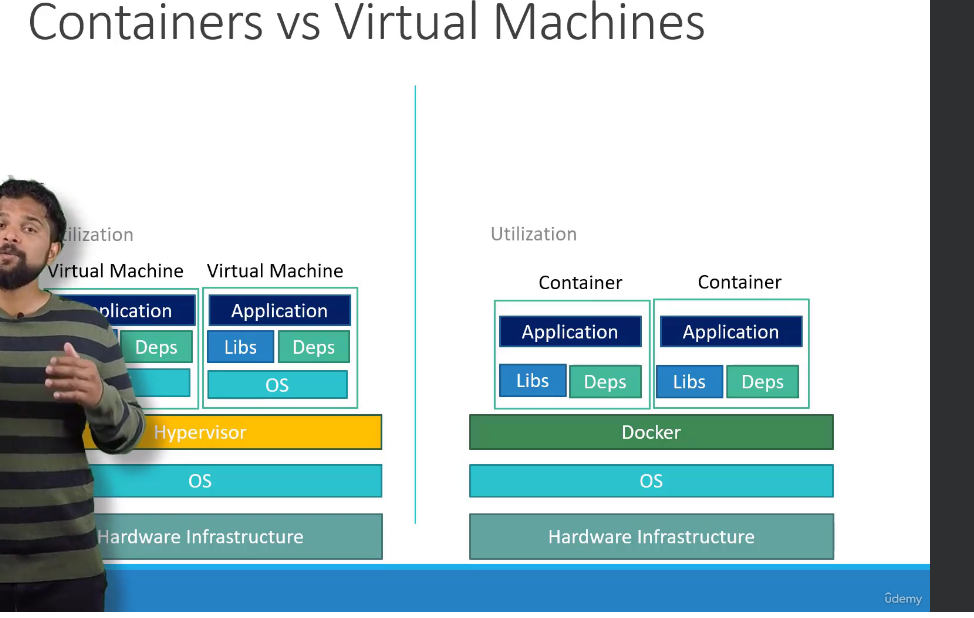
Docker

Containers are completely isolated environments, having there own processes/services, networking, memory(mounts).



Docker container are running instances of docker images

Docker registry

Container Orchestration – Automatically creating and managing containers

1. HA
2. Load balanced application
3. YAML based syntax

K8s Architecture

Node: Physical machine or VM on which k8s is installed , it is also called worker node.

Cluster : A set of nodes, if a node fails your application will still be available from other nodes

Master : It is another node with k8s installed on it, It is responsible for managing the cluster

1. It has information about members of the cluster stored
2. How nodes are monitored?
3. When a node fails how do you move the workload of the field to another worker node

Master node actual does the orchestration of the worker node.

K8s Components

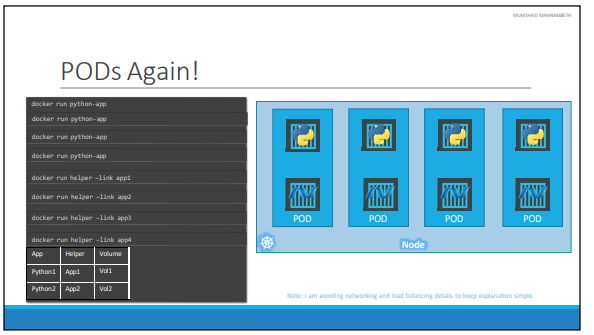
1. K8s API server – Act as frontend for k8s, all the users, CLI, managements devices connect to k8s.
2. Etcd service – Distributed key value store to store all data used to manage the cluster.
3. Kubelet service – Agent running on each node of the cluster.
4. Container run time – IT is used to run containers.
5. Controllers – Brain . The notice and respond when nodes goes down and bring up new containers.
6. Schedulers – Responsible for distributing tasks across multiple nodes.

A screenshot of a computer

Description automatically generated

Kubectl: Kube Command line tool

Kubectl tool is used to deploy and manage applications on a k8s cluster.



PODS: Single instance of an application, smallest object you can create in a k8s.

POD is 1:1 relationship with a container.

**Kubectl run nginx: Create a pod and deploys an instance of nginx docker image**

**Kubectl describe pod nginx**: Detailed information about the nginx pod.

Kubectl get pods -o wide: Details view of the running pods

**YAML:**

Key Value Pair

Fruit: Apple

Vegetable: Peas

Liquid: Water

Meat: Chicken

Array/Lists:

Fruits:

* Orange
* Apple
* Banana

Dictionary / Map

Banana:

Calories: 105

Fat: 0.4

Carbs: 27g

PODS Definition YAML components:

1. apiVersion: Version of k8s API used to create the k8s objects (v1, apps/v1)
2. Kind: Type of object we are trying to create (Pod, Deployment, Service, Replica set etc.)
3. Metadata: It has name and labels
4. Spec:

Replication Controllers: It help us to run multiple instances of pod in k8s cluster, thus providing HA.

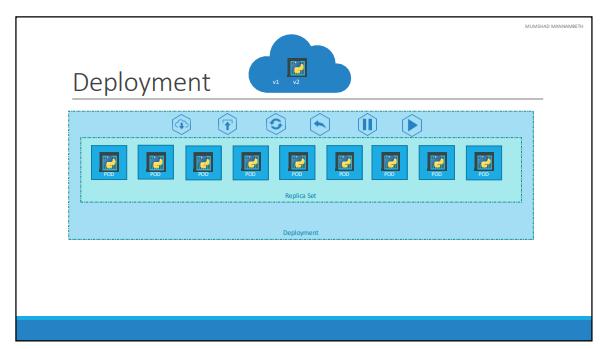
1. Load balancing – Across same and multiple nodes as well.
2. Scaling

Replication Controller: Old technology replaced by Replica set.

Selector key is available in replica set but not in replication controller.

