Azure Services

- Azure services range from simple web services for hosting your business presence in the cloud to running fully virtualized computers for you to run your custom software solutions.
- Azure provides a wealth of cloud-based services like remote storage, database hosting, and centralized account management.
- Azure also offers new capabilities like AI and Internet of Things (IoT).

Cloud computing

- **Cloud computing helps to**
  - Lower your operating costs.
  - Run your infrastructure more efficiently.
  - Scale as your business needs change.
- **Cloud provides on-demand access to:**
  - A nearly limitless pool of raw compute, storage, and networking components.
  - Speech recognition and other cognitive services that help make your application stand out from the crowd.
  - Analytics services that deliver telemetry data from your software and devices.

Azure

- Azure is cloud computing platform
- Azure uses technology knows as virtualization

Azure portal

- The Azure portal is a web-based, unified console that provides an alternative to command-line tools.
- With the Azure portal, you can manage your Azure subscription by using a graphical user interface. You can:
  - Build, manage, and monitor everything from simple web apps to complex cloud deployments.
  - Create custom dashboards for an organized view of resources.
  - Configure accessibility options for an optimal experience.
- You can create a custom dashboard from azure portal

Azure Marketplace

- Azure Marketplace helps connect users with Microsoft partners, independent software vendors, and startups that are offering their solutions and services, which are optimized to run on Azure.
- Azure Marketplace customers can find, try, purchase, and provision applications and services from hundreds of leading service providers.
- All solutions and services are certified to run on Azure.

Azure Services and Faunctions

Compute	
Service Name	**Service Function**
Azure Virtual Network	Connects VMs to incoming virtual private network (VPN) connections.
Azure Load Balancer	Balances inbound and outbound connections to applications or service endpoints.
Azure Application Gateway	Optimizes app server farm delivery while increasing application security.
Azure VPN Gateway	Accesses Azure Virtual Networks through high-performance VPN gateways.
Azure DNS	Provides ultra-fast DNS responses and ultra-high domain availability.
Azure Content Delivery Network	Delivers high-bandwidth content to customers globally.
Azure DDoS Protection	Protects Azure-hosted applications from distributed denial of service (DDOS) attacks.

Azure Traffic Manager	Distributes network traffic across Azure regions worldwide.
Azure ExpressRoute	Connects to Azure over high-bandwidth dedicated secure connections.
Azure Network Watcher	Monitors and diagnoses network issues by using scenario-based analysis.
Azure Firewall	Implements high-security, high-availability firewall with unlimited scalability.
Azure Virtual WAN	Creates a unified wide area network (WAN) that connects local and remote sites.

Storage	
Service Name	**Service Function**
Azure Blob storage	Storage service for very large objects, such as video files or bitmaps.
Azure File storage	File shares that can be accessed and managed like a file server.
Azure Queue storage	A data store for queuing and reliably delivering messages between applications.
Azure Table storage	Table storage is a service that stores non-relational structured data (also known as structured NoSQL data) in the cloud, providing a key/attribute store with a schemeless design.

Databases	
Service Name	**Service Function**
Azure Cosmos DB	Globally distributed database that supports NoSQL options.
Azure SQL Database	Fully managed relational database with auto-scale, integral intelligence, and robust security.
Azure Database for MySQL	Fully managed and scalable MySQL relational database with high availability and security.
Azure Database for PostgreSQL	Fully managed and scalable PostgreSQL relational database with high availability and security.
SQL Server on Azure Virtual Machines	Service that hosts enterprise SQL Server apps in the cloud.
Azure Synapse Analytics	Fully managed data warehouse with integral security at every level of scale at no extra cost.
Azure Database Migration Service	Service that migrates databases to the cloud with no application code changes.
Azure Cache for Redis	Fully managed service caches frequently used and static data to reduce data and application latency.
Azure Database for MariaDB	Fully managed and scalable MariaDB relational database with high availability and security.

Web	
Service Name	**Description**
Azure App Service	Quickly create powerful cloud web-based apps.
Azure Notification Hubs	Send push notifications to any platform from any back end.
Azure API Management	Publish APIs to developers, partners, and employees securely and at scale.
Azure Cognitive Search	Deploy this fully managed search as a service.
Web Apps feature of Azure App Service	Create and deploy mission-critical web apps at scale.
Azure SignalR Service	Add real-time web functionalities easily.

IoT	
Service Name	**Description**
IoT Central	Fully managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage IoT assets at scale.
Azure IoT Hub	Messaging hub that provides secure communications between and monitoring of millions of IoT devices.
IoT Edge	Fully managed service that allows data analysis models to be pushed directly onto IoT devices, which allows them to react quickly to state changes without needing to consult cloud-based AI models.

