What is Azure

What is Azure?

Azure is a ever-growing set of cloud services that help meet current and future business challenges.

What can you do with Azure?

You run virtual machines with your existing applications or explore new software. Azure also has artificial intelligence and machine learning services with many capabilites like with Hearing and Speech.

Azure Accounts

You need a subcription to use Azure services. If you are learning modules within Microsoft, You will have a subscription but its called Learn Sandbox.

If you are using your own applications and business needs, You can create an account and then you can create additional subscriptions. Some companies might have numerous subscriptions. One for your overall business but then seperate subscriptions for development, marketing and sales department. Once you create a subscription, you can start adding resources.

If you are new you can create and account and play around with it. You could create a new subscription that allows you to start paying for Azure services you need beyond the limits of a free acount.

Create an Azure account

You can purchase Azure directly from Microsoft or buy it from a third party. You can even purchase Azure from a managed-cloud solutions for Azure.

What is a Azure free acount?

Azure free acount gives you access to Popular products for 12 months.
You also get $200 credit to use within the first 30 days.
You'll have access to more than 25 products that are always free.

Azure free account is basically a way for new users to get started and explore. You need a phone number to get started, a credit card, and a Microsoft or Github account. The credit card is for verification purposes only. You will not be charged for any services until you upgrade to a paid subcription.

Azure free student account

Free student account gives you access to certain Azure services for 12 months. You also get a $100 credit to use in the first 12 months unlike the reguar Azure free account which offers up to only 30 days. You also get Free access to certain software developer tools. The best part of it, I guess, is you do not need a credit card to sign up! Whooo hoo students!

Learning Sandbox

Learning Sandbox creates temporary subscription that's added to your Azure account. This temporary subscription allows you to create Azure resources during a Learning module. This sandbox would be a preferred method because you can test azure out at no cost.

Describe cloud computing

Cloud computing is the delivery of computing services over the internet. Computing services include common IT infrastructure such as virtual machines, storage, databases, and networking. This also includes things like Internet of Things(IoT), machine learning(ML) and artificial intelligence(AI)

This is great becuase cloud computing uses the internet to deliver these services, it doesn't have to be constrained by phyiscal infrastructure the same way that a traditional datacenter is.

Describe the shared responsibility model

Shared responsibility model, these responsibilities get shared between the cloud provider and the consumer. Physical security, power, cooling, and network connectivity are the responsibility of the cloud provider. At the same time the consumer is responsible for the data and information stored in the cloud, The consumer is also responsible for access security, meaning you only give access to those who need it.

NOTE: An anology, is the Consumer is in charge of whatever they bring into the house and also in charge of securing the house, the Cloud provider is in charge of everything else.

However, if you are using a cloud SQL database, then the user is in charge of the info that gets put into it but the cloud provider is responsible for maintaining the actual database.

Note: If you upload a virtual machine and have the sql database inside of it, the consumer is in charge of the whol sql database including maintenance.

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, etc)
- The accounts and identities of the people, services, and devices within your organization

The cloud provider is always responisble 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

Define Cloud Models

PRIVATE CLOUD MODEL- A private cloud that delivers IT services over the internet that is used by a single entity. Downside, is it comes with greater cost and fewer of the benefits

PUBLIC CLOUD- it is built, controlled, and maintained by a third-party cloud provider. Anyone that wants to purchase cloud services can access and use resources. The general public availability is what separates the public cloud from private key.

HYBRID CLOUD- Uses both public and private clouds in an interconnected environment. This is a really versatile cloud model. For instance, A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources. It also can be used to provide an extra layer of security, like users can flexibly choose which services to keep in public cloud and which to deploy to their private cloud.

MULTI-CLOUD- Uses a service providers cloud model, but also has another service provider cloud service as well. The reason would be that there are different features from different cloud providers. SO in this cloud model you deal with two or more public cloud providers and manage resources and secruity in both environments.

AZURE ARC- is a set of technologies that helps manage your cloud environment. Azure Arc can help manage cloud environment, whether it is public cloud soley on Azure, or a private cloud in your datacenter, a hybrid configuration, or even a mult-cloud environment running on multop cloud providers at once.

AZURE VMWARE SOLUTION- Let's say you already have VMware in a private cloud and want to migrate to a public or hybrid cloud. Azure VMware solution lets you run your VMware workloads in Azure with seamless integration and scalability.

Consumption-based model

CAPITAL EXPENDITURE(CapEx)- Means a one time, up-front expenditure to purchase or secure tangible resources. A new building, repaving the parking lot, building a datacenter, or buying a company vehicle are examples of CapEX.

OPERATION EXPENDITURE(OPEx)- means to spend money on services or products over time. Renting a convention center, leasing a company vehicle, or signing up for cloud services are all examples of OPEx.

Cloud computing falls under Operational expenditures because cloud computing operates on a consumption-based model, With this model you don't pay for the physical infrastructure, the electricity, the security or anything else associated with maintaining a datacenter.

CLOUD PRICING MODELS- Cloud Computing is the delivery of computing services over the internet by using a pay-as-you-go pricing model. You usually pay only for the cloud services you use, which helps you:

- Plan and manage your operating costs
- Run your infrastructure more efficiently
- Scale as your business needs change

Cloud computing is a way to rent compute power and storage from someone else's datacenter. Essentially you could treat the cloud resources like you would with resources in your own datacenter. The big difference with the cloud , is that when you are done using the resources, you give them back and only billed with what you only use.

Benefits of High availability and Scalability

HIGH AVAILABILITY- It is important that the resources are available when needed. High availability focuses on ensuring maximum availability, regardless of disruptions or events that may occur. Azure is a highly available cloud environment with uptime guarantees depending on the service-level agreements(SLA)

SCALABILITY- This refers to the ability to adjust resources to meet demand. If you suddently experience peak traffic and your systems are overwhelmed, the ability to scale means you can add more resources to better handle the increased demand. Another benefit of scalability is that you aren't overpaying for services. Again the cloud is a consumption-based model, you only pay for what you use. If demand drops, you can reduce your resources and because of that, you can reduce your cost.

Scaling has two varieties: Vertical and Horizontal.
Vertical scaling is focused on increasing or decreasing the capabilities of resources. Adding more CPU's or RAM to a virtual machine
Horizontal scaling is adding or subtracting a number of resources. Adding Virutal machines or containers

Benefits of reliability and predictability in the cloud

RELIABILITY- This is the ability of a system to recover from failures and continue to function.

PREDICTABILITY- Microsoft Azure Well-Architected Framework, allows you to deploy a solution that is built around this framework and you have a solution who cost and performance are predictable.

PERFORMANCE- This 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 need more resources, autoscaling can deploy addtional resources to meet the demand, and also can scale back when the demand drops. If the traffic is heavily focues on one area, load balancing will help you redirect some of the overload to less stressed areas.

COST- Cost predictability is focused on predicting or forecasting the cost of the cloud spend. You can track your resources use in real time, monitor resources to ensure that you're using them in the most efficient way. Tools like Total Cost of Ownership(TCO) or Pricing Calculater to get an estimate of potential cloud spend.

Benefits of security and governance

Cloud features support governance and compliance. Things like set templates help ensure that all your deployed resources meet corporate standards and government regulatory requirements. You can update all your resources to new standards as standards change. Cloud-based auditing helps flags any resource that's out of compliance with your corporate standards and provides mitigation strategies. Depending on your operating model, software patches and updates may also automatically be applied, which helps with both governance and security.

With security, you could maximize control , Infrastructure as a service provides you with physical resources but lets you manage the operating systems and installed software, including patches and maintenance. Platform as a service or software as a service deployments may be the best cloud strategies for you.

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

Benefits of manageability in the cloud

MANAGEMENT “OF” THE CLOUD

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

- Automatically scale resource to 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 web portal
- Using a command line interface
- Using Powershell
- Using APIs

Cloud service types

Each cloud service type determines the flexibility you'll have with managing and configuring resources. You will also know the shared responsibilty model that applies to each cloud service type and various use cases for each cloud service type.

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.

The responsibilites of the cloud provider for IaaS:

- Maintain the hardware
- Network Connectivity(to the internet)
- Physical security.

The responsibilities of the client(Customer) for IaaS:

EVERYTHING Else:

- Operating system installation
- Configuration
- maintenance
- Network configuration
- database
- storage configuration, etc

Note: IaaS places the largest share of responsibilty with the customer!

Examples:

- Lift and Shift migration: Standing up cloud resources similar to your on-prem datacenter, and then simply movign the things runnong on-prem to running on the IaaS infrastructure.
- Testing and Development: You have made configurations for development and test environments that you need rapidly replicate. You can stand up or shut down the different environments rapidly with an IaaS structure, while maintaining complete control.

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)

Cloud provider responsibilities for PaaS:

- maintains the physical infrastructure
- physical security
- connection to the internet
- operating systems
- middleware
- development tools
- business intelligence services which make up the cloud solution

Note: In Platform as a Service , you do not have to worry about the licensing or patching for operating systems and databases. PaaS provides a complete development environment without the headache of maintaining all the development infrastructure.

Customer is responsible for PaaS:

- Information Data
- Devices
- Accounts and identies

Note: Depending on the set up, Customer can be responsible for:
- Identity and directory infrastructure
- Applications
- Network controls

Examples of PaaS:

- Development framework: Provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to Excel macro, PaaS lets developers create applications using built-in software components. Cloud features like scalability, high-availability, and multi-teneant capabilty are included, reducing the amount of coding that developers must do.
- Analytics or business intelligence: Tools provided as a service with PaaS allow organiations to anaylze and mine their data, finding insights a

Software as a Service

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

However, It is the LEAST flexible, but its also the easiest to get up and running. Requires the least amount of tecnical knowledge or expertise to fully employ

This service places the MOST responsibility on the cloud provider and the least on the customer. SaaS environment customer is just responsible for :

- Data that you input into system
- devices that you allow to connect to the system
- Users that you have acess

Everything else falls on the cloud provider:

- Physical Security of datacenters
- power
- network connectivity
- application development and patching

Examples:

- Email and Messaging
- Business productivity applications
- Finance and expense tracking

Architectural components of Azure

Throughout Azure, This module focuses on the core architectural components of Azure. The core architectural components of Azure may be broken down into two main groupings: The physical infrastructure and the management infrastructure.

Physical Infrastructure

Starts with datacenters. They are the same as large corporate datacenters. They have resources arranged in racks, with dedicated power, cooling, and networking infrastructure.
Azure has datacenters around the world. They are not directly accessible. These 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.

https://infrastructuremap.microsoft.com/ This gives you a chance to interactively explore the underlying Azure infrastructure

Regions

A region is 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 brilliantly assigns and controls the resources within each region to ensure workloads are appropriately balanced.

When you deploy a resource in Azure, you will need to choose the region where your resource is deployed.

Note: Some services or virtual machine features are only available in certain regions, such as specific VM sizes or storage types. There are also some global Azure services that don't require you to select a particular region, such as Microsoft Entra ID, Azure Traffic Manager, and Azure DNS.

Availability Zones

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

Note: To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions. Not all Regions currently support availability zones.

USE AVAILABILITY ZONES IN YOUR APPS

Azure can help your app be highly available through availability zones, that way you ensure your services and data are redundant so you can protect your information in case of failure.

Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases. These zones fall into three categories:

- Zone services : You can pin the resource to a specific zone

- Zone-redundant services: The platform replicates automatically across zones

- Non-regional services: Services are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.

But if this wasn't enough, if there was an event the could be so large that it impacts multiple availability zones in a single region. Azure has Reigion pairs!

Region Pairs

Azure regions are paired with another region within the same geography like US, Europe, or Asia , it is at least 300 miles away. This will allow for the replication of resoures across 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.

Note: Not all azure services automatically replicate data or automatically fall back from a failed region. Recovery and replication must be configured by the customer.

Examples of region pairs:

- West US paired with East US and South-East Asia paired with East Asia. They are directly connected and far enough apart more than 300 miles apart and would be isolated from regional disasters, this is a recipe for reliable services and data redundancy.

MORE ADVANTAGES OF REGION PAIRS:

- If an outage occurs, one region out of every pair is prioritzed to make sure at least one is restored as quickly as possible for applications hosted in that region pair.

- Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.

- Data continues to reside with the same geography as its pair for tax and law-enforcement jurisdiction purposes.

Most regions are paired in two directions, meaning they are backup for the region that provides a backup for them like West US and East US. Some regions only has one-direction pairing, meaning, its primary region does not provide backup for its secondary regions.

SOVEREIGN REGIONS

Along with regular regions, Azure has sovereign regions. These 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.

Examples of Sovereign regions:
- 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.

Note: Obviously for Security purposes.

Azure Managment infrastructure

Management infrastructure includes Azure resources and resource groups, subscriptions and accounts. Understanding the hierarchical organization will help you plan your projects and products within Azure.

Azure resources and resource groups

A resource is the basic building block of Azure. Anything you create , provision, deploy ,etc is a resource. Virtual Machines, Virtual network, and databases, cognitive services, etc are all considered resources within Azure.

Resource groups are simply groupings of resources. when you create resource, you're required to place it into a resource group. A resource group can contain many resources, or a single resource can only be in one resource group at a time. Some resources may be moved between resource groups but when you move a resource to a new group, it will no longer be associated with the former group. Resource groups cannot be nested, which means you can't put resource group B inside of resource group A.

If you apply an action to a resource group, that means that action will apply to all resources in that resource group. if you delete a resource group, all resources in that group, will be deleted. if you grant or deny access to a resource group, that means all the resources in that group will be granted or denied as well.

Try to provision resources in a resource group structure that best suits your needs.

For instance, when you set up a dev environment, grouping all resources together means you can deprovision all of the associated resources at once by deleting the resource group. if you are provisioning compute resources that will need three different access schemas, it is best to group resources based on the access schema and then assign access at the resource group level.

These aren't neccessarily hard rules about how you use resource groups but its recommeneded to consider how to set up your resource groups to maximize their usefulness for you.

Azure subscriptions

subscriptions are a unit of management, billing and scale. Subscriptions allow you to logically organize your resource and facilitate billing.

Using Azure requires an Subscription. It will provide you with authenticated and authorized access to Azure products and services. A subscription links to an Azure account, which is an identity in Microsoft Entra ID or in a directory that Microsoft Entra ID trusts.

An Account can have multiple subscriptions, but its only required to have one. Of course, with Multiple subscriptions, you can have different types of billing requirements. Azure separate billing reports and invoices for each subscription so that you can organize and manage costs.

Azure applies access-managment policies at the subscription level and you can create separate subscriptions to reflect different organizational structures. An example is within a business, you have different departments to which you apply distinct Azure subscription policies. This billing model allows you to manage and control access to the resources that users provision with specific subscriptions.

CREATE ADDITIONAL AZURE SUBSCRIPTIONS

Similiar to using resources groups to separate resources by function or access, You can create additional subscriptions for resource or billing management purposes. You would want to create additional subscriptions to seperate:

- Environments : Create separate environments for development and testing, security or or to isolate data for compliance reasons.

- Organizational structures: Create subscriptions to reflect different organizational structures. You could limit oen team to lower-cost resources, while the IT department a full range.

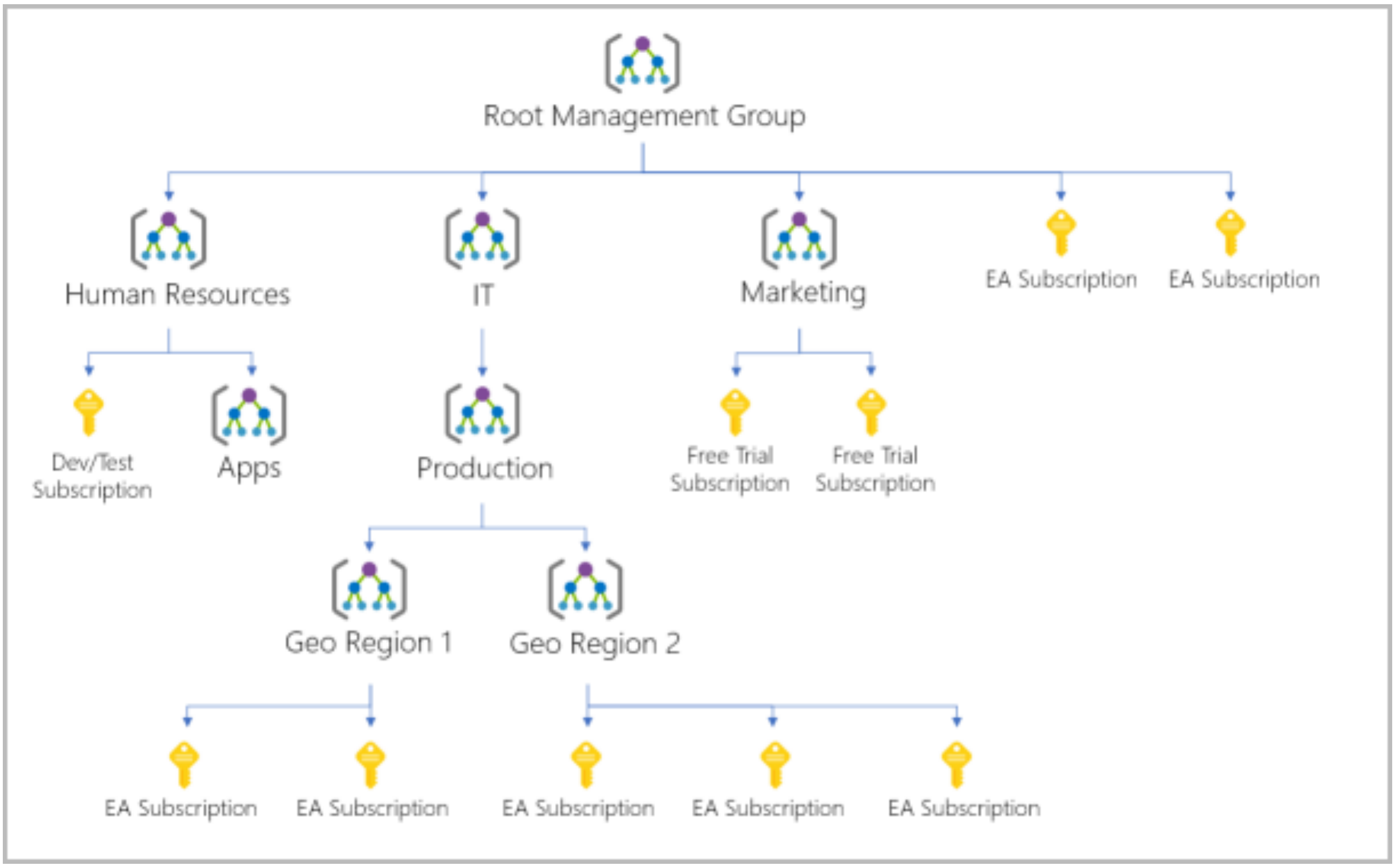
- Billing: You can create subscriptions to manage and track costs based on your needs. You can create one subscription for your productions workloads and another subscription for your development and testing workloads.

AZURE MANAGEMENT GROUPS

Resources are gathered into resource groups, and resource groups are gathered into subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group, the same way that resource groups inherit settings from subscriptions and resources inherit from resource groups. Management groups give you enterprise-grade management at a large scale, no matter what type of subscriptions you might have. Management groups can be nested.

MANAGEMENT GROUP, SUBSCRIPTIONS, AND RESOURCE GROUP HIERARCHY

You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management.



- **Create a hierarchy that applies a policy.** You could limit VM locations to the US West Region in a group called Production. This policy will inherit onto all the subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions. Cool thing, this security policy can't be altered by the resource or subscription owner, which allows for improved governance.

- **Provide user access to multiple subscriptions**. By moving multiple subscriptions under a management group, you can create one Azure role-based access control(Azure RBAC) assignment on the management group. Assigning Azure RBAC at the management group level means that all sub-management groups , subscriptions, resource groups, and resources underneath that management group would also inherit those permissions. One assignment on the management group can enable users to have access to everything they need instead of scripting Azure RBAC over different subscriptions.

Important Facts about management groups:

- 10,000 management groups can be supported in a single directory.

- A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.

- Each management group and subscription can support only one parent.

Azure Compute and networking services

Virtual Machines

Virtual machines are a form of virtualized servers. VMs provide infrastructure as a service(IaaS)

- You have total control over the operating system(OS)
- The ability to run custom software
- To use custom hosting configurations

Azure VMs gives you the flexibilty of virtualization without having to buy and maintain the physical hardware that runs the VM. Remember its basically IaaS, meaning you have to configure , update and maintain the software that runs on the VM

You could create or use an already created image to rapidly provisions VMs.

SCALE VMs IN AZURE

You can run single VMs for testing, development, or minor tasks, you can Group VMs together to provide high availability, scalabilty and redundancy. Azure can also manage the grouping of VMs for you with features such as scale sets and availability sets.

VIRTUAL MACHINE AVAILABILITY SETS

Virtual machines availabilty sets are another tool to help you build a more resilient, highly available environment. They are designed to ensure that VMs stagger updates and have varied power and network connectivity, preventing you from losing all your VMs with a single network or power failure

Availability sets do this by grouping VMs in two ways. Update domain and fault domain

Update domain: groups Vms that can be rebooted at the same time. This allows you to apply updates while knowing that only one update domain grouping will be offline at a time. All of the machines in one domain will be updated. Whichever update group going through the update process is given 30-minute time to recover before maintenance on on the next update domain starts.

Fault domain: groups your Vms by common power source and network switch. By default, an availability set will split your VMs across up to three fault domains. This will help protect against a physical power or networking failure by having VMs in different fault domains.

There is no additional cost for configuring an availabilty set. You only pay for the VM instances you create.

Azure Virtual Desktop

Azure Virutal desktop is another type of Virtual Machine. GUI to be honest.

ENHANCED SECURITY

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 ona personal device is reduced and also, user sessions are isolated in both single and multi-sessions enivironments.

MULTI-SESSION WINDOWS 10 OR WINDOWS 11 DEPLOYMENT

Azure virtual desktop lets you use Windows 10 or Windows 11 Enterprise multi-session and is the only Windows client-based operating system that enables multiple concuurrent users on a single VM.

Azure Containers

If you want to run multiple instances of an application on a single host machine, containers are an excellent choice.

WHAT ARE CONTAINERS

Containers are virtualization environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. You do not manage the operating system for a container. Containers are lightweight and designed to be created ,scaled out, and stoppped dynamically. You can deploy virtual machines as application demand increases but containers liek mention before are more light weight, more agile method.

AZURE CONTAINER INSTANCES

These instances aer a platform as a service (PaaS) offering. Azure Container instances allow you to upload your containers and then service will run the containers for you.

AZURE CONTAINER APPS

Container Apps allow you to get up and running right away, they remove the container management piece and they're a PaaS offering. They also 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 is a container orchestration service. An orchestration manages the lifecycle of the containers. When you're deploying a fleet of containers, AKS can make fleet management simpler and more efficient.

USER CONTAINERS IN YOUR SOLUTIONS

Containers are often used to create solutions by using a microservice architecture is where you break solutions into smaller, independent pieces. You might split a website into a container hosting your front end and storage aren't being stressed. With containers, you could scale the back end separately to improve performance. If something necessitated such a change, you could also choose to change the storage service or modify the front end without impacting any of the other components.

Azure Functions

Azure functions is an event-driven, serverless compute option that doesn't require maintaining virtual machines or containers. If you build an app using VMs or containers, those resources have to be “running” in order for your app to function. With Azure functions, an even wakes the function, alleviating the need to keep resources provisioned when there are no events

BENEFITS OF AZURE FUNCTIONS

Using AF is ideal when you're only concerned about the code running your service and not about the underlying platform or infrastructure. Functions are commonly used when need to perform work in response to an event(often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

Azure Functions can be used to automatically resize images uploaded to a cloud storage container, ensuring they meet specific size requirements for your application, and trigger a notification to your team when a critical error occurs in your system, providing real-time alerts for immediate action.

Application hosting options

You might want to use VM or containers to host your solutions. However Azure App Service is another option for hosting

AZURE APP SERVICE

APS 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. App service supports Windows and Linux. It enables automated deployments from Github, Azure DevOps, or any Git repo to support a continuous deployment model.

It is robust hosting option that you can use to host your apps in Azure. It lets you focus on building and maintaining your app, and Azure focuses on keeping the environment up and running. Azure App Service is an HTTP-based service for hosting web applications, REST APIs and mobile backends. it supports multiple languages, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also support both Windows and Linux environments.

TYPES OF APP SERVICES

APP service can host :

- Web apps
- API apps
- WebJobs
- Mobile apps

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.

These app styles are hosted in the same infrastructure and share these benefits. This flexibilty makes App Service the ideal choice to host web-oriented applications

WEB APPS

App service includes full support for hosting web apps by using ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python. You can choose either windows or Linux as host operating system.

API APPS

Much like hosting a website, you can build REST-based web APIs by using your choice of language and framework. You get full Swagger support and the ability to package and publish your API in Azure Marketplace. The produced apps can be consumed from any HTTP- or HTTPS-based client.

WEBJOBS

Webjobs feature to run a program. They can be scheduled or run by a trigger. WebJobs are often used to run background tasks as part of your application logic

MOBILE APPS

Use the Mobile Apps feature of App Service to quickly build a back end for iOS and Android apps. With just a few actions in the Azure porta

- Store mobile app data in a cloud-based SQL database.
- Authenticate customers against common social providers, such as MSA, Google, Twitter, and Facebook.
- Send push notifications.
- Execute custom back-end logic in C# or Node.js.

Virtual Networking

Azure virtual networks and virtual subnets enable Azure resources, such as VMs, web apps, and databases, to communicate with each other, with users on the internet, and with your on-premises client computers. You can think of an Azure network as an extension of your on-premises network with resources that link other Azure resources.

Azure Virtual networks provide:

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources

- Route network traffic
- Filter network traffic
- Connect virtual networks

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

- Public endpoints have a public IP address and can be accessed from anywhere in the world.
- Private endpoints exist within a virtual network and have a private IP address from within the address space of that virtual network.

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.

COMMUNICATE BETWEEN AZURE RESOURCES

You will want to enable Azure resources to communicate securely with each other. You can do that in one of two ways:

- Virtual networks can connect not only VMs but other Azure resources, such as the App Service Environment for Power Apps, Azure Kubernetes Service, and Azure virtual machine scale sets.
- Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

COMMUNICATE WITH ON-PREMISES RESOURCES

- Point-to-site virtual private network connections are from a computer outside your organization back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect to the Azure virtual network.
- Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.
- Azure ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet. ExpressRoute is useful for environments where you need greater bandwidth and even higher levels of security.

ROUTE NETWORK TRAFFIC

Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows:

- Route tables allow you to define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
- Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or Azure ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

FILTER NETWORK TRAFFIC

Azure virtual networks enable you to filter traffic between subnets by using the following approaches:

- Network security groups are Azure resources that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
- Network virtual appliances are specialized VMs that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

CONNECT VIRTUAL NETWORKS

You can link virtual networks together by using virtual network peering. Peering allows two virtual networks to connect directly to each other. Network traffic between peered networks is private, and travels on the Microsoft backbone network, never entering the public internet. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.

User-defined routes (UDR) allow you to control the routing tables between subnets within a virtual network or between virtual networks. This allows for greater control over network traffic flow.

Azure ExpressRoute

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider. You can establish connections to Microsoft cloud services like Microsoft Azure and Microsoft 365. This allows you to connect offices, datacenters, or other facilities to the Microsoft Cloud. EACH location would have its own ExpressRoute circuit.

Connectivity can be from an any-toany (IP-VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. Express route connections do not go over the public internet.

This allows ExpressRoute connections to OFFER reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet.

FEATURES AND BENEFITS OF EXPRESSROUTE

- 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.

CONNECTIVITY TO MICROSOFT CLOUD SERVICES

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

GLOBAL CONNECTIVITY

You can also enable EXPRESSROUTE GLOBAL REACH to exchange data across your ON-PREMISES networks and resources running in Azure.(cloud)

BUILT-IN REDUNDANCY

Each connectivity provider uses redundant devices to ensure that connections with Microsoft are highly available. You can configure multiple circuits to complement this feature

EXPRESSROUTE CONNECTIVITY MODELS

- CloudExchange colocation refers to your datacenter, office, or other facility being physically co-located at a cloud exchange, such as an ISP. If your facility is co-located at a cloud exchange, you can request a virtual cross-connect to the Microsoft cloud.

POINT-TO-POINT ETHERNET CONNECTION

Point-to-point ethernet connection refers to using a point-to-point connection to connect your facility to the Microsoft cloud

ANY-TO-ANY NETWORKS

you can integrate your wide area network(WAN) with azure by providing connections to yoru offices and datacenters. Azure integrates with your WAN connection to provide a connection to provide a connection like you would have between your datacenter and any branch offices.

DIRECTLY FROM EXPRESSROUTE SITES

You can connect directly into the Microsoft's global network at a peering location strategically distributed across the world. ExpressRoute Direct provides dual 100 Gbps or 10-Gbps connectivity, which supports Active/Active connectivity at scale.

SECURITY CONSIDERATIONS

With ExpressRoute, your data doesn't travel over the public internet, so its not EXPOSED to the potential risks associated with internet communications. ExpressRoute is a private connection from your on-premises infrastructure to your Azure infrastructure. Even if you have an ExpressRoute connection, DNS queries, certificate revocation list checking, and Azure Content Delivery Network request are still sent over the public internet.

Azure DNS

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

BENEFITS OF AZURE DNS

- Reliability and performance

- Security
- Ease to Use
- Customizable virtual networks
- Alias records

RELIABILITY AND PERFORMANCE

DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers, providing resiliency and high availability. Azure DNS uses anycast networking, so each DNS query is answered by the closest available DNS server to provide fast performance and high availabiity for your domain

SECURITY

Azure DNS is based on Azure Resource Manager

- 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.

NOTE:

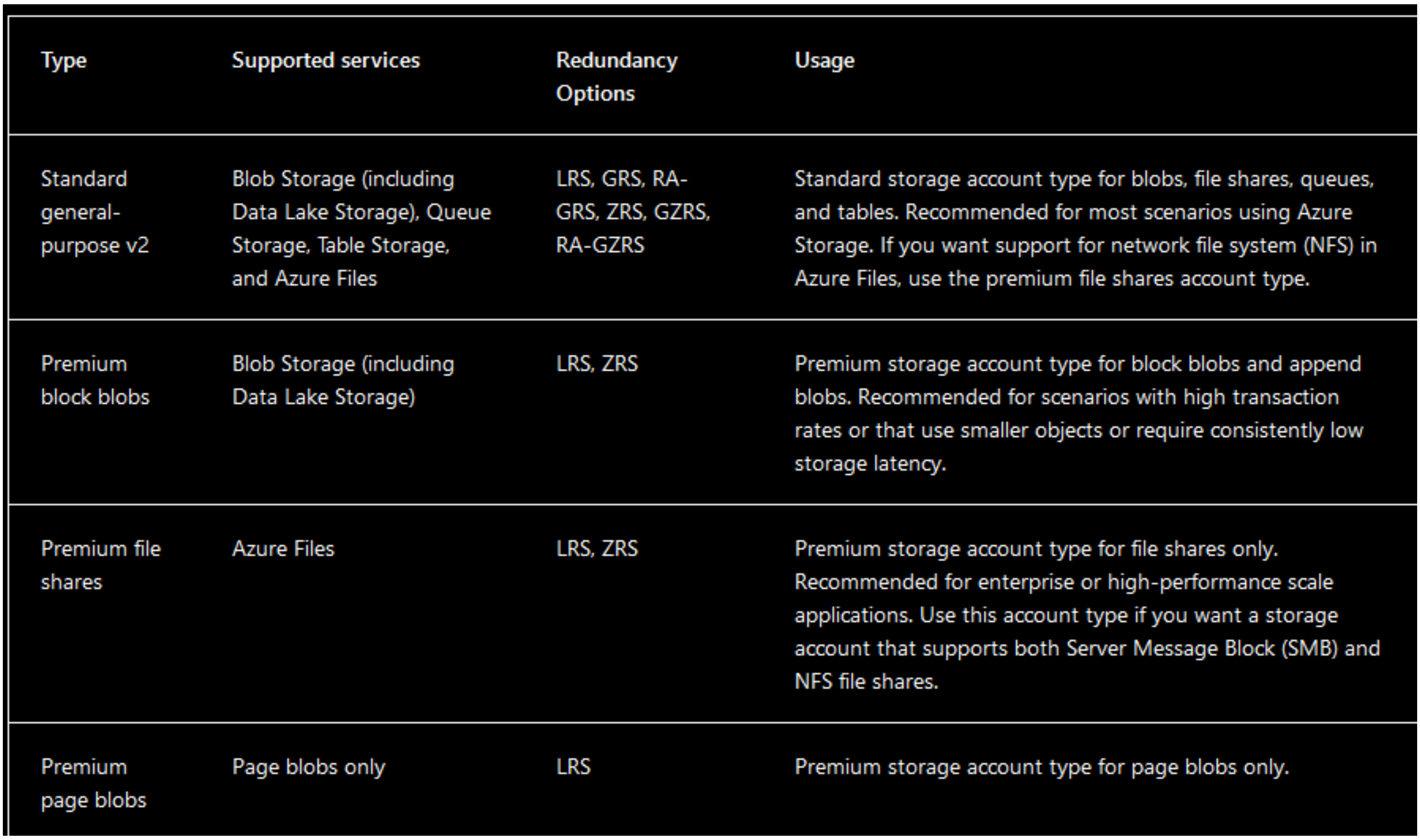
- Azure role-based access control (Azure RBAC) to control who has access to specific actions for your organization.
- Activity logs to monitor how a user in your organization modified a resource or to find an error when troubleshooting.
- Resource locking to lock a subscription, resource group, or resource.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

Azure storage services

Azure storage accounts

List of redundancy options

- 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)

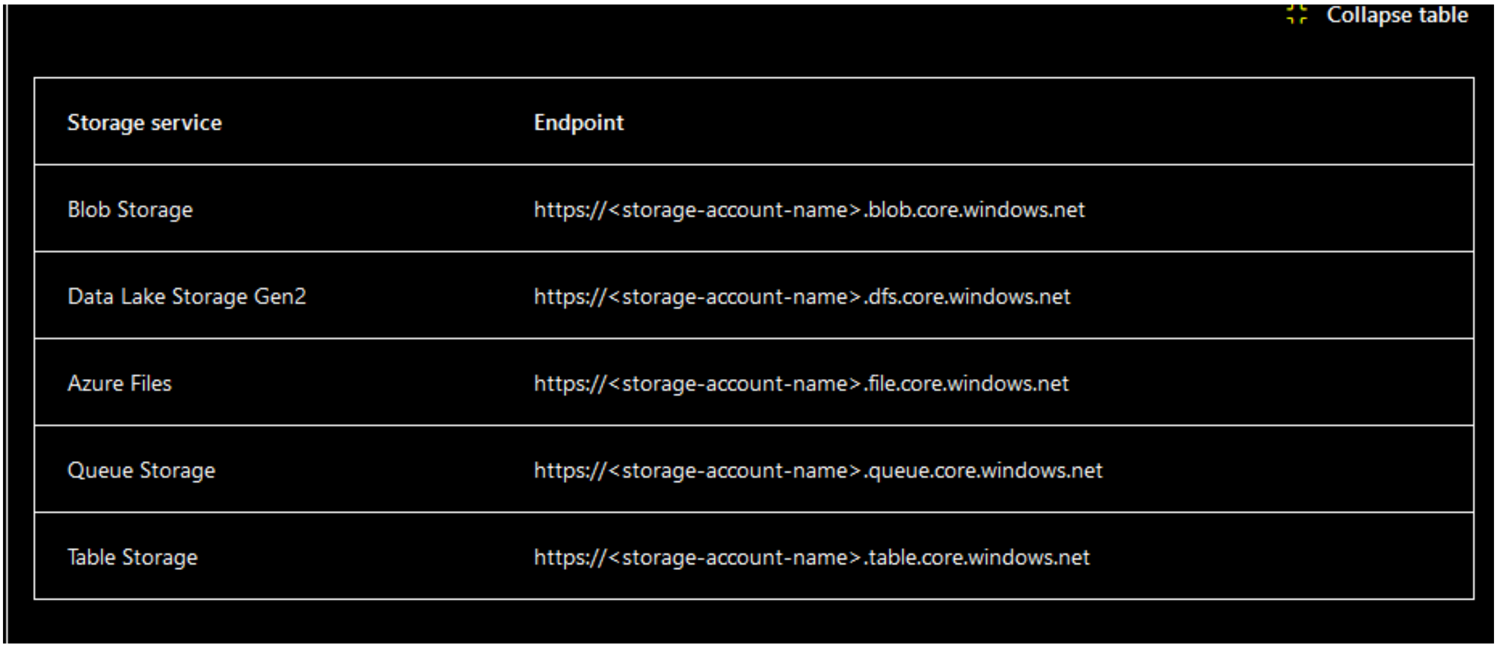


Type	Supported services	Redundancy Options	Usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios 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

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. The combination of the account name and the Azure Storage service endpoint forms the endpoints for your storage account.

- Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only.
- Your storage account name must be unique within Azure. No two storage accounts can have the same name. This supports the ability to have a unique, accessible namespace 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

I understand this section, by using chatgpt and asking questions, I have a good idea. If not, I'll come back and fill this section out.

Azure storage services

AZURE BLOBS

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. Blob storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.

Think ESPN, NBA.COM or any sports organization. With the amount of photos, stats, videos. Perfect for Blob storage, probably premium tier for sure.

