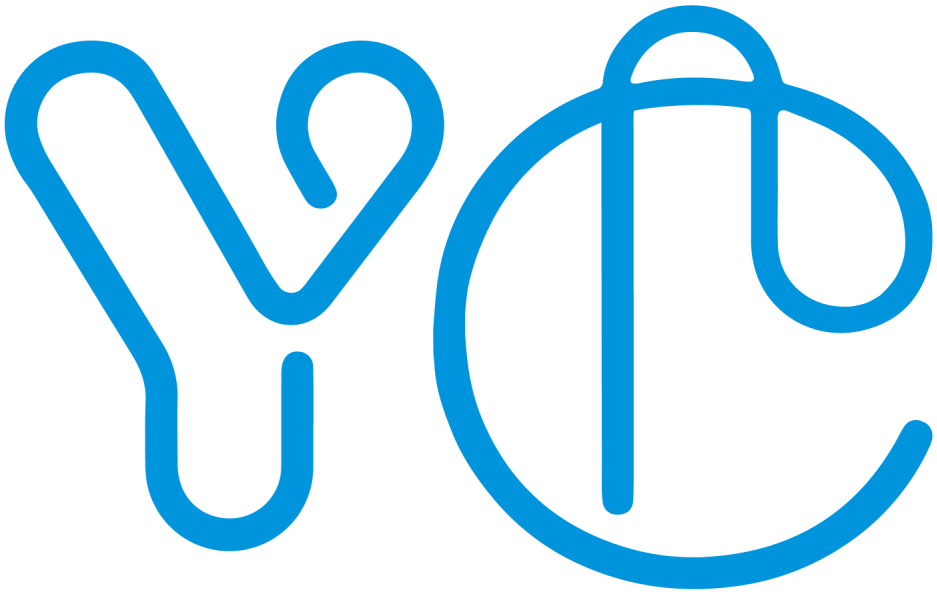
Prepare

AZ-900

Azure Fundamentals

Yatharth Chauhan

WELCOME TO MY WORLD



yatharthchauhan.me

CONNECT WITH ME

WELCOME TO PREPARE MICROSOFT AZURE FUNDAMENTALS (AZ-900)

AUTHOR: Yatharth Chauhan (Github: YatharthChauhan2362)
Exam: Microsoft Azure Fundamentals (AZ-900)

Microsoft Certified: Azure Fundamentals (AZ-900) - Yatharth Chauhan

Microsoft Learn: Microsoft Azure Fundamentals

Table of Contents

↑

AZ-900: Microsoft Azure Fundamentals

Cloud Basics

What's cloud

- Delivery of computing services over the Internet using a pay-as-you-go pricing model.
  - in other words: a way to rent compute power and storage from someone else's data center.
- **Pay-as-you-go**: You're billed only for what you use.
  - Instead of maintaining CPUs and storage in your data center, you rent them for the time that you need them
    - The cloud provider takes care of maintaining the underlying infrastructure for you.
  - **On-demand access**:
    - You can treat cloud resources like you would your resources in your own data center. When you're done using them, you give them back
- The real value of the cloud: speed
  - Enables you to quickly solve your business challenges and bring cutting edge solutions to your users.
  - In less time than it takes to eat lunch, you can create & deploy a website on Azure
- A foundational building block of everything from digital transformation to the next big startup.

Why move to the cloud

- Move faster and innovate in ways that were once nearly impossible
- Two-trends in world:
  - Teams are delivering new features to their users at record speeds.
    - Software releases were once scheduled in terms of months or even years.
      - Today, teams are releasing features in smaller batches
        - Allows to schedule multiple releases a day
  - End users expect an increasingly rich and immersive experience with their devices and with software.
    - Many ways to interact with devices
      - E.g. they can recognize your face & voice commands
      - E.g. mobile phones, PCs, tablets, VR headsets, webpages...
  - The cloud provides on-demand access to:
    - A nearly limitless pool of raw compute, storage, and networking components.
    - Speech recognition and other cognitive services that help make your application stand out from the crowd.
    - Analytics services that enable you to make sense of telemetry data coming back from your software and devices.
- While migrating your existing apps to virtual machines is a good start, the cloud is more than just "a different place to run your virtual machines".
  - It can provide AI and machine-learning, storage (that grows with your needs) and more.

Benefits of Cloud Computing

- Not an all-or-nothing service
  - You can gradually move to cloud, called also ***lift and shift***
- You're able to spend more time on what matters and less time managing the underlying details.

Cost effective

- Provides **pay-as-you-go** or **consumption-based** pricing model.
  - No upfront infrastructure costs
  - No need to purchase and manage costly infrastructure/hardware that you may not use to its fullest
  - The ability to pay for additional resources only when they are needed
  - The ability to stop paying for resources that are no longer needed
- Enables better cost predictions using pricing of individual resources/services.
  - You can analyze future growth using historical data.

Scalable

- Increase or decrease the resources and services used based on the demand or workload at any given time
- Cloud computing supports both:
  - **Horizontal scaling**
    - Scaling "out"
    - Adding more servers that function together as one unit
  - **Vertical scaling**
    - Scaling "up"
    - Adding resources to increase the power of an existing server
      - e.g.Add more CPUs, or add more memory
- Scaling can be done manually or automatically based on e.g.
  - specific triggers such as CPU utilization

Elastic

- Cloud computing system can automatically add & remove resources to meet the current demand.
- E.g.
  - Add resources for the peak operating hours during which most people access the application
    - Only pay for increased resources during those hours
  - Remove the resources when the traffic normalizes
    - Do not pay anymore

Current

- Eliminates the burdens of maintaining software patches, hardware setup, upgrades, and other IT management tasks
  - automatically done
- The computer hardware is maintained and upgraded by the cloud provider
  - e.g. if a disk fails it'll be replaced by the cloud provider

Reliable

- Cloud provider offers data backup, disaster recovery, and data replication services
- Redundancy is often built into cloud services architecture
  - so if one component fails, a backup component takes its place
  - this is referred to as **fault tolerance** and it ensures that your customers aren't impacted when a disaster occurs.

Global

- Fully redundant datacenters located in various regions all over the globe.
- Enables local presence close to your customers to give them the best response time
- Replicate your services into multiple regions for redundancy and locality
- Select a specific region to ensure you meet data-residency and compliance laws for your customers.

Secure

- You have:
  - **Physical security**
    - Who can access the building, who can operate the server racks, and so on
    - Walls, cameras, gates, security personnel, employees have access only to those resources that they've been authorized to manage.
  - **Digital security**
    - Who can connect to your systems and data over the network.
    - E.g. only authorized users to be able to log into virtual machines or storage systems running in the cloud
    - Have tools to mitigate security threats that you can use.
- Broad set of policies, technologies, controls, and expert technical skills
  - can provide better security than most organizations can otherwise achieve

Cloud Deployment Models

- Defines
  - where your data is stored
  - how your customers interact with it – how do they get to it
  - where do the applications run?
- Choose depending on your budget, and on your security, scalability, and maintenance needs.
  - E.g. how much of your own infrastructure you want or need to manage.

Public cloud

- Most common deployment model
- No local hardware to manage or keep up-to-date, everything runs on your cloud provider's hardware.
- Save additional costs by sharing computing resources with other cloud users.
- Can use multiple public cloud providers of varying scale.
- **Example use case**
  - Deploy a blog / web application quickly wihout worrying about purchasing, managing or maintaining the hardware on which it runs.

Advantages of public cloud

- High scalability/agility: you don't have to buy a new server in order to scale
- Pay-as-you-go pricing: you pay only for what you use, no CapEx costs
- You're not responsible for maintenance or updates of the hardware

- Minimal technical knowledge to set up and use: you can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available

Disadvantages of public cloud

- Specific security requirements that cannot be met by using public cloud
- Government policies, industry standards, or legal requirements which public clouds cannot meet
- You don't own the hardware or services and cannot manage them as you may want to
- Unique business requirements, such as having to maintain a legacy application might be hard to meet

Private cloud

- Cloud environment in your own datacenter
- Provide self-service access to compute resources to users in your organization.
- A simulation of a public cloud to users, but you remain completely responsible for the purchase and maintenance of the hardware and software services you provide.
- Users can be external customer or specific internal departments such as Accounting or Human Resources.
- **Example use case**
    - Have data that cannot be put in the public cloud e.g. because a government policy requires specific data to be kept in-country or privately.

Advantages of private cloud

- Ensure the configuration can support any scenario or legacy application
- Control (and responsibility) over security
- Meet strict security, compliance, or legal requirements

Disadvantages of private cloud

- Initial CapEx costs & must purchase the hardware for startup and maintenance
- Owning the equipment limits the agility - to scale you must buy, install, and setup new hardware
    - Private clouds require IT skills and expertise that's hard to come by

Hybrid cloud

- Combines public and private clouds, allowing you to run your applications in the most appropriate location.
- Helpful when you have some things that cannot be put in the cloud, maybe for legal reasons.
- **Example use cases**
    - Host a website in the public cloud and link it to a highly secure database hosted in your private cloud (or on-premises datacenter).
    - Some specific pieces of data that cannot be exposed publicly (such as medical data) which needs to be held in your private datacenter.
    - An application that run on old hardware that can't be updated. Keep the old system & connect it to the public cloud for authorization or storage.

Advantages of hybrid cloud

- Keep any systems running and accessible that use out-of-date hardware or an out-of-date operating system
- Have flexibility with what you run locally versus in the cloud
    - Easier migration to Azure
    - **Cloud-bursting**: Use cloud when your compute resources are not enough
    - Pass data back and forth: Process part of your data in cloud, part of it on-premises.
- Take advantage of economies of scale from public cloud providers for services and resources where it's cheaper, and then supplement with your own equipment when it's not
- Use your own equipment to meet security, compliance, or legacy scenarios where you need to completely control the environment

Disadvantages of hybrid cloud

- More expensive than selecting one deployment model since it involves some CapEx cost up front
- More complicated to set up and manage

Compute and Serverless and Storage

- Cloud is like ***electricity***
    - only pay for what you need
    - don't worry about how & when power plants upgrade to the latest technology.
    - you don't manage scaling, e.g. many people can move to town and light will stay on
- **Cloud computing**
    - Solves management of hardware and software
    - = Renting resources, like storage space or CPU cycles, on another company's computers
    - **Flexible** and **cost-efficient**,
        - E.g. you only pay for what you use.
- **Cloud Provider**
    - Provides cloud computing services
    - E.g. Microsoft, Amazon, Google
    - Typical services:
        - **Compute power**: such as Linux/Windows servers or web applications
        - **Storage**: such as files and databases and blobs
        - **Networking**: such as secure connections between the cloud provider and your company/datacenter
        - **Analytics**: such as visualizing telemetry and performance data

Compute Power

- Choose how you want work to be done based on your resources and needs.
- **Virtual Machines (VM)**
    - Emulation of a computer, like your desktop / laptop
    - Includes operating system and hardware, you can install any software on it.
    - More control and responsibility over maintenance.
    - Cloud provider runs it for you in one of its datacenters
        - Often sharing that server with other VMs
- **Containers**

    - Consistent, isolated execution environment for application
    - Similar to VM but they don't require guest operating system
        - They can run on different guest systems
            - Highly portable, can run on-premises or in the cloud with often no changes to application.
        - Takes few seconds/lesser time to start up as there's no OS to initialize
    - Application and its dependencies are packaged into a container
    - **Docker**
        - Open source
        - The leading platform for managing containers.

Serverless computing

- Lets you run application code without creating, configuring, or maintaining a server
- Your application is broken into separate functions that runs when triggered by some action/event
- Good for automation e.g. serverless process that automatically sends an email confirmation after a customer makes an online purchase.
- pay for the processing time used by each function as it executes.
    - ❗ On contrast, VMs and containers are running even if the applications on them are idle.

Storage

- Most devices and applications read and/or write data
    - E.g. when leaving a voicemail
- Cloud providers offers different services
    - e.g. for storing a text you can use file on disk.
    - e.g. for relationships in address book, you can use a database
- Advantage of a cloud-based data storage is you can scale to meet your needs.

IaaS vs PaaS vs SaaS

Three categories of cloud computing

- 📝 IaaS, PaaS, SaaS.
- Allows using a combination of these types of infrastructure.
    - E.g. Microsoft 365 Apps on company computers (SaaS), VMs (IaaS) on Azure and Azure SQL Database (PaaS) to store your data.

Infrastructure as a service (IaaS)

- Instant computing infrastructure, provisioned and managed over the internet.
- Aims to give you the most control over the provided hardware that runs your application
- 📝 E.g. virtual machines (VMs), storage, and operating systems.
- You rent hardware instead of buying
- Ensuring that a service is up and running is a shared responsibility (see shared responsibility model
    - cloud provider ensures the cloud infrastructure is functioning correctly
    - cloud customer ensures the service they are using is

    - configured correctly
    - up to date
    - available to their customers.

Common IaaS use cases

- **Migrating workloads**: Managed similar to on-prem infrastructure & provides easy migration path.
- **Test and development**: Teams can quickly set-up & dispose test/dev environments with fast & economical scaling.
- **Storage, backup and recovery**: Organizations avoid the capital outlay and complexity of storage management.
    - Useful for managing unpredictable demand and steadily growing storage needs.
    - can also simplify the planning and management of backup and recovery systems.

Platform as a service (PaaS)

- Provides an environment for building, testing, and deploying software applications
    - Can add features such authentication.
- Aims to help creating an application quickly without managing the underlying infrastructure.
    - 📝 E.g. for a web app / Azure SQL databases you don't need to install an operating system, web server, or even system updates.
- Resources are purchased on a pay-as-you-go basis and accessed over a secure Internet connection.

Common PaaS use cases

Development framework

- Lets developers create applications using built-in software components.
- 📝 Cloud features such as scalability, high-availability, and multi-tenant capability are included
- Reducing the amount of coding that developers must do.

Analytics or business intelligence

- Tools provided as a service with PaaS allow organizations to analyze and mine their data.
- They can find insights and patterns, and predict outcomes to improve business decisions such as forecasting, product design, and investment returns.

Software as a service (SaaS)

- Software that is centrally hosted and managed for the end customer.
- Usually based on an architecture where one version of the application is used for all customers
- Usually licensed through a monthly or annual subscription
- 📝 E.g. Office 365, Skype, and Dynamics CRM Online.

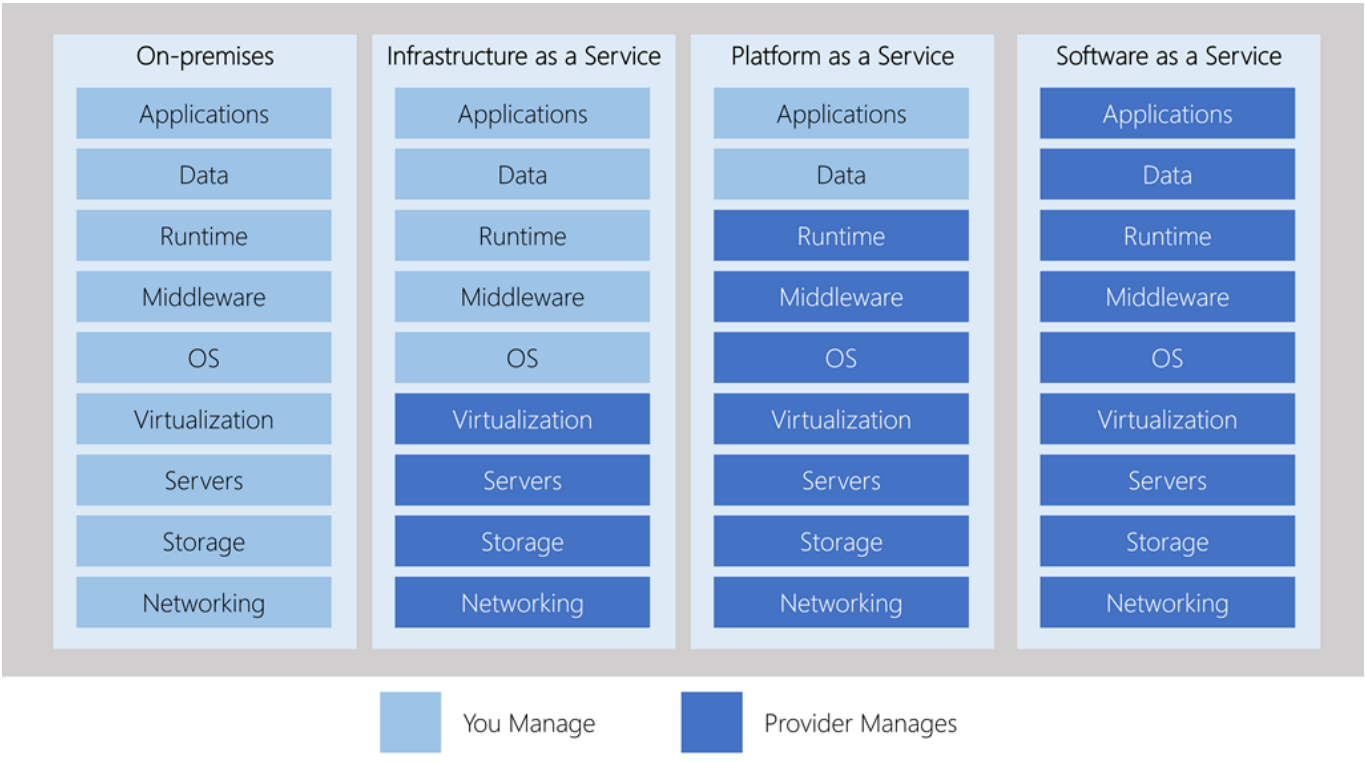
Cost and Ownership

IaaS	PaaS	SaaS

	IaaS	PaaS	SaaS
Upfront costs	None, pay for what you use	None, pay for what you use	None, monthly / annual subscription
User ownership	purchase, installation, configuration, and management of their own software, operating systems, middleware, and applications	development of their own applications	not responsible for any maintenance or management of that software.
Cloud provider ownership	underlying cloud infrastructure (such as virtual machines, storage, and networking) is available for the user.	operating system management, network, and service configuration.. typically everything except user application	provision, management, and maintenance of the application software

Management responsibilities

- These categories are layers on top of each other
  - Abstraction order: SaaS > PaaS > IaaS
  - Abstraction = Hide details, quicker production but less control over the underlying hardware.
- IaaS: user is responsible for managing the operating systems, data, and applications.
- PaaS: user is responsible for the applications and data they run and store.
- SaaS: user just uses the software.



Cloud Compliance

- Provider can help you comply with regulations and standards
- Think about:
    - How compliant is the cloud provider when it comes to handling sensitive data?
    - How compliant are the services offered by the cloud provider?
    - How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?
    - What terms are part of the privacy statement for the provider?

Some compliance offerings

CJIS

- CJIS = Criminal Justice Information Services
- Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy
- Microsoft Azure adheres to the same requirements that law enforcement and public safety entities must meet.

CSA STAR Certification

- CSA = Cloud Security Alliance
- Independent third-party assessment of a cloud provider's security posture
- Ensures:
    - ISO/IEC 27001 certificationis achieved
    - Criteria specified in the Cloud Controls Matrix (CCM) are met
        - Also assesed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

GDPR

- GDPR = General Data Protection Regulation, european privacy law
- Imposes rules for collecting & analyzing data tied to EU residents.
- The GDPR applies no matter where you are located.

EU Model Clauses

- EU Standard Contractual Clauses
- Guarantees around transfers of personal data outside of the EU.
- Ensures customers can use cloud service to move data freely through cloud from Europe to the rest of the world.