**Replica set uses selector label to monitor the pods with matching label in the k8s Cluster**

Deployments : Rolling updates and rollbacks for the underlying pods, pausing and resuming changes.



When we first create a deployment, it triggers a rollout, a new rollout creates a new deployment revision

**Recreate Strategy:**  It will delete all the pods and then create the pods which application downtime



**Rolling Update: Default deployment strategy**

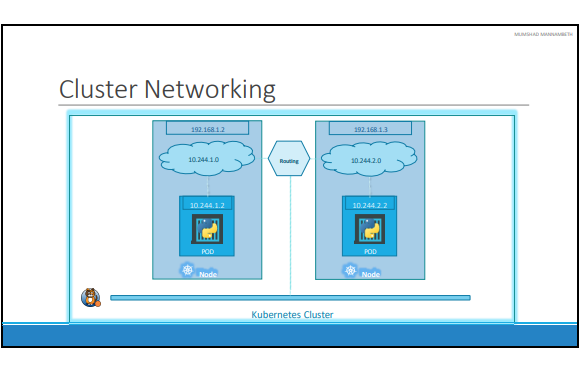
Recreate and Rolling Update logs has different messages

--record=true used to record the deployment history in kubectl rollout history command

IP address is assigned to POD rather than Docker container

All containers/PODS can communicate to one another without NAT.

All nodes can communicate with all containers and vice-versa without NAT.



K8s services enable communication between various components within and outside of the application. Services help us to achieve loosing coupling in microservices.

A computer screen shot of a diagram

Description automatically generated

Usecase of K8 Service:

1. To listen to a port on the node and forward requests on that port to a port on the port running the web application.
2. Above service is called Node Port Service.

* Node Port – Where the service make an internal port accessible on a port on the node.
* ClusterIP – The service creates a virtual IP inside the cluster to enable communication between different services such as frontend and backend servers.
* LoadBalancer – IT would distribute the load across the different web servers in your frontend.

A screenshot of a computer

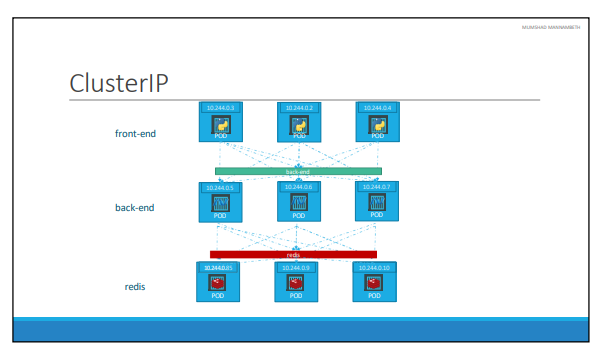
Description automatically generated

Nodeport range – 30000 to 32767

Nodeport – 30008

**IP address of PODS are dynamic in nature because pods can be deleted and created at any point of time**

**Cluster IP:**

****

[gagandeepp/example-voting-app-kubernetes (github.com)](https://github.com/gagandeepp/example-voting-app-kubernetes)

Config Maps: They are used to pass configuration data in the form of key value pairs in k8s.

1. Create Config Map
2. Inject into Pod

Secrets: Used to store the password and keys in k8s

1. Create Secret
2. Inject Secret

Objects store in secrets and etcd are just base64 encoded.

Service Accounts: Used by machines

1GB : 1000 MB

1GiB: 1024 MiB

1MiB: 1024 KiB

1KiB: 1024 bytes

Taint: To avoid placing all the pods on a node , we taint a node.

Toleration: The pod which can be scheduled on a node using k8s scheduler.

Taints are done on Node

Toleration are set on Pods.

Taint levels:

1. NoSchedule : Pods are Either nodes are not scheduled or evicted from existing nodes.
2. PreferNoSchedule
3. NoExecute

**Pods are not scheduled on Master node because Master node has No Schedule taint set on it.**

Node Selector: The mechanism by which we can schedule a pod on a particular node.

Node Affinity: We cannot provide advance expressions like or not with node selectors, to cater those we have node affinity.

Multicontainer Pods in K8s:

1. Adapter: Adapter container process logs from different pods in a common format
2. Sidecar: Deploying logging agent alongside a web server
3. Ambassador: Outsourcing proxy logic to separate container.

For example a process that pulls a code or binary from a repository that will be used by the main web application. That is a task that will be run only one time when the pod is first created. Or a process that waits for an external service or database to be up before the actual application starts. That's where **initContainers**comes in.

An **initContainer**is configured in a pod like all other containers, except that it is specified inside a initContainers section

PODS Lifecycle:

1. Pending
2. Running
3. Succeeded.
4. Failed.
5. Unknown.

PODS Conditions:

1. PodScheduled -When Pod is scheduled on a node.
2. Initialized – When Pod is initialized.
3. ContainerReady – When multiple containers of the Pod are ready
4. Ready –

Readiness Probe – When pod is up and running and ready to serve the traffic. If the readiness probe condition is met on the pod then only k8s will set the POD condition to Ready and sends the traffic to the POD otherwise it will not send the request to POD.

httpGet : For web app

tcpSocket: For DB connection

exec: To run some script

Liveness Probe: A liveness probe is used to periodically test check the application container is healthy or not. If the

Monitoring K8s Cluster: DataDog, Promethus, Metrics Server

Kubelet – Running on pod and it has component cAdvisor (Container Advisor) which send the

Performance metrics from pods and exposing them through Kubelet API to make the metrics available to metrics server.

Labels and Selectors are used to group things together.

Labels are like properties attached to k8s resources

Selectors are like filters which is used to filter the k8s resources.

Annotations: Are used to record build information, contact details etc.

Pod restartPolicy is set to Always by default.

