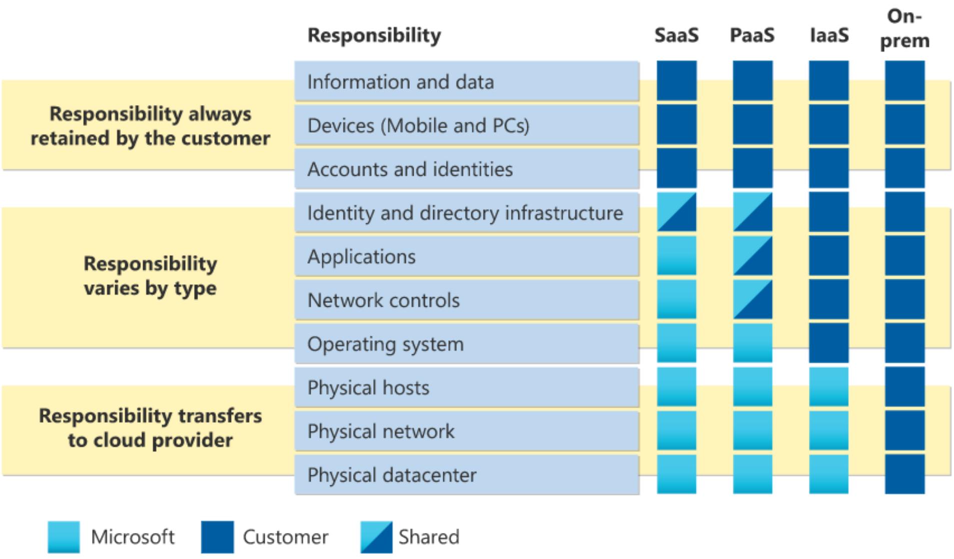
Azure

What is cloud computing?

Cloud Computing is the delivery of computing services over the internet.Computing Services include common IT infrastructure as virtual machines , storage, databases and networking. Cloud Services also expand the traditional IT offerings to include things like Internet Of things (IoT) , machine learning and Artificial intelligence.

Describe the shared responsibility model?

The following diagram highlights how the Shared Responsibility Model informs who is responsible for what, depending on the cloud service type.



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

□ Microsoft ■ Customer ◩ Shared

When using a cloud provider, you'll always be responsible for:

- The information and data stored in the cloud
- Devices that are allowed to connect to your cloud (cell phones, computers, and so on)
- The accounts and identities of the people, services, and devices within your organization

The cloud provider is always responsible for:

- The physical datacenter
- The physical network

- The physical hosts

Your service model will determine responsibility for things like:

- Operating systems
- Network controls
- Applications
- Identity and infrastructure

Cloud Models

- ### Private Cloud

  Private cloud is like a corporate data center with internet access, for one company only. It offers more control but is less cost-effective than public cloud, and can be on-site or off-site.

- ### Public Cloud

  A public cloud is built, controlled, and maintained by a third-party cloud provider. With a public cloud, anyone that wants to purchase cloud services can access and use resources. The general public availability is a key difference between public and private clouds.

- ### Hybrid Cloud

  A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment. A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources. Hybrid cloud can be used to provide an extra layer of security.

- ### Multi Cloud

  A fourth, and increasingly likely scenario is a multi-cloud scenario. In a multi-cloud scenario, you use multiple public cloud providers. Maybe you use different features from different cloud providers. Or maybe you started your cloud journey with one provider and are in the process of migrating to a different provider. Regardless, in a multi-cloud environment you deal with two (or more) public cloud providers and manage resources and security in both environments.

Describe the consumption-based model

Cloud computing saves money compared to traditional data centers by being OpEx (pay-as-you-go) instead of CapEx (upfront cost). With cloud computing, you only pay for the resources you use, allowing you to easily scale up or down based on your needs. This eliminates the risk of over or under-provisioning resources that happen with traditional data centers.

The benefits of high availability and scalability in the cloud

When building or deploying a cloud application, two of the biggest considerations are uptime (or availability) and the ability to handle demand (or scale).

High availability

When you’re deploying an application, a service, or any IT resources, it’s important the resources are available when needed. High availability focuses on ensuring maximum availability, regardless of disruptions or events that may occur.

When you’re architecting your solution, you’ll need to account for service availability guarantees. Azure is a highly available cloud environment with uptime guarantees depending on the service. These guarantees are part of the service-level agreements (SLAs).

Scalability

Another major benefit of cloud computing is the scalability of cloud resources. Scalability refers to the ability to adjust resources to meet demand. If you suddenly experience peak traffic and your systems are overwhelmed, the ability to scale means you can add more resources to better handle the increased demand.

The other benefit of scalability is that you aren't overpaying for services. Because the cloud is a consumption-based model, you only pay for what you use. If demand drops off, you can reduce your resources and thereby reduce your costs.

Scaling generally comes in two varieties: vertical and horizontal. Vertical scaling is focused on increasing or decreasing the capabilities of resources. Horizontal scaling is adding or subtracting the number of resources.

Vertical scaling

With vertical scaling, if you were developing an app and you needed more processing power, you could vertically scale up to add more CPUs or RAM to the virtual machine. Conversely, if you realised you had over-specified the needs, you could vertically scale down by lowering the CPU or RAM specifications.

Horizontal scaling

With horizontal scaling, if you suddenly experienced a steep jump in demand, your deployed resources could be scaled out (either automatically or manually). For example, you could add additional virtual machines or containers, scaling out. In the same manner, if there was a significant drop in demand, deployed resources could be scaled in (either automatically or manually), scaling in.

Reliability

Reliability is the ability of a system to recover from failures and continue to function. It's also one of the pillars of the Microsoft Azure Well-Architected Framework.

The cloud, by virtue of its decentralised design, naturally supports a reliable and resilient infrastructure. With a decentralised design, the cloud enables you to have resources deployed in regions around the world. With this global scale, even if one region has a catastrophic event other regions are still up and running. You can design your applications to automatically take advantage of this increased reliability. In some cases, your cloud environment itself will automatically shift to a different region for you, with no action needed on your part.

Predictability

Predictability in the cloud lets you move forward with confidence. Predictability can be focused on performance predictability or cost predictability. Both performance and cost predictability are heavily influenced by the Microsoft Azure Well-Architected Framework. Deploy a solution built around this framework and you have a solution whose cost and performance are predictable.

Performance

Performance predictability focuses on predicting the resources needed to deliver a positive experience for your customers. Autoscaling, load balancing, and high availability are just some of the cloud concepts that support performance predictability. If you suddenly need more resources, autoscaling can deploy additional resources to meet the demand, and then scale back when the demand drops. Or if the traffic is heavily focused on one area, load balancing will help redirect some of the overload to less stressed areas.

Cost

Cost predictability is focused on predicting or forecasting the cost of the cloud spend. With the cloud, you can track your resource use in real time, monitor resources to ensure that you're using them in the most efficient way, and apply data analytics to find patterns and trends that help better plan resource deployments. You can even use tools like the Total Cost of Ownership (TCO) or Pricing Calculator to get an estimate of potential cloud spend.

The benefits of Security and Governance in the Cloud

Whether you're deploying infrastructure as a service or software as a service, cloud features support governance and compliance. Things like set templates help ensure that all your deployed resources meet corporate standards and government regulatory requirements. Plus, you can update all your deployed resources to new standards as standards change.

On the security side, you can find a cloud solution that matches your security needs. If you want maximum control of security, infrastructure as a service provides you with physical resources but lets you manage the operating systems and installed software, including patches and maintenance.

And because the cloud is intended as an over-the-internet delivery of IT resources, cloud providers are typically well suited to handle things like distributed denial of service (DDoS) attacks, making your network more robust and secure.

The benefits of manageability in the Cloud

A major benefit of cloud computing is the manageability options. There are two types of manageability for cloud computing that you'll learn about in this series, and both are excellent benefits.

Management of the Cloud

Management of the cloud speaks to managing your cloud resources. In the cloud, you can:

- Automatically scale resource deployment based on need.
- Deploy resources based on a preconfigured template, removing the need for manual configuration.
- Monitor the health of resources and automatically replace failing resources.
- Receive automatic alerts based on configured metrics, so you're aware of performance in real time.

Management in the cloud

Management in the cloud speaks to how you're able to manage your cloud environment and resources. You can manage these:

- Through a web portal.
- Using a command line interface.
- Using APIs.
- Using PowerShell.

Infrastructure as a Service

Infrastructure as a service (IaaS) is the most flexible category of cloud services, as it provides you the maximum amount of control for your cloud resources. In an IaaS model, the cloud provider is responsible for maintaining the hardware, network connectivity (to the internet), and physical security. You're responsible for everything else: operating system installation, configuration, and maintenance; network configuration; database and storage configuration; and so on. With IaaS, you're essentially renting the hardware in a cloud datacenter, but what you do with that hardware is up to you.

Scenarios

Some common scenarios where IaaS might make sense include:

- Lift-and-shift migration: You're setting up cloud resources similar to your on-prem datacenter, and then simply moving the things running on-prem to running on the IaaS infrastructure.
- Testing and development: You have established configurations for development and test environments that you need to rapidly replicate. You can start up or shut down the different environments rapidly with an IaaS structure, while maintaining complete control.

Ex: Azure VM , Azure Blob , Azure Virtual Networks.

Platform as a Service

Platform as a service (PaaS) is a middle ground between renting space in a datacenter (infrastructure as a service) and paying for a complete and deployed solution (software as a service). In a PaaS environment, the cloud provider maintains the physical infrastructure, physical security, and connection to the internet. They also maintain the operating systems, middleware, development tools, and business intelligence services that make up a cloud solution. In a PaaS scenario, you don't have to worry about the licensing or patching for operating systems and databases.

Scenarios

Some common scenarios where PaaS might make sense include:

- Development framework: PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to the way you create an Excel macro, PaaS lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
- Analytics or business intelligence: Tools provided as a service with PaaS allow organizations to analyse and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investment returns, and other business decisions.

Ex: Azure App Service , Azure SQL DB , Azure Kubernetes Service

Software as a Service

Software as a service (SaaS) is the most complete cloud service model from a product perspective. With SaaS, you're essentially renting or using a fully developed application. Email, financial software, messaging applications, and connectivity software are all common examples of a SaaS implementation.

While the SaaS model may be the least flexible, it's also the easiest to get up and running. It requires the least amount of technical knowledge or expertise to fully employ.

Scenarios

Some common scenarios for SaaS are:

- Email and messaging.
- Business productivity applications.
- Finance and expense tracking.

Ex: Azure AD, Dynamics 365 , Microsoft 365.

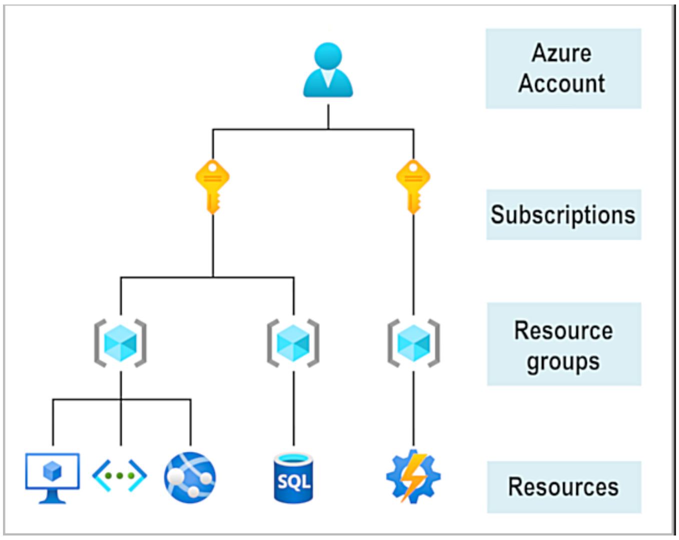
Core Architectural Components Of Azure

Azure is a continually expanding set of cloud services that help you meet current and future business challenges. Azure gives you the freedom to build, manage, and deploy applications on a massive global network using your favourite tools and frameworks.**Limitless innovation.** Build intelligent apps and solutions with advanced technology, tools, and services to take your business to the next level.