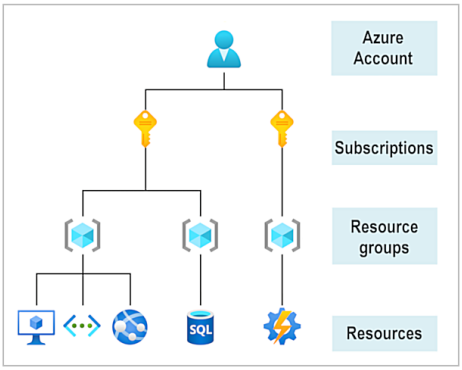
Big Data	
Service Name	**Description**
Azure Synapse Analytics	Run analytics at a massive scale by using a cloud-based enterprise data warehouse that takes advantage of massively parallel processing to run complex queries quickly across petabytes of data.
Azure HDInsight	Process massive amounts of data with managed clusters of Hadoop clusters in the cloud.
Azure Databricks	Integrate this collaborative Apache Spark-based analytics service with other big data services in Azure.

AI	
Service Name	**Description**
Azure Machine Learning Service	Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the cloud.
Azure ML Studio	Collaborative visual workspace where you can build, test, and deploy machine learning solutions by using prebuilt machine learning algorithms and data-handling modules.

Cognitive Services API	
Service Name	**Description**
Vision	Use image-processing algorithms to smartly identify, caption, index, and moderate your pictures and videos.
Speech	Convert spoken audio into text, use voice for verification, or add speaker recognition to your app.
Knowledge mapping	Map complex information and data to solve tasks such as intelligent recommendations and semantic search.
Bing Search	Add Bing Search APIs to your apps and harness the ability to comb billions of webpages, images, videos, and news with a single API call.
Natural Language processing	Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.

Cognitive Services API	
Service Name	**Description**
Azure DevOps	Use development collaboration tools such as high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. Formerly known as Visual Studio Team Services.
Azure DevTest Labs	Quickly create on-demand Windows and Linux environments to test or demo applications directly from deployment pipelines.

Azure Account



Azure free account

- Free access to popular Azure products for 12 months.
- A credit to spend for the first 30 days.
- Access to more than 25 products that are always free.
- Azure Free Student Account
    - Free access to certain Azure services for 12 months.
    - A credit to use in the first 12 months.
    - Free access to certain software developer tools.

Azure Models

Deployment model	Deployment model
Public cloud	Services are offered over the public internet and available to anyone who wants to purchase them. Cloud resources, such as servers and storage, are owned and operated by a third-party cloud service provider, and delivered over the internet.
Private cloud	A private cloud consists of computing resources used exclusively by users from one business or organization. A private cloud can be physically located at your organization's on-site (on-premises) datacenter, or it can be hosted by a third-party service provider.
Hybrid cloud	A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them.

1. **Public cloud**
    - No capital expenditures to scale up.
    - Applications can be quickly provisioned and deprovisioned.
    - Organizations pay only for what they use.
2. **Private cloud**
    - Hardware must be purchased for start-up and maintenance.
    - Organizations have complete control over resources and security.
    - Organizations are responsible for hardware maintenance and updates.
3. **Hybrid cloud**
    - Provides the most flexibility.
    - Organizations determine where to run their applications.
    - Organizations control security, compliance, or legal requirements.

Cloud computing Advantages

- **High availability:** Depending on the service-level agreement (SLA) that you choose, your cloud-based apps can provide a continuous user experience with no apparent downtime, even when things go wrong.
- **Scalability:** Apps in the cloud can scale vertically and horizontally:
  - Scale vertically to increase compute capacity by adding RAM or CPUs to a virtual machine.
  - Scaling horizontally increases compute capacity by adding instances of resources, such as adding VMs to the configuration.
- **Elasticity:** You can configure cloud-based apps to take advantage of autoscaling, so your apps always have the resources they need.
- **Agility:** Deploy and configure cloud-based resources quickly as your app requirements change.
- **Geo-distribution:** You can deploy apps and data to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region.
- **Disaster recovery:** By taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your apps with the confidence that comes from knowing that your data is safe in the event of disaster.