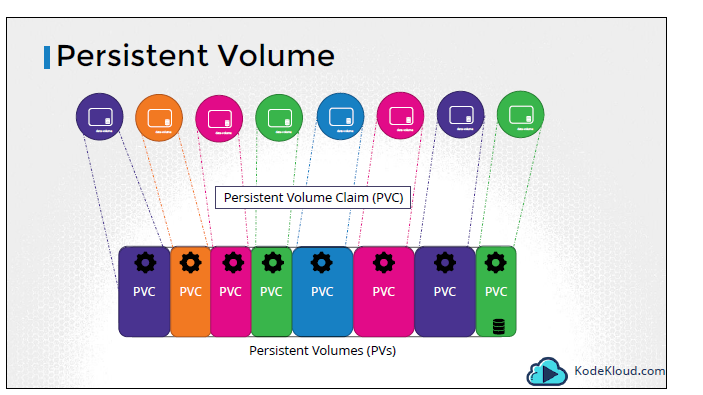
Jobs are recreated one after the another only when previous Job is success.

Volumes: To persist data of a container we attach volume to the container.

A screenshot of a computer

Description automatically generated

Persistent Volume: It is a cluster wide pool of storage volumes configured by an administrator to be used by users deploying applications on the cluster.



Persistent Volume Claims: Administrator create PV , user create PVC to use the storage.

Every PVC is bounded to single PV.

Static Provisioning: Manually provision on Cloud and then using the storage in PV.

Storage Class: We can automatically provision storage on GCP. Storage class will create PV for us in the backend.

Stateful Set: Pods are created in sequential order.They maintain sticky identity throughout their lifecycle. Ex: {pod\_name}-0

PodmanagementPolicy: Parallel to avoid sequential pod creation

Headless Service: It is a service without IP address and doesn’t do load balancing. IT create dns entries for each pod name and subdomain.

It is a normal service file with ClusterIP set to None.

Authentication and Authorization in K8s

Kube-apiserver: Controlling access to api server

Authentication: User ID and passwords/token stored in files, certificates , LDAP/Keberos, Service accounts

Define username,password and userid in CSV file and pass it to kubeapiserver with flag –basic-auth-file and restart the kubeapiserver

KubeConfig file: It will have server url, certificates and keys to connect to k8s cluster

Available in $HOME/.kube/config

It has 3 sections

1. Clusters: Dev, Prod, Testing Environment
2. Contexts: Which user account is used to access which cluster
3. Users: User accounts (Admin, Dev user etc)

API Groups: /metrics, /healthz, /version, /api, /apis, /logs

Core: /api

Named: /apis

Kubectl proxy: IT launches a proxy service on port 8001 and use credentials from kubeconfig file to access the cluster.

Authorization: RBAC, ABAC

Node Authorizer

ABAC: Attribute based Access control is defined by Policy in json format and we associate a user with set of permissions

{“kind”: “Policy”, “spec”: {“user”: “dev-user”, “namespace”: “\*”, “resource”: “pods”, “apiGroup”: “\*”}}

RBAC: Role based access control we associate a role with set of permissions.

Open Policy Agent: 3rd party tool that Helps with admission control and authorization.

Default mode is Always allow.

Resources in K8s are namespaced or cluster scoped.

Admission controllers are used to add restrictions like:

* Use docker image from internal repository
* Do not run docker container as admin
* Do not use latest tag on docker images

Examples of admission controllers:

1. AlwaysPullImages
2. DefaultStorageClass
3. EventRateLimit
4. NamespaceAutoProvision (Deprecated)- NamespaceLifecycle is new controller
5. NamespaceExists(Deprecated)- NamespaeLifecycle is new controller

Custom Resource Definitions (CRD): Used to define the custom kind value

Operator: Package Custom Resource and Custom controller as an extension so that it can be reused.

**. What is Kubernetes and why is it important for developers?**

* **Answer**: Kubernetes (K8s) is an open-source platform for automating the deployment, scaling, and management of containerized applications. It is important for developers because it abstracts away the complexity of managing containerized applications and provides features like automated scaling, load balancing, service discovery, and fault tolerance. Developers can focus more on writing code while Kubernetes handles deployment and operational concerns.

**2. What is a pod in Kubernetes?**

* **Answer**: A **pod** is the smallest and simplest Kubernetes object. A pod represents a single instance of a running process in a cluster and can host one or more containers that share the same network, storage, and namespace. Containers within the same pod can communicate with each other via localhost and can also share volumes.

**3. What is the difference between a Deployment and a StatefulSet in Kubernetes?**

* **Answer**:
  + **Deployment**: Manages stateless applications. It ensures that a specified number of identical pods are running at all times. Deployments support rolling updates and easy scaling.
  + **StatefulSet**: Manages stateful applications where each pod has a unique identity (e.g., database clusters). It ensures that pods are given a stable hostname, persistent storage, and ordered deployment/termination.

**4. What is a Service in Kubernetes and what types of Services are there?**

* **Answer**: A **Service** in Kubernetes is an abstraction that defines a logical set of pods and a policy by which to access them. Services provide stable network endpoints for accessing applications. The main types of services are:
  + **ClusterIP**: Default type, exposes the service on an internal IP address within the cluster.
  + **NodePort**: Exposes the service on a static port on each node's IP address, accessible outside the cluster.
  + **LoadBalancer**: Exposes the service externally via a cloud provider's load balancer (e.g., AWS, GCP).
  + **ExternalName**: Maps the service to an external DNS name.

**5. What is a ConfigMap and how is it used in Kubernetes?**

* **Answer**: A **ConfigMap** is a Kubernetes object used to store non-sensitive configuration data in key-value pairs. It can be used to configure application settings, environment variables, or command-line arguments. ConfigMaps allow you to separate configuration from code, making your application more flexible and portable.

**6. What is a Secret in Kubernetes?**

* **Answer**: A **Secret** is a Kubernetes object that stores sensitive data, such as passwords, OAuth tokens, or SSH keys. Secrets are stored in an encoded format, and Kubernetes ensures that sensitive data is only accessible to authorized users and pods.

