

Azure AZ-900 Study Notes

Cloud Basics

- What's Cloud Computing: Delivery of computing services over the internet on a pay-as-you-go basis, allowing you to rent resources like compute power and storage. The cloud provider manages the infrastructure, offering on-demand access to resources for fast, scalable solutions.
-
- Why Move to the Cloud:
 -
 - Faster feature delivery and innovation
 - Provides on-demand access to unlimited resources and services like AI, machine learning, and analytics
 - Allows richer user experiences with devices and applications
- Benefits of Cloud Computing:
 -
 - Cost-Effective: Pay for what you use, no upfront infrastructure costs, and better cost predictability.
 - Scalable: Easily scale resources up or out based on demand, either manually or automatically.
 - Elastic: Automatically adjust resources to meet current demand, only paying for what you use.
 - Current: Automatic updates and hardware management handled by the provider.
 - Reliable: Built-in fault tolerance with data backup and disaster recovery.
 - Global: Datacenters worldwide enable redundancy, compliance, and fast local service.
 - Secure: Provides physical and digital security with advanced tools and controls to mitigate security risks.

Cloud Deployment Models (Public vs Private vs Hybrid Cloud)

- Public Cloud: Most common model, where everything runs on the cloud provider's hardware. It's highly scalable, pay-as-you-go, and requires minimal technical expertise. However, it may not meet specific security or regulatory requirements, and you don't control the hardware.
- Private Cloud: Hosted in your own datacenter, providing self-service access to resources. You maintain full control over security and configuration, meeting strict legal and compliance needs, but it requires high upfront costs, maintenance, and limits agility.
- Hybrid Cloud: Combines public and private clouds, allowing you to use the most appropriate model for different workloads. It offers flexibility, supports legacy systems, and enables cloud-bursting. However, it is more expensive and complex to manage than a single model.

Compute & Serverless & Storage

- Cloud is like Electricity: Pay only for what you need without managing upgrades or scaling, similar to how electricity is provided.
- Cloud Computing: Renting resources like storage or CPU from another company's computers, offering flexibility and cost-efficiency—paying only for what you use.
- Cloud Providers: Companies like Microsoft, Amazon, and Google provide services like compute power, storage, networking, and analytics.

Compute Power:

- Virtual Machines (VMs): Emulated computers with full control but more maintenance responsibility.
- Containers: Lightweight, isolated environments without a guest OS, highly portable, and quick to start.

Serverless Computing

- Run code without managing servers, paying only for execution time, ideal for automation.

Storage

- Cloud-based storage scales to meet needs, offering services for files or databases based on usage.

IaaS vs PaaS vs SaaS

Three categories of cloud computing

- IaaS (Infrastructure as a Service): Provides instant computing infrastructure like VMs, storage, and operating systems, offering maximum control. You rent hardware, sharing responsibility with the provider. Common uses include workload migration, test and development, and storage management.
- PaaS (Platform as a Service): Provides a platform for building, testing, and deploying applications without managing infrastructure. Common uses include development frameworks and analytics tools, enabling rapid application development with scalability and high availability.
- SaaS (Software as a Service): Centrally hosted and managed software delivered via subscription. Examples include Office 365 and Skype, providing users with applications without the need for installation or maintenance.

Cost and Ownership

- **IaaS**: Pay-as-you-go; users manage software, OS, and applications while the provider handles infrastructure.
- **PaaS**: Pay-as-you-go; users manage applications, while the provider handles OS and services.
- **SaaS**: Subscription-based; provider manages and maintains the entire application.

Management responsibilities

- **IaaS**: User manages OS, data, and apps.
- **PaaS**: User manages apps and data.
- **SaaS**: User just uses the software.

Cloud Compliance

- Provider can help you comply with regulations and standards
- Think about:
 - How compliant is the cloud provider when it comes to handling sensitive data?
 - How compliant are the services offered by the cloud provider?
 - How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?
 - What terms are part of the privacy statement for the provider?
- Providers help with compliance, and certifications include CJIS, GDPR, HIPAA, ISO/IEC 27018, SOC, NIST, and others. Ensure the provider's compliance with specific standards and regulations for your data.

Scaling

- **Vertical Scaling (Up/Down):** Increase or decrease memory, storage, or compute power on existing VMs.
- **Horizontal Scaling (Out/In):** Add or remove VMs to distribute workloads. Scale down when resources are not needed to save money.
- **Cost Optimization:** Tools like Azure Advisor and Azure Cost Management help optimize cloud usage and costs.