Azure Accounts

To create and use Azure services, you need an Azure subscription. When you're completing Learn modules, most of the time a temporary subscription is created for you, which runs in an environment called the Learn sandbox. When you're working with your own applications and business needs, you need to create an Azure account, and a subscription will be created for you. After you've created an Azure account, you're free to create additional subscriptions.

For example, your company might use a single Azure account for your business and separate subscriptions for development, marketing, and sales departments. After you've created an Azure subscription, you can start creating Azure resources within each subscription.



Azure Physical Infrastructure

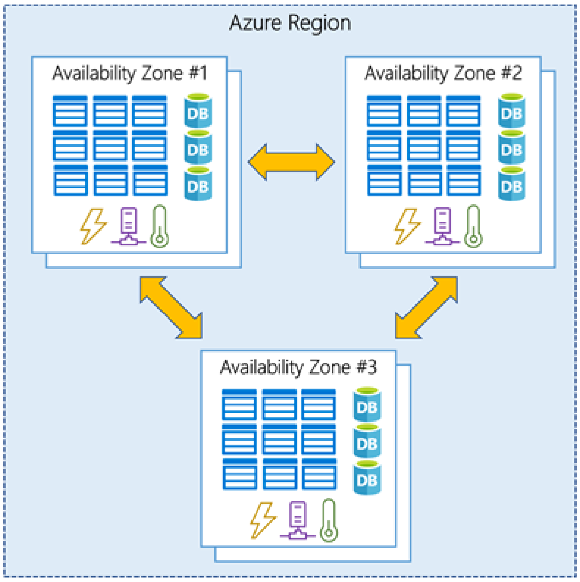
As a global cloud provider, Azure has datacenters around the world. However, these individual datacenters aren’t directly accessible. Datacenters are grouped into Azure Regions or Azure Availability Zones that are designed to help you achieve resiliency and reliability for your business-critical workloads.

Regions

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

Availability Zones

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



Availability Zones in your apps

Data redundancy is crucial to protect information from hardware failures.

- **Self-hosting requires building duplicate environments,** which is expensive and complex.
- **Azure offers availability zones** as a simpler and potentially more cost-effective solution for high availability.
- **Availability zones** allow replicating resources across geographically separate locations within a region, improving your application's resilience.
- **Duplicating services and data transfer** between zones might incur additional costs.

Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support availability zones fall into three categories:

- Zonal services: You pin the resource to a specific zone (for example, VMs, managed disks, IP addresses).
- Zone-redundant services: The platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).
- Non-regional services: Services are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.

Region Pairs

Most Azure regions are paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away. This approach allows for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect an entire region.

Examples of region pairs in Azure are West US paired with East US and South-East Asia paired with East Asia. Because the pair of regions are directly connected and far enough apart to be isolated from regional disasters, you can use them to provide reliable services and data redundancy.

Sovereign Regions

In addition to regular regions, Azure also has sovereign regions. Sovereign regions are instances of Azure that are isolated from the main instance of Azure. You may need to use a sovereign region for compliance or legal purposes.

Azure sovereign regions include:

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

Azure Resources and Resources groups

Resources:

- Basic building blocks of Azure (VMs, databases, etc.)Each resource is a separate entity.
- **Resource Groups:**
    - Containers for grouping related resources.
    - One resource can only belong to one group at a time.
    - Resource groups cannot be nested.

- **Benefits of Resource Groups:**
    - Easier management: Apply actions (delete, access control) to the entire group at once.
    - Organization: Group resources based on project, purpose, or access needs.
- **Example:**
    - Temporary dev environment: Group all resources together for easy deletion.
    - Resources with different access needs: Group based on access and assign permissions at the group level.

In short, think of resources as individual Legos and resource groups as Lego boxes. Group your Legos (resources) based on your project for better organization and management.

Azure Subscriptions

In Azure, subscriptions are a unit of management, billing, and scale. Similar to how resource groups are a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing.

Management, Billing, and Scale:

- Subscriptions are core units for managing Azure resources, billing, and scaling your cloud environment.
- **Organization and Access:** Similar to resource groups for resources, subscriptions help organize resource groups logically and manage billing.
- **Required for Azure Usage:** An Azure subscription is essential for accessing and provisioning resources in Azure.
- **Linked to Azure Account:** Each subscription links to an Azure account, which is your identity for accessing Azure services.
- **Multiple Subscriptions per Account (Optional):** One Azure account can have multiple subscriptions for different billing and access control needs.
- **Subscription Boundaries:** Subscriptions define boundaries for Azure resources:
    - **Billing Boundary:**
      Defines how an Azure account is billed for resource usage. Separate

subscriptions allow for independent cost tracking and invoices.

    - **Access Control Boundary:** Allows applying access-management policies at the subscription level,
      enabling control over resource access based on organisational structures.

- **Creating Additional Subscriptions:** Similar to resource groups, you can create additional subscriptions for various purposes:
    - **Environments:** Separate subscriptions for development/testing, security, or data isolation for compliance.
    - **Organisational Structures:** Align subscriptions with different departments, allowing for granular access control based on resource needs.
    - **Billing Management:** Create subscriptions for specific cost tracking and billing needs, like separating production and development environments.

In essence, Azure subscriptions provide a way to organize your cloud resources, manage access and billing, and tailor your Azure environment to your specific needs.

Azure Management Groups

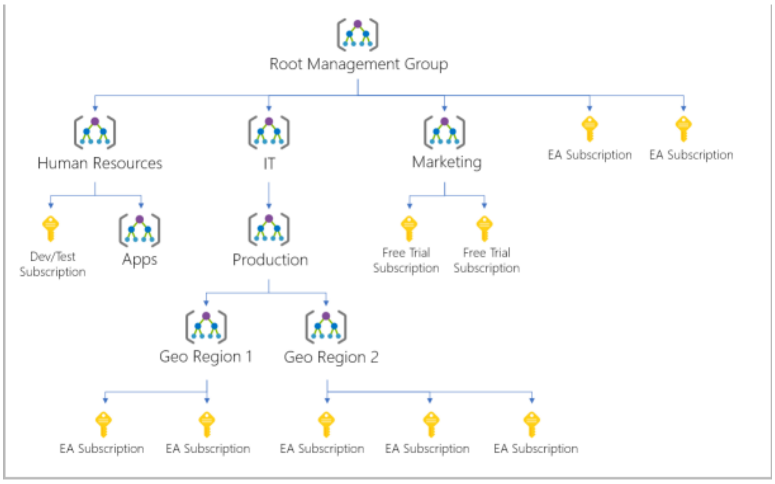
The final piece is the management group. Resources are gathered into resource groups, and resource groups are gathered into subscriptions.

Challenge:

- When managing numerous Azure subscriptions across applications, teams, and locations, resource groups and subscriptions alone might not provide enough organization.
- **Solution:** Azure Management Groups offer a level of hierarchy above subscriptions.
- **Function:**
    - Group subscriptions into logical containers.
    - Apply governance policies (access, compliance) to the entire group.
    - Inherit settings similar to how resource groups inherit from subscriptions.

- **Benefits**:
  - **Enterprise-grade Management:** Efficiently manage access, policies, and compliance across a large number of subscriptions.
  - **Unified Governance:** Apply policies consistently across all subscriptions within a management group.
  - **Simplified Access Control:** Assign Azure RBAC permissions at the group level for inheritance by all resources within.
- **Structure**:
  - Management groups can be nested up to six levels deep (excluding root and subscription levels).
  - Each group and subscription can have only one parent.
- **Examples**:
  - **Enforce Security Policies:** Limit VM locations within a "Production" group to ensure compliance.
  - **Simplify User Access:** Assign permissions at the group level to grant access to everything users need within that group.
- **Limits**:
  - A single directory can support up to 10,000 management groups.

In summary, Azure Management Groups provide a powerful tool for organizing and managing complex Azure environments with many subscriptions, ensuring consistent policies and simplified access control.



Azure Virtual Machines

With Azure Virtual Machines (VMs), you can create and use VMs in the cloud. VMs provide infrastructure as a service (IaaS) in the form of a virtualised server and can be used in many ways. Just like a physical computer, you can customize all of the software running on your VM. VMs are an ideal choice when you need:

- Total control over the operating system (OS).
- The ability to run custom software.
- To use custom hosting configurations.

Virtualisation without Hardware Management:

- Azure VMs offer virtualisation benefits without the need to purchase and maintain physical hardware.
- **Flexibility with VM Images:**
  - Create VMs quickly using pre-configured images containing OS and software.
  - Option to create custom VM images for specific needs.
- **Scalability for Various Needs:**
  - Run single VMs for basic tasks.
  - Group VMs for high availability, scalability, and redundancy using:
    - Virtual Machine Scale Sets: Manage and update a large number of identical VMs for efficient resource use.
    - Virtual Machine Availability Sets:
Enhance VM resiliency by grouping VMs across update and fault domains to prevent single point of failure.
- **Benefits of Using Azure VMs:**
  - **Testing and Development:** Easily create and destroy VMs with different configurations for testing and development purposes.
  - **Cloud-based Applications:** Run applications in the cloud for cost-efficiency and scalability, especially for applications with fluctuating demand.
  - **Extending Datacenters:** Expand on-premises network capabilities by creating VMs in Azure's virtual network.

    - **Disaster Recovery:** Implement cost-effective disaster recovery by creating VMs in Azure
    during outages and shutting them down upon primary datacenter recovery.
    - **Cloud Migration (Lift and Shift):** Easily migrate from physical servers to the cloud by creating VMs from server images with minimal changes.
- **VM Resource Selection:** When provisioning VMs, you can choose associated resources like:
    - Size (processing power and memory)
    - Storage disks (HDD, SSD, etc.)
    - Networking configuration (virtual network, IP address, ports)

Virtual Desktop

Another type of virtual machine is the Azure Virtual Desktop. Azure Virtual Desktop is a desktop and application virtualisation service that runs on the cloud. It enables you to use a cloud-hosted version of Windows from any location. Azure Virtual Desktop works across devices and operating systems, and works with apps that you can use to access remote desktops or most modern browsers.

Enhance Security

- **Centralised Management:** Manage user desktops securely with Microsoft Entra ID.
- **Strong Authentication:** Enforce multi-factor authentication to prevent unauthorized access.
- **Granular Access Control:** Assign specific permissions (RBAC) to users, limiting access to only what they need.
- **Data Isolation:** Data and applications reside in the cloud, not on local devices, reducing the risk of data breaches.
- **Session Isolation:** User sessions are isolated in both single and multi-user environments, further enhancing security.

Multi Session windows 10 or Windows 11 Deployment

Azure Virtual Desktop lets you use Windows 10 or Windows 11 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM. Azure Virtual Desktop also provides a more consistent experience with broader application support compared to Windows Server-based operating systems.

Azure Containers

Containers are a virtualisation environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. Unlike virtual machines, you don't manage the operating system for a container. Virtual machines appear to be an instance of an operating system that you can connect to and manage. Containers are lightweight and designed to be created, scaled out, and stopped dynamically. It's possible to create and deploy virtual machines as application demand increases, but containers are a lighter weight, more agile method. Containers are designed to allow you to respond to changes on demand. With containers, you can quickly restart if there's a crash or hardware interruption. One of the most popular container engines is Docker, and Azure supports Docker.

Azure Container Instances

Azure Container Instances offer the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services. Azure Container Instances are a platform as a service (PaaS) offering. Azure Container Instances allow you to
upload your containers and then the service will run the containers for you.