Capital expenses vs. operating expenses

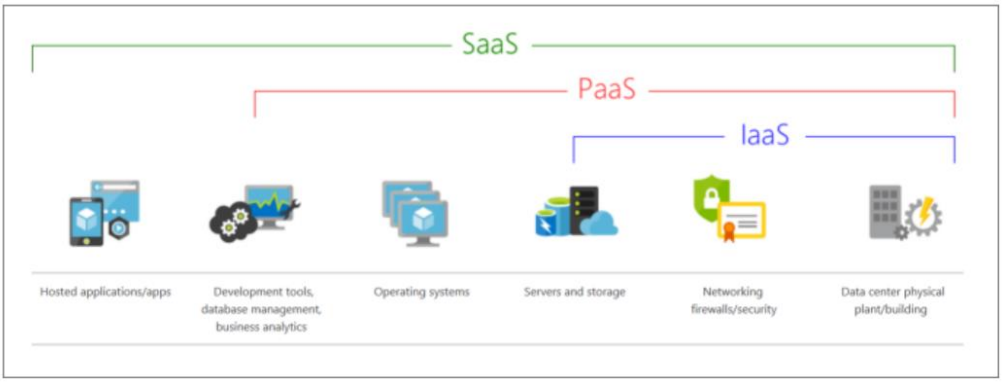
- **Capital Expenditure (CapEx):**
  - is the up-front spending of money on physical infrastructure, and then deducting that up-front expense over time.
  - The up-front cost from CapEx has a value that reduces over time.
- **Operational Expenditure (OpEx)**
  - With Operating Expenses (OpEx), you are only responsible for the computing resources that you use.
  - There is no up-front cost, as you pay for a service or product as you use it.
  - Is spending money on services or products now, and being billed for them now.
  - You can deduct this expense in the same year you spend it

Cloud computing is a consumption-based model

- Cloud service providers operate on a consumption-based model, which means that end users only pay for the resources that they use. Whatever they use is what they pay for.
- A consumption-based model has many benefits, including:
  - No upfront costs.
  - No need to purchase and manage costly infrastructure that users might not use to its fullest.
  - The ability to pay for additional resources when they are needed.
  - The ability to stop paying for resources that are no longer needed.

Cloud Service Models

- **IaaS (Infrastructure-as-a-Service)**
  - This cloud service model is the closest to managing physical servers;
  - A cloud provider will keep the hardware up-to-date
    - In an IaaS environment, the cloud tenant (Cloud Provider) is responsible for routine hardware maintenance.
  - but operating system maintenance and network configuration is up to you as the cloud tenant.
- **PaaS (Platform-as-a-Service)**
  - This cloud service model is a managed hosting environment.
  - The cloud provider manages the virtual machines and networking resources, and the cloud tenant deploys their applications into the managed hosting environment.
  - For example,
    - **Azure App Services** provides a managed hosting environment where developers can upload their web applications, without having to worry about the physical hardware and software requirements
- **SaaS (Software-as-a-Service)**
  - In this cloud service model, the cloud provider manages all aspects of the application environment, such as virtual machines, networking resources, data storage, and applications.
  - The cloud tenant only needs to provide their data to the application managed by the cloud provider.
  - For example,
    - Microsoft Office 365 provides a fully working version of Microsoft Office that runs in the cloud.
    - All you need to do is create your content, and Office 365 takes care of everything else.



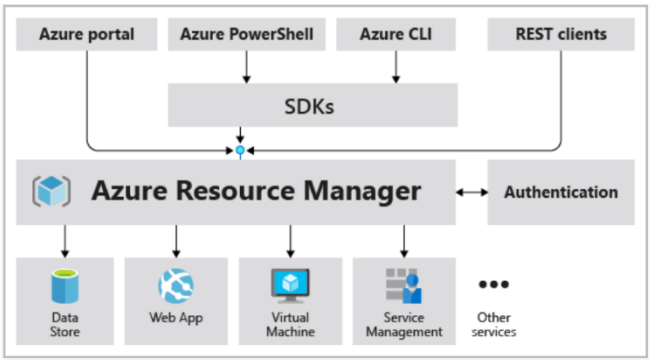
Cloud service model comparison

IaaS	PaaS	SaaS
IaaS is the most flexible category of cloud services. It aims to give you complete control over the hardware that runs your application. Instead of buying hardware, with IaaS, you rent it.	This cloud service model is a managed hosting environment.	SaaS is software that's centrally hosted and managed for you and your users or customers. Usually one version of the application is used for all customers, and it's licensed through a monthly or annual subscription.
No CapEx. Users have no up-front costs.	No CapEx. Users have no up-front costs.	No CapEx. Users have no up-front costs.
Consumption-based model. Organizations pay only for what they use and operate under an Operational Expenditure (OpEx) model.	Consumption-based model. Users pay only for what they use, and operate under an OpEx model.	Pay-as-you-go pricing model. Users pay for the software they use on a subscription model, typically monthly or yearly, regardless of how much they use the software.
Examples: • Azure Virtual Machines • Deploys several custom applications to azure	**Examples:** • Azure SQL Database • Azure Cosmo DB • Azure Backup	**Examples:** • Office 365 •

Serverless Computing

- Like PasS, Serverless computing enables developers to build applications faster by eliminating the need for them to manage infrastructure.
- With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code.
- Serverless architectures are highly scalable and event-driven, only using resources when a specific function or trigger occurs.
-

Resource Group



- Resource groups are a fundamental element of the Azure platform.
- A resource group is a logical container for resources deployed on Azure.
- These resources are anything you create in an Azure subscription like VMs, Azure Application Gateway instances, and Azure Cosmos DB instances.
- All resources must be in a resource group, and a resource can only be a member of a single resource group.
- Many resources can be moved between resource groups with some services having specific limitations or requirements to move.
- **Resource groups can't be nested.**
- Before any resource can be provisioned, you need a resource group for it to be placed in.
- **Life Cycle**
    - If you delete a resource group, all resources contained within it are also deleted.
    - Resource groups make it easy to remove a set of resources all at once.
- **Authorization**
    - Resource groups are also a scope for applying role-based access control (RBAC) permissions.
    - By applying RBAC permissions to a resource group, you can ease administration and limit access to allow only what's needed.

Azure Resource Manger

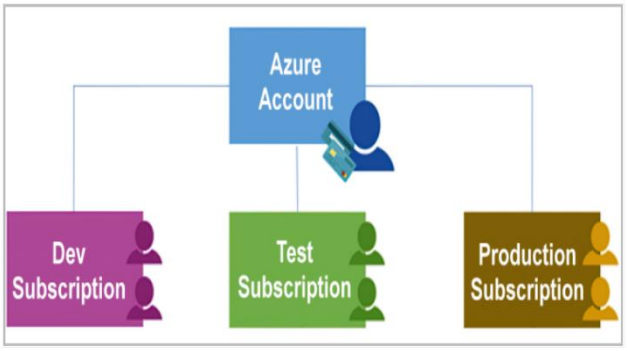
- Azure Resource Manager is the deployment and management service for Azure.
- It provides a management layer that enables you to create, update, and delete resources in your Azure account.
- You use management features like access control, locks, and tags to secure and organize your resources after deployment.

- When a user sends a request from any of the Azure tools, APIs, or SDKs, Resource Manager receives the request.
- It authenticates and authorizes the request.
- Resource Manager sends the request to the Azure service, which takes the requested action.
- Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.

Azure Recourse Manger Benefits

- Manage your infrastructure through declarative templates rather than scripts. A Resource Manager template is a JSON file that defines what you want to deploy to Azure.
- Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.
- Redeploy your solution throughout the development life cycle and have confidence your resources are deployed in a consistent state.
- Define the dependencies between resources so they're deployed in the correct order.
- Apply access control to all services because **RBAC (Role Based Access Control)** is natively integrated into the management platform.
- Apply tags to resources to logically organize all the resources in your subscription.

- Clarify your organization's billing by viewing costs for a group of resources that share the same tag.



Azure Subscriptions

- Using Azure requires an Azure subscription.
- A subscription provides you with authenticated and authorized access to Azure products and services.
- It also allows you to provision resources.
- An Azure subscription is a logical unit of Azure services that links to an Azure account, which is an identity in Azure Active Directory (Azure AD) or in a directory that Azure AD trusts.
- An account can have one subscription or multiple subscriptions that have different billing models and to which you apply different access-management policies.
- You can use Azure subscriptions to define boundaries around Azure products, services, and resources.

There are two types of subscription boundaries that you can use:

Billing boundary:

- This subscription type determines how an Azure account is billed for using Azure.
- You can create multiple subscriptions for different types of billing requirements.
- Azure generates separate billing reports and invoices for each subscription so that you can organize and manage costs.

Access control boundary:

- Azure applies access-management policies at the subscription level, and you can create separate subscriptions to reflect different organizational structures.
- An example is that 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

Azure management groups

- Azure management groups are containers for the subscriptions
- Azure management group provides access, policies and compliance to subscription.
- **If we apply conditions to management group, it will automatically apply to all subscriptions in it**
    - For example, you can apply policies to a management group that limits the regions available for VM creation. This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region.
- All subscriptions with single management group must trust the same Azure AD trust.

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.
- Each management group can have many children.
- All subscriptions and management groups are within a single hierarchy in each directory.

