purchase them. Cloud resources, such as servers and storage, are owned and operated by a third-party cloud service provider, and delivered over the internet. No capital expenditures to scale up. Applications can be quickly provisioned and deprovisioned. Organizations pay only for what they use.
- **Private cloud:** Consists of computing resources used exclusively by users from one business or organization. A private cloud can be physically located at your organization's on-site (on-premises) datacenter, or it can be hosted by a third-party service provider. Hardware must be purchased for start-up and maintenance. Organizations have complete control over resources and security. Organizations are responsible for hardware maintenance and updates.
- **Hybrid cloud:** Computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them. Provides the most flexibility, Organizations determine where to run their applications. Organizations control security, compliance, or legal requirements

Capital expenses vs. operating expenses

- **Capital Expenditure (CapEx)** is the up-front spending of money on physical infrastructure, and then deducting that up-front expense over time. The up-front cost from CapEx has a value that reduces over time.
- **Operational Expenditure (OpEx)** is spending money on services or products now, and being billed for them now. You can deduct this expense in the same year you spend it. There is no up-front cost, as you pay for a service or product as you use it.

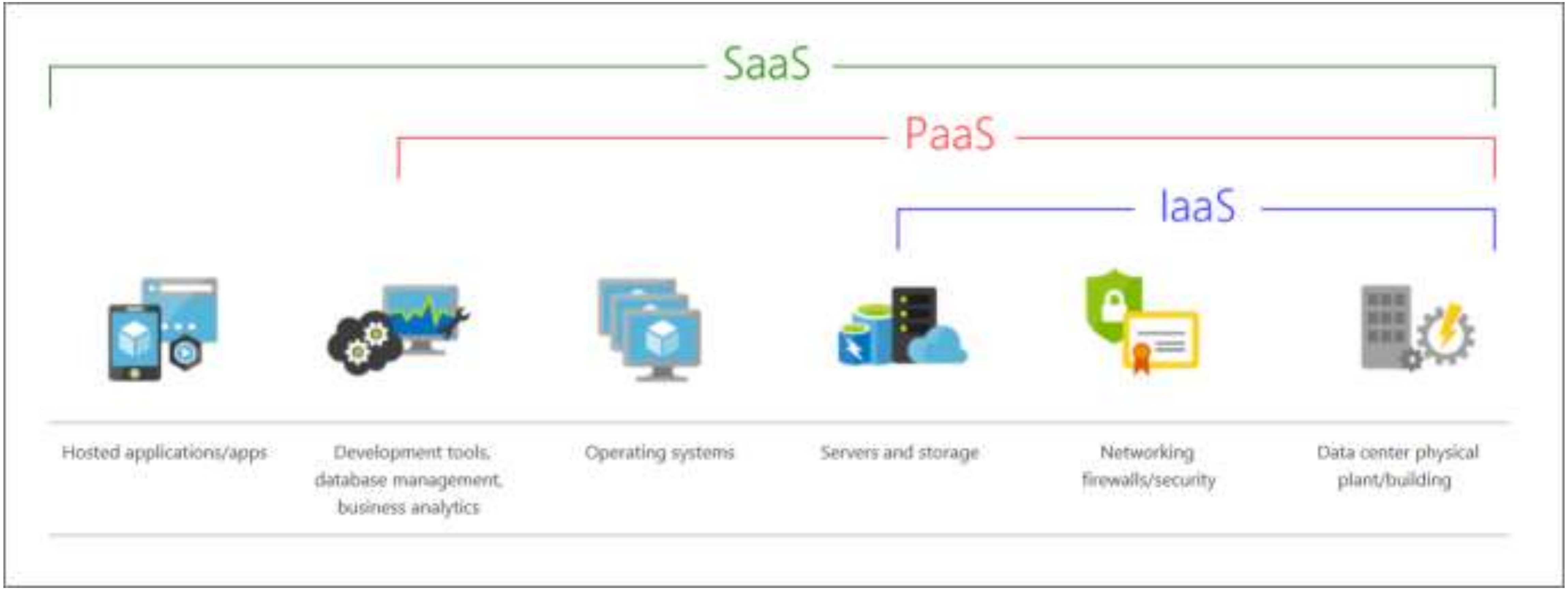
Describe different cloud services

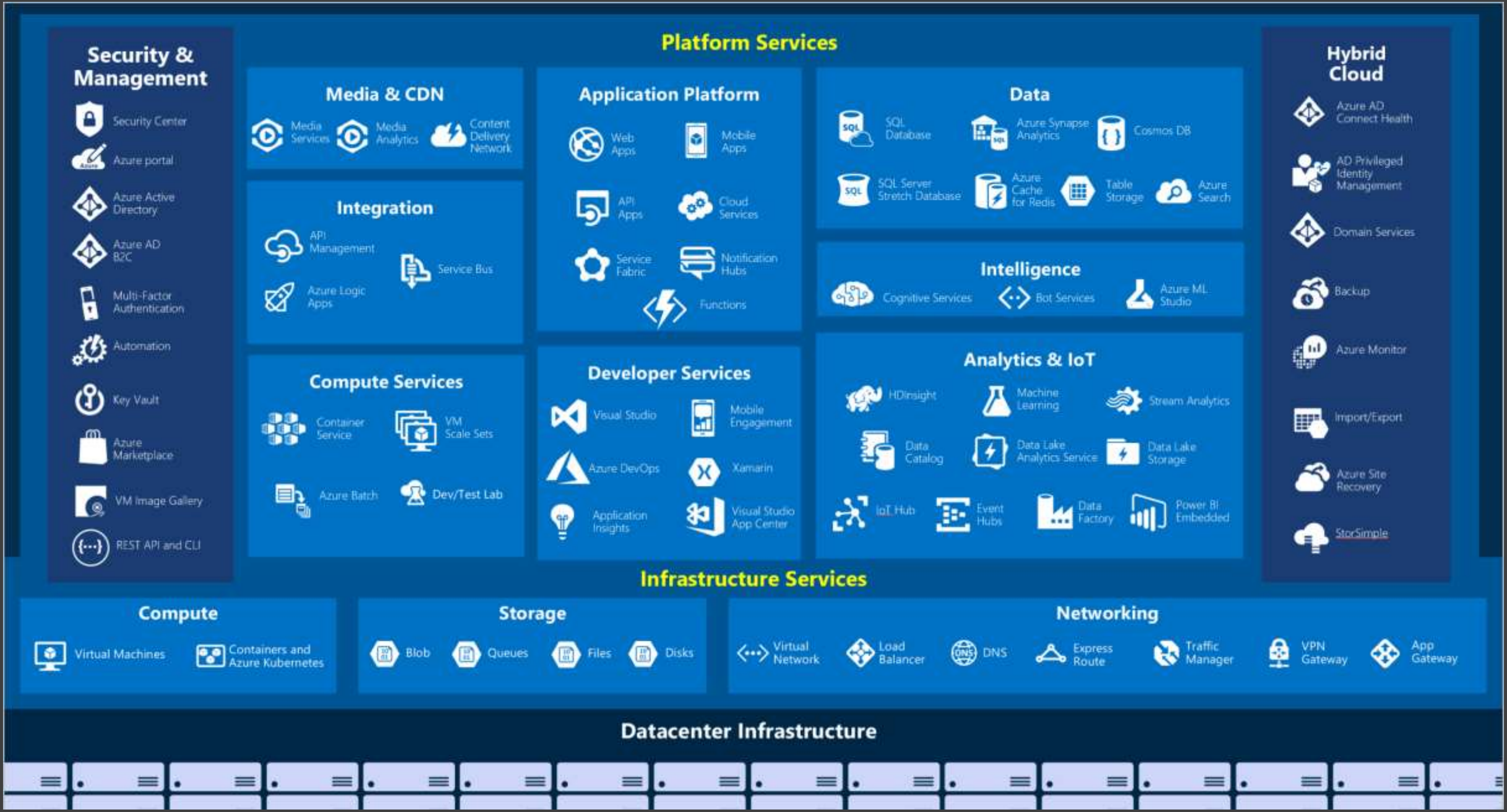
IaaS : *Infrastructure-as-a-Service:* This cloud service model is the closest to managing physical servers; a cloud provider will keep the hardware up-to-date, but operating system maintenance and network configuration is up to you as the cloud tenant.

PaaS : *Platform-as-a-Service:* This cloud service model is a managed hosting environment. The cloud provider manages the virtual machines and networking resources, and the cloud tenant deploys their applications into the managed hosting environment.

SaaS : *Software-as-a-Service:* In this cloud service model, the cloud provider manages all aspects of the application environment, such as virtual machines, networking resources, data storage, and applications. The cloud tenant only needs to provide their data to the application managed by the cloud provider.

The following illustration demonstrates the services that might run in each of the cloud service models.


SaaS
PaaS
IaaS
Hosted applications/apps
Development tools, database management, business analytics
Operating systems
Servers and storage
Networking firewalls/security
Data center physical plant/building



Platform Services

Security & Management

- Security Center
- Azure portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Key Vault
- Azure Marketplace
- VM Image Gallery
- REST API and CLI

Media & CDN

- Media Services
- Media Analytics
- Content Delivery Network

Integration

- API Management
- Service Bus
- Azure Logic Apps

Compute Services

- Container Service
- VM Scale Sets
- Azure Batch
- Dev/Test Lab

Application Platform

- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Notification Hubs
- Functions

Developer Services

- Visual Studio
- Mobile Engagement
- Azure DevOps
- Xamarin
- Application Insights
- Visual Studio App Center

Data

- SQL Database
- Azure Synapse Analytics
- Cosmos DB
- SQL Server Stretch Database
- Azure Cache for Redis
- Table Storage
- Azure Search

Intelligence

- Cognitive Services
- Bot Services
- Azure ML Studio

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Storage
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud

- Azure AD Connect Health
- AD Privileged Identity Management
- Domain Services
- Backup
- Azure Monitor
- Import/Export
- Azure Site Recovery
- StorSimple

Infrastructure Services

Compute

- Virtual Machines
- Containers and Azure Kubernetes

Storage

- Blob
- Queues
- Files
- Disks

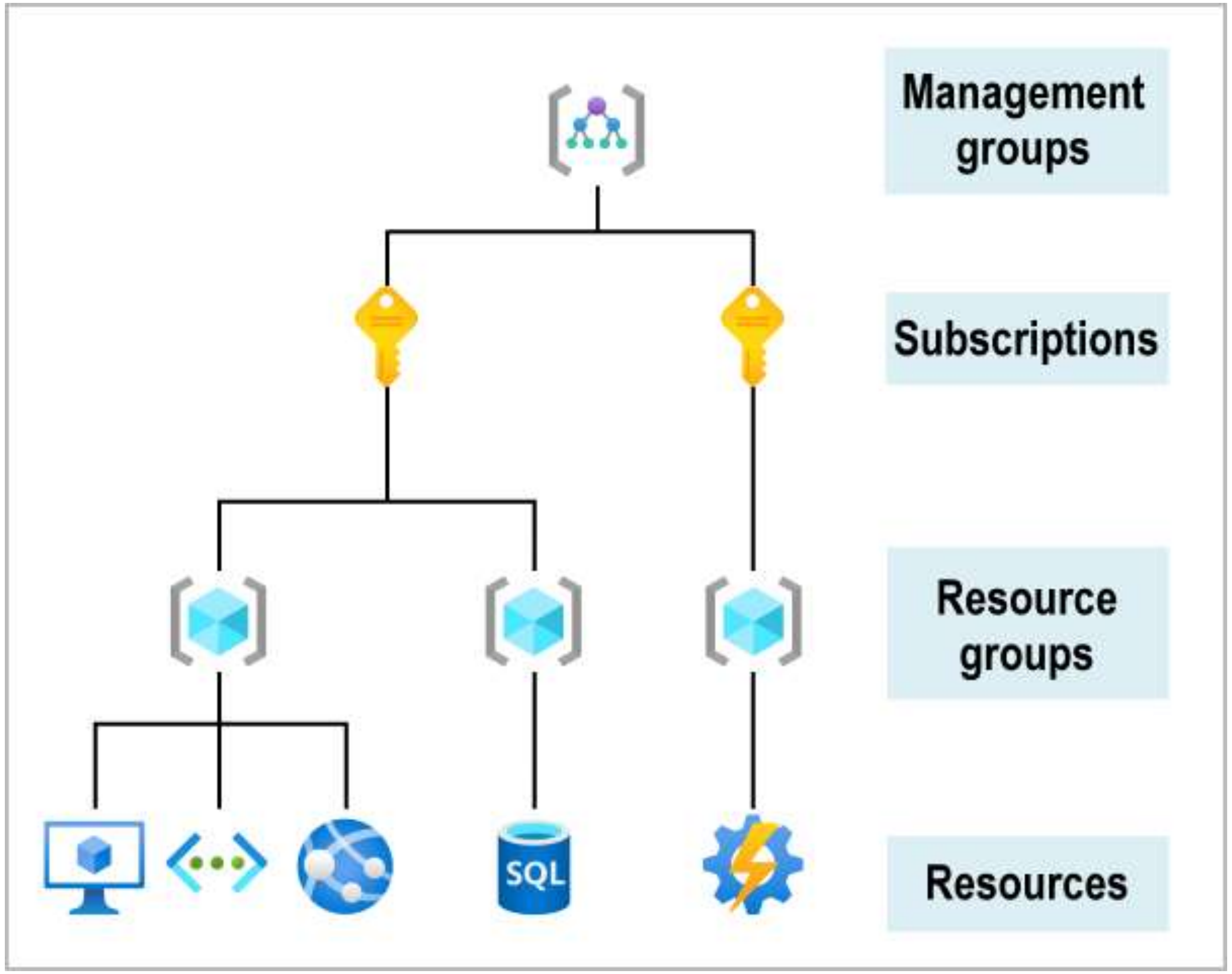
Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure

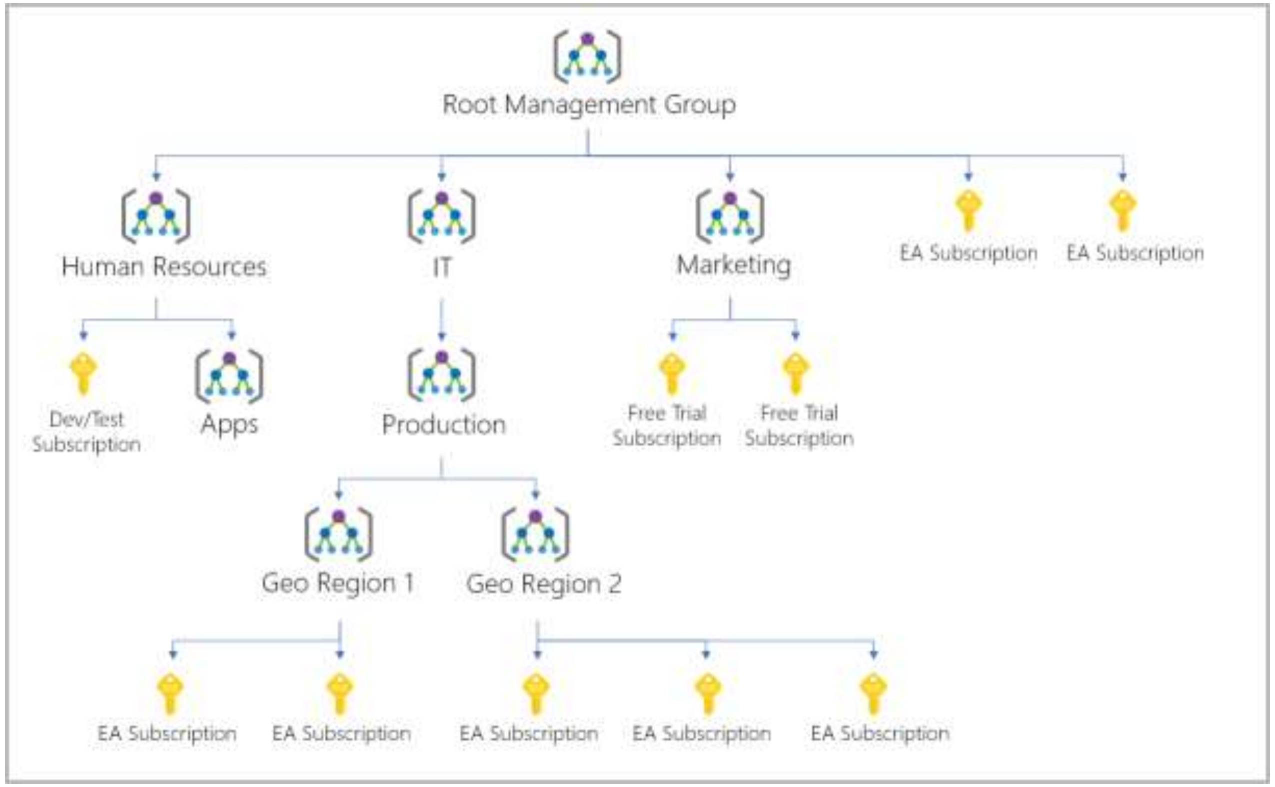
Azure subscriptions, management groups, and resources

- **Resources**: Resources are instances of services that you create, like virtual machines, storage, or SQL databases.
- **Resource groups**: Resources are combined into resource groups, which act as a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Subscriptions**: A subscription groups together user accounts and the resources that have been created by those user accounts. For each subscription, there are limits or quotas on the amount of resources that you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Management groups**: These groups help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.



Hierarchy of management groups and subscriptions

- You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management.
- All resources must be in a resource group, **and a resource can only be a member of a single resource group**. Many resources can be moved between resource groups with some services having specific limitations or requirements to move.
- **Resource groups can't be nested**. Before any resource can be provisioned, you need a resource group for it to be placed in



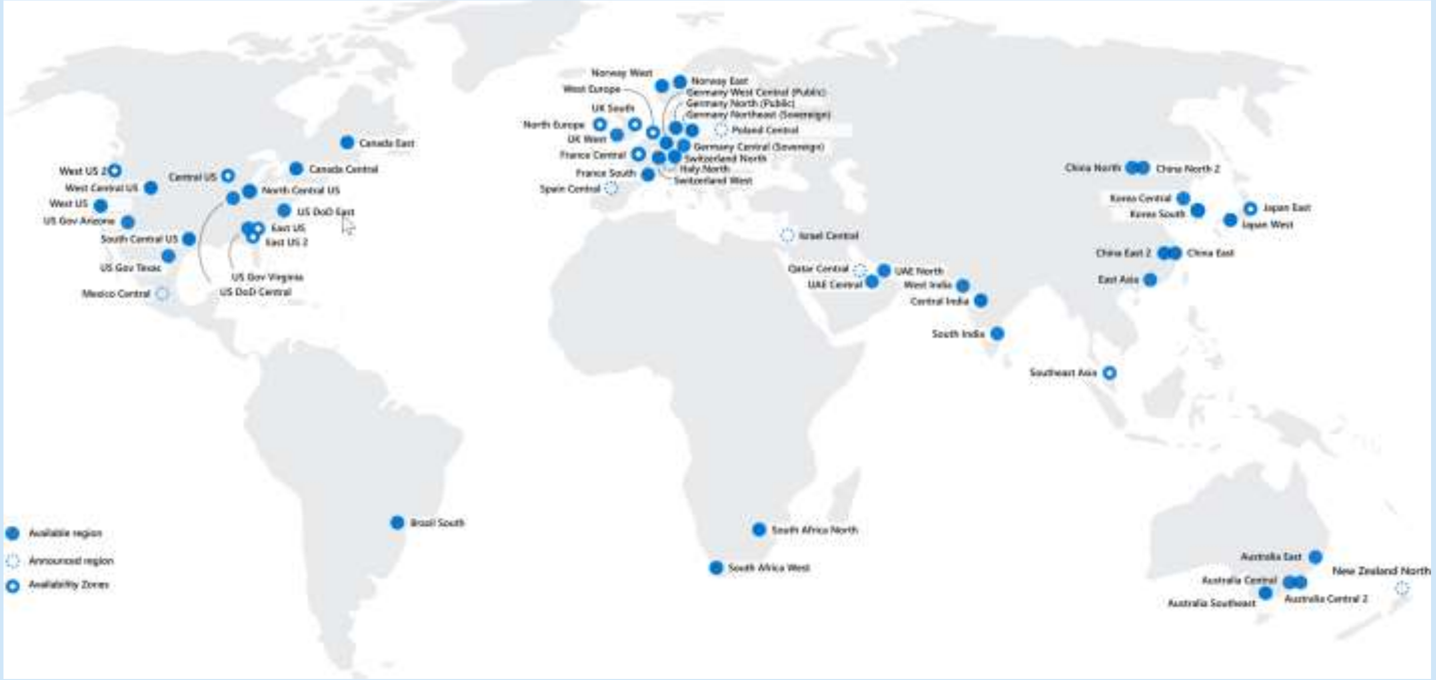
Important facts about management groups

- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.
- Each management group and subscription can support only one parent.
- Each management group can have many children.
- All subscriptions and management groups are within a single hierarchy in each directory.

Geographies

- Azure divides the world into geographies that are defined by geopolitical boundaries or country borders.
- An Azure geography is a discrete market typically containing **two or more** regions that preserves data residency and compliance boundaries.
- This division has several benefits.
  - Geographies allow customers with specific data residency and compliance needs to keep their data and applications close.
  - Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.
  - Geographies are fault-tolerant to withstand complete region failure through their connection to dedicated high-capacity networking infrastructure.
- Geographies are broken up into the following areas:
  - Americas
  - Europe
  - Asia Pacific
  - Middle East and Africa

Azure regions

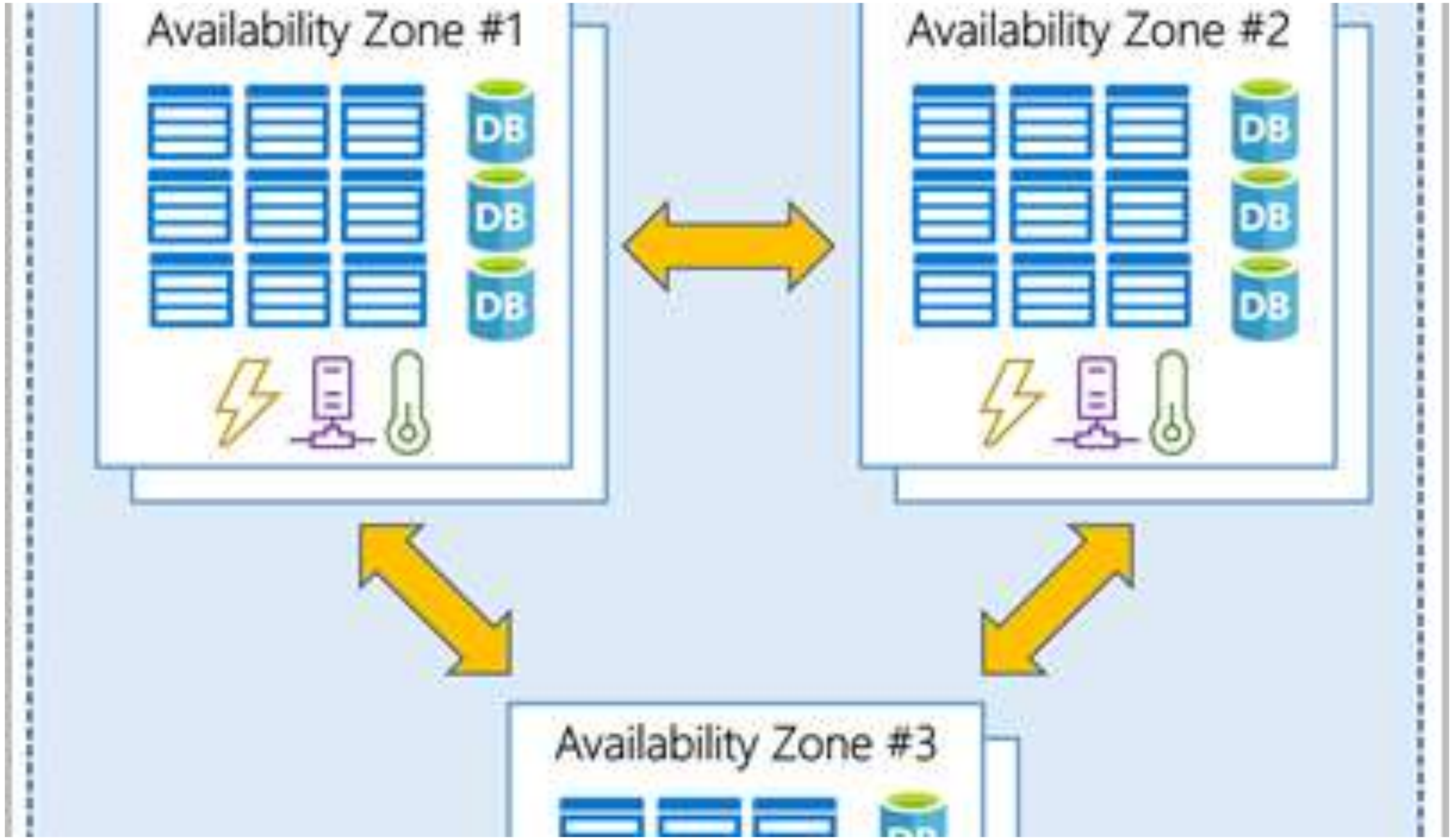


- A *region* is a geographical area on the planet that contains at least one but potentially multiple datacenters that are nearby and networked together with a low-latency network.
- Azure intelligently assigns and controls the resources within each region to ensure workloads are appropriately balanced.