Azure Container Apps

Azure Container Apps are similar in many ways to a container instance. They allow you to get up and running right away, they remove the container management piece, and they're a PaaS offering. Container Apps have extra benefits such as the ability to incorporate load balancing and scaling. These other functions allow you to be more elastic in your design.

Azure Kubernetes Service

Azure Kubernetes Service (AKS) is a container orchestration service. An orchestration service manages the lifecycle of containers. When you're deploying a fleet of containers, AKS can make fleet management simpler and more efficient.

Use containers in your solutions

Containers are often used to create solutions by using a microservice architecture. This architecture is where you break solutions into smaller, independent pieces. For example, you might split a website into a container hosting your front end, another hosting your back end, and a third for storage. This split allows you to separate portions of your app into logical sections that can be maintained, scaled, or updated independently.

Azure Functions

Azure Functions is an event-driven, serverless compute option that doesn't require maintaining virtual machines or containers. With Azure Functions, an event wakes the function, alleviating the need to keep resources provisioned when there are no events.

Benefits Of Azure Functions

- **Focus on Code, Not Infrastructure:** With Functions, you write code for your application logic without
worrying about servers, scaling, or underlying infrastructure.
- **Event-Driven Execution:** Functions are triggered by events like HTTP requests, timers, or messages from other Azure services.
- **Ideal for Short-Running Tasks:** Functions are perfect for tasks that complete quickly (within seconds) in response to an event.
- **Automatic Scaling:** Functions automatically scale up or down based on real-time demand, optimizing resource utilization.
- **Pay-Per-Use Model:** You only pay for the compute time your function uses while running, reducing costs for variable workloads.
- **Stateless or Stateful Options:**
    - Stateless functions (default) behave independently for each event, like a clean slate each time.
    - Durable Functions (stateful) maintain context across function invocations for scenarios requiring state management.

- **Serverless Core, Flexible Deployment:**
  - Functions leverage serverless architecture for simplicity.
  - They can also be deployed in non-serverless environments for specific needs, offering flexibility.

Azure App Service

App Service enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and high availability.

- **Broad Language Support:** Develop in your preferred language, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python.
- **No Server Management:** Focus on code – App Service handles server infrastructure, patching, and scaling.
- **Automatic Scaling & High Availability:** Seamlessly scales resources up or down to meet demand and ensures app uptime.
- **Continuous Deployment:** Automate deployments from GitHub, Azure DevOps, or any Git repository for streamlined workflows.
- **Platform Flexibility:** Supports both Windows and Linux environments for deployment options.
- **HTTP-Based Service:** Ideal for hosting web applications, REST APIs, and mobile backends.

Types of Sevices

- Web Apps
- API apps
- mobile apps
- Web jobs

App Service handles most of the infrastructure decisions you deal with in hosting web-accessible apps:

- Deployment and management are integrated into the platform.
- Endpoints can be secured.

- Sites can be scaled quickly to handle high traffic loads.
- The built-in load balancing and traffic manager provide high availability.

1. **Web Apps:**

- **Supported Languages:** Build dynamic websites using ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python.
- **OS Flexibility:** Choose between Windows or Linux for your web app's foundation.

2. **API Apps:**

- **RESTful API Development:** Create secure, scalable RESTful APIs using your preferred language and framework.
- **Swagger Integration:** Leverage Swagger for API documentation and simplified integration.
- **Azure Marketplace Distribution:** Publish your API for broader consumption through Azure Marketplace.

3. **WebJobs:**

- **Background Task Automation:** Run background processes seamlessly within your web app, API app, or mobile app.
- **Programming Language Options:** Utilize .exe, Java, PHP, Python, or Node.js programs or scripts.
- **Trigger-Based Execution:** Schedule tasks or trigger them based on specific events.

4. **Mobile Apps:**

- **Simplified Back-End Development:** Quickly establish a robust back end for your iOS and Android mobile applications.
- **Azure Portal Management:** Configure key functionalities like data storage, authentication, push
notifications, and custom logic directly within the Azure portal.
- **Cloud Database Integration:** Store mobile app data securely in a cloud-based SQL database.
- **User Authentication:** Integrate common social providers like Microsoft Account, Google, Twitter, and Facebook for user authentication.

- **Push Notification Delivery:** Send targeted notifications to your mobile app users.
- **Custom Back-End Logic:** Implement custom server-side functionality using C# or Node.js.
- **Mobile SDK Support:**
  Leverage Azure App Service's SDKs to streamline development for native iOS and Android apps, Xamarin, and React Native environments.

In summary, Azure App Service empowers developers to build and host a diverse range of applications – from web apps and APIs to mobile backends and background jobs. Its flexibility, scalability, and managed infrastructure make it a compelling choice for developers seeking a robust cloud hosting platform.

Azure Networks

Azure virtual networks act like secure highways in the cloud, allowing your resources (VMs, web apps, databases) to communicate with each other, the internet, and even your on-premises network.

Azure virtual networking supports both public and private endpoints to enable communication between external or internal resources with other internal resources.

Isolation And Segmentation

Azure virtual networks provide a foundation for creating private networks within Azure. These networks isolate your resources (VMs, web apps, databases) from the public internet, enhancing security. Here's a simplified breakdown:

- **Isolation:** Virtual networks create private address spaces for your resources, keeping them separate from the public internet.
- **IP Addresses:** You define a custom IP address range for your virtual network, ensuring these
  addresses are not routable over the public internet.
- **Subnets:** Further segmentation is achieved by dividing the virtual network address space into subnets, which can group related resources.
- **Name Resolution:** Azure's built-in name resolution service or your own internal/external DNS

servers can be used for efficient resource discovery within the network.

In essence, Azure virtual networks offer a secure and organized way to connect your cloud resources, forming the building blocks for robust cloud architectures.

Internet Communications

You can enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer.

Communication between Azure Resources

1. **Virtual Network Connectivity:**
    - This method allows various Azure resources within the same virtual network to communicate directly with each other. This includes:
        - Virtual Machines (VMs)
        - App Service environments (for Power Apps, etc.)
        - Azure Kubernetes Service (AKS) clusters
        - Azure virtual machine scale sets
2. **Service Endpoints:**
    - This approach enables secure communication between Azure resources in a virtual network and specific Azure services. Traffic travels over the Microsoft Azure backbone network, never entering the public internet. Examples include:
        - Azure SQL databases
        - Azure storage accounts

Benefits of both methods:

- Enhanced security: Communication remains within the secure confines of the Azure network.
- Optimized routing: Traffic takes the most efficient path within the Azure infrastructure.

Communicate with on-premises resources

Azure virtual networks allow you to seamlessly extend your local network to the cloud. This enables secure communication between your on-premises resources and Azure services.

1. **Point-to-Site VPN:**
   - Ideal for individual users who need secure remote access to specific resources within your Azure virtual network.
   - Users initiate encrypted VPN connections from their devices to connect directly to the virtual network.
2. **Site-to-Site VPN:**
   - Perfect for establishing a secure connection between your entire on-premises network and your Azure virtual network.
   - Creates an encrypted tunnel over the internet, allowing devices in both environments to communicate as if they were on the same local network.
3. **Azure ExpressRoute:**
   - Provides the most robust connection option – a dedicated private link directly between your on-premises network and Azure, bypassing the public internet altogether.
   - Offers superior bandwidth and enhanced security compared to VPNs, making it ideal for mission-critical workloads and sensitive data transfer.

Choosing the right method depends on your specific needs:

- For individual remote access, point-to-site VPN offers a simple and secure solution.
- For broader connectivity between your entire on-premises network and Azure, site-to-site VPN provides a cost-effective option.
- When security and bandwidth are paramount, Azure ExpressRoute establishes the most reliable and secure private connection.

Route Traffic Management and Filtering

Default Routing:

- By default, Azure automatically routes traffic between:

    - Subnets within a virtual network
    - Connected virtual networks
    - On-premises networks (if connected)
    - The internet (if public IP addresses are used)

- **Custom Routing (Optional):**
    - **Route Tables:** Define granular rules for traffic flow between subnets. You can create custom route tables to control how data packets are directed.
    - **Border Gateway Protocol (BGP):** Used in conjunction with VPN gateways, Route Server, or ExpressRoute to propagate routing information from your on-premises network to Azure virtual networks.
- **Traffic Filtering:**
    - **Network Security Groups (NSGs):** Azure resources that contain rules to allow or block traffic based on:
        - Source and destination IP addresses
        - Ports
        - Protocols
    - **Network Virtual Appliances (NVAs):** Specialized VMs acting as firewalls or WAN optimizers, providing advanced traffic filtering capabilities.

In essence, Azure virtual networks offer a comprehensive suite of tools to manage and secure the flow of data within your cloud environment. This ensures optimal network performance and enhanced security for your resources.

Connect Virtual Networks

Virtual Network Peering:

- Enables direct connections between two virtual networks.
- Traffic stays private on the Microsoft backbone network, bypassing the public internet.
- Resources in peered networks can communicate seamlessly with each other.

- Peering can connect virtual networks even across different Azure regions, forming a global interconnected network.

2. User-Defined Routes (UDRs):

- Provide granular control over routing tables within a virtual network or between peered networks.
- Allow you to define custom rules for how data packets are directed between subnets or virtual networks.
- Offer greater flexibility in managing network traffic flow within your Azure environment.

Choosing the Right Method:

- Use virtual network peering when you need direct, private communication between resources in separate virtual networks.
- Use UDRs when you require more granular control over traffic flow within a network or between peered networks.

Together, virtual network peering and UDRs empower you to build secure and adaptable network architectures in Azure.

Azure Virtual Private Networks

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks. VPNs can enable networks to safely and securely share sensitive information.

VPN gateways

An Azure VPN gateway acts as a secure bridge between your Azure virtual network and on-premises resources or other virtual networks. It facilitates private encrypted communication over the public internet.

Connectivity Options:

- **Site-to-Site VPN:** Connects your on-premises datacenter to an Azure virtual network.

- **Point-to-Site VPN:** Enables individual devices to securely connect to a virtual network.
- **Network-to-Network VPN:** Connects virtual networks to each other for broader communication within Azure.

2. Secure Tunneling:

- All data transfer is encrypted within a private tunnel, ensuring security while traversing the internet.

3. Single Gateway, Multiple Connections:

- A single VPN gateway per virtual network can manage connections to various locations, including on-premises sites and other virtual networks.

4. VPN Types: Policy-Based vs. Route-Based

- **Policy-Based VPN:**
  - Uses statically defined IP address ranges to determine traffic encryption.
  - Well-suited for simple network configurations with minimal changes.
- **Route-Based VPN (Recommended):**
  - Leverages network routing protocols to decide which tunnel to use for each data packet.
  - More flexible and adaptable to network changes, such as adding new subnets.
  - Preferred choice for on-premises device connections, virtual network connections (network-to-network), point-to-site connections, multisite connections, and coexistence with Azure ExpressRoute gateways.

5. Authentication:

- Azure VPN gateways primarily use pre-shared keys for authentication, providing a shared secret for secure communication.

High Availability Scenarios

Azure VPN Gateway offers several mechanisms to guarantee business continuity and minimize downtime for your connections:

1. Active/Standby (Default):

- This is the default deployment model for VPN gateways.
- Behind the scenes, Azure actually provisions two VPN gateway instances – one active and one standby.
- If a disruption occurs with the active instance, the standby automatically takes over, ensuring minimal interruption (usually just a few seconds) to ongoing connections.

2. Active/Active Configuration (BGP Required):

- This approach utilizes two active VPN gateway instances, each with a unique public IP address.
- You establish separate VPN tunnels from your on-premises device to both public IP addresses, achieving load balancing and increased availability.
- For even greater redundancy, you can deploy an additional VPN device on-premises.