**7. How do you scale applications in Kubernetes?**

* **Answer**: Scaling applications in Kubernetes is done by increasing or decreasing the number of pod replicas managed by a **Deployment** or **StatefulSet**. You can scale manually with the kubectl scale command:

bash

Copy code

kubectl scale deployment my-app --replicas=3

Kubernetes can also automatically scale pods using the **Horizontal Pod Autoscaler** (HPA), which adjusts the number of pods based on CPU utilization or other custom metrics.

**8. What is the purpose of a Kubernetes namespace?**

* **Answer**: A **namespace** in Kubernetes is a way to logically divide cluster resources into multiple environments, often used for isolation (e.g., dev, test, prod). Namespaces allow you to organize and manage resources more effectively, especially in larger clusters where multiple teams or projects are running.

**9. What is Helm in Kubernetes?**

* **Answer**: **Helm** is a package manager for Kubernetes that allows you to define, install, and upgrade Kubernetes applications using **charts** (pre-configured Kubernetes resources). Helm simplifies deployment by providing reusable templates and parameterization, making it easier to deploy complex applications.

**10. Explain Kubernetes Ingress and its use cases.**

* **Answer**: **Ingress** is an API object that manages external access to services within a Kubernetes cluster, typically HTTP/HTTPS. It provides a way to expose multiple services under a single IP address or DNS name. It also supports features like SSL termination, path-based routing, and load balancing. Ingress controllers, such as NGINX or Traefik, are required to manage ingress resources.

**11. How do you manage logs in Kubernetes?**

* **Answer**: Logs from Kubernetes pods can be accessed using kubectl logs:

bash

Copy code

kubectl logs <pod-name>

For centralized log management, developers typically use tools like **Fluentd**, **Elasticsearch**, and **Kibana (EFK)** or **Prometheus** and **Grafana** for monitoring and visualization. Kubernetes does not have a built-in logging solution but can integrate with these tools.

**12. What are Kubernetes Volumes, and how are they different from persistent storage?**

* **Answer**: **Volumes** in Kubernetes are used to store data and make it available to containers within pods. They have a lifecycle that is independent of the pod’s lifecycle, which means data can persist even after a pod is deleted.
  + **Persistent Volumes (PV)**: These are storage resources in the cluster that provide persistent storage to pods. Persistent Volumes are managed independently of pods, and they can be backed by different storage systems (e.g., NFS, cloud storage, etc.).
  + **Persistent Volume Claims (PVC)**: A claim for storage by a pod, allowing the pod to request storage of a specific size and storage class.

**13. How does Kubernetes handle self-healing?**

* **Answer**: Kubernetes automatically monitors the health of your application using **Liveness** and **Readiness** probes.
  + **Liveness probe** checks if the container is still running. If it fails, Kubernetes restarts the container.
  + **Readiness probe** checks if the container is ready to serve traffic. If it fails, Kubernetes will stop routing traffic to that pod until it becomes ready again.
* Kubernetes also ensures that the desired state is maintained, for example, by replacing crashed pods with new ones.

**14. How do you manage Kubernetes deployments across multiple environments (dev, staging, prod)?**

* **Answer**: Kubernetes allows you to define different configurations for various environments by using **namespaces**and **configuration management tools** like **Helm**, **Kustomize**, or **ConfigMaps/Secrets**. For example, different values.yaml files or overlays can be used for each environment, enabling seamless deployments to different clusters.
* Using kubectl contexts and namespaces helps separate configurations for each environment while keeping the deployment consistent.

**15. What is the difference between kubectl apply and kubectl create?**

* **Answer**:
  + **kubectl apply** is used to create or update a resource. It compares the resource configuration with the existing state and applies any changes.
  + **kubectl create** is used only to create a resource. If the resource already exists, it will result in an error.

**16. What are Kubernetes Labels and Annotations?**

* **Answer**:
  + **Labels** are key-value pairs used to organize and select groups of resources, enabling you to filter and categorize objects for scheduling, scaling, and other purposes.
  + **Annotations** are also key-value pairs but are intended to store non-identifying metadata for Kubernetes objects. They can be used for storing information like deployment history or build information.

**17. How do you perform a rolling update in Kubernetes?**

* **Answer**: A **rolling update** in Kubernetes is performed automatically when you update the image of a **Deployment**. Kubernetes ensures zero downtime by gradually replacing old pods with new ones.

bash

Copy code

kubectl set image deployment/my-deployment my-container=my-image:latest

Kubernetes will update the deployment one pod at a time, ensuring that the application remains available during the update.

**18. What is the role of an Ingress Controller in Kubernetes?**

* **Answer**: An **Ingress Controller** is a piece of software that manages the routing of external HTTP and HTTPS traffic to internal services in a Kubernetes cluster. It implements the rules defined in Ingress resources and allows for features like SSL termination, path-based routing, and host-based routing.

**19. What is a DaemonSet in Kubernetes?**

* **Answer**: A **DaemonSet** ensures that a copy of a specific pod is running on every node in the cluster (or on specific nodes). This is useful for services that need to run on all nodes, such as log collectors or monitoring agents.

**20. What is the role of the kubelet in Kubernetes?**

* **Answer**: The **kubelet** is an agent that runs on each node in the Kubernetes cluster. It ensures that containers are running in pods and that the desired state of the node is maintained. The kubelet interacts with the Kubernetes API server to report the node's status and manage the container lifecycle.

Kubernetes consists of several key components that work together to manage and orchestrate containerized applications. These components can be categorized into two main groups: **Control Plane** (Master Node) and **Node Components**(Worker Nodes). Here’s an overview of the major Kubernetes components:

**1. Control Plane (Master Node) Components**

The Control Plane manages the overall cluster and is responsible for making global decisions about the cluster, such as scheduling, scaling, and managing the desired state of the system.