HIPAA

- HIPAA = Health Insurance Portability and Accountability Act
- US federal law that regulates patient Protected Health Information (PHI)
- HIPAA Business Associate Agreement (BAA)
    - Adheres o certain security and privacy provisions in HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act.
- Azure offers BAA as contract addendum to assist customers individual compliance.

ISO/IEC 27018

- ISO/IEC 27018 = International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27018
- Covers the processing of personal information by cloud service providers

MTCS Singapore

- MTCS = Multi-Tier Cloud Security (MTCS) Singapore
- MTCS 584:2013 asses for IaaS & PaaS & SaaS service classifications.

SOC 1, 2, and 3

- SOC = Service Organization Controls
- Cloud services audited at least annually against the SOC report framework by independent third-party auditors.
- Audit covers controls for data security, availability, processing integrity, and confidentiality
    - as applicable to in-scope trust principles for each service.

NIST CSF

- NIST CSF = National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
    - NIST is agency of United States Department of Commerce.
- Voluntary framework that defines security guidelines, and best practices to manage cybersecurity-related risks.
- Azure have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits & is certified
    - Also validated by the Health Information Trust Alliance (HITRUST)
        - a leading security and privacy standards development and accreditation organization

UK Government G-Cloud

- Cloud computing certification for services used by government entities in UK.
- Azure has received official accreditation from the UK Government Pan Government Accreditor.

Scaling

- Suppose you deployed your website and it becomes popular. You realize that your site can't effectively manage all the requests it's receiving. To solve the problem, you'll need to increase the server's hardware capacity.
- Scale refers to adding network bandwidth, memory, storage, or compute power to achieve better performance.
- **Dynamic scalability architecture** is an architectural model based on a system of predefined scaling conditions that trigger the dynamic allocation of IT resources from resource pools

Scaling up /down or vertical scaling

- Increase (up) or decrease (down) the memory, storage, or compute power on an existing virtual machine.
- E.g. add additional memory to a web or database server to make it run faster.

Scaling out/in or horizontal scaling

- Add (out) or remove (in) virtual machines to power your application.
- E.g., create many virtual machines configured in exactly the same way and use a load balancer to distribute work across them.

Scale down or scale in

- Do if you needed to scale up or scale out only temporarily.
- Help you save money.
- Services that help you optimize cloud spend:
    - Azure Advisor, Azure Cost Management
    - You can use these to identify where you're using more than you need
        - and then scale back to the capacity you're actually using.
    - See also Cloud Economics - Cost Optimization Best Practices

Azure Basics

- Azure is Microsoft's private & public cloud computing platform
- Provides developers & IT admins tools to provide, build, manage, and deploy applications.
    - on a massive global network
    - freedom to choose tools and frameworks
- More than 90% of Fortune 500 companies run on the Microsoft Cloud [source]

Azure services

- More than 100 services..
- **Compute services** such as VMs and containers that can run your applications
- **Database services** that provide both relational and NoSQL choices
- **Identity services** that help you authenticate and protect your users
- **Networking services** that connect your datacenter to the cloud, provide high availability or host your DNS domain
- **Storage solutions** that can accommodate massive amounts of both structured and unstructured data
- **AI and machine-learning** services can analyze data, text, images, comprehend speech, and make predictions using data
- See also list of Azure services

How Azure works

- It uses virtualization
    - Uses an abstraction layer called **hypervisor**.
        - Separates tight coupling between hardware (CPU, RAM, GPU..) and its operating system
        - Emulates a real computer in a **virtual machine**

        - Can run multiple virtual machines in same time
        - Optimizes capacity of abstracted hardware
        - Can run any OS such as Windows, Linux & macOS
- Azure repeats virtualization in massive scale
    - Each data center has many racks filled with servers
    - Each server includes a hypervisor to run multiple virtual machines.
    - A network switch provides connectivity to all those servers
    - One server in each rack runs a special software called **fabric controller**
        - Each fabric controller is connected to another software called as **orchestrator**
            - Orchastrator manages everything in Azure, including responding user requests
                - Users requests using **Azure API**
                    - Azure API can be reached in many ways including Azure Portal
                - Orchestrator packages everything it's needed and sends to package & request to fabric controller.

Purchasing and Licensing Options

Azure purchasing options

1. From Microsoft by signing up through Azure website Azure.com
    - Monthly billing
2. From Microsoft through a Microsoft representative
    - Monthly billing
3. From a Microsoft partner
    - CSP = **Cloud Solution Provider**
        - Offer a range of complete managed cloud solutions for Azure.
    - Your partner will provide you with access to Azure, manage your billing, and provide support.

Licensing

Free-trial

- Free access to some Azure products for 12 months
- $200 USD credit to spend for the first 30 days on any service.
- Sign-up from sign-up page

Pay-as-you-go

- Get billed for services as you use them

CSP (Cloud Solution Provider)

- Buy Azure services from a Microsoft Partner organization
- You will be billed by the partner organization.
- First line Azure support will be provided by the partner organization.

Azure in Open licensing

- You buy from a third party reseller using a 12 month upfront commitment
- Buy Azure Monetary Commitment credits to use in your subscription.

Enterprise Agreement (EA)

- For big enterprises
- **EA Portal**: enterprise overview of all the spending and budgeting for organization's Azure spend
- **Discounts**: E.g. up to 30% cheaper virtual machines.
- **Enterprise Level Capabilities and Features**: Access to enterprise-only service.

Account, Subscription, Support and Billing

- Requires: Phone number, credit card identity verification, Microsoft/GitHub account.

Subscription

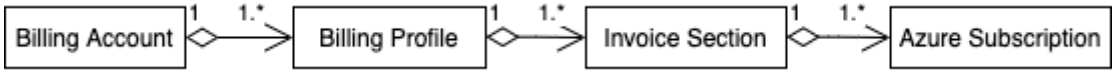
- Used to create and use Azure services
- Created for you when you sign up
- 📝 Logical container used to provision resources in Azure such as virtual machines, databases and more.
- 📝 When you create an Azure resource like a VM, you identify the subscription it belongs to
  - As you use the VM, the usage of the VM is aggregated and billed monthly.
- 📝 Each subscription is a separate entity that can't be merged.

Multiple Azure Subscriptions

- You can create new subscriptions to separate e.g.
  - **Environments**
    - E.g. for testing, security, or to isolate data for compliance reasons.
    - 💡 Useful because resource access control occurs at the subscription level.
  - **Organizational structures**
    - E.g. limit a team to lower-cost resources & allow IT department a full range
    - 💡 Allows you to manage and control access to the resources that users provision within each subscription
  - **Billing**
    - Costs are first aggregated at the subscription level
      - Manage and track costs based on your needs
    - E.g. for production, development, testing
- Or due to **subscription limits**:
  - Subscriptions are bound to some hard limitations
    - E.g. the maximum number of Express Route circuits per subscription is 10

Billing

- You'll receive a monthly invoice with payment instructions provided
  - You also can get set up for multiple invoices.
- Customize billing

- Allows you to e.g. have single invoice for organization but organize charges by department, team, or project.
- Billing structure:
  - 

  - Each **billing account** has billing profile
    - Each **billing profile** has different invoice sections
      - Each **invoice section** can be coupled to different subscriptions.
        - Each invoice section is a line item on the invoice that shows the charges incurred that month

Support

Free

- 24/7 access to the online documentation, community support, and new Azure capabilities demo videos on YouTube
- Demo videos by Azure engineers are available on Azure Friday, Microsoft Mechanics, Azure portal how-to videos playlists
- **Azure Quickstart Center**: Guided experience in the portal.
- **Azure Service Health**: Insights on issues related to your Azure services
- **Azure Advisor**: Personalized recommendations on how to optimize your cost and performance.

Basic support

- Included free for everyone.
- Billing and subscription management support
- Ability to submit as many support tickets as you need
  - Either through • Help + support on top right menu or on resource level (Resource blade -> Support + troubleshooting -> New support request)

Community support

Channel	Description
Azure Knowledge Center	The Azure Knowledge Center is a searchable database that contains answers to common support questions.
Microsoft Tech Community	Get support by reading responses to Azure technical questions from Microsoft's developers and testers.
Stack Overflow	You can review answers to questions from the development community.
Server Fault	Review community responses to questions about System and Network Administration in Azure.
Azure Feedback Forums	Read ideas and suggestions for improving Azure made by Azure users.

Channel	Description
Twitter	Tweet `@AzureSupport` to get answers and support from the official Microsoft Azure Twitter channel.

Paid

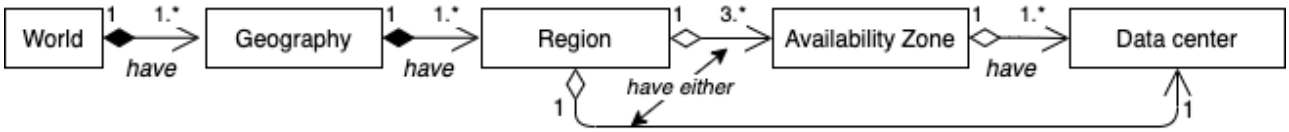
- Azure Support plans

	Developer	Standard	Professional Direct
Best for	Non-critical workloads	Production workloads	Business-critical workloads
Reactive technical support	1 business day response	1-hour response for critical cases	1-hour response + priority tracking of critical cases
Proactive technical support	Not applicable	Not applicable	Access to a pool of technical experts

- You can also purchase Azure Premier support
    - faster response times
    - Architecture/code review
    - onsite support..

Azure Data Centers

- Azure provides more than 100 redundant & secure facilities worldwide linked with a network.
    - Allows you to
        - gain global reach with local presence
        - keep your data secure and compliant with local laws



-
- You can pick the region and sometimes availability zone you want resources deployed into.
    - ❗ You can't select a specific datacenter or location within a datacenter.

Regions

- Regions = Contains at least one, but often multiple datacenters that are nearby and networked together with a low-latency network.
    - Azure assigns and controls the resources within each region to ensure workloads are appropriately balanced.
    - E.g. West US, Canada Central, West Europe, Australia East, and Japan West.
- ❗ Some services or virtual machine features are only available in certain regions, such as specific virtual machine sizes or storage types.
- Azure regions as of February 2020:

- 💡 Regions provide better scalability, redundancy, and preserves data residency for your services.
- Read more: Azure regions

Special regions

- For compliance or legal purposes.
- **Azure Government**
  - ***US DoD Central***, ***US Gov Virginia***, ***US Gov Iowa*** and more
  - 📝 Physical and logical network-isolated instances of Azure for US government agencies and partners.
- ***China East***, ***China North*** and more
  - Unique partnership between Microsoft and 21Vianet
  - Microsoft does not directly maintain the datacenters.

Geographies

- Each region belongs to a single *geography*
- Defined by geopolitical boundaries or country borders.
- Has specific service availability, compliance, and data residency/sovereignty rules applied to it
- Fault-tolerant to withstand complete region failure through their connection to dedicated networking infrastructure
  - 📝 **Fault-tolerance**: App ability to self-detect and correct all types of problems in its environment
- **Data residency**
  - Defines the legal or regulatory requirements imposed on data
  - Based on the country or region in which it resides
  - 💡 An important consideration when planning out your application data storage.
- Geographies are broken up into the following areas
  - Americas
  - Europe
  - Asia Pacific
  - Middle East and Africa
- Read more: Azure geographies

Availability Zones

- 📝 Physically separate datacenters within an Azure region.
- 💡 Allows you to make applications highly available through redundancy.
  - Replicate your compute, storage, networking, and data resources in other zones.
  - Costs more
  - Primarily for VMs, managed disks, load balancers, and SQL databases
  - **Zonal services**: Pin resource to a specific zone.
  - **Zone-redundant services**: Replicates automatically across zones.
- Have independent power, cooling, and networking
- Set up to be an ***isolation boundary***
  - If one zone goes down, the other continues working
- Identified as 1-2-3
  - Logically mapped to the actual physical zones for each subscription independently.
  - Availability Zone 1 in a given subscription might refer to a different physical zone than Availability Zone 1 in a different subscription.
- Connected through high-speed, private fiber-optic networks.
- ❗ There are regions that do not support (multiple) availability zones

Region Pairs

- Each Azure region is always paired with another region within the same geography
  - E.g. West US paired with East US, and South East Asia paired with East Asia
- Pairs are at least 300 (≈ 500 km) miles away.
- Allows for the replication of resources, e.g. virtual machine storage
  - Some services offer automatic geo-redundant storage using region pairs.
- Reduce the likelihood of interruptions to both regions
  - E.g. natural disasters, civil unrest, power outages, or physical network outages
- If one region fails, services automatically fail over to the other region in its region pair.
- Data continues to reside within the same geography as its pair (except for Brazil South) for tax and law enforcement jurisdiction purposes.
- If there's an extensive Azure outage =>
  - One region out of every pair is prioritized to make sure at least one is restored as quick as possible,
- Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.

Interacting with Azure

- **Azure portal** for interacting with Azure via a Graphical User Interface (GUI)
- **Azure PowerShell**, **Azure Command-Line Interface (CLI)** and **Azure SDKs** for command line and automation-based interactions with Azure
- **Azure Cloud Shell** for a web-based command-line interface
- **Azure mobile app** for monitoring and managing your resources from your mobile device

Azure portal

- Public website you can access with any browser: portal.azure.com
- Lets you create, manage, monitor your Azure resources (almost anything you can do on Azure).
- Guides you through complex administrative tasks using wizards and tooltips.
- **Resource panel**
  - In the left-hand sidebar & lists main resource types.
  - The resources listed are part of your ***favorites***.
  - Customizable, can also change default view ***Home*** through Dashboard > Settings
- **Azure Marketplace**
  - Provision services (more than 8.000) from different providers, all certified to run on Azure.
    - e.g. virtual machine images, databases, application build and deployment software, developer tools, threat detection, and blockchain.
- Using Azure portal gets repetitive and are candidates for automation with CLI & PowerShell

Top menu

- 
- Can start **Cloud Shell** using icon (>_)
- **Directory and subscription**
  - Open using Book and Filter icon to show the Directory + subscription pane.
  - You change your subscription or change to another directory.
- **Notifications**: bell icon to see list the last actions that have been carried out
- **Settings**: Gear icon
  - • Set color & contrast themes, • default view when you sign in, • inactivity sign out delay, • toast notifications • language and regional format.
- **Help pane**: Question mark icon to show the Help pane
  - Includes: • Help + Support • What's new • Azure roadmap • Launch guided tour • Keyboard shortcuts • Show diagnostics • Privacy statement
  - **Help + support**
    - Create or track a support ticket
    - Monitor service health e.g. planned maintenances, global issues, health history etc..
    - Can also be done at resource level: Resource blade -> Support + troubleshooting -> New support request
- **Feedback pane**: Smiley icon to send feedback.
- **Profile settings**: Select on your name in the top right-hand corner, a menu opens with a few options:
  - Sign in with another account, or sign out entirely
  - View your account profile, where you can change your password
  - Or to more by clicking on ... => • Check your permissions • View your bill (takes you to Cost Management + Billing - Invoices page) • Update your contact information

Azure Advisor

- Free service built into Azure that provides recommendations on high availability, security, performance, operational excellence, and cost
- Advisor analyzes your deployed services and looks for ways to improve your environment across those areas.
- You can view recommendations in the portal or download them in PDF or CSV format.

Dashboards

- High-level details about your Azure environment.
- Customize by moving and resizing tiles, and displaying services
  - At the top you to create, upload, reset, download (JSON), edit, clone, switch, delete and share a dashboard.
  - In **Tile Gallery** you have different tiles such as Clock, ARM data, Audit Logs, Service Health, AD Connect.
    - Some tiles have editable settings, e.g. for clock you can set the time zone.
  - 💡 You can take elements on child panes and put them on your dashboard. Hover the item in `...` menu select "Pin to Dashboard"
- Multiple dashboards are supported, and you can switch between them as needed.
  - E.g. DB admin would have a dashboard that contains views of the SQL database service
  - E.g. Azure Active Directory administrator would have views of the users and groups within Azure AD
- You can share your dashboards with other team members.
  - You can unpublish to unshare.
- You can use role-based access control (RBAC) to control who can access that dashboard.
- Azure stores dashboards within resource groups as JSON files
  - so you can customize them programmatically
  - 💡 The easiest starting point is to download the dashboard JSON as previously described and edit that file.
  - 💡 You can also distribute the dashboard JSON file to other users.
- The default dashboard is named Dashboard.

Azure PowerShell

- 📝 Module that you can install for Windows PowerShell or PowerShell Core (cross-platform, linux/win/macOS)
- E.g. create a new virtual machine: `New-AzVM -ResourceGroupName "MyResourceGroup" -Name "TestVm" -Image "UbuntuLTS"`
- Scripting environment for automation just like Azure CLI

Azure CLI

- 📝 Cross-platform (linux/win/macOS) command-line program that connects to Azure and executes commands on Azure.
- E.g. to create VM first login `az login` then create a resource group and execute:
  - `az vm create --resource-group MyResourceGroup --name TestVm --image UbuntuLTS --generate-ssh-keys`

Azure Cloud Shell

- 📝 Browser-based command-line for managing and developing Azure resources.
  - Like an interactive console that you run in the cloud.
- 📝 You can reach on portal (top right `>_`icon)
  - or through visiting shell.azure.com
- 📝 Two experiences to choose from: Bash, Powershell

    - Both include access Azure CLI and to Azure PowerShell (Azure command-line interfaces)
        - Even more: .NET Core, Python, Java, Node.js, Go, vim, nano, emacs, git, maven, make, npm...
- It's persistent: Any data you place is kept across sessions.
    - You're prompted to create an Azure Storage Account when you access the Azure Cloud Shell.
    - This storage area is used as your `$HOME` folder.

Azure mobile app

- Microsoft Azure mobile app to access, manage, and monitor Azure.
- IOS + Android

Azure SDKs

- For a range of languages and frameworks, and REST APIs
- Lets you use to manage and control Azure resources programmatically including automation.

Access public and private preview features

- With *Azure Preview Features*, you can test beta and other pre-release features, products, services, software, and regions.
- E.g. • new storage types • new Azure services, such as Machine Learning enhancements • new or enhanced integration with other platforms • new APIs for services
- Get notified about GA (general availability) releases
    - In portal, you can periodically check "What's New" link on the help menu (?).
    - Or use Azure Updates pages.
- Preview portal through preview.portal.azure.com
    - Typical portal preview features provide performance, navigation, and accessibility improvements
- Preview types:

	Public preview	Private preview
SLA	✗	✗
Support	☑	✗
Available to	All customers	Only specific
Access	Through preview features page, or in in Azure Portal click on **New** and search for preview	Typically by invite only issued by the product team

Service-level Agreements (SLA)

- Formal documents to define the performance standards that apply to Azure.