3. ExpressRoute Failover:

- Configure a VPN gateway as a backup for your Azure ExpressRoute connection.
- While ExpressRoute offers built-in resiliency, it's not immune to outages.
- A VPN gateway acting as a failover path ensures connectivity to your virtual networks even if an ExpressRoute disruption occurs.

4. Zone-Redundant Gateways (Availability Zones):

- In regions with Availability Zones, deploy your VPN gateways in a zone-redundant configuration for enhanced resiliency and scalability.
- This physically and logically separates gateway instances within a region, protecting your on-premises network connectivity from zone-level failures.
- Zone-redundant gateways require specific SKUs and utilize Standard public IP addresses instead of Basic ones.

Choosing the Right Approach:

- Active/Standby (default) offers a solid foundation for most scenarios.

- Consider active/active for situations requiring load balancing and maximum availability.
- Utilize ExpressRoute failover when a backup connection is crucial for critical workloads.
- Zone redundancy is ideal for regions with Availability Zones to safeguard against zone-specific outages.

Azure ExpressRoute

Azure ExpressRoute offers a dedicated and secure connection between your on-premises network and Microsoft cloud services, bypassing the public internet. Here's a breakdown of key features and benefits:

How it Works:

- Establish an ExpressRoute circuit with a connectivity provider.
- Connect your offices, data centers, or other facilities to Microsoft cloud services like Azure and Microsoft 365.
- Choose from various connectivity options: any-to-any network, point-to-point Ethernet, or virtual cross-connection.

Benefits:

- **Reliability and Speed:** ExpressRoute avoids the public internet, resulting in more reliable connections, faster speeds, and lower latency.
- **Security:** Data travels on a private connection, minimizing security risks associated with the public internet.
- **Global Reach:** Connect to Microsoft cloud services across all regions and even establish
  communication between your geographically remote sites using ExpressRoute Global Reach.
- **Dynamic Routing:** Border Gateway Protocol (BGP) ensures efficient routing between your network and Microsoft cloud resources.
- **Built-in Redundancy:** Inherent redundancy within ExpressRoute and the option to configure multiple circuits guarantee high availability.

Connectivity Models:

- **CloudExchange Co-location:** Connect virtually to the Microsoft cloud from your co-located facility.

- **Point-to-Point Ethernet:** Establish a dedicated Ethernet connection between your site and Microsoft.
- **Any-to-Any Connection:** Integrate your Wide Area Network (WAN) with Azure for seamless connectivity across your locations.
- **ExpressRoute Direct:** Connect directly to Microsoft's global network at peering locations for high-bandwidth workloads.

Security Considerations:

- While ExpressRoute secures your data transfer, certain traffic like DNS queries and content delivery requests may still utilize the public internet.

In essence, Azure ExpressRoute provides a reliable, secure, and high-performance connection to Microsoft cloud services, ideal for organizations seeking a robust and private cloud connectivity solution.

Azure DNS

Azure DNS is a cloud-based domain hosting service offered by Microsoft Azure. It allows you to manage your domain names using the same familiar Azure platform you use for other cloud services.

Here's a breakdown of the key benefits:

- **Reliability and Performance:**
  - Leverages Microsoft's global network for high availability and fast response times.
  - Uses anycast networking to route DNS queries to the closest server for optimal performance.
- **Security**:
  - Built on Azure Resource Manager with robust security features:
    - Role-based access control (RBAC) for granular permission management.
    - Activity logs for monitoring and troubleshooting.
    - Resource locking to prevent accidental modifications.
- **Ease of Use:**
  - Manage DNS records for both Azure services and external domains from a central location.

    - Integrates seamlessly with the Azure portal, PowerShell, CLI, and SDKs for familiar management experience.
- **Advanced Features:**
    - **Customizable Virtual Networks:** Use your own domain names within private Azure virtual networks.
    - **Alias Records:** Simplify management by pointing domain names to Azure resources like public IP addresses or Content Delivery Network (CDN) endpoints.

In summary, Azure DNS offers a reliable, secure, and user-friendly domain hosting solution that integrates effortlessly with other Azure services.

Azure Storages

Azure Storage Accounts

A storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in this account is secure, highly available, durable, and massively scalable.

When you create your storage account, you'll start by picking the storage account type. The type of account determines the storage services and redundancy options and has an impact on the use cases. Below is a list of redundancy options that will be covered later in this module:

- Locally redundant storage (LRS)
- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Zone-redundant storage (ZRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

Type	Supported Services	Redundancy Options	Usage

Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type.
Premium block blobs	Blob Storage (including Data Lake Storage)	LRS, ZRS	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency.
Premium file shares	Azure Files	LRS, ZRS	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares.
Premium page blobs	Page blobs only	LRS	Premium storage account type for page

			blobs only.

Storage Account Endpoints

Azure Storage Accounts: Unique Namespace for Your Cloud Data

Azure Storage Accounts provide a fundamental element for storing your data within Azure. Here's a key benefit to remember:

- **Unique Namespace:** Each storage account has a unique name, ensuring a distinct identifier for your data objects within Azure.

Naming Rules:

- Storage account names must be:
  - Between 3 and 24 characters long.
  - Composed only of lowercase letters and numbers.
- Uniqueness across Azure: No two storage accounts can share the same name.

This naming convention guarantees a well-organized and identifiable storage structure for your cloud resources in Azure.

Storage Service	Endpoint
Blob Storage	https://<storage-account-name>.blob.core.windows.net
Data Lake Storage Gen2	https://<storage-account-name>.dfs.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net
Queue Storage	https://<storage-account-name>.queue.core.windows.net
Table Storage	https://<storage-account-name>.table.core.windows.net

Azure Storage Redundancy

Azure Storage offers robust data protection mechanisms to safeguard your information from potential disruptions. Here's a breakdown of the key concepts:

Data Redundancy:

- Your data is always stored in multiple copies within Azure Storage.
- This redundancy ensures your storage accounts meet their availability and durability targets, even in unforeseen circumstances.

- Common threats mitigated by redundancy include:
    - Hardware failures
    - Network outages
    - Power disruptions
    - Natural disasters

Choosing the Right Redundancy Option:

The ideal redundancy option depends on your specific needs, balancing cost and availability requirements. Here are key factors to consider:

- **Replication within the Primary Region:** Azure offers various replication options within the primary region where your storage account resides. These options provide different levels of data protection.
- **Geo-Replication (Optional):**
    - Replicate your data to a secondary region geographically distant from the primary region.
    - This offers superior protection against large-scale regional disasters.
- **Read Access to Geo-Replicated Data (Optional):**
    - Configure your geo-replicated data to allow read access from the secondary region if the primary region becomes unavailable.
    - This ensures business continuity and minimizes downtime during disruptions.

By carefully considering these factors, you can select the optimal Azure Storage redundancy configuration that aligns with your specific data protection and accessibility requirements.

Redundancy in the Primary Region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region, locally redundant storage (LRS) and zone-redundant storage (ZRS).

Locally Redundant Storage

Locally redundant storage (LRS) is a cost-effective storage option within Azure Storage, but it offers the most basic level of data redundancy. Here's a breakdown of its key characteristics:

- **Replication:** Data is replicated three times within the same data center where your storage account resides.
- **Durability:** LRS provides at least 11 nines of durability (99.999999999%) for your data objects over a year.
- **Cost:** LRS is the most affordable redundancy option in Azure Storage.
- **Data Protection:** LRS safeguards your data against hardware failures like server rack or drive malfunctions.

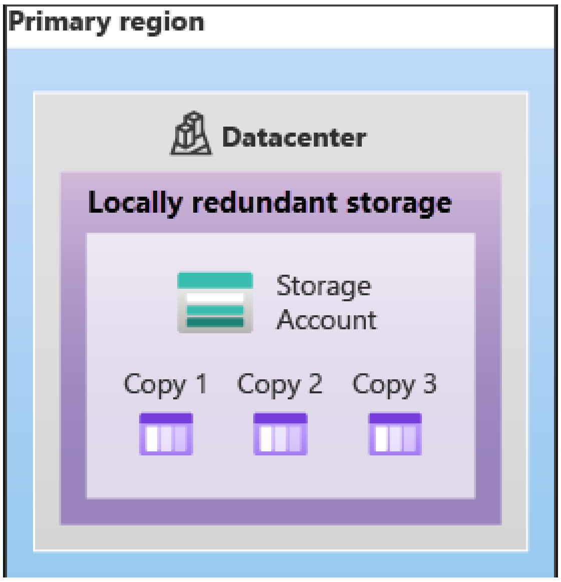
Limitations of LRS:

- **Disaster Vulnerability:** If a large-scale disaster (fire, flood) strikes the data center, all
  replicas of your storage account data might be lost or unrecoverable.
- **Limited Availability:** LRS doesn't offer read access to replicated data in case the primary data center becomes unavailable.

When to Use LRS:

- Suitable for storing non-critical data that can be easily recreated in case of a disaster.
- Ideal for scenarios where cost is a primary concern and data availability during outages is not essential.

Microsoft recommends using alternative redundancy options like zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS) for scenarios requiring higher data availability and protection against regional disasters. These options offer data replication across geographically dispersed locations, ensuring business continuity and minimizing downtime during disruptions.



Zone-Redundant Storage

Zone-redundant storage (ZRS) is a data redundancy option in Azure Storage designed for high availability within Availability Zone-enabled regions. Here's a detailed explanation of its features and benefits:

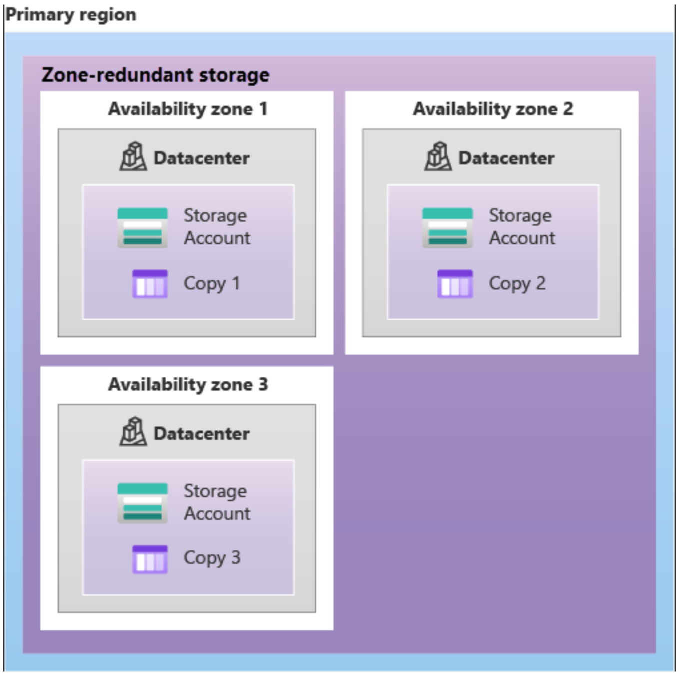
- **Synchronous Replication:** ZRS replicates your data objects synchronously across all three
  Availability Zones in the primary region you select. This ensures that your data is always up-to-date across all zones.
- **Durability:** ZRS offers exceptional durability of at least 12 nines (99.9999999999%) for your stored objects over a year.
- **Data Availability:** Even if an entire Availability Zone becomes unavailable, your data remains
  accessible for both read and write operations. There's no need to remount Azure file shares from connected clients.
- **Networking Updates:** When a zone outage occurs, Azure might initiate network updates like DNS repointing to ensure continued data access. These updates may
  temporarily impact applications that access data before the updates are complete.

Use Cases for ZRS:

- **High Availability:** ZRS is ideal for scenarios where maintaining continuous data access is critical, even during zone-level outages.