* **API Server (kube-apiserver)**:
  + The API Server is the central point for all communication within the Kubernetes cluster. It exposes the Kubernetes API and acts as a gateway for interacting with the cluster.
  + It receives REST requests, validates them, and then processes them, either directly or by passing them to the relevant components of the system.
  + The API server is responsible for managing the cluster's state by interacting with the etcd database and other components.
* **etcd**:
  + **etcd** is a highly available, consistent key-value store used by Kubernetes to store cluster configuration data and the state of the cluster. It stores all the Kubernetes objects, such as pods, services, and deployments, in the form of key-value pairs.
  + etcd is crucial for maintaining the desired state of the system and ensuring data consistency.
* **Scheduler (kube-scheduler)**:
  + The **kube-scheduler** is responsible for selecting a node for newly created pods. It looks at the available nodes and assigns pods to them based on resource availability, constraints, and other factors like affinity, taints, and tolerations.
  + It is also responsible for scheduling pods in a way that meets the cluster’s resource requirements and limits.
* **Controller Manager (kube-controller-manager)**:
  + The **kube-controller-manager** runs controllers that regulate the state of the cluster. Controllers are responsible for maintaining the desired state of objects in the cluster, such as ensuring that the number of replicas for a deployment matches the desired number or managing the lifecycle of pods and nodes.
  + Some examples of controllers include the **Replication Controller**, **Deployment Controller**, **Node Controller**, and **Job Controller**.
* **Cloud Controller Manager (cloud-controller-manager)**:
  + The **cloud-controller-manager** is used when running Kubernetes on cloud providers. It interacts with the cloud provider's APIs to manage cloud-specific resources (e.g., load balancers, volumes, network interfaces).
  + It allows the Kubernetes cluster to integrate with cloud-specific components like cloud load balancers or storage volumes.

**2. Node Components (Worker Node)**

These components run on each worker node in the Kubernetes cluster. They are responsible for running the actual workloads (pods) and communicating with the control plane.

* **kubelet**:
  + The **kubelet** is an agent that runs on each node and ensures that containers are running in pods. It registers the node with the API server and ensures that the containers on the node are running as per the desired state specified in the cluster.
  + It also monitors the health of the containers and reports status back to the API server.
* **kube-proxy**:
  + The **kube-proxy** runs on each node and maintains network rules that allow communication between pods. It is responsible for load balancing and proxying network traffic to the appropriate pod, based on the Kubernetes Service definitions.
  + It can operate in different modes: **userspace proxy**, **iptables proxy**, or **IPVS proxy**, depending on the configuration and environment.
* **Container Runtime**:
  + The **container runtime** is responsible for running the containers on the node. Kubernetes supports multiple container runtimes, including Docker, containerd, and CRI-O.
  + It pulls container images from container registries and runs the containers inside pods.
* **Pod**:
  + A **pod** is the smallest and simplest Kubernetes object. It represents a single instance of a running process in the cluster. Pods can contain one or more containers that share the same network, storage, and namespace.

**3. Optional/Additional Components**

These components are optional or may exist as part of your Kubernetes deployment depending on your use case or architecture.

* **Ingress Controller**:
  + An **Ingress Controller** is a component that manages access to services in the cluster, typically HTTP and HTTPS traffic. It provides features like load balancing, SSL termination, and routing of external traffic to internal services based on rules defined in **Ingress** resources.
* **Metrics Server**:
  + The **metrics server** is responsible for collecting resource usage metrics (CPU, memory, etc.) from nodes and pods. These metrics are used for autoscaling purposes, such as **Horizontal Pod Autoscaling (HPA)** and **Vertical Pod Autoscaling (VPA)**.
* **CNI (Container Network Interface)**:
  + CNI is a plugin that provides network connectivity to containers within a pod. Kubernetes does not define how containers are connected to the network, but uses CNI plugins to implement networking. Popular CNI plugins include **Flannel**, **Calico**, and **Weave**.

The **Kubernetes lifecycle** refers to the stages that Kubernetes objects (such as Pods, Deployments, and Services) go through from their creation to termination. Kubernetes is a highly dynamic system, and resources are continually created, updated, and terminated as part of the overall lifecycle management.

Below is an overview of the **Kubernetes lifecycle** with a focus on key resources like Pods, Nodes, and Deployments.

**1. Pod Lifecycle**

A **Pod** is the smallest and most basic deployable unit in Kubernetes. A Pod encapsulates one or more containers and the resources that they need to run. The Pod lifecycle describes the stages a Pod goes through from creation to termination.

**Key Phases of a Pod Lifecycle:**

1. **Pending**: The Pod has been accepted by the Kubernetes system, but one or more containers have not been started. This can occur if the Pod is waiting for resources (e.g., CPU, memory) to become available.
2. **Running**: The Pod has been assigned to a node, and at least one container within the Pod is running.
3. **Succeeded**: All containers in the Pod have terminated successfully with an exit code of 0. Once the Pod enters this state, it is finished running.
4. **Failed**: All containers in the Pod have terminated, but at least one container exited with a non-zero exit code, indicating failure.
5. **Unknown**: The state of the Pod cannot be determined, usually due to an issue with the node hosting the Pod (e.g., node is unreachable).

**Pod Lifecycle Management:**

* **Pod Creation**: Pods are created via YAML configuration files or using kubectl run or other controllers like Deployments, StatefulSets, etc.
* **Pod Termination**: Pods are terminated when they are no longer needed, either due to a manual deletion or due to a rolling update (e.g., in Deployments).
* **Pod Deletion**: Kubernetes allows graceful deletion of Pods, which involves stopping containers and cleaning up resources. If the terminationGracePeriodSeconds is set, Kubernetes waits that many seconds before forcefully terminating the Pod.

