Zane Alderfer

Professor Rieks

IST 615

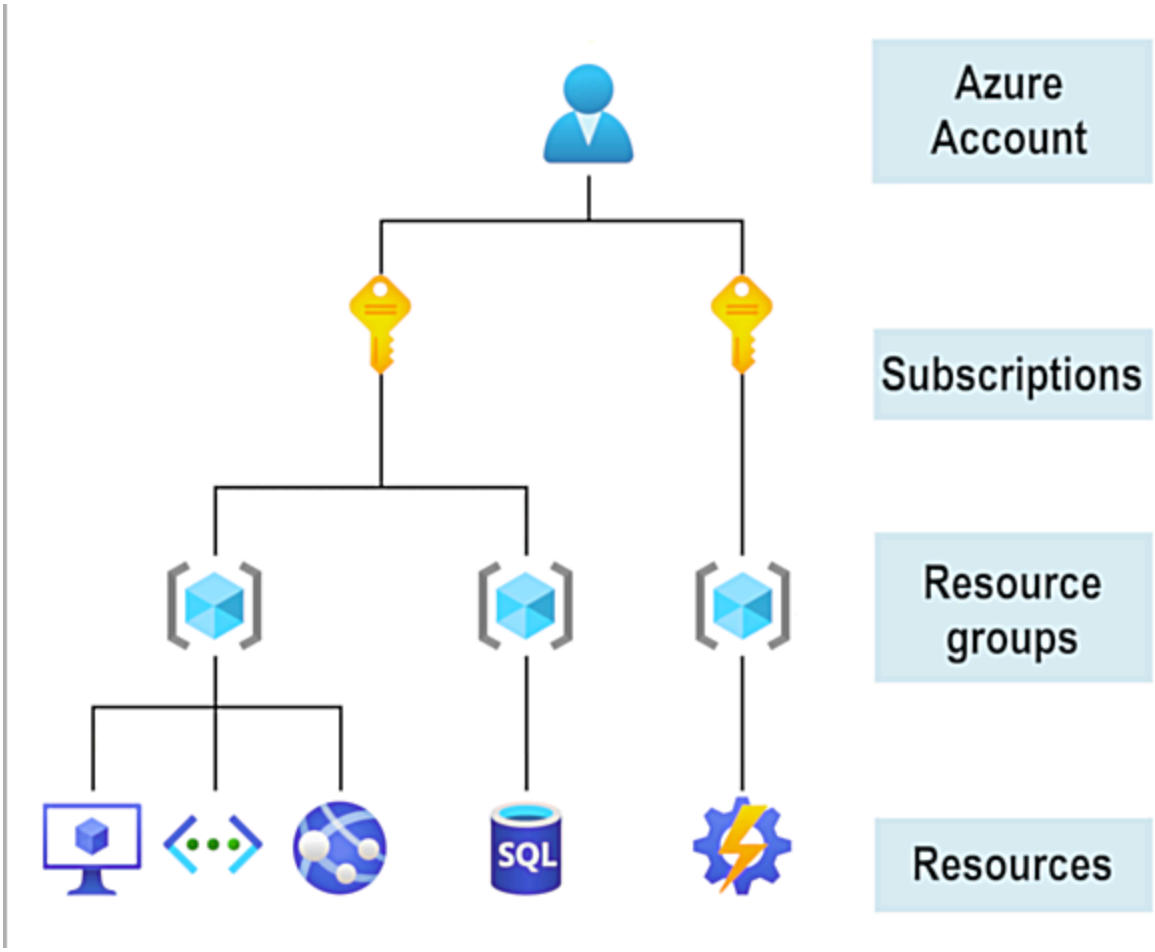
2/27/23

Azure Lab Part 2

Describe the core architectural components of Azure

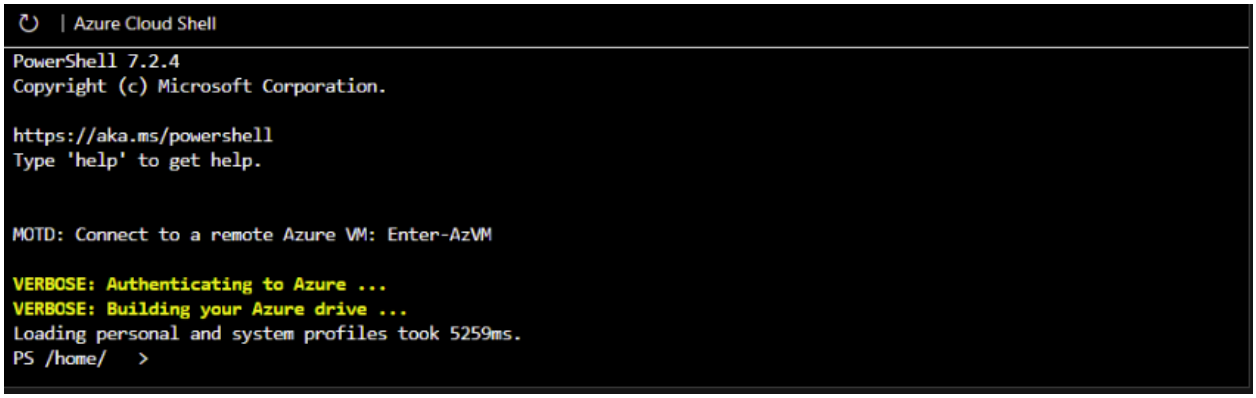
Azure provides more than 100 services that enable you to do everything from running your existing applications on virtual machines to exploring new software paradigms, such as intelligent bots and mixed reality.

Using Azure requires the user to create an account, create subscriptions which then leads to the user being able to create resource groups as seen in the graphic below.

