Azure Compute

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

1. Total control over the operating system (OS).
2. The ability to run custom software.
3. 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.
However, as an IaaS offering, you still need to configure, update, and maintain the software that runs on the VM.

Image:-

- You can even create or use an already created image to rapidly provision VMs.
- You can create and provision a VM in minutes when you select a preconfigured VM image.

An image is a template used to create a VM and may already include an OS and other software, like development tools or web hosting environments.

Scale VMs:-

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

1. 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.
- The number of VM instances can automatically increase or decrease in response to demand, or you can set it to scale based on a defined schedule.
- Virtual machine scale sets also automatically deploy a load balancer to make sure that your resources are being used efficiently.
- With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

2. Virtual machine availability sets

Virtual machine availability sets are another tool to help you build a more resilient, highly available environment.

Availability sets 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.

1. **Update domain:**
    - The update domain groups VMs that can be rebooted at the same time.
    - This setup allows you to apply updates while knowing that only one update domain grouping is offline at a time.
    - All of the machines in one update domain update.
    - An update group going through the update process is given a 30-minute time to recover before maintenance on the next update domain starts.
2. **Fault domain:**
    - The fault domain groups your VMs by common power source and network switch.
    - By default, an availability set splits your VMs across up to three fault domains.
    - This helps protect against a physical power or networking failure by having VMs in different fault domains (thus being connected to different power and networking resources).

Azure virtual desktop:-

- Azure Virtual Desktop is a desktop and application virtualization service that runs on the cloud.

- It enables you to use a cloud-hosted version of Windows from any location.
- Azure Virtual Desktop works across devices and operating systems, and works with apps that you can use to access remote desktops or most modern browsers.

Enhance security

- Azure Virtual Desktop provides centralized security management for users' desktops with Microsoft Entra ID.
- You can enable multi factor authentication to secure user sign-ins.
- You can also secure access to data by assigning granular role-based access controls (RBACs) to users.
- With Azure Virtual Desktop, the data and apps are separated from the local hardware.
- The actual desktop and apps are running in the cloud, meaning the risk of confidential data being left on a personal device is reduced.
- Additionally, user sessions are isolated in both single and multi-session environments.

Multi-session Windows 10 or Windows 11 deployment

- Azure Virtual Desktop lets you use Windows 10 or Windows 11 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM.

- Azure Virtual Desktop also provides a more consistent experience with broader application support compared to Windows Server-based operating systems.

Azure containers:-

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

Azure Container Instances

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

Azure Container Apps

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

Azure Kubernetes Service

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

Use containers in your solutions

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

Imagine your website back-end reaches capacity, but the front end and storage aren't 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 event wakes the function, alleviating the need to keep resources provisioned when there are no events.
- Using Azure Functions 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 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, so they may be a good choice when demand is variable.
- Azure Functions runs your code when it triggers and automatically deallocates resources when the function is finished.
- In this model, Azure only charges you for the CPU time used while your function runs.
- Functions can be either stateless or stateful.
- When they're **stateless** (the default), they behave as if they restart 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.
- Functions are a key component of serverless computing.
- They're also a general compute platform for running any type of code.
- If the needs of the developer's app change, you can deploy the project in an environment that isn't serverless.
- This flexibility allows you to manage scaling, run on virtual networks, and even completely isolate the functions.

Azure App Service

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

- It offers automatic scaling and high availability.
- App Service supports Windows and Linux.

- It enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.
- Azure App Service is a robust hosting option that you can use to host your apps in Azure.
- Azure App Service 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 back ends.
- It supports multiple languages, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also supports both Windows and Linux environments.