**2. Node Lifecycle**

A **Node** in Kubernetes represents a worker machine in the cluster. It could be either a physical or virtual machine.

**Key Phases of a Node Lifecycle:**

1. **Ready**: The node is functioning properly, has sufficient resources, and can accept Pods.
2. **NotReady**: The node is not functioning properly. This can be due to resource exhaustion, network failure, or a system error.
3. **Unknown**: The status of the node is unknown, typically when the Kubernetes control plane cannot reach the node.

* **Node Registration**: Nodes register themselves with the Kubernetes control plane when they start up.
* **Node Maintenance**: Nodes can be drained or cordoned for maintenance, which means no new Pods are scheduled on them, and existing Pods are moved to other nodes.
* **Node Deletion**: Nodes can be removed from the cluster if they are no longer needed or are permanently down.

**3. Deployment Lifecycle**

A **Deployment** manages the lifecycle of Pods and ReplicaSets. It ensures that the desired number of replicas of a Pod are running at all times.

**Key Phases of a Deployment Lifecycle:**

1. **Scaling**: A Deployment can be scaled up (increasing the number of replicas) or scaled down (decreasing the number of replicas). Kubernetes will automatically create or delete Pods as needed.
2. **Rolling Update**: When you update a Deployment (e.g., changing the container image or environment variables), Kubernetes performs a rolling update. It gradually replaces old Pods with new ones to minimize downtime.
3. **Rollback**: If a new deployment causes issues, you can roll back to the previous version using the kubectl rollout undo command.
4. **Paused Deployment**: A Deployment can be paused temporarily, which prevents it from making further changes to Pods (useful during troubleshooting).
5. **Progressing**: A Deployment enters the "Progressing" state when it is updating or scaling.

**4. Service Lifecycle**

A **Service** in Kubernetes provides a stable endpoint for accessing a set of Pods. Services can be of various types like ClusterIP, NodePort, LoadBalancer, and ExternalName.

**Key Phases of a Service Lifecycle:**

1. **Creation**: A Service is created with specific selectors to match Pods based on labels.
2. **Binding**: The Service is associated with the Pods it targets (using label selectors).
3. **Accessing**: Once the Service is created and bound to Pods, users and other services can access the application using the Service's IP and port.
4. **Deletion**: When the Service is no longer needed, it is deleted, and the associated resources (like ClusterIP or load balancer) are cleaned up.

**5. StatefulSet Lifecycle**

A **StatefulSet** is a Kubernetes controller that manages stateful applications. Unlike Deployments, StatefulSets provide guarantees about the ordering and uniqueness of Pods.

**Key Phases of a StatefulSet Lifecycle:**

1. **Pod Creation**: StatefulSet ensures that Pods are created in a specific order and are given stable, unique network identities.
2. **Scaling**: StatefulSets allow you to scale the number of replicas, and it ensures that Pods are added or removed in a controlled manner.
3. **Pod Termination**: Pods in a StatefulSet are terminated in reverse order, ensuring that their resources are freed up in the right sequence.
4. **Rolling Update**: StatefulSets support rolling updates, where Pods are updated one by one to ensure the application remains available during the update.

**6. ReplicaSet Lifecycle**

A **ReplicaSet** is a Kubernetes controller responsible for maintaining a stable set of replica Pods running at any given time. It is often managed indirectly by a Deployment.

**Key Phases of a ReplicaSet Lifecycle:**

1. **Pod Creation**: A ReplicaSet creates and ensures the desired number of Pods are running.
2. **Scaling**: ReplicaSets allow you to scale up or down the number of Pods based on the specified replica count.
3. **Pod Deletion**: If the ReplicaSet is scaled down, Pods are terminated to match the desired replica count.
4. **Rolling Update**: When associated with a Deployment, ReplicaSets can be updated automatically during a rolling update.

**7. Resource Lifecycle (ConfigMaps, Secrets, Volumes, etc.)**

Other resources like **ConfigMaps**, **Secrets**, and **Volumes** also have their lifecycles in Kubernetes. These resources are typically created and used by Pods to provide configuration data, secrets, or persistent storage.

1. **Creation**: Resources are created via YAML files or kubectl commands.
2. **Binding**: These resources are bound to Pods (for example, ConfigMaps or Secrets are mounted as environment variables or volumes).
3. **Deletion**: Once they are no longer needed, these resources can be deleted either manually or automatically (through resource deletion policies).

**8. Job and CronJob Lifecycle**

A **Job** runs a batch task to completion, while a **CronJob** runs a task at scheduled intervals.

**Key Phases of a Job Lifecycle:**

1. **Creation**: Jobs are created to run specific tasks until completion.
2. **Completion**: A Job completes successfully when the specified number of Pods successfully terminate.
3. **Failure**: If the Pod fails, the Job will retry based on the specified backoff policy.
4. **Deletion**: Jobs can be deleted once completed or when no longer needed.

**Key Phases of a CronJob Lifecycle:**

1. **Scheduled**: CronJobs are created and scheduled to run at specified times.
2. **Execution**: CronJobs execute their task at the specified intervals.
3. **Completion/Failure**: As with Jobs, a CronJob's tasks will complete successfully or fail.
4. **Deletion**: CronJobs can be deleted after the task schedule or once no longer required.

**Kubernetes Object Lifecycle Summary:**

1. **Creation**: The object is created using YAML files or kubectl commands.
2. **Configuration**: The object is configured with parameters like replicas, resource limits, selectors, etc.
3. **Deployment**: The object is deployed into the Kubernetes cluster, where the control plane ensures that it is operating as expected.
4. **Scaling**: Objects can be scaled up or down based on the resource needs.
5. **Updating**: Changes (e.g., container image, resource limits) can be made to the object via updates or rolling updates.
6. **Termination**: When no longer needed, objects are deleted from the cluster, freeing up resources.