Azure Basics

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

Azure services

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

How Azure works

- It uses virtualization

- Uses an abstraction layer called hypervisor.
 - Separates tight coupling between hardware (CPU, RAM, GPU..) and its operating system
 - Emulates a real computer in a virtual machine
 - Can run multiple virtual machines in same time
 - Optimizes capacity of abstracted hardware
 - Can run any OS such as Windows, Linux & macOS
- Azure repeats virtualization in massive scale
 - Each data center has many racks filled with servers
 - Each server includes a hypervisor to run multiple virtual machines.
 - A network switch provides connectivity to all those servers
 - One server in each rack runs a special software called fabric controller
 - Each fabric controller is connected to another software called as orchestrator
 - Orchestrator manages everything in Azure, including responding user requests
 - Users requests using Azure API
 - Azure API can be reached in many ways including Azure Portal
 - Orchestrator packages everything it's needed and sends to package & request to fabric controller.

Purchasing & Licensing Options

Azure purchasing options

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

Licensing

Free-trial

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

Pay-as-you-go

- Get billed for services as you use them

CSP (Cloud Solution Provider)

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

Azure in Open licensing

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

Enterprise Agreement (EA)

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

Account, Subscription, Support and Billing

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

Subscription

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

Multiple Azure Subscriptions

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

Billing

- You'll receive a monthly invoice with payment instructions provided
 - You also can get set up for multiple invoices.
- Customize billing
 - Allows you to have single invoice for organization e.g. but organize charges by department, team, or project.
 - Billing structure:
 - Each billing account has billing profile
 - Each billing profile has different invoice sections
 - Each invoice section can be coupled to different subscriptions.
 - Each invoice section is a line item on the invoice that shows the charges incurred that month

Support

- Free Support:
 - 24/7 access to online documentation, community support, and demo videos.
 - Tools like Azure Quickstart Center, Azure Service Health, and Azure Advisor for insights and recommendations.
 - Basic support: Free for all users, including billing and subscription management, unlimited support tickets, and community support via forums and Twitter.
- Paid Support Plans:
 - Developer: For non-critical workloads; 1-day response time.
 - Standard: For production workloads; 1-hour response for critical cases.
 - Professional Direct: For business-critical workloads; 1-hour response, priority tracking, and access to technical experts.
 - Azure Premier Support: Offers faster response times, architecture/code reviews, and onsite support.

Azure Data Centers

- **Global Reach:** Azure operates over 100 secure and redundant facilities worldwide, allowing you to deploy resources in regions while complying with local laws. You can choose the region but not a specific datacenter.
- **Regions:** Each region contains multiple datacenters linked by low-latency networks, ensuring scalability and redundancy. Some services are region-specific.
- **Special Regions:**
 - **Azure Government:** Isolated for U.S. government use.
 - **China Regions:** Operated through a partnership with 21Vianet.
- **Geographies:** Regions belong to specific geographies defined by geopolitical boundaries (Americas, Europe, Asia Pacific, Middle East, Africa) with unique compliance and data residency rules.

- **Availability Zones:** Separate datacenters within a region, providing high availability through redundancy. Zones have independent power, cooling, and networking to maintain fault tolerance.
- **Region Pairs:** Azure regions are paired (e.g., West US and East US), ensuring that if one region fails, services failover to its pair. They help minimize downtime during disasters and planned updates, with automatic geo-redundant storage available in some services.

Interacting with Azure

- **Azure Portal:** A browser-based graphical interface to create, manage, and monitor Azure resources. Includes wizards, customizable dashboards, notifications, and access to the Azure Marketplace for provisioning services.
- **Azure PowerShell & CLI:** Command-line tools for automation and resource management. PowerShell is for Windows/Linux/Mac, while CLI is cross-platform.
- **Azure Cloud Shell:** A browser-based command-line interface accessible via the portal, offering Bash or PowerShell experiences with persistent storage.
- **Azure Mobile App:** Manage and monitor Azure resources on the go, available for iOS and Android.
- **Azure SDKs:** Programmatically manage Azure resources with SDKs for various languages, and access public preview features.
- **Azure Advisor:** A free built-in tool offering recommendations on availability, security, performance, and cost, downloadable in various formats.
- **Dashboards:** Customizable, high-level views of your Azure environment with role-based access control (RBAC) for sharing.
- **Preview Features:** Test pre-release Azure features and get notified about updates via the portal or Azure Updates pages.
- Preview portal through preview.portal.azure.com
 - Typical portal preview features provide performance, navigation, and accessibility improvements

Service-level Agreements (SLA)

- **SLAs (Service Level Agreements):** Formal documents that define performance standards for Azure services. They include performance targets (e.g., uptime and connectivity), and outline compensation (service credits) if performance is below standards. No SLAs for free or shared-tier services.
- **Key SLA Characteristics:**
 - Performance Targets:** Specific to each product, such as uptime guarantees (99.9% to 99.999%).
 - Service Credits:** Compensation if uptime is lower than SLA guarantees.
- **Composite SLA:** Combining SLAs from multiple services results in a lower overall SLA. You can improve this with fallback paths (e.g., using a queue as a backup).