- **Data Governance:** ZRS keeps your data replicated within a specific region, which can be helpful for adhering to data residency regulations.

In summary, ZRS provides a compelling redundancy option for workloads demanding high availability within a region. It offers synchronous replication, exceptional durability, and uninterrupted data access during zone disruptions, making it a strong choice for critical business applications.



Redundancy in a Secondary Region

For applications requiring high durability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region. If the data in your storage account is copied to a secondary region, then your data is durable even in the event of a catastrophic failure that prevents the data in the primary region from being recovered.

When you create a storage account, you select the primary region for the account. The paired secondary region is based on Azure Region Pairs, and can't be changed.

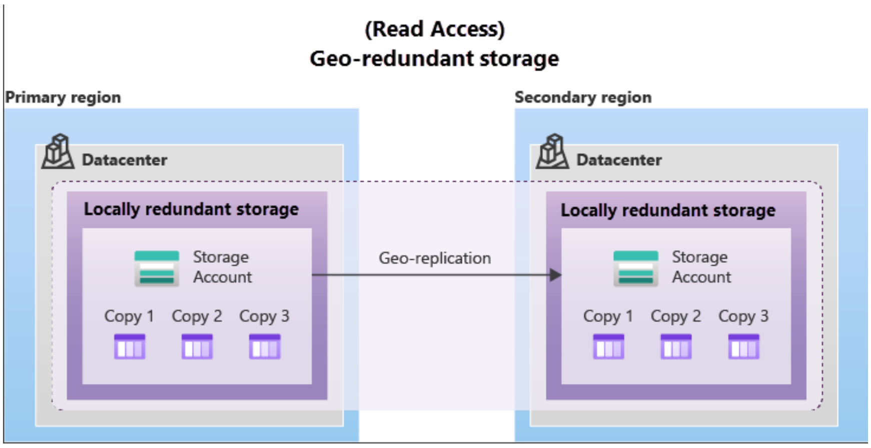
Azure Storage offers two options for copying your data to a secondary region: geo-redundant storage (GRS) and geo-zone-redundant storage (GZRS). GRS is similar to running LRS in two regions, and GZRS is similar to running ZRS in the primary region and LRS in the secondary region.

By default, data in the secondary region isn't available for read or write access unless there's a failover to the secondary region. If the primary region becomes unavailable, you can choose to fail over to the secondary region. After the failover has completed, the secondary region becomes the primary region, and you can again read and write data.

> Because data is replicated to the secondary region asynchronously, a failure that affects the primary region may result in data loss if the primary region can't be recovered. The interval between the most recent writes to the primary region and the last write to the secondary region is known as the recovery point objective (RPO). The RPO indicates the point in time to which data can be recovered. Azure Storage typically has an RPO of less than 15 minutes, although there's currently no SLA on how long it takes to replicate data to the secondary region.

Geo- redundant storage

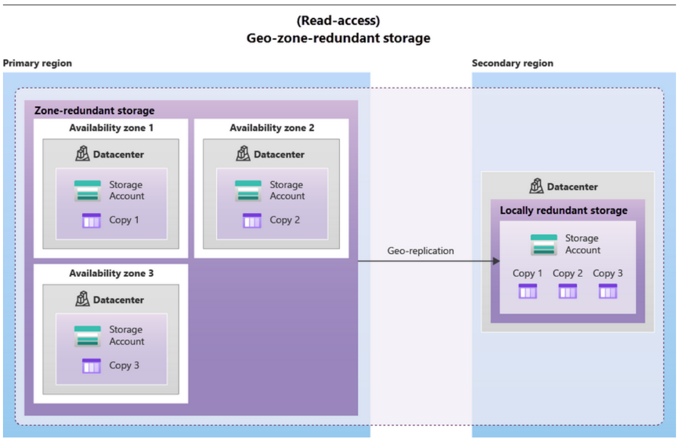
GRS copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region (the region pair) using LRS. GRS offers durability for Azure Storage data objects of at least 16 nines (99.99999999999999%) over a given year.



Geo-zone-redundant storage

GZRS combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region (similar to ZRS) and is also replicated to a secondary geographic region, using LRS, for protection from regional disasters. Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.

GZRS is designed to provide at least 16 nines (99.99999999999999%) of durability of objects over a given year.



Read Access to data in Secondary Region

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. However, if you enable read access to the secondary region, your data is always available, even when the primary region is running optimally. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

Azure Storage Services

- **Azure Blobs**: A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.
- **Azure Files**: Managed file shares for cloud or on-premises deployments.

- **Azure Queues**: A messaging store for reliable messaging between application components.
- **Azure Disks**: Block-level storage volumes for Azure VMs.
- **Azure Tables:** NoSQL table option for structured, non-relational data.

Azure Storage: Benefits

- **Durable and Highly Available:** Redundancy protects your data from hardware failures and outages. Optional replication across regions safeguards against disasters.
- **Secure:** Encrypts data at rest and offers granular access control.
- **Scalable:** Adapts to your storage needs seamlessly.
- **Managed:** Saves you time by handling infrastructure management.
- **Accessible:** Data is reachable from anywhere via HTTP(S) and multiple programming languages. Tools include client libraries, REST API, Azure PowerShell, Azure CLI,
  Azure portal, and Azure Storage Explorer.

Azure Blobs

Azure Blob storage is a cloud-based object storage solution for massive amounts of unstructured data, like text or binary files.

Benefits:

- **Durable and scalable:** Stores large amounts of data reliably with optional disaster recovery via regional replication.
- **Secure**: Encrypts data at rest and offers access control.
- **Easy to use:** Upload blobs and let Azure manage the storage.
- **Accessible from anywhere:** Reach data via HTTP(S) and various tools like client libraries, REST API, and the Azure portal.

Ideal uses:

- Serving images and documents directly on webpages.
- Storing files for shared access.
- Streaming video and audio.

- Data backup, restore, disaster recovery, and archiving.
- Data analysis (on-premises or Azure-hosted services).

Access tiers:

- **Hot**: Frequently accessed data (e.g., website images).
- **Cool**: Infrequently accessed data (e.g., customer invoices) - stored at least 30 days.
- **Cold**: Rarely accessed data (e.g., long-term backups) - stored at least 90 days.
- **Archive**: Rarely accessed data with flexible latency requirements (e.g., legal archives) - stored at least 180 days.

Tier Selection:

- **Account Level:** Only hot and cool tiers can be configured for the entire storage account.
- **Blob Level:** All tiers (hot, cool, cold, archive) can be assigned to individual blobs during upload or even later.

Availability vs. Cost:

- **Cool and Cold Tiers:**
    - Slightly lower availability compared to hot tier (acceptable trade-off for reduced storage costs).
    - Maintain high durability, retrieval latency, and throughput similar to hot data.
    - Incur higher access costs compared to hot tier.
- **Archive Tier:**
    - Lowest storage cost but highest data retrieval and access cost.
    - Data is stored offline, resulting in longer retrieval times.

Azure Files

Azure File storage offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols. Azure Files file shares can be mounted concurrently by cloud or on-premises deployments. SMB Azure file shares are accessible from Windows, Linux, and macOS clients. NFS Azure Files shares are accessible from Linux or macOS clients. Additionally, SMB Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Familiar Access:

- Utilize industry-standard SMB or NFS protocols to access files from various platforms, including Windows, Linux, and macOS.
- **Effortless Management:** No need to manage hardware or operating systems. Azure handles storage infrastructure and maintenance.
- **Simplified Administration:** Manage Azure file shares through the Azure portal, Azure Storage Explorer, PowerShell cmdlets, or Azure CLI.
- **Enhanced Reliability:** Azure Files is built for high availability, eliminating concerns about local outages or hardware failures.
- **Streamlined Application Integration:** Access file share data directly using familiar file system I/O APIs, enabling seamless application migration and development.

Ideal for:

- Replacing on-premises file shares with a cloud-based solution.
- Sharing files across geographically dispersed teams.
- Supporting file-based workloads in Azure virtual machines.

Azure Queues

Azure Queues provide a message queuing service for handling large volumes of messages in the cloud. Here's a breakdown of its key functionalities:

- **Message Storage:** Store a vast number of messages (potentially millions) within your storage account limitations.
- **Message Size:** Each message can hold up to 64 KB of data.
- **Global Accessibility:** Access and manage messages from anywhere via authenticated HTTP(S) calls.
- **Asynchronous Processing:** Queues are ideal for creating work backlogs to be processed asynchronously.

Common Use Cases:

- **Queueing Tasks:** Implement a queue to store tasks that can be processed later by worker applications or Azure Functions.
- **Event Notifications:** Create a notification system by placing messages in the queue when specific events occur.
- **Throttling Workloads:** Use queues to buffer incoming requests and manage peak workloads effectively.

Benefits of Using Queues with Azure Functions:

- **Triggered Actions:** Azure Functions can be configured to initiate actions upon receiving messages from the queue.
- **Decoupled Workflows:** Queues decouple message sending from message processing, enabling independent scaling and development of applications.

In essence, Azure Queues offer a robust and scalable solution for managing message flows and coordinating asynchronous operations in your cloud applications.

Azure Disks

Azure Disks, also known as Azure managed disks, provide high-performance block storage for your Azure Virtual Machines (VMs). They function similarly to physical disks but offer the advantages of virtualisation, including:

- **Simplified Management:** Azure handles disk provisioning and management, freeing you to focus on applications.
- **Enhanced Reliability:** Virtualised storage offers greater resiliency and availability compared to physical disks.

Key Points:

- Block-level storage volumes dedicated to individual VMs.
- Provision the disk, and Azure takes care of the rest.
- Offers superior performance and reliability compared to physical disks.

In essence, Azure Disks streamline storage management for your Azure VMs, ensuring optimal performance and reliability.

Azure Tables

Azure Tables offer a cloud-based NoSQL data storage solution for large volumes of structured, non-relational data. Here's a concise overview of its capabilities:

- **Scalable Storage:** Efficiently handle massive datasets with ease.
- **NoSQL Structure:** Store data without predefined schemas, offering flexibility for evolving data models.
- **Hybrid and Multi-Cloud Friendly:** Accessible from both on-premises and other cloud environments, supporting hybrid and multi-cloud architectures.
- **Always Available:** Designed for high availability, ensuring consistent data access.

Ideal for:

- Storing application data that doesn't require complex relational structures.
- Building web applications or mobile backends that require flexible data models.
- Supplementing relational databases with unstructured data or frequently changing data schemas.

In summary, Azure Tables provide a powerful and scalable solution for managing large, non-relational datasets in the cloud.

Azure Data Migration Options

Azure Migrate: A one-stop hub for managing your cloud migration journey:

- **Unified Platform:** A centralized portal to initiate, manage, and track your migration progress.
- **Diverse Tools:** Offers a range of tools for assessment and migration, including:
  - **Azure Migrate: Discovery and assessment:** Analyzes on-premises servers for migration readiness.
  - **Azure Migrate: Server Migration:** Migrates VMs (VMware, Hyper-V, physical), public cloud VMs, and more to Azure.
- **Integrations:** Works seamlessly with other Azure services, third-party tools, and ISV offerings.

- **Assessment and Migration:** The Azure Migrate hub streamlines both assessment and migration processes for your on-premises infrastructure.

Integrated Tools

- **Azure Migrate: Discovery and assessment**. Discover and assess on-premises servers running on VMware, Hyper-V, and physical servers in preparation for migration to Azure.
- **Azure Migrate: Server Migration**. Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.
- **Data Migration Assistant**. Data Migration Assistant is a stand-alone tool to assess SQL Servers. It helps pinpoint potential problems blocking migration. It identifies unsupported features, new features that can benefit you after migration, and the right path for database migration.
- **Azure Database Migration Service**. Migrate on-premises databases to Azure VMs running SQL Server, Azure SQL Database, or SQL Managed Instances.
- **Azure App Service migration assistant**. Azure App Service migration assistant is a standalone tool to assess on-premises websites for migration to Azure App Service. Use Migration Assistant to migrate .NET and PHP web apps to Azure.
- **Azure Data Box**. Use Azure Data Box products to move large amounts of offline data to Azure.