Here’s an overview of the **different kinds** in Kubernetes:

**1. Workloads (App-related Resources)**

Workloads are the primary way to run applications on Kubernetes. They define how to run your containerized applications and manage their lifecycle.

* **Pod**:
  + The smallest and simplest unit in Kubernetes, a pod is a group of one or more containers that share storage, network resources, and run in a shared context. Pods are typically the smallest unit that you deploy and scale in Kubernetes.
* **Deployment**:
  + A **Deployment** manages a set of replicas of pods, ensuring that the correct number of pods are running at any given time. Deployments are often used for stateless applications. They support rolling updates, rollbacks, and scaling.
* **StatefulSet**:
  + A **StatefulSet** is used for managing stateful applications, where each pod has a unique identity and stable storage. It ensures that pods are created, updated, and deleted in a predictable order, and it guarantees stable network identity and persistent storage.
* **DaemonSet**:
  + A **DaemonSet** ensures that a copy of a pod is running on all (or a subset of) nodes in the cluster. It’s often used for running background services, like logging agents or monitoring tools, that need to run on every node.
* **ReplicaSet**:
  + A **ReplicaSet** ensures that a specified number of identical pods are running at all times. It’s commonly used by Deployments to maintain the desired number of replicas. A ReplicaSet can independently manage pods but is typically controlled by a Deployment.
* **Job**:
  + A **Job** creates one or more pods and ensures that they successfully complete. Jobs are used for running batch or one-off tasks that don’t need to persist for the lifetime of the application.
* **CronJob**:
  + A **CronJob** is similar to a **Job**, but it runs on a scheduled basis, similar to cron jobs in UNIX/Linux systems. CronJobs are used for periodic tasks, like backups or sending reports.

**2. Networking Resources**

Networking resources define how different parts of the Kubernetes cluster communicate with each other and with the external world.

* **Service**:
  + A **Service** defines a logical set of pods and provides a stable IP address and DNS name to access those pods. Services abstract the network details of the pods and provide a consistent way for other components to communicate with them. Types of services include:
    - **ClusterIP** (default): Exposes the service on an internal IP within the cluster.
    - **NodePort**: Exposes the service on a static port on each node's IP address.
    - **LoadBalancer**: Exposes the service externally through a cloud provider’s load balancer.
    - **ExternalName**: Maps the service to an external DNS name.
* **Ingress**:
  + **Ingress** is a set of rules that define how external HTTP/HTTPS traffic should be routed to services within the cluster. It can also handle SSL termination, host-based routing, and path-based routing.
* **NetworkPolicy**:
  + **NetworkPolicy** allows you to control the traffic between pods and external systems. It defines rules about which pods can communicate with which other pods or services in the cluster.

**3. Storage Resources**

Storage resources are used to manage persistent storage for your containers and workloads.

* **PersistentVolume (PV)**:
  + A **PersistentVolume** is a piece of storage in the cluster, provisioned by an administrator or dynamically provisioned. PVs represent actual physical storage resources like NFS, cloud storage, or block storage devices.
* **PersistentVolumeClaim (PVC)**:
  + A **PersistentVolumeClaim** is a request for storage by a user. It specifies the size and access modes (e.g., ReadWriteOnce, ReadOnlyMany) for the storage. A PVC is bound to a PV that satisfies the request.
* **StorageClass**:
  + A **StorageClass** is used to define the properties of storage resources available in the cluster, such as the type of storage (SSD, HDD, etc.), performance characteristics, and how storage is provisioned (dynamically or manually).
* **EmptyDir**:
  + An **EmptyDir** is a temporary storage volume that is created when a pod is assigned to a node. It exists as long as the pod exists, and is erased when the pod is deleted.

**4. Configuration Resources**

Configuration resources allow you to store and manage configuration data and secrets within the cluster.

* **ConfigMap**:
  + A **ConfigMap** is used to store non-sensitive configuration data in key-value pairs. It allows you to separate configuration from application code, making applications more flexible and portable.
* **Secret**:
  + A **Secret** is similar to a ConfigMap but is used to store sensitive data, such as passwords, tokens, or SSH keys. Secrets are stored in an encoded format and can be mounted as files or environment variables in pods.
* **SecretManager** (if integrated with cloud providers like GCP or AWS):
  + Some cloud providers integrate their Secret Management tools, like AWS Secrets Manager or GCP Secret Manager, with Kubernetes, allowing you to securely store and access sensitive information from within the cluster.

**5. Access Control Resources**

These resources are used to define who can access which resources and actions in the Kubernetes cluster.

* **Role**:
  + A **Role** defines a set of permissions within a specific namespace. It grants access to resources like pods, services, secrets, etc. It specifies what actions can be performed (e.g., get, list, create, update).
* **ClusterRole**:
  + A **ClusterRole** is similar to a Role, but it grants permissions across the entire cluster rather than within a single namespace.
* **RoleBinding**:
  + A **RoleBinding** grants the permissions defined in a **Role** to a user or a set of users within a specific namespace.
* **ClusterRoleBinding**:
  + A **ClusterRoleBinding** grants the permissions defined in a **ClusterRole** to users across the entire cluster, not limited to a specific namespace.

**6. Monitoring and Logging Resources**

These resources are important for observability, tracking the performance of the system, and troubleshooting.

* **PodDisruptionBudget (PDB)**:
  + A **PodDisruptionBudget** ensures that a minimum number of pods are running during voluntary disruptions like node maintenance or upgrades. It helps maintain the availability of your application during disruptions.
* **HorizontalPodAutoscaler (HPA)**:
  + The **HorizontalPodAutoscaler** automatically adjusts the number of pod replicas in a deployment based on resource utilization (CPU, memory) or custom metrics.
* **VerticalPodAutoscaler (VPA)**:
  + The **VerticalPodAutoscaler** automatically adjusts the resource requests and limits (CPU, memory) for individual pods based on usage.
* **Metrics Server**:
  + The **Metrics Server** collects resource usage metrics (CPU, memory) from nodes and pods. These metrics are used by the HPA and other controllers to make scaling decisions.
* **Prometheus and Grafana**:
  + **Prometheus** is an open-source monitoring system used to collect metrics from Kubernetes components, while **Grafana** is a visualization tool that allows you to create dashboards for visualizing those metrics.