- **Application SLAs:** Customize your own SLAs for Azure applications, aiming for high availability (e.g., 99.99%) using self-healing solutions.
- **Resiliency:** Ability to recover from failures, including high availability and disaster recovery, which ensures services can continue despite issues.
- **High Availability:** Refers to system uptime. More availability increases complexity and costs, and interdependencies between services can impact the overall SLA.

Azure Resource Manager (Resources & Resource Groups & Management Groups)

- **Azure Resource:** Anything you create in an Azure subscription, such as VMs or CosmosDB. Use a consistent naming convention (e.g., cloudarchitecture-prod-infrastructure-rg) for easy identification. Provides fine-grained access management with RBAC, and supports tagging for organization and automation. Resources can have up to 50 tags, and some can be moved between resource groups or subscriptions.
- **Tagging:** Helps organize, search, and automate resources (e.g., shutdown tags for cost-saving automation). Not all resource types support tags, and tags are not inherited from parent resources.
- **Resource Locks:** Prevent accidental modification or deletion of critical resources. Read-only or delete locks can be applied, and they override RBAC permissions. Only "Owner" or "User Access Administrator" can create/delete locks.
- **Resource Groups:** Logical containers for organizing resources, tied to a region. Deleting a group deletes all resources within. Supports RBAC, tags, and locks, and helps with organizing by environment, type, or department. A resource can only belong to one group, and groups cannot be nested.
- **Management Groups:** Used to group multiple subscriptions, inheriting RBAC assignments and policies for better enterprise management.

Compliance in Azure

- **Microsoft Privacy Statement:** Explains how Microsoft processes personal data across services, websites, apps, and devices.
- **Microsoft Trust Center:** Provides detailed information about security, privacy, and compliance across Microsoft cloud products, along with curated resources.
- **Service Trust Portal:** Offers downloadable audit reports and compliance guides to help manage regulatory requirements.
- **Compliance Manager:** A free risk assessment dashboard that tracks compliance status, provides recommendations, and allows for evidence management. It integrates information from Microsoft's audits and your organization's self-assessments, generating a Compliance Score and Excel reports for auditors.

- **Azure Security Center:** Provides a compliance dashboard with continuous risk assessments, offering insights into security posture and adherence to standards like CIS, PCI DSS, and 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

Azure provides on-demand computing resources like multi-core processors, virtual machines (VMs), containers, and serverless computing, allowing you to run applications without managing infrastructure. You pay only for what you use.

Common Azure compute methods:

- **Virtual Machines (IaaS)**
- **Containers**
- **Azure App Service**
- **Serverless computing**

Choosing a strategy is flexible; you can mix options based on your needs. For example, use VMs or containers for core applications and serverless computing for quick tasks. Control varies from most (VMs) to least (serverless computing).

Virtual Machines

Virtual Machines (IaaS): VMs are software emulations of physical computers, providing full control over the OS and allowing you to install custom software. Azure handles the physical hardware, while you manage the software on the VM.

Use Cases:

- Test and development for different OS/application setups.
- Handling demand fluctuations by scaling up/down VMs.
- Extending datacenters to the cloud or for disaster recovery.
- "Lift and shift" from physical servers to the cloud.

Scaling and Availability:

- 99.99% uptime guarantee with two or more instances in Availability Zones.
- **Availability sets:** Logical grouping of VMs with fault and update domains for high availability during planned/unplanned maintenance.
- **VM Scale Sets:** Automatically manage and scale groups of identical VMs based on demand.

Azure Batch: Large-scale job scheduling and compute management, ideal for tasks requiring raw or supercomputer-level compute power. It handles the entire process from scaling VMs to managing jobs.

Containers

- **Containers:** Lightweight virtualization environment for running applications. Unlike VMs, containers use the host's OS, reducing resource usage. They bundle application dependencies and allow multiple isolated applications to run on a single host, making them more efficient and faster than VMs.
- **Containers in Azure:**
 - **Azure Container Instances (PaaS):** Simplest way to run containers without managing infrastructure.
 - **Azure Kubernetes Service (AKS):** Full orchestration for managing, scaling, and deploying containerized applications.
- **Kubernetes:** A popular orchestration tool for automating container management across clouds, handling scaling, networking, storage, and more, with pod management and fault tolerance.
- **Microservices:** Break applications into independent, small services managed by separate teams. Each service can be scaled, updated, or deployed independently, promoting continuous innovation, easier maintenance, and fault isolation.
- **Microservices in Azure:**
 - **Azure Service Fabric:** A distributed systems platform for deploying microservices 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