Azure Data Box

Azure Data Box: Effortless Transfer of Large Datasets

Moving Massive Data to Azure? Azure Data Box Has You Covered.

Azure Data Box offers a secure and efficient solution for migrating large volumes of data (over 40 TB) to Azure, ideal for scenarios with limited network bandwidth.

Key Features:

- **High Capacity:** The Data Box device boasts a massive usable storage capacity of 80 TB.

- **Secure Transport:** Ruggedized casing protects your data during transfer via a regional carrier.
- **Simplified Setup:** Easily configure the Data Box using the local web UI and integrate it with your network.
- **End-to-End Tracking:** The Azure portal monitors the entire data transfer process.

Ideal Use Cases:

- **One-Time Migrations:** Transferring large on-premises data archives to Azure.
- **Media Library Migration:** Moving offline media libraries to create an online Azure repository.
- **Bulk Data Transfers:** Uploading large datasets for initial seeding or periodic backups.
- **Disaster Recovery:** Exporting a copy of Azure data for on-premises disaster recovery.
- **Data Export:** Transferring data out of Azure for regulatory or security purposes.
- **Workload Migration:** Migrating data back to on-premises or another cloud provider.

Data Security:

- Data on the Data Box is encrypted at rest and in transit.
- Upon data upload completion, Data Box disks are wiped clean according to NIST 800-88r1 standards.

In essence, Azure Data Box provides a reliable and cost-effective solution for seamlessly migrating large datasets to or from your Azure cloud environment.

Azure File Movement Options

Beyond Bulk Migration: Efficient Tools for Individual Files and Small Datasets

While Azure provides robust solutions for large-scale data transfers, there are also valuable tools for managing individual files and smaller datasets:

AzCopy:

- Command-line utility for versatile data movement between storage accounts, locally, and even across cloud providers.
- Key functionalities:
    - Uploading and downloading files.
    - Copying files between storage accounts.
    - File synchronisation (one-directional).
- Important Note: AzCopy doesn't offer bi-directional file synchronization based on timestamps or metadata.

Azure Storage Explorer:

- Standalone application for graphical file and blob management within your Azure storage account.
- Available for Windows, macOS, and Linux.
- Leverages AzCopy under the hood for data transfer tasks.
- Enables uploading, downloading, and moving data between storage accounts.

Azure File Sync:

- Tool for centralising file shares in Azure Files while preserving the benefits of on-premises file servers.
- Essentially transforms your Windows file server into a miniature content delivery network (CDN).
- Key advantages:
    - Bi-directional file synchronisation between local servers and Azure Files.
    - Access data locally using various protocols (SMB, NFS, FTPS) supported by Windows Server.
    - Global reach through multiple cache locations.
    - Seamless failover by deploying Azure File Sync on a new server within the same datacenter.
    - Cloud tiering: frequently accessed files stay local, while less used ones are stored cost-effectively in the cloud.

In essence, these tools empower you to efficiently manage and interact with your data in Azure Storage, catering to both large-scale migrations and individual file operations.

Azure Directory Service

Microsoft Entra: A Comprehensive Identity and Access Management Solution

Microsoft Entra offers a robust suite of cloud-based identity and access management (IAM) services that cater to various needs:

Microsoft Entra ID (formerly Azure AD):

- **Cloud-based IAM:** Manages user identities for accessing Microsoft cloud applications and custom-developed applications.
- **On-premises AD Integration:** Connects with on-premises Active Directory for a unified identity experience.
- **Enhanced Security:** Detects suspicious sign-in attempts and offers features like multi-factor authentication and self-service password reset.

Key Users:

- **IT Administrators:** Control access to applications and resources.
- **App Developers:** Integrate single sign-on (SSO) and leverage existing user credentials within applications.
- **Users:** Manage their identities and perform self-service actions.
- **Subscription Users:** Existing subscribers to Microsoft 365, Office 365, Azure, and Dynamics CRM Online already use Entra ID for authentication.

Key Services:

- **Authentication:** Verifies user identities for secure access to applications and resources.
- **Single Sign-On (SSO):** Enables users to access multiple applications with a single login.
- **Application Management:** Provides tools for managing cloud and on-premises applications (e.g., Application Proxy, SaaS apps, My Apps portal).
- **Device Management:** Supports device registration and integration with Microsoft Intune for enhanced control.

Connecting On-premises AD with Entra ID:

- **Microsoft Entra Connect:** Synchronizes user identities between on-premises AD and Entra ID, enabling consistent access controls and features across both environments.

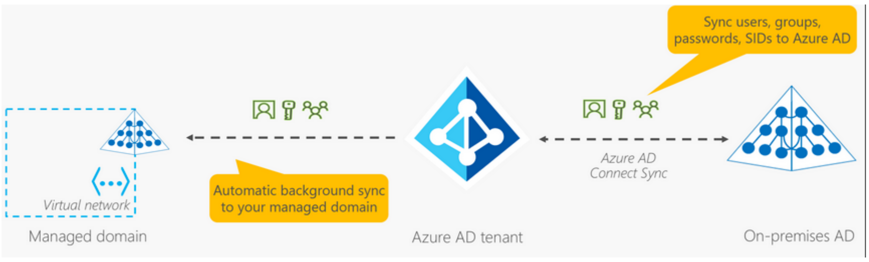
Microsoft Entra Domain Services:

- **Managed Domain Service:** Offers domain join, group policy, LDAP, and Kerberos/NTLM authentication in the cloud.
- **Benefits:**
    - Eliminates the need to manage and patch domain controllers (DCs).
    - Enables legacy applications requiring traditional authentication to run in Azure.
    - Seamless integration with existing Entra tenant and credentials for a smooth lift-and-shift of on-premises resources to Azure.

Key Functionalities:

- Creates a managed domain with a unique namespace in your chosen Azure region.
- Deploys and manages two Windows Server DCs as a replica set within Azure.
- Offers one-way synchronisation of identity information from Entra ID to the managed domain.
- Enables connected Azure applications, services, and VMs to leverage domain join, group policy, LDAP, and Kerberos/NTLM authentication.

In summary, Microsoft Entra provides a centralized and secure IAM solution for managing user identities, applications, and devices across cloud and on-premises environments.


Sync users, groups, passwords, SIDs to Azure AD
Virtual network
Managed domain
Automatic background sync to your managed domain
Azure AD tenant
Azure AD Connect Sync
On-premises AD

Azure Authentication Method

Understanding User Authentication in Azure: Balancing Security and Convenience

Azure offers a robust authentication framework to verify user identities for accessing cloud resources. Here's a breakdown of key concepts:

What is Authentication?

Authentication is the process of confirming a user's (or device's) identity through credentials like passwords. It's analogous to presenting ID while traveling - it verifies your identity but doesn't guarantee access.

Azure's Authentication Methods:

Azure supports various authentication methods, catering to a spectrum of security and convenience needs:

- **Password Authentication:** Traditional method using usernames and passwords (low security, high convenience).
- **Single Sign-On (SSO):**
  Users sign in once and access multiple applications with that credential (increased convenience, security relies on the initial authentication).
- **Multi-factor Authentication (MFA):** Requires an extra verification factor besides passwords (e.g., code sent to phone) for enhanced security.
- **Passwordless Authentication:** Eliminates passwords altogether, using factors like biometrics or possession of a device (high security, high convenience).

Why Use Single Sign-On (SSO)?

- **Reduced Complexity:** Users manage only one ID and password, simplifying access management.
- **Improved Security:** Access control is tied to a single identity, streamlining user role changes and account management.
- **Reduced Help Desk Burden:** Fewer password-related issues like lockouts and resets.

Multi-factor Authentication (MFA) for Enhanced Security:

MFA adds an extra layer of security by requiring two or more verification elements during sign-in, categorized as:

- **Knowledge Factors:** Something the user knows (e.g., challenge question).
- **Possession Factors:** Something the user has (e.g., code sent to phone).
- **Inherent Factors:** Something the user is (e.g., fingerprint, face scan).

MFA significantly strengthens security as compromising a password alone wouldn't grant access.

Microsoft Entra Multifactor Authentication:

This Microsoft service provides MFA capabilities, allowing users to choose additional verification methods during sign-in.

Passwordless Authentication: Convenience Meets Security

Passwordless methods provide a more convenient user experience by eliminating passwords:

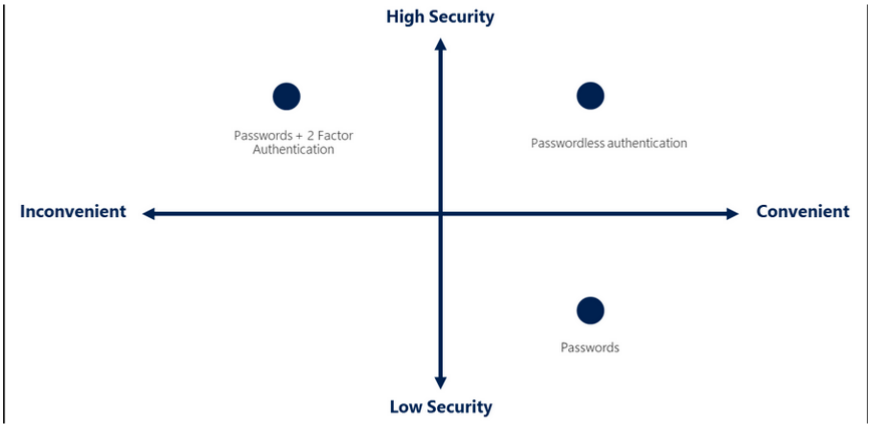
- **Setup:** The user's device (something they have) is registered with Azure for authentication.
- **Verification:** Upon login, the user provides a secondary factor like a PIN, fingerprint, or facial recognition (something they know or are).

Azure's Passwordless Options:

- **Windows Hello for Business:** Ideal for dedicated work PCs, leveraging biometrics and PINs for secure access.
- **Microsoft Authenticator App:** Transforms smartphones into passwordless credentials using notifications and confirmations.
- **FIDO2 Security Keys:** Standards-based physical tokens (USB, Bluetooth, NFC) for secure passwordless authentication.

Choosing the Right Method:

The optimal authentication method depends on your organization's specific security requirements and user convenience preferences. Azure's flexible framework empowers you to strike the right balance.


High Security
Passwords + 2 Factor Authentication
Passwordless authentication
Inconvenient
Convenient
Passwords
Low Security

Azure External Identities

Collaborating Securely with External Identities in Azure

Azure empowers you to interact securely with users outside your organization through Microsoft Entra External Identities. This functionality caters to various scenarios:

Business-to-Business (B2B) Collaboration:

- **Seamless Sign-In:**
  External users leverage their preferred identities (corporate, government-issued, social like Google/Facebook) to access your resources.
- **Managed Access:** You control access to your applications (Microsoft apps, SaaS apps, custom apps) using Microsoft Entra ID or Azure AD B2C.
- **Guest User Representation:** B2B collaboration users appear in your directory as guest users.

B2B Direct Connect:

- **Mutual Trust:** Establish a two-way trust connection with another Microsoft Entra organization for seamless collaboration.
- **Teams Shared Channels:** External users access your resources from within their Teams instance using shared channels.
- **No Directory Representation:** B2B direct connect users aren't in your directory but are visible within Teams shared channels and reports.

Azure Active Directory B2C (B2C):

- **Consumer and Customer Identity Management:** Manage identity and access for consumers and customers using your custom-developed or modern SaaS applications (excluding Microsoft apps) through Azure AD B2C.