**7. Cluster and Node Management**

These resources help with managing nodes, clusters, and the overall health of the system.

* **Node**:
  + A **Node** is a physical or virtual machine in the Kubernetes cluster. It runs the **kubelet** and the container runtime, allowing it to run pods.
* **Namespace**:
  + A **Namespace** is a way to divide cluster resources into multiple logical groups. It is commonly used to separate environments (e.g., dev, test, prod) or teams within a cluster.
* **Taint** and **Toleration**:
  + **Taints** are applied to nodes, preventing pods from being scheduled on them unless they have a matching **toleration**. This mechanism is used to control which pods can run on which nodes.
* **ResourceQuota**:
  + A **ResourceQuota** allows administrators to limit the amount of resources (e.g., CPU, memory, storage) that can be consumed in a particular namespace.

**How These Resources Work Together**

* When a user or application needs persistent storage, a **PersistentVolumeClaim (PVC)** is created. The PVC specifies the amount of storage, the access modes, and optionally the **StorageClass**.
* If a matching **PersistentVolume (PV)** is available (either statically provisioned or dynamically created via the StorageClass), Kubernetes will bind the PVC to the PV.
* If no matching PV is available, Kubernetes will use the **StorageClass** to provision a new PV dynamically and bind it to the PVC.
* Once bound, the storage is available for the pod, and it will persist even if the pod is deleted, ensuring that the data remains intact.

**Summary of Key Concepts**

* **PersistentVolume (PV)**: Represents the actual storage resource, which is either manually or dynamically provisioned.
* **PersistentVolumeClaim (PVC)**: A request for storage by a user, specifying required storage size, access modes, and optionally a StorageClass.
* **StorageClass**: A way to define and manage different types of storage (e.g., SSD, HDD) and specify how storage should be provisioned in Kubernetes, supporting dynamic provisioning.

**Comparison of Service Types**

| **Service Type** | **Internal Access** | **External Access** | **Load Balancer** | **Use Case** |
| --- | --- | --- | --- | --- |
| **ClusterIP** | Yes | No | No | Internal communication between pods |
| **NodePort** | Yes | Yes | No | Exposes service on a port on each node’s IP |
| **LoadBalancer** | Yes | Yes | Yes | Exposes service externally via a cloud load balancer |
| **ExternalName** | Yes | Yes (DNS name) | No | Maps to external DNS name for external service discovery |

**When to Use Each Service Type**

* **ClusterIP**: Use when the service only needs to be accessed internally within the Kubernetes cluster, like communication between pods.
* **NodePort**: Use when you need to expose the service externally but don’t have or need an external load balancer. This is mostly used in development or testing environments.
* **LoadBalancer**: Use when you're in a cloud environment (like AWS, GCP, or Azure) and want to expose the service externally with a cloud-managed load balancer.
* **ExternalName**: Use when you want to reference an external service by DNS name without creating a load balancer or proxying traffic through Kubernetes.

Kubernetes clusters have 4 system namespaces.

default - the default namespace used when no other namespace is specified

kube-node-lease - manages the lease objects associated with the heartbeats of each of the cluster's nodes

kube-public - to be used for resources that may need to be visible or readable by all users throughout the whole cluster

kube-system - used for components created by the Kubernetes system

RoleDescription

**Kubernetes Engine Admin**

Provides access to full management of clusters and their Kubernetes API objects. A user with this role will be able to create, edit and delete any resource in **any** cluster and subsequent namespaces.

**Kubernetes Engine Developer**

Provides access to Kubernetes API objects inside clusters. A user with this role will be able to create, edit, and delete resources in **any** cluster and subsequent namespaces.

**Kubernetes Engine Cluster Admin**

Provides access to management of clusters. A user with this role will not have access to create or edit resources within any cluster or subsequent namespaces directly, but will be able to create, modify, and delete any cluster.

**Kubernetes Engine Viewer**

Provides read-only access to GKE resources. A user with this role will have read-only access to namespaces and their resources.

**Kubernetes Engine Cluster Viewer**

Get and list access to GKE Clusters. This is the minimal role required for anyone who needs to access resources within a cluster's namespaces.

* Grant the account the Kubernetes Engine Cluster Viewer role by running the following:

gcloud projects add-iam-policy-binding ${GOOGLE\_CLOUD\_PROJECT} \

--member=serviceAccount:team-a-dev@${GOOGLE\_CLOUD\_PROJECT}.iam.gserviceaccount.com \

--role=roles/container.clusterViewer

* Roles with single rules can be created with kubectl create

kubectl create role pod-reader \

--resource=pods --verb=watch --verb=get --verb=list

1. Create a role binding between the team-a-developers serviceaccount and the developer-role:

kubectl create rolebinding team-a-developers \

--role=developer --user=team-a-dev@${GOOGLE\_CLOUD\_PROJECT}.iam.gserviceaccount.com

When a cluster is shared in a multi-tenant set up, it's important to make sure that users are not able to use more than their fair share of the cluster resources. A resource quota object (ResourceQuota) will define constraints that will limit resource consumption in a namespace. A resource quota can specify a limit to object counts (pods, services, stateful sets, etc), total sum of storage resources (persistent volume claims, ephemeral storage, storage classes ), or total sum of compute resources. (cpu and memory).

kubectl create quota test-quota \

--hard=count/pods=2,count/services.loadbalancers=1 --namespace=team-a