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

Both Azure Functions and Logic Apps can create orchestrations, but differ in development approach and functionality:

- **State:**
 - **Functions:** Stateless (with Durable Functions for state).
 - **Logic Apps:** Stateful.
- **Development:**
 - **Functions:** Code-first (imperative).
 - **Logic Apps:** GUI-based (declarative).
- **Connectivity:**
 - **Functions:** Custom bindings via code.
 - **Logic Apps:** Many pre-built connectors, B2B integrations.
- **Actions:**
 - **Functions:** Code-based activity functions.
 - **Logic Apps:** Pre-made actions.
- **Monitoring:**
 - **Functions:** Azure Application Insights.
 - **Logic Apps:** Azure Portal, Log Analytics.
- **Management:**
 - **Functions:** REST API, Visual Studio.
 - **Logic Apps:** Azure Portal, REST API, PowerShell, Visual Studio.
- **Execution:**
 - **Functions:** Can run locally or in the cloud.
 - **Logic Apps:** Cloud-only

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: Requires on-premises storage
 - Azure: Azure data storage
- Compliance and Security:
 - On-premises: Dedicated servers required for privacy and security
 - Azure: Client-side encryption and encryption at rest
- Store Structured and Unstructured Data:
 - On-premises: Additional IT resources with dedicated servers required
 - Azure: Azure Data Lake and portal analyze and manage all types of data
- Replication and High Availability:
 - On-premises: More resources, licensing, and servers required

- Azure: Built-in replication and redundancy features available
- Application Sharing and Access to Shared Resources:
 - On-premises: File sharing requires additional administration resources
 - Azure: File sharing options available without additional license
- Relational Data Storage:
 - On-premises: Needs a database server with a database admin role
 - Azure: Offers database-as-a-service options
- Distributed Storage and Data Access:
 - On-premises: Expensive storage, networking, and compute resources needed
 - Azure: Azure Cosmos DB provides distributed access
- Messaging and Load Balancing:
 - On-premises: Hardware redundancy impacts budget and resources
 - Azure: Azure Queue provides effective load balancing
- Tiered Storage:
 - On-premises: Management of tiered storage needs technology and labor skill set
 - Azure: Automated tiered storage of data available

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
 - Add 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 Services:

- **Notification Hubs:** Push notifications to any platform.
- **API Management:** Secure API publishing.
- **Cognitive Search:** Managed search-as-a-service.
- **SignalR:** Real-time web functionalities.

IoT:

- **IoT Central:** Manage IoT devices.
- **IoT Hub:** Secure device communication.
- **IoT Edge:** Local data analysis on IoT devices.

Big Data:

- **Synapse Analytics, HDInsight, Databricks, Data Lake Analytics, Data Lake Store, Data Factory:** Big data processing and analytics.

AI:

- **Machine Learning:** Cloud-based model development.
- **Cognitive Services:** Pre-built AI APIs for vision, speech, and language.
- **Machine Learning Studio:** Visual workspace for model building.

DevOps:

- **Azure DevOps:** Pipelines, repos, and agile tools for continuous integration and delivery.
- **DevTest Labs:** Pre-configured testing environments.

Shared Responsibility Model

- Cloud security is a shared responsibility of both cloud providers and customers.
- Azure has many security certifications from outside auditors.
- Physical security
 - Handled by Microsoft
 - Walls, cameras, gates, security personnel

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

Cloud computing levels

As you move from on-premises to cloud services (IaaS, PaaS, SaaS), responsibilities shift from the customer to the cloud provider. In on-premises, the customer manages everything. With IaaS, the customer handles data and applications, while the provider manages infrastructure. In PaaS, the provider also manages the operating system. In SaaS, the provider manages almost everything, with the customer only responsible for data governance and access. Customer responsibilities decrease from IaaS to SaaS.

Data governance & rights management:

- On-prem: Customer
- IaaS: Customer
- PaaS: Customer
- SaaS: Customer

Client endpoints:

- On-prem: Customer
- IaaS: Customer
- PaaS: Customer
- SaaS: Customer

Account & access management:

- On-prem: Customer
- IaaS: Customer
- PaaS: Customer
- SaaS: Customer

Identity & directory infrastructure:

- On-prem: Customer
- IaaS: Customer
- PaaS: Cloud provider & Customer
- SaaS: Cloud provider & Customer

Application:

- On-prem: Customer
- IaaS: Customer
- PaaS: Cloud provider & Customer
- SaaS: Cloud provider

Network controls:

- On-prem: Customer

- IaaS: Customer
- PaaS: Cloud provider & Customer
- SaaS: Cloud provider

Operating system:

- On-prem: Customer
- IaaS: Customer
- PaaS: Cloud provider
- SaaS: Cloud provider

Physical host:

- On-prem: Customer
- IaaS: Cloud provider
- PaaS: Cloud provider
- SaaS: Cloud provider

Physical network:

- On-prem: Customer
- IaaS: Cloud provider
- PaaS: Cloud provider
- SaaS: Cloud provider

Physical datacenter:

- On-prem: Customer
- IaaS: Cloud provider
- PaaS: Cloud provider
- SaaS: Cloud provider

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 continuous assessments & recommendations.