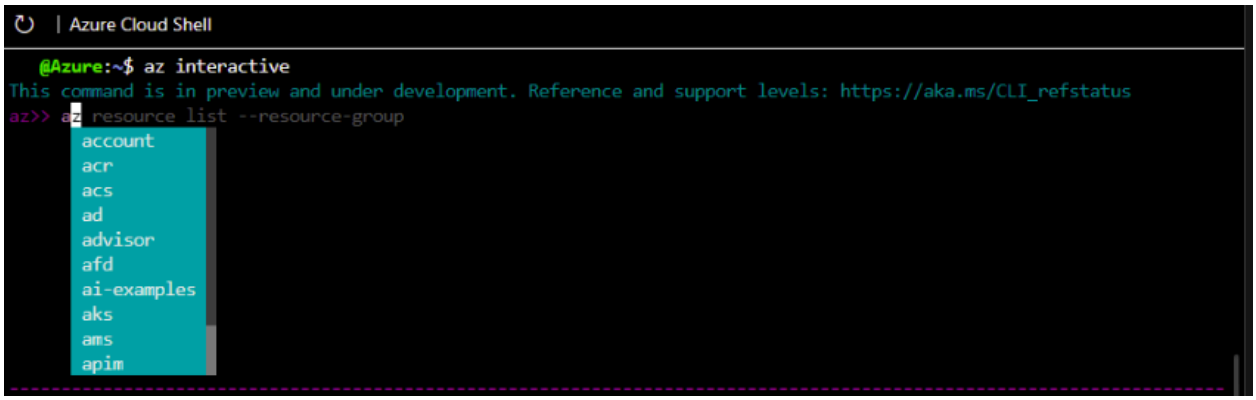


Azure offers free accounts as well as student free accounts. The free account allows free access to products for 12 months and a credit to use for 30 days while the free student account allows free access for 12 months and credit to use for the first 12 months.

Using the learn sandbox of Azure calls for some tasks: Use the powershell, Use the Bash CLI, Use Azure CLI interactive mode, and Use the Azure portal. Launching the powershell CLI looks like the graphic below.

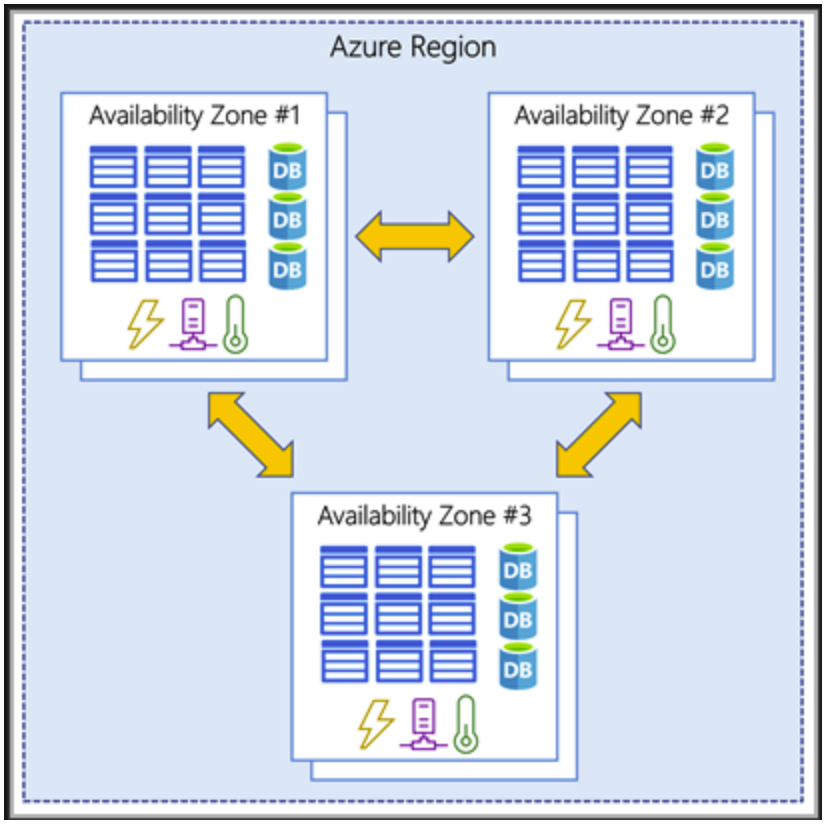


The BASH CLI is similar to the powershell CLI and can be used if the user is more familiar with it. You can use the letters az to start an Azure command in the BASH mode. Using the Azure CLi interactive mode allows the user to work in what resembles an IDE as seen below.

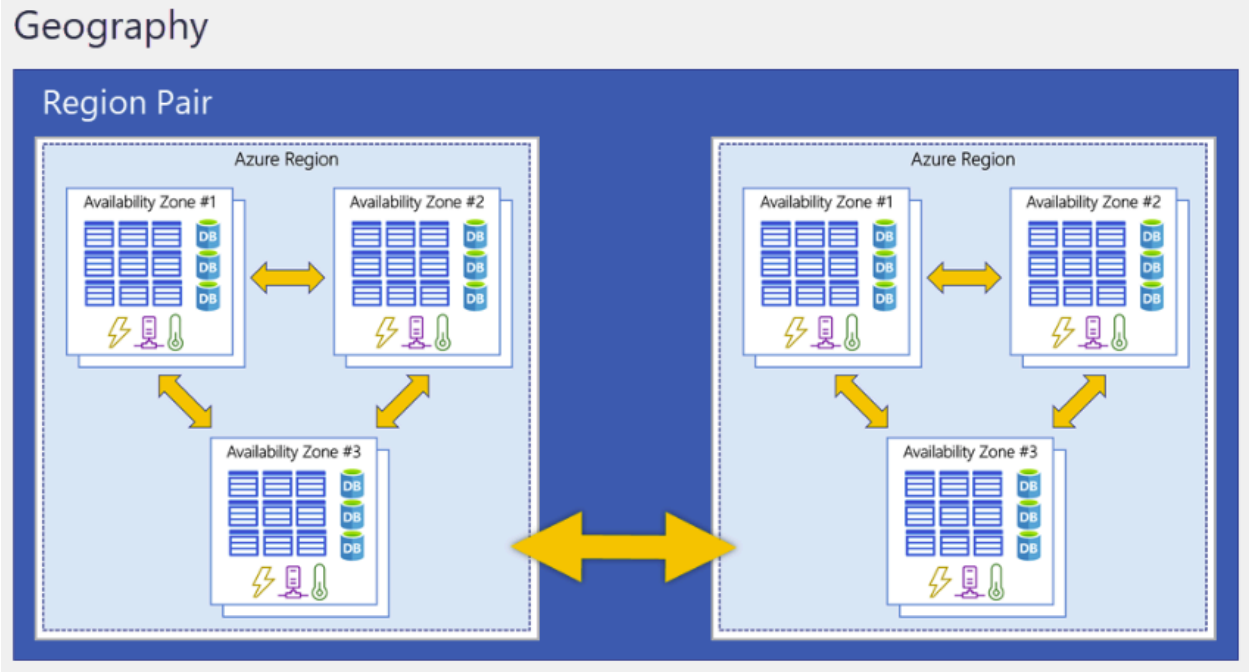


Finally, the Azure portal can bring the user directly to sandbox exercises with a link.

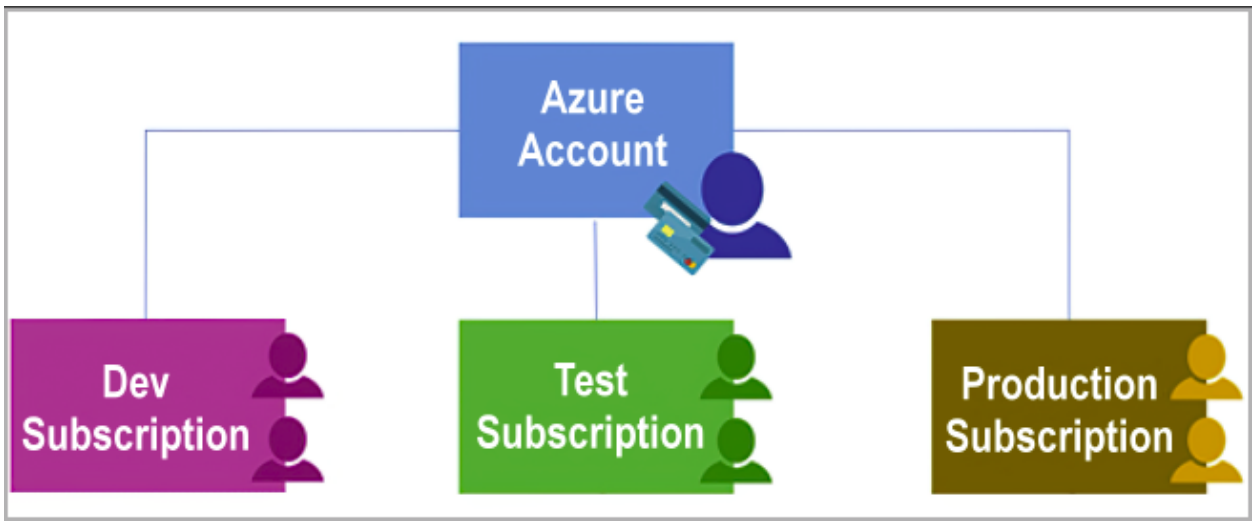
Like other cloud computing services, Azure uses availability zones, region pairs to effectively operate their data centers. A region contains at least one data center. If it has multiple, they are networked together with a low-latency network. Availability zones are physically separate data centers within an Azure region as seen below.



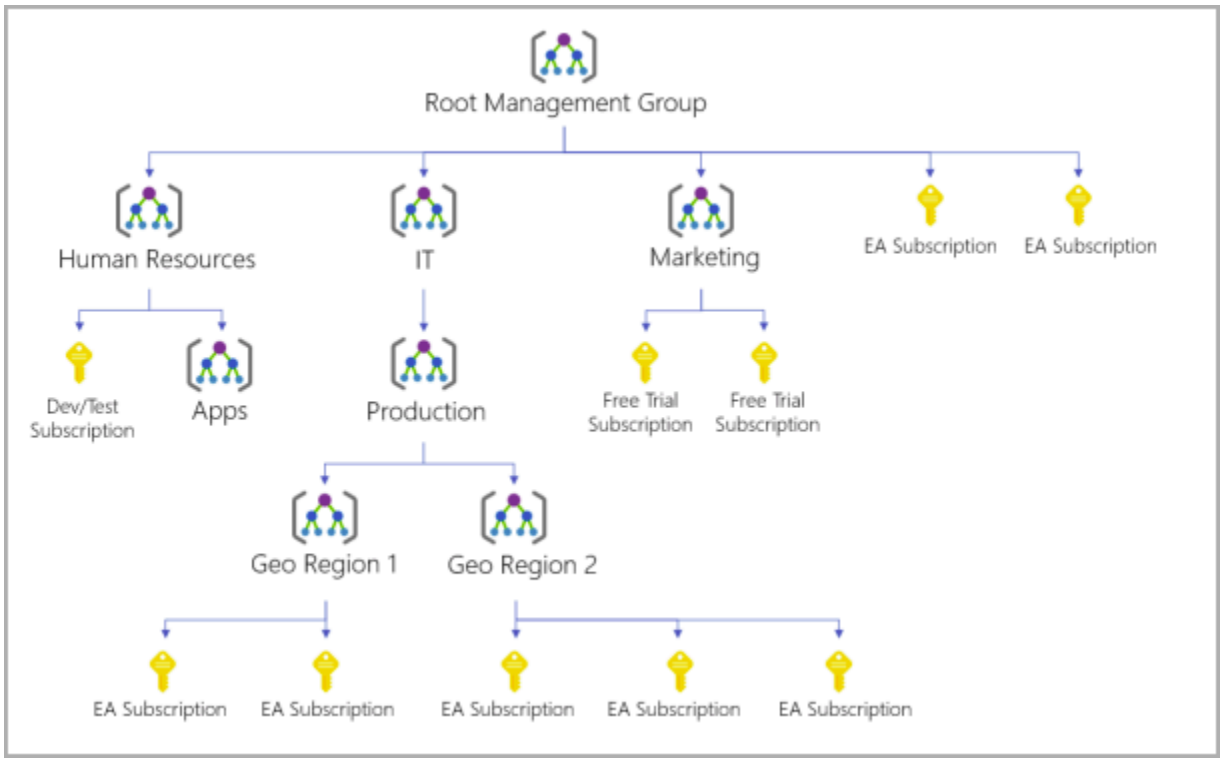
There are also region pairs involved which allow for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect an entire region. An example of this can be seen below.



Azure has resources and resource groups. Anything you create, provision, deploy, etc. is a resource. VMs, databases, cognitive services are all considered resources within Azure. Resource groups are then groupings of these resources. Subscriptions are a unit of management, billing, and scale. This is a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing. Using Azure requires an Azure subscription. This can be seen below.



Management Groups are the final piece. If you have many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups can do that. An example of this can be seen below.



Describe Azure compute and networking services

You can run single VMs for testing, development, or minor tasks. Or you can group VMs together to provide high availability, scalability, and redundancy. Scale sets let you create and manage a group of identical, load-balanced VMs. If you simply created multiple VMs with the same purpose, you'd need to ensure they were all configured identically and then set up network routing parameters to ensure efficiency. Availability sets are another tool to help you build a more resilient, highly available environment. Availability sets group VMs by updating the domain and faulting domain.

Azure Virtual Desktop provides centralized security management for users' desktops with Microsoft Entra ID. The data and apps are separated from the local hardware. The actual desktop and apps are running in the cloud, meaning the risk of confidential data being left on a personal drive is reduced.

Containers are a visualization environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. Container instances offer the fastest and simplest way to run a container in Azure, apps are similar to instances but can incorporate load balancing and scaling. Azure Kubernetes Service is a container orchestration service. This manages the lifecycle of containers.

Azure Functions are ideal when you're only concerned about the code running your service and not about the underlying platform or infrastructure. They are often used when your platform needs to work in response to an event. Functions scale automatically and can be either stateless or stateful.

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. App service includes full support for web apps by using numerous coding languages on a Windows or LInux operating system. You can get support for API apps as well. Webjob apps are supported which are often used to run background tasks as part of an application logic. Mobile apps are also supported by app services.

Azure provides the following key networking capabilities:

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources
- Route network traffic
- Filter network traffic
- Connect virtual networks

Isolation and segmentation allow you to create multiple virtual networks. This defines an IP address. Internet communications are enabled from the internet by assigning a public IP address to an Azure resource. Using Virtual networks and service endpoints, Azure resources can communicate securely with each other. Using point-to-site virtual private network connections, site-to-site, and Azure ExpressRoute, resources can be linked together in on-premise environments.

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in a dedicated subnet of the virtual network and enable the following connectivity:

- Connect on-premises datacenters to virtual networks through a site-to-site connection.
- Connect individual devices to virtual networks through a point-to-site connection.
- Connect virtual networks to other virtual networks through a network-to-network connection.

By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure. With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an active/active configuration. Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections. ExpressRoute circuits have resiliency built in. In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration.

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider. There are several benefits to using ExpressRoute as the connection service between Azure and on-premises networks.

- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute Global Reach.
- Dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP).
- Built-in redundancy in every peering location for higher reliability.

ExpressRoute enables direct access to the following services in all regions:

- Microsoft Office 365
- Microsoft Dynamics 365
- Azure compute services, such as Azure Virtual Machines
- Azure cloud services, such as Azure Cosmos DB and Azure Storage

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. ExpressRoute uses the BGP. BGP is used to exchange routes between on-premises networks and resources running in Azure. Each connectivity provider uses redundant devices to ensure that connections established with Microsoft are highly available. Co-location refers to your datacenter, office, or other facility being physically co-located at a cloud exchange, such as an ISP. Point-to-point ethernet connection refers to using a point-to-point connection to connect your facility to the Microsoft cloud. With any-to-any connectivity, you can integrate your wide area network (WAN) with Azure by providing connections to your offices and datacenters.

Azure DNS leverages the scope and scale of Microsoft Azure to provide numerous benefits, including:

- Reliability and performance
- Security
- Ease of Use
- Customizable virtual networks
- Alias records

DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers, providing resiliency and high availability. Azure DNS is based on Azure Resource Manager, which provides features such as:

- Azure role-based access control (Azure RBAC) to control who has access to specific actions for your organization.
- Activity logs to monitor how a user in your organization modified a resource or to find an error when troubleshooting.
- Resource locking to lock a subscription, resource group, or resource. Locking prevents other users in your organization from accidentally deleting or modifying critical resources.

Azure DNS can manage DNS records for your Azure services and provide DNS for your external resources as well. Azure DNS is integrated in the Azure portal and uses the same credentials, support contract, and billing as your other Azure services. Azure DNS also supports private DNS domains.

Describe Azure storage services

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. Below is a list of redundancy options that will be covered later in this module:

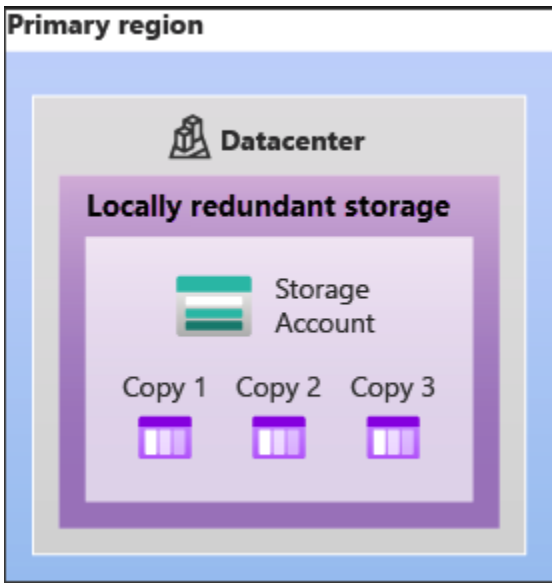
- Locally redundant storage (LRS)
- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Zone-redundant storage (ZRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

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.

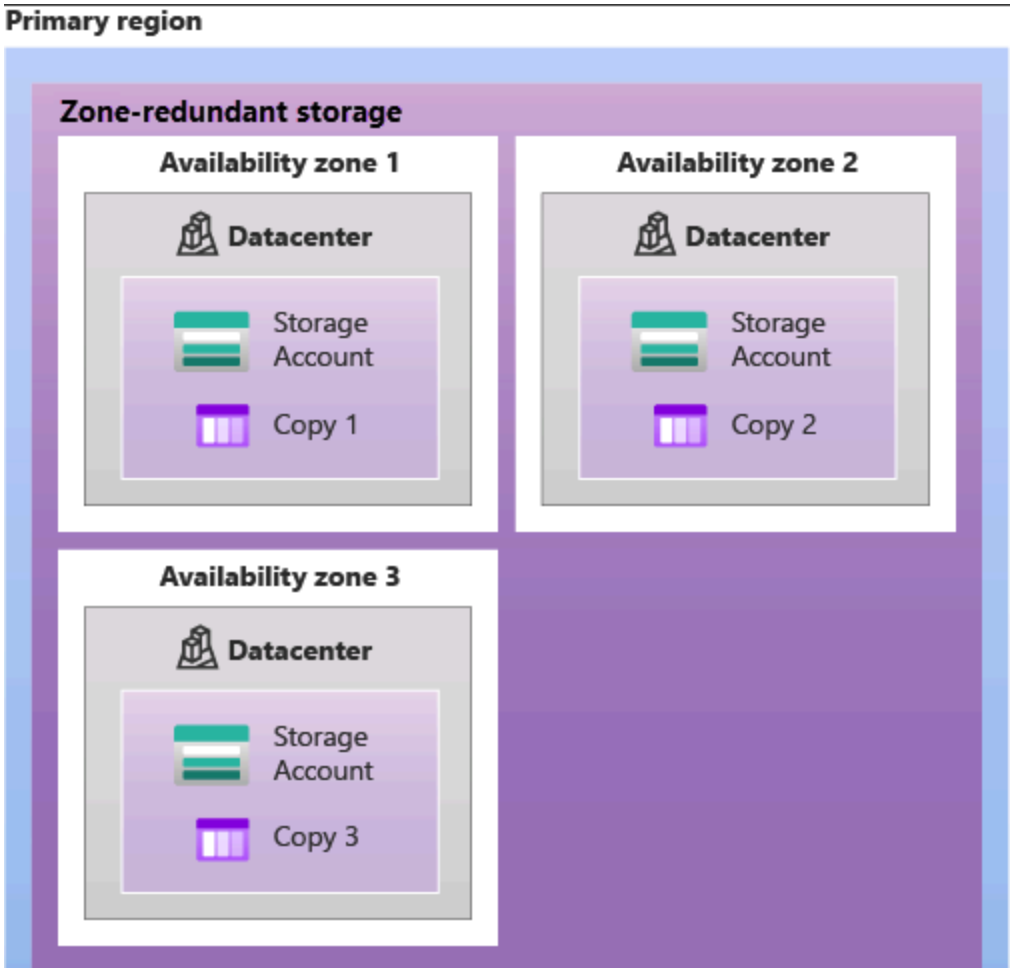
One of the benefits of using an Azure Storage Account is having a unique namespace in Azure for your data. In order to do this, every storage account in Azure must have a unique-in-Azure account name.

Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events such as transient hardware failures, network or power outages, and natural disasters. Redundancy ensures that your storage account meets its availability and

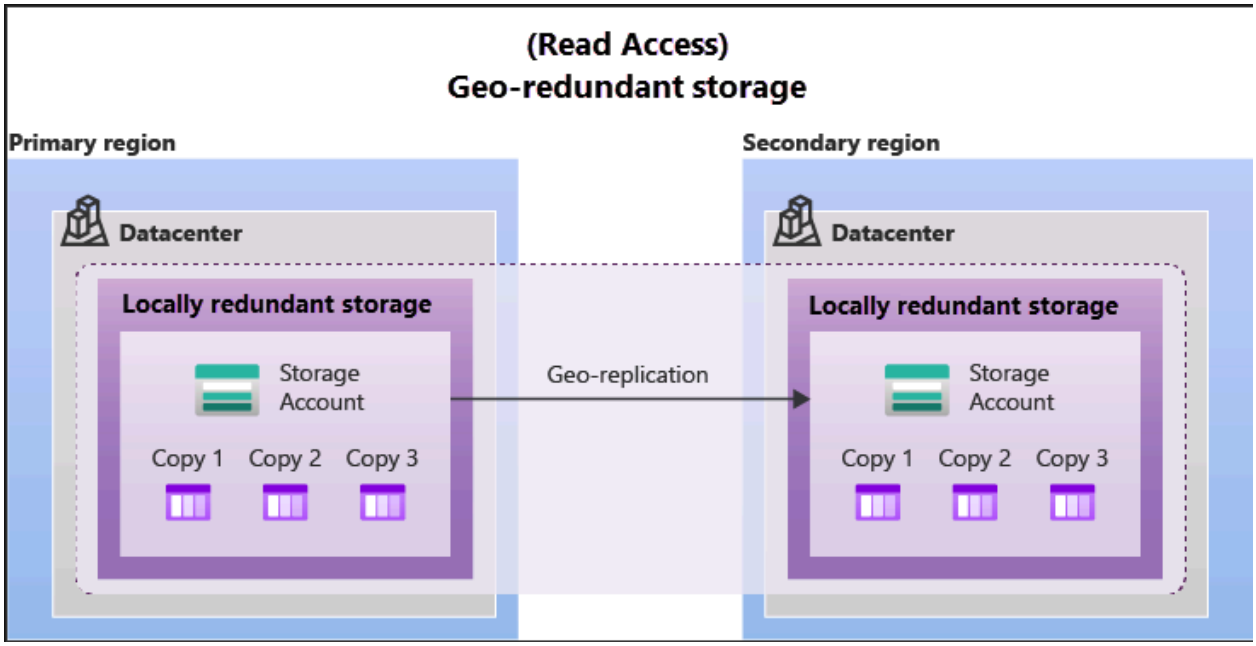
durability targets even in the face of failures. Locally redundant storage (LRS) replicates your data three times within a single data center in the primary region.



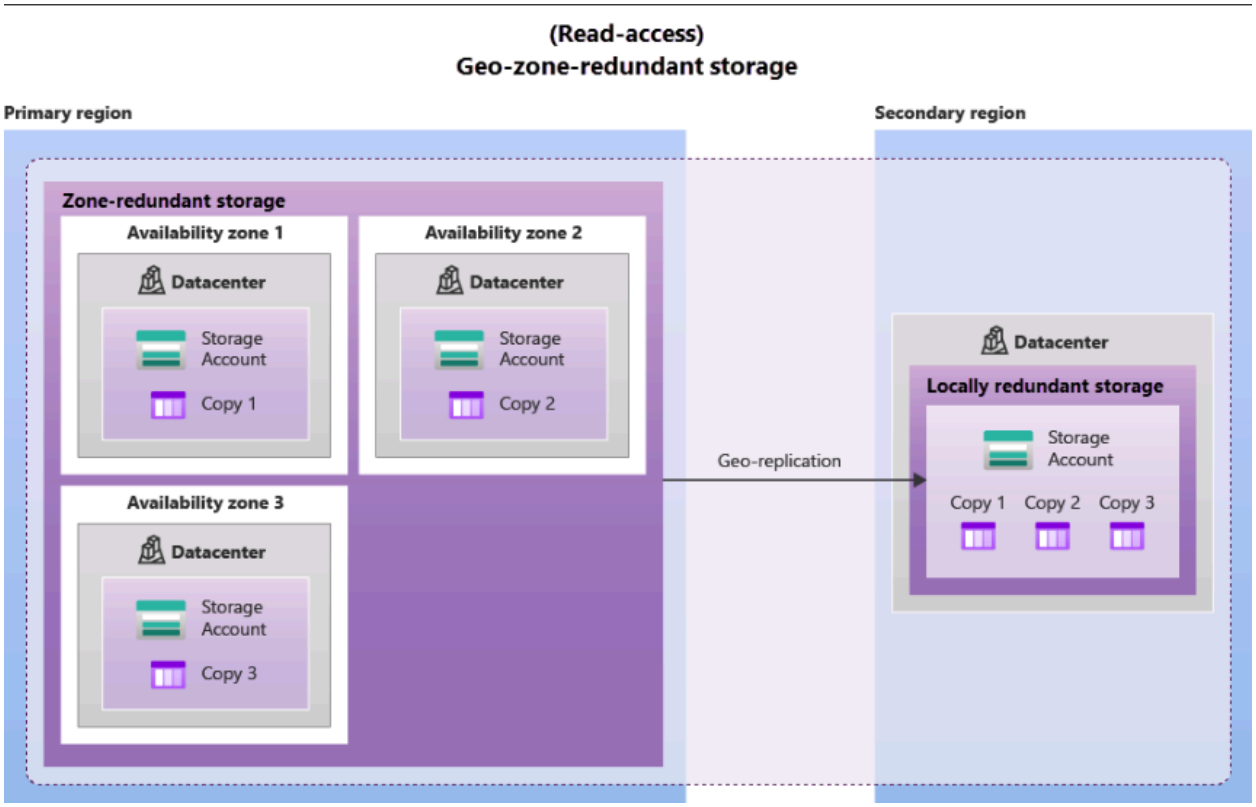
LRS is the lowest-cost redundancy option and offers the least durability compared to other options. For Availability Zone-enabled Regions, zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region.



With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable. GRS copies your data synchronously three times within a single physical location in the primary region using LRS.



GZRS combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication.



Azure Blob storage is an object storage solution for the cloud. It can store massive amounts of data, such as text or binary data. Azure Blob storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold. Objects in blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. Data stored in the cloud can grow at an exponential pace. To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency of access and planned retention period. Data stored in the cloud can be handled differently based on how it's generated, processed, and accessed over its lifetime. 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. Azure Queue storage is a service for storing large numbers of messages. Once stored, you can access the messages from anywhere in the world via authenticated calls using HTTP or HTTPS. Azure Disk storage, or Azure managed disks, are block-level storage volumes managed by Azure for use with Azure VMs. Conceptually, they’re the same as a physical disk, but they’re virtualized – offering greater resiliency and availability than a physical disk. Azure Table storage stores large amounts of structured data.

Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud. Azure Migrate functions as a hub to help you manage the assessment and migration of your on-premises datacenter to Azure. It provides the following:

- **Unified migration platform**: A single portal to start, run, and track your migration to Azure.
- **Range of tools**: A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.
- **Assessment and migration**: In the Azure Migrate hub, you can assess and migrate your on-premises infrastructure to Azure.

Azure Data Box is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device that has a maximum usable storage capacity of 80 terabytes. Data Box is ideally suited to transfer data sizes larger than 40 TBs in scenarios with no to limited network connectivity. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

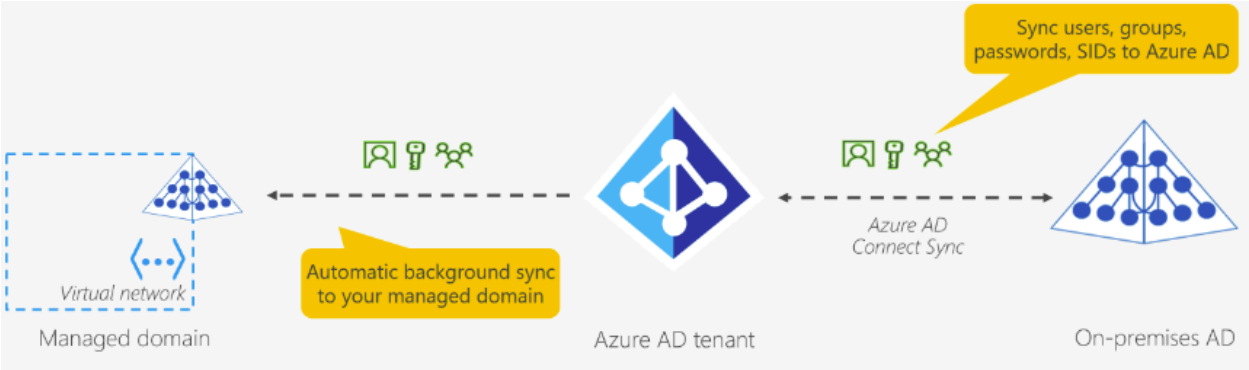
AzCopy is a command-line utility that you can use to copy blobs or files to or from your storage account. With AzCopy, you can upload files, download files, copy files between storage accounts, and even synchronize files. Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your Azure Storage Account. It works on Windows, macOS, and Linux operating systems and uses AzCopy on the backend to perform all of the file and blob management tasks. Azure File Sync is a tool that lets you centralize your file shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server.

Describe Azure identity, access, and security

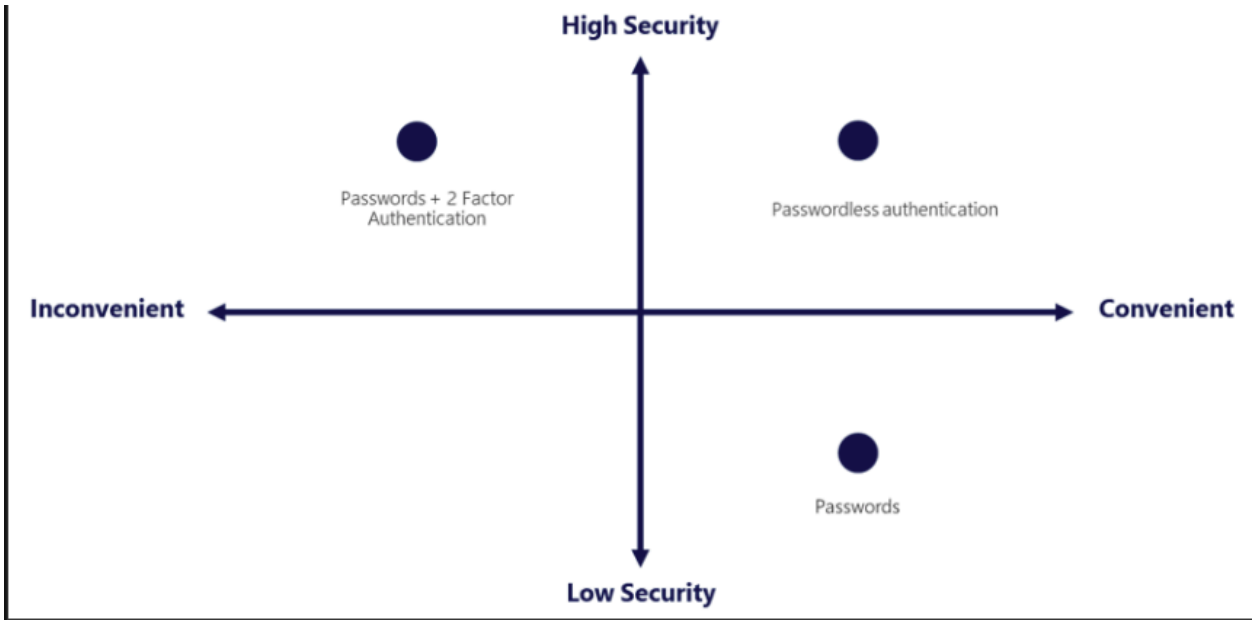
Microsoft Entra ID is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Microsoft Entra ID can also help you maintain your on-premises Active Directory deployment. Microsoft Entra ID is for:

- **IT administrators**. Administrators can use Microsoft Entra ID to control access to applications and resources based on their business requirements.
- **App developers**. Developers can use Microsoft Entra ID to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- **Users**. Users can manage their identities and take maintenance actions like self-service password reset.
- **Online service subscribers**. Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Microsoft Entra ID to authenticate into their account.

If you had an on-premises environment running Active Directory and a cloud deployment using Microsoft Entra ID, you would need to maintain two identity sets. However, you can connect Active Directory with Microsoft Entra ID, enabling a consistent identity experience between cloud and on-premises. Microsoft Entra Domain Services is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. A Microsoft Entra Domain Services managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. When you create a Microsoft Entra Domain Services managed domain, you define a unique namespace. This namespace is the domain name.

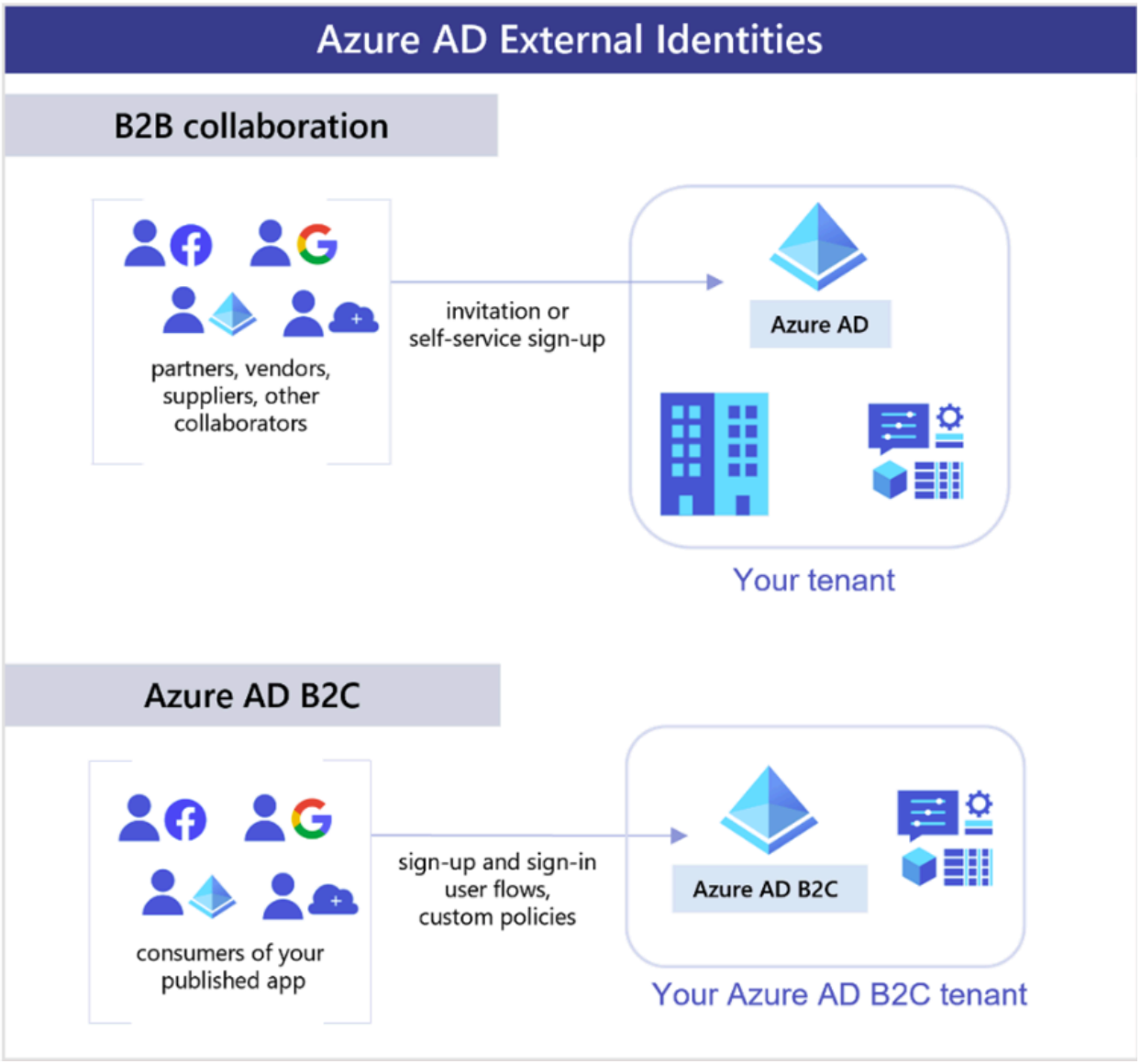


Authentication is the process of establishing the identity of a person, service, or device. It requires the person, service, or device to provide some type of credential to prove who they are.