- Specify also what happens if a service or product fails to perform to a governing SLAs specification.
- There are SLAs for individual Azure products and services.
- ❗ Azure does not provide SLAs for most services under the Free or Shared tiers
  - e.g. Azure Advisor
- Three key characteristics of SLAs for Azure products and services:
  1. **Performance Targets**
     - Specific to each Azure product and service.
     - E.g. uptime guarantees or connectivity rates
  2. **Uptime and Connectivity Guarantees**
     - 📝 Monthly Uptime % = `(Maximum Available Minutes-Downtime) / Maximum Available Minutes X 100`
     - 📝 Range from 99.9% ("three nines") to 99.999% ("five nines") for any paid tier service.
       - In other words minimum SLA for all non-free Azure services are 99.9%
     - E.g. Azure Cosmos DB (Database) service SLA offers 99.999 percent uptime
       - meaning it allows for about 5 minutes of total downtime per year.
       - also includes low-latency commitments of less than 10 milliseconds on DB read + write operations.
  3. 📝 **Service credits**
     - Given to paying Azure customers if uptime percentage is lower than given in SLA.
     - Describe how Microsoft will respond if an Azure product or service fails to perform to its governing SLAs specification.
     - E.g. customers may have a discount applied to their Azure bill, as compensation for an under-performing Azure product or service.
- Read more: SLA Summary for Azure Services

Composite SLA

- Result of combining SLAs across different service offerings.
- 📝 Calculating downtime
  - E.g. web app (99.95% SLA from Azure) writes to SQL database (99.99% SLA from Azure)
    - Composite SLA = `99.95 percent × 99.99 percent = 99.94 percent`
      - = `0.9995 * 0.9999 = 0.9994`
    - Means combined probability of failure is higher than the individual SLA values
- You can improve the composite SLA by creating independent fallback paths.
  - E.g. if the SQL Database is unavailable, you can put transactions into a queue for processing at a later time.
    - Web app (99.95%) writes to either SQL Database (99.99%) or queue (99.9%)
    - Application is still available even if it can't connect to the database.
      - ❗ But it fails if both the database and the queue fail simultaneously.
    - If the expected percentage of time for a simultaneous failure is **0.0001 × 0.001**
      - the composite SLA for this combined path of a database or queue would be:
        - `1.0 – (0.0001 × 0.001) = 99.99999 percent`
    - If we add the queue to our web app, the total composite SLA is:
    - `99.95 percent × 99.99999 percent = ~99.95 percent`
    - Improves SLA but application logic gets more complicated
      - You are paying more to add the queue support and there may be data-consistency issues you'll have to deal with due to retry behavior.

Application SLA

- By creating your own SLAs, you can set performance targets to suit your specific Azure application.
- 💡 >= four 9's (99.99%) SLA performance targets =>
  - manual intervention from failures may not be enough (difficult to be quick enough)
  - should have self-diagnosing & self-healing solutions.

Resiliency

- **Resiliency** is the ability of a system to recover from failures and continue to function.
- High availability and disaster recovery are two crucial components of resiliency
  - 📝 **Disaster recovery**: When Godzilla destroys your data center, you do have alternative locations to keep providing your service and protocols/means for the other location to know how to keep delivering the service.
- **Failure Mode Analysis (FMA)**
  - Goal:
    - Identify possible points of failure.
    - Define how the application will respond to those failures.
- Read more: Designing resilient applications for Azure

High availability

- 📝 Availability is often given as percentage uptime
- Refers to the time that a system is functional and working.
- Most providers prefer to maximize the availability of their Azure solutions by minimizing downtime.
  - ❗ As you increase availability, you also increase the cost and complexity of your solution.
  - As your solution grows in complexity, you will have more services depending on each other.
    - You might overlook possible failure points in your solution if you have any interdependent services.
    - 💡 E.g. a workload that requires 99.99 percent uptime shouldn't depend upon a service with a 99.9 percent SLA.
- Read more: Availability choices for Azure compute

Azure Resource Manager-Resources and Resource Groups and Management Groups

Azure Resource

- Anythings you create in an Azure subscription
- E.g. virtual machines, Application Gateways, and CosmosDB instances
- 💡 Good to have consistent naming convention e.g.: `cloudarchitecture-prod-infrastructure-rg`
  - what it's used for (`cloudarchitecture`)
  - environment (`prod`)
  - the types of resources contained within (`infrastructure`)
  - type of resource it is itself (`rg` = resource group)
- Provides fine-grained access management through role-based access control (RBAC)

- 📝 You can move some resources that supports move to a new resource group or subscription if they support move operation.

Tagging

- Helps you better search, filter, and organize these resources
- Name/value pairs of text data that you can apply to resources and resource groups
- E.g.
  - department (like finance, marketing, and more)
  - environment (prod, test, dev)
  - cost center
  - life cycle and automation (like shutdown and startup of virtual machines)
- 💡📝 Good way to group your billing data
  - E.g. VMs on production that belongs to a cost center A.
- 💡 Help with monitoring
  - You can set-up alerts based on tags e.g. if a resource fails notification goes to the finance department.
- 💡 Help with automation
  - E.g. `shutdown:6PM` and `startup:7AM` tag TO automate the shutdown and startup of virtual machines in development environments during off-hours to save costs.
- 💡 Help with automation Governance through Policies
  - E.g. ensure that all resources have the Department tag associated with them and block creation if it doesn't exist.
- ❗ Limitations:
  - A resource can have up to 50 tags.
  - 📝 Tags aren't inherited from parent resources.
  - 📝 Not all resource types support tags

Resource locks

- 📝 Blocks modification (**Read-only**) or deletion (**Delete**) of the resource.
  - For more granular control of what can be deployed e.g. see Azure policies
- Read-only allows only `HTTP GET` requests
  - ❗ Can lead to unexpected results e.g. listing all objects in a storage account requires `POST` request is denied
- 📝 You must remove the lock in order to perform forbidden activity.
- Apply regardless of RBAC permissions
- 📝 Protects against accidental deletion
- 💡 Use to protect key resources that could have a large impact if they were removed or modified
  - E.g. ExpressRoute circuits, virtual networks, critical databases, and domain controllers
- Only "Owner" and "User Access Administrator" can create/delete locks
  - It requires access to `Microsoft.Authorization/locks/*`

Azure Resource Group

- Also an Azure resource so it can have locks, tags, RBAC permissions etc.
  - It's free!
- Logical container for resources deployed on Azure.

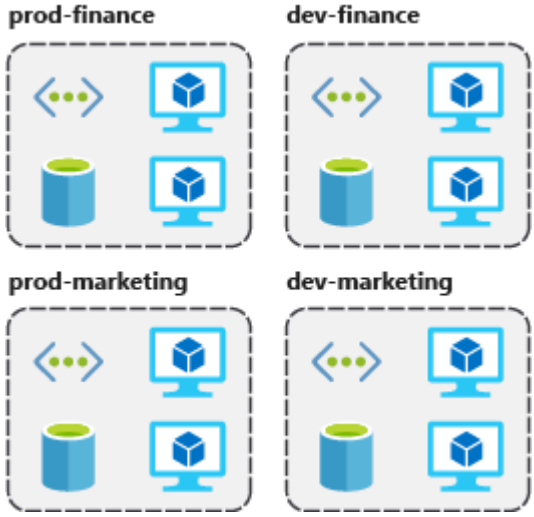
- Tied to a region & subscription itself.
  - 📝 But can contain resources from different regions
    - ❗ If region the RG goes down, the management of the RG would not work.
- Helps you organize resources
  - You can place resources of e.g. similar usage, type, or location in same group.
- 📝 If you delete a resource group, all resources contained within are also deleted.
- Authorization
  - Scope for applying role-based access control (RBAC) permissions.
  - Permissions are inherited in all resources that the group has.
- ❗ All resources must be in a resource group and a resource can only be a member of a single resource group.
  - Before any resource can be provisioned, you need a resource group
- ❗ Some services has specific limitations or requirements to move from one resource group to another
- ❗ Can't be nested.
- Can see history of the deployments to a resource group

Organizing resource groups

- By type (virtual networks, virtual machines, cosmos dbs)
  - 

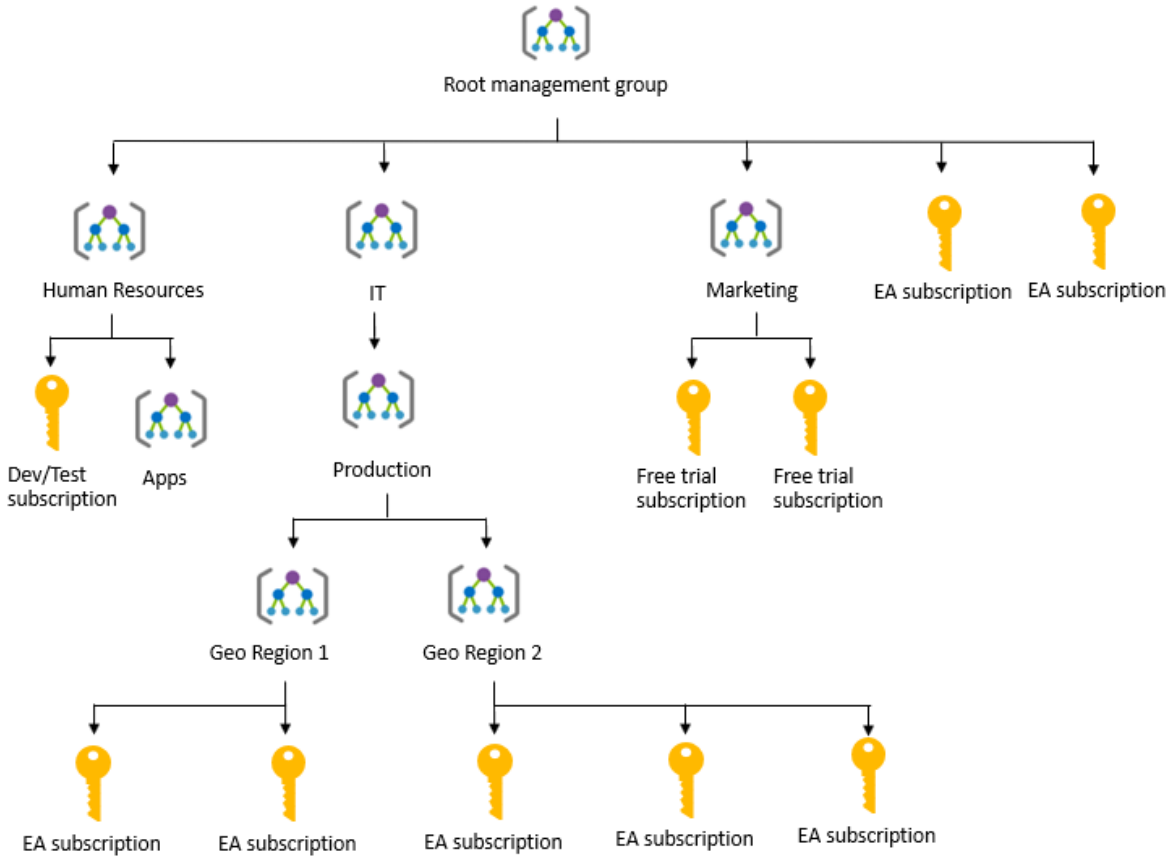
- By environment (prod, qa, dev)
  - 

- By department (marketing, finance, human resources)
  - 

- Combining strategies e.g. environment and department:
  - 

- By authorization
  - By who needs to administer them.
  - See RBAC
  - E.g. databases in database administration group to give access to database administrators.
- By life cycle
  - Allows you to e.g. delete after experimentation.
- By billing
  - A way to filter and sort the data to better understand where costs are allocated.

Management Groups

- Groups multiple subscriptions.
- Can have RBAC assignments and policies
  - Inherited by underlying subscriptions
- Good for enterprises
- E.g.
  - 

Compliance in Azure

Microsoft Privacy Statement

- privacy.microsoft.com/privacystatement
- Explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.
- Applies to the interactions Microsoft has with you and Microsoft products such as Microsoft services, websites, apps, software, servers, and devices.

Microsoft Trust Center

- microsoft.com/trust-center
- 📝 In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
- Recommended resources in the form of a curated list of the most applicable and widely used resources for each topic.
- Direct guidance and support

Service Trust Portal

- servicetrust.microsoft.com
- 📝 Can download
  - audit reports produced by external auditors
  - Microsoft-authored reports about its cloud services.
- Also has compliance guides to help you understand how you can use Microsoft cloud service features to manage compliance with various regulations.
- Hosts Compliance Manager, companion feature to the Trust Center.

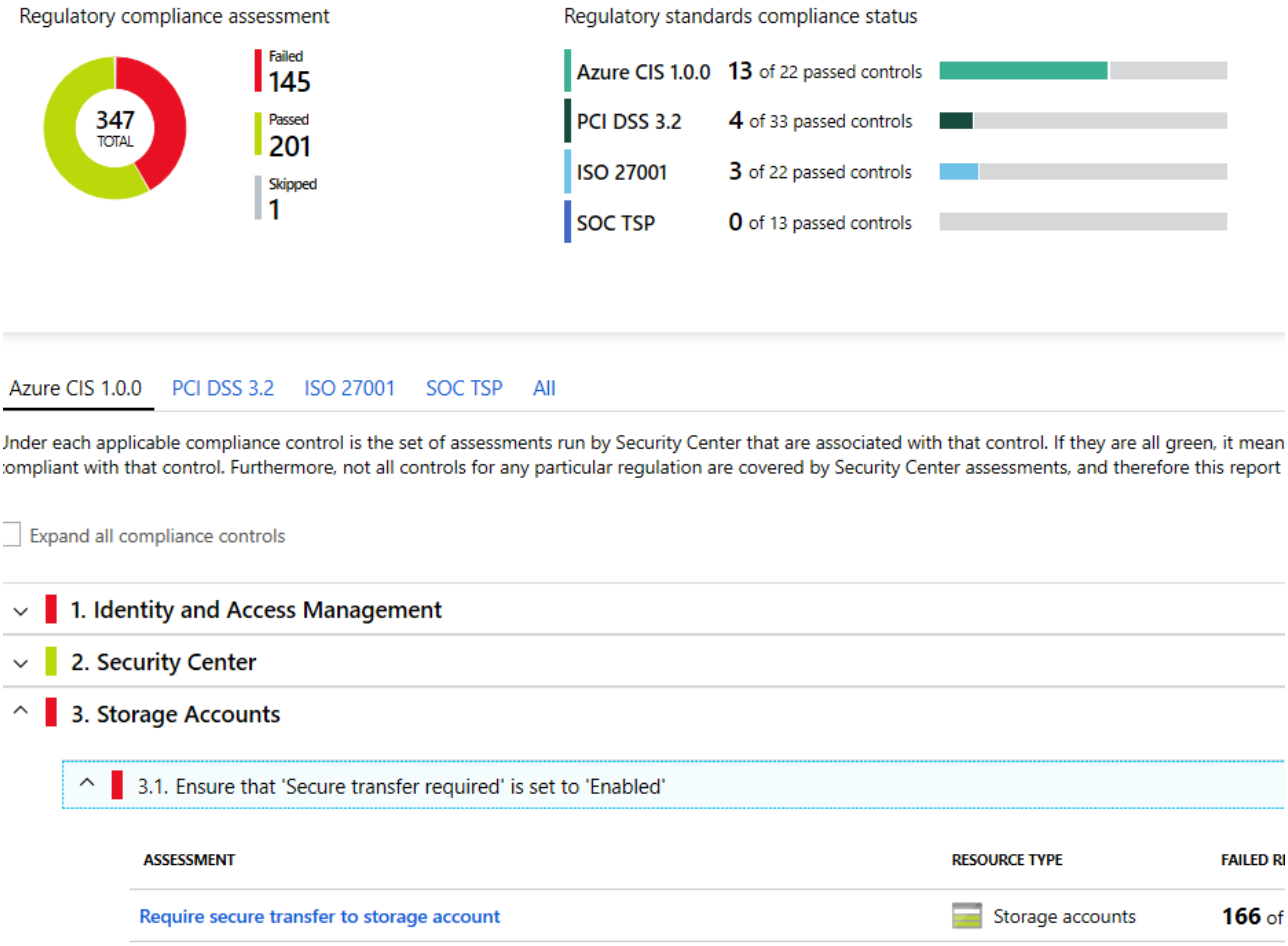
Compliance Manager

- servicetrust.microsoft.com/ComplianceManager
- Free workflow-based risk assessment dashboard with
  - summary of your data protection, compliance stature, recommendations for improvement
- Features:
  - Combines the following three items:
    1. Information provided by Microsoft to auditors and regulators e.g.ISO 27001, ISO 27018, and NIST.
    2. Information that Microsoft compiles internally for its compliance with regulations (such as HIPAA and the EU GDPR).
    3. An organization's self-assessment of their own compliance with these standards and regulations.
  - Repository in which to upload and manage evidence and other artifacts related to compliance activities.
  - Assign, track, and record compliance and assessment-related activities
    - Help your organization cross team barriers to achieve your organization's compliance goals.
  - ***Compliance Score*** to help you track your progress with onging risk assessments.
    - Recommends also actions as part of the risk assessment.
  - Excel reports that document the compliance activities performed by Microsoft and your organization.
    - 💡 Can be provided to auditors, regulators, and other compliance stakeholders

Azure Security Center

- 📝 Global service in Azure that includes regulatory compliance dashboard of **your** services.
- Insights into your compliance posture based on continuous assessments
- Analyzes risk factors in your hybrid cloud environment according to security best practices

- Overall security score, assessment against e.g. CIS, PCI DSS 3.2.1, SOC, ISO 27001..



Azure Services

- Microsoft notifies at least 1 months before ending support for an Azure service that does NOT have a successor service.
- **App Hosting**
  - Run entire your web application on a managed platform on Linux & Windows
  - In Azure Marketplace there are huge range of third party products you can run on Azure
    - Including SAP & SQL database solutions
- **Integration**
  - Logic apps and service bus connect applications & services
  - Allow for workflows to orchestrate business processes on cloud or on-premises
- **Security**
  - Security is integrated in every aspect of Azure
  - Hardened structures (designed to withstand a range of threats) & global security intelligence monitoring
  - **Azure Identity Management** gives you tight control to choose who gets access to what.

Compute

- Primarily for performing calculations, executing logic and running applications
- On-demand & computing service for running cloud-based applications

- Provides computing resources like multi-core processors and supercomputers via virtual machines and containers.
- Provides serverless computing to run apps without requiring infrastructure setup or configuration.
- Pay only for the resources you use and only for as long as you're using them.
- Four common techniques for performing compute in Azure:
    - Virtual machines IaaS: Infrastructure as a Service
    - Containers
    - Azure App Service
    - Serverless computing

Choosing a computing strategy

- "All or nothing" is not needed when choosing a cloud computing strategy.
- Each provides benefits as well as tradeoffs against other options.
- E.g. serverless computing removes the need for you to manage infrastructure
    - Serverless computing expects work to be completed quickly; usually within seconds or less.
    - You might run your core application on a virtual machine or container but offload some of the data processing onto a serverless app.
- Most control to least control: Virtual machines, containers, serverless computing
- Learn more: Overview of Azure compute options

Virtual Machines

- Infrastructure as a service (IaaS)
- Virtual machines, or VMs, are software emulations of physical computers.
- They include a virtual processor, memory, storage, and networking resources.
- They host an operating system (OS), and you're able to install and run software like a physical computer.
- You can connect to VM & control it using a remote desktop client.
- Good choice when you need:
    - Total control over the operating system (OS)
    - The ability to run custom software
    - To use custom hosting configurations
- Azure takes care of the physical hardware
    - You take care of configuring, updating, and maintaining the software that runs on the VM.
- An **image** is a template used to create a VM.
    - Includes an OS and often other software, like development tools or web hosting environments.

Examples of use-cases

- **During test + dev** as it's easy to create different OS & application configurations. Easy to delete when not needed.
- **Minor tasks**. E.g. application handles fluctations in demand and shut down VMs when you don't need them & quickly start them to meet a suddenly increased demand.
- **Extending your datacenter** to the cloud, e.g. running SharePoint.

- **During disaster recovery**. E.g. if primary datacenter fails, create VMs running on Azure to run your critical applications and then shut them down when the primary datacenter becomes operational again.
- **Lift and shift**: Moving from physical datacenter to cloud. You can take image of the server & run within a VM with little to no changes.
- Learn more: Typical scenarios for running Azure VMs

Scaling and High Availability

- 99.99% uptime guarantee for all Virtual Machines that have two or more instances deployed across two or more Availability Zones.

Domains & maintenance events

Update domains

- Groups of VMs and underlying physical hardware that can be rebooted at the same time.

Planned maintenance events

- When the underlying Azure fabric that hosts VMs is updated by Microsoft.
- Done to patch security vulnerabilities, improve performance, and add or update features.
- Often no impact, sometimes requires reboot.
- When the VM is part of an availability set, the Azure fabric updates are sequenced so not all of the associated VMs are rebooted at the same time.
    - VMs are put into different **update domains**

Fault domains

- Fault domain = rack of servers.
- provides the physical separation of your workload across different power, cooling, and network hardware that support the physical servers in the data center server racks.
- In the event the hardware that supports a server rack becomes unavailable, only that rack of servers is affected by the outage.

Unplanned maintanance events

- Involve a hardware failure in the data center e.g. a power outage or disk failure
- VMs that are part of an availability set automatically switch to a working physical server so the VM continues to run.
- The group of virtual machines that share common hardware are in the same **fault domain**.

Availability sets

- Logical grouping of two or more VMs that help keep your application available during planned or unplanned maintenance.
- With an availability set, you get:
    - ❗ Up to three **fault domains**
        - each have a server rack with dedicated power and network resources.
    - Five logical **update domains**

        - ❗ can be increased to a maximum of 20.
- There's no cost for an availability set.
    - Only pay for the VMs within the availability set.
- 💡📝 Recommended for high availability.

Virtual machine scale sets

- Lets you create & manage a group of identical, load balanced VMs.
- Allow you to centrally manage, configure, and update a large number of VMs to provide highly available applications.
- The number of VM instances can automatically increase or decrease in response to demand or a defined schedule.
- 💡 Helps you build large-scale services for areas such as compute, big data, and container workloads.
- Provides high availability through regional or multiple Availability Zones deployment options.

Azure Batch

- Large-scale job scheduling and compute management.
- When running a job, batch:
    1. Starts a pool of compute VMs for you
    2. Installs applications and staging data
    3. Runs jobs with as many tasks as you have
    4. Identifies failures
    5. Requeues work
    6. Scales down the pool as work completes
- 💡 Good for cases where you need raw computing power or supercomputer level compute power.

Containers

- Virtualization environment for running applications.
- Bundles apps + operating system + runtime.
- Run on top of a host operating system like VMs.
    - But unlike VMs, containers don't include an operating system for the apps running inside the container.
        - A container doesn't use virtualization
    - Instead, containers bundle the libraries and components needed to run the application and use the existing host OS running the container.
        - Those not waste resources simulating virtual hardware with a redundant OS.
            - You can run multiple isolated applications on a single container host.
            - Much more lightweight than VMs.
                - Allows you to quickly respond to changes in demand or failure
        - E.g. if five containers are running on a server with a specific Linux kernel, all five containers and the apps within them share that same Linux kernel.
- The container orchestrator can start, stop, and scale out application instances as needed.
    - Faster than VM (seconds instead of minutes)
- You can use same server to host multiple container applications
    - They are secured and isolated

- More efficient than VM
    - Run containers side by side without sacrificing isolation.
    - Much smaller in size
    - Development process is simplified. Dev env = prod env.

Containers in Azure

Azure Container Instances

- PaaS: Fastest & simplest way to run containers
- No configuration of VM or any other additional services.
- Just upload containers + run with automatic scaling

Azure Kubernetes Service

- Orchestration = The task of automating, managing, and interacting with a large number of containers
- Azure Kubernetes Service (AKS) is a complete orchestration service for containers
- You can migrate existing apps to AKS e.g. :
    1. Convert an existing application to one or more containers and then publish one or more container images to the Azure Container Registry.
    2. Deploy the containers to an AKS cluster using the Azure portal or the command line.
    3. Azure AD controls access to AKS resources.
    4. You access SLA-backed Azure services, such as Azure Database for MySQL, via OSBA.
    5. Optionally, AKS is deployed with a virtual network.

Kubernetes

- Most popular option for managing container-based workloads
- Combines container management automation with an API
- Cloud-native: Can run across different clouds
- **Pod management**
    - Manages placement of pods
    - 1 pod = 1 or more containers on a node
        - If node is removed = Kubernetes move affected workloads to different node.
    - If one pod crashes = Kubernetes creates new instance
    - Pods can be scaled manually or automatically (horizontal)
- Spreads deployment to minimize downtime
    - If update is problematic, it can roll-back
- Can manage storage
    - Persistent volumes to represent data storage to one or more containers
    - Data can be persisted across many pod instances
    - Can utilize cloud-based storage and data system e.g. Azure storage + Cosmos DB
- Can manage networking
    - Can expose pods to internet
    - Load balances traffic across multiple replicas of a pod
    - Network isolation
    - Policy-driven network security.
    - Manage communication + name resolution between pods

- It can be extended with additional capabilities
    - E.g. cloud events on pod creation, custom pod scheduling logic, on-demand provisioning of managed cloud services.

Micro-services

- Architecture where you break solutions into smaller, independent pieces.
- Allows you to separate portions of your app into logical sections that can be maintained, scaled, or updated independently.
- Each service has small code-base that can be managed by a small development team.
- Don't need to share same technology stack, libraries or frameworks.
    - Each team can choose the right tool for the job.
    - Single development team can test & build & deploy a service
- Results in continuous innovation and faster release cadence.
- Smaller scope =
    - Easier to understand code-base
    - Easier for new team members to get started
- Each micro-service is completely autonomous with no cross-dependencies.
    - Provides fault isolation: If one goes down, it does not take out all application
- Communicates with each other using APIs.
    - APIs encapsulate internal functionality.
        - Internal implementation details of each services are encapsulated behind their interface.
    - 💡 Good practices:
        - Reduce interdependencies
        - Introduce orchestration / management layer in the higher level consuming application to coordinate calls and combine results.
- 💡 Good for:
    - High release velocity
    - Highly scalable applications
    - Applications with rich domains / subdomains
    - Organizations with small development teams

Micro-services deployment

- Allows each microservice to be deployed independently of every other microservice.
- A team can update an existing service without rebuilding/redeploying the entire application.
- They can easily roll back & roll forward & update if something goes wrong.
- Makes bug fixes + feature releases more manageable & less risky
- Allows each microservice
    - to be scaled independently
    - persist own data & external state without common repository layer
- E.g. one for front-end, one for back-end and one for storage.
    - If back-end reaches capacity but not others, you can scale it individually.
    - Allows you replace storage microservice without affecting rest of the application.

Azure Service Fabric

- Distributed systems platform

- Runs in Azure or on-premises

App Service

- Azure App Service is an HTTP-based service.
- Enables you to build and host many types of web-based solutions without managing infrastructure.
- E.g. you can host web apps, mobile back-ends, and RESTful APIs in several supported programming languages.
- Supports different frameworks such as .NET, .NET Core, Java, Ruby, Node.js, PHP, Python..
- Can scale on both both Windows and Linux-based environments.

Mobile apps

- Allows developers to create mobile backend as a service (MBaaS)
- Features include
  - Autoscaling
  - Offline data synchronization
  - Broadcasting push notifications
  - Integration with identity providers including Azure Active Directory, Google, Twitter, Facebook, and Microsoft

Azure Marketplace

- Online store that hosts applications that are certified and optimized to run in Azure.
- Many types of applications are available, e.g. AI / web applications.
- Deployments from the store are done via the Azure portal using a wizard-style user interface.
  - Makes evaluating different solutions easy.

Pricing tiers

- Categories

Category	Description
Dev / Test	Ideal for less demanding workloads. Focused on providing shared infrastructure. Additional features include custom domains / SSL and manual scale.
Production	Ideal for more demanding workloads. Additional features include staging slots, daily backups, and a traffic manager.
Isolated	Ideal for workloads that require advanced networking and fine-grained scaling.

- Within each category, there are different pricing tiers.

Scale up an App Service

1. Open the Azure portal
2. From the left-hand navigation menu (may need to click on menu icon), select **Dashboard**
3. Select the **App Service** with the name you chose it in the previous exercise.

4. Under **Settings** you see many configurable settings
5. Select **Scale up (App service plan)**.

Serverless Computing

- Serverless computing services in Azure are:
  - Azure Functions and Azure Logic Apps

Serverless concepts

Abstraction of servers

- Completely abstracts the underlying hosting environment.
- No infrastructure configuration / maintenance.
  - Basically deploy your code and it runs with high availability.
- Automatically scaling, performance and allocation/deallocation of resources
  - You never explicitly reserve capacity.

Event-driven scale

- Good fit for workloads that respond to incoming events.
- Events include triggers by e.g.
  - timers e.g. if a function needs to run every day at 10:00 AM UTC
  - HTTP e.g. API and webhook scenarios
  - queues e.g. with order processing)
- Triggers & bindings
  - A function contains both code and metadata about its triggers and bindings.
  - Triggers define how a function is invoked
  - Bindings provide a declarative way to connect to services from within the code.
- The platform automatically schedules the function to run and scales the number of compute instances based on the rate of incoming events.

Micro-billing

- Pay only for the time the code runs.
- No active function executions occur = they're not charged.
- E.g. if the code runs once a day for two minutes, they're charged for one execution and two minutes of computing time.

Azure Functions

- Can execute code in almost any modern language.
- Commonly used when you need to perform work in response to an event.
- Can be either
  - **Stateless** (the default)
    - Behave as if restarted every time responding to an event
  - **Stateful** (called "Durable Functions")
    - Has a context to track prior activity.

- Open-source, can deploy anywhere. See Azure functions host

Azure Logic Apps

- Execute workflows designed to automate business scenarios and built from predefined logic blocks.
- Every logic app workflow starts with a trigger (many can be scheduled) and runs actions
    - Actions include data conversions and flow controls (e.g. conditional / switch statements, loops, and branching)
- You create using a visual designer on the Azure portal or in Visual Studio.
    - The workflows are persisted as a JSON file with a known workflow schema.
- Azure provides over 200 different connectors and processing blocks to interact with different services
    - You can also build custom connectors to interact.
- Often no code is written.
- E.g. a ticket arrives in ZenDesk, you could detect the intent of the message with cognitive services and then create an item in SharePoint to track the issue.

Functions vs. Logic Apps

Functions and Logic Apps can both create complex orchestrations. An orchestration is a collection of functions or steps, that are executed to accomplish a complex task. With Azure Functions, you write code to complete each step, with Logic Apps, you use a GUI to define the actions and how they relate to one another.

You can mix and match services when you build an orchestration, calling functions from logic apps and calling logic apps from functions. Here are some common differences between the two.

	Functions	**Logic Apps**
State	Normally stateless, but Durable Functions provide state	Stateful
Development	Code-first (imperative)	Designer-first (declarative)
Connectivity	Write code for custom bindings from many binding types	Large collection of connectors, Enterprise Integration Pack for B2B scenarios, build custom connectors
Actions	Each activity is an Azure function; write code for activity functions	Large collection of ready-made actions
Monitoring	Azure Application Insights	Azure portal, Log Analytics
Management	REST API, Visual Studio	Azure portal, REST API, PowerShell, Visual Studio
Execution context	Can run locally or in the cloud	Runs only in the cloud.

Storage

- Secure, durable, scalable, and easily accessible from across the globe.
- E.g. persistent data across devices for mobile applications.

- Uses REST API endpoints that make data available to huge range of application types & platforms e.g. .NET, JAVA, NODE.

Benefits

- **Automated backup and recovery**: mitigates the risk of losing data if there is any unforeseen failure or interruption.
- **Replication across the globe**
  - Copies your data to protect it against any planned or unplanned events
    - e.g. scheduled maintenance or hardware failures.
  - Allows you to replicate your data at multiple locations across the globe.
- **Support for data analytics**: supports performing analytics on your data consumption.
- **Encryption capabilities**: You have tight control over who can access the data.
- **Multiple data types**: Almost any e.g. videos, text, like binary files. Many options for SQL and NoSQL data.
- **Data storage in virtual disks**: Up to 32 TB. Significant when you're storing heavy data such as videos and simulations.
- **Storage tiers**: To prioritize access to data based on frequently used vs rarely used information.

Types of data

Structured data

- Also called **relational data**
- Data that adheres to a schema.
  - Defines table, fields, clear relationship between two
- Can be stored in e.g. database table with rows and columns.
- Relies on keys to indicate how one row in a table relates to data in another row of another table.
- 💡 It's easy to enter, query, and analyze.
  - All of the data follows the same format.
  - E.g. sensor data or financial data.

Semi-structured data

- Also called as **non-relational** or **NoSQL data**.
- Doesn't fit neatly into tables, rows, and columns.
- Instead uses tags or keys that organize and provide a hierarchy for the data.

Unstructured data

- Encompasses data that has no designated structure to it
- There are no restrictions on the kinds of data it can hold.
  - e.g. PDF document, a JPG image, a JSON file, video content, etc
- 💡 More prominent as businesses try to tap into new data sources.

Azure Storage

- Includes disks attached to virtual machines, file shares, databases
- They can expand & shrink necessarily

- Common characteristics:
  - **Durable** and highly available with redundancy and replication.
  - **Secure** through automatic encryption and role-based access control.
  - **Scalable** with virtually unlimited storage.
  - **Managed**, handling maintenance and any critical problems for you.
  - **Accessible** from anywhere in the world over HTTP or HTTPS.

Azure Blob Storage

- Also known as **Azure blobs**
- Good for very large objects, such as video files or bitmaps
- Unstructured, meaning that there are no restrictions on the kinds of data it can hold.
- 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.
- Lets you
  - Stream large video or audio files directly to the user's browser from anywhere in the world.
  - Send large volumes of data directly to the browser.
- 💡 Also used to store data for backup, disaster recovery, and archiving.
- 📝 Ability to store up to 8 TB of data for virtual machines (VM disks)

Storage tiers

1. **Hot storage tier**: optimized for storing data that is accessed frequently.
2. **Cool storage tier**: optimized for data that are infrequently accessed and stored for at least 30 days.
3. **Archive storage tier**: for data that are rarely accessed and stored for at least 180 days with flexible latency requirements.

Azure Disk Storage

- Also known as **Azure disks**
- Provides disks for virtual machines, applications, and other services to access and use as they need.
- In the background they are page-blobs in a blob storage
- Allows data to be persistently stored and accessed from an attached virtual hard disk.
- Disks can be managed or unmanaged by Azure, and therefore managed and configured by the user.
- 💡 Use-case examples: Lift and shift
  - Storing data that is not required to be accessed from outside the virtual machine to which the disk is attached.
- Different sizes and performance levels
  - Solid-state drives (SSDs)
  - Hard disk drives (HDDs)
- 💡 Use standard SSD and HDD disks for less critical workloads
  - Premium SSD disks for mission-critical production applications.
- Durable: ZERO% annualized failure rate.

Azure Data Lake Storage

- 📝 Allows you to perform analytics on your data usage and prepare reports.
- Stores both structured and unstructured data.

- Combines the scalability and cost benefits of object storage with the reliability and performance of the Big Data file system capabilities.
- Supports batch queries, interactive queries, real-time analytics, machine learning, and being a data warehouse.

Azure File Storage

- Also known as **Azure files**
- File shares that you can access and manage like a file server
- Fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol.
- Ensures the data is encrypted at rest and in transit.
- Can be mounted concurrently by cloud or on-premises Windows, Linux, and macOS.
- 📝 Any number of Azure virtual machines or roles can mount and access the file storage share simultaneously.
- 💡 Good to share files anywhere in the world, diagnostic data, or application data sharing.

Azure Queue Storage

- A data store for queuing and reliably delivering messages between applications
- 💡 Helps build flexible applications and separate functions for better durability across large workloads
  - When application components are decoupled, they can scale independently
  - Provides asynchronous message queueing for communication between application components
- Typically, there are one or more sender components and one or more receiver components.
  - Sender components add messages to the queue
  - Receiver components retrieve messages from the front of the queue for processing
- 💡 Use-case examples:
  - Create a backlog of work and to pass messages between different Azure web servers.
  - Distribute load among different web servers/infrastructure and to manage bursts of traffic.
  - Build resilience against component failure when multiple users access your data at the same time.

Azure Table Storage

- NoSQL data Store
- Scheme-less design

Encryption Types

Azure Storage Service Encryption (SSE)

- For data at rest helps you secure your data.
- It encrypts the data before storing it and decrypts the data before returning it.
- Encryption & decryption are transparent to the user.

Client-side encryption

- Data is already encrypted by the client libraries.
- Azure stores the data in the encrypted state at rest, which is then decrypted during retrieval.

Replication

- Set up when you create a storage account
- Ensures that your data is durable and always available
- Provides regional and geographic replications
    - Protects data against natural disasters and other local disasters like fire or flooding.

On-premises storage vs Azure data storage

Why migrate to cloud

- **Cost effectiveness**
    - Pay-as-you go
    - No dedicated hardware to be purchased, installed, configured and maintained. = no up-front expense (or capital cost).
    - Scalable: No need to have idle hardware
- **Reliability**
    - Managed data backup, load balancing, disaster recovery, and data replication as services to ensure data safety and high availability.
- **Storage types**
    - On-premises => often requires numerous servers and administrative tools for each storage type.
    - Azure has different storage options for each part of your solution.
- **Agility**
    - Requirements and technologies change: No need to reprovisioning & deployment of new infrastructure.
    - Create new services in minutes = change storage back-ends quickly without needing a significant hardware investment.

Comparison

Needs	On-premises	Azure data storage
Compliance and security	Dedicated servers required for privacy and security	Client-side encryption and encryption at rest
Store structured and unstructured data	Additional IT resources with dedicated servers required	Azure Data Lake and portal analyzes and manages all types of data
Replication and high availability	More resources, licensing, and servers required	Built-in replication and redundancy features available
Application sharing and access to shared resources	File sharing requires additional administration resources	File sharing options available without additional license
Relational data storage	Needs a database server with database admin role	Offers database-as-a-service options
Distributed storage and data access	Expensive storage, networking, and compute resources needed	Azure Cosmos DB provides distributed access

Needs	On-premises	Azure data storage
Messaging and load balancing	Hardware redundancy impacts budget and resources	Azure Queue provides effective load balancing
Tiered storage	Management of tiered storage needs technology and labor skill set	Azure offers automated tiered storage of data

Databases

- Multiple database services to store a wide variety of data types and volumes.
- Have global connectivity and instant data availability

Azure Cosmos DB

- 📝 Globally distributed (= multiple regions) database service
- Supports schema-less data, stores JSON
- 💡 Good for **Always On** applications to support constantly changing data.
  - Helps with failover during regional disaster
  - Transparent multi-master replication, 99.999% high availability for both reads and writes
- 💡 Good for data used by & maintained by users around the globe.