Tiers

Free

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

Azure Defender

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

Use-cases

Incident response

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

Incident response stages

- You can use Security Center during the [detect](#), [assess](#), and [diagnose](#) stages.

Detect

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

Assess

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

Diagnose

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

Recommendations to enhance security

Security policy

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

Recommendations

- Based on security policies for potential vulnerabilities.
- Guide you through the process of configuring the needed security controls.

- E.g. if you have workloads that do not require the Azure SQL Database Transparent Data Encryption (TDE) policy, turn off the policy at the subscription level and enable it only in the resources groups where SQL TDE is required.

Identity and Access (Azure AD)

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

Authentication and authorization

- Azure provides services to manage both through [Azure Active Directory](#)

Authentication

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

Authorization

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

Azure Active Directory

- Called also as Azure AD.
- Cloud-based identity service.
- Can synchronize with existing on-premises Active Directory or can be used stand-alone.
- Allows to share identities in cloud (e.g. Microsoft 365), mobile on-premises applications.
- No SLA for free tier, 99.9% for standard & premium
- Some services:
 - Authentication.
 - Self-service password reset
 - [Multi-factor authentication \(MFA\)](#)
 - Custom banned password list, and smart lockout services.
 - [Single-Sign-On \(SSO\)](#)

- Application management. Manage cloud and on-premises apps using Azure AD Application Proxy, SSO, the My apps portal (also referred to as Access panel), and SaaS apps.
- Business to business (B2B) identity services: Manage guest users and external partners.
- Business-to-Customer (B2C) identity services: Customize and control how users sign up, sign in, and manage their profiles when using apps & services.
- Device Management
 - Manage how your cloud or on-premises devices access your corporate data.

Single sign-on

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

SSO with Azure Active Directory

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

Multi-factor authentication

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

Azure AD MFA

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

Providing identities to services

- Valuable for services to have identities
- Often, and against best practices, credential information is embedded in configuration files.
 - With no security around these configuration files, anyone with access to the systems or repositories can access these credentials and risk exposure.

Service identities in Azure AD

Service principals

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

Managed identities

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

Roles in Azure

- All co-exists.
- Three categories: [classic roles](#), [azure roles](#), [azure ad roles](#)

Classic roles

- Before [Role-based access control](#) was introduced there were 3 roles:
 - Account Administrator: One per Azure account
 - Service Administrator: One per Azure subscription
 - Co-Administrator: 200 per subscription

Role-based access control

- Called also Azure roles.
- Provides fine-grained access management for Azure resources
- Role
 - Sets of permissions
 - E.g. "Read-only" or "Contributor"
 - Identities are mapped to roles directly or through group membership.
- Role assignments

- When you are assigned to a role, RBAC allows you to perform specific actions, such as read, write, or delete.
- E.g.
 - Allow one user to manage VMs in a subscription
 - Allow an application to access all resources in a resource group.
- Can be granted at the service instance level, but they also flow down the Azure Resource Manager hierarchy.
 - Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.
- Segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
- Four fundamental Azure roles: Owner, Contributor, Reader, User Access Administrator

Azure AD Roles

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

Privileged Identity Management

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

Encryption (Azure Key Vault, Certificates)

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

Encryption types

Symmetric encryption

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

Asymmetric encryption

- Uses a public key and private key pair.
 - Either key can encrypt but a single key can't decrypt its own encrypted data.
 - To decrypt, you need the paired key.

- Used for things like Transport Layer Security (TLS) (used in HTTPS) and data signing.

Encryption ways

Encryption at rest

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

Encryption in transit

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

Encryption on Azure

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

Azure Storage Service Encryption

- Allows you encrypt raw storage.
- Automatically encrypts your data before persisting it to e.g. Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage
 - and decrypts the data before retrieval.
- The handling of process is transparent to applications.
 - Encryption, encryption at rest, decryption, and key management

Azure Disk Encryption

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

Transparent data encryption (TDE)

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

Azure Key Vault

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

Azure certificates

Transport Layer Security (TLS)

- Basis for encryption of website data in transit.
- Uses certificates to encrypt and decrypt data.
 - have a life cycle that requires administrator management
 - expired TLS certificates open security vulnerabilities.
- Certificates used in Azure are x.509 v3 that can be y
 - signed by a trusted certificate authority
 - or self-signed
 - not trusted by default as signed by its own creator
 - good for development + testing
- Can contain a private or a public key
 - Keys have an identifiable thumbprint

- used in the Azure configuration file to identify which certificate a cloud service should use.