Special Azure regions

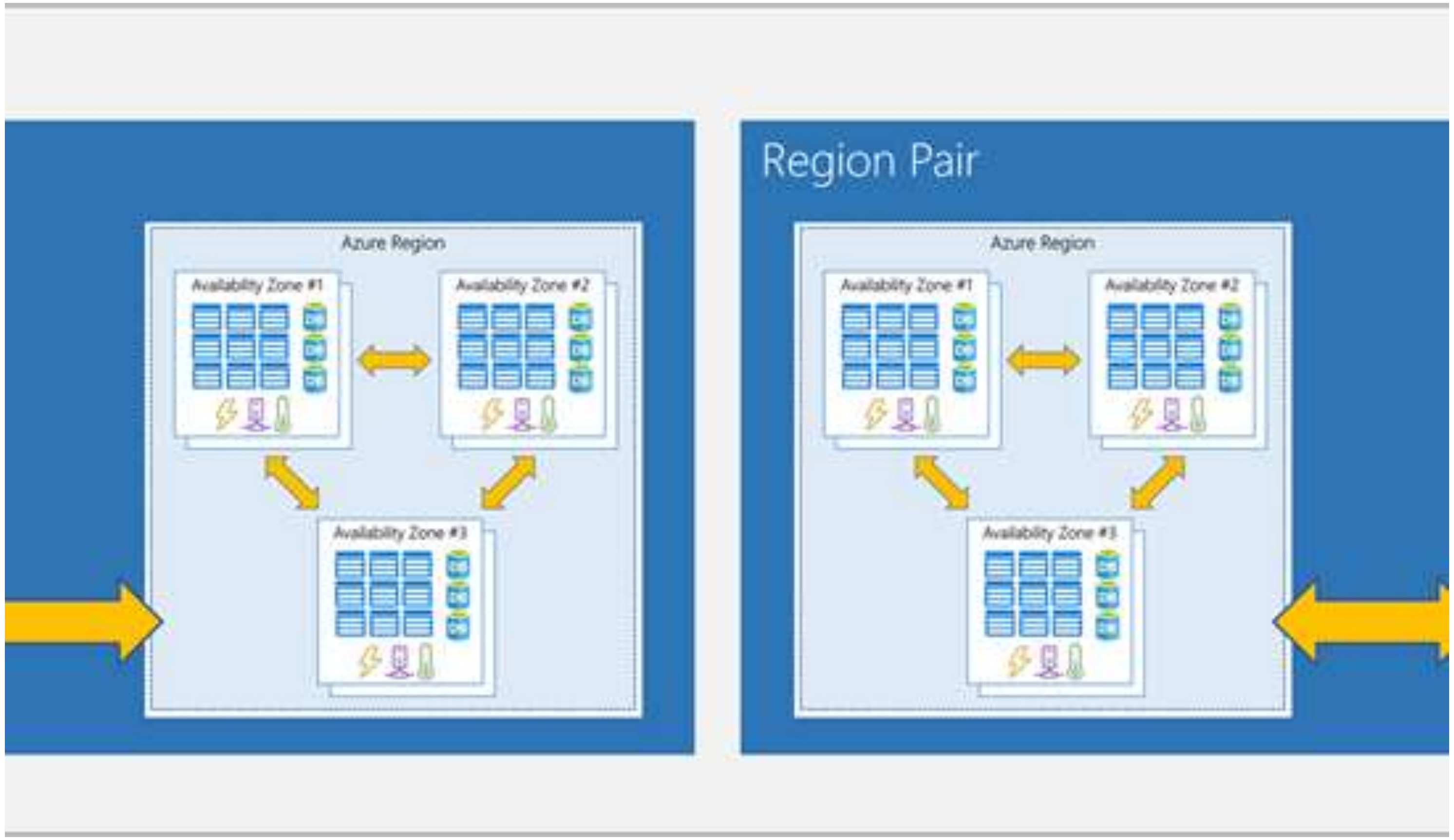
- **US DoD Central, US Gov Virginia, US Gov Iowa and more:** These regions are physical and logical network-isolated instances of Azure for U.S. government agencies and partners. These datacenters are operated by screened U.S. personnel and include additional compliance certifications.
- **China East, China North, and more:** These regions are available through a unique partnership between Microsoft and 21Vianet, whereby Microsoft doesn't directly maintain the datacenters.

Azure availability zones



- Availability zones (AZ) are physically separate datacenters within an Azure region.
- Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking.
- An availability zone is set up to be an *isolation boundary*. If one zone goes down, the other continues working.
- Availability zones are connected through high-speed, private fiber-optic networks.

Azure region pairs

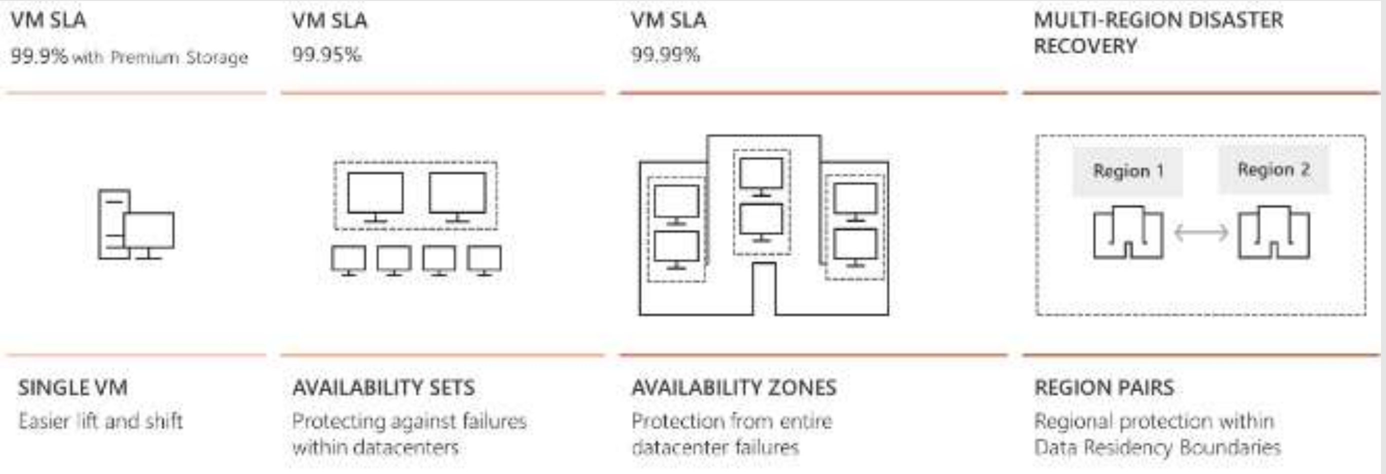


- Each region is always paired with another region within the same geography at least 300 miles away.
- This approach allows for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect both regions at once.
- If a region in a pair was affected by a natural disaster, for instance, services would automatically failover to the other region in its region pair.

Availability Sets

- Way for you to ensure your application remains online if a high-impact maintenance event is required, or if a hardware failure occurs.
- Availability sets are made up of Update domains (UD) and Fault domains (FD).
  - **Update domains**. When a maintenance event occurs the update is sequenced through update domains. Sequencing updates using update domains ensures that the entire datacenter isn't unavailable during platform updates and patching. Update domains are a logical section of the datacenter, and they are implemented with software and logic.
  - **Fault domains**. Provide for the physical separation of your workload across different hardware in the datacenter. This includes power, cooling, and network hardware that supports the physical servers located in server racks. In the event the hardware that supports a server rack becomes unavailable, only that rack of servers would be affected by the outage.

Availability Option



VM SLA
99.9% with Premium Storage

SINGLE VM
Easier lift and shift

VM SLA
99.95%

AVAILABILITY SETS
Protecting against failures within datacenters

VM SLA
99.99%

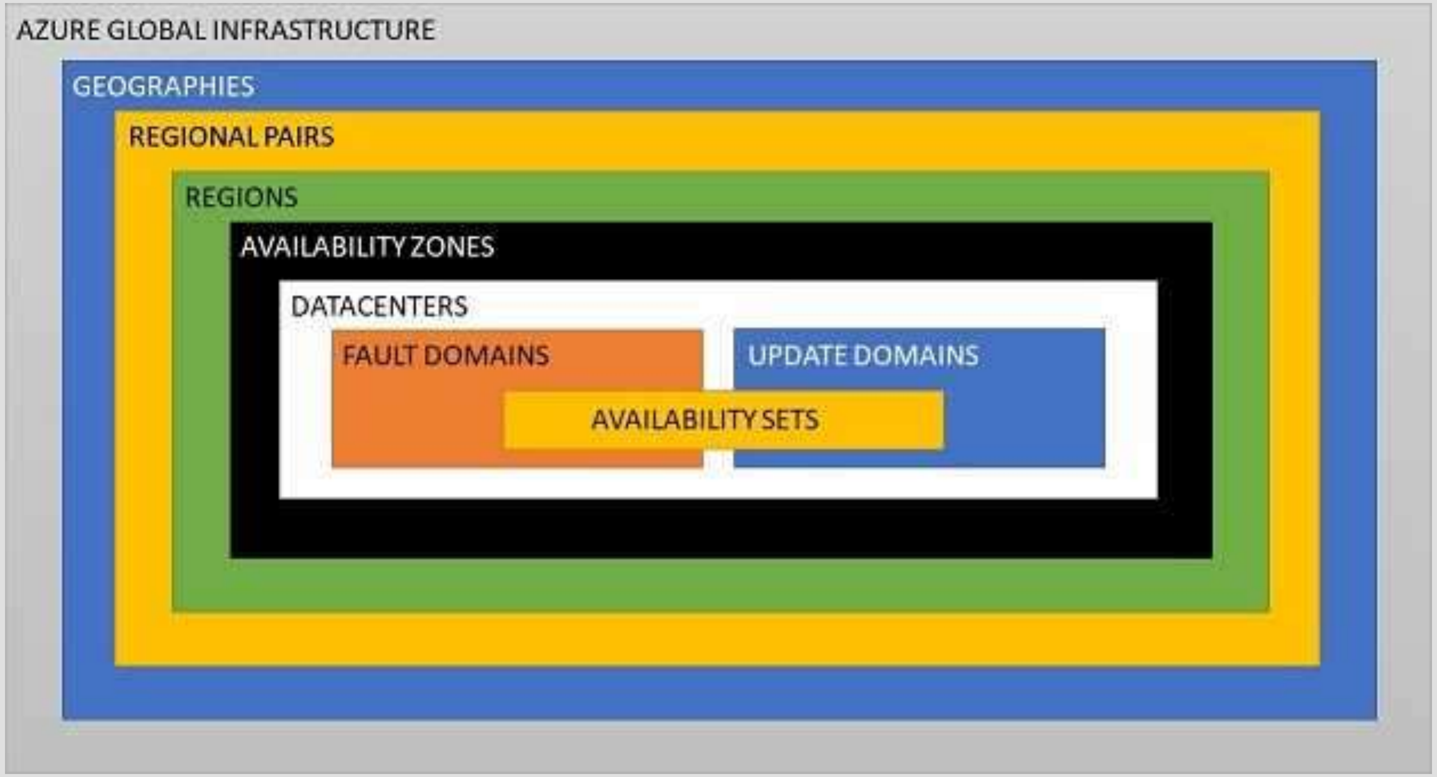
AVAILABILITY ZONES
Protection from entire datacenter failures

MULTI-REGION DISASTER RECOVERY

REGION PAIRS
Regional protection within Data Residency Boundaries

- A single virtual machine with premium storage has an SLA of 99.9%.
- By placing virtual machines in an availability set, you protect against datacenter failures and increases the SLA to 99.95%.
- Adding virtual machines to availability zones protects from entire datacenter failures and increases the SLA to 99.99%, which is highest level of protection that is provided.