With App Service, you can host most common app service styles like:

- Web apps
- API apps
- WebJobs
- Mobile apps

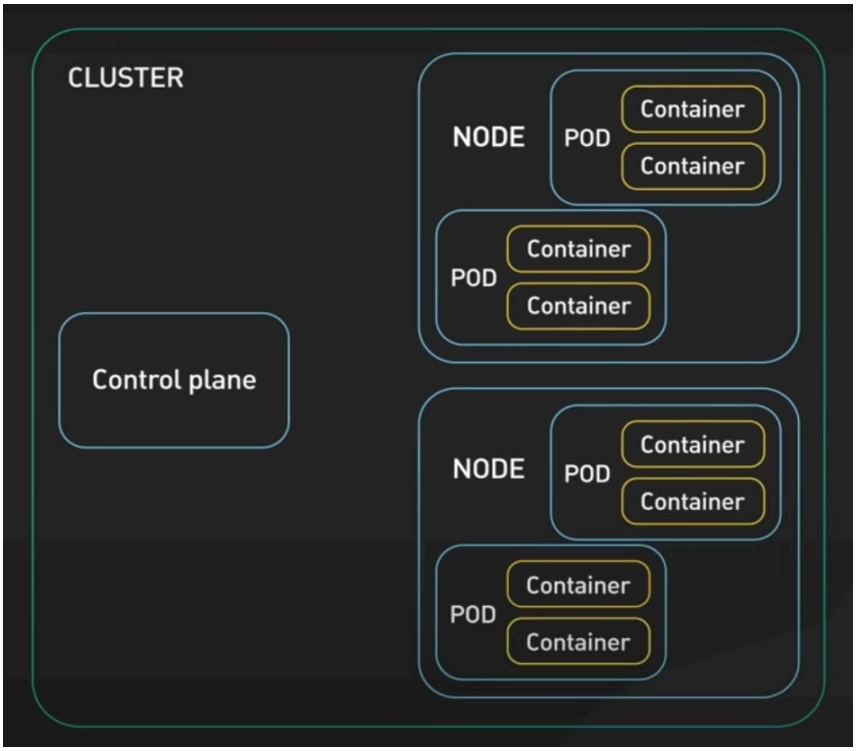
App Service handles most of the infrastructure decisions you deal with in hosting web-accessible apps:

- 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.

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

Kubernetes:-

Kubernetes is an open-source container orchestration platform.
It automates the deployment, scaling, and management of containerized applications.
A Kubernetes cluster is a set of machines, called nodes, that are used to run containerized applications.



There are two core pieces in a Kubernetes cluster.

1. The first is the **control plane**.

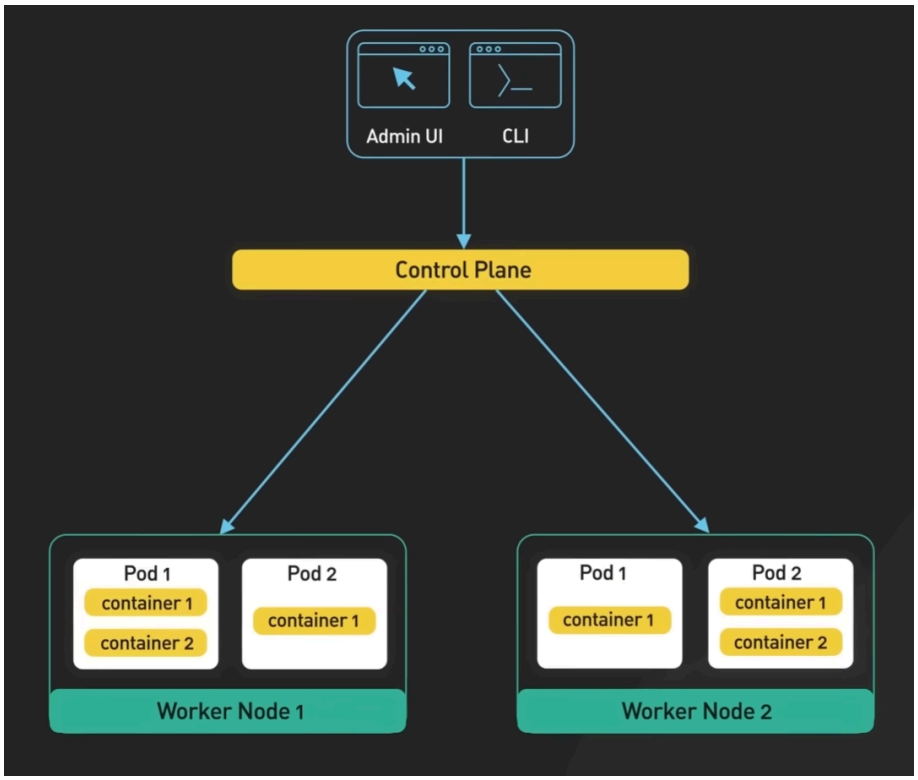
It is responsible for managing the state of the cluster.