Types of certificates

Service certificates

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

Management certificates

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

Network Protection

- Important to secure your network from attacks and unauthorized access
- Use a layered approach
 - not enough to just focus on securing the network perimeter or the network security between services inside a network.
 - helps reduce your risk of exposure through network-based attacks
 - secure your internet-facing resource, internal resources, and communication between on-premises networks
 - Combine multiple Azure networking and security services
 - E.g. use Azure Firewall to protect inbound and outbound traffic to the Internet, and Network Security Groups to limit traffic to resources inside your virtual networks.

Internet protection

- Perimeter of the network
- Focused on limiting and eliminating attacks from the internet.
- Only allow inbound and outbound communication where necessary

- ensure they are restricted to only the ports and protocols required
 - You can use [Azure Security Center](#) for this.

Firewall

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

Azure Firewall

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

Azure Application Gateway

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

Network virtual appliances (NVAs)

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

Distributed Denial of Service (DDoS) Protection

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

Azure DDoS Protection

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

Service tiers

Basic

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

Standard

- Tuned specifically to Microsoft Azure Virtual Network resources
- Requires no application changes.
- Dedicated traffic monitoring and machine learning algorithms.
- Policies are applied to public IP addresses associated with resources deployed in virtual networks

- e.g. Azure Load Balancer and Application Gateway.
- Mitigates:
 - Volumetric attacks: The attackers goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
 - Protocol attacks: Render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
 - Resource (application) layer attacks: Target web application packets to disrupt the transmission of data between hosts.

Traffic inside your virtual network

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

Virtual network security

Network Security Groups (NSGs)

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

Service endpoints

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

Network integration

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

Virtual private network (VPN)

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

Azure ExpressRoute

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

Microsoft Azure Information Protection (AIP)

- Helps to classify and optionally protect (encrypt) documents and emails by applying labels.
- Labels can be applied
 - automatically based on rules and conditions
 - or manually

- E.g. when a user saves a Microsoft Word document containing a credit card number, a custom tooltip is displayed. The tooltip recommends labeling the file as Confidential \ All Employees configured by the administrator.
- After your content is classified, you can track and control how the content is used. E.g. you can:
 - Analyze data flows to gain insight into your business
 - Detect risky behaviors and take corrective measures
 - Track access to documents
 - Prevent data leakage or misuse of confidential information
- You can purchase AIP either as a standalone solution, or through one of the following Microsoft licensing suites:
 - Enterprise Mobility + Security
 - or Microsoft 365 Enterprise

Microsoft Defender for Identity

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

Microsoft Defender for Identity components

Microsoft Defender for Identity portal

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

Microsoft Defender for Identity sensor

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

Microsoft Defender for Identity cloud service

- Runs on Azure infrastructure
- Deployed in the United States, Europe, and Asia.
- Connected to [Microsoft Intelligent Security Graph](#)
 - Threats signals are seamlessly shared across all the services in Microsoft 365 Defender, 6.5 trillion signals daily.
 - Microsoft 365 Defender
 - Formerly known as Microsoft Threat Protection
 - Consists of different Azure security services

- E.g. Office ATP, Microsoft Defender ATP, SmartScreen, Exchange Online Protection (EOP)
- Provides comprehensive security across multiple attack vectors.
- Allows you to use [Microsoft Graph Security API](#)
 - Connects Microsoft security products, services, and partners
 - Can be used to
 - streamline security operations
 - improve threat protection, detection, and response capabilities.

Microsoft Security Development Lifecycle (SDL)

- Security in Development: Introduces security and privacy considerations across all phases of development, helping developers build secure software, reduce costs, and meet compliance requirements. Security is everyone's responsibility.
- Defining Security Requirements: Set security requirements early during design and planning to address functionality changes and threats. Factors include legal standards, internal practices, and known threats.
- Tracking and Reporting: Define metrics and track security tasks using bug-tracking systems to ensure accountability. Set KPIs and label security tasks by severity.
- Threat Modeling: Use threat modeling to assess security risks at the design level, identify vulnerabilities, and apply appropriate mitigations.
- Design Requirements: Ensure secure design with features like encryption, authentication, and logging. Apply cryptography standards using only trusted libraries.
- Third-Party Components: Manage security risks from third-party and open-source software, plan for vulnerabilities, and validate regularly.
- Security Tools: Use approved tools for secure coding and integrate them into development processes, staying up-to-date with the latest versions.
- Static & Dynamic Analysis: Perform static analysis (SAST) to identify code vulnerabilities before compilation, and dynamic analysis to test for runtime issues in an integrated environment.
- Penetration Testing: Simulate hacker attacks to uncover vulnerabilities and test operational weaknesses.
- Incident Response: Establish a response plan for new threats with a dedicated Product Security Incident Response Team (PSIRT), and test it regularly.