Virtual Machines

- Virtual machines are software emulations of physical computers.
- **Virtual Machines provides infrastructure as a service (IaaS)** and can be used in different ways.

- Just like a physical computer, you can customize all of the software running on the VM.
- VMs are an ideal choice when you need:
    - Total control over the operating system (OS).
    - The ability to run custom software.
    - To use custom hosting configurations.
- An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM. You still need to configure, update, and maintain the software that runs on the VM.
- An **Image** is a template used to create a VM.
- These templates already include an OS and often other software, like development tools or web hosting environments.
- **When to use VMs**
    - During testing and development.
    - When running applications in the cloud
    - When extending your datacenter to the cloud.
    - During disaster recovery.
        - If a primary datacenter fails, you can create VMs running on Azure to run your critical applications and then shut them down when the primary datacenter becomes operational again.
        - you can get significant cost savings by using an **IaaS-based approach to disaster recovery**
    - VMs are also an excellent choice when you move from a physical server to the cloud (also known as **lift and shift**).
    - You can run single VMs for testing, development, or minor tasks. Or you can group VMs together to provide high availability, scalability, and redundancy

Virtual machine scale sets

- Virtual machine scale sets let you create and manage a group of identical, load-balanced VMs.
- Scale sets allow you to centrally manage, configure, and update a large number of VMs in minutes to provide highly available applications.
- With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

Azure Batch

- Azure Batch enables large-scale parallel and high-performance computing (HPC) batch jobs with the ability to scale to tens, hundreds, or thousands of VMs.
- WebJobs are often used to run background tasks as part of your application logic.

When you're ready to run a job, Batch does the following:

1. Starts a pool of compute VMs for you.
2. Installs applications and staging data.
3. Runs jobs with as many tasks as you have.
4. Identifies failures.
5. Requeues work.
6. Scales down the pool as work completes.

Azure App Service

- With Azure App Service, you can quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform.
- App Service is a platform as a service (PaaS) offering.
- App Service enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure.
- It offers automatic scaling and high availability.
- App Service supports Windows and Linux and enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.
- With App Service, you can host most common app service styles like:
    - 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.

Containers and Kubernetes

- Container Instances and Azure Kubernetes Service are Azure compute resources that you can use to deploy and manage containers
- Containers are lightweight, virtualized application environments.
- Using containers, you can run multiple instances of a application on a single host machine.
- Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host.
- Containers are designed to allow you to respond to changes on demand.
- One of the most popular container engines is **Docker**, which is supported by Azure.
- **Azure Container Services**
    - Azure Container Instances offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services.
    - It's a platform as a service (PaaS) offering that allows you to upload your containers, which it runs for you.
- **Azure Kubernetes services**
    - The task of automating, managing, and interacting with a large number of containers is known as orchestration.
    - Azure Kubernetes Service is a complete orchestration service for containers with distributed architectures and large volumes of containers.

Microservices

- Containers are often used to create solutions by using a microservice architecture.
- This architecture is where you break solutions into smaller, independent pieces.

Serverless computing

- Serverless computing is the abstraction of servers, infrastructure, and operating systems.
- Serverless computing includes the abstraction of servers, an event-driven scale, and micro-billing
- With serverless computing, Azure takes care of managing the server infrastructure and the allocation and deallocation of resources based on demand.
- With serverless computing, they pay only for the time their code runs. If no active function executions occur, they're not charged. For example, if the code runs once a day for two minutes, they're charged for one execution and two minutes of computing time.
- Azure has two implementations of serverless compute:
    - **Azure Functions**:
        - Functions are a key component of serverless computing.
        - Functions can execute code in almost any modern language.
        - Functions are ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure.
        - They're commonly used when you 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.
        - Functions scale automatically based on demand
        - With functions, Azure runs your code when it's triggered and automatically deallocates resources when the function is finished
        - Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they're restarted every time they respond to an event. When they're stateful (called Durable Functions), a context is passed through the function to track prior activity.

        - Can run locally or in the cloud.
    - **Azure Logic Apps**:
        - Logic apps are designed in a web-based designer and can execute logic triggered by Azure services without writing any code.
        - Logic apps are similar to functions. Both enable you to trigger logic based on an event. Where functions execute code, logic apps execute workflows that are designed to automate business scenarios and are built from predefined logic blocks.
        - Runs only in the cloud.

With Functions, you write code to complete each step.
With Logic Apps, you use a GUI to define the actions and how they relate to one another.

Azure Virtual Desktop

- Azure Virtual Desktop is a desktop and application virtualization service that runs on the cloud. It enables your users to use a cloud-hosted version of Windows from any location.
- User sign-in to Azure Virtual Desktop is fast because user profiles are containerized by using FSLogix.
- Azure Virtual Desktop also improves security by using reverse connect technology.
- Azure Virtual Desktop lets you use Windows 10 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM.
-

Azure virtual networking

- Azure virtual networks 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 links other Azure resources.
- Azure virtual network allows you to create multiple isolated virtual networks.
- You can also configure the virtual network to use an internal or an external DNS server.
- A VM in Azure can connect to the internet by default.
- You can enable incoming connections from the internet by assigning a public IP address to the VM or by putting the VM behind a public load balancer.
- **Virtual networks**
    - 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**
    - You can use service endpoints to 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 networks**
        - The typical approach to a virtual private network (VPN) connection is from a computer outside your organization, back into your corporate network.
        - In this case, the client computer initiates an encrypted VPN connection to connect that computer to the Azure virtual network.
    - **Site-to-site virtual private networks**
        - A site-to-site VPN links 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**
        - For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach.
        - ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet. (You'll learn more about ExpressRoute in a separate unit later in this module.)
- **Route network traffic**
    - **Route tables**
        - A route table allows you to define rules about how traffic should be directed.
        - Azure automatically creates a route table for each subnet within an Azure virtual network and adds system default routes to the table.
    - **Border Gateway Protocol**
        - Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.
- **Filter network traffic**
    - **Network security groups**
        - A network security group is an Azure resource that can contain multiple inbound and outbound security rules.
        - Network security groups have security rules that enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces.
        - 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**
        - A network virtual appliance is a specialized VM 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.
- **Peering**
    - Peering enables resources in each virtual network to communicate with each other.
- **User-defined routes (UDR)**
    - User-defined routes (UDR) are a significant update to Azure's Virtual Networks that allows for greater control over network traffic flow.

- This method allows network administrators to control the routing tables between subnets within a VNet, as well as between VNets.

Azure VPN

- They’re typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet).
- **For example**,
  - let's say that your offices on the East coast region of North America need to access your company's private customer data, which is stored on servers that are physically located in a West coast region. A VPN can connect your East coast offices to your West coast servers allowing your company to securely access your private customer data.
- A VPN gateway enable the following connectivity:
  1. Connect on-premises datacenters to virtual networks through a site-to-site connection.
  2. Connect individual devices to virtual networks through a point-to-site connection.
  3. Connect virtual networks to other virtual networks through a network-to-network connection.
- **To connect your datacenter to a VPN gateway, you'll need these on-premises resources:**
  - A VPN device that supports policy-based or route-based VPN gateways
  - A public-facing (internet-routable) IPv4 address

Azure ExpressRoute

- For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach.
- ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet.
- ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider.
- With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.
- ExpressRoute connections don't go over the public Internet.
- Border Gateway Protocol (BGP)
    - ExpressRoute uses the Border Gateway Protocol (BGP) routing protocol.
    - BGP is used to exchange routes between on-premises networks and resources running in Azure.
    - This protocol enables dynamic routing between your on-premises network and services running in the Microsoft cloud.
- ExpressRoute supports the following models that you can use to connect your on-premises network to the Microsoft cloud:
    1. CloudExchange colocation
    2. Point-to-point Ethernet connection
    3. Any-to-any connection
    4. Directly from ExpressRoute sites

IOT HUB

- From a cloud-to-device perspective, IoT Hub allows for command and control.
- Azure IoT Hub is a managed service that's hosted in the cloud and that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages.
- IoT Hub monitoring helps you maintain the health of your solution by tracking events such as device creation, device failures, and device connections.

Azure IoT Central

- Azure IoT Central builds on top of IoT Hub by adding a dashboard that allows you to connect, monitor, and manage your IoT devices.
- The visual user interface (UI) makes it easy to quickly connect new devices and watch as they begin sending telemetry or error messages.
- You can watch the overall performance across all devices in aggregate, and you can set up alerts that send notifications when a specific device needs maintenance.
- Finally, you can push firmware updates to the device.