In production environments, the control plane usually runs on multiple nodes that span across several data center zones.

2. The second is a set of **worker nodes**.

These nodes run the containerized application workloads.

The containerized applications run in a Pod.



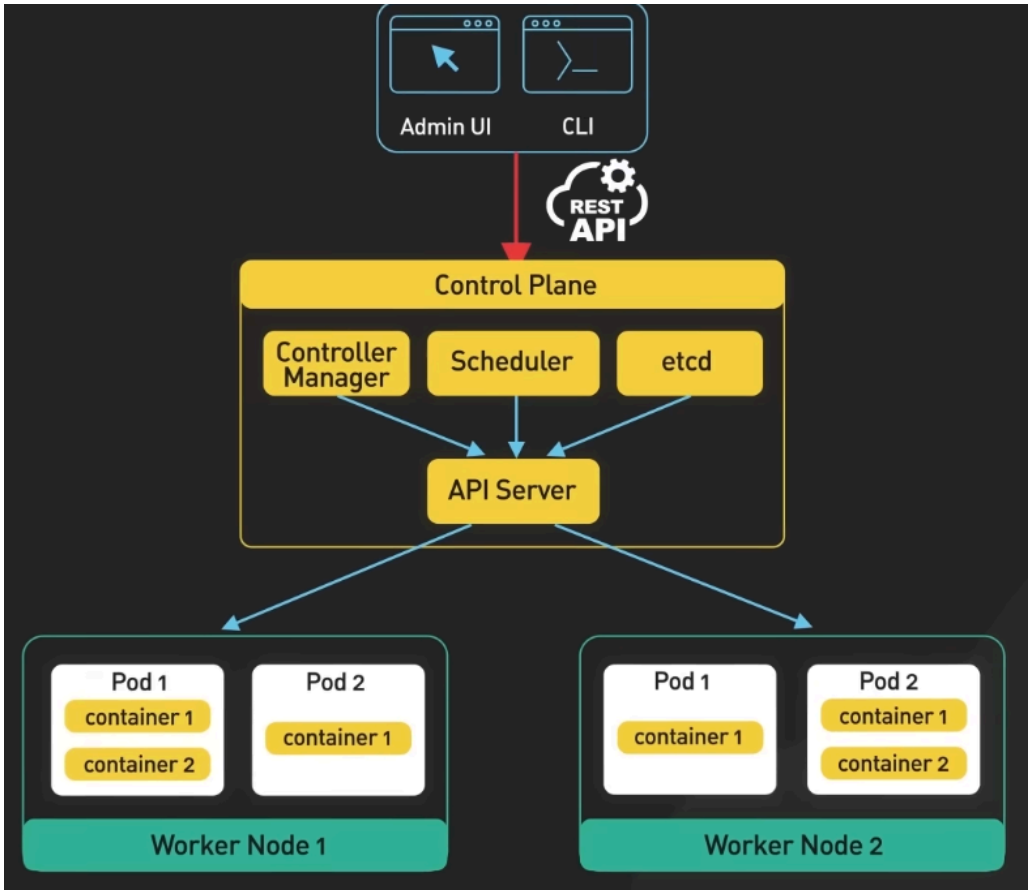
Pods are the smallest deployable units in Kubernetes. A pod hosts one or more containers and provides shared storage and networking for those containers.

Pods are created and managed by the Kubernetes control plane. They are the basic building blocks of Kubernetes applications.

Now let's dive a bit deeper into the control plane.

It consists of a number of core components.

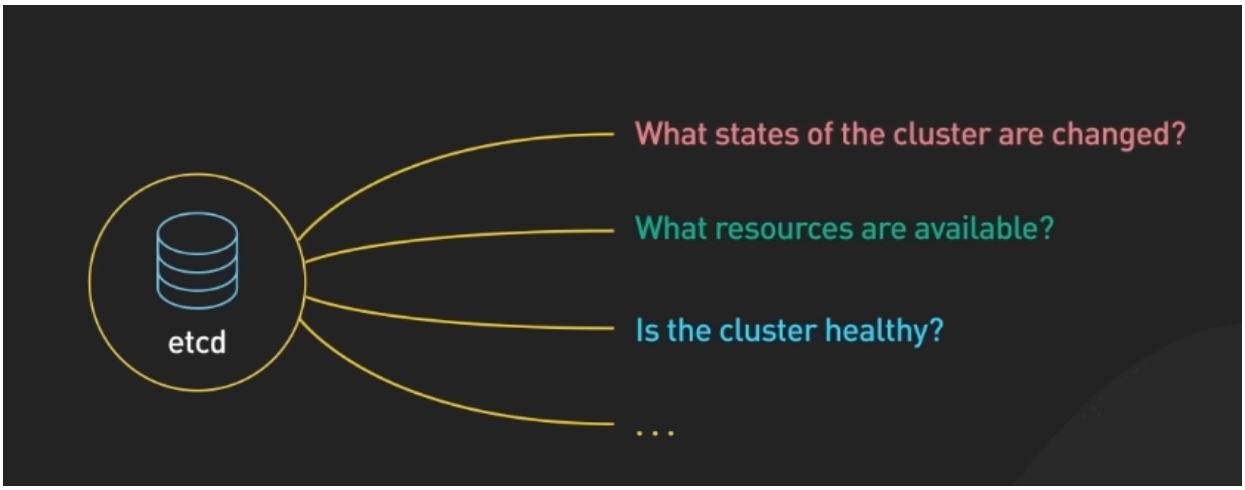
They are the API server, etcd, scheduler, and the controller manager.

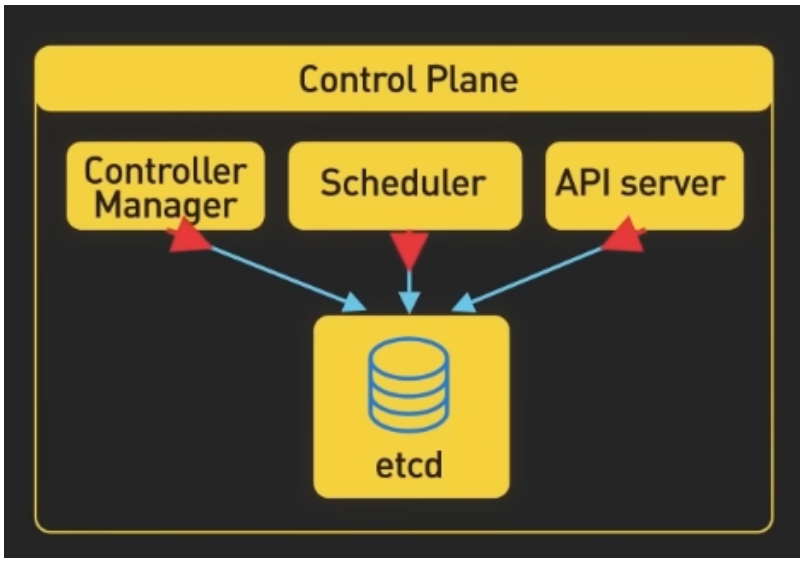


The API server is the primary interface between the control plane and the rest of the cluster.

It exposes a RESTful API that allows clients to interact with the control plane and submit requests to manage the cluster.

Etcd is a distributed key-value store.It stores the cluster's persistent state. It is used by the API server and other components of the control plane to store and retrieve information about the cluster.





The scheduler is responsible for scheduling pods onto the worker nodes in the cluster.