Azure Policy & Azure Blueprints

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

Azure Policy

- Each policy enforces rules over specified or all resources.

- Allows your infrastructure stay compliant with:
 - corporate standards, cost requirements, service-level agreements, industry compliance frameworks (ISO 27001, NIST 800-53, etc).
- E.g. a policy that allows virtual machines of only a certain size in your environment.
- Evaluates both new and existing resources for compliance.
 - Can deny new uncompliant resources from being created
 - Can stop existing resources from being updated to an uncompliant state.
 - Does not remove uncompliant resources!
 - Can only audit existing & new resources
 - Identifying non-compliant resources
 - Can alter the resource properties.

Azure Policy vs RBAC

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

Creating a policy

1. Create a [policy definition](#)
2. Assign a definition to a [scope](#) of resources
3. View policy evaluation results

Policy Definition

- What to evaluate and what action to take
- Has
 - conditions under which it is enforced
 - accompanying effect that takes place if the conditions are met
- E.g. restrict the locations that your organization can specify when deploying resources
- Represented as a JSON file, many [samples on GitHub](#)

Policy effects

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

Policy Scope

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

Policy Assignment

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

Policy Initiatives

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

Azure Blueprints

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

Azure Blueprints vs Resource Manager templates

- No need to choose between them & can use both.
 - Each blueprint can consist of zero or more Resource Manager template artifacts.
- Differences:
 - **Azure Blueprints:**
 - **Packages:** Resource groups, policies, role assignments, and Resource Manager template deployments.
 - **Storage:** Natively in Azure.
 - **Tracking:** Observes what should be deployed and what was deployed.
 - **Deployment scope:** Several subscriptions.
 - **Resource Manager templates:**
 - **Packages:** Resource groups, policies, role assignments.
 - **Storage:** Either locally or in source control.
 - **Tracking:** No active connection or relationship from deployed resources to the template.
 - **Deployment scope:** Subscription or resource group.

Azure Blueprints vs Azure Policy

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

Monitoring (Azure Monitor & Azure Service Health)

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

Azure Monitor

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

Data sources

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

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

Diagnostic settings

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

Application Insights

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

Azure Monitor for containers

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

Azure Monitor for VMs

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

Responding

Azure Alerts

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

Autoscale

- Uses Autoscale to ensure that you have the right amount of resources running to manage the load on your application effectively.
- Enables you to create rules that use metrics from Azure Monitor, to determine when to scale

- Help reduce your Azure costs by removing resources that are not being used.
- You provide the logic that determines when Autoscale should increase or decrease resources.

Azure Service Health

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

Economies of Scale

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

Capital Expenditure (CapEx) vs Operational Expenditure (OpEx)

- Before: up-front cost in hardware and infrastructure to start or grow a business (CapEx)
 - With cloud: Use services without significant upfront costs or equipment setup time (OpEx)
- Hybrid solution = combine both in cloud with using both on-premises (CapEx) and cloud (OpEx)
- Also possible to have CapEx in cloud with e.g. [Azure Reserved VM Instances](#)
- CapEx model is also sometimes used in cloud

Capital Expenditure (CapEx)

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

Costs of CapEx

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

Benefits of CapEx

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

Operational Expenditure (OpEx)

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

Billing of OpEx

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

Costs of OpEx

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

Benefits of OpEx


- CapEx challenge: Demand and growth can be unpredictable and can outpace expectation
- Companies wanting to try a new product or service don't need to invest in equipment
 - Instead, they pay as much or as little for the infrastructure as required.
- OpEx is particularly appealing if the demand fluctuates or is unknown
- Enables cloud agility

- Ability to rapidly change an IT infrastructure to adapt to the evolving needs of the business
- Manage your costs dynamically, optimizing spending as requirements change.
- E.g. service peaks one month => pay more, demand drops next month => pay less

Azure Costs & Tools

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

Usage meters

- Used to determine Azure costs for each billing period
- When you provision an Azure resource, Azure creates one or more meter instances for that resource.
 - They are charged based on usage
- The meters track the resources' usage, and generate a usage record that is used to calculate your bill.
- Each meter tracks a particular kind of usage.
- The usage that a meter tracks correlates to a number of billable units.
 - Those units are charged to your account for each billing period.
- E.g. when you deploy a single virtual machine:
 - Azure might have following meters tracking:
 - Compute Hours, IP Address Hours
 - Data Transfer In, Data Transfer Out
 - Standard Managed Disk, Standard Managed Disk Operations
 - Standard IO-Disk, Standard IO-Block Blob Read, Standard IO-Block Blob Write, Standard IO-Block Blob Delete
 -  If you de-allocate a VM you'll not pay for it. However, your persistent disks remain in your subscription that you pay for.
- Meters and pricing vary per product
- Often have different pricing tiers based on the size or capacity of the resource.

