Git

What is Git?

Git is a distributed version control system that helps manage and track changes in the source code efficiently.

What is GitHub?

GitHub is a web-based platform that uses Git to store and collaborate on code.

Version Control System

A Version Control System (VCS) is a software tool that helps manage and track changes to files and maintain a complete history of those changes.
Listed below are the functions of a VCS

- Allows developers to work simultaneously.
- Does not allow overwriting each other's changes.
- Maintains a history of every version.

Following are the types of VCS

- Centralized version control system (CVCS).
- Distributed/Decentralized version control system (DVCS).

What is VSC?

- VCS helps to track and manage changes to source code.
- Experimentation of code changes
- Reduce storage
- Maintain the different version of the code
- Encryption when uploading or downloading the files or data.

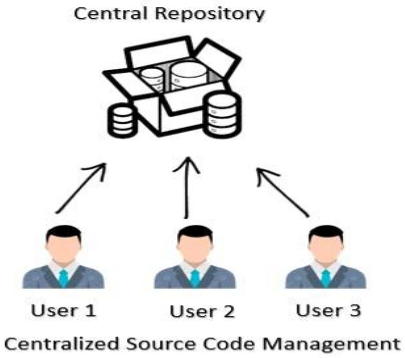
Type of VCS

1. Local Version control system
2. Centralized version control system
3. Distributed version control system

What is Centralised Version Control?

- It is used for managing the versions of the codes.
- Any developer can view/modify the code of another developer.
- If the central server fails, we can lose the data
- Continuous internet is required for connecting and storing the data (Slow Process)
- Code is not available locally

-> Operate on sync model, dependency on network.
-> Encryption is missing while pull and push the files to remote repository.
-> Local repository is not available.
-> If server goes down the repo will be gone. To overcome we need to take the back up.

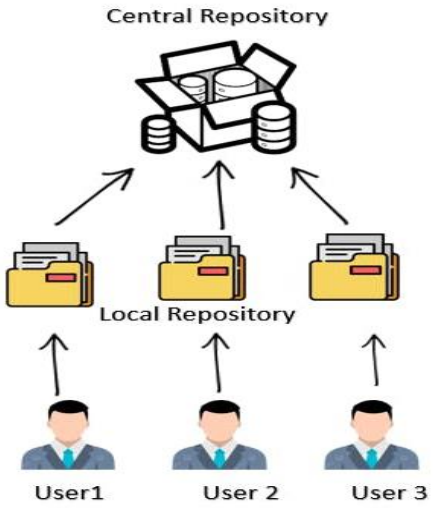


Distributed Version Control System:

- Git invented by Linus Torvalds in 2005
- GitHub is a web-based platform that uses Git to store and collaborate on code.
- You can access the code fast as the code is stored in a local repository as well
- If the remote repository goes down, every developer has their own code store at the local repository
- **Version control is done**

-> Encryption is available when data is traveling over the internet, pull and push. Data encrypted. SHA 256 (secure hash algorithm).

-> No dependency on the internet.

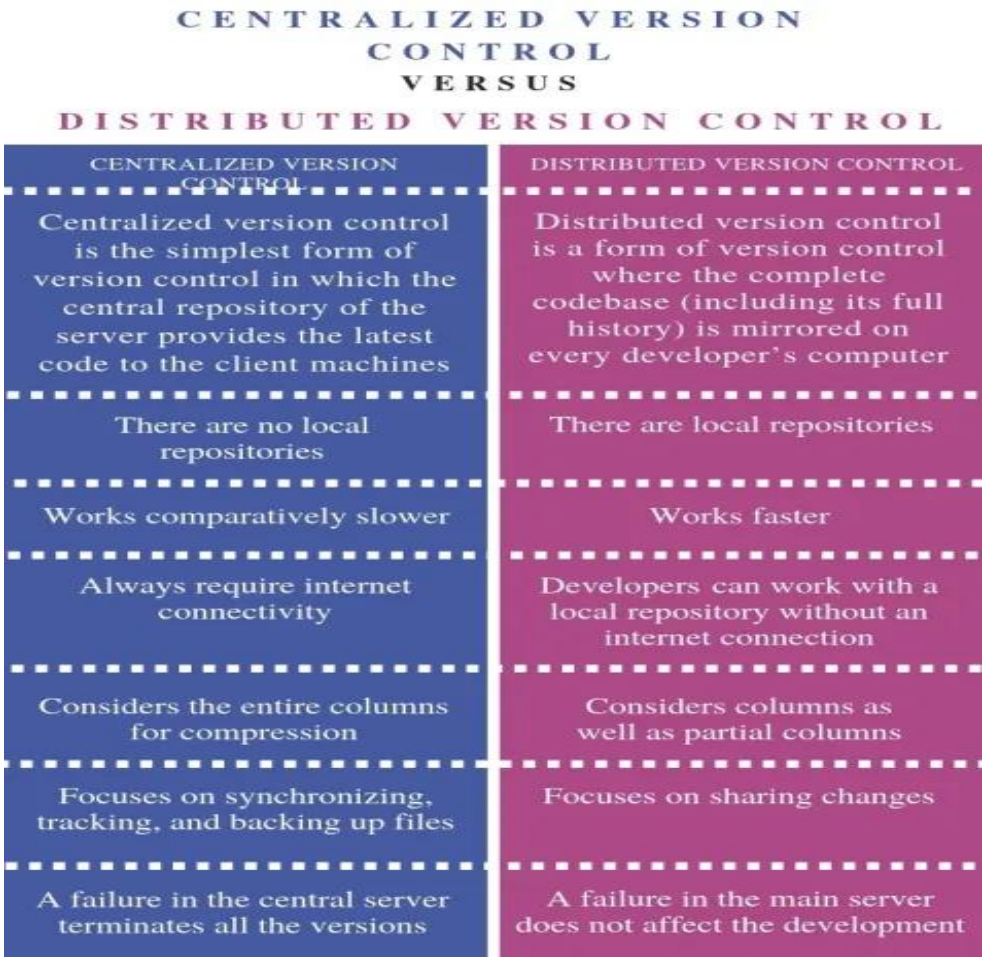


Difference between CVCS and DVCS?

Difference Between CVCS and DVCS

1. Every time user need to pull the data from the server and push back once done
2. Only online access available
3. Slower as command needs to communicate to the server
4. If Central repository is down , Developer can't work

1. It has the local repository and remote server repository so continuous connection is not required
2. Both online offline access available
3. Fast as it deals with local repository
4. No impact of central repository failure, as it use local for code



Types of VCS:

CVCS Tools

1. Team Foundation server (TFS) - ms office
2. Sub version - SVN

DVCS tools

1. Tortoise
2. Mercurial
3. Git

What is Git?

Git is a distributed version control system that helps manage and track changes in the source code efficiently.

https://learngitwithpra9.hashnode.dev/git-source-code-management-part-1

Three Stages of Git:

1. **Untracked or Working Area:** The file exists but is not part of Git version control
2. **Staging Area:** The file has been added to Git version control but changes have not been committed
3. **Commit:** The changes/modification of the code has been committed

The Git config command

To register a username:

```
$ git config --global user.name "Ram"
```

To register an email address for the given author:

```
$ git config --global user.email "Jaisitarama@gmail.com"
```

To check configuration settings;

This command used to list all the settings that Git can find at that point.

```
$ git config --list
```

Git configuration levels

Git allows configurations at **three different levels**, each overriding the previous one.

- **Local**: It is the default level in Git. Git config will write to a local level if no configuration option is given.
- **Global:** The global level configuration is **user-specific configuration**. User-specific means, it is applied to an individual **operating system user**.
- **System:** The system-level configuration is applied **across an entire system**. The entire system means all users on an operating system and all repositories.

Level	Scope	Command Example	Config File Location
System	Applies to **all users on the system**.	git config --system user.name "Alice"	/etc/gitconfig (Linux/macOS), or C:\ProgramData\Git\config (Windows)
Global	Applies to **all repositories for the current user**.	git config --global user.name "Alice"	~/.gitconfig or ~/.config/git/config
Local	Applies only to a **single Git repository**	git config --local user.name "Alice"	.git/config in the repo directory

- Git uses settings in this **precedence order**: local > global > system.

Git Terminology

Branch

In Git, a **branch** is a lightweight movable pointer to a commit. It allows developers to create a separate copy of the project (codebase) to work on a feature, bug fixes, or experiment **without affecting the main project (codebase)**.

- A **branch** is a lightweight pointer to a commit.
- Branches enable **parallel development** (multiple features at once).
- The default branch is usually called **main** or **master.**

Checkout

Checkout is a command used to **switch between different branches** or **to restore files in the working directory** to a previous state.

- **Switching Branches**
  To switch to an existing branch named "feature-branch":
  ```
  $ git checkout feature-branch
  ```
- **Restoring a File to a Previous State**
  To restore a specific file, "example.txt," to the version in the last commit:
  ```
  $ git checkout -- file.txt
  ```

Cherry-Picking

The **`git cherry-pick`** command is used to **apply a specific commit from one branch to another branch without merging the entire branch.**
In case you made a mistake and committed a change into the wrong branch, but do not want to merge the whole branch. You can revert the commit and cherry-pick it on another branch.

```
$ git cherry-pick <commit-hash>
```

Clone

The **`git clone`** command is used to **copy a remote repository to local machine**. It downloads the entire repository, including all its files, commit history, and branches, to your local machine.

Fetch

`git fetch` only **downloads the latest changes from the remote repository without merging the changes.**
It downloads the latest commits, branches, and tags from a remote repository without automatically merging

HEAD

HEAD is the representation of the last commit in the current checkout branch.
"HEAD" refers to a **Pointer to the current commit/branch.**

Index

The Git index is a **staging area** between the **working directory and repository**.
The Git index is a temporary staging area that stores a snapshot of the working tree.

Master
Default primary branch (historically master, now often main).

Merge
In Git, merge is a command used to **integrates (combine) changes from one branch into another. It combines the histories of two branches.**
It integrates the histories of the branches, allowing the **integration of new features or fixes into the main codebase.**

Origin
In Git, "origin" is the **default name for the remote repository URL**

Pull/Pull Request
'git pull' is a **combination** of two commands: **'git fetch'** and **'git merge'**. It fetches the latest changes from the remote repository and automatically merges them with the local branch. It downloads the latest changes and merges them into the current branch, creating a merge commit if necessary.

Pull: The git pull command fetches and merges changes from a remote repository to a local repository.
Pull Request: A pull request is a **request to merge code changes** from one branch into another within a repository.

Push
git push command is used to **upload local commits to remote repository.**

Rebase
Git rebase is a command used to **integrate changes from one branch onto another by moving or combining linear commits.** With rebase, you can apply a series of commits from one branch onto another, resulting in a linear commit history.

You would use 'git rebase' when you want to:
- Incorporate changes from one branch onto another with a linear commit history.
- Squash multiple commits into a single commit for a cleaner history.
- Edit or reorder commits to improve readability or resolve conflicts.

Remote
In Git, a remote is a reference to a version of a repository hosted on a server, commonly used to collaborate with others.
A remote version of the repo.

Repository
A **repository (or repo)** is a central storage space where **Git stores all the files and directories of a project, along with their complete history**. It contains the **entire version history** of the project, including all the commits and branches.
It keeps track of all changes made to the codebase, allowing developers to collaborate, review, and manage different versions of the project efficiently.

Stash

The `git stash` command is used **to temporarily save changes** that **are not ready to be committed yet**. It is useful when you need to **switch to a different branch or apply a hotfix but don't want to commit incomplete work.** You can later retrieve the changes from the stash using **`git stash apply` or `git stash pop`.**

Tag

A **tag** is a reference to a specific commit that is used to Marks specific points in project history (e.g., releases)., it is used to mark important events like releases or versions.

Tags are often used to create a snapshot of the project at a particular moment.
There are two types of tags.

1. **Light-weighted tag**
2. **Annotated tag**

Upstream And Downstream

"Upstream" refers to the **original repository** or **branch** from which the code is cloned, essentially the source of the code.
"Downstream" refers **local repository or branches** that **receive updates from the upstream.**

Git Revert

In Git, the revert command is used to **create a new commit that undoes a previous commit**

```
$ git revert <commit_hash>
```

Git Reset

It is used to **unstage the changes from the commit.** It will **rollback** to file into **working directory from staging area or index area.**

```
$ git reset HEAD <filename>
```

In Git, the reset command is used to undo changes by moving the current branch to a specific commit.

- Soft: Moves the branch pointer to the specified commit but leaves the changes in the staging area.

  ```
  $ git reset --soft <commit_hash>
  ```

- Mixed: Moves the branch pointer to the specified commit and clears the staging area, but keeps the changes in the working directory.

  ```
  $ git reset –mixed <commit_hash>
  ```

- Hard: Moves the branch pointer to the specified commit and discards all changes in the staging area and working directory.

  ```
  $ git reset --hard <commit_hash>
  ```

Git Ignore

In Git, a **.gitignore** file is used to **specify which files and directories should be ignored by Git.** This helps keep the repository clean by excluding unnecessary files, such as temporary files, build artifacts, and sensitive information, from being tracked.

Git Diff

It is used to show the differences between **two versions of a file, commit, or branch.**

```
$ `git diff file.txt`
```

In Git, the diff command is used to show the differences between changes in the working directory, staging area, or between commits. It highlights what changes have been made to the code, making it easier to review modifications.

1. **Show differences between working directory and staging area:**
   ```
   $ git diff
   ```
2. **Show differences between staging area and the latest commit:**
   ```
   $ git diff --staged
   ```
3. **Show differences between two commits:**
   ```
   $ git diff <commit1_hash> <commit2_hash>
   ```
4. **Show differences between a file in two commits:**
   ```
   $ git diff <commit1_hash> <commit2_hash> -- <file_path>
   ```

Git Flow: A Branching Model for Efficient Collaboration

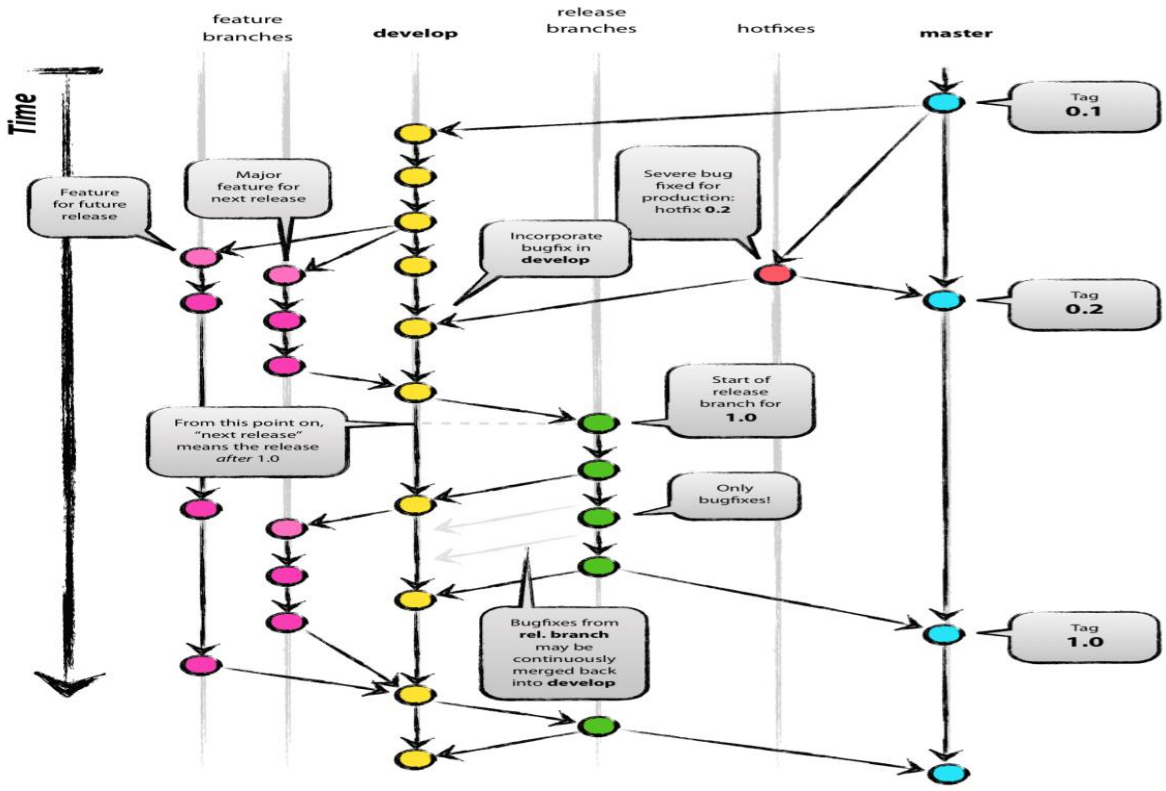
Git Flow is a branching model for Git that uses multiple branches to manage code changes.

It provides a **structured and efficient workflow for managing feature development, releases, and maintenance.** It defines a set of roles and rules for branches to ensure a smooth collaboration process.

Key Branches in Git Flow

Git Flow defines two **permanent branches** and multiple **supporting branches**:

Branch	Purpose
main (or master)	It contains production-ready code (stable and deployable code).
develop	Integration branch for features. All changes merge here before release. (**Serves as the integration branch where feature branches are merged before being released.**)
feature/*	**Temporary branches used to develop new features. These are branched from develop.** Short-lived branches for new functionality (branched from develop).
release/*	Prepares a new production release (branched from develop). **Used to prepare for a new production release. Created from develop and merged into both master and develop after the release**
hotfix/*	Emergency fixes for production (branched from main). **Used to quickly fix issues in production. Created from master and merged back into both master and develop.**



How Git Flow Works

A. Feature Development

1. **Create a feature branch**:
   ```
   # git checkout develop
   # git checkout -b feature/user-authentication
   ```
2. **Commit changes**:
   ```
   # git add .
   # git commit -m "Add login functionality"
   ```
3. **Merge back to** develop:
   ```
   # git checkout develop
   # git merge feature/user-authentication
   # git branch -d feature/user-authentication
   ```

B. Preparing a Release

1. **Create a release branch**:
   ```
   # git checkout develop
   # git checkout -b release/1.0.0
   ```
2. **Test & bug-fix** (no new features here).
3. **Merge to** main **& tag**:
   ```
   # git checkout main
   # git merge release/1.0.0
   # git tag -a v1.0.0 -m "Initial release"
   ```
4. **Update** develop:
   ```
   # git checkout develop
   # git merge release/1.0.0
   # git branch -d release/1.0.0
   ```

C. Hotfixes (Emergency Production Fixes)

1. **Branch from** main:
   ```
   # git checkout main
   # git checkout -b hotfix/login-bug
   ```
2. **Fix & merge back**:
   ```
   # git checkout main
   # git merge hotfix/login-bug
   # git tag -a v1.0.1 -m "Fixed login bug"
   # git checkout develop
   # git merge hotfix/login-bug
   # git branch -d hotfix/login-bug
   ```

Alternatives to Git Flow

- **GitHub Flow**: Single main branch + feature branches (simpler).
- **Trunk-Based Development**: Fewer branches, frequent commits (used by Google, Netflix).

Git Squash

In Git, squash refers to the process of **combining multiple commits into a single commit** for a **cleaner history.**

- **Squash the last n commits:**
  ```
  $ git rebase -i HEAD~<n>
  ```
- Replace <n> with the number of commits to squash.
- In the interactive rebase editor, change "pick" to "squash" (or "s") for the commits to combine.
  ```
  pick <commit-hash> Commit message 1
  squash <commit-hash> Commit message 2
  squash <commit-hash> Commit message 3
  ```
- Save and exit the editor. Git will combine the selected commits into one and prompt you to provide a new commit message.

Git Rm

In Git, the rm command is used to **remove files from both the working directory and the staging area.**

```
$ git rm <file_name>
```

Git Fork

A Git fork **creates a personal copy of another user's repository**
To resolve an issue for a bug that you found, you can:

- Fork the repository.
- Make the fix.
- Forward a pull request to the project owner.

12 Git Commands

There are many different ways to use Git. Git supports many command-line tools and graphical user interfaces. The Git command line is the only place where you can run all the Git commands.

Basic Git Commands

Here is a list of most essential Git commands that are used daily.

1. Git Config command
2. Git init command
3. Git clone command
4. Git add command
5. Git commit command
6. Git status command
7. Git push Command
8. Git pull command
9. Git Branch Command
10. Git Merge Command
11. Git log command
12. Git remote command

1) Git config command

In Git, the **git config** command is used to **set configuration options for Git repositories**. like your **username, email address, default editor, and other settings**. These settings can be applied at different levels: system, global, and local.

Syntax

- **Set user name:**

```
$ git config --global user.name "Your Name"
```

- **Set user email:**

```
$ git config --global user.email "your.email@example.com"
```

- **Set the default text editor:**

```
$ git config --global core.editor "your_editor"
```

- **View current configuration settings:**

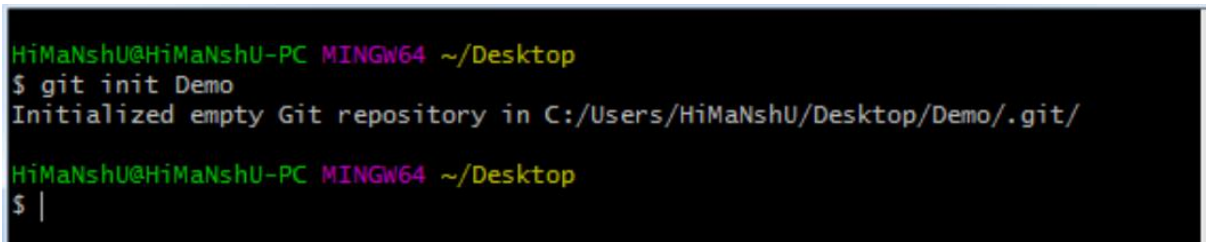
```
$ git config --list
```

2) Git Init command

This command is used to create a local repository. This init command will **initialize an empty repository.**

Syntax

```
$ git init Demo
```



3) Git clone command

The git clone command is used to create a copy of an existing repository.

Syntax

```
$ git clone URL
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (master)
$ git clone https://github.com/ImDwivedi1/Git-Example.git
Cloning into 'Git-Example'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (3/3), done.
```

4) Git add command

This command is used to add one or more files to staging (Index) area.
Syntax
To add one file

```
$ git add Filename
```

To add more than one file

```
$ git add*
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (master)
$ git add README.md
```

5) Git commit command

Commit command is used in two scenarios. They are as follows.

Git commit -m

The commit command is used to save changes to the local repository.
Each commit represents **a snapshot of the project** at a specific point in time, allowing for a detailed history of changes and easy rollback if needed.
Syntax

```
$ git commit -m " Commit Message"
```

Git commit -a

This command commits any files added in the repository with git add and also commits any files you have changed since then.
Syntax

```
$ git commit -a
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (master)
$ git commit -a -m "Adding the key of c"
[master (root-commit) 758797a] Adding the key of c
 1 file changed, 2 insertions(+)
 create mode 100644 README.md
```

6) Git status command

The status command is used to **display the state of the working directory and the staging area.**

Syntax

```
$ git status
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (master)
$ git status
On branch master
Your branch is based on 'origin/master', but the upstream is gone.
  (use "git branch --unset-upstream" to fixup)

nothing to commit, working tree clean
```

7) Git push Command

The push command is used to **upload local repository content to a remote repository.**

Git push origin master

This command sends the changes made on the master branch, to your remote repository.

Syntax

```
$ git push [remote] master
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (mast
er)
$ git push origin master
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$ git push origin master
Everything up-to-date

HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$
```

Git push -all

This command pushes all the branches to the server repository.

Syntax

```
$ git push --all
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$ git push --all
Everything up-to-date

HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$
```

Push tags:

Syntax

```
$ git push --tags
```

8) Git pull command

The pull command is used to **fetch and merge changes from a remote repository into the current branch.**

Syntax

```
$ git pull URL
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (master)
$ git pull https://github.com/ImDwivedi1/Git-Example
warning: no common commits
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (3/3), done.
From https://github.com/ImDwivedi1/Git-Example
 * branch            HEAD       -> FETCH_HEAD
fatal: refusing to merge unrelated histories

HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/Git-example (master)
$
```

9) Git Branch Command

This command **displays a list all the branches available in the repository.**

Syntax

- List all branches:
  ```
  $ git branch
  ```
- Create a new branch:
  ```
  $ git branch <branch_name>
  ```
- Switch to a branch:
  ```
  $ git branch <branch_name>
  ```
- Create and switch to a new branch:
  ```
  $ git branch -b <branch_name>
  ```
- Rename a branch:
  ```
  $ git branch -m <old_branch_name> <new_branch_name>
  ```
- Delete a branch:
  ```
  $ git branch -d <branch_name>
  ```
- Show the last commit on each branch:
  ```
  $ git branch -v
  ```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$ git branch
* master

HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
```

10) Git Merge Command

the merge command is used **to combine changes from different branches into a single branch.**

This command is commonly **used to integrate feature branches, bug fixes, or other contributions into the main codebase.**

Syntax

- Merge a branch into the current branch:
  ```
  $ git merge <branch_name>
  ```

- Merge a branch without creating a merge commit (fast-forward merge):

Performs a fast-forward merge if possible, updating the current branch to match the specified branch without creating a merge commit.

```
$ git merge --ff-only <branch_name>
```

- Squash and merge a branch:
  Combines all commits from the specified branch into a single commit in the current branch.

```
$ git merge --squash <branch_name>
```

- Abort a merge in progress:
  Cancels an ongoing merge operation and reverts the working directory to the state before the merge.

```
$ git merge --abort>
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$ git merge master
Already up to date.
```

11) Git log Command

The log command is used to **display the commit history of a repository.**
It shows a list of commits along with information like commit hashes, authors, dates, and commit messages.

This command is used to check the commit history.
Syntax

- Log command:

```
$ git log
```

- Show a specified number of commits:

```
$ git log -n <number>
$ git log -n 5
```

- Show commits by a specific author:

```
$ git log --author="Author Name"
```

- Show commits containing a specific keyword:

```
$ git log --grep="keyword"
```

- Show a summary of each commit (shot format - one line per commit):

```
$ git log --oneline
```

- Show a graphical representation of the commit history:

```
$ git log --graph
```

- Show changes introduced by each commit:

```
$ git log -p
```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$ git log
commit 1d2bc037a54eba76e9f25b8e8cf7176273d13af0 (HEAD -> master, origin/master,
origin/HEAD)
Author: ImDwivedi1 <52317024+ImDwivedi1@users.noreply.github.com>
Date:   Fri Aug 30 11:05:06 2019 +0530

    Initial commit
```

12) Git remote Command

The remote command is used to **manage and interact with remote repositories.**

Syntax

- List all remote repositories:
  ```
  $ git remote -v
  ```
- Add a new remote repository:
  ```
  $ git remote add <remote_name> <repository_url>
  ```
- Remove a remote repository:
  ```
  $ git remote remove <remote_name>
  ```
- Rename a remote repository:
  ```
  $ git remote rename <old_name> <new_name>
  ```
- Show details of a specific remote:
  ```
  $ git remote show <remote_name>
  ```
- Update remote references:
  ```
  $ git remote update
  ```

```
HiMaNshU@HiMaNshU-PC MINGW64 ~/Desktop/gitexample2 (master)
$ git remote add origin https://github.com/ImDwivedi1/GitExample2
fatal: remote origin already exists.
```

Git Flow / Git Branching Model

Git Stash
Git stash
Git stash save
Git stash list
Git stash apply
Git stash changes
Git stash pop
Git stash drop
Git stash clear
Git stash branch

Git Tags

Git Merge Conflict

$ git mergetool

https://media.licdn.com/dms/document/media/v2/D4E1FAQG-A8EirXkWMQ/feedshare-document-pdf-analyzed/B4EZQmafNuGYAc-/0/1735811358843?e=1737590400&v=beta&t=VKeR0i-B-kjaUxRHrvZYRf1wUuBSmYR_DtfGrXMh0EY

https://media.licdn.com/dms/document/media/v2/D561FAQGHhm0aWFvW6Q/feedshare-document-pdf-analyzed/B56ZQLw9WMGQAY-/0/1735364193676?e=1738195200&v=beta&t=oq4Dejgh_RhLu2JGc-KYsfcrcLuStAkw5dHmGbnzHWc

Docker

Docker is containerization technology tool.
Kubernetes is container orchestration tool.

What is Docker?

Docker is a containerization platform for developing, shipping, and running applications in **containers**—lightweight, isolated environments that package code and dependencies.

Key Concepts

- **Container**: A runtime instance of an image (like a lightweight VM).
- **Image**: A read-only template with instructions to create a container (e.g., nginx:alpine).
- **Dockerfile**: A script to build custom images.
- **Docker Hub**: Public registry for images (like GitHub for containers).

Docker

- Docker is mini-OS and Lightweight containers and fast responsible.

- **Docker has container runtime**, it helps to run container or manage the life cycle of the container.
- **Containers**—lightweight, isolated environments that package code and dependencies.
- **Container is ephemeral** - short life or lived, containers can die or revive anytime.
- A Docker container is a **lightweight, executable package** that includes application code, a runtime environment (e.g., Python, Node.js), libraries, and all other dependencies required to run the application.

Containerization:

It's all about deploy application with required dependencies is known as containerization.

Kubernetes:

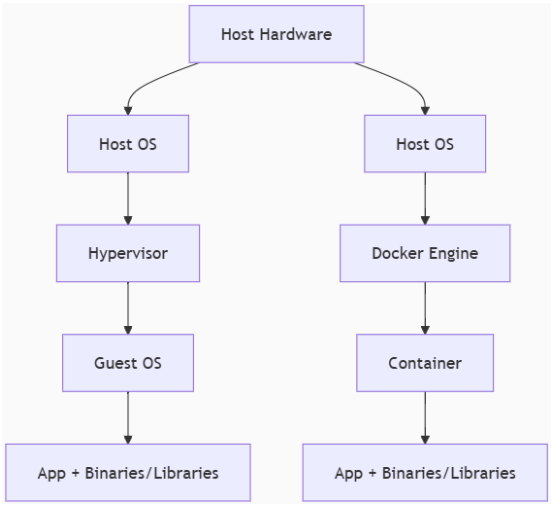
Kubernetes is an orchestration platform for running and managing container for many (100's of) containers runtimes.

Virtualization:

-

Docker vs. Virtual Machines (VMs)

Feature	**Docker**	**VM**
Isolation	Process-level (light)	Hardware-level (heavy)
Boot Time	Seconds	Minutes
Performance	Near-native	Overhead
Image Size	MBs	GBs



Container Engine:

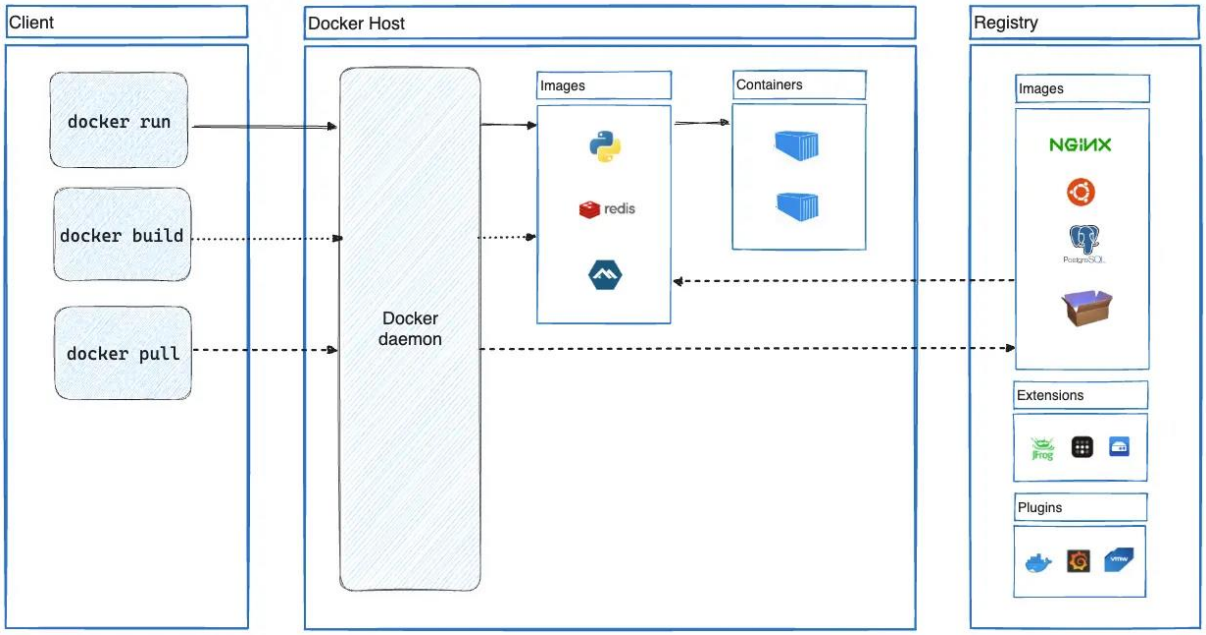
Software which helps to **implement containerization on a machine or server** is caller container Engine.

Tool:

Docker, Jail, Crio.

Docker Architecture:

- **Docker Daemon**: Background service managing containers/images.
- **Docker Client**: CLI (docker) to interact with the daemon.
- **Docker Registry**: Stores images (e.g., Docker Hub, AWS ECR).



Docker CLI/Client:

Docker client is a tool helps **interact with Docker** and **manage** containers, images, networks, and volumes directly from the command line. It is a powerful interface for Docker, providing commands to perform tasks such as building, running, and stopping containers, as well as managing Docker images and networking.

Some common Docker CLI commands include:

- **docker run**: Used to create and start a container from images.
- **docker build**: Builds a Docker image from a Dockerfile.
- **docker pull**: Downloads an image from a Docker registry like Docker Hub.
- **docker ps**: Lists all running containers.
- **docker images**: Lists all available Docker images in server.
- **docker push**: Uploads an image to a Docker registry.
- **docker stop**: Stops a running container.
- **docker rm**: Removes a stopped container.
- **docker exec:** Executes a command inside a running container.
- **docker start:** Starts a stopped container.
- **docker logs:** Displays logs from a container.
- **docker attach:** Attaches to a running container's main process (useful for debugging).

Docker Daemon (Docker service):

Docker daemon manages all the services by **communicating with other daemons** (**services**). It manages docker objects such as images, containers, networks, and volumes with the help of the API requests of Docker.

(**The Docker daemon** listens for **Docker API requests** and **manages Docker objects** such as **images, containers, networks,** and **volumes**.)

Docker Host

In simple terms:

- **Docker Host** is the machine or environment where the **Docker Engine** is installed and running.
- It provides the environment where containers are created, managed, and executed.
- **Docker Host** is responsible for **managing Docker containers and images**, as well as **handling the resources** (CPU, memory, disk, etc.) needed to run them.

Docker Registry

Registry:

- It is a collection of all dependencies and docker container images
- All the docker images are stored in the docker registry.

Docker pull:

- It helps to download the images or dependencies from registry on to the docker host.
  # Docker pull <image name:version>

Docker Images

- **Image** is collection of layers. (Hash tag or commit id). An image contains **instructions** to create a docker container. It helps to create container from docker images.
- A Docker image includes the application code, libraries, dependencies, tools, and other files required to run an application.

Docker Container

- **A Docker container** is a **runtime instance of a Docker image**. It is a **lightweight, executable package** that includes application code, a runtime environment (e.g., Python, Node.js), libraries, and all other dependencies required to run the application.
- Containers are created from docker images. With the help of Docker API or CLI, we can start, stop, delete, or move a container.

Docker Services:

➔ After docker install, we must follow 3 steps (or) activities.

1. Start the docker services.
   Ex: **service docker start**
2. Enable docker services at boot time.
   chkconfig docker on
3. Add the user account to the docker root group.
   Ex: **usermod -a -G dockerroot <username>**

➔ After installing docker, it will create group called **dockerroot**. We must add user account to the docker root group.

Docker commands:

How to check docker client and engine version?
docker version

How to check docker server configuration?
docker info

How to find the container image?
Docker images

How to check the container information?
Docker ps -a
Or
Docker ps -> it will shows only live or running containers

How to create images?
Docker build –tag <image Name> <file path to docker file>

How to create a container?
Docker run -it <image name or Id> <container shell ex: sh, bash>
Note : -it is used for create and log into the container

How to close a container and come out?
Type exit in container and click on enter.

How to come out from container without closing session?
Ctrl + pq

How to stop container?
Docker container stop <container id or name>

How to start container?
Docker container start <container id or name>

How to log into the container or docker exec command?
Docker exec -it <container name or id > <container shell>

Note: the container should be running and up to log into the container. If container is stopped or not running, we have to start and log in.

How to start and log into a container?
Docker start -ai <container name or id >
Note: Here we can't change the shell, default shell is sh

Create or update container names?
Docker rename <old container name > <new container name>

How to name a container while creating?

Docker run -name <container name> -it <image id> <container shell>

How to delete containers?
Docker rm <container id or name>
Note: always delete a container when status is showing as exited.
docker rm <container id or name> --force (to remove container forcefully)

How to delete multiple containers?
Docker rm < container name1> name2 name3 etc…

How to delete docker images?
Docker rmi <image name or id >
Note: it will only delete images not the container running from those images.

Image tagging:
Two types of image tags are available.

1. **Local tag**
   Local tag helps to create an alias name use case on docker server or host. We can't upload local tag images to docker registry
   # Docker image tag <source image name or id > <new image name >
2. **Remote tag**
   We can generate image alias both for use case or keeping images on docker host and upload to the docker registry.
   # Docker tag <source image name or id > <docker hub id>/<new image name>:<image version>

How to login to docker hub from cli mode?
Docker login

How to push images to docker registry or hub?
Docker push <image name>
Note: **only use image names to push images to docker hub**

How to logout from docker hub?
Docker logout

Docker image inspect:
Inspect command shows the properties of the image.

How to get the image meta data info or properties?
Docker image inspect <image id or name>

How to get the container meta data info or properties?
Docker container inspect <container name or id>

Docker image history:
This command helps to check the layers of the image or code of the image.
Docker image history

Docker layer:
Docker build follows the process of interpretation it will check the code line by line.
If we have 4 lines in a code
First line code is correct it will create hashtag or commit id. If the hashtag crated this will generate a layer.

Image is a collection of layers
In dockerfile output layers are arranged in descending order
The last line of the layer in an image automatically considered as image id.
Each line of code in dockerfile we have to call as instruction.
If instruction executed correctly docker will create layer, all these instructions are written in a file is called dockerfile. For docker file no extension.

Docker build is process of converting instructions into layers if all layers are successfully executed then it will generate a docker image else if one of the instructions fails then layer will not generate. If one of the layers fails then docker image fails to generate.

Dockerfile:

- Dockerfile helps to create images,
- File contains instructions.
- These instructions more look like Linux commands.

Work flow of docker image process:

1. Crete project folder
2. Cd into folder, create dockerfile. Name is Dockerfile.
3. Open the dockerfile, write the code and save it.
   Eg: FROM python:3.12
   WORKDIR /usr/local/app
   # Install the application dependencies
   COPY requirements.txt ./
   RUN pip install --no-cache-dir -r requirements.txt
   # Copy in the source code
   COPY src ./src
   EXPOSE 5000
   # Setup an app user so the container doesn't run as the root user
   RUN useradd app
   USER app
   CMD ["uvicorn", "app.main:app", "--host", "0.0.0.0", "--port", "8080"]
4. Excute it (Image build process)
   Commad:
   Docker image build –tag <image_name > <docker file path>
5. Result: docker ps
6. Then push to docker hub.

Dockerfile Basics
Example Dockerfile for a Node.js app:
dockerfile

```
FROM node:18-alpine          # Base image
WORKDIR /app                 # Set working directory
COPY package*.json ./        # Copy dependency files
RUN npm install              # Install dependencies
COPY . .                     # Copy app code
EXPOSE 3000                  # Declare port
CMD ["npm", "start"]         # Default command
```

Build and Run:

- docker build -t my-node-app .
- docker run -p 3000:3000 my-node-app

Docker instructions:

- **FROM <image>** - this specifies the base image that the build will extend.
- **WORKDIR <path>** - this instruction specifies the "working directory" or the path in the image where files will be copied and commands will be executed.
- **COPY <host-path> <image-path>** - this instruction tells the builder to copy files from the host and put them into the container image.
- **RUN <command>** - this instruction tells the builder to run the specified command. It executed at time of image build process.
- **ENV <name> <value>** - this instruction sets an environment variable that a running container will use.
- **EXPOSE <port-number> -** this instruction sets configuration on the image that indicates a port the image would like to expose.
- **USER <user-or-uid>** - this instruction sets the default user for all subsequent instructions.
- **CMD ["<command>", "<arg1>"]** - this instruction sets the default command a container using this image will run. It executed at time of container creation.
- **ENTRYPOINT [command param1 param2]:** specifies the main command to execute when a container starts.

For more information about docker installations:
https://docs.docker.com/get-started/docker-concepts/building-images/writing-a-dockerfile/

Docker Networking

Docker Networking

- **Bridge**: Default network for containers on the same host.
- **Host**: Shares the host's network stack.
- **Overlay**: Connects containers across multiple hosts (Swarm/Kubernetes).

Example:

- docker network create my-net
- docker run --network=my-net nginx

Docker Networking refers to how Docker containers communicate with each other and the outside world. Docker uses a network model that allows containers to connect to one another and to external systems while ensuring isolation, security, and scalability.

Key Concepts in Docker Networking:

1. **Container Networking**: Each container gets its own network stack (IP address, ports, etc.) when it is created, and it can communicate with other containers and external services based on its network configuration.
2. **Network Drivers**: Docker uses different network drivers to control how containers communicate. Each driver defines a networking mode (e.g., bridge, host, overlay, etc.) and manages the behaviour of containers in that network.

   The Docker Network command is the main command that would allow you to create, manage, and configure your Docker Network. Let's see what the sub-commands can be used with the Docker Network command. to know more about Creating a Network in Docker and Connecting a Container to That Network.

3. **IP Addresses and Ports**: Each container gets its own IP address on the network. Containers can expose ports, allowing external systems to communicate with them (e.g., HTTP on port 80).
4. **Network Isolation**: Containers can be isolated in different networks for better security and control. By default, containers that are part of the same network can communicate with each other, while containers on different networks are isolated.

Docker Network Drivers:

Docker supports several types of network drivers, each designed for different use cases:

1. Bridge Network (default)

- Bridge networks create a **virtual bridge between host and the container**. Containers connected to the network can communicate with each other, but they're isolated from those outside the network.
- **Description**: This is the default network driver when you create a container. Containers on a bridge network are connected to a virtual bridge (a software-based network bridge) on the host system. **Containers can communicate with each other through this bridge and can be accessed externally by exposing ports.**
- **bridge:** If you build a container without specifying the kind of driver, the container will only be created in the bridge network, which is the default network.

Run a container on the bridge network (default)
$ docker run -d --name my_container --network bridge my_image

2. Host Network

- **Description**: When a container is run on the host network, **it shares the host's network stack directly.** The **container doesn't get its own IP address** but uses the **host's IP and network interfaces.** It can access all ports and services available on the host machine.
- **host:** Containers will not have any IP address they will be directly created in the system network which will remove isolation between the docker host and containers.

Run a container on the host network

$ docker run -d --name my_container --network host my_image

3. Overlay Network

- **Description**: Overlay networks allow containers to **communicate across multiple Docker hosts.** This network driver is commonly used when deploying applications in a **Swarm** or **Kubernetes** cluster. It abstracts the underlying network and connects containers across different hosts over a virtual network.
- **Use Case**: Ideal for multi-host communication in a Docker Swarm or Kubernetes cluster.

- **overlay:** overlay network will enable the connection between multiple Docker demons and make different Docker swarm services communicate with each other

Create an overlay network
$ docker network create --driver overlay my_overlay_network

Run containers on the overlay network (example in Swarm mode)
$ docker service create --name my_service --network my_overlay_network my_image

4. None Network

- **Description**: This driver disables networking for the container entirely. The container will not have any network interfaces or be able to communicate with other containers or the external network.
- **Use Case**: Used when you want to isolate a container from any networking (e.g., for security reasons or when running an application that doesn't require networking).

- **none:** IP addresses won't be assigned to containers. These containments are not accessible to us from the outside or from any other container.

Run a container with no network access
$ docker run -d --name my_container --network none my_image

5. Macvlan Network

- macvlan is another advanced option that **allows containers to appear as physical devices on your network.** It works by assigning each container in the network a unique MAC address.
- **Description**: The Macvlan driver allows containers to appear as individual devices on the physical network. Each container gets its own MAC address and IP address, making it behave as if it is a physical device connected to the network.
- **Use Case**: Useful when you need containