Syllabus

Candidates for this exam have skills and experience working with an area of information technology, such as infrastructure management, database management, or software development.

- Describe cloud concepts (25–30%)
- Describe Azure architecture and services (35–40%)
- Describe Azure management and governance (30–35%)

Describe cloud concepts (25–30%)

Describe cloud computing

• Define cloud computing
• Describe the shared responsibility model
• Define cloud models, including public, private, and hybrid
• Identify appropriate use cases for each cloud model
• Describe the consumption-based model
• Compare cloud pricing models Describe the benefits of using cloud services
• Describe the benefits of high availability and scalability in the cloud
• Describe the benefits of reliability and predictability in the cloud
• Describe the benefits of security and governance in the cloud
• Describe the benefits of manageability in the cloud Describe cloud service types
• Describe infrastructure as a service (IaaS)
• Describe platform as a service (PaaS)
• Describe software as a service (SaaS)
• Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS)

Describe Azure architecture and services (35–40%)

Describe the core architectural components of Azure

• Describe Azure regions, region pairs, and sovereign regions
• Describe availability zones
• Describe Azure datacenters
• Describe Azure resources and resource groups
• Describe subscriptions
• Describe management groups
• Describe the hierarchy of resource groups, subscriptions, and management groups

Describe Azure compute and networking services

• Compare compute types, including container instances, virtual machines (VMs), and functions
• Describe VM options, including Azure Virtual Machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop
• Describe resources required for virtual machines
• Describe application hosting options, including the Web Apps feature of Azure App Service, containers, and virtual machines
• Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and Azure ExpressRoute
• Define public and private endpoints

Describe Azure storage services
• Compare Azure storage services
• Describe storage tiers
• Describe redundancy options
• Describe storage account options and storage types
• Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync
• Describe migration options, including Azure Migrate and Azure Data Box
Describe Azure identity, access, and security
• Describe directory services in Azure, including Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra and Azure Active Directory Domain Services (Azure AD DS) • Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication, and passwordless
• Describe external identities and guest access in Azure
• Describe Conditional Access in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
• Describe Azure role-based access control (RBAC)
• Describe the concept of Zero Trust
• Describe the purpose of the defense in depth model
• Describe the purpose of Microsoft Defender for Cloud

Describe Azure management and governance (30–35%)

Describe cost management in Azure
• Describe factors that can affect costs in Azure
• Compare the Pricing calculator and the Total Cost of Ownership (TCO) calculator
• Describe the Azure Cost Management and Billing tool

• Describe the purpose of tags

Describe features and tools in Azure for governance and compliance
• Describe the purpose of Azure Blueprints
• Describe the purpose of Azure Policy
• Describe the purpose of resource locks
• Describe the purpose of the Service Trust Portal

Describe features and tools for managing and deploying Azure resources
• Describe the Azure portal
• Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell
• Describe the purpose of Azure Arc
• Describe Azure Resource Manager and Azure Resource Manager templates (ARM templates)

Describe monitoring tools in Azure
• Describe the purpose of Azure Advisor
• Describe Azure Service Health
• Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights

Study Material

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.

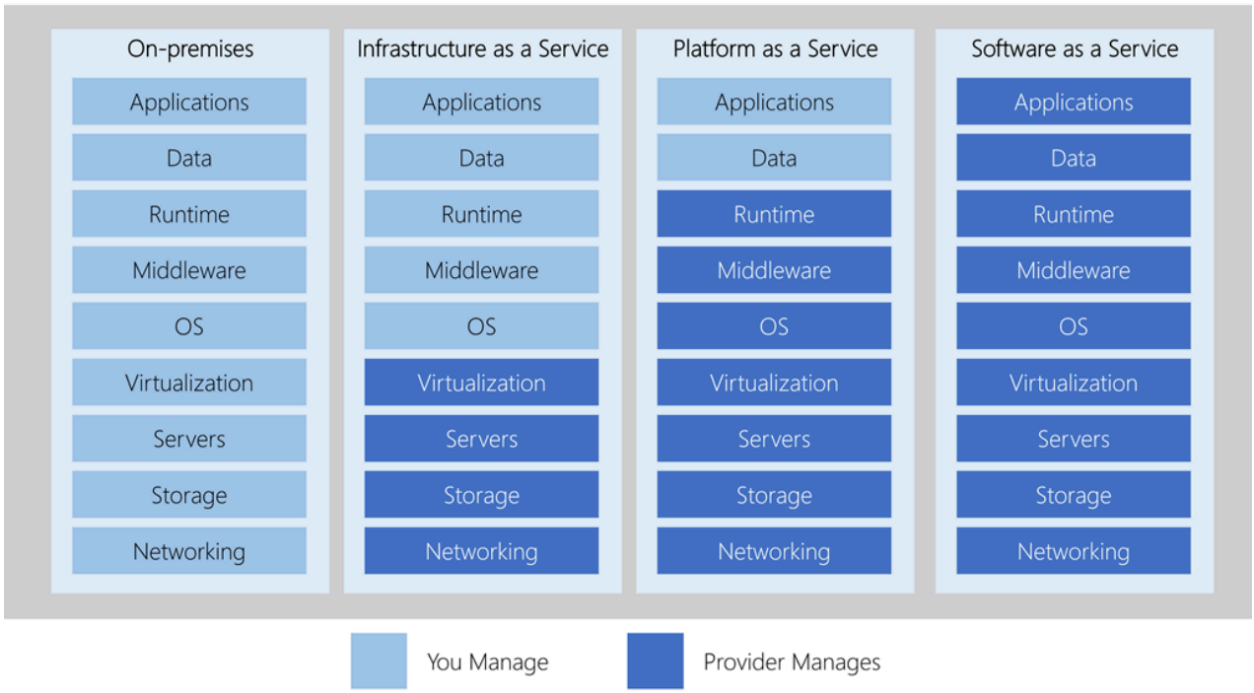
Serverless computing

- 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.

Shared Responsibility Model:-



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 certification is 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.

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

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.

Account, Subscription, Support and Billing

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

Subscription

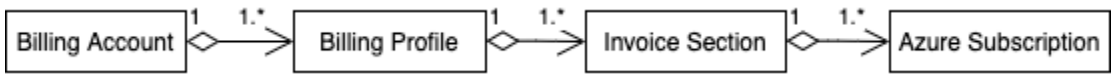
- Used to create and use Azure services

- 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

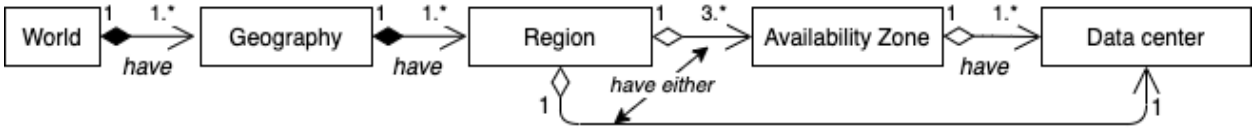
- You'll receive a monthly invoice with payment instructions provided
    - You also can get set up for multiple invoices.
- Customize billing
    - Allows you to e.g. have single invoice for organization but organize charges by department, team, or project.
    - Billing structure:
        - 

        - 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

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

Azure Resource Manager (Resources & Resource Groups & 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

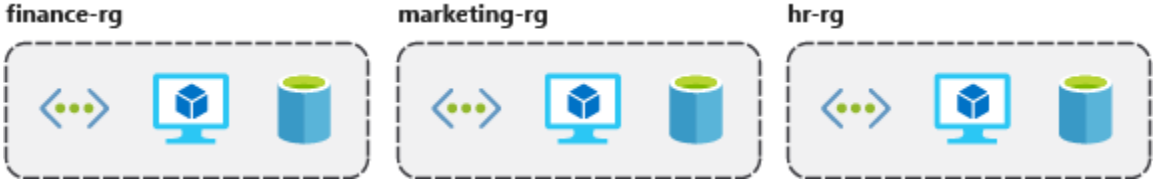
- Also an Azure resource so it can have locks, tags, RBAC permissions etc.
    - It's free!
- Logical container for resources deployed on Azure.
- Tied to a region & subscription itself.
    - 📝 But can contain resources from different regions
        - ❗ If region the RG goes down, the management of 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

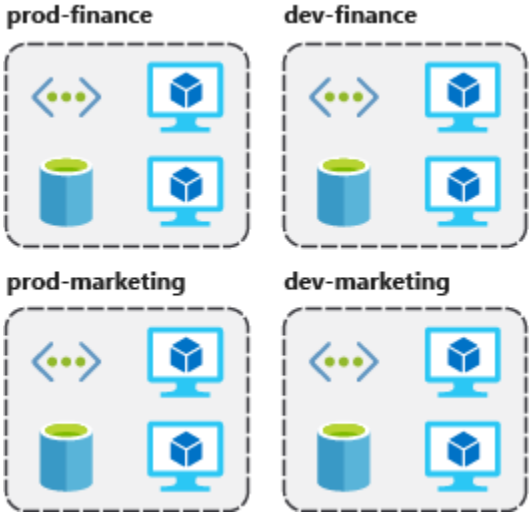
- ❗ Some services has specific limitations or requirements to move from one resource group to another
- ❗ Can't be nested.
- Can see history of the deployments to a resource group

Organizing resource groups

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

- By environment (prod, qa, dev)
  - 

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

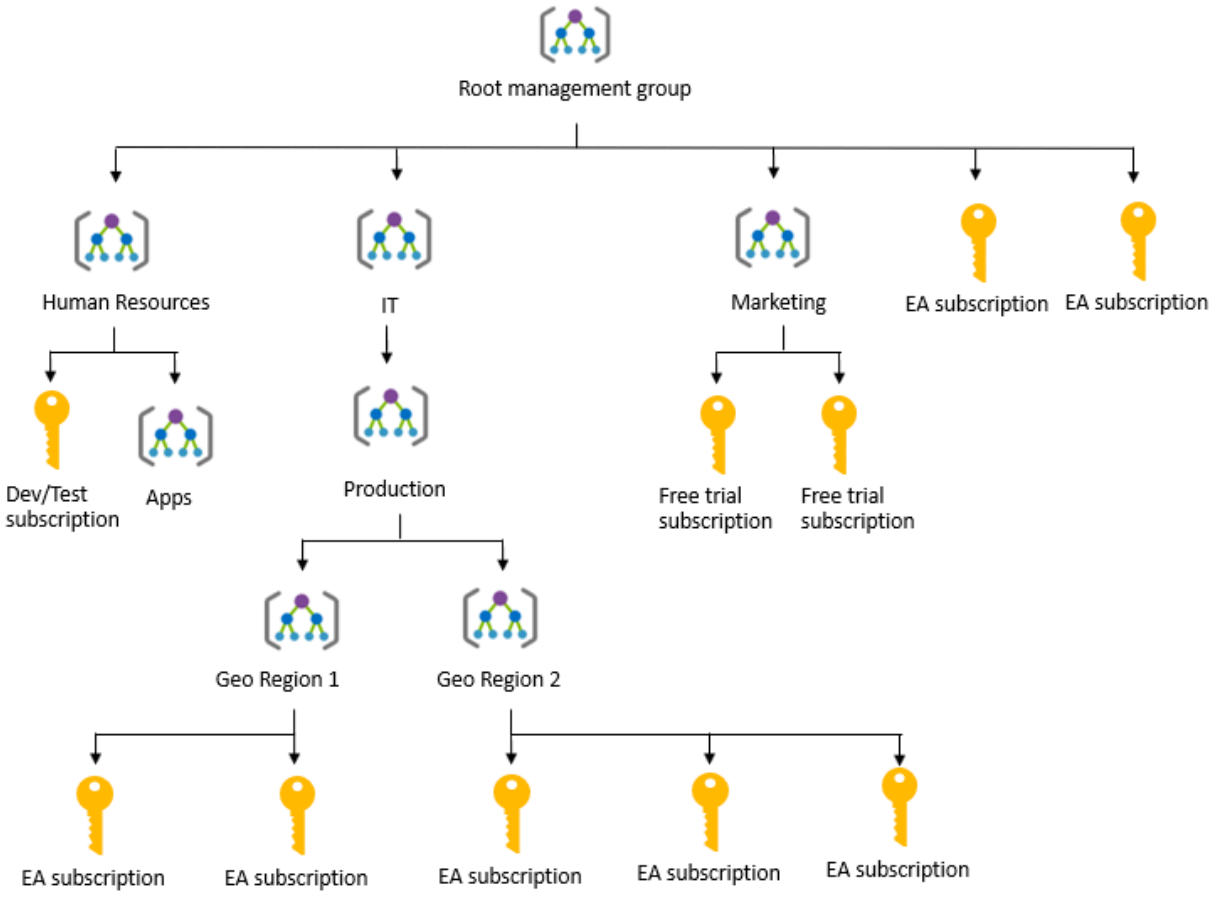
- Combining strategies e.g. environment and department:
  - 

- 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.

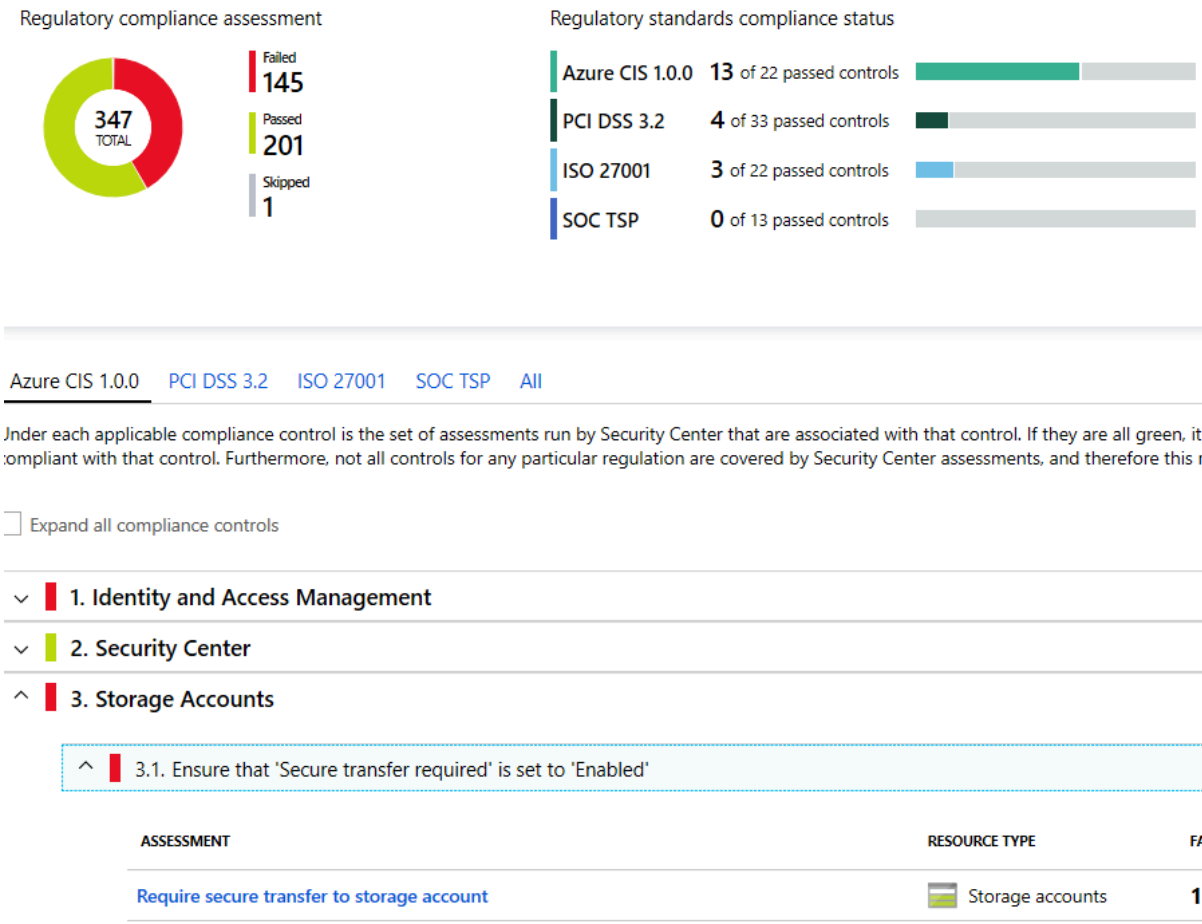
Compliance Manager

- 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:
        - Information provided by Microsoft to auditors and regulators e.g.ISO 27001, ISO 27018, and NIST.
        - Information that Microsoft compiles internally for its compliance with regulations (such as HIPAA and the EU GDPR).

        - 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

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:
    i. Starts a pool of compute VMs for you
    ii. Installs applications and staging data
    iii. Runs jobs with as many tasks as you have
    iv. Identifies failures
    v. Requeues work
    vi. 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. :
    i. Convert an existing application to one or more containers and then publish one or more container images to the Azure Container Registry.
    ii. Deploy the containers to an AKS cluster using the Azure portal or the command line.
    iii. Azure AD controls access to AKS resources.
    iv. You access SLA-backed Azure services, such as Azure Database for MySQL, via OSBA.
    v. 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
    - A pod is a group of one or more containers that share the same network namespace and can communicate with eachother via 'localhost'
    - 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 Application Programming Interface (API)
    - 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.
- Azure services:
    - Azure SQL Database
    - Azure Cosmos DB (SQL API)

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.
- Azure services:
    - Azure Cosmos DB (MongoDB API, Cassandra API)
    - Azure Table Storage
    - Azure Queue Storage

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 services:
    - Azure Blob Storage
    - Azure File Storage
    - Azure Data Lake Storage
    - Azure Disk Storage

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
- Schema-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
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

Azure HDInsight

- 📝 A big data and advanced analytics service providing open-source analytics, processing and integrations with big data frameworks, including:
    - Apache Hadoop
    - Apache Spark
    - Apache HBase
    - Apache Kafka

- Useful for big data tasks such as ETL (Extract, Transform, Load), data warehousing, machine learning, and IoT.

Networking

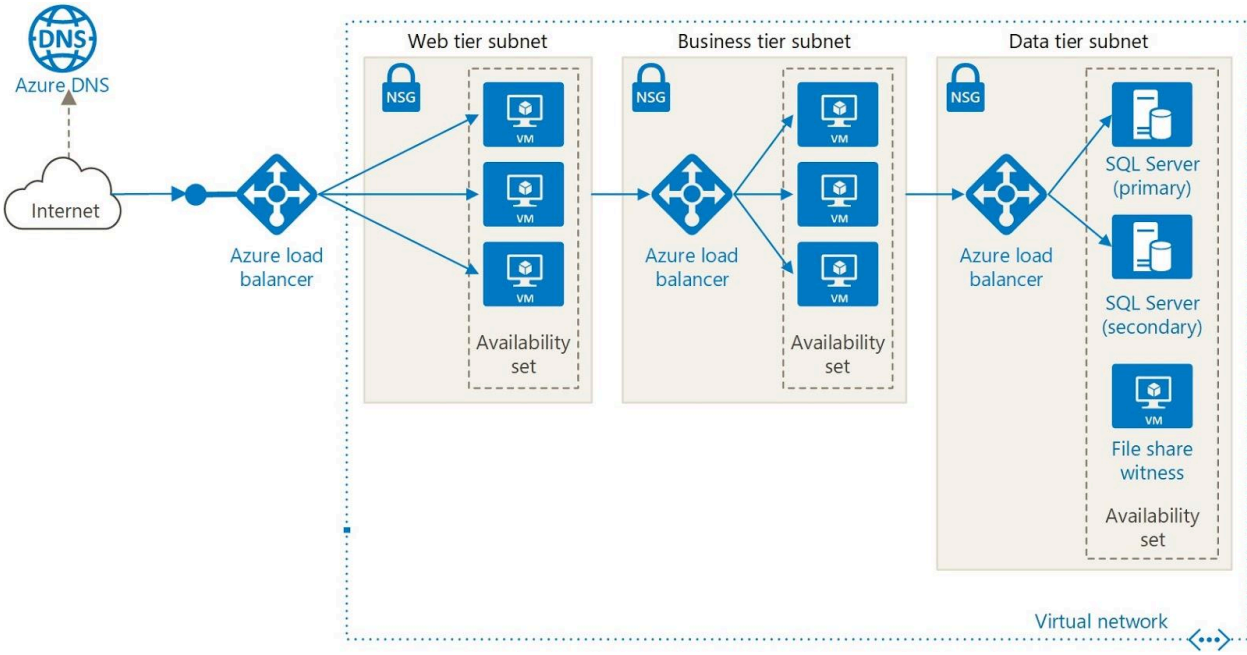
- Helps you optimize application performance & scalability
- Links compute resources and provides access to applications
- Configure & control traffic into and out of Azure efficiently e.g. from on-premises to Azure and vice versa.

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)

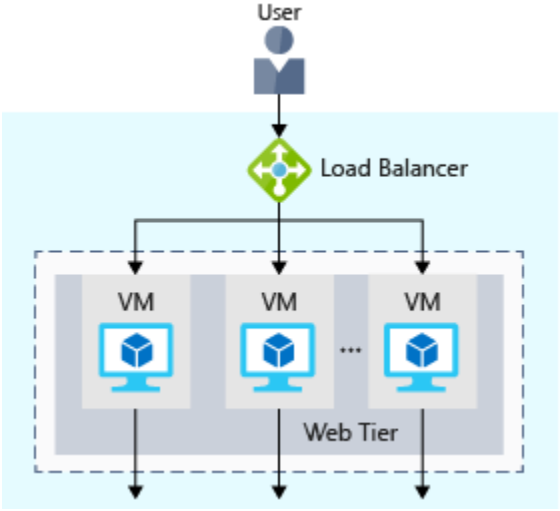
- 📝 Control what traffic can flow through a virtual network.
- Allows or denies inbound network traffic to your Azure resources.
- Can be thought as a cloud-level firewall for your network.
- E.g. web tier allows inbound traffic on ports 22 (SSH) and 80 (HTTP).
    - Port 22 enables you to connect directly 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

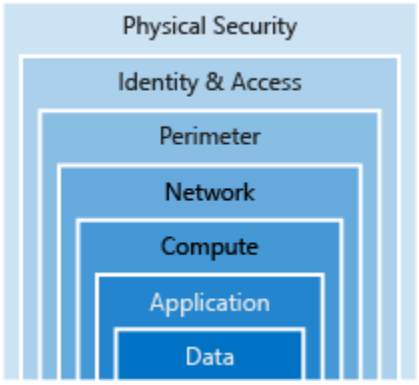
- 📝 Creates labs consisting of pre-configured Windows & Linux environments or Azure Resource Manager templates.
- Good for testing can use to test or demo your applications directly from your deployment pipelines.

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

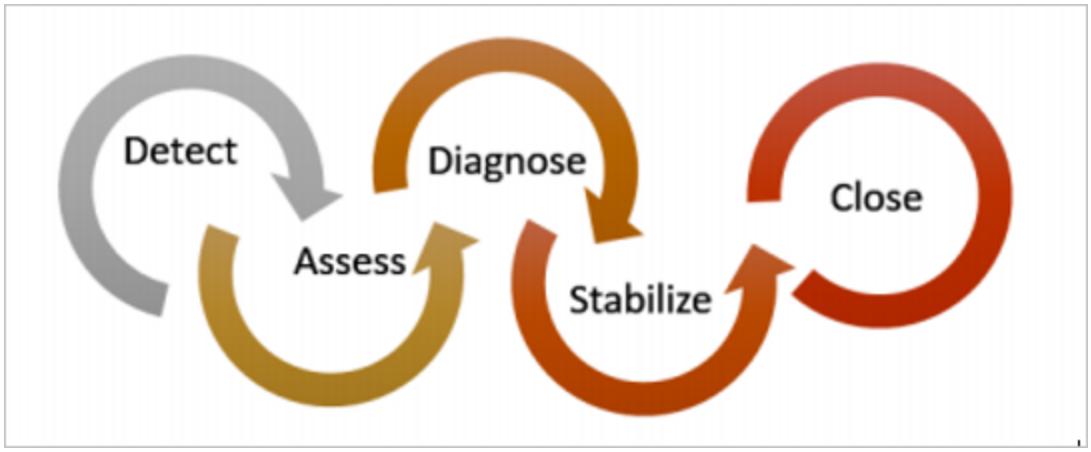
- Formerly known as Azure security center standard edition
- Provides a full suite of security-related services including
    - continuous monitoring
    - threat detection
    - just-in-time access control for ports
- $15 per node per month, 30-day free trial available
- ❗ To upgrade to the Standard 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

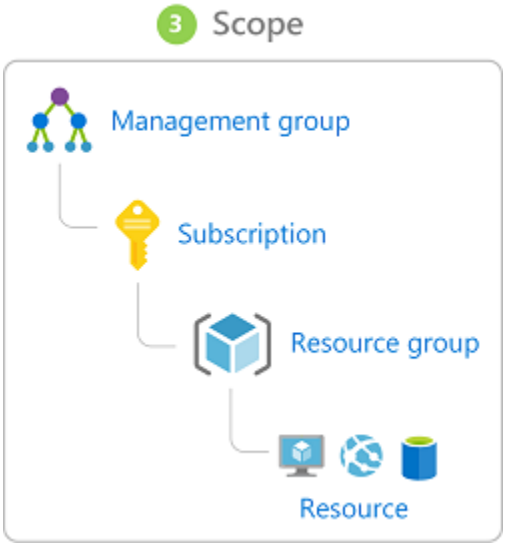
- All co-exists.
- Three categories: classic roles, azure roles, azure ad roles

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.