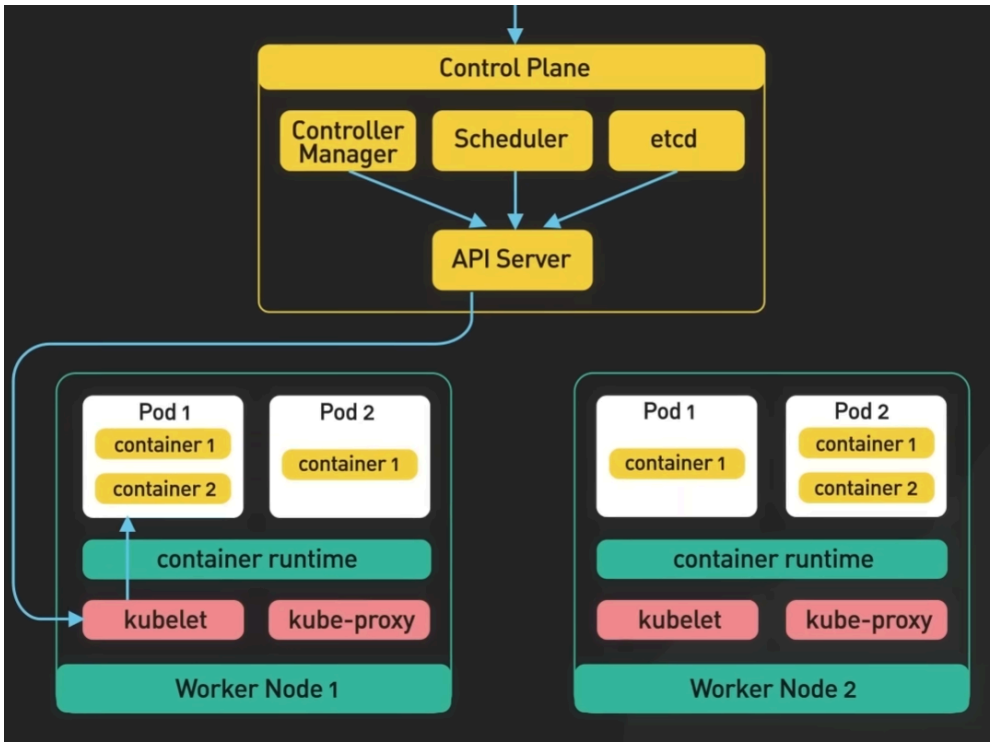
It uses information about the resources required by the pods and the available resources on the worker nodes to make placement decisions.

The controller manager is responsible for running controllers that manage the state of the cluster.

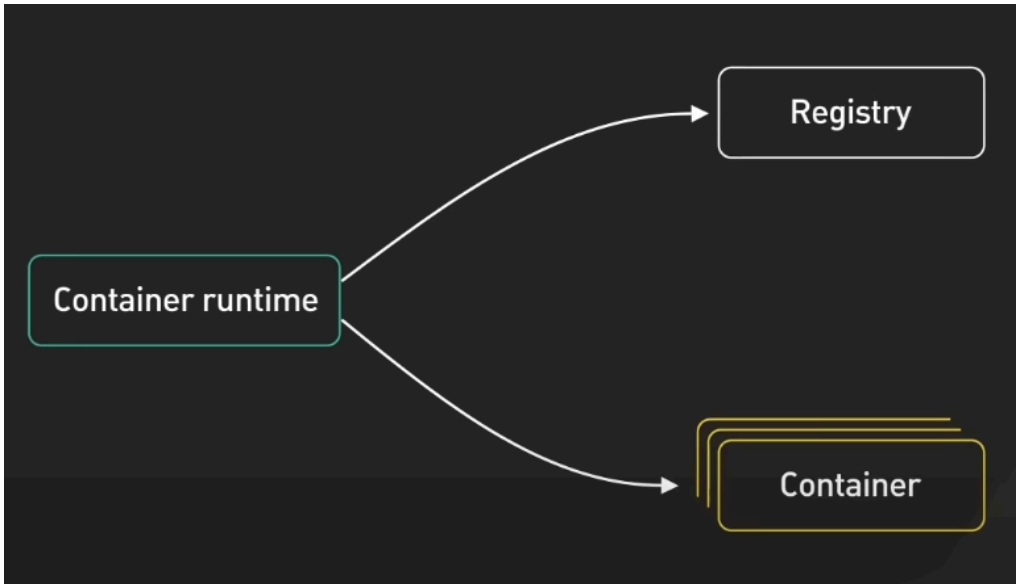
Some examples include the replication controller, which ensures that the desired number of replicas of a pod are running, and the deployment controller, which manages the rolling update and rollback of deployments.

Next, let's dive deeper into the worker nodes.