Azure Cache for Redis

- Caches frequently used and static data to reduce data and application latency

Azure SQL Database Options

- **Azure Database for MySQL**: Fully managed and scalable MySQL
- **Azure Database for PostgreSQL**: Fully managed and scalable PostgreSQL
- **Azure Database for MariaDB**: Fully managed and scalable MariaDB
- **SQL server on VMs**: Host SQL servers in own VPNs

Azure SQL Database

- Relational database as a service (DaaS)
- Based on the latest stable version of the Microsoft SQL Server database engine.
- High-performance, reliable, fully managed and secure database

Azure Database Migration Service

- Allows to migrate existing SQL Server to Azure
- Performs all of the required steps.
- Minimal downtime
- Uses the **Microsoft Data Migration Assistant**
  - Generate assessment reports that provide recommendations

Azure Synapse Analytics

- Formerly **SQL Data Warehouse**
- 📝 A cloud data warehouse for the enterprise
- Characterized by high resiliency through automatic scaling.
- Massive parallel processing (MPP) to run complex queries quickly across petabytes of data

Networking

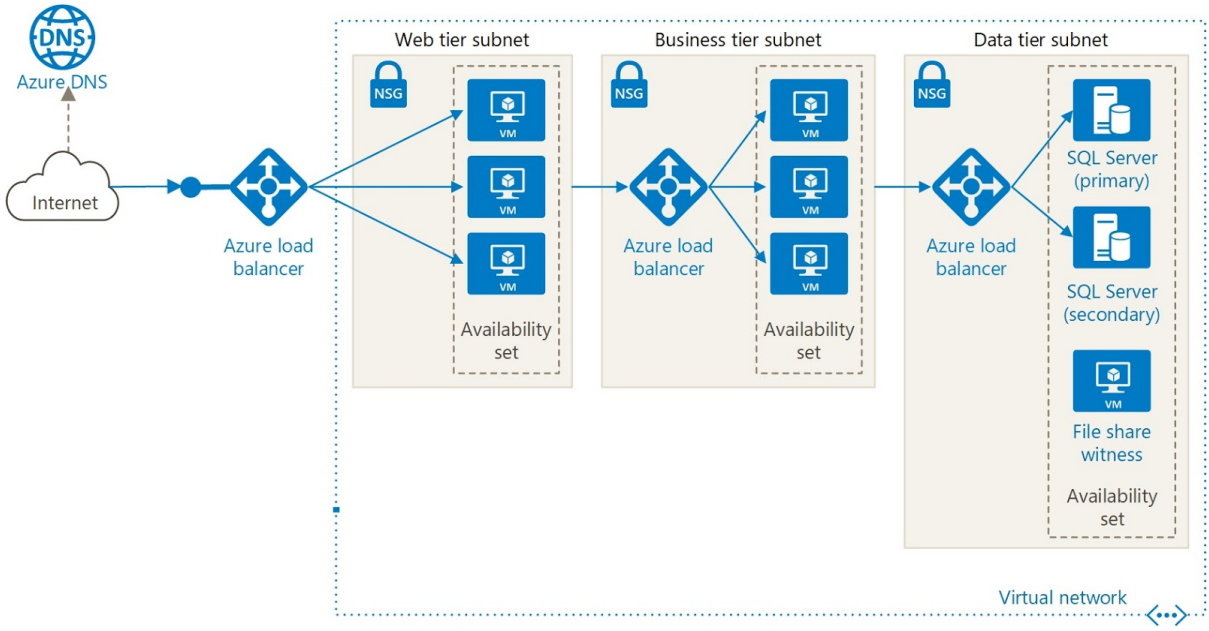
- Helps you optimize application performance & scalability
- Links compute resources and provides access to applications
- Configure & control traffic into and out of Azure efficiently e.g. from on-premises to Azure and vice versa.

Loosely Coupled Architecture

- Architecture behind Azure
- Different services/components that sends and receives data from one another
    - They have little to no knowledge about other components.
- See also micro-services.
- 💡 Recommended because:
    - Can be updated independently: Allows non-breaking changes as long as communication strategy is consistent.
    - Allows services to be changed without significant impact to the rest of the system.
    - Can be scaled proportionally.
        - Scale up/down, out/in only services that are relevant.
        - 💡 Take advantage of asynchronous messaging in Azure for communication for scalability.

N-tier architecture

- Can be used to build loosely coupled architectures.
- Divides an application into two or more logical tiers.
    - A higher tier can access services from a lower tier, but a lower tier should never access a higher tier.
- Tiers help separate concerns and are ideally designed to be reusable.
- Simplifies maintenance: Tiers can be updated or replaced independently, and new tiers can be inserted if needed.
- *Three-tier* refers to an *n-tier* application that has three e.g.
    - Web tier (front-end)
    - Application tier (back-end that runs application logic)
    - Data tier (database)



    - Observe that each tier can access services only from a lower tier.
- Read more

Concepts

Region

- One or more Azure data centers within a specific geographic location
- E.g. East US, West US, and North Europe

Azure Virtual Network

- Enable you to group and isolate related systems
- Logically isolated network on Azure
- Allows Azure resources to securely communicate with • each other • VPNS • the internet • on-premises networks
- ❗ Scoped to a single region
- 💡📝 Virtual networks, subnets, NICs (network interfaces) are free (no $$) resources
    - Public IP addresses, reserved IP, network appliances such as VPN Gateway & Application Gateway are charged.
- You choose which networks your virtual network can reach, whether that's the public internet or other networks in the private IP address space.

Subnet

- A virtual network can be segmented into one or more subnets.
- Help you organize and secure your resources in discrete sections.
- E.g. users interact with the web tier directly, so that VM has a public IP address along with a private IP address.
    - Users don't interact with the application or data tiers, so these VMs each have a private IP address only.

VPN Gateway

- 📝 Also called **virtual network gateway**
- 📝 Provide a secure connection between an Azure Virtual Network and an on-premises location over the internet.
- 📝 Your on-premises network is represented as **Local network gateway** object in Azure.
- E.g. enables you to keep your data tiers in on-premises network, and web tier in cloud.
- Azure manages the physical hardware for you, virtual networks & gateways are configured through software.
- 📝 ❗ Must be deployed in a subnet called gateway subnet.

Network security group (NSG)

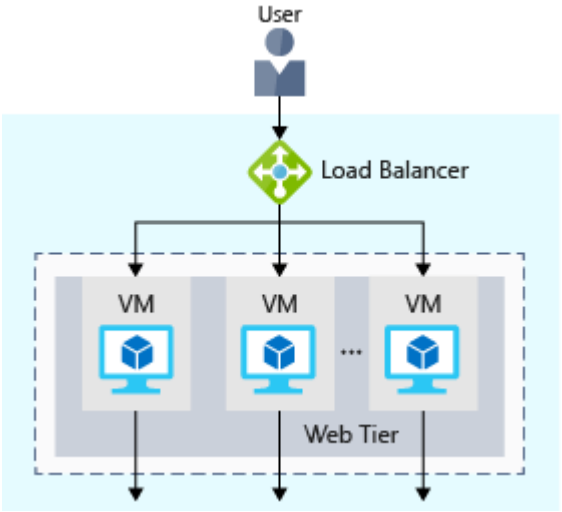
- 📝 Control what traffic can flow through a virtual network.
- Allows or denies inbound network traffic to your Azure resources.
- Can be thought as a cloud-level firewall for your network.
- E.g. web tier allows inbound traffic on ports 22 (SSH) and 80 (HTTP).
    - Port 22 enables you to connect directly to Linux systems over SSH.
        - You might configure VPN access to your virtual network to increase security.
- 💡 Configure a NSG to accept traffic only from known sources, such as IP addresses that you trust.

Other services

- **Azure ExpressRoute**
    - Connects to Azure over high-bandwidth dedicated secure connections
- **Azure Network Watcher**
    - Monitors and diagnoses network issues using scenario-based analysis
- **Azure Virtual WAN**
    - Creates a unified wide area network (WAN), connecting local and remote sites
- Network protection services: • Azure DDoS Protection • Azure Firewall

Load Balancing

- Increases availability & resiliency
    - **Availability**: to how long your service is up and running without interruption
        - High availability (HA), or highly available = a service that's up and running for a long period of time.
        - Five nines availability: Guaranteed to be running 99.999 percent of the time
    - **Resiliency** refers to a system's ability to stay operational during abnormal conditions e.g.
        - Natural disasters, system maintenance, spikes in traffic, threats made by malicious parties
- Load balancer distributes traffic evenly among each system in a pool.
    - The idea is to have additional systems ready, in case one goes down or serving too many users.
- The load balancer becomes the entry point to the user.
    - The user doesn't know (or need to know) which system the load balancer chooses to receive the request.

- 

    - If a VM is unavailable or stops responding, the load balancer stops sending traffic to it.
- In 3-tier architecture, the app and data tiers can also have a load balancer. It all depends on what your service requires.
- You can configure your own load balancer on a VM, or use Azure Load Balancer, Azure Application Gateway, Content Delivery Network or Azure Traffic Manager.

Azure Load Balancer

- Microsoft does the maintenance for you.
    - There's no infrastructure or software for you to maintain
- Define the forwarding rules based on the source IP and port to a set of destination IP/ports.
- Supports inbound and outbound scenarios (internal + external load balancer)
- Provides low latency and high throughput
    - **Low latency**: computer network that is optimized to process a very high volume of data messages with minimal delay (latency).
- Scales up to millions of flows for all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) applications
- Use-cases:
    - incoming internet traffic
    - internal traffic across Azure services
    - port forwarding for specific
    - Outbound connectivity for VMs in your virtual network

Azure Application Gateway

- Better option if all of your traffic HTTP.
- Load balancer designed for web applications
    - It's application layer (OSI layer 7) load balancing since it understands the structure of the HTTP message.
- It uses Azure Load Balancer at the transport level (TCP) behind the scenes.
- Functionalities:
    - **Cookie affinity**
        - Useful when you want to keep a user session on the same backend server.
    - **SSL termination**

        - Can manage your SSL certificates and pass unencrypted traffic to the backend servers to avoid encryption/decryption overhead.
        - Full end-to-end encryption for applications that require that.
    - **Web application firewall**
        - Supports a sophisticated firewall (WAF) with detailed monitoring and logging to detect malicious attacks against your network infrastructure.
    - **URL rule-based routes**
        - Route traffic based on URL patterns, source IP address and port to destination IP address and port.
        - Helpful when setting up a content delivery network.
    - **Rewrite HTTP headers**
        - Addadd or remove information from the inbound and outbound HTTP headers of each request to enable important security scenarios, or scrub sensitive information such as server names.

Azure Content Delivery Network

- Caches content at nodes across the world and provide better performance to end users.
- Allows distributed network of servers that can efficiently deliver web content to users to minimize latency.
- Can be hosted in Azure or any other location.
- 💡 Use-cases:
    - web applications containing multimedia content
    - a product launch event in a particular region,
    - or any event where you expect a high-bandwidth requirement in a region.

DNS

- DNS, or Domain Name System, is a way to map user-friendly names to their IP addresses.
    - E.g. contoso.com might map to IP address of the load balancer at the web tier, `40.65.106.192`.
- You can bring your own DNS server or use Azure DNS

Azure DNS

- A hosting service for DNS domains that runs on Azure infrastructure.
- Provides ultra-fast DNS responses and ultra-high domain availability

Azure Traffic Manager

- DNS based traffic load balancer
- Allows you to make e.g. your website located in the United States, load faster for users located in Europe or Asia.
- Uses the DNS server that's closest to the user to direct user traffic to a globally distributed endpoint.
- It directs the client web browser to a preferred endpoint.
- Can route traffic in a few different ways, using e.g. to the endpoint with the lowest latency.
- You can connect Traffic Manager to your own on-premises networks.

Network latency

- The time it takes for data to travel over the network.
- Typically measured in milliseconds.
- Bandwidth vs Latency
  - Bandwidth = the amount of data that can fit on the connection.
  - Latency = the time it takes for that data to reach its destination.
- Affected by factors such as:
  - type of connection you use
  - how your application is designed
  - biggest factor = distance
- One way to reduce latency is to provide exact copies of your service in more than one region using Azure Traffic Manager.

Load Balancer vs Azure Traffic Manager

- Azure Load Balancer distributes traffic within the same region.
  - Traffic Manager works at the DNS level, and directs the client to a preferred endpoint across regions.
- Both help with resiliency in different ways.
  - Load Balancer detects an unresponsive VM => it directs traffic to other VMs in the pool.
  - Traffic Manager monitors the health of your endpoints, finds an unresponsive endpoint => it directs traffic to the next closest endpoint that is responsive.

Other Azure Services

Web

- **Azure Notification Hubs**
  - Send push notifications to any platform from any back end.
- **Azure API Management**
  - Publish APIs to developers, partners, and employees securely and at scale.
- **Azure Cognitive Search**
  - Fully managed search as a service.
- **Azure SignalR Service**
  - Add real-time web functionalities easily.

Internet of things

- Internet allows any item that's online-capable to access valuable information
  - This ability is for devices to garner & relay information for data analysis is called Internet of Things (IoT).
  - E.g. smart watches, smart thermostats, smart refrigerators. Personal computers used to be the norm.
- **IoT Central**
  - SaaS to manage IoT devices
- **Azure IoT Hub**
  - Takes data, coordinates in and out
  - Integrates sensors, devices and manages them.

    - Messaging hub that provides secure communications between and monitoring of devices
    - **IoT Edge**
        - Allows pushing data analysis models directly onto IoT devices
        - Allowing them to react quickly to state changes without needing to consult cloud-based AI models.

Big data

- Big Data = large volumes of data
    - E.g data from weather systems, communications systems, genomic research, imaging platforms
- Hard to analyze and make decisions
    - Traditional forms of processing and analysis becomes no longer appropriate.
    - Solution: Open source cluster technologies
- Azure supports a broad range of technologies and services to provide big data and analytic solutions.
- **Some examples**
    - Azure Synapse Analytics
    - **Azure HDInsight**
        - Process big data through Hadoop clusters
        - More complete than Azure Data Lake Analytics
    - **Azure Data Lake Analytics**
        - Transform big data on Azure data lake
    - **Azure Databricks**
        - Apache Spark–based analytics service
        - Can be integrated with other Big Data services in Azure.
    - **Data Lake Store**
        - Secure, massively scalable and built to the open HDFS standard
    - **Azure Data Factory**
        - Pipelines for data analysis

Artificial Intelligence

- The core is Machine Learning.
    - Allows computers to use existing data to forecast future behaviors, outcomes, and trends.
    - Computers learn without being explicitly programmed.
- Forecasts or predictions can make apps and devices smarter.
    - E.g. when you shop online, machine learning helps recommend other products you might like based on what you've purchased.

Azure Machine Learning Service

- Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models.
- Can auto-generate a model and auto-tune it for you.
- Lets you start training on your local machine, and then scale out to the cloud

Azure Cognitive services

- AI SaaS services (pre-built APIs)

- **Vision**: Image-processing algorithms to smartly identify, caption, index, and moderate your pictures and videos.
- **Speech**: Convert spoken audio into text, use voice for verification, or add speaker recognition to your app.
- **Knowledge mapping**: Map complex information and data in order to solve tasks such as intelligent recommendations and semantic search.
- **Bing Search**: Add Bing Search APIs to your apps and harness the ability to comb billions of webpages, images, videos, and news with a single API call.
- **Natural Language processing**: Allow your apps to process natural language with pre-built scripts, evaluate sentiment and learn how to recognize what users want.

Azure Machine Learning Studio

- Collaborative, drag-and-drop visual workspace for machine learning solutions
- Allows to build, test, and deploy machine learning models with algorithms and data-handling modules

DevOps

- Brings together people, processes, and technology, automating software delivery to provide continuous value to your users.

Azure DevOps

- 📝 Azure DevOps Services (formerly known as Visual Studio Team Services, or VSTS)
- Provides development collaboration tools including pipelines, Git repositories, configurable Kanban boards, and automated load testing
    - Consists of:
        - **Azure Repos**: Source control for your code.
        - **Azure Pipelines**: providing build & release services for continuous integration & delivery
        - **Azure Boards**: Agile tools that support planning and tracking work items
        - **Azure Test Plans**: Tools for testing your applications
        - **Azure Artifacts**: Allows teams to work with `maven`, `npm` and `NuGet` packages, like purpose as artifactory

Azure DevTest Labs

- 📝 Creates labs consisting of pre-configured Windows & Linux environments or Azure Resource Manager templates.
- Good for testing can use to test or demo your applications directly from your deployment pipelines.

Security

Shared Responsibility Model

- Cloud security is a shared responsibility of both cloud providers and customers.
- Azure has many security certifications from outside auditors.
- **Physical security**

    - Handled by Microsoft
    - Walls, cameras, gates, security personnel
    - Strict procedures for employees
- **Digital security**
    - Handled by customer + Microsoft
    - Azure has tools to mitigate security threats, consumer is responsible to use the tools.
    - E.g. role-based access control, multi factor authentication, encryption, monitoring tools such as login failures, suspicious locations, DDoS protection, real-time telemetry & firewalls.
- ❗ You **always** retain responsibility for: Data, Endpoints, Accounts, Access management (identities)

Cloud computing levels

- 📝 From maximum effort to your side to minimum: IaaS, PaaS, SaaS

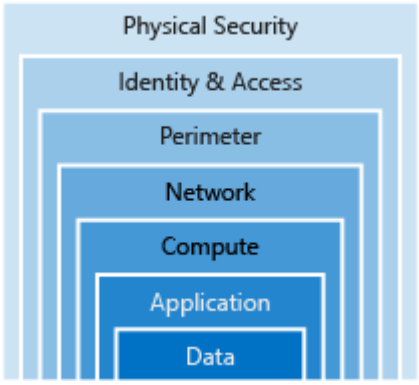
Responsibility	**On-prem**	**IaaS**	**PaaS**	**SaaS**
Data governance & rights management	🤪	🤪	🤪	🤪
Client endpoints	🤪	🤪	🤪	🤪
Account & access management	🤪	🤪	🤪	🤪
Identity & directory infrastructure	🤪	🤪	☁️ 🤪	☁️ 🤪
Application	🤪	🤪	☁️ 🤪	☁️
Network controls	🤪	🤪	☁️ 🤪	☁️
Operating system	🤪	🤪	☁️	☁️
Physical host	🤪	☁️	☁️	☁️
Physical network	🤪	☁️	☁️	☁️
Physical datacenter	🤪	☁️	☁️	☁️

- Cloud provider: ☁️
- Customer: 🤪

Defence in Depth

- Strategy to slow the advance of an attack to get unauthorized access to information.
- Layered approach: Each layer provides protection, so if one layer is breached, a subsequent prevents further exposure.
- Applied by Microsoft, both in physical data centers and across Azure services.

Layers

- 

Data

- In almost all cases attackers are after data.
- Data can be in database, stored on disk inside VMs, on a SaaS application such as a Microsoft 365 app or in cloud storage.
- Those storing and controlling access to data to ensures that it's properly secured
- Often regulatory requirements dictates controls & processes
    - to ensure confidentiality, integrity, and availability.

Application

- Ensure 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.
- Integrate security into the application development life cycle,

Compute

- Secure access to virtual machines.
- Implement endpoint protection and keep systems patched and current.
    - Malware, unpatched systems, and improperly secured systems open your environment to attacks.

Networking

- Limit communication between resources.
- Deny by default.
    - Allow only what is required
- Restrict inbound internet access and limit outbound, where appropriate.
- Implement secure connectivity to on-premises networks.

Perimeter

- Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

Identity and access

- Control access to infrastructure and change control.

- Access granted is only what is needed
- Use single sign-on and multi-factor authentication.
- Audit events and changes.