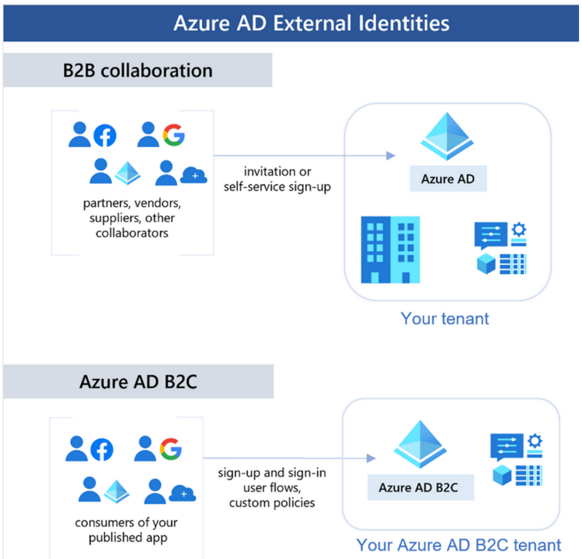
Choosing the Right Capability:

The optimal approach depends on your collaboration needs and resource sharing requirements. You can even combine these capabilities for a tailored solution.

Enabling Collaboration with Microsoft Entra B2B:

- **Simplified Guest User Management:** Easily invite guest users from other tenants (including social identities) to collaborate.
- **Granular Access Control:** Ensure appropriate access for guest users through self-attestation or reviewer participation in access reviews.

In essence, Microsoft Entra External Identities provides a secure and flexible framework for collaboration with external users, fostering a productive and trusted multi-organizational environment.


Azure AD External Identities
B2B collaboration
partners, vendors, suppliers, other collaborators
invitation or self-service sign-up
Azure AD
Your tenant
Azure AD B2C
consumers of your published app
sign-up and sign-in user flows, custom policies
Azure AD B2C
Your Azure AD B2C tenant

Azure Conditional Access

Securing Access with Conditional Access in Microsoft Entra

Microsoft Entra (formerly Azure AD) offers Conditional Access, a powerful tool for managing user access to resources based on various identity signals.

What is Conditional Access?

Conditional Access acts as a gatekeeper, analyzing user identity signals - such as location, device, and user role - to enforce access policies. This empowers

IT admins to:

- **Enhance User Productivity:** Allow secure access from anywhere, anytime.
- **Protect Organizational Assets:** Implement granular access controls to safeguard resources.
- **Contextual Multi-Factor Authentication (MFA):** Prompt for MFA only when necessary (e.g., unusual login location).

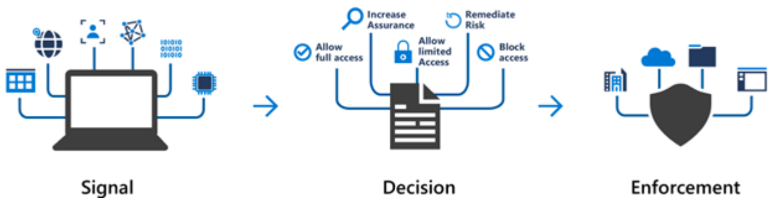
How Does Conditional Access Work?

1. **Signal Collection:** During sign-in, Conditional Access gathers user signals.
2. **Policy Enforcement:** Based on the signals, a decision is made to:
    - **Grant Access:** Allow full access when signals meet policy criteria (e.g., familiar location).
    - **Deny Access:** Block access entirely for high-risk scenarios (e.g., untrusted location).
    - **Challenge for MFA:** Require additional verification (e.g., unknown location).

Conditional Access Use Cases:

- **MFA Based on Context:** Enforce MFA for specific user roles, locations, or network conditions.
- **Approved Client Applications:** Restrict access to services only through authorized applications (e.g., specific email clients).
- **Managed Device Access:** Mandate access from devices meeting security and compliance standards.
- **Blocking Untrusted Access:** Prevent access attempts from unrecognized or risky locations.

In essence, Conditional Access provides a dynamic and layered security approach, ensuring that access to organizational resources is granted based on a combination of factors, not just usernames and passwords.



Azure Role base access control

Granular Access Control with Azure RBAC

Azure Role-Based Access Control (RBAC) empowers you to manage access to cloud resources based on the principle of least privilege. This ensures users have only the permissions necessary to perform their tasks.

Challenges of Manual Permission Management:

- Assigning granular permissions to each individual in a large team becomes cumbersome.
- Updating access requirements with new resources or team members is a constant effort.

Azure RBAC to the Rescue:

- **Predefined Roles:** Azure offers built-in roles with predefined access permissions for common cloud resource actions.
- **Custom Roles:** Create custom roles for specific needs beyond built-in options.
- **Simplified Management:** Assign users or groups to roles, granting them all associated permissions.

Role Assignments and Scopes:

- **Roles:** Define access permissions.
- **Scopes:** Determine which resources the access applies to (e.g., management group, subscription, resource group, individual resource).

Azure RBAC Hierarchy:

- Permissions assigned at a parent scope (e.g., management group) are inherited by child scopes (e.g., subscriptions, resource groups, resources).
    - **Owner:** Full control at all levels within the assigned scope.
    - **Reader:** View permissions within the assigned scope.

Azure RBAC Enforcement:

- Applies to actions initiated against Azure resources through Azure Resource Manager (management service).
- Doesn't enforce access at the application or data level (application security is separate).

- Uses an "allow" model: Combining role assignments grants cumulative permissions.

In essence, Azure RBAC provides a flexible and efficient framework for managing access to Azure resources, ensuring users have the right level of permissions to perform their jobs securely.

Zero Trust Model

Understanding Zero Trust Security: A Paradigm Shift in Cybersecurity

Zero Trust is a security philosophy that challenges traditional network-centric security models. It assumes that no user or device, regardless of location (inside or outside the network), can be inherently trusted. Every access request must be thoroughly verified before granting access to resources.

Why Zero Trust?

The modern digital landscape demands a more robust security approach due to:

- **Increased Complexity:** Hybrid and multi-cloud environments introduce new security challenges.
- **Mobile Workforce:** Traditional perimeter security doesn't protect a distributed workforce.
- **Evolving Threats:** The cyber threat landscape is constantly evolving and requires adaptable defenses.

Zero Trust Security Principles:

- **Verify Explicitly:**
  Every access request, regardless of origin, undergoes rigorous authentication and authorization checks using all available data points.
- **Least Privilege Access:** Users are granted only the minimum access permissions
  (Just-In-Time/Just-Enough-Access) needed for their specific tasks, minimizing potential damage in case of a breach.
- **Assume Breach:** Security
  measures are designed to minimize the impact of a breach by segmenting

access and continuously verifying end-to-end encryption. Advanced analytics are used to detect threats and improve defenses.

Traditional vs. Zero Trust Security:

Traditionally, organizations relied on a "castle and moat" approach, where a secure network perimeter protected internal resources. Only approved devices could access the network, and external access was heavily restricted.

Zero Trust flips this model. It doesn't trust any entity by default, even those within the network perimeter. Everyone must authenticate, and access is granted based on verification, not location.

Benefits of Zero Trust:

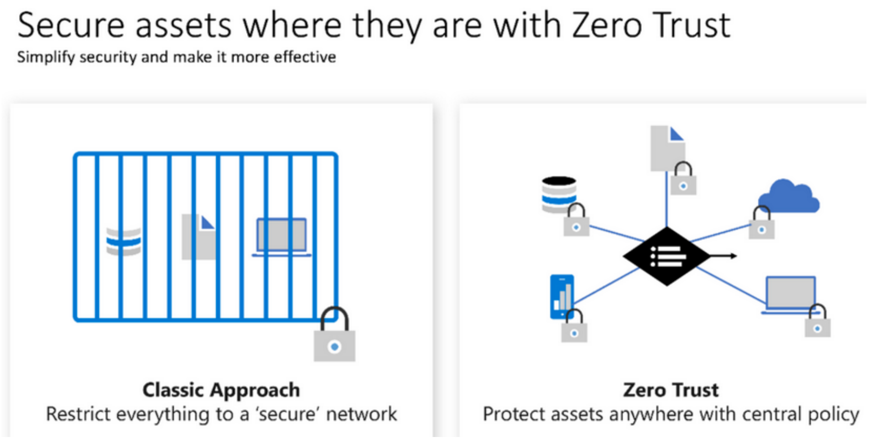
- **Enhanced Security:** Mitigates security risks by minimizing blast radius in case of a breach.
- **Improved User Experience:** Secure access from anywhere, anytime, on any device.
- **Greater Flexibility:** Adapts to the evolving IT landscape and supports a mobile workforce.

Implementing Zero Trust:

The transition to Zero Trust involves a cultural shift within an organization, along with changes in security policies and technologies such as:

- Multi-factor Authentication (MFA)
- Conditional Access
- Identity and Access Management (IAM)
- Data Loss Prevention (DLP)

By embracing Zero Trust, organizations can build a robust and adaptable security posture that protects resources in today's dynamic and interconnected world.



Secure assets where they are with Zero Trust

Simplify security and make it more effective

Classic Approach
Restrict everything to a 'secure' network

Zero Trust
Protect assets anywhere with central policy

Microsoft Defender for Cloud

Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.

Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyber attacks, and streamline security management. Deployment of Defender for Cloud is easy, it's already natively integrated to Azure.

1. **Protection Everywhere:**
    - Monitors Azure services seamlessly.
    - Deploys Log Analytics agents automatically for non-Azure environments.
    - Extends Azure Defender plans to non-Azure machines via Azure Arc for hybrid and multi-cloud setups.
2. **Azure-Native Protections:**
    - Detects threats across Azure PaaS and data services.
    - Helps classify data in Azure SQL and provides vulnerability assessments.
    - Enhances network security by limiting exposure to brute force attacks and implementing just-in-time VM access.
3. **Defend Your Hybrid Resources:**
    - Adds Defender for Cloud capabilities to protect non-Azure servers in hybrid environments.

- Customized threat intelligence and prioritized alerts for specific environments.
- Utilizes Azure Arc for enhanced security features in on-premises machines.

4. **Defend Resources in Other Clouds:**
    - Extends protection to AWS and GCP resources.
    - CSPM features, container threat detection, and advanced defenses for multi-cloud environments.

Assess, Secure, and Defend:

1. **Continuously Assess:**
    - Conducts vulnerability assessments for virtual machines, container registries, and SQL servers.
    - Integrates with Microsoft Defender for Endpoint for comprehensive threat and vulnerability management.
2. **Secure:**
    - Implements security policies tailored to the environment using Azure Policy controls.
    - Monitors and assesses new resource deployments for adherence to security best practices.
    - Utilizes Azure Security Benchmark for secure configuration standards.
    - Provides a secure score for evaluating security posture and prioritizing recommendations.
3. **Defend:**
    - Generates security alerts detailing affected resources and suggesting remediation steps.
    - Offers advanced threat protection features for virtual machines, SQL databases, containers, web applications, and networks.
    - Conducts fusion kill-chain analysis to correlate alerts and understand attack campaigns comprehensively.

4. Advanced Threat Protection

Defender for cloud provides advanced threat protection features for many of your deployed resources, including virtual machines, SQL databases, containers, web applications, and your network. Protections include securing the management ports of your VMs with just-in-time access, and adaptive application controls to create allowlists for what apps should and shouldn't run on your machines.

Conclusion:
Defender for Cloud offers a holistic approach to security management by continuously assessing, securing, and defending your resources and workloads across diverse environments. With its native integration, comprehensive protection features, and actionable insights, it empowers organizations to strengthen their security posture effectively.

Microsoft Purview

Microsoft Purview is a comprehensive suite of solutions designed to provide organizations with a unified view of their data, spanning on-premises, multicloud, and software-as-a-service environments. By leveraging automated data discovery, sensitive data classification, and end-to-end data lineage, Microsoft Purview offers insights that enable effective data management and governance.