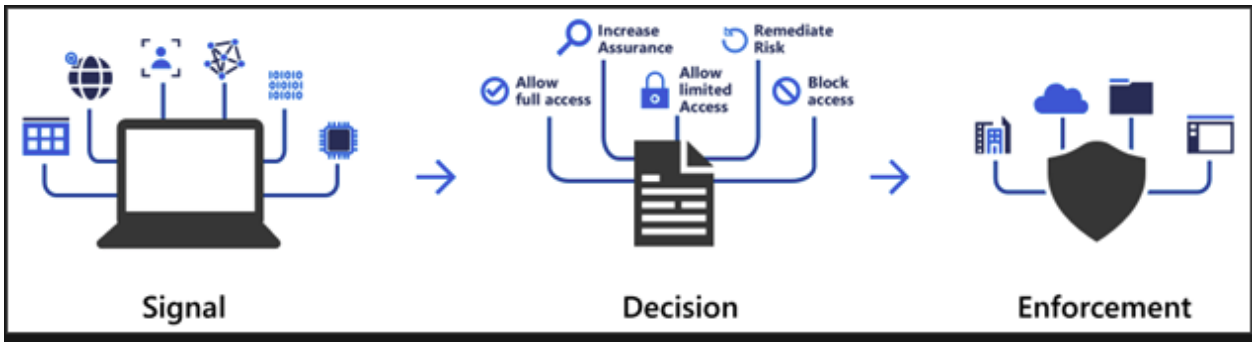
Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications from different providers. For SSO to work, the different applications and providers must trust the initial authenticator. Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process. MFA helps protect against a password compromise in situations where the password was compromised but the second factor wasn't. Features like MFA are a great way to secure your organization, but users often get frustrated with the additional security layer on top of having to remember their passwords. People are more likely to comply when it's easy and convenient to do so. Windows Hello for Business is ideal for information workers that have their own designated Windows PC. You may already be using the Microsoft Authenticator App as a convenient multifactor authentication option in addition to a password. The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication.

An external identity is a person, device, service, etc. that is outside your organization. Microsoft Entra External ID refers to all the ways you can securely interact with users outside of your organization. If you want to collaborate with partners, distributors, suppliers, or vendors, you can share your resources and define how your internal users can access external organizations.

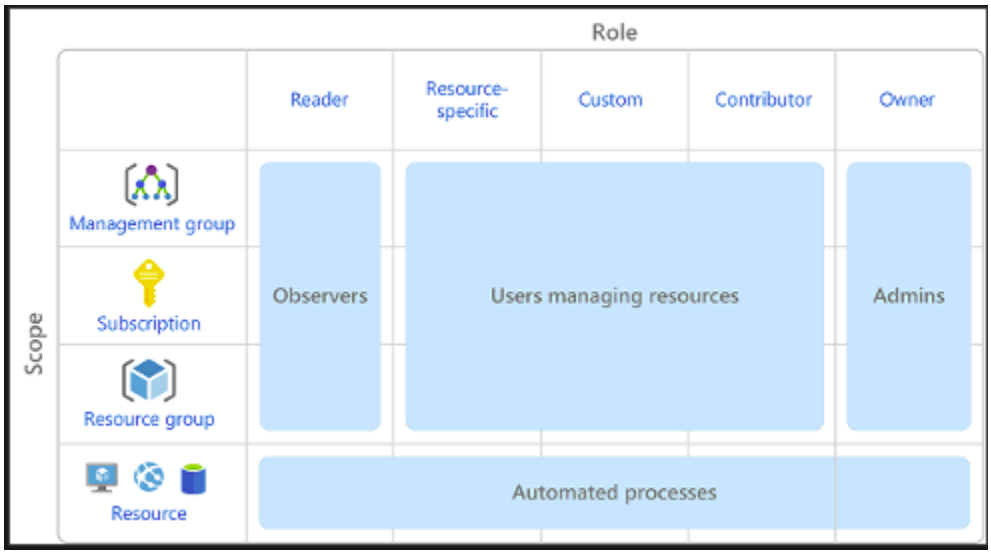


Conditional Access is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and

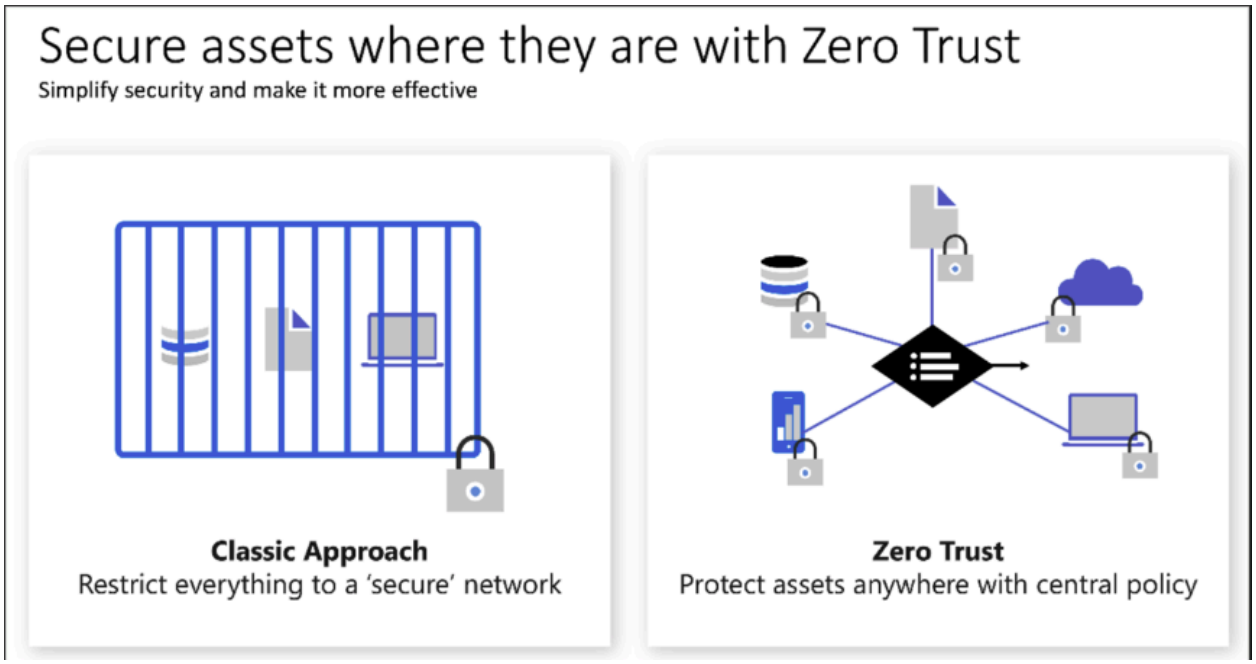
what device the user is requesting access from. Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for a second authentication factor if they're at a known location.



Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to. The following diagram shows the relationship between roles and scopes. A management group, subscription, or resource group might be given the role of owner, so they have increased control and authority.



Zero Trust is a security model that assumes the worst case scenario and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.



The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it. Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense. The identity and access layer is all about ensuring that identities are secure, that access is granted only to what's needed, and that sign-in events and changes are logged. The network perimeter protects from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure. At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network. Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.