Azure Sphere

- Azure Sphere creates an end-to-end, highly secure IoT solution for customers that encompasses everything from the hardware and operating system on the device to the secure method of sending messages from the device to the message hub.
- Azure Sphere ensures a secure channel of communication between the device and Azure by controlling everything from the hardware to the operating system and the authentication process.
- Azure Sphere has built-in communication and security features for internet-connected devices.
- Azure Sphere comes in three parts:
    - Sphere micro-controller unit (MCU)
        - which is responsible for processing the operating system and signals from attached sensors.
    - Linux operating system (OS)
        - that handles communication with the security service and can run the vendor's software.
    - Azure Sphere Security Service, also known as AS3.
        - Its job is to make sure that the device has not been maliciously compromised. When the device attempts to connect to Azure, it first must authenticate itself, per device, which it does by using certificate-based authentication. If it authenticates successfully, AS3 checks to ensure that the device hasn't been tampered with. After it has established a secure channel of communication, AS3 pushes any OS or approved customer-developed software updates to the device

Which Services will use?

- IoT Hub -- That promises a preemptive maintenance service agreement.
- Iot Central - fleet of delivery vehicles that transport products from warehouses to distribution centers, and from distribution centers to stores and homes.
- Azure Spare - touchless point-of-sale solution for self-checkout.

CmdLets

- Azure PowerShell is a shell with which developers and DevOps and IT professionals can execute commands called cmdlets (pronounced command-lets).

Azure Advisor

- Azure Advisor evaluates your Azure resources and makes recommendations to help improve
    - Reliability
    - Security
    - Performance
    - achieve operational excellence
    - reduce costs. Advisor is designed to help you save time on cloud optimization.
- The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

Azure Monitor

- Azure Monitor is a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment.

Service Health

- Service Healh helps you keep an eye on several event types:
    - Service Issues
    - Planned maintenance
    - Health advisories

Which Services will use?

- Azure Advisor -- wants to optimize its cloud spend
- Azure monitor -- The Tailwind Traders e-commerce website is experiencing intermittent errors, and the team is unsure of the cause.
- Azure Health -- Specifically, its cloud operations team wants to let stakeholders know about upcoming planned downtime in advance.

Microsoft Defender

- Microsoft Defender for Cloud is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises.
- **Defender for Cloud can:**
    - Monitor security settings across on-premises and cloud workloads.
    - Automatically apply required security settings to new resources as they come online.
    - Provide security recommendations that are based on your current configurations, resources, and networks.
    - Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
    - Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources. You can also use adaptive application controls to define rules that list allowed applications to ensure that only applications you allow can run.

    - Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred.
    - Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.
- Secure score is a measurement of an organization's security posture.
- Defender for Cloud to get a centralized view of all of its security alerts.
- The company will also use Azure Monitor Workbooks to automate responses to threats.

workbook that does the following steps:

1. When the alert is triggered, open a ticket in the IT ticketing system.
2. Send a message to the security operations channel in Microsoft Teams or Slack to make sure the security analysts are aware of the incident.
3. Send all of the information in the alert to the senior network admin and to the security admin. The email message includes two user option buttons: Block or Ignore.

Azure Key Vault

- Azure Key Vault is a centralized cloud service for storing an application's secrets in a single, central location.
- It provides secure access to sensitive information by providing access control and logging capabilities.

What can Azure Key Vault do

1. **Manage secrets**
    a. You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
2. **Manage encryption keys**
    a. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
3. **Manage SSL/TLS certificates**
    a. Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for both your Azure resources and your internal resources.
4. **Store secrets backed by hardware security modules (HSMs)**
    a. These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

What are the benefits of Azure Dedicated Host?

1. Gives you visibility into, and control over, the server infrastructure that's running your Azure VMs.
2. Helps address compliance requirements by deploying your workloads on an isolated server.
3. Let’s you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

Security posture

- Your security posture is your organization's ability to protect from and respond to security threats.

- The common principles used to define a security posture are **(CIA)** known collectively as CIA
  - Confidentiality
  - integrity,
  - availability

Network security group

- A network security group enables you to filter network traffic to and from Azure resources within an Azure virtual network.
- You can think of NSGs like an internal firewall.
- An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

Azure Firewall

- Azure Firewall is a managed, cloud-based network security service that helps protect resources in your Azure virtual networks.
- It's a fundamental building block for your private network that enables virtual machines and other compute resources to securely communicate with each other, the internet, and on-premises networks.
- Azure Firewall is a stateful firewall.
- Azure Firewall provides a central location to create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- **Azure Firewall provides many features, including:**
  - Built-in high availability.
  - Unrestricted cloud scalability.
  - Inbound and outbound filtering rules.
  - Inbound Destination Network Address Translation (DNAT) support.
  - Azure Monitor logging.
- **What can I configure with Azure Firewall?**
  - Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
  - Network rules that define source address, protocol, destination port, and destination address.
  - Network Address Translation (NAT) rules that define destination IP addresses and ports to translate inbound requests.
- **Which of the following provides web application firewall (WAF)**
  - Azure Application Gateway
  - Azure Front Door
  - Azure Content Delivery Network

- **What kinds of attacks can DDoS Protection help prevent?**
  - Volumetric attacks
  - Protocol attacks
  - Resource-layer (application-layer) attacks (only with web application firewall)

TCO (Total Cost of Ownership) Calculator

- The TCO Calculator helps you estimate the cost savings of operating your solution on Azure over time, instead of in your on-premises datacenter.