Solution Areas:

1. **Risk and Compliance:**
   - Utilizes Microsoft 365 services such as Teams, OneDrive, and Exchange as core components.
   - Aids in protecting sensitive data across various platforms and devices.
   - Identifies data risks and facilitates compliance with regulatory requirements.
   - Streamlines the process of getting started with regulatory compliance.
2. **Unified Data Governance:**
   - Offers robust solutions for managing data across diverse environments.
   - Enables creation of an up-to-date map of the entire data estate, including classification and lineage.
   - Identifies storage locations of sensitive data within the estate.

- Facilitates secure access for data consumers to valuable data.
- Generates insights into data storage and usage patterns.
- Manages access to data securely and at scale.

Key Features:

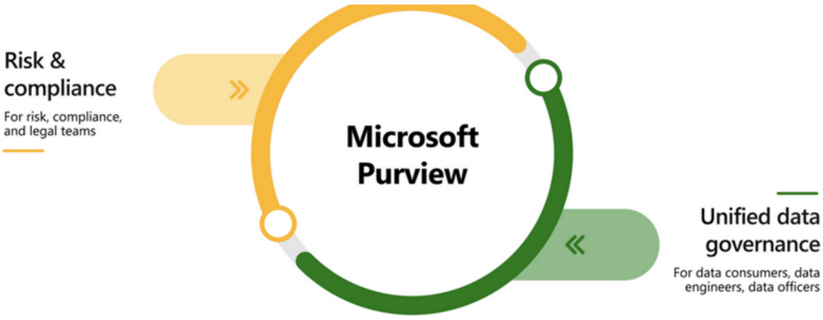
1. **Automated Data Discovery:**
    - Automatically discovers data across on-premises, multicloud, and SaaS environments.
2. **Sensitive Data Classification:**
    - Classifies data based on sensitivity to ensure appropriate protection measures are applied.
3. **End-to-End Data Lineage:**
    - Establishes lineage to track the origin and movement of data throughout its lifecycle.

Benefits:

1. **Comprehensive Insights:**
    - Provides a unified view of the entire data landscape, enhancing visibility and understanding.
2. **Enhanced Security and Compliance:**
    - Helps in protecting sensitive data and ensuring compliance with regulatory standards.
3. **Efficient Data Governance:**
    - Streamlines data management processes and facilitates informed decision-making.
4. **Scalable and Secure Access Management:**
    - Manages access to data securely and efficiently, even at scale.

Conclusion:

Microsoft Purview empowers organizations with the tools and insights necessary to effectively manage, protect, and govern their data across diverse environments. By offering comprehensive solutions for risk and compliance as well as unified data governance, Purview enables organizations to stay in control of their data assets while navigating the complexities of modern data ecosystems.


Risk & compliance
For risk, compliance, and legal teams
Microsoft Purview
Unified data governance
For data consumers, data engineers, data officers

Azure Policy

1. **Policy Definition:**
    - Azure Policy allows you to define individual policies or groups of related policies known as initiatives.
    - Policies enforce rules across resource configurations to maintain compliance with corporate standards.
2. **Policy Evaluation and Enforcement:**
    - Azure Policy evaluates resources and highlights those that are not compliant with defined policies.
    - It can prevent noncompliant resources from being created, ensuring adherence to standards.
3. **Granular Policy Application:**
    - Policies can be set at various levels such as resource, resource group, subscription, etc.
    - Policies are inherited, automatically applying to all resources within the parent grouping.
4. **Built-in Policy Definitions:**
    - Azure Policy comes with built-in policy and initiative definitions covering areas like Storage, Networking, Compute, Security Center, and Monitoring.
    - These predefined policies cover common compliance requirements, simplifying policy management.

5. **Automatic Remediation:**
    - In some cases, Azure Policy can automatically remediate noncompliant resources and configurations to maintain integrity.
    - For instance, missing tags or noncompliant configurations can be automatically fixed by Azure Policy.
6. **Exception Handling:**
    - Azure Policy allows for exceptions to be flagged for specific resources that should not be automatically remediated.
    - This ensures that certain resources can be exempted from automatic fixes while still maintaining compliance.
7. **Integration with Azure DevOps:**
    - Azure Policy integrates with Azure DevOps, applying policies relevant to pre-deployment and post-deployment phases of applications.
    - This ensures that compliance requirements are met throughout the application lifecycle.
8. **Initiatives for Comprehensive Compliance:**
    - Azure Policy initiatives group related policies together to track compliance for larger objectives.
    - Each initiative contains multiple policy definitions aimed at achieving specific compliance goals.

By leveraging Azure Policy's capabilities, organizations can establish and maintain compliance across their Azure resources effectively. From defining policies to automatic enforcement and integration with development pipelines, Azure Policy provides a comprehensive solution for maintaining compliance standards.

Resource Locks in Azure

Resource locks in Azure provide an additional layer of protection against accidental deletion or modification of critical resources. By applying resource locks, you can safeguard resources, resource groups, or even entire subscriptions from unwanted changes.

Types of Resource Locks:
There are two types of resource locks available in Azure:

1. **Delete Lock:**
    - Prevents users from deleting a resource.
    - Authorized users can still read and modify the resource, but deletion is restricted.
2. **ReadOnly Lock:**
    - Prevents users from deleting or updating a resource.
    - Users can only read the resource, similar to the permissions granted by the Reader role.

Managing Resource Locks:
Resource locks can be managed through various methods, including the Azure portal, PowerShell, Azure CLI, or Azure Resource Manager templates.

1. **Azure Portal:**
    - Navigate to the Settings section of any resource's Settings pane in the Azure portal.
    - Here, you can view existing locks, add new locks, or delete existing locks.
2. **PowerShell:**
    - Use PowerShell cmdlets such as `New-AzResourceLock`, `Get-AzResourceLock`, and `Remove-AzResourceLock` to manage resource locks programmatically.
3. **Azure CLI:**
    - Utilize Azure CLI commands such as `az lock create`, `az lock show`, and `az lock delete` to manage resource locks from the command line interface.
4. **Azure Resource Manager Template:**
    - Define resource locks within Azure Resource Manager templates to apply locks during resource provisioning.

Deleting or Changing a Locked Resource:
While resource locks prevent accidental changes, they can still be modified following a two-step process:

1. **Remove the Lock:**
    - To modify a locked resource, the lock must first be removed.

- After removing the lock, users with appropriate permissions can proceed with the desired actions.

2. **Perform the Action:**

    - Once the lock is removed, users can apply any action permitted by their permissions.
    - Resource locks apply independently of RBAC permissions, meaning even resource owners must remove the lock before performing blocked activities.

Conclusion:
Resource locks in Azure provide an essential mechanism for protecting critical resources from accidental deletion or modification. By understanding the types of locks available and how to manage them through various methods, users can ensure the security and integrity of their Azure resources effectively.

Azure Resource Manager and Azure ARM templates

Overview:

Azure Resource Manager (ARM) is the primary deployment and management service for Azure, allowing users to create, update, and delete resources in their Azure accounts. Infrastructure as Code (IaC) is a concept where infrastructure is managed through code, enabling automated and consistent deployment and management of resources.

ARM Benefits:

With Azure Resource Manager, users can:

1. **Declarative Templates:**

    - Manage infrastructure through declarative templates (JSON files) rather than scripts, defining what to deploy to Azure.

2. **Group Management:**

    - Deploy, manage, and monitor resources as a group, simplifying management tasks.

3. **Consistent Deployment:**

    - Re-deploy solutions throughout the development lifecycle with confidence, ensuring consistent resource states.

4. **Dependency Management:**
    - Define dependencies between resources to ensure they're deployed in the correct order.
5. **Access Control:**
    - Apply access control through Role-Based Access Control (RBAC), integrated into the management platform.
6. **Resource Tagging:**
    - Apply tags to logically organize resources and clarify billing.

Infrastructure as Code (IaC):
Infrastructure as Code involves managing infrastructure through code, enabling automated deployments and configurations. ARM templates and Bicep are examples of using IaC with Azure Resource Manager.

ARM Templates:

ARM templates allow users to describe resources in a declarative JSON format, providing several benefits:

1. **Declarative Syntax:**
    - Declare desired infrastructure state without writing procedural commands.
2. **Repeatable Results:**
    - Deploy infrastructure consistently throughout the development lifecycle.
3. **Orchestration:**
    - Azure Resource Manager orchestrates the deployment of resources in the correct order, often in parallel.
4. **Modular Files:**
    - Break templates into reusable components and link them together at deployment time.

Bicep:
Bicep is a language that uses a simpler and more concise syntax than JSON for deploying Azure resources. Benefits of Bicep include:

1. **Support for all Resource Types:**

    - Immediate support for all preview and GA versions of Azure services.

2. **Simple Syntax:**
    - Concise and easy-to-read syntax, requiring no previous knowledge of programming languages.
3. **Repeatable Results:**
    - Deploy infrastructure consistently, with idempotent Bicep files enabling multiple deployments to produce the same resource states.
4. **Orchestration and Modularity:**
    - Resource Manager orchestrates deployments, and Bicep supports modular code for reusability and simplicity.

By leveraging ARM templates or Bicep, users can implement Infrastructure as Code practices to automate and manage Azure resources efficiently and consistently.

Azure Health, Azure Service Health , Azure Monitor

Managing your Azure resources effectively requires a comprehensive approach to security, performance, and cost-efficiency. Here's a breakdown of three key Azure services that work together to achieve these goals:

1. Azure Advisor: Recommendations at Your Fingertips

- **Function:** Analyzes your Azure resources and offers personalized recommendations.
- **Benefits:**
    - Saves time on cloud optimization.
    - Improves reliability, security, performance, and operational excellence.
    - Reduces costs through optimization.
- **Key Features:**
    - Suggested actions for each recommendation (take action, postpone, dismiss).
    - Categorization of recommendations for easy navigation (Reliability, Security, Performance, Operational Excellence, Cost).
    - Availability via Azure portal and API.

    - Notification options for new recommendations.

2. Azure Service Health: **Keeping You Informed**

- **Function:** Provides a comprehensive view of your Azure resource health.
- **Components:**
    - **Azure Status:** Global view of Azure service health (outages).
    - **Service Health:** Focused view on your specific Azure services and regions (outages, planned maintenance).
    - **Resource Health:** Tailored view of individual resource health (virtual machines, etc.).
- **Benefits:**
    - Proactive awareness of potential issues.
    - Ability to plan for maintenance activities.
    - Historical data for trend analysis.
    - Support links for troubleshooting.

3. Azure Monitor: **In-Depth Monitoring and Alerting**

- **Function:** Collects data, analyzes it, visualizes it, and allows actions based on insights.
- **Scope:** Monitors Azure resources, on-premises resources, and even multi-cloud resources.
- **Components:**
    - **Log Analytics:** Tool for writing and running queries on collected data (simple or complex analysis).
    - **Azure Monitor Alerts:** Automated notifications when thresholds are crossed (metrics or logs).
    - **Application Insights:** Monitors web applications (Azure, on-premises, or other clouds).
- **Benefits:**
    - Real-time and historical performance insights across all layers of your application architecture.
    - Customizable dashboards and visualizations.

    - Automated alerts for critical events.
    - Ability to trigger autoscaling based on metrics.

Working Together:

These three services work in concert to optimize your Azure environment:

- **Azure Advisor** identifies areas for improvement.
- **Azure Service Health** keeps you informed about potential issues.
- **Azure Monitor** provides detailed insights and allows proactive actions.

By leveraging this powerful trio, you can ensure the security, performance, and cost-effectiveness of your Azure resources, giving you peace of mind and a strong foundation for your cloud applications.