Billing

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

Factors affecting costs

Resource type

- Costs are resource-specific
- The usage that a meter tracks and the number of meters associated with a resource depend on the resource type.

- The rate per billable unit depends on the resource type you are using.

Services

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

Location

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

Bandwidth

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

Billing zone

- A Zone is a geographical grouping of Azure Regions for billing purposes.
- Each zone has different outbound data transfer prices.
- Zones:
 - Zone 1: United States, US Government, Europe, Canada, UK, France, Switzerland
 - Zone 2: East Asia, Southeast Asia, Japan, Australia, India, Korea
 - Zone 3: Brazil, South Africa, UAE
 - DE Zone 1: Germany.

Tools

Azure pricing calculator

- Free web-based tool: <https://azure.microsoft.com/en-us/pricing/calculator/>
- Get estimate costs without deploying and running those services or without manually pricing out each service from the Azure service pricing pages.
 - Can save results in your Azure account, export as Excel or shared as an URL.
- You select Azure services and modify properties and options of the services.
 - Outputs the costs per service and total cost for the full estimate
 - Modifiable properties:
 - Region: E.g. Southeast Asia, central Canada, western United States, northern Europe...
 - Tier: E.g. Free Tier, Basic Tier, etc.
 - Billing Options: Per type of customers and subscriptions for a chosen product.
 - Support Options: Included / paid support options.
 - Programs and Offers: Available price offerings according to your customer or subscription type.
 - Azure Dev/Test Pricing: Available if subscription is based on a Dev/Test offer.

- On the pricing calculator page, you'll see several tabs:
 - Products. Lists all Azure services, allows you put together services for your estimate.
 - Customizable e.g. for VMs you select region, OS, size, running hours.
 - Example Scenarios. Common solutions to add all the components, e.g. VMs + load balancer.
 - Saved Estimates. Your previously saved estimates.
 - FAQ

Azure Advisor

- Free service that provides recommendations on
 - high availability, security, performance, operational excellence, and cost.
- Analyzes your deployed services and gives personalized recommendations.
- Cost recommendation areas:
 - Reduce costs by eliminating unprovisioned Azure ExpressRoute circuits
 - Finds circuits that have been in the provider status of Not Provisioned for more than one month.
 - Recommends deleting the circuit.
 - Buy reserved instances to save money over pay-as-you-go
 - Analyzes your VM usage over the last 30 days,
 - Determines & shows if you could save money in the future by purchasing reserved instances.
 - Shows the regions and sizes where you potentially have the most savings
 - Right-size or shutdown underutilized virtual machines
 - Monitors your virtual machine usage for 14 days.
 - Identifies underutilized virtual machines, allows you to scale down/in to reduce your costs.
 - E.g. VMS with average CPU utilization of $\leq 5\%$ (adjustable up to 20%)
 - E.g. network usage ≤ 7 MB for +4 days.

Azure Cost Management

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

Azure TCO calculator

- Compares on-prem vs cloud costs.
 - Describe your infrastructure: servers, databases, storages, networking
 - Adjust assumptions: adjust values for e.g. VM costs, electricity costs, IT labor costs.
 - Compare costs & see how much you can save
- Web-based tool: azure.microsoft.com/pricing/tco
- TCO = Total Cost of Ownership

Cost Optimization Best Practices

Save on infrastructure

Use Azure credits

- \$50 per month for Visual Studio Professional, \$150 per month for Visual Studio Enterprise
- Separate Azure subscription under your account that renews each month while you remain an active Visual Studio subscriber
- No SLA, development and testing only
 - Azure suspends VMs used for production or that run more than 120 hours.

Use spending limits

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

Use reserved instances

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

Choose low-cost locations and regions

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

Research available cost-saving offers

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

Right-size underutilized virtual machines

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

Deallocate virtual machines in off hours

- No need to run VMs every hour of every day if they're only used during certain periods.

- Shut down when not in use and start back up on a schedule
 - Saves money on compute costs, but you still pay for storage.
- Can use [automation accounts](#) or auto-shutdown feature on a virtual machine to schedule automated shutdowns.

Delete unused virtual machines

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

Migrate to PaaS or SaaS services

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

Save on licensing costs

Linux vs. Windows

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

Azure Hybrid Benefit

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

Use Dev/Test subscription offers

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

Bring your own SQL Server license

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

Use SQL Server Developer Edition

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

Use constrained instance sizes for database workloads

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