ACCESSING BLOB STORAGE

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. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

Blob storage tiers

- **Hot access tier**: Optimized for storing data that is accessed frequently (for example, images for your website).
- **Cool access tier**: Optimized for data that is infrequently accessed and stored for at least 30 days (for example,

invoices for your customers).
- **Cold access tier**: Optimized for storing data that is infrequently accessed and stored for at least 90 days.
- **Archive access tier**: Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

considerations:

- Hot and cool access tiers can be set at the account level. The cold and archive access tiers aren't available at the account level.
- Hot, cool, cold, and archive tiers can be set at the blob level, during or after upload.
- Data in the cool and cold access tiers can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool and cold data, a lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.
- Archive storage stores data offline and offers the lowest storage costs, but also the highest costs to rehydrate and access data.

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.

BENEFITS

- **Shared access**: Azure file shares support the industry standard SMB and NFS protocols, meaning you can seamlessly replace your on-premises file shares with Azure file shares without worrying about application compatibility.
- **Fully managed**: Azure file shares can be created without the need to manage hardware or an OS. This means you don't have to deal with patching the server OS with critical security upgrades or replacing faulty hard disks.
- **Scripting and tooling**: PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure file shares as part of the administration of Azure applications. You can create and manage Azure file shares using Azure portal and Azure Storage Explorer.
- **Resiliency**: Azure Files has been built from the ground up to always be available. Replacing on-premises file shares with Azure Files means you don't have to wake up in the middle of the night to deal with local power outages or network issues.
- **Familiar programmability**: Applications running in Azure can access data in the share via file system I/O APIs. Developers can therefore use their existing code and skills to migrate existing applications. In addition to System IO APIs, you can use Azure Storage Client Libraries or the Azure Storage REST API.

AZURE QUEUES (Think AMAZON)

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. A queue can contain as many messages as your storage account has room for (potentially millions). Each individual message can be up to 64 KB in size. Queues are commonly used to create a backlog of work to process asynchronously.
Queue storage can be combined with compute functions like Azure Functions to take an action when a message is received. For example, you want to perform an action after a customer uploads a form to your website. You could have the submit button on the website trigger a message to the Queue storage. Then, you could use Azure Functions to trigger an action once the message was received.

AMAZON real example

A real company that utilizes queues in a similar manner is Amazon. Amazon, one of the world's largest e-commerce companies, relies heavily on queue-based systems to manage order processing, inventory management, and fulfillment operations.
When a customer places an order on Amazon's website or mobile app, the order details are added to a queue in real-time. Amazon employs a distributed architecture with multiple processing nodes and microservices that monitor the order queue and handle order processing tasks asynchronously. This allows Amazon to scale its operations dynamically to handle fluctuations in demand and ensure timely order fulfillment, even during peak shopping seasons.

AZURE DISKS (Autodesk)

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. With managed disks, all you have to do is provision the disk, and Azure will take care of the rest.

Autodesk real example

Autodesk, a global leader in 3D design, engineering, and entertainment software, utilizes Azure Disks to power its virtual machines for various purposes, including development, testing, and production workloads.

Autodesk's software suite, which includes industry-standard tools like AutoCAD, Revit, and Maya, requires robust and scalable infrastructure to support its diverse customer base and complex workloads. By leveraging Azure Disks for VM storage, Autodesk benefits from features such as high-performance SSD storage, scalability, and reliability, allowing them to deploy and manage their software applications efficiently in the cloud.

Azure Tables (Advertisement companies)

Azure Table storage stores large amounts of structured data. Azure tables are a NoSQL datastore that accepts authenticated calls from inside and outside the Azure cloud. This enables you to use Azure tables to build your hybrid or multi-cloud solution and have your data always available. Azure tables are ideal for storing structured, non-relational data.

Real example

, advertising companies can scale their operations, optimize campaign performance, and drive customer engagement more effectively in today's digital advertising landscape. These solutions provide the flexibility, scalability, and performance required to handle the complex data management and processing needs of modern advertising campaigns across various digital channels and platforms.

Azure data migration options

AZURE MIGRATE

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

You can use a single portal to start, run, and track your migration to Azure

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 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. The Data Box is transported to and from your datacenter via a regional carrier. A rugged case protects and secures the Data Box from damage during transit.

Data Box is ideally suited to transfer data sizes larger than 40 TBs in scenarios with no to limited network connectivity.

Scenarios:

- Onetime migration - when a large amount of on-premises data is moved to Azure.
- Moving a media library from offline tapes into Azure to create an online media library.
- Migrating your VM farm, SQL server, and applications to Azure.
- Moving historical data to Azure for in-depth analysis and reporting using HDInsight.
- Initial bulk transfer - when an initial bulk transfer is done using Data Box (seed) followed by incremental transfers over the network.
- Periodic uploads - when large amount of data is generated periodically and needs to be moved to Azure.

If you go away from Azure or like another cloud vendor, Azure can export your data back to your on-premise data center or a whole other vendor:

- Disaster recovery - when a copy of the data from Azure is restored to an on-premises network. In a typical disaster recovery scenario, a large amount of Azure data is exported to a Data Box. Microsoft then ships this Data Box, and the data is restored on your premises in a short time.
- Security requirements - when you need to be able to export data out of Azure due to government or security requirements.
- Migrate back to on-premises or to another cloud service provider - when you want to move all the data back to on-premises, or to another cloud service provider, export data via Data Box to migrate the workloads.

Once the data from your import order is uploaded to Azure, the disks on the device are wiped clean in accordance with NIST 800-88r1 standards. For an export order, the disks are erased once the device reaches the Azure datacenter.

Azure file movement options

Azure also has tools designed to help you move or interact with individual files or small file groups. Among those tools are AzCopy, Azure Storage Explorer, and Azure File Sync.

AzCopy

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. AzCopy can even be configured to work with other cloud providers to help move files back and forth between clouds.

NOTE:

Synchronizing blobs or files with AzCopy is one-direction synchronization. When you synchronize, you designated the source and destination, and AzCopy will copy files or blobs in that direction. It doesn't synchronize bi-directionally based on timestamps or other metadata.

AZURE STORAGE EXPLORER

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. With Storage Explorer, you can upload to Azure, download from Azure, or move between storage accounts.

AZURE FILE SYNC

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. It’s almost like turning your Windows file server into a miniature content delivery network. Once you install Azure File Sync on your local Windows server, it will automatically stay bi-directionally synced with your files in Azure.

Some things you can do with AFS:

- Use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS.
- Have as many caches as you need across the world.
- Replace a failed local server by installing Azure File Sync on a new server in the same datacenter.
- Configure cloud tiering so the most frequently accessed files are replicated locally, while infrequently accessed files are kept in the cloud until requested.

Azure identity, access and security

You have to know about directory services in Azure, authentication methods and access control. On top of that, you need to know about Zero Trust and defense in depth and how they keep your cloud safer. Also need to know about the Microsoft Defender “for” the cloud.

Azure directory services

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.
For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization. Microsoft Entra ID is Microsoft's cloud-based identity and access management service. With Microsoft Entra ID, you control the identity accounts, but Microsoft ensures that the service is available globally

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Microsoft Entra ID, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Microsoft Entra ID can detect sign-in attempts from unexpected locations or unknown devices.

Who uses Microsoft Entra ID?

- **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.

What does Microsoft Entra ID do?

- **Authentication**: This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- **Application management**: You can manage your cloud and on-premises apps by using Microsoft Entra ID. Features like Application Proxy, SaaS apps, the My Apps portal, and single sign-on provide a better user experience.

• **Device management**: Along with accounts for individual people, Microsoft Entra ID supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Can I connect my on-premises AD with Microsoft Entra ID?

MICROSOFT ENTRA CONNECT

Microsoft Entra Connect synchronizes user identities between on-premises Active Directory and Microsoft Entra ID. Microsoft Entra Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems.

What is Microsoft Entra Domain Services?

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. Just like Microsoft Entra ID lets you use directory services without having to maintain the infrastructure supporting it, with Microsoft Entra Domain Services, you get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

It also allows you to run legacy applications in the cloud that cannot use modern authentication methods or where oyu don't want directory lookups to always go back to an on-premises AD DS environment.

How does Microsoft Entra Domain Services work?

When you create a Microsoft Entra Domain Services managed domain, you define a unique namespace. This namespace is the domain name. Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set.
You don't need to manage, configure, or update these DCs. The Azure platform handles the DCs as part of the managed domain, including backups and encryption at rest using Azure Disk Encryption.

Applications, services, and VMs in Azure that connect to the managed domain can then use common Microsoft Entra Domain Services features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.

Azure authentication methods

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. Authentication is like presenting ID when you’re traveling. It doesn’t confirm that you’re ticketed, it just proves that you're who you say you are. Azure supports multiple authentication methods, including standard passwords, single sign-on (SSO), multifactor authentication (MFA), and passwordless.

What's single sign-on

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.

Single sign-on is only as secure as the initial authenticator because the subsequent connections are all based on the security of the initial authenticator.

What's multifactor authentication

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.

Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate. These elements fall into three categories:

- Something the user knows – this might be a challenge question.
- Something the user has – this might be a code that's sent to the user's mobile phone.
- Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan.

What's passwordless authentication

Passwordless authentication needs to be set up on a device before it can work. For example, your computer is something you have. Once it’s been registered or enrolled, Azure now knows that it’s associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.
Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Microsoft Entra ID:

- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 security keys

Windows Hello for Business

I USE THIS AT MY NEW JOB

Windows Hello for Business is ideal for information workers that have their own designated Windows PC. The biometric and PIN credentials are directly tied to the user's PC, which prevents access from anyone other than the owner. With public key infrastructure (PKI) integration and built-in support for single sign-on (SSO), Windows Hello for Business provides a convenient method for seamlessly accessing corporate resources on-premises and in the cloud.

FIDO2 security keys

I have this at my NEW JOB

FIDO2 security keys

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.
FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign-in to their resources without a username or password by using an external security key or a platform key built into a device.
Users can register and then select a FIDO2 security key at the sign-in interface as their main means of authentication. These FIDO2 security keys are typically USB devices, but could also use Bluetooth or NFC. With a hardware device that handles the authentication, the security of an account is increased as there's no password that could be exposed or guessed.

Azure external identities

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. If you're a developer creating consumer-facing apps, you can manage your customers' identity experiences.

The following capabilities make up External Identities:

- **Business to business (B2B) collaboration** - Collaborate with external users by letting them use their preferred identity to sign-in to your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.). B2B collaboration users are represented in your directory, typically as guest users.
- **B2B direct connect** - Establish a mutual, two-way trust with another Microsoft Entra organization for seamless collaboration. B2B direct connect currently supports Teams shared channels, enabling external users to access your resources from within their home instances of Teams. B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.
- **Microsoft Azure Active Directory business to customer (B2C)** - Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.

Depending on how you want to interact with external organizations and the types of resources you need to share, you can use a combination of these capabilities.
With Microsoft Entra ID, you can easily enable collaboration across organizational boundaries by using the

Microsoft Entra B2B feature. Guest users from other tenants can be invited by administrators or by other users. This capability also applies to social identities such as Microsoft accounts.
You also can easily ensure that guest users have appropriate access. You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access. The reviewers can give their input on each user's need for continued access, based on suggestions from Microsoft Entra ID. When an access review is finished, you can then make changes and remove access for guests who no longer need it.

Azure conditional access

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 helps IT administrators:

- Empower users to be productive wherever and whenever.
- Protect the organization's assets.

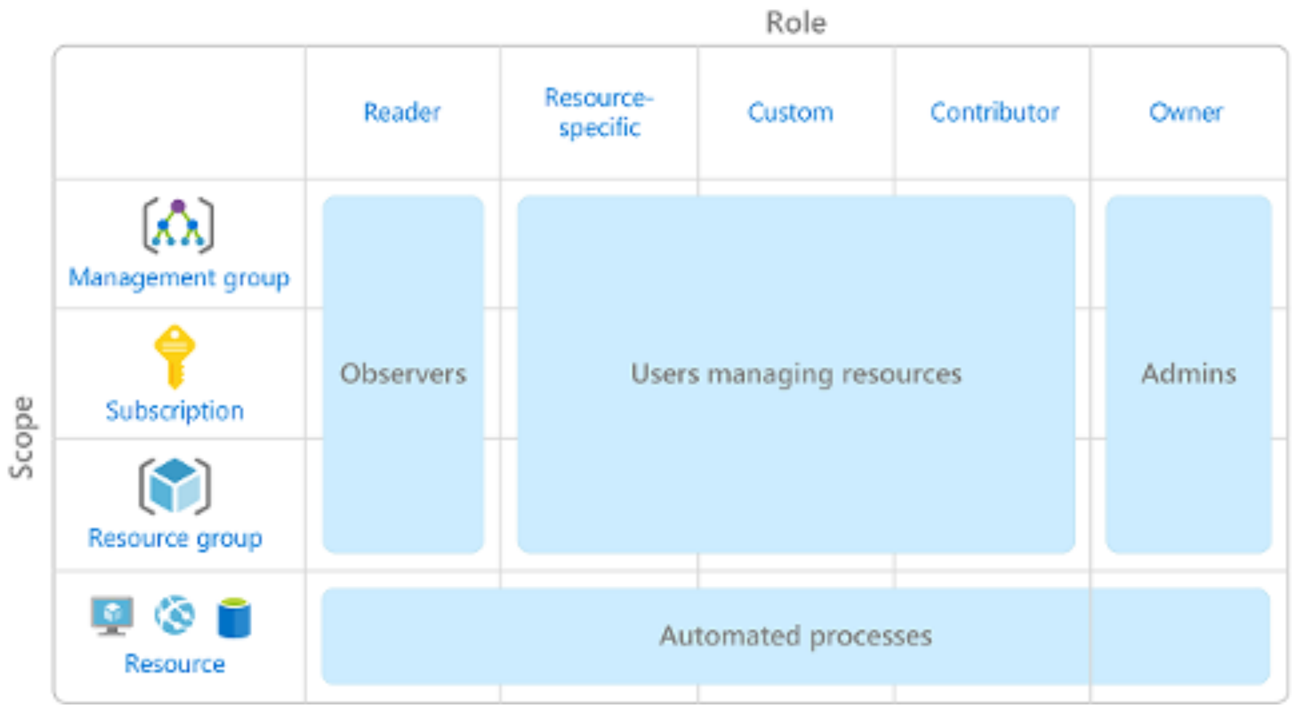
Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.
During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

Azure role-based access control

When you have multiple IT and engineering teams, how can you control what access they have to the resources in your cloud environment? The principle of least privilege says you should only grant access up to the level needed to complete a task. If you only need read access to a storage blob, then you should only be granted read access to that storage blob. Write access to that blob shouldn’t be granted, nor should read access to other storage blobs. It’s a good security practice to follow.
However, managing that level of permissions for an entire team would become tedious. Instead of defining the detailed access requirements for each individual, and then updating access requirements when new resources are created or new people join the team, Azure enables you to control access through Azure role-based access control (Azure RBAC).
Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all the associated access permissions.
So, if you hire a new engineer and add them to the Azure RBAC group for engineers, they automatically get the same access as the other engineers in the same Azure RBAC group. Similarly, if you add additional resources and point Azure RBAC at them, everyone in that Azure RBAC group will now have those permissions on the new resources as well as the existing resources.

How is role-based access control applied to resources?

Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to.



Observers, users managing resources, admins, and automated processes illustrate the kinds of users or accounts that would typically be assigned each of the various roles.
Azure RBAC is hierarchical, in that when you grant access at a parent scope, those permissions are inherited by all child scopes. For example:

- When you assign the Owner role to a user at the management group scope, that user can manage everything in all subscriptions within the management group.
- When you assign the Reader role to a group at the subscription scope, the members of that group can view every resource group and resource within the subscription.

How is Azure RBAC enforced?

Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager. Resource Manager is a management service that provides a way to organize and secure your cloud resources.
You typically access Resource Manager from the Azure portal, Azure Cloud Shell, Azure PowerShell, and the Azure CLI. Azure RBAC doesn't enforce access permissions at the application or data level. Application security must be handled by your application.
Azure RBAC uses an allow model. When you're assigned a role, Azure RBAC allows you to perform actions within the scope of that role. If one role assignment grants you read permissions to a resource group and a different role assignment grants you write permissions to the same resource group, you have both read and write permissions on that resource group.

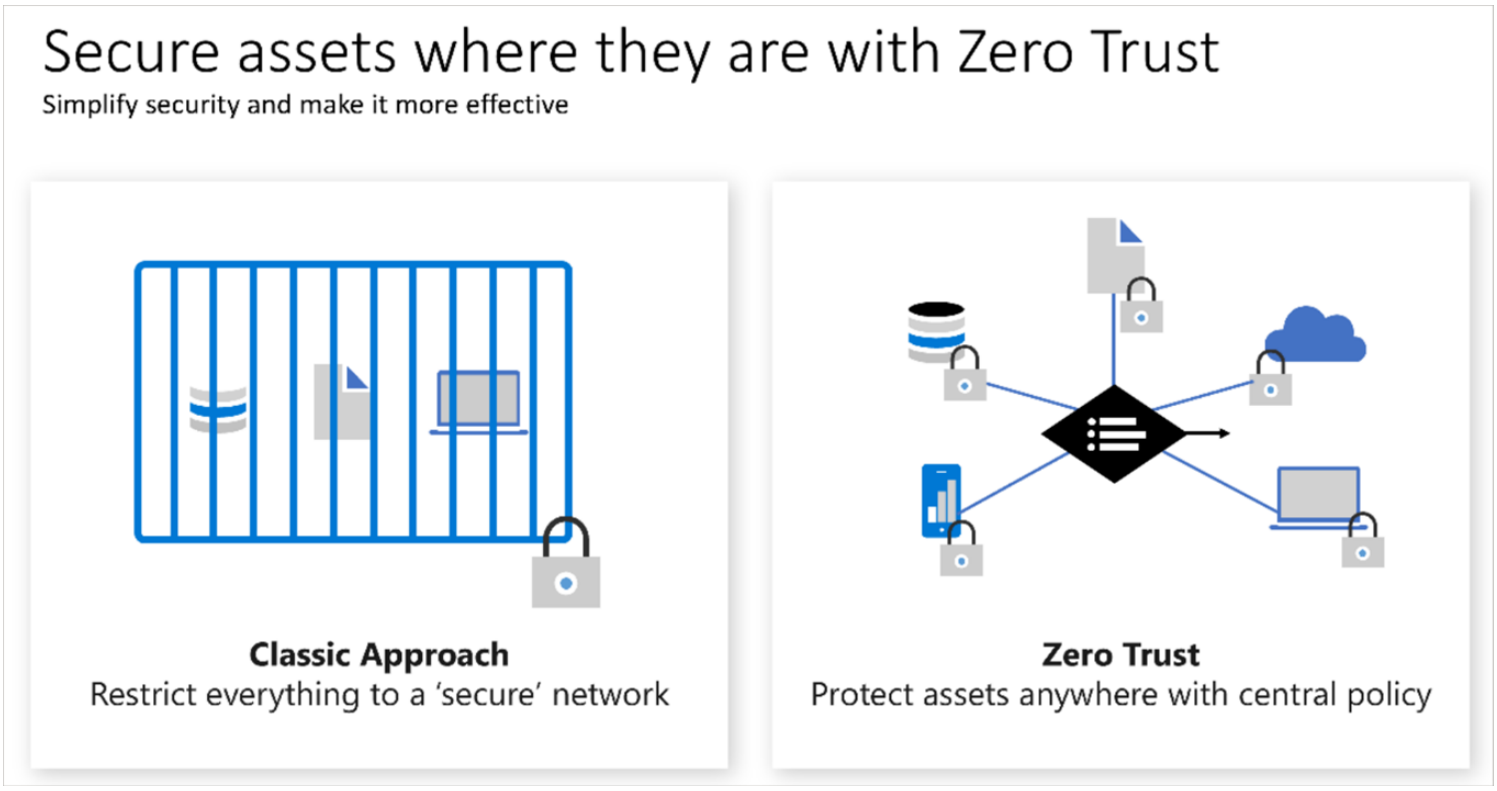
zero trust model

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.
Today, organizations need a new security model that effectively adapts to the complexity of the modern environment; embraces the mobile workforce: and protects people, devices, applications, and data wherever they're located.
To address this new world of computing, Microsoft highly recommends the Zero Trust security model, which is based on these guiding principles:

- **Verify explicitly** - Always authenticate and authorize based on all available data points.
- **Use least privilege access** - Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
- **Assume breach** - Minimize blast radius and segment access. Verify end-to-end encryption. Use analytics to get visibility, drive threat detection, and improve defenses.

Adjusting to Zero Trust

Traditionally, corporate networks were restricted, protected, and generally assumed safe. Only managed computers could join the network, VPN access was tightly controlled, and personal devices were frequently restricted or blocked.
The Zero Trust model flips that scenario. Instead of assuming that a device is safe because it’s within the corporate network, it requires everyone to authenticate. Then grants access based on authentication rather than location.



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

defense-in-depth

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.
A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.

LAYERS OF DEFENSE-IN-DEPTH

- The physical security layer is the first line of defense to protect computing hardware in the datacenter.
- The identity and access layer controls access to infrastructure and change control.
- The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The network layer limits communication between resources through segmentation and access controls.
- The compute layer secures access to virtual machines.
- The application layer helps ensure that applications are secure and free of security vulnerabilities.
- The data layer controls access to business and customer data that you need to protect.

PHYSICAL SECURITY

Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense.

IDENTITY AND ACCESS

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.

PERIMETER

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.

NETWORK

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.

COMPUTE

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

APPLICATION

Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.

DATA

Those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

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.

Many Azure-native services are already monitored and protected without needing any deployment.

However if you have on-premises datacenter or are also operating in another cloud environment, monitoring of Azure services may not give you a complete picture of your security situation.

Defender for Cloud can automatically deploy a **Log Analytics agent** to gather security-related data. For Azure machines, deployment is handled directly. For hybrid and multi-cloud environments, Microsoft Defender plans are extended to non Azure machines with the help of **Azure Arc**. **Cloud security posture management (CSPM)** features are extended to multi-cloud machines without the need for any agents.

AZURE-NATIVE PROTECTIONS

Defender for Cloud helps you detect threats across:

- **Azure PaaS services** – Detect threats targeting Azure services including Azure App Service, Azure SQL, Azure Storage Account, and more data services. You can also perform **anomaly detection** on your Azure activity logs using the native integration with Microsoft Defender for Cloud Apps (formerly known as Microsoft Cloud App Security).
- **Azure data services** – Defender for Cloud includes capabilities that help you automatically classify your data in Azure SQL. You can also get **assessments** for potential vulnerabilities across Azure SQL and Storage services, and recommendations for how to mitigate them.
- **Networks** – Defender for Cloud helps you limit exposure to brute force attacks. By reducing access to virtual machine ports, using the **just-in-time VM access**, you can harden your network by preventing unnecessary access. You can set **secure access policies** on selected ports, for only authorized users, allowed source IP address ranges or IP addresses, and for a limited amount of time.

DEFENDING RESOURCES RUNNING ON OTHER CLOUDS

Defender for Cloud can also protect resources in other clouds (such as **AWS** and **GCP**).
For example, if you've connected an Amazon Web Services (AWS) account to an Azure subscription, you can enable any of these protections:

- Defender for Cloud's **CSPM** features extend to your AWS resources. This **agentless plan assesses your AWS**

resources according to AWS-specific security recommendations, and includes the results in the secure score. The resources will also be assessed for **compliance with built-in standards** specific to AWS (**AWS CIS, AWS PCI DSS, and AWS Foundationa**l Security Best Practices). Defender for Cloud's asset inventory page is a multi-cloud enabled feature helping you manage your AWS resources alongside your Azure resources.
- Microsoft Defender for **Containers** extends its container threat detection and advanced defenses to your Amazon EKS Linux clusters.
- Microsoft Defender for **Servers** brings **threat detection** and **advanced defenses** to your Windows and Linux EC2 instances.

ASSESS, SECURE AND DEFEND

Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

- Continuously assess – Know your security posture. Identify and track vulnerabilities.
- Secure – Harden resources and services with Azure Security Benchmark.
- Defend – Detect and resolve threats to resources, workloads, and services.

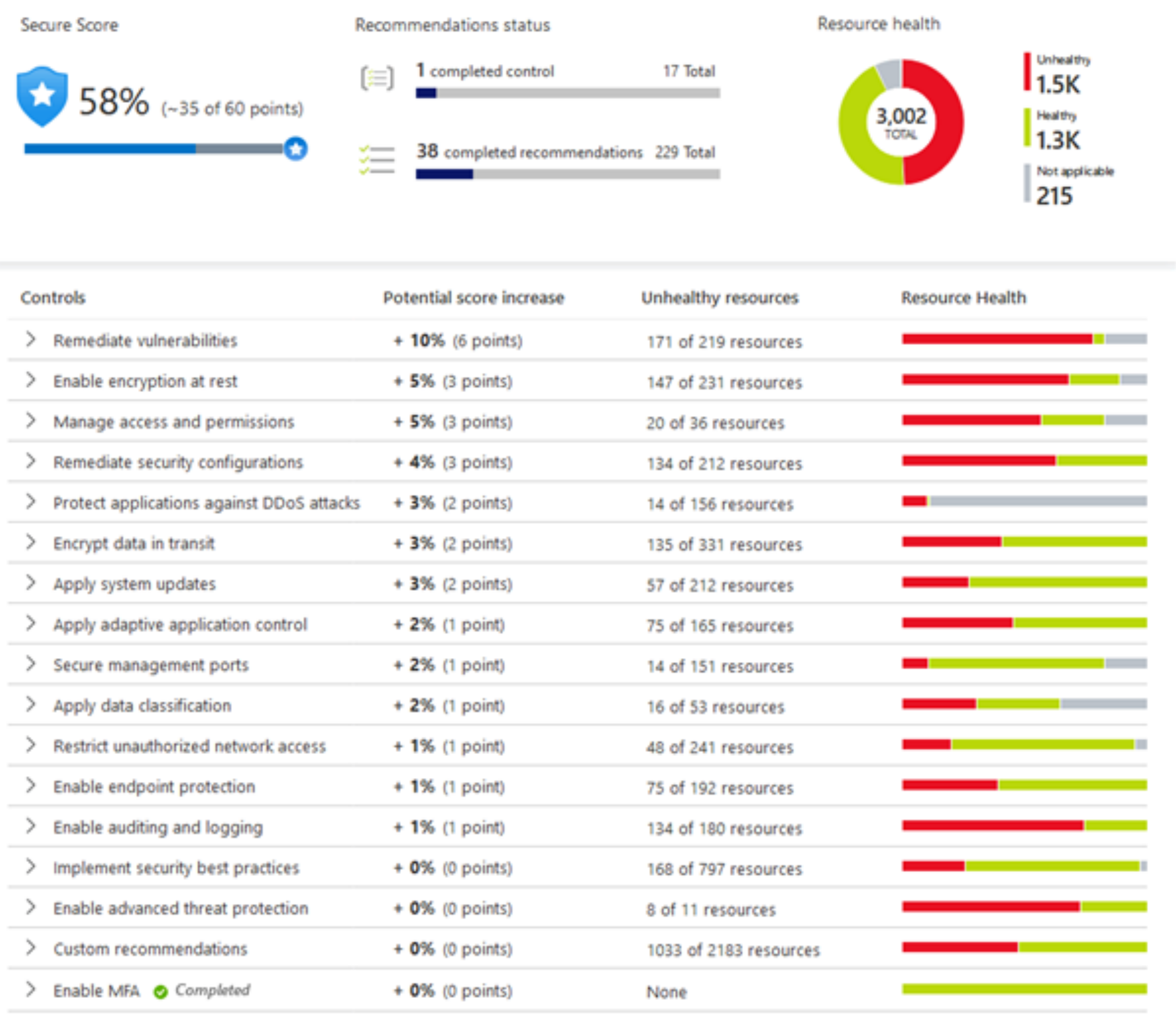
CONTINUOUSLY ASSESS

Defender for cloud helps you continuously assess your environment. Defender for Cloud includes vulnerability assessment solutions for your virtual machines, container registries, and SQL servers.
Microsoft Defender for servers includes automatic, native integration with Microsoft Defender for Endpoint. With this integration enabled, you'll have access to the vulnerability findings from Microsoft threat and vulnerability management.
Between these assessment tools you'll have regular, detailed vulnerability scans that cover your compute, data, and infrastructure. You can review and respond to the results of these scans all from within Defender for Cloud.