Physical security

- Building security & controlling access to computing hardware.
- First line of defense

Azure Security Center

- Monitoring service that provides threat protection across all services
  - both in Azure, and on-premises.
- Gives security recommendations based on your configurations, resources, and networks.
  - Part of https://www.cisecurity.org/cis-benchmarks/
- Automatic security assessments through continuous monitoring to identify potential vulnerabilities before they can be exploited.
- Just-in-time access control for ports through Azure Defender
- Analyzes & identifies identify potential inbound attacks
  - then helps to investigate threats and any post-breach activity that might have occurred.
- Control apps
  - Only the apps you validate are allowed to execute.
  - Uses machine learning to detect and block malware from being installed on services
- Helps with compliance through continous assesments & recommendations.

Tiers

Free

- Available as part of any Azure subscription
- Limited to assessments and recommendations of Azure resources only.

Azure Defender

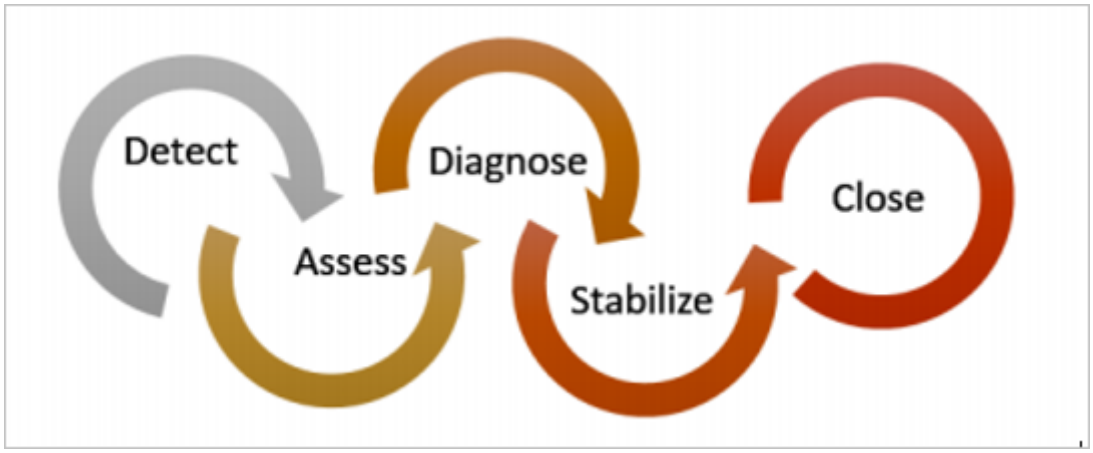
- Formerly known as **Azure security center standard edition**
- Provides a full suite of security-related services including
  - continuous monitoring
  - threat detection
  - just-in-time access control for ports
- $15 per node per month, 30-day free trial available
- ❗ To upgrade to the Standard tier, you must be assigned the role of *Subscription Owner*, *Subscription Contributor*, or *Security Admin*.

Use-cases

Incident response

- 💡 Have an incident response plan in place before an attack occurs.

Incident response stages

- 

- You can use Security Center during the detect, assess, and diagnose stages.

Detect

- Review the first indication of an event investigation.
- E.g. you can use the Security Center dashboard to review the initial verification that a high-priority security alert was raised.

Assess

- Perform the initial assessment to obtain more information about the suspicious activity.
- E.g. obtain more information about the security alert.

Diagnose

- Conduct a technical investigation and identify containment, mitigation, and workaround strategies.
- E.g., follow the remediation steps described by Security Center in that particular security alert.

Recommendations to enhance security

Security policy

- Set of controls that are recommended for resources within that specified subscription or resource group
- You can reduce the chances of a significant security event by configuring a security policy

Recommendations

- Based on security policies for potential vulnerabilities.
- Guide you through the process of configuring the needed security controls.
- E.g. if you have workloads that do not require the Azure SQL Database Transparent Data Encryption (TDE) policy, turn off the policy at the subscription level and enable it only in the resources groups where SQL TDE is required.

Identity and Access (Azure AD)

- Old-school corporate security
  - Network perimeters, firewalls, and physical access controls
  - Does not work good with bring your own device (BYOD), mobile apps, and cloud applications.
- Identity = new primary security boundary
  - Proper authentication and assignment of privileges is critical to maintaining control of your data.
  - Allows to maintain a security perimeter outside physical control
  - Possible to always be sure who has the ability to see & manipulate data and infrastructure with single sign-on and appropriate role-based access configuration.

Authentication and authorization

- Azure provides services to manage both through Azure Active Directory

Authentication

- 📝 Verification of a person or service looking to access a resource.
  - Establishes if they are who they say they are.
- Challenges a party for legitimate credentials, and provides the basis for creating a security principal for identity and access control use.
- Sometimes called az **AuthN**.

Authorization

- 📝 Establishes what level of access an authenticated person or service has.
- Specifies what data they're allowed to access and what they can do with it.
- Sometimes shortened to **AuthZ**.

Azure Active Directory

- Called also as **Azure AD**.
- Cloud-based identity service.
- Can synchronize with existing on-premises Active Directory or can be used stand-alone.
- Allows to share identities in cloud (e.g. Microsoft 365), mobile on-premises applications.
- ❗ 📝 No SLA for free tier, 99.9% for standard & premium
- Some services:
  - **Authentication**.
    - Self-service password reset
    - Multi-factor authentication (MFA)
    - Custom banned password list, and smart lockout services.
  - **Single-Sign-On (SSO)**
  - **Application management**. Manage cloud and on-premises apps using Azure AD Application Proxy, SSO, the My apps portal (also referred to as Access panel), and SaaS apps.
  - **Business to business (B2B) identity services**: Manage guest users and external partners.
  - **Business-to-Customer (B2C) identity services**: Customize and control how users sign up, sign in, and manage their profiles when using apps & services.
  - **Device Management**
    - Manage how your cloud or on-premises devices access your corporate data.

Single sign-on

- More identities for single user
  - = more passwords & harder for users to remember them
  - = more risk of credential-related security incident
  - = harder management: more account lockouts and password reset requests
    - if a user leaves an organization = all identities must be tracked down
- Single sign-on (SSO) = single identity
  - = one password to access across all applications
  - 📝 less effort to manage e.g. if someone leaves an organization
- 📝 Allows you to use third-party e.g. on-prem identities in Azure.

SSO with Azure Active Directory

- Ability to combine data sources into an intelligent **security graph**.
  - Graph enables the ability to
    - provide threat analysis
    - real-time identity protection
- Applied to all accounts in Azure AD (can be synchronized from on-prem).
- Centralized identity provider is good
  - centralized security controls, reporting, alerting, and administration of the identity infrastructure.
- E.g. allows signing into email and Office 365 documents without having to reauthenticate.

Multi-factor authentication

- Called also MFA
- Requires two or more elements for full authentication.
  - Element categories:
    - **Something you know**
      - E.g. a password or the answer to a security question
    - **Something you possess**
      - E.g. a mobile app that receives a notification or a token-generating device
    - **Something you are**
      - E.g. a fingerprint or face scan used often on mobile devices.
- 💡 Enable it wherever possible for more security.

Azure AD MFA

- Integrates also with other third-party MFA providers.
- 💡 Always use at least for Global Administrator role in Azure AD.
- 📝 You can activate conditionally using **Azure AD Identity Protection**
  - E.g. any time a user is signing in from an unknown computer.

Providing identities to services

- Valuable for services to have identities
- Often, and against best practices, credential information is embedded in configuration files.

    - With no security around these configuration files, anyone with access to the systems or repositories can access these credentials and risk exposure.

Service identities in Azure AD

Service principals

- **Identity**: A thing that can be authenticated.
    - e.g. users with user name + password
    - e.g. applications or other servers with secret keys or certificates.
- **Principal**: an identity acting with certain roles or claims
    - You can have same identity but different role which you are executing.
        - E.g. running `sudo` on a Bash prompt or on Windows using "run as Administrator."
    - Groups are often also considered principals because they can have rights assigned.
- **Service principal** = an identity that is used by a service or application that can be assigned roles.

Managed identities

- Azure infrastructure automatically takes care of authenticating the service and managing the account.
- Can be instantly created for any Azure service that supports it
- Allows the authenticated service secure access of other Azure resources just like any AD account.

Roles in Azure

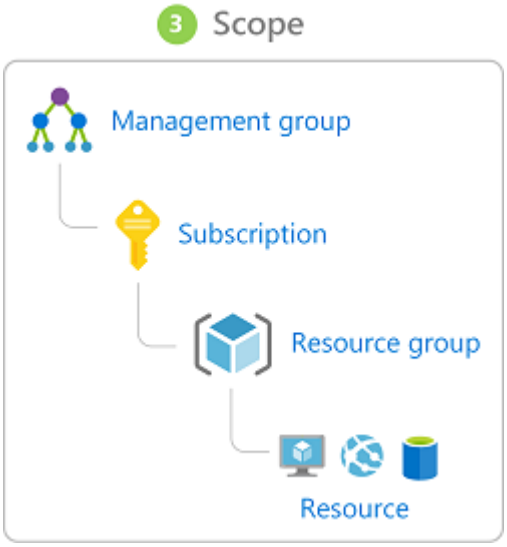
- All co-exists.
- Three categories: classic roles, azure roles, azure ad roles

Classic roles

- 📝 Before Role-based access control was introduced there were 3 roles:
    - **Account Administrator**: ❗ One per Azure account
    - **Service Administrator**: ❗ One per Azure subscription
    - **Co-Administrator**: ❗ 200 per subscription

Role-based access control

- Called also **Azure roles**.
- 📝 Provides fine-grained access management for Azure resources
- **Role**
    - Sets of permissions
    - E.g. "Read-only" or "Contributor"
    - Identities are mapped to roles directly or through group membership.
- **Role assignments**
    - When you are assigned to a role, RBAC allows you to perform specific actions, such as read, write, or delete.
    - E.g.
        - Allow one user to manage VMs in a subscription
        - Allow an application to access all resources in a resource group.

- Can be granted at the service instance level, but they also flow down the Azure Resource Manager hierarchy.
    - Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.
    - 

- 💡 Segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
- Four fundamental Azure roles: **Owner**, **Contributor**, **Reader**, **User Access Administrator**

Azure AD Roles

- On-tenant level
- **Global Administrator**: Person who signs up for Azure AD tenant, can do anything.
- Also **User Administrator**, **Billing Administrator**

Privileged Identity Management

- Also known as **Azure AD Privileged Identity Management (PIM)**
- Includes ongoing auditing of role members
    - needed as their organization changes and evolves.
- Provides:
    - Oversight of role assignments
    - Self-service
    - Just-in-time role activation
    - Azure AD and Azure resource access reviews.

Encryption (Azure Key Vault, Certificates)

- Process of making data unreadable and unusable to unauthorized viewers.
- To use or read the encrypted data, it must be decrypted with a secret key.
- Last & strongest line of defense in a layered security strategy.

Encryption types

Symmetric encryption

- Uses the same key to encrypt and decrypt the data.
- E.g. a desktop password manager application like password orbit encrypts your passwords with your key (derived from your master password & key file). The same key is used when the data needs to be retrieved.

Asymmetric encryption

- Uses a public key and private key pair.
  - Either key can encrypt but a single key can't decrypt its own encrypted data.
  - To decrypt, you need the paired key.
- Used for things like Transport Layer Security (TLS) (used in HTTPS) and data signing.

Encryption ways

Encryption at rest

- Encryption of data at rest
  - Data at rest = data that has been stored on a physical medium
    - e.g. server disk, database or storage account.
- Ensures that data is unreadable without decryption keys/secret
- E.g. if an attacker obtain a hard drive with encrypted data and did not have access to the encryption keys, the attacker would not compromise the data without great difficulty.
- 💡 Good to encrypt e.g.
  - critical financial information, intellectual properties, personal data about customers, employees data, even keys & secrets used for the encryption of the data itself.

Encryption in transit

- Data actively moving from one location to another
  - e.g. across the internet or through a private network.
- Protects the data from outside observers
  - Only the receiver has the secret key that can decrypt the data to a usable form.
- Secure transfer can be handled by several different layers.
  - e.g. in application layer = HTTPS
  - e.g. in network layer = secure channel like virtual private network (VPN)

Encryption on Azure

- For raw storages: Azure Storage Service Encryption
- For virtual machine disks: Azure Disk Encryption
- For databases: Transparent data encryption (TDE)
- For secrets: Azure Key Vault

Azure Storage Service Encryption

- Allows you encrypt raw storage.
- Automatically encrypts your data before persisting it to e.g. Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage
  - and decrypts the data before retrieval.

- The handling of process is transparent to applications.
    - Encryption, encryption at rest, decryption, and key management

Azure Disk Encryption

- Helps you encrypt your Windows and Linux IaaS virtual machine disks.
- Uses BitLocker in Windows and the dm-crypt in Linux to provide volume encryption for the OS and data disks.
- Integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets
    - and you can use managed service identities for accessing Key Vault.

Transparent data encryption (TDE)

- Protection for:
    - Azure SQL Database: Enabled by default.
    - Azure Synapse Analytics
- Performs real-time encryption and decryption at rest of
    - the database
    - associated backups
    - transaction log files
- Uses a symmetric key called the database encryption key.
    - Bring your own key (BYOK) is also supported with keys stored in Azure Key Vault.

Azure Key Vault

- Stores & manages
    - **Secrets**: e.g. passwords, certificates, Application Programming Interface (API) keys, and other secrets.
    - **Keys**: create and control the encryption keys used to encrypt your data.
    - **Certificates**: provision, manage, and deploy your public and private SSL / TLS
        - You can create a policy that directs Key Vault to manage the life cycle of a certificate.
        - You can provide contact information for notification about life-cycle events of expiration and renewal of certificate.
        - You can automatically renew certificates with selected issuers
        - Read more on Azure certificates
- Keys/secrets can be either protected by software or hardware security modules (HSMs)
- Provides secure access, permission control (RBAC) & access logging.
- Simplifies administration e.g. easier to enroll/renew certs.
- Integrate with other Azure services e.g. storage accounts, container registries, event hubs...
    - Applications with managed service identities enabled can automatically and seamlessly acquire the secrets they need.

Azure certificates

Transport Layer Security (TLS)

- Basis for encryption of website data in transit.
- Uses certificates to encrypt and decrypt data.

    - have a life cycle that requires administrator management
    - expired TLS certificates open security vulnerabilities.
- Certificates used in Azure are x.509 v3 that can be y
    - signed by a trusted certificate authority
    - or self-signed
        - not trusted by default as signed by its own creator
        - good for development + testing
- Can contain a private or a public key
    - Keys have an identifiable thumbprint
        - used in the Azure configuration file to identify which certificate a cloud service should use.

Types of certificates

Service certificates

- Attached to a specific cloud service
    - Enables secure communication to and from the service.
    - E.g. if you deploy a web site, you would want to supply a certificate that can authenticate an exposed HTTPS endpoint.
    - Defined in your service definition =>
        - automatically deployed to the VM that is running an instance of your role.
- You can manage service certificates separately from your services
    - You can also upload service certificates to Azure
    - E.g. a developer could upload a service package that refers to a certificate that an IT manager has previously uploaded to Azure.
        - An IT manager can manage and renew that certificate (changing the configuration of the service) without needing to upload a new service package.
- To update a certificate, you don't need to re-deploy a service package
    - Upload a new certificate
    - Change the thumbprint value in the service configuration file.

Management certificates

- Allow you to authenticate with the classic deployment model.
- Allows automation of configuration and deployment of some Microsoft / Azure services.
    - e.g. Visual Studio or the Azure SDK
- Are not related to cloud services.

Network Protection

- Important to secure your network from attacks and unauthorized access
- Use a layered approach
    - not enough to just focus on securing the network perimeter or the network security between services inside a network.
    - helps reduce your risk of exposure through network-based attacks

    - secure your internet-facing resource, internal resources, and communication between on-premises networks
    - Combine multiple Azure networking and security services
        - E.g. use Azure Firewall to protect inbound and outbound traffic to the Internet, and Network Security Groups to limit traffic to resources inside your virtual networks.

Internet protection

- Perimeter of the network
- Focused on limiting and eliminating attacks from the internet.
- Only allow inbound and outbound communication where necessary
    - ensure they are restricted to only the ports and protocols required
        - You can use Azure Security Center for this.

Firewall

- Service that grants server access based on the originating IP address of each request.
- Helps you to provide inbound protection at the perimeter
- You create firewall rule
    - Firewall rule = Ranges of IP addresses to allow access the server.
    - Often includes specific network protocol and port information.

Azure Firewall

- Managed, highly available & scalable, network-level, firewall as a service
- Inbound protection for mainly non-HTTP/S protocols.
    - E.g. Remote Desktop Protocol (RDP), Secure Shell (SSH), and File Transfer Protocol (FTP).
- Outbound protection for all ports and protocols
    - Also application-level protection for outbound HTTP/S.

Azure Application Gateway

- Load balancer that includes a **Web Application Firewall (WAF)**
    - Provides protection from common, known vulnerabilities in websites.
- Designed to protect HTTP traffic.

Network virtual appliances (NVAs)

- Ideal options for non-HTTP services or advanced configurations
- Similar to hardware firewall appliances.

Distributed Denial of Service (DDoS) Protection

- Any resource exposed on the internet is at risk of being attacked by a denial of service attack.
- Attacks attempt to overwhelm a network resource
    - sends so many requests that the resource becomes slow or unresponsive.
- Combine Azure DDoS Protection with application design best practices.

Azure DDoS Protection

- Brings DDoS mitigation capacity to every Azure region
- Protects your Azure applications by monitoring traffic at the Azure network edge before it can impact your service's availability.
- You are notified using Azure Monitor metrics within a few minutes of attack detection.

Service tiers

Basic

- Automatically enabled as part of the Azure platform.
- Always-on traffic monitoring and real-time mitigation of common network-level
- Used by Microsoft's online services use.

Standard

- Tuned specifically to Microsoft Azure Virtual Network resources
- Requires no application changes.
- Dedicated traffic monitoring and machine learning algorithms.
- Policies are applied to public IP addresses associated with resources deployed in virtual networks
  - e.g. Azure Load Balancer and Application Gateway.
- Mitigates:
  - **Volumetric attacks**: The attackers goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
  - **Protocol attacks**: Render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
  - **Resource (application) layer attacks**: Target web application packets to disrupt the transmission of data between hosts.

Traffic inside your virtual network

- Allows you to limit communication between resources to only what is required.

Virtual network security

Network Security Groups (NSGs)

- Provide a list of allowed and denied communication to and from network interfaces and subnets.
  - Used for communication between virtual machines
- Filter network traffic to and from Azure resources in an Azure virtual network.
  - by source and destination IP address, port, and protocol
- Can contain multiple inbound and outbound security rules

Service endpoints

- You can restrict access of services to service endpoints.
  - Allows you to remove public internet access to your services
- Service access become limited to your virtual network.

Network integration

- Integrate on-premises networks <=> services in Azure
- Different ways: VPN, ExpressRoute

Virtual private network (VPN)

- Establish secure communication channels between networks.
- Connects Azure Virtual Network to an on-premises VPN device
- Provide secure communication in-between.

Azure ExpressRoute

- Use to provide a dedicated, private connection between your network and Azure
- Lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider.
- Very secure as it sends traffic over the private circuit instead of over the public internet.
    - You can send this traffic through appliances for further traffic inspection.

Microsoft Azure Information Protection (AIP)

- Helps to classify and optionally protect (encrypt) documents and emails by applying labels.
- Labels can be applied
    - automatically based on rules and conditions
    - or manually
- E.g. 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` configured by the administrator.
- After your content is classified, you can track and control how the content is used. E.g. you can:
    - Analyze data flows to gain insight into your business
    - Detect risky behaviors and take corrective measures
    - Track access to documents
    - Prevent data leakage or misuse of confidential information
- You can purchase AIP either as a standalone solution, or through one of the following Microsoft licensing suites:
    - Enterprise Mobility + Security
    - or Microsoft 365 Enterprise

Microsoft Defender for Identity

- Formerly **Azure Advanced Threat Protection (ATP)**
- Cloud-based security solution that identifies, detects, helps you investigate threats.
- Capable of detecting known malicious attacks and techniques, security issues such as compromised identities, and risks/threats against your network.
- Can be integrated with on-premises Microsoft Defender ATP

Microsoft Defender for Identity components

Microsoft Defender for Identity portal

- Own portal at portal.atp.azure.com
  - ❗ User accounts must be assigned to an Azure AD security group that has access to the Azure ATP portal to be able to sign in.
- Through it you can monitor and respond to suspicious activity.
- Allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors.
- Monitor, manage, and investigate threats in your network environment.

Microsoft Defender for Identity sensor

- Sensors are installed directly on your domain controllers.
- 📝 Monitors domain controller traffic without requiring a dedicated server or configuring port mirroring.

Microsoft Defender for Identity cloud service

- Runs on Azure infrastructure
- Deployed in the United States, Europe, and Asia.
- Connected to **Microsoft Intelligent Security Graph**
  - Threats signals are seamlessly shared across all the services in Microsoft 365 Defender, 6.5 trillion signals daily.
    - **Microsoft 365 Defender**
      - Formerly known as **Microsoft Threat Protection**
      - Consists of different Azure security services
      - E.g. Office ATP, Microsoft Defender ATP, SmartScreen, Exchange Online Protection (EOP)
  - Provides comprehensive security across multiple attack vectors.
  - Allows you to use Microsoft Graph Security API
    - Connects Microsoft security products, services, and partners
    - Can be used to
      - streamline security operations
      - improve threat protection, detection, and response capabilities.

Microsoft Security Development Lifecycle (SDL)

- Set of guidance, best practices, tools, and processes
  - used internally at Microsoft to build more secure products and services.
- Introduces security and privacy considerations throughout all phases of the development process.
- Helps developers
  - build highly secure software
  - address security compliance requirements
  - reduce development costs.

Provide training

- Security is everyone's job
  - E.g. developers, service engineers, and program and project managers.
- Everyone must understand
  - security basics
  - how to build security into software & services
  - attacker's perspective, their goals, and the art of the possible

Define security requirements

- Security requirements must be updated continuously in order to address changes in required functionality and changes to the threat landscape.
- Optimal time to define the security requirements is during the initial design and planning stages.
  - Early planning allows development teams to integrate security in ways that minimize disruption.
- Factors that influence security requirements include, but are not limited to:
  - Legal and industry requirements
  - Internal standards and coding practices
  - Review of previous incidents
  - Known threats
- Track requirements through e.g.
  - work-tracking system
  - telemetry from the engineering pipeline.

Define metrics and compliance reporting

- Essential to define the minimum acceptable levels of security quality
  - and to hold engineering teams accountable to meeting that criteria.
- Good to define as early as possible to apply standards throughout the entire project.
- E.g. all known vulnerabilities discovered with a "critical" or "important" severity rating must be fixed with a specified time frame.
- Track & report security work
  - Allows to have key performance indicators (KPIs)
  - Ensures security tasks are completed
  - Bug/work tracking mechanism should allow for security defects and security work items
    - to be clearly labeled as security
    - marked with their appropriate security severity
- Read more about defining metrics and compliance reporting at:
  - SDL Privacy Bug Bar Sample
  - Add or modify an Azure DevOps field to track work
  - SDL Security Bug Bar Sample

Perform threat modeling

- USE in environments where there is a meaningful security risk.

- Allows development teams to consider, document, and discuss the security implications of designs.
- Applying a structured approach to threat scenarios helps a team.
    1. Effectively and less expensively identify security vulnerabilities
    2. Determine risks from those threats
    3. make security feature selections and establish appropriate mitigations.
- You can apply threat modeling at the component, application, or system level.
- Read more: Threat Modeling

Establish design requirements

- Assurance activities that help engineers implement more secure features, e.g. well engineered for security.
- Methods e.g. cryptography, authentication, and logging.
- Complicated design & security features are likely to result in vulnerabilities.
- Crucial to apply consistently and with a understanding of the protection they provide.

Define and use cryptography standards

- Encrypt in transit to protect data from being alteration & unintended disclosure when moving.
- Making an incorrect choice when using any aspect of cryptography can be catastrophic.
    - Best to develop clear encryption standards with specifics on every element of the encryption implementation.
- Only use industry-vetted encryption libraries: Encryption should be left to experts.
- See the Microsoft SDL Cryptographic Recommendations whitepaper for more.

Manage security risks from using third-party components

- Understand the impact of security vulnerability in third-party components to rest of the system.
- Plan to respond when new vulnerabilities are discovered & consider additional validation
- Read more:
    - Managing Security Risks Inherent in the Use of Third-Party Components
    - Managing Security Risks Inherent in the Use of Open-Source Software

Use approved tools

- Define and publish a list of approved tools and their associated security checks.
    - e.g. compiler/linker options and warnings.
- Strive to
    - use the latest version of approved tools (such as compiler versions)
    - utilize new security analysis functionality and protections.
- Read more:
    - Recommended Tools, Compilers and Options for x86, x64, and ARM processors (whitepaper)
    - SDL Resources

Perform Static Analysis Security Testing (SAST)

- Analyzing source code prior to compilation
    - provides a highly scalable method of security code review

    - helps ensure that secure coding policies are being followed
- Typically integrated into the commit pipeline to identify vulnerabilities each time the software is built or packaged.
- Some offerings replace flawed (e.g. unsafe/banned) functions while developer is coding.
- Read more:
    - Microsoft DevSkim on GitHub
    - Roslyn Security Guard Rules
    - Visual Studio Marketplace
    - Analyzing C/C++ Code Quality by Using Code Analysis
    - Microsoft BinSkim on GitHub

Perform Dynamic Analysis Security Testing

- Performs run-time verification when all components are integrated and running.
- Achieved using a tool
    - e.g. a suite of pre-built attacks
    - e.g. to specifically monitor application behavior for memory corruption, user privilege issues, and other critical security problems.
- Some tools can be more readily integrated into the CI/CD pipeline
    - e.g. such as web app scanning tools
- Other such as fuzzing requires a different approach.
- Read more:
    - Visual Studio Marketplace
    - Automated Penetration Testing with White-Box Fuzzing

Perform penetration testing

- Security analysis of a software system by simulating the actions of a hacker.
- Uncovers potential vulnerabilities resulting from e.g.
    - coding errors, system configuration faults, or other operational deployment weaknesses.
- Finds the broadest variety of vulnerabilities
- Often performed in conjunction with automated and manual code reviews.
- Read more:
    - Attack Surface Analyzer
    - SDL Security Bug Bar Sample

Establish a standard incident response process

- Crucial for addressing new threats that can emerge over time
- The plan should be created in coordination with your organization's dedicated Product Security Incident Response Team (PSIRT).
- Your incident response plan should:
    - Include who to contact if a security emergency occurs
    - Establish the protocol for security servicing (including plans for code inherited from other groups within the organization and for third-party code)
    - Be tested before it is needed
- Read more:
    - Using Azure Security Center for an incident response

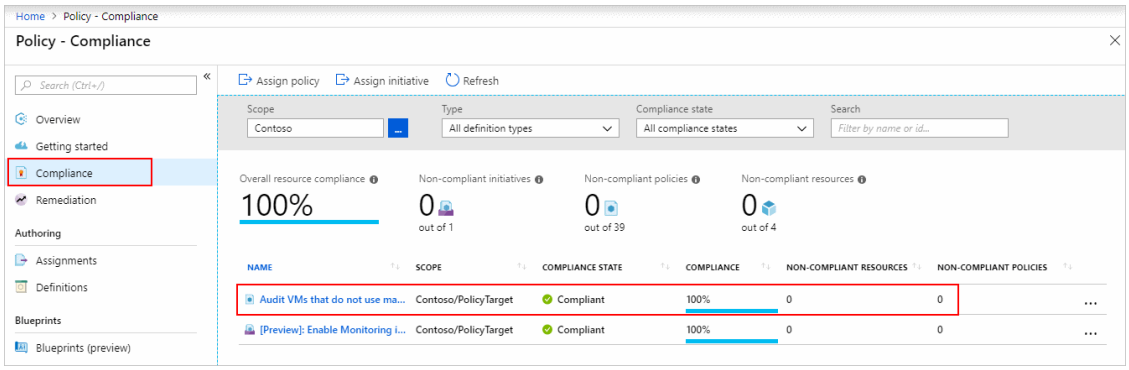
- Microsoft Incident Response and shared responsibility for cloud computing
- Microsoft Security Response Center

Governance

Azure Policy and Azure Blueprints

- Allows you to ensure standards are followed for all IT allocated resources.
- Old way was having the IT team define and deploy all cloud-based assets
  - Bad: reduces the team agility and ability to innovate
  - Instead: enforce and validate your standards while still team(s) to create and own their own resources in the cloud.

Azure Policy

- Each policy enforces rules over specified or all resources.
- Allows your infrastructure stays compliant with e.g.
  - corporate standards, cost requirements, service-level agreements.
- E.g. a policy that allows virtual machines of only a certain size in your environment.
- Evaluates both new and existing resources for compliance.
  - Can deny new uncompliant resources from being created
  - Can stop existing resources from being updated to an uncompliant state.
    - ! Does not remove uncompliant resources!
  - Can only audit existing & new resources
    - Identifying non-compliant resources
    - 

  - Can alter the resource properties.

Azure Policy vs RBAC

- RBAC focuses on user actions at different scopes.
  - e.g. the contributor role for a resource group allows contribution to a resource group
- Azure Policy focuses on resource properties
  - both during deployment and for already-existing resources.
- Azure Policy controls properties such as the types or locations of resources.
- Unlike RBAC, Azure Policy is a **default-allow-and-explicit-deny system**.

Creating a policy

1. Create a policy definition
2. Assign a definition to a scope of resources
3. View policy evaluation results

Policy Definition

- What to evaluate and what action to take
- Has
  - conditions under which it is enforced
  - accompanying effect that takes place if the conditions are met
- E.g. restrict the locations that your organization can specify when deploying resources
- Represented as a JSON file, many samples on GitHub
  - E.g. policy to only allow specific virtual machine sizes:

```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "not": {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "in": "[parameters('listOfAllowedSKUs')]" // replacement
token that will be filled in when the policy definition is applied to a
scope
        }
      }
    ]
  },
  "then": {
    "effect": "Deny"
  }
}
```

Policy effects

- Create or update a resource through Azure Resource Manager are evaluated by Azure Policy first.
- Each policy definition in Azure Policy has a single effect
  - **Deny**: The resource creation/update fails due to policy.
  - **Disabled**: The policy rule is ignored (disabled). Often used for testing.
  - **Append**: Adds additional parameters/fields to the requested resource during creation or update.
    - E.g. adding tags
  - **Audit**, **AuditIfNotExists**: Creates a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
  - **DeployIfNotExists**: Executes a template deployment when a specific condition is met.
    - E.g. run new deployment if SQL is deployed to configure it.

Policy Scope

- Determines what resources or grouping of resources the policy assignment gets enforced on.
- Range from a management group to resource groups.

Policy Assignment

- Policy definition that has been assigned to take place within a specific scope.
- Are inherited by all child resources
- You can exclude a subscope from the policy assignment.
    - e.g. enforce a policy for an entire subscription and then exclude a few select resource groups.
- ❗ May take up to 30 minutes to take effect

Policy Initiatives

- Allows you to organize one or multiple policies.
    - 💡 Recommended only for one policy if you anticipate increasing the number of policies over time.
- Helps you track your compliance state for a larger goal
- Simplify the process of managing and assigning policy definitions
    - E.g. initiative ***Enable Monitoring in Azure Security Center*** has policies:
        - ***Monitor unencrypted SQL Database in Security Center***
            - For monitoring unencrypted SQL databases and servers.
        - ***Monitor OS vulnerabilities in Security Center***
            - For monitoring servers that do not satisfy the configured baseline.
        - ***Monitor missing Endpoint Protection in Security Center***
            - For monitoring servers without an installed endpoint protection agent.

Azure Blueprints

- Makes it easier to adhere to security or compliance requirements, whether government or industry requirements.
- Used often by cloud architects & central information technology groups.
- Azure Blueprints is a declarative way to orchestrating deployment of:
    - Role assignments
    - Policy assignments
    - Azure Resource Manager templates
    - Resource groups
- 💡 Useful in Azure DevOps scenarios as it makes automation easier.
- Implementation
    1. Create an Azure Blueprint
    2. Assign the blueprint
    3. Track the blueprint assignments
- Tracking and auditing: Observes relationship between the definition (what **should** be deployed) and the blueprint assignment (what **was** deployed)
- 😍 Backed by the globally distributed Azure Cosmos database with replication.

Azure Blueprints vs Resource Manager templates

- No need to choose between them & can use both.
    - Each blueprint can consist of zero or more Resource Manager template artifacts.
- Differences:

	Azure Blueprints	Resource Manager templates
Packages	resource groups, policies, role assignments, and Resource Manager template deployments	resource groups, policies, role assignments
Storage	Natively in Azure	Either locally or in source control.
Tracking	Observes what should be deployed and was deployed	There's no active connection/relationship from deployed resources to the template
Deployment scope	Several subscription	Subscription or resource group

Azure Blueprints vs Azure Policy

- A policy is a default-allow and explicit-deny system focused on resource properties during deployment and for already existing resources.- A policy can be included as one of many artifacts in a blueprint definition.
- Blueprints also support using parameters with policies and initiatives.

Monitoring-Azure Monitor and Azure Service Health

- 📝 For auditing, any interaction with Azure is recorded as **Azure Activity Log**

Azure Monitor

- Solution for collecting, analyzing, and acting on telemetry from cloud and on-premises environments.
- Helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.
- Aggregated view of different monitoring data
- Increases availability and performance
- Can be integrated with different services
    - 📝 E.g. Azure Service Health to e.g. see if an issue is global.
- Azure Monitor has its own features for visualizing monitoring data
    - Also can send data different tools such as Dashboards, Views, Power BI

Data sources

- **Application monitoring data**
    - About the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data**
    - Data about the operating system on which your application is running.

    - This could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data**
    - Data about the operation of an Azure resource.
- **Azure subscription monitoring data**
    - Data about the operation and management of an Azure subscription.
    - Data about the health and operation of Azure itself.
- **Azure tenant monitoring data**
    - Data about the operation of tenant-level Azure services, such as Azure Active Directory.

Diagnostic settings

- Collected from e.g. virtual machines and web apps
- **Activity Logs** record when resources are created or modified
- **Metrics** tell you how the resource is performing and the resources that it's consuming.
- Some data types are: guest-level monitoring, performance counters, event logs, crash dumps, sinks, agents.

Application Insights

- Monitors availability, performance, and usage of web applications
- Leverages data analysis platform in Log Analytics for queries
- Can diagnose errors without waiting for a user to report them.
- Integrates with variety of development tools

Azure Monitor for containers

- Monitors the performance of workloads in Kubernetes clusters in Azure Kubernetes Service (AKS).
- Collecting memory and processor metrics from controllers, nodes, and containers
- Container logs are also collected.

Azure Monitor for VMs

- Monitors on-premises, or cloud VMs at scale
- Analyzes the performance and health of Windows and Linux VMs
    - also their different processes and interconnected dependencies on other resources & external processes.

Responding

Azure Alerts

- Azure Monitor proactively notifies you of critical conditions using.
    - e.g. sending a text or email to an administrator who is responsible for investigating an issue.
- Alert rules based on metrics can provide alerts in almost real-time, based on numeric values.
- Alert rules based on logs allow for complex logic across data, from multiple sources.

Autoscale

- Uses Autoscale to ensure that you have the right amount of resources running to manage the load on your application effectively.
- Enables you to create rules that use metrics from Azure Monitor, to determine when to scale
    - Help reduce your Azure costs by removing resources that are not being used.
    - You provide the logic that determines when Autoscale should increase or decrease resources.

Azure Service Health

- 📝 Comprehensive view of the health status of Azure
- Notifies you about Azure services that affect you with impact & information.
    - 📝 Can set-up automatic alerts
- Guides you to prepare for planned maintenance & other changes that could affect the availability of your resources.
- Consists of:
    - **Azure Status**: Global view of the health state of all Azure services.
    - **Service Health**: customizable dashboard that tracks the Azure services you're using in the regions where you use them
        - Shows events such as ongoing service issues, upcoming planned maintenance, or relevant Health advisories
    - **Resource Health**: helps you diagnose and obtain support when an Azure service issue affects your resources.
        - Personalized dashboard of your resources' health
        - Provides technical support to help you mitigate problems
        - Shows when you resources was unavailable because of Azure problems
            - Helps you to understand if an SLA was violated.

Economies

Economies of Scale

- Ability to do things more efficiently or at a lower-cost per unit when operating at a larger scale.
- Cloud providers are large businesses leveraging the benefits of economies of scale.
    - Providers can then pass the savings on to their customers.
- Cloud providers can also make deals with local governments and utilities to get tax savings
    - lowering the price of power, cooling, and high-speed network connectivity between sites.
- Enables end users (customers) to acquire hardware at a lower cost than what you could achieve on your own.

Capital Expenditure-CapEx vs Operational Expenditure-OpEx

- Before: up-front cost in hardware and infrastructure to start or grow a business (CapEx)
    - With cloud: Use services without significant upfront costs or equipment setup time (OpEx)
- 📝 Hybrid solution = combine both in cloud with using both on-premises (CapEx) and cloud (OpEx)

- Also possible to have CapEx in cloud with e.g. Azure Reserved VM Instances
- CapEx model is also sometimes use in cloud

Capital Expenditure (CapEx)

- Spending of money on physical infrastructure up front
  - and then deducting that expense from your tax bill over time.
- An upfront cost, which has a value that reduces over time.

Costs of CapEx

- E.g. server, storage, network, backup & archive, organization continuity and disaster recovery, datacenter infrastructure, technical personal.

Benefits of CapEx

- Plan your expenses at the start of a project or budget period.
- Your costs are fixed, meaning you know exactly how much is being spent.
- 💡 Appealing when you need to predict the expenses before a project starts due to a limited budget.

Operational Expenditure (OpEx)

- Spending money on services or products now and being billed for them now.
  - There's no upfront cost: You pay for a service or product as you use it
- Deduct expense from your tax bill in the same year.