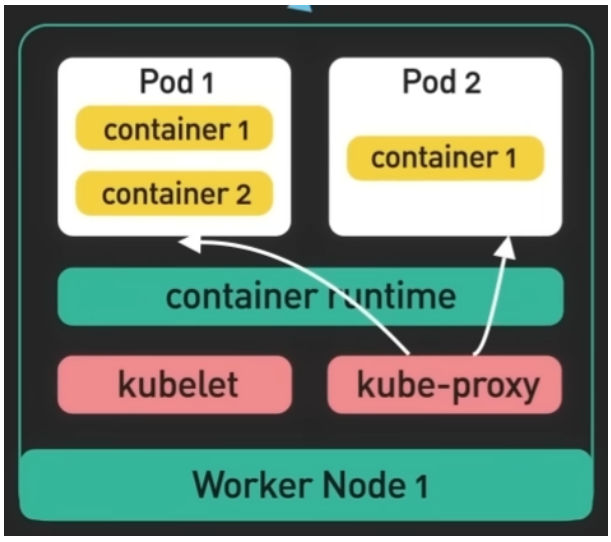
The core components of Kubernetes that run on the worker nodes include kubelet, container runtime, and kube proxy.
The kubelet is a daemon that runs on each worker node.
It is responsible for communicating with the control plane.
It receives instructions from the control plane about which pods to run on the node, and ensures that the desired state of the pods is maintained.



The container runtime runs the containers on the worker nodes.
It is responsible for pulling the container images from a registry, starting and stopping the containers, and managing the containers' resources.



The kube-proxy is a network proxy that runs on each worker node. It is responsible for routing traffic to the correct pods.
It also provides load balancing for the pods and ensures that traffic is distributed evenly across the pods.



Advantages:

- Kubernetes is scalable and highly available.
- It provides features like self-healing, automatic rollbacks, and horizontal scaling.
- It makes it easy to scale our applications up and down as needed, allowing us to respond to changes in demand quickly.
- Kubernetes is portable.
- It helps us deploy and manage applications in a consistent and reliable way regardless of the underlying infrastructure.
- It runs on-premise, in a public cloud, or in a hybrid environment.
- It provides a uniform way to package, deploy, and manage applications.

Disadvantages

- The number one drawback is complexity. Kubernetes is complex to set up and operate.
- The upfront cost is high, especially for organizations new to container orchestration.
- It requires a high level of expertise and resources to set up and manage a production Kubernetes environment.
- The second drawback is cost.
- Kubernetes requires a certain minimum level of resources to run in order to support all the features we mentioned above.
- It is likely an overkill for many smaller organizations.

One popular option that strikes a reasonable balance is to offload the management of the control plane to a managed Kubernetes service. Managed Kubernetes services are provided by cloud providers.

Some popular ones are Amazon EKS, GKE on Google Cloud, and AKS on Azure.
These services allow organizations to run the Kubernetes applications without having to worry about the underlying infrastructure.
They take care of tasks that require deep expertise, like setting up and configuring
the control plane, scaling the cluster, and providing ongoing maintenance and support.
This is a reasonable option for a mid-size organization to test out Kubernetes.

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

Public Endpoints:

Public endpoints have a public IP address and can be accessed from anywhere in the world.

Private Endpoints:

Private endpoints exist within a virtual network and have a private IP address from within the address space of that virtual network.

Networking Capabilities

Azure virtual networks provide the following key networking capabilities:

Isolation and segmentation:-

- Azure virtual network allows you to create multiple isolated virtual networks.
- When you set up a virtual network, you define a private IP address space by using either public or private IP address ranges.
- The IP range only exists within the virtual network and isn't internet routable.
- You can divide that IP address space into subnets and allocate part of the defined address space to each named subnet.
- For name resolution, you can use the name resolution service built into Azure.
- You also can configure the virtual network to use either an internal or an external DNS server.

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 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:-

Azure virtual networks enable you to link resources together in your on-premises environment and within your Azure subscription.

In effect, you can create a network that spans both your local and cloud environments. There are three mechanisms for you to achieve this connectivity:

- **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

By default, 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.
- This feature 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 virtual private networks

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to

prevent eavesdropping or other attacks. VPNs can enable networks to safely and securely share sensitive information.

VPN gateways

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

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

All data transfer is encrypted inside a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network. However, you can use one gateway to connect to multiple locations, which includes other virtual networks or on-premises datacenters.