SECURE

From authentication methods to access control to the concept of Zero Trust, security in the cloud is an essential basic that must be done right. In order to be secure in the cloud, you have to ensure your workloads are secure. To secure your workloads, you need security policies in place that are tailored to your environment and situation. Because policies in Defender for Cloud are built on top of Azure Policy controls, you're getting the full range and flexibility of a world-class policy solution. In Defender for Cloud, you can set your policies to run on management groups, across subscriptions, and even for a whole tenant.

The list of recommendations is enabled and supported by the Azure Security Benchmark. This Microsoft-authored, Azure-specific, benchmark provides a set of guidelines for security and compliance best practices based on common compliance frameworks.



Secure Score

58% (~35 of 60 points)

Recommendations status

1 completed control 17 Total

38 completed recommendations 229 Total

Resource health

3,002 TOTAL

Unhealthy 1.5K

Healthy 1.3K

Not applicable 215

Controls	Potential score increase	Unhealthy resources	Resource Health
Remediate vulnerabilities	+ 10% (6 points)	171 of 219 resources	
Enable encryption at rest	+ 5% (3 points)	147 of 231 resources	
Manage access and permissions	+ 5% (3 points)	20 of 36 resources	
Remediate security configurations	+ 4% (3 points)	134 of 212 resources	
Protect applications against DDoS attacks	+ 3% (2 points)	14 of 156 resources	
Encrypt data in transit	+ 3% (2 points)	135 of 331 resources	
Apply system updates	+ 3% (2 points)	57 of 212 resources	
Apply adaptive application control	+ 2% (1 point)	75 of 165 resources	
Secure management ports	+ 2% (1 point)	14 of 151 resources	
Apply data classification	+ 2% (1 point)	16 of 53 resources	
Restrict unauthorized network access	+ 1% (1 point)	48 of 241 resources	
Enable endpoint protection	+ 1% (1 point)	75 of 192 resources	
Enable auditing and logging	+ 1% (1 point)	134 of 180 resources	
Implement security best practices	+ 0% (0 points)	168 of 797 resources	
Enable advanced threat protection	+ 0% (0 points)	8 of 11 resources	
Custom recommendations	+ 0% (0 points)	1033 of 2183 resources	
Enable MFA ✓ *Completed*	+ 0% (0 points)	None	

DEFEND

Defender for Cloud also helps you defend your environment by providing security alerts and advanced threat protection features.

SECURITY ALERTS

When Defender for Cloud detects a threat in any area of your environment, it generates a security alert. Security alerts:
- Describe details of the affected resources
- Suggest remediation steps
- Provide, in some cases, an option to trigger a logic app in response

Whether an alert is generated by Defender for Cloud or received by Defender for Cloud from an integrated security product, you can export it. Defender for Cloud's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis, to help you better understand the full story of an attack campaign, where it started, and what kind of impact it had on your resources.

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.

Cost Management in Azure

Know the factors that impact costs in Azure and tools to help you both predict potential costs and monitor and control costs

Factors that can affect costs in Azure

Azure shifts development costs from the capital expense (CapEx) of building out and maintaining infrastructure and facilities to an operational expense (OpEx)

- Resource type
- Consumption
- Maintenance
- Geography
- Subscription type
- Azure Marketplace

RESOURCE TYPE

When you provision an Azure resource, Azure creates metered instances for that resource. The meters track the resources' usage and generate a usage record that is used to calculate your bill.

EXAMPLES

With a storage account, you specify a type such as blob, a performance tier, an access tier, redundancy settings, and a region. Creating the same storage account in different regions may show different costs and changing any of the settings may also impact the price.

With a virtual machine (VM), you may have to consider licensing for the operating system or other software, the processor and number of cores for the VM, the attached storage, and the network interface. Just like with storage, provisioning the same virtual machine in different regions may result in different costs.

CONSUMPTION

Pay-as-you-go has been a consistent theme throughout, and that’s the cloud payment model where you pay for the resources that you use during a billing cycle. If you use more compute this cycle, you pay more. If you use less in the current cycle, you pay less. It’s a straight forward pricing mechanism that allows for maximum flexibility.

, Azure also offers the ability to commit to using a set amount of cloud resources in advance and receiving discounts on those “reserved” resources. Many services, including databases, compute, and storage all provide the option to commit to a level of use and receive a discount, in some cases up to 72 percent.

MAINTENANCE

The flexibility of the cloud makes it possible to rapidly adjust resources based on demand. Using resource groups can help keep all of your resources organized. In order to control costs, it’s important to maintain your cloud environment

GEOGRAPHY

When you provision most resources in Azure, you need to define a region where the resource deploys. Azure infrastructure is distributed globally, which enables you to deploy your services centrally or closest to your customers, or something in between. With this global deployment comes global pricing differences. The cost of power, labor, taxes, and fees vary depending on the location. Due to these variations, Azure resources can differ in costs to deploy depending on the region.

Network traffic is also impacted based on geography. For example, it’s less expensive to move information within Europe than to move information from Europe to Asia or South America.

NETWORK TRAFFIC

Billing zones are a factor in determining the cost of some Azure services.
Bandwidth refers to data moving in and out of Azure datacenters. Some inbound data transfers (data going into Azure datacenters) are free. For outbound data transfers (data leaving Azure datacenters), data transfer pricing is based on zones.

SUBSCRIPTION TYPE

Some Azure subscription types also include usage allowances, which affect costs.
For example, an Azure free trial subscription provides access to a number of Azure products that are free for 12 months. It also includes credit to spend within your first 30 days of sign-up. You'll get access to more than 25 products that are always free (based on resource and region availability).

Azure Marketplace lets you purchase Azure-based solutions and services from third-party vendors. This could be a server with software preinstalled and configured, or managed network firewall appliances, or connectors to third-party backup services.

Pricing and Total Cost of Ownership Calculators

The pricing calculator and the total cost of ownership (TCO) calculator are two calculators that help you understand potential Azure expenses. Both calculators are accessible from the internet, and both calculators allow you to build out a configuration. However, the two calculators have very different purposes.

PRICING CALCULATOR

The pricing calculator and the total cost of ownership (TCO) calculator are two calculators that help you understand potential Azure expenses. Both calculators are accessible from the internet, and both calculators allow you to build out a configuration. However, the two calculators have very different purposes.

you can estimate the cost of any provisioned resources, including compute, storage, and associated network costs. You can even account for different storage options like storage type, access tier, and redundancy.

TCO CALCULATOR

The TCO calculator is designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure. With the TCO calculator, you enter your current infrastructure configuration, including servers, databases, storage, and outbound network traffic. The TCO calculator then compares the anticipated costs for your current environment with an Azure environment supporting the same infrastructure requirements.

Microsoft Management tool

WHAT IS COST MANAGEMENT

Cost Management provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.
Cost analysis is a subset of **Cost Management** that provides a quick visual for your Azure costs. Using cost analysis, you can quickly view the total cost in a variety of different ways, including by billing cycle, region, resource, and so on.

You use cost analysis to explore and analyze your organizational costs. You can view aggregated costs by organization to understand where costs are accrued and to identify spending trends. And you can see accumulated costs over time to estimate monthly, quarterly, or even yearly cost trends against a budget.

COST ALERTS

Cost alerts provide a single location to quickly check on all of the different alert types that may show up in the Cost Management service. The three types of alerts that may show up are:

- Budget alerts
- Credit alerts
- Department spending quota alerts.

BUDGET ALERTS

Budget alerts notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition of the budget. Cost Management budgets are created using the **Azure portal** or the **Azure Consumption API.**

DEPARTMENT SPENDING QUOTA ALERTS

Department spending quota alerts notify you when department spending reaches a fixed threshold of the quota.

Spending quotas are configured in the EA portal. Whenever a threshold is met, it generates an email to department owners, and appears in cost alerts. For example, 50 percent or 75 percent of the quota.

BUDGETS

A budget is where you set a spending limit for Azure. You can set budgets based on a subscription, resource group, service type, or other criteria. When you set a budget, you will also set a budget alert. When the budget hits the budget alert level, it will trigger a budget alert that shows up in the cost alerts area. If configured, budget alerts will also send an email notification that a budget alert threshold has been triggered.

A more advanced use of budgets enables budget conditions to trigger automation that suspends or otherwise modifies resources once the trigger condition has occurred.

Purpose of tags

As your cloud usage grows, it's increasingly important to stay organized. A good organization strategy helps you understand your cloud usage and can help you manage costs.

One way to organize related resources is to place them in their own subscriptions. You can also use resource groups to manage related resources. Resource tags are another way to organize resources. Tags provide extra information, or metadata, about your resources.

- **Resource management** Tags enable you to locate and act on resources that are associated with specific workloads, environments, business units, and owners.
- **Cost management and optimization** Tags enable you to group resources so that you can report on costs, allocate internal cost centers, track budgets, and forecast estimated cost.
- **Operations management** Tags enable you to group resources according to how critical their availability is to your business. This grouping helps you formulate service-level agreements (SLAs). An SLA is an uptime or performance guarantee between you and your users.
- **Security** Tags enable you to classify data by its security level, such as public or confidential.
- **Governance and regulatory compliance** Tags enable you to identify resources that align with governance or regulatory compliance requirements, such as ISO 27001. Tags can also be part of your standards enforcement efforts. For example, you might require that all resources be tagged with an owner or department name.
- **Workload optimization and automation** Tags can help you visualize all of the resources that participate in complex deployments. For example, you might tag a resource with its associated workload or application name and use software such as Azure DevOps to perform automated tasks on those resources.

HOW DO I MANAGE RESOURCE TAGS?

You can add, modify, or delete resource tags through Windows PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.

you can also use Azure Policy to enforce tagging rules and conventions.