Billing of OpEx

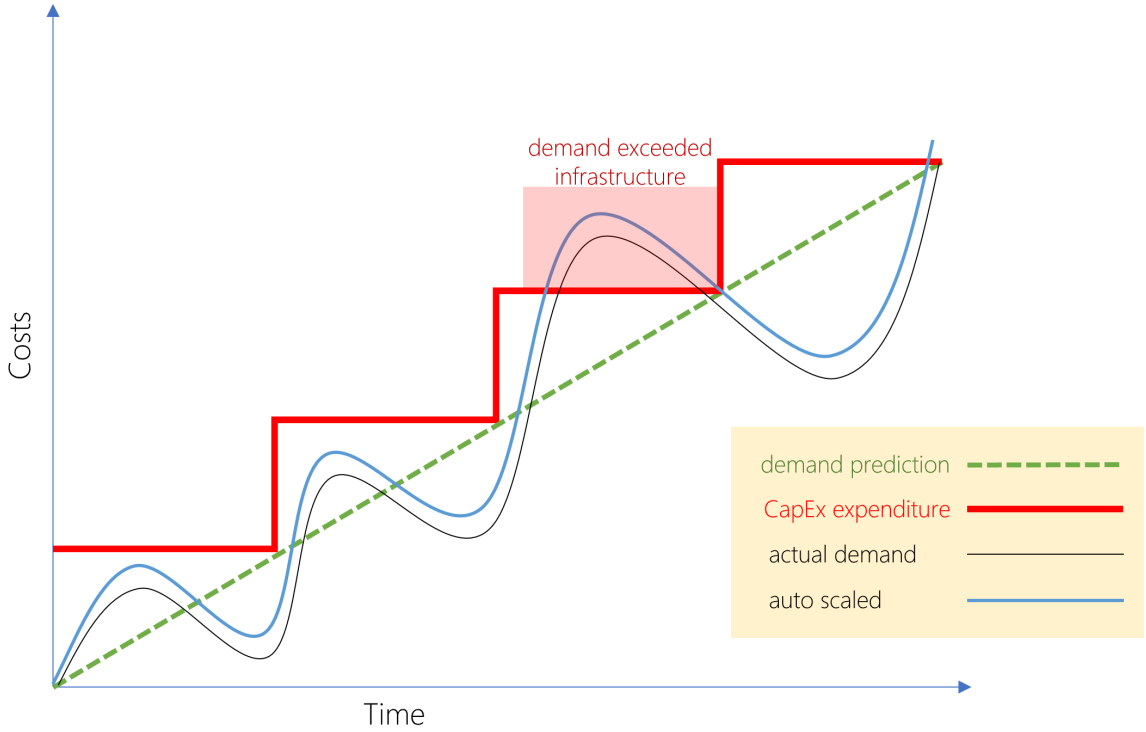
- As soon as the provider provisions resources, billing starts
  - your responsibility to de-provision the resources when they aren't in use so that you can minimize costs.
- Cloud computing can bill in various ways e.g.
  - Number of users, CPU usage time, allocated RAM, I/O operations per second (IOPS), and storage space.
- Billing at the user or organization level.
- **Pay-per-use** (or subscription model)
  - Designed for both organizations and users
  - billed for the services used, typically on a recurring basis
  - E.g. when using a dedicated cloud service, you could pay based on server hardware and usage.

Costs of OpEx

- Leasing software and customized features
- Scaling charges based on usage/demand instead of fixed hardware or capacity.
- 💡 Plan for backup traffic and disaster recovery traffic to determine the bandwidth needed.

Benefits of OpEx

- CapEx challange: Demand and growth can be unpredictable and can outpace expectation



- Companies wanting to try a new product or service don't need to invest in equipment
  - Instead, they pay as much or as little for the infrastructure as required.
- OpEx is particularly appealing if the demand fluctuates or is unknown
- Enables **cloud agility**
  - Ability to rapidly change an IT infrastructure to adapt to the evolving needs of the business
  - Manage your costs dynamically, optimizing spending as requirements change.
  - E.g. service peaks one month => pay more, demand drops next month => pay less

Azure Costs and Tools

- There's always the challenge of balancing cost against performance.

Usage meters

- Used to determine Azure costs for each billing period
- When you provision an Azure resource, Azure creates one or more meter instances for that resource.
  - They are charged based on usage
- The meters track the resources' usage, and generate a usage record that is used to calculate your bill.
- Each meter tracks a particular kind of usage.
- The usage that a meter tracks correlates to a number of **billable unit**s.
  - Those units are charged to your account for each billing period.
- E.g. when you deploy a single virtual machine:
  - Azure might have following meters tracking:
    - Compute Hours, IP Address Hours
    - Data Transfer In, Data Transfer Out
    - Standard Managed Disk, Standard Managed Disk Operations
    - Standard IO-Disk, Standard IO-Block Blob Read, Standard IO-Block Blob Write, Standard IO-Block Blob Delete

    - ! If you de-allocate a VM you'll not pay for it. However, your persistent disks remain in your subscription that you pay for.
- Meters and pricing vary per product
- Often have different pricing tiers based on the size or capacity of the resource.

Billing

- At the end of each monthly billing cycle:
    - the usage values are charged to your payment method
    - the meters are reset
- Check the billing page in the Azure portal:
    - summary of your current usage
    - any invoices from past billing cycles

Factors affecting costs

Resource type

- Costs are resource-specific
- The usage that a meter tracks and the number of meters associated with a resource depend on the resource type.
- The rate per billable unit depends on the resource type you are using.

Services

- Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers
- Azure usage rates and billing periods can differ between them.
- Some subscription types also include usage allowances, which affect costs.
- Different billing structure apply to products and services from third-party vendors are available in the Azure Marketplace

Location

- Varies based on popularity, demand, and local infrastructure costs in a location.
- See choose low cost locations and regions.

Bandwidth

- Bandwidth = data moving in and out of Azure datacenters.
- Mostly inbound data (data to Azure) transfers are free.
    - Outbound data transfers (from Azure to outside) costs based on Billing Zones
        - Moving data between Azure regions counts as outbound data transfer.

Billing zone

- A Zone is a geographical grouping of Azure Regions for billing purposes.
- Each zone has different outbound data transfer prices.
- Zones:
    - Zone 1: United States, US Government, Europe, Canada, UK, France, Switzerland

    - Zone 2: East Asia, Southeast Asia, Japan, Australia, India, Korea
    - Zone 3: Brazil, South Africa, UAE
    - DE Zone 1: Germany.

Tools

Azure pricing calculator

- Free web-based tool: https://azure.microsoft.com/en-us/pricing/calculator/
- Get estimate costs without deploying and running those services or without manually pricing out each service from the Azure service pricing pages.
    - 📝 Can save results in your Azure account, export as Excel or shared as an URL.
- You select Azure services and modify properties and options of the services.
    - Outputs the costs per service and total cost for the full estimate
    - Modifiable properties:
        - **Region**: E.g. Southeast Asia, central Canada, western United States, northern Europe...
        - **Tier**: E.g. Free Tier, Basic Tier, etc.
        - **Billing Options**: Per type of customers and subscriptions for a chosen product.
        - **Support Options**: Included / paid support options.
        - **Programs and Offers**: Available price offerings according to your customer or subscription type.
        - **Azure Dev/Test Pricing**: Available if subscription is based on a Dev/Test offer.
- On the pricing calculator page, you'll see several tabs:
    - **Products**. Lists all Azure services, 📝 allows you put together services for your estimate.
        - Customizable e.g. for VMs you select region, OS, size, running hours.
    - **Example Scenarios**. Common solutions to add all the components, e.g. VMs + load balancer.
    - **Saved Estimates**. Your previously saved estimates.
    - **FAQ**

Azure Advisor

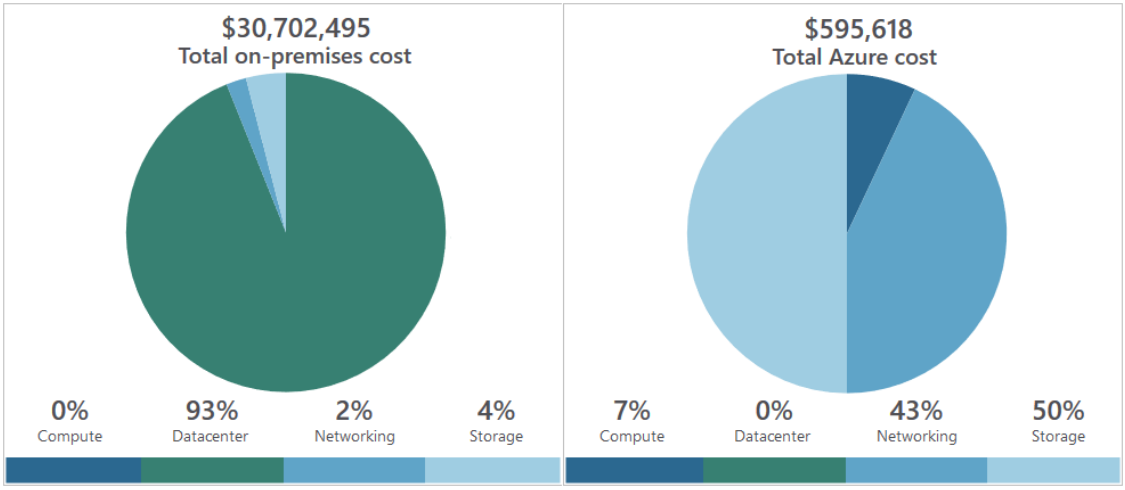
- Free service that provides recommendations on
    - 📝 high availability, security, performance, operational excellence, and cost.
- Analyzes your deployed services and gives personalized recommendations.
- Cost recommendation areas:
    - **Reduce costs by eliminating unprovisioned Azure ExpressRoute circuits**
        - Finds circuits that have been in the provider status of Not Provisioned for more than one month.
        - Recommends deleting the circuit.
    - **Buy reserved instances to save money over pay-as-you-go**
        - Analyzes your VM usage over the last 30 days,
        - Determines & shows if you could save money in the future by purchasing reserved instances.
        - Shows the regions and sizes where you potentially have the most savings
    - **Right-size or shutdown underutilized virtual machines**
        - Monitors your virtual machine usage for 14 days.
        - Identifies underutilized virtual machines, allows you to scale down/iin to reduce your costs.

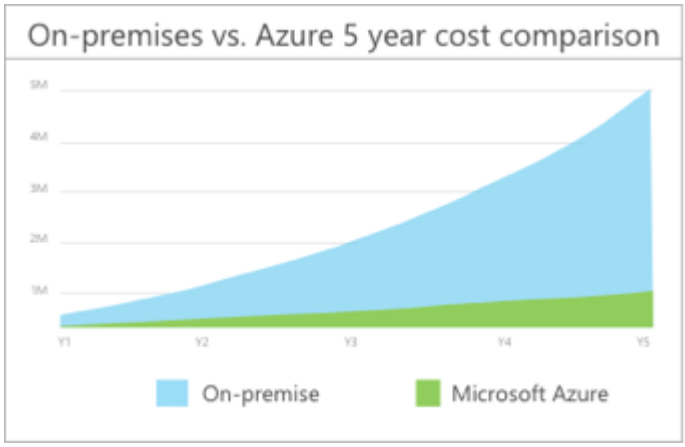
    - E.g. VMS with average CPU utilization of <= 5% (adjustable up to 20%)
    - E.g. network usage <= 7 MB for +4 days.

Azure Cost Management

- Free tool that for greater insights into costs.
- You can set budgets, schedule reports, and analyze your cost areas.
    - Historical breakdowns of services
    - Tracking against budget that's set

Azure TCO calculator

- Compares on-prem vs cloud costs.
    1. Describe your infrastructure: servers, databases, storages, networking
    2. Adjust assumptions: adjust values for e.g. VM costs, electricity costs, IT labor costs.
    3. Compare costs & see how much you can save
    - 

    - 

- Web-based tool: azure.microsoft.com/pricing/tco
- TCO = Total Cost of Ownership

Cost Optimization Best Practices

Save on infrastructure

Use Azure credits

- $50 per month for Visual Studio Professional, $150 per month for Visual Studio Enterprise

- Separate Azure subscription under your account that renews each month while you remain an active Visual Studio subscriber
- ❗ No SLA, development and testing only
  - Azure suspends VMs used for production or that run more than 120 hours.

Use spending limits

- ❗ Not available on pay-only subscriptions, only for subscriptions with a monthly Azure credits.
- Helps you to prevent from exhausting the credit on your account within each billing period.
  - Resets after each period
- Activated by default, you can adjust the spending limit as desired or turn it off.

Use reserved instances

- Purchase Windows/Linux VMs for one-year or three-year terms with payment of entire period or monthly.
- Allows to save save up to 70 to 80 percent off the pay-as-you-go cost
- 💡 Good for static and predictable virtual machines.

Choose low-cost locations and regions

- Prices vary across locations and regions
- 💡 Good idea to use them in locations and regions where they cost less.
- ❗ Consider also that moving data between locations can cost extra and total price can get more expensive.
  - Good idea to have them in same region to reduce egress (outgoing network bandwith) traffic between them.

Research available cost-saving offers

- Keep up to date with offers, and switch to ones with most benefits
- See Azure Updates for updates, roadmaps and announcements.

Right-size underutilized virtual machines

- Over-sized virtual machines are a common unnecessary expense on Azure
- Azure Cost Management & Azure Advisor might recommend right-sizing or shutting down VMs.
- Right-sizing = resizing it to a proper size
  - E.g. downgrading `Standard_D4sv3` with 90% idle VM to `Standard_D2sv3` to reduce 50% cost.
- ❗ Resizing a VM requires it to be stopped, resized, and then restarted.
  - 💡 Takes a few minutes so plan for an outage, or shift your traffic to another instance

Deallocate virtual machines in off hours

- No need to run VMs every hour of every day if they're only used during certain periods.
- Shut down when not in use and start back up on a schedule
  - Saves money on compute costs, 📝 but you still pay for storage.
- Can use automation accounts or **auto-shutdown** feature on a virtual machine to schedule automated shutdowns.

Delete unused virtual machines

- Saves you on infrastructure costs but also potentially on licensing and operations.

Migrate to PaaS or SaaS services

- Evaluate your architecture if it's beneficial to move to PaaS.
    - Azure operateS hardware efficiently and therefore offer PaaS services cheaper.
- Neutral evolution is to go from IaaS to PaaS iteratively when moving to cloud.
- PaaS saves on resource and operational costs.
- Effort varies
    - SQL Server to => Azure SQL Database is very easy.
    - Hard to move multi-tier application to a container or serverless-based architecture
        - No quick winds from cost-saving perspective
- Azure Architecture Center can give ideas for transforming application & best-practices.

Save on licensing costs

Linux vs. Windows

- The cost of the product can be different based on the OS you choose.
- Useful to compare pricing to determine whether you can save money.

Azure Hybrid Benefit

- Allows you to use existing
    - on-premises Windows Server licenses on Azure VMs. (***Azure Hybrid Benefit for Windows Server***)
    - SQL Server licenses for Azure SQL Databases. (***Azure Hybrid Benefit for SQL Server***)
- Pay only linux rates for those virtual machines
- ❗ Through Software Assurance licenses only.

Use Dev/Test subscription offers

- If you're on Enterprise Agreement: Enterprise Dev/Test
    - Else Pay-As-You-Go (PAYG) Dev/Test
- Discounts:
    - No license charges for Windows workloads, only billing you at the Linux rate
    - SQL Server & other software under Visual Studio subscription (formerly known as MSDN) are included.
- ❗ Users (except testers) must be covered under a Visual Studio subscription
- ❗ Only for non-production workloads

Bring your own SQL Server license

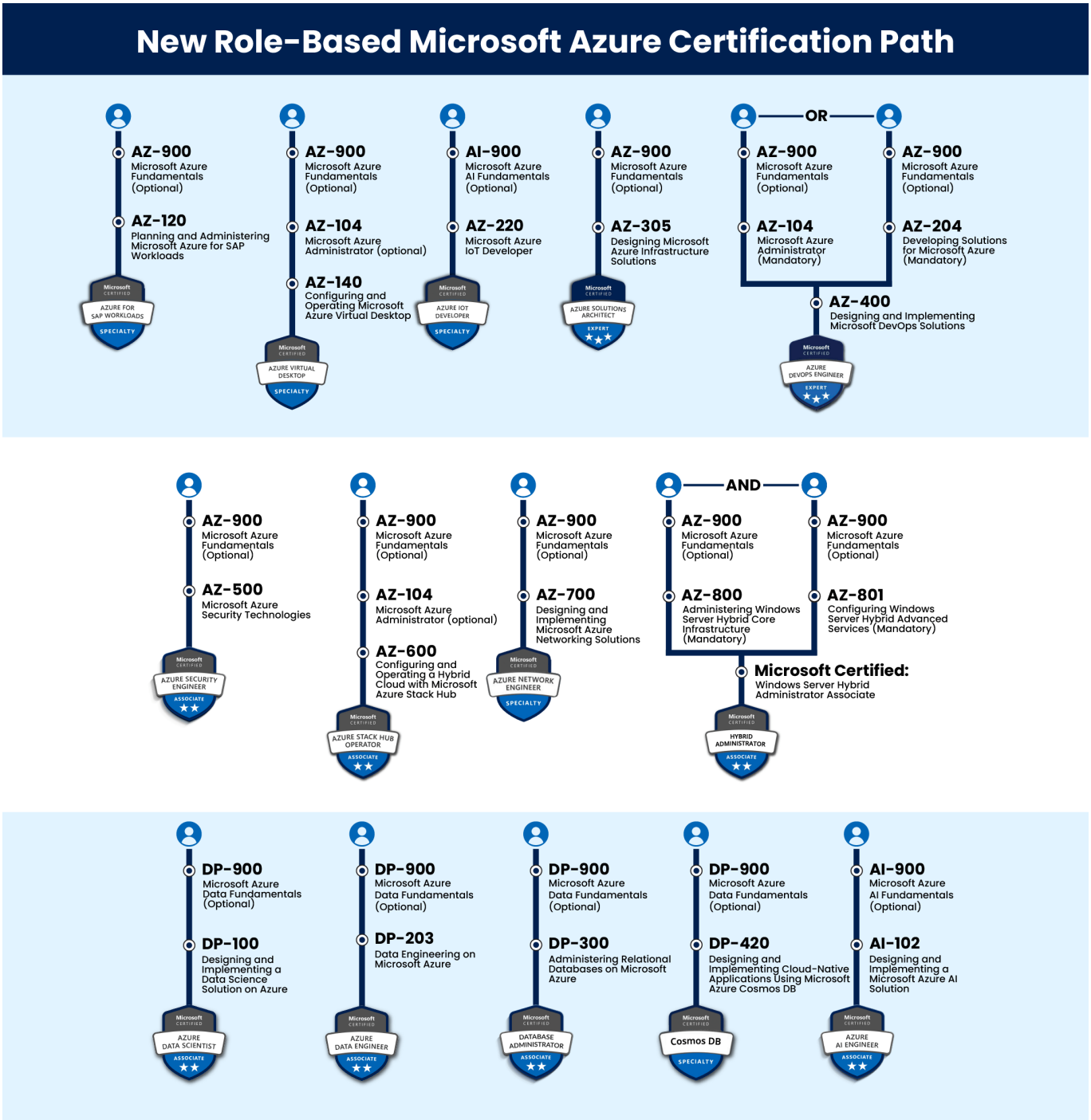
- ❗ For customers with Enterprise Agreement
- Use unused on-prem licenses on Azure
- In Azure marketplace search for `BYOL SQL`

Use SQL Server Developer Edition

- Free product for nonproduction use.
- Has all the same features that Enterprise Edition has
- Can find SQL Server images for Developer Edition on the Azure Marketplace for development & testing.

Use constrained instance sizes for database workloads

- Many have high requirements for memory, storage, or I/O bandwidth.
    - Often have low requirements for CPU core counts
- Can use VM sizes with lower vCPU count
- Databases like SQL Server and Oracle are licensed per CPU
    - Allows you to reduce licensing cost by up to 75 percent.



Thank You.