When setting up a VPN gateway, you must specify the type of VPN - either policy-based or route-based. The primary distinction between these two types is how they determine which traffic needs encryption. In Azure, regardless of the VPN type, the method of authentication employed is a preshared key.

- **Policy-based VPN gateways** specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP

addresses to choose the tunnel where that packet is going to be sent through.

- **Route-based gateways** IPSec (Internet Protocol Security) tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.

Use a route-based VPN gateway if you need any of the following types of connectivity:

- Connections between virtual networks
- Point-to-site connections
- Multisite connections
- Coexistence with an Azure ExpressRoute gateway

High-availability scenarios

If you're configuring a VPN to keep your information safe, you also want to be sure that it's a highly available and fault tolerant VPN configuration. There are a few ways to maximize the resiliency of your VPN gateway.

1. Active/standby

- By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure.

- When planned maintenance or unplanned disruption affects the active instance, the standby instance automatically assumes responsibility for connections without any user intervention.
- Connections are interrupted during this failover, but they typically restore within a few seconds for planned maintenance and within 90 seconds for unplanned disruptions.

2. Active/active

- With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an active/active configuration.
- In this configuration, you assign a unique public IP address to each instance.
- You then create separate tunnels from the on-premises device to each IP address.
- You can extend the high availability by deploying an additional VPN device on-premises.

3. Express Route failover

- Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections.
- ExpressRoute circuits have resiliency built in. However, they aren't immune to physical problems that affect the cables delivering connectivity or outages that affect the complete ExpressRoute location.
- In high-availability scenarios, where there's risk associated with an outage of an ExpressRoute circuit, you can also provision a VPN gateway that uses the internet as an alternative method of connectivity. In this way, you can ensure there's always a connection to the virtual networks.

4. Zone-redundant gateways

- In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration.
- This configuration brings resiliency, scalability, and higher availability to virtual network gateways.
- Deploying gateways in Azure availability zones physically and logically separates gateways within a region while protecting your on-premises network connectivity to Azure from zone-level failures.
- These gateways require different gateway stock keeping units (SKUs) and use Standard public IP addresses instead of Basic public IP addresses.

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.

This connection is called an ExpressRoute Circuit.

With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

This feature allows you to connect offices, data centers, or other facilities to the Microsoft cloud.

Each location would have its own ExpressRoute circuit.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility.

ExpressRoute connections don't go over the public Internet.

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

Features and benefits of ExpressRoute

There are several benefits to using ExpressRoute as the connection service between Azure and on-premises networks.

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

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 enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, say you had an office in Asia and a datacenter in Europe, both with ExpressRoute circuits connecting them to the Microsoft network. You could use ExpressRoute Global Reach to connect those two facilities, allowing them to communicate without transferring data over the public internet.

Dynamic routing

ExpressRoute uses the BGP. 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.

Built-in redundancy

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

ExpressRoute connectivity models

ExpressRoute supports four models that you can use to connect your on-premises network to the Microsoft cloud:

- CloudExchange colocation
- Point-to-point Ethernet connection
- Any-to-any connection
- Directly from ExpressRoute sites

1. Colocation at a cloud exchange

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

2. 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.

3. Any-to-any networks

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

4. Directly from ExpressRoute sites

You can connect directly into 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, reducing the 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 requests 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

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

- Reliability and performance

- Security
- Ease of 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 the closest available DNS server answers each DNS query, providing fast performance and high availability for your domain.

Security

Azure DNS is based on Azure Resource Manager, which provides features such as:

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

Ease of use

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

Because Azure DNS is running on Azure, it means you can manage your domains and records with the Azure portal, Azure PowerShell cmdlets, and the cross-platform Azure CLI. Applications that require automated DNS management can integrate with the service by using the REST API and SDKs.

Customizable virtual networks with private domains

Azure DNS also supports private DNS domains. This feature allows you to use your own custom domain names in your private virtual networks, rather than being stuck with the Azure-provided names.

Alias records

Azure DNS also supports alias record sets. You can use an alias record set to refer to an Azure resource, such as an Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network (CDN) endpoint. If the IP address of the underlying resource changes, the alias record set seamlessly updates itself during DNS resolution. The alias record set points to the service instance, and the service instance is associated with an IP address.