Summary


AZURE GLOBAL INFRASTRUCTURE
GEOGRAPHIES
REGIONAL PAIRS
REGIONS
AVAILABILITY ZONES
DATACENTERS
FAULT DOMAINS
UPDATE DOMAINS
AVAILABILITY SETS

Core Services

Region	Networking	Database	Big Data & Analytics
Region Pairs	Virtual Network	*Cosmo DB*	Synapse
Geographies	Load Balancer	*Azure SQL database*	HDInsight
Availability Option	VPN Gateway	*SQL data warehouse (Rep)*	Data Lake Analytics
Availability Sets	Application Gateway	*Database Migration Service*	Serverless Computing
Availability Zones	Content Delivery Network	*Azure Market Place*	Functions
Resource Groups	Storage	Identify Azure solutions	Logic Apps
Azure Resource Manager	Azure Storage	Internet of Things	
Compute	Blob	IoT Central	DevOps Services & Azure Lab
Virtual Machine	Table	Azure IoT Hub	Azure App Services
Virtual Machine Scale Set	Queue	Artificial Intelligence	Azure Management Tools
App Service	File	*Vision & Speech*	Azure Portal & CLI
Functions	Disk	*Language*	PowerShell & Cloud Shell
Azure Container Instances		*Knowledge*	REST API
Azure Kubernetes Services		*Search*	Azure Advisor

Azure Compute & networking services

Azure Virtual Network fundamentals

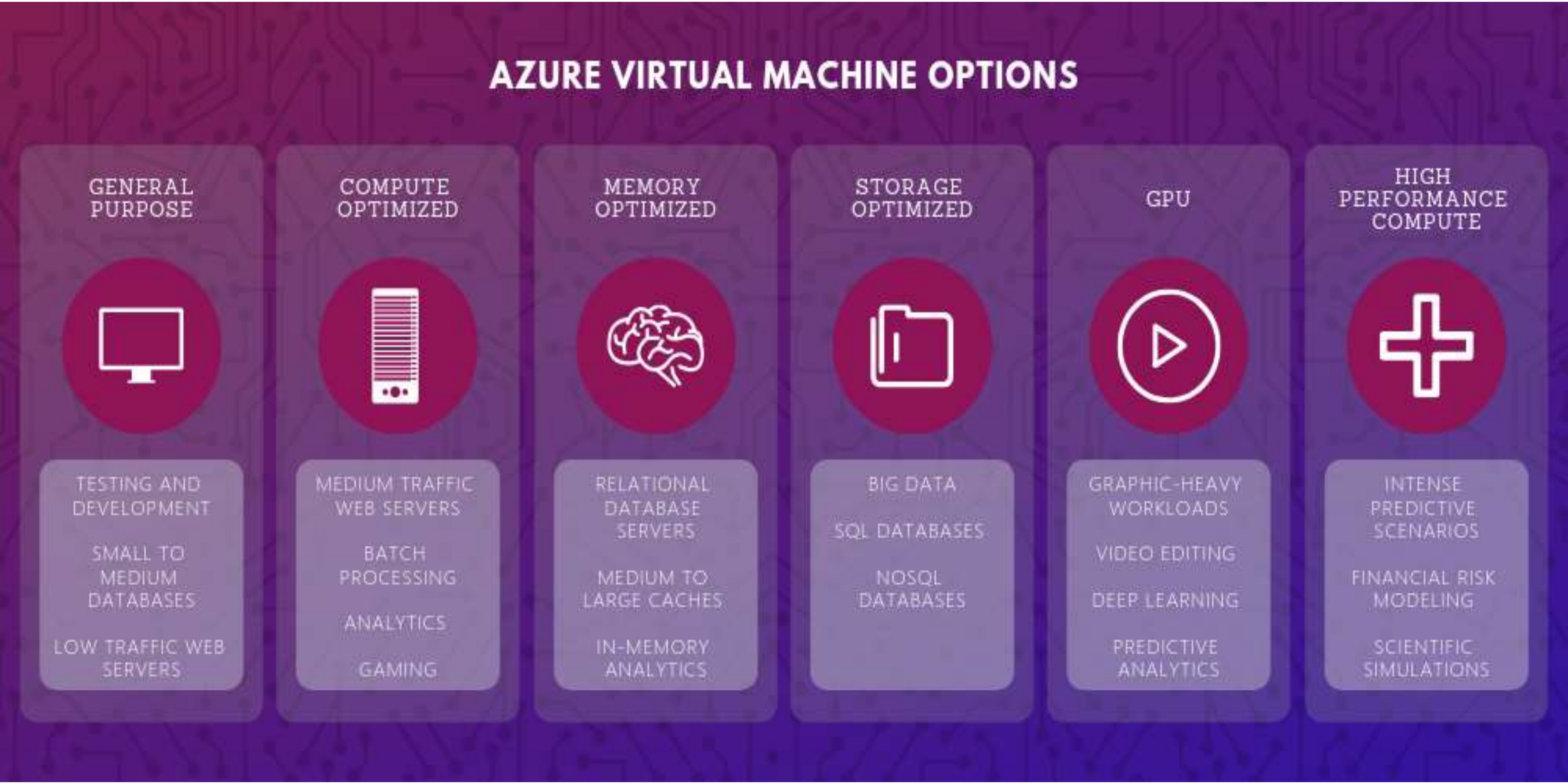
- *Azure virtual networks* enable Azure resources, such as VMs, web apps, and databases, to communicate with each other, with users on the internet, and with your on-premises client computers. You can think of an Azure network as a set of resources that links other Azure resources.
- Azure virtual networks provide the following key networking capabilities:
  - Isolation and segmentation
  - Internet communications
  - Communicate between Azure resources
  - Communicate with on-premises resources
  - Route network traffic
  - Filter network traffic
  - Connect virtual networks

Virtual machines

- Virtual machines are software emulations of physical computers.
- They include a virtual processor, memory, storage, and networking resources. VMs host an operating system, and you can install and run software just like a physical computer.
- Virtual Machines provides infrastructure as a service (IaaS) and can be used in different ways.
- When you need total control over an operating system and environment, VMs are an ideal choice. Just like a physical computer, you can customize all the software running on the VM. This ability is helpful when you're running custom software or custom hosting configurations.

Decide when to use Azure Virtual Machines

- With Azure Virtual Machines, you can create and use VMs in the cloud. VMs provide infrastructure as a service (IaaS) in the form of a virtualized server and can be used in many ways. Just like a physical computer, you can customize all of the software running on the VM. VMs are an ideal choice when you need:
  - Total control over the operating system (OS).
  - The ability to run custom software.
  - To use custom hosting configurations.
- An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM. You still need to configure, update, and maintain the software that runs on the VM.
- You can create and provision a VM in minutes when you select a preconfigured VM image. Selecting an image is one of the most important decisions you'll make when you create a VM. An image is a template used to create a VM. These templates already include an OS and often other software, like development tools or web hosting environments.



AZURE VIRTUAL MACHINE OPTIONS

GENERAL PURPOSE

- TESTING AND DEVELOPMENT
- SMALL TO MEDIUM DATABASES
- LOW TRAFFIC WEB SERVERS

COMPUTE OPTIMIZED

- MEDIUM TRAFFIC WEB SERVERS
- BATCH PROCESSING
- ANALYTICS
- GAMING

MEMORY OPTIMIZED

- RELATIONAL DATABASE SERVERS
- MEDIUM TO LARGE CACHES
- IN-MEMORY ANALYTICS

STORAGE OPTIMIZED

- BIG DATA
- SQL DATABASES
- NOSQL DATABASES

GPU

- GRAPHIC-HEAVY WORKLOADS
- VIDEO EDITING
- DEEP LEARNING
- PREDICTIVE ANALYTICS

HIGH PERFORMANCE COMPUTE

- INTENSE PREDICTIVE SCENARIOS
- FINANCIAL RISK MODELING
- SCIENTIFIC SIMULATIONS

Virtual machine scale sets

- Virtual machine scale sets are an Azure compute resource that you can use to deploy and manage a set of identical VMs.
- With all VMs configured the same, virtual machine scale sets are designed to support true autoscale.
- No pre-provisioning of VMs is required. For this reason, it's easier to build large-scale services targeting big compute, big data, and containerized workloads.
- As demand goes up, more VM instances can be added. As demand goes down, VM instances can be removed. The process can be manual, automated, or a combination of both.

What are containers?

- Containers are a virtualization environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host.
- Unlike virtual machines, you don't manage the operating system for a container.
- Virtual machines appear to be an instance of an operating system that you can connect to and manage, but containers are lightweight and designed to be created, scaled out, and stopped dynamically.
- While it's possible to create and deploy virtual machines as application demand increases, containers are designed to allow you to respond to changes on demand. With containers, you can quickly restart in case of a crash or hardware interruption. One of the most popular container engines is Docker, which is supported by Azure.

Manage containers

- Containers are managed through a container orchestrator, which can start, stop, and scale out application instances as needed. There are two ways to manage both Docker and Microsoft-based containers in Azure: Azure Container Instances and Azure Kubernetes Service (AKS).
- **Azure Container Instances**
- Azure Container Instances offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services.
- It's a platform as a service (PaaS) offering that allows you to upload your containers, which it runs for you.
- **Azure Kubernetes Service**
- The task of automating, managing, and interacting with a large number of containers is known as orchestration.
- Azure Kubernetes Service is a complete orchestration service for containers with distributed architectures and large volumes of containers.

Functions

- Functions are ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure.
- They're commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.
- Using a virtual machine-based approach, you'd incur costs even when the virtual machine is idle. With functions, Azure runs your code when it's triggered and automatically deallocates resources when the function is finished. In this model, you're only charged for the CPU time used while your function runs.
- Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they're restarted every time they respond to an event. When they're stateful (called Durable Functions), a context is passed through the function to track prior activity.

Isolation and segmentation

- Virtual Network allows you to create multiple isolated virtual networks. When you set up a virtual network, you define a private IP address space by using either public or private IP address ranges.
- You can divide that IP address space into subnets and allocate part of the defined address space to each named subnet.
- For name resolution, you can use the name resolution service that's built in to Azure. You also can configure the virtual network to use either an internal or an external DNS server.

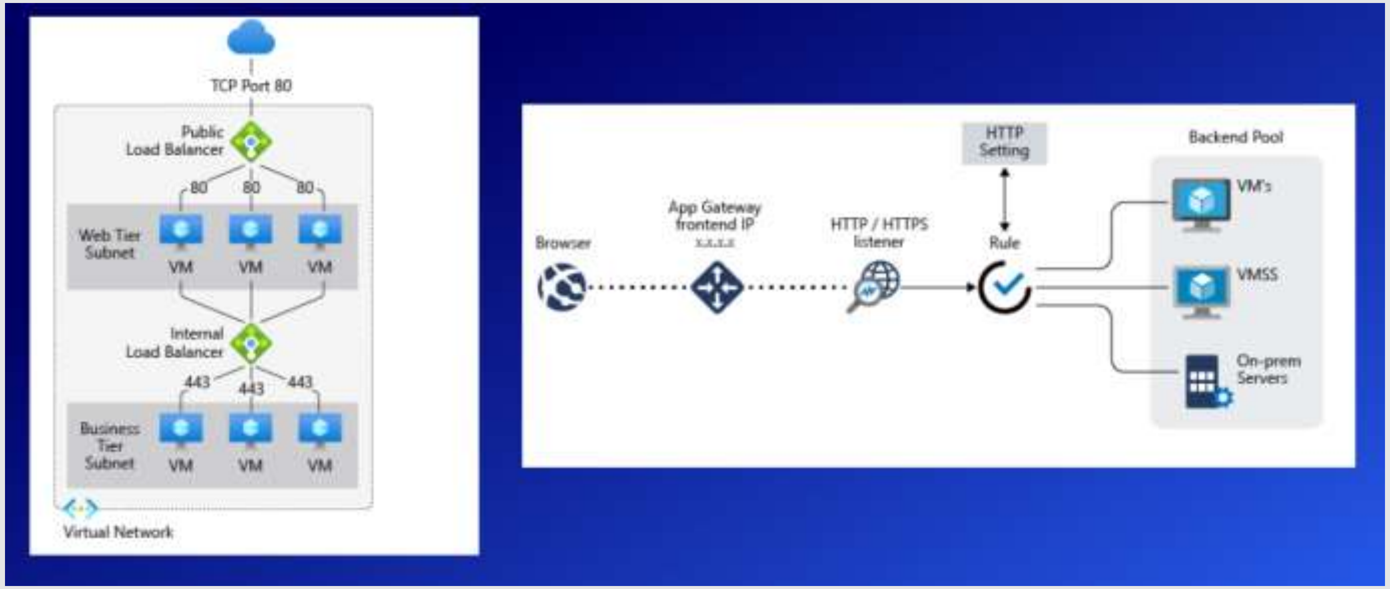
Communicate between Azure resources

Service endpoints You can use service endpoints to connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

Communicate with on-premises resources

- **Point-to-site virtual private networks** The typical approach to a virtual private network (VPN) connection is from a computer outside your organization, back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect that computer to the Azure virtual network.
- **Site-to-site virtual private networks** A site-to-site VPN links your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.
- **Azure ExpressRoute** For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach. ExpressRoute provides dedicated private connectivity to Azure that doesn't travel over the internet

Load Balancer



- A load balancer is a network device that distributes traffic according to some algorithm between multiple servers.
- If you have multiple virtual machines, and you want each of them, let's say you have two of them, and you want them to split the traffic 50/50, you're going to need to put a load balancer in front of that in order for traffic to be evenly divided, that is a load balancer device.
- Load Balancer supports inbound and outbound scenarios,
- Provides low latency and high throughput, and scales up to millions of flows for all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) applications.
- You can use Load Balancer with incoming internet traffic, internal traffic across Azure services, port forwarding for specific traffic, or outbound connectivity for VMs in your virtual network.

Filter network traffic

Network security groups A network security group is an Azure resource that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol

Content Delivery Network

- A content delivery network are servers that you don't control that will actually store your files to distribute to your users that will basically speed up your application.
- The way that it works is instead of having a single server that serves every single file of your application, what you would is end up with is a distributed network of servers that conserve some of the files, the static files, the images, the java scripts, the CSS videos, anything that doesn't change, a CDN can help you by reducing the amount of traffic to your server, as well as delivering traffic in a lot quicker way.
- There's a couple of reasons why this is.
  - One of them is the CDN network is globally distributed, whereas your server might just be running within one region, let's say it's East U.S. region, the CDN would have European African, Asian servers and that would be a lot quicker to serve traffic.
  - The second reason is the way that your browser operates, it will know that there's multiple different URLs, different domain names, and will make requests to those servers concurrently, as opposed to queuing up this requests to a single domain.   So it will add a maximum since six requests to a single domain name, but if you had a CDN that basically doubles the number of requests that go out at once.
- CDN can really speed up your application, Microsoft Azure offers CDN services.

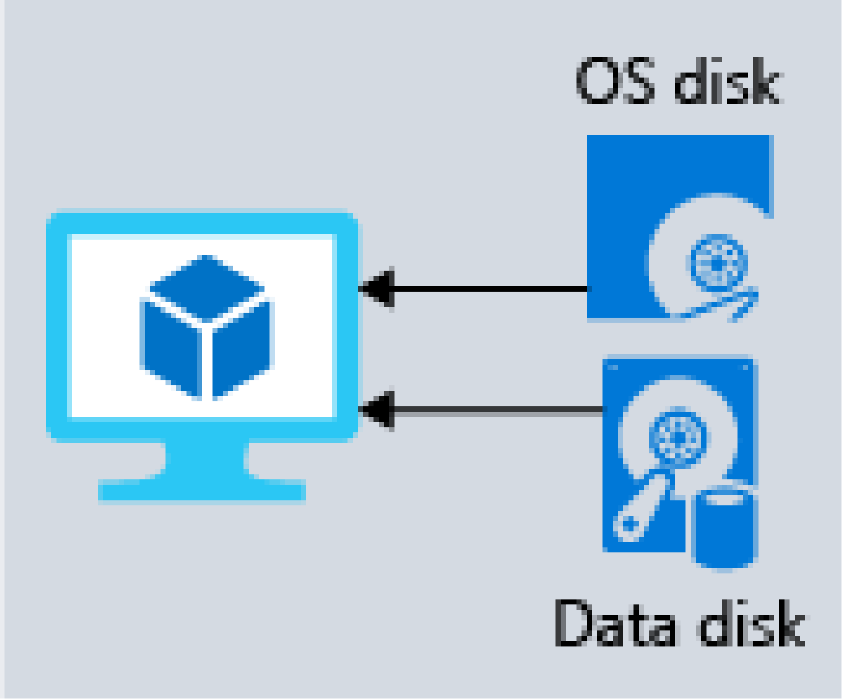
Explore Azure Storage services

Storage Types

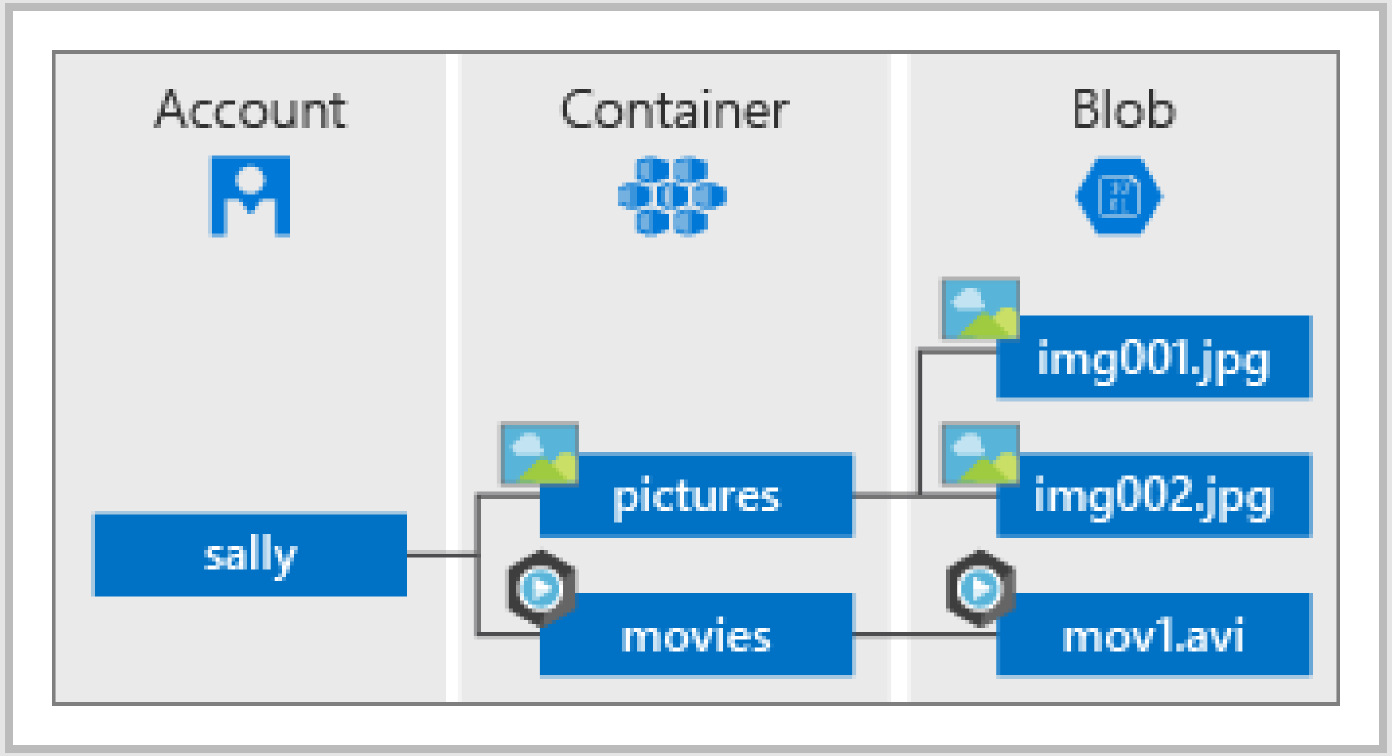
- **Disk storage:** Provides disks for virtual machines, applications, and other services to access and use as they needs, allows data to be persistently stored and accessed from an attached virtual hard disk. The disks can be managed or unmanaged by Azure, and therefore managed and configured by the user. Typical scenarios for using disk storage are if you want to lift and shift applications that read and write data to persistent disks. Disks come in many different sizes and performance levels, from solid-state drives (SSDs) to traditional spinning hard disk drives (HDDs), with varying performance abilities and cost.
- **Containers (Blobs):** Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data. Blob storage is ideal for: Serving images or documents directly to a browser, Storing files for distributed access, Streaming video and audio etc
- **Files:** Set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access.
- **Queues** Queue service is used to store and retrieve messages, queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are generally used to store lists of messages to be processed asynchronously. For example, say you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue.
- **Tables**: Storage stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud. Azure tables are ideal for storing structured, non-relational data.

Disk storage fundamentals

- Disk Storage provides disks for Azure virtual machines. Applications and other services can access and use these disks as needed, similar to how they would in on-premises scenarios.
- Disk Storage allows data to be persistently stored and accessed from an attached virtual hard disk.
- Disks come in many different sizes and performance levels, from solid-state drives (SSDs) to traditional spinning hard disk drives (HDDs), with varying performance tiers.
- You can use standard SSD and HDD disks for less critical workloads, premium SSD disks for mission-critical production applications, and ultra disks for data-intensive workloads



Azure Blob storage fundamentals



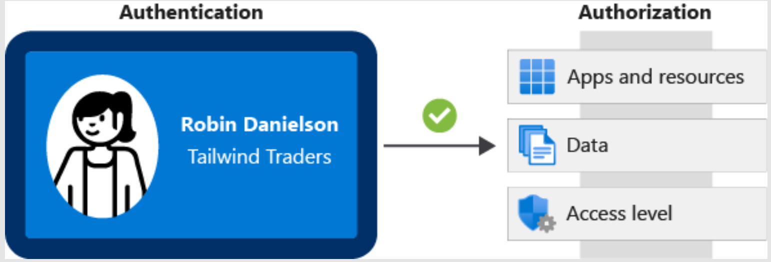
- Azure Blob Storage is an object storage solution for the cloud. It can store massive amounts of data, such as text or binary data. Azure Blob Storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold. Blob Storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.
- Blobs aren't limited to common file formats. A blob could contain gigabytes of binary data streamed from a scientific instrument, an encrypted message for another application, or data in a custom format for an app you're developing. One advantage of blob storage over disk storage is that it does not require developers to think about or manage disks; data is uploaded as blobs, and Azure takes care of the physical storage needs.
- Blob Storage is ideal for:
  Serving images or documents directly to a browser.
  - Storing files for distributed access.
  - Streaming video and audio.
  - Storing data for backup and restore, disaster recovery, and archiving.
  - Storing data for analysis by an on-premises or Azure-hosted service.
  - Storing up to 8 TB of data for virtual machines.
  - You store blobs in containers, which helps you organize your blobs depending on your business needs.
  - The following diagram illustrates how you might use Azure accounts, containers, and blobs.

Understand Blob access tiers

- Data stored in the cloud can grow at an exponential pace. To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency of access and planned retention period.
- Azure Storage offers different access tiers for your blob storage, helping you store object data in the most cost-effective manner. The available access tiers include:
  - **Hot access tier**: Optimized for storing data that is accessed frequently
  - **Cool access tier**: Optimized for data that is infrequently accessed and stored for at least 30 days
  - **Archive access tier**: Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

Secure access to your applications by using Azure identity services

Compare authentication and authorization



- **What is authentication?**
- Authentication is the process of establishing the identity of a person or service that wants to access a resource. It involves the act of challenging a party for legitimate credentials and provides the basis for creating a security principal for identity and access control. It establishes whether the user is who they say they are.
- **What is authorization?**
- Authentication establishes the user's identity, but authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.
- **How are authentication and authorization related?**
- Here's a diagram that shows the relationship between authentication and authorization:

What is Azure Active Directory?

- Active Directory is related to Azure AD, but they have some key differences.
- Microsoft introduced Active Directory in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems by using a single identity per user.
- For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your own organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Azure AD will be familiar to you.
- When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

What services does Azure AD provide?

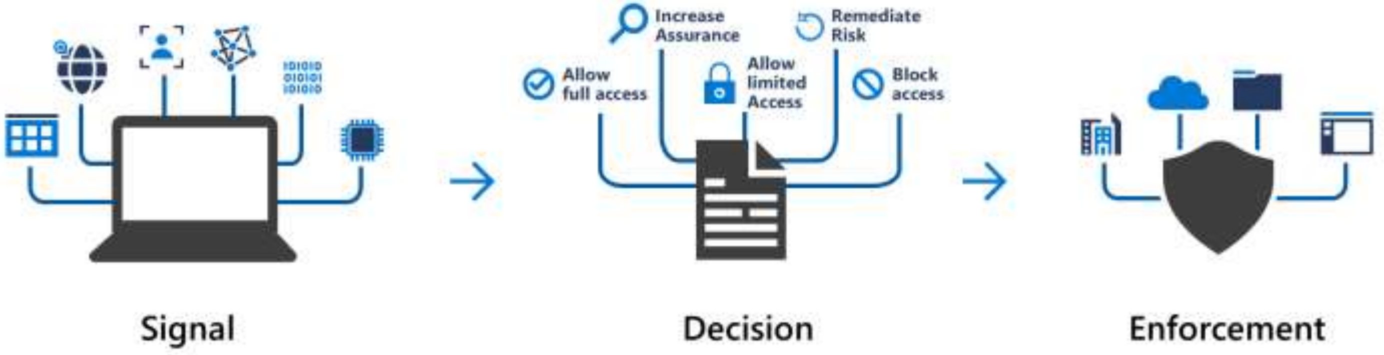
- Azure AD provides services such as:
- **Authentication**
- This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on**
- SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- **Application management**
- You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also called the *access panel*), and single sign-on provide a better user experience.
- **Device management**
- Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

What's Azure AD Multi-Factor Authentication?

- Azure AD Multi-Factor Authentication is a Microsoft service that provides multifactor authentication capabilities. Azure AD Multi-Factor Authentication enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.
- These services provide Azure AD Multi-Factor Authentication capabilities:
- **Azure Active Directory**
- The Azure Active Directory free edition enables Azure AD Multi-Factor Authentication for administrators with the *global admin* level of access, via the Microsoft Authenticator app, phone call, or SMS code. You can also enforce Azure AD Multi-Factor Authentication for all users via the Microsoft Authenticator app only, by enabling *security defaults* in your Azure AD tenant.
- Azure Active Directory Premium (P1 or P2 licenses) allows for comprehensive and granular configuration of Azure AD Multi-Factor Authentication through Conditional Access policies (explained shortly).
- **Multifactor authentication for Office 365**
- A subset of Azure AD Multi-Factor Authentication capabilities is part of your Office 365 subscription.

What's Conditional Access?

- Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity *signals*. These signals include who the user is, where the user is, and what device the user is requesting access from.
- Conditional Access helps IT administrators:
- Empower users to be productive wherever and whenever.
- Protect the organization's assets.
- Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.
- During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.



Azure Information Protection (AIP)

- Azure Information Protection is a cloud-based solution that helps organizations classify and (optionally) protect its documents and emails by applying labels. Labels can be applied automatically (by administrators who define rules and conditions), manually (by users), or with a combination of both (where users are guided by recommendations).

Usage scenario

- When a user saves a Microsoft Word document containing a credit card number, a custom tooltip is displayed. The tooltip recommends labeling the file as *Confidential/ All Employees*, which is a label that the administrator has configured. This label classifies the document and protects it.
- After your content is classified (and optionally protected), you can then track and control how the content is used. For example, you can analyze data flows to gain insight into your business; detect risky behaviors and take corrective measures; track access to documents; and prevent data leakage or misuse.

Azure Advanced Threat Protection (ATP)

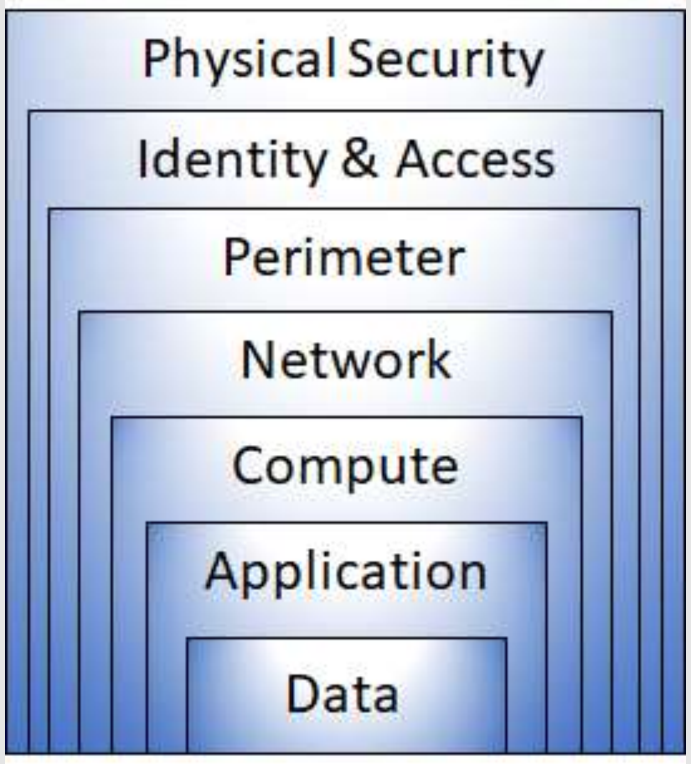
- Cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Azure ATP is capable of detecting known malicious attacks and techniques, security issues, and risks against your network.

Azure Advanced Threat Protection components

- **Azure Advanced Threat Protection (ATP) portal**. Azure ATP has its own portal, through which you can monitor and respond to suspicious activity. The Azure ATP portal allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors. You can also use the portal to monitor, manage, and investigate threats in your network environment.
- **Azure Advanced Threat Protection (ATP) sensor**. Azure ATP sensors are installed directly on your domain controllers. The sensor monitors domain controller traffic without requiring a dedicated server or configuring port mirroring.
- **Azure Advanced Threat Protection (ATP) cloud service**. Azure ATP cloud service runs on Azure infrastructure and is currently deployed in the United States, Europe, and Asia. Azure ATP cloud service is connected to Microsoft's intelligent security graph.

Secure network connectivity on Azure

What is defense in depth?



- The objective of *defense in depth* is to protect information and prevent it from being stolen by those who aren't authorized to access it.
- A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.
- **Layers of defense in depth**
- You can visualize defense in depth as a set of layers, with the data to be secured at the center.
- Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert telemetry that security teams can act upon, either automatically or manually.

Layers of defense in depth

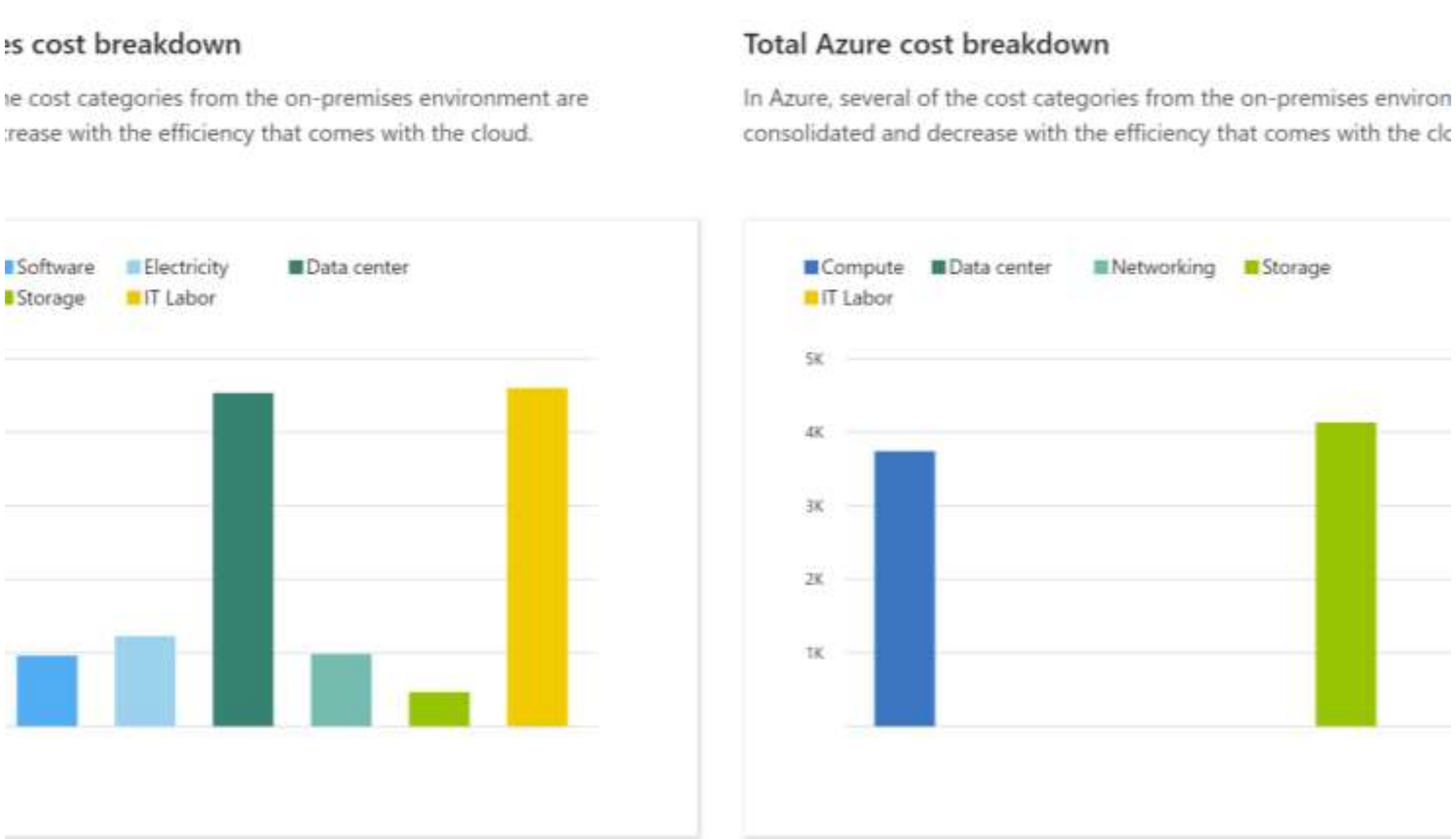
- **Physical security:** Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense. With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately. Microsoft uses various physical security mechanisms in its cloud datacenters.
- **Identity and access**: At this layer, it's important to: Control access to infrastructure and change control. Use single sign-on (SSO) and multifactor authentication. Audit events and changes. The identity and access layer is all about ensuring that identities are secure, access is granted only to what's needed, and sign-in events and changes are logged
- **Perimeter:** At this layer, it's important to: Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users. Use perimeter firewalls to identify and alert on malicious attacks against your network. At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.
- **Network:** At this layer, it's important to: Limit communication between resources. Deny by default. Restrict inbound internet access and limit outbound access where appropriate. Implement secure connectivity to on-premises networks. At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.
- **Compute:** At this layer, it's important to: Secure access to virtual machines. Implement endpoint protection on devices and keep systems patched and current. Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.
- **Application:** At this layer, it's important to: Ensure that applications are secure and free of vulnerabilities. Store sensitive application secrets in a secure storage medium. Make security a design requirement for all application development. Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.
- **Data:** In almost all cases, attackers are after data: Stored in a database. Stored on disk inside virtual machines. Stored in software as a service (SaaS) applications, such as Office 365. Managed through cloud storage.

Part 3: Azure management and governance

What factors affect cost?

- **Resource type:** A number of factors influence the cost of Azure resources. They depend on the type of resource or how you customize it. For example, with a storage account you specify a type (such as block blob storage or table storage), a performance tier (standard or premium), and an access tier (hot, cool, or archive). These selections present different costs.
- **Usage meters:** When you provision a resource, Azure creates *meters* to track usage of that resource. Azure uses these meters to generate a usage record that's later used to help calculate your bill.
- **Resource usage:** In Azure, you're always charged based on what you use. As an example, let's look at how this billing applies to deallocating a VM. In Azure, you can delete or deallocate a VM. Deleting a VM means that you no longer need it. The VM is removed from your subscription, and then it's prepared for another customer. Deallocating a VM means that the VM is no longer running.
- **Azure subscription types:** Some Azure subscription types also include usage allowances, which affect costs. For example, an Azure free trial subscription provides access to a number of Azure products that are free for 12 months. It also includes credit to spend within your first 30 days of sign-up. And you get access to more than 25 products that are always free (based on resource and region availability).
- **Azure Marketplace:** You can also purchase Azure-based solutions and services from third-party vendors through Azure Marketplace. Examples include managed network firewall appliances or connectors to third-party backup services. Billing structures are set by the vendor.

Compare costs by using the Total Cost of Ownership Calculator



es cost breakdown

e cost categories from the on-premises environment are
rease with the efficiency that comes with the cloud.

Total Azure cost breakdown

In Azure, several of the cost categories from the on-premises environ
consolidated and decrease with the efficiency that comes with the clc

- The TCO Calculator helps you estimate the cost savings of operating your solution on Azure over time, instead of in your on-premises datacenter.
- The term *total cost of ownership* is commonly used in finance. It can be hard to see all the hidden costs related to operating a technology capability on-premises. Software licenses and hardware are additional costs.
- With the TCO Calculator, you enter the details of your on-premises workloads. Then you review the suggested industry average cost (which you can adjust) for related operational costs. These costs include electricity, network maintenance, and IT labor. You're then presented with a side-by-side report. Using the report, you can compare those costs with the same workloads running on Azure.
- The following image shows one example.

Pricing Calculator

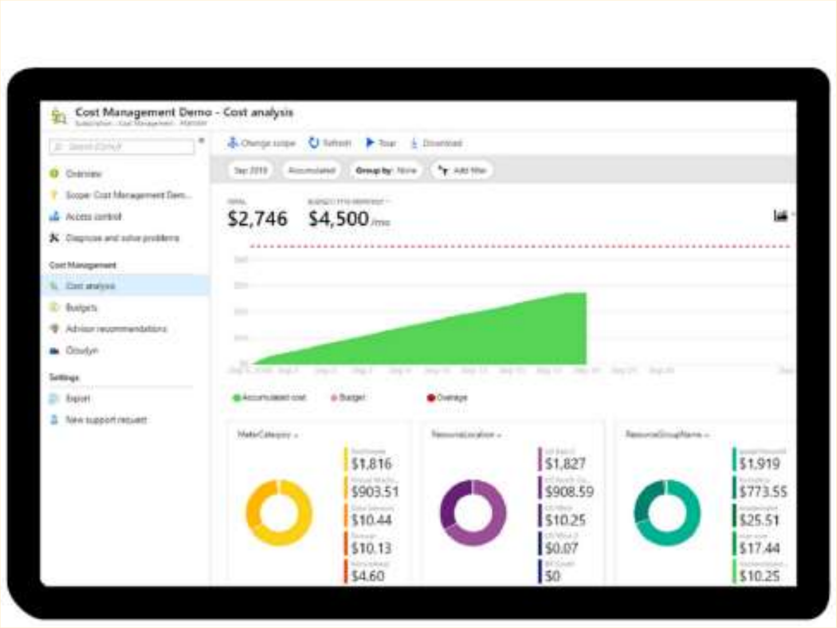
- The Pricing Calculator is a tool that helps you estimate the cost of Azure products. It displays Azure products in categories, and you choose the Azure products you need and configure them according to your specific requirements. Azure then provides a detailed estimate of the costs associated with your selections and configurations.
- Get a new estimate from the Pricing Calculator by adding, removing, or reconfiguring your selected products. You also can access pricing details, product details, and documentation for each product from the Pricing Calculator.
- The options that you can configure in the Pricing Calculator vary between products, but basic configuration options include:
  - **Region**. Lists the regions from which you can provision a product. Southeast Asia, central Canada, the western United States, and Northern Europe are among the possible regions available for some resources.
  - **Tier**. Sets the type of tier you wish to allocate to a selected resource, such as Free Tier, Basic Tier,
  - **Billing Options**. Highlights the billing options available to different types of customer and subscriptions for a chosen product.
  - **Support Options**: Allows you to pick from included or paid support pricing options for a product.
  - **Programs and Offers**. Allows you to choose from available price offerings according to your customer or subscription type.
  - **Azure Dev/Test Pricing**. Lists the available development and test prices for a product. Dev/Test pricing applies only when you run resources within an Azure subscription that is based on a Dev/Test offer.

Azure Cost Management

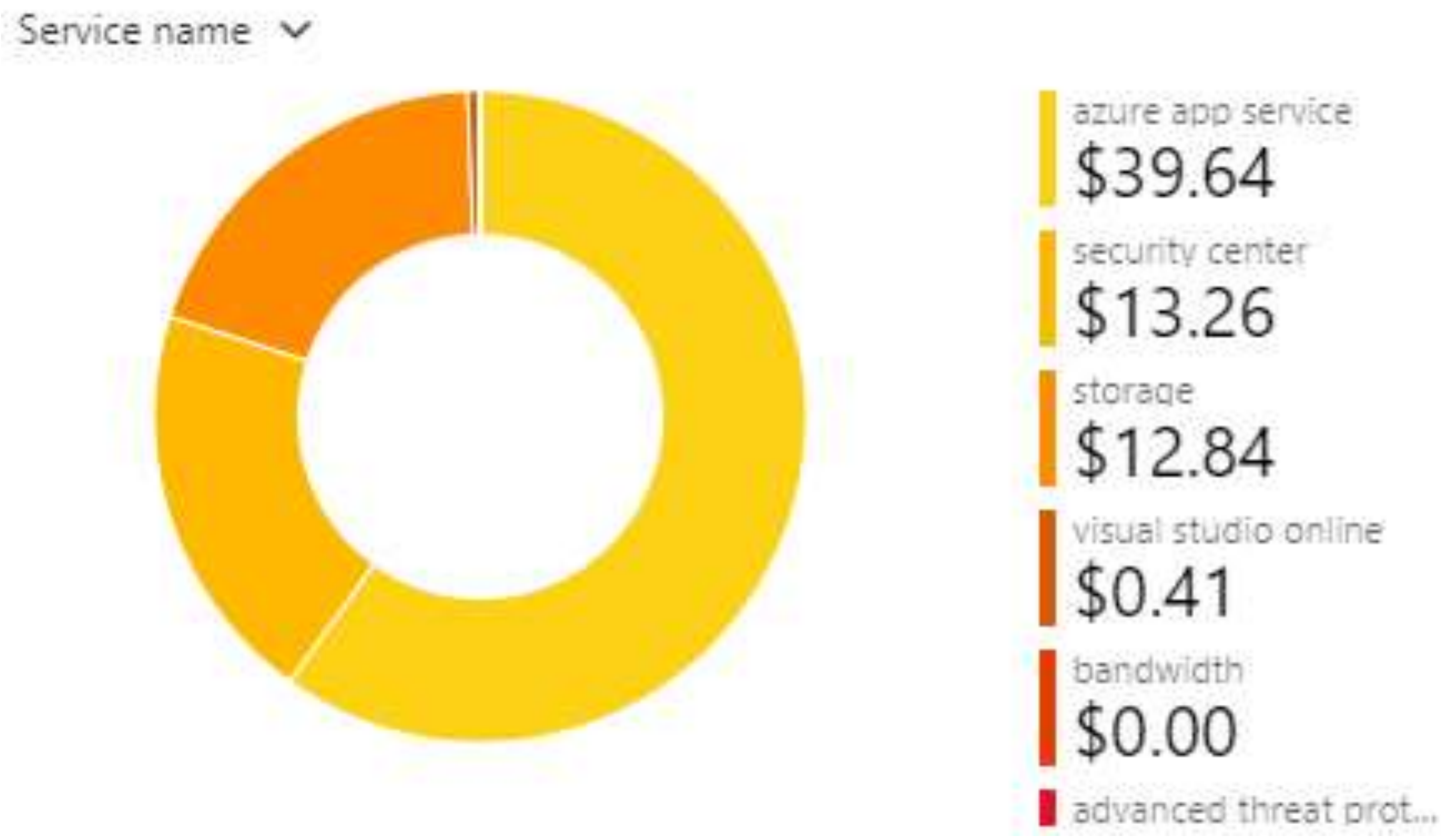
- Cost Management is an Azure product that provides a set of tools for monitoring, allocating, and optimizing your Azure costs.

The main features of the Azure Cost Management toolset include:

- Reporting. Generate reports using historical data to forecast future usage and expenditure.
- Data enrichment. Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.
- Budgets. Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.
- Alerting. Get alerts based on your cost and usage budgets.
- Recommendations. Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.
- Price. Free to Azure customers



Use Azure Cost Management + Billing to control spending



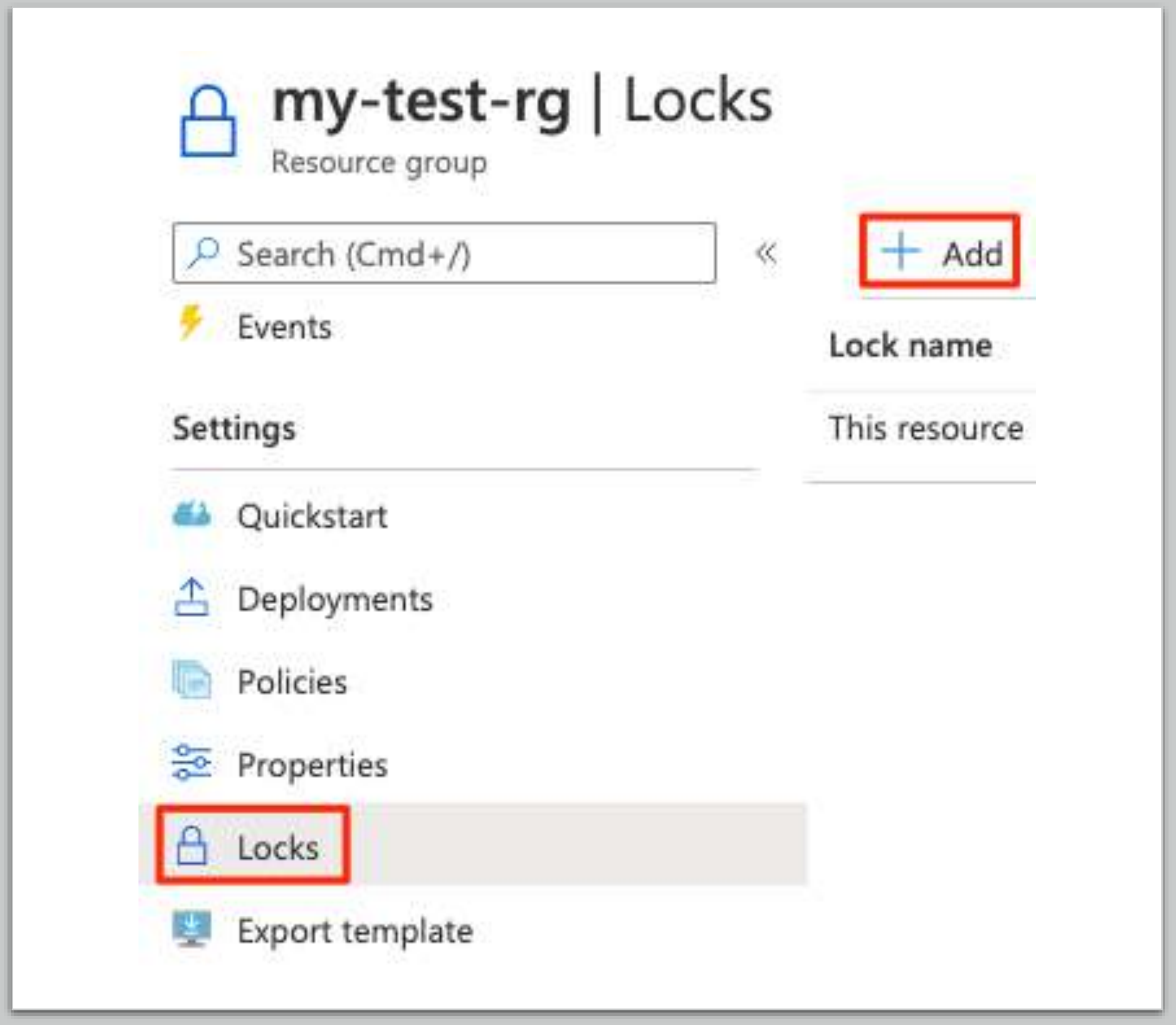
- Azure Cost Management + Billing is a free service that helps you understand your Azure bill, manage your account and subscriptions, monitor and control Azure spending, and optimize resource use.
- The following image shows current usage broken down by service:

Organize your Azure resources by using tags

- As your cloud usage grows, it's increasingly important to stay organized. A good organization strategy helps you understand your cloud usage and can help you manage costs.
- One way to organize related resources is to place them in their own subscriptions. You can also use resource groups to manage related resources. Resource *tags* are another way to organize resources. Tags provide extra information, or metadata, about your resources.
- This metadata is useful for:
  - **Resource management**
  - **Cost management and optimization**
  - **Operations management**
  - **Security**
  - **Governance and regulatory compliance**
  - **Workload optimization and automation**

Prevent accidental changes by using resource locks

- You can manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template.
- To view, add, or delete locks in the Azure portal, go to the **Settings** section of any resource's **Settings** pane in the Azure portal.
- Here's an example that shows how to add a resource lock from the Azure portal. You'll apply a similar resource lock in the next part.



What levels of locking are available?

- You can apply locks to a subscription, a resource group, or an individual resource. You can set the lock level to **CanNotDelete** or **ReadOnly**.
- **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.

How do I delete or change a locked resource?

- Although locking helps prevent accidental changes, you can still make changes by following a two-step process.
- To modify a locked resource, you must first remove the lock. After you remove the lock, you can apply any action you have permissions to perform. This additional step allows the action to be taken, but it helps protect your administrators from doing something they might not have intended to do.
- Resource locks apply regardless of RBAC permissions. Even if you're an owner of the resource, you must still remove the lock before you can perform the blocked activity.

Combine resource locks with Azure Blueprints

- What if a cloud administrator accidentally deletes a resource lock? If the resource lock is removed, its associated resources can be changed or deleted.
- To make the protection process more robust, you can combine resource locks with Azure Blueprints.
- Azure Blueprints enables you to define the set of standard Azure resources that your organization requires. For example, you can define a blueprint that specifies that a certain resource lock must exist. Azure Blueprints can automatically replace the resource lock if that lock is removed.

Choose the best tools for managing and configuring your Azure environment

What is Azure Marketplace?

- Helps connect users with Microsoft partners, independent software vendors, and startups that are offering their solutions and services, which are optimized to run on Azure.
- Azure Marketplace customers can find, try, purchase, and provision applications and services from hundreds of leading service providers.
- All solutions and services are certified to run on Azure. Solution catalog spans several industry categories such as open-source container platforms, virtual machine images, databases, application build and deployment software, developer tools, threat detection, and blockchain.
- You can provision end-to-end solutions quickly and reliably, hosted in your own Azure environment. At the time of writing, there are more than 8,000 listings.

What is the Azure portal?

- Web-based, unified console that provides an alternative to command-line tools.
- You can manage your Azure subscription by using a graphical user interface.
  - Build, manage, and monitor everything from simple web apps to complex cloud deployments
  - Create custom dashboards for an organized view of resources.
  - Configure accessibility options for an optimal experience.
- Azure portal is designed for resiliency and continuous availability.
- The Azure portal updates continuously and requires no downtime for maintenance activities.

The Azure mobile app

- The Azure mobile app provides iOS and Android access to your Azure resources when you're away from your computer. With it, you can:
  - Monitor the health and status of your Azure resources.
  - Check for alerts, quickly diagnose and fix issues, and restart a web app or virtual machine (VM).
  - Run the Azure CLI or Azure PowerShell commands to manage your Azure resources.

Azure PowerShell

- Azure PowerShell is a shell with which developers can execute commands called cmdlets (pronounced *command-lets*).
- These commands call the Azure Rest API to perform every possible management task in Azure.
- Cmdlets can be executed independently or combined into a script file and executed together to orchestrate:
  - The routine setup, teardown, and maintenance of a single resource or multiple connected resources.
  - The deployment of an entire infrastructure, which might contain dozens or hundreds of resources, from imperative code.
  - Capturing the commands in a script makes the process repeatable and automatable.
  - Azure PowerShell is available for Windows, Linux, and Mac, and you can access it in a web browser via Azure Cloud Shell.
  - Windows PowerShell has helped Windows-centric IT organizations automate many of their on-premises operations for years, and these organizations have built up a large catalog of custom scripts and cmdlets, as well as expertise.

The Azure CLI

- The Azure CLI command-line interface is an executable program with which a developer can execute commands in Bash.
- Commands call the Azure Rest API to perform every possible management task in Azure.
- You can run the commands independently or combined into a script and executed together for the routine setup, teardown, and maintenance of a single resource or an entire environment.
- In many respects, the Azure CLI is almost identical to Azure PowerShell in what you can do with it. Both run on Windows, Linux, and Mac, and can be accessed in a web browser via Cloud Shell. The primary difference is the syntax you use. If you're already proficient in PowerShell or Bash, you can use the tool you prefer.

Choose the best monitoring service for visibility, insight, and outage mitigation

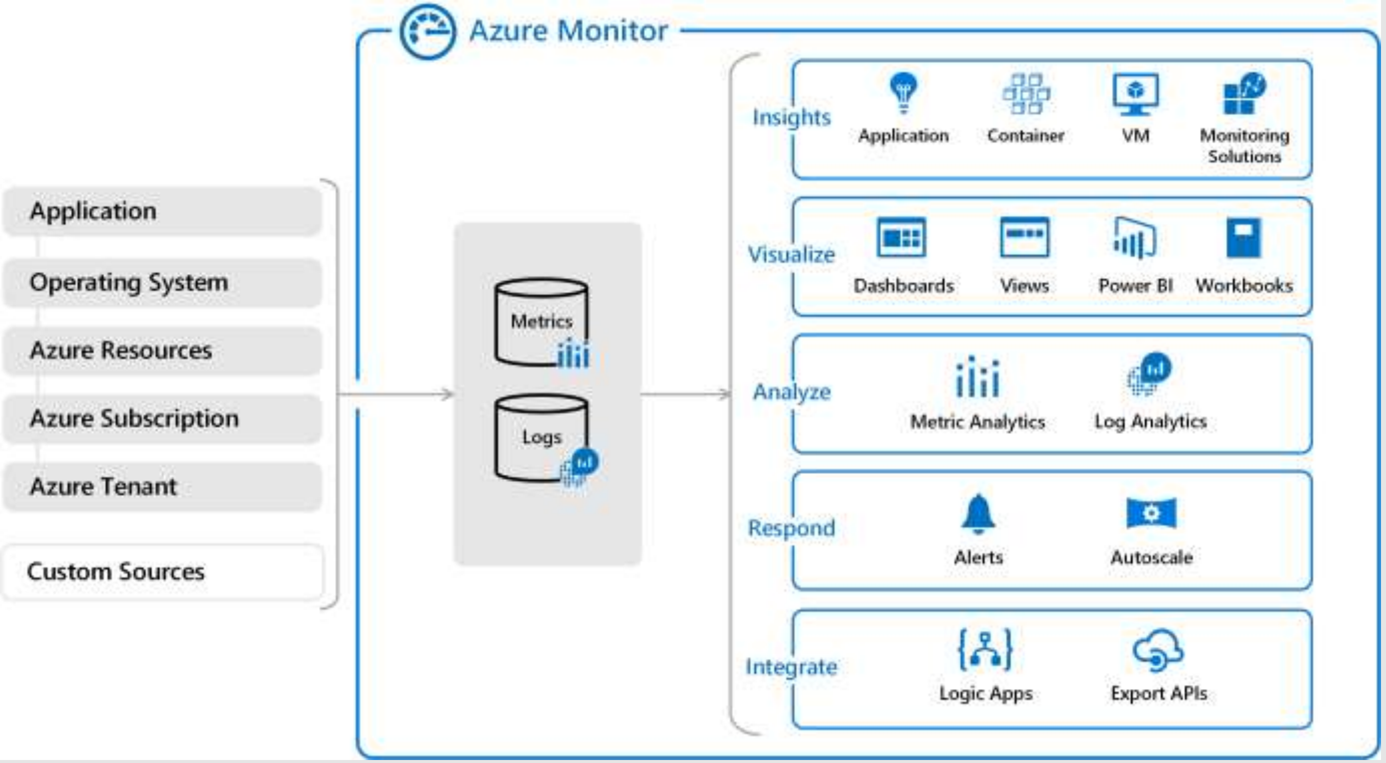
Azure Advisor

- Azure Advisor evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Advisor is designed to help you save time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

The recommendations are divided into five categories:

- **Reliability**: Used to ensure and improve the continuity of your business-critical applications.
- **Security**: Used to detect threats and vulnerabilities that might lead to security breaches.
- **Performance**: Used to improve the speed of your applications.
- **Cost**: Used to optimize and reduce your overall Azure spending.
- **Operational Excellence**: Used to help you achieve process and workflow efficiency, resource manageability, and deployment best practices.

Azure Monitor



Azure Monitor is a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment.

Azure Service Health

- Azure Service Health provides a personalized view of the health of the Azure services, regions, and resources you rely on.
- The status.azure.com website, which displays only major issues that broadly affect Azure customers, doesn't provide the full picture. But Azure Service Health displays both major and smaller, localized issues that affect you. Service issues are rare, but it's important to be prepared for the unexpected. You can set up alerts that help you triage outages and planned maintenance. After an outage, Service Health provides official incident reports, called root cause analyses (RCAs), which you can share with stakeholders.

Service Health helps you keep an eye on several event types:

- **Service issues** are problems in Azure, such as outages, that affect you right now. You can drill down to the affected services, regions, updates from your engineering teams, and find ways to share and track the latest information.
- **Planned maintenance** events can affect your availability. You can drill down to the affected services, regions, and details to show how an event will affect you and what you need to do. Most of these events occur without any impact to you and aren't shown here. In the rare case that a reboot is required, Service Health allows you to choose when to perform the maintenance to minimize the downtime.
- **Health advisories** are issues that require you to act to avoid service interruption, including service retirements and breaking changes. Health advisories are announced far in advance to allow you to plan.

Thank You