Azure Cost Management + Billing

Azure Cost Management + Billing is a free service that helps you understand your Azure bill, manage your account and subscriptions, monitor and control Azure spending, and optimize resource use.

Tags

- Tags help you manage costs associated with the different groups of Azure products and resources.
- You can apply tags to groups of Azure resources to organize billing data.

service credit

A service credit is the percentage of the fees you paid that are credited back to you according to the claim approval process.

General availability (GA).

- After a new Azure service is validated and tested, it's released to all customers as a production-ready service. This is known as general availability (GA).

Multifactor authentication

- Multifactor authentication is a process where a user is prompted during the sign-in process for an additional form of identification

Conditional Access

- Conditional Access is a tool that Azure Active Directory 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 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.
- **Where is Conditional Access available?**
    - To use Conditional Access, you need an Azure AD Premium P1 or P2 license. If you have a Microsoft 365 Business Premium license, you also have access to Conditional Access features.

Conditional Access is useful when you need to:

- Require multifactor authentication to access an application. You can configure whether all users require multifactor authentication or only certain users, such as administrators. You can also configure whether multifactor authentication applies to access from all networks or only untrusted networks.
- Require access to services only through approved client applications.
- Require users to access your application only from managed devices.
- Block access from untrusted sources, such as access from unknown or unexpected locations.

What services does Azure AD provide?

- Authentication
- Single Sign-on
- Application Management
- Device Management

Azure AD Connect

- Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD

Scope

- Role-based access control is applied to a scope,
- Scopes include:
    - A management group (a collection of multiple subscriptions).
    - A single subscription.
    - A resource group.
    - A single resource.

When should I use Azure RBAC?

- Allow one user to manage VMs in a subscription and another user to manage virtual networks.
- Allow a database administrator group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

Azure RBCA

- Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager.
- You can access Resource Manager from the
    - Azure portal
    - Azure Cloud Shell
    - Azure PowerShell
    - Azure CLI.
- Azure RBAC doesn't enforce access permissions at the application or data level.
- You can apply Azure RBAC to an individual person or to a group.
- You can also apply Azure RBAC to other special identity types, such as service principals and managed identities.
- You manage access permissions on the Access control (IAM) pane in the Azure portal.
- A resource lock prevents resources from being accidentally deleted or changed.
- You can set the lock level to CanNotDelete or ReadOnly.

Azure Policy

- Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources.
- These policies enforce different rules and effects over your resource configurations so that those configurations stay compliant with corporate standards.
- Azure Policy enables you to define both individual policies and groups of related policies, known as initiatives.
- Azure Policy evaluates your resources and highlights resources that aren't compliant with the policies you've created.
- Azure Policy can also prevent noncompliant resources from being created.
- **Implementing a policy in Azure Policy involves these three steps:**
    - Create a policy definition.
    - Assign the definition to resources.
    - Review the evaluation results.
- Policy evaluation happens about once per hour.
    - If you make changes to your policy definition and create a policy assignment, that policy is evaluated over your resources within the hour.

Enable Monitoring in Azure Security Center initiative

- Enable Monitoring in Azure Security Center initiative, the following policy definitions are included:
    - Monitor unencrypted SQL Database in Security Center
    - Monitor OS vulnerabilities in Security Center
    - Monitor missing Endpoint Protection in Security Center

Azure Blueprints

- Azure Blueprints can automatically replace the resource lock if that lock is removed.
- Azure Blueprints orchestrates the deployment of various resource templates and other artifacts, such as:
    - Role assignments
    - Policy assignments
    - Azure Resource Manager templates
    - Resource groups
- Implementing a blueprint in Azure Blueprints involves these three steps:
    - Create an Azure blueprint.
    - Assign the blueprint.
    - Track the blueprint assignments.
- Blueprints are also versioned. Versioning enables you to track and comment on changes to your blueprint.
- Each component in the blueprint definition is known as an artifact.

The Cloud Adoption Framework includes these stages:

1. Define your strategy.
2. Make a plan.
3. Ready your organization.
4. Adopt the cloud.
5. Govern and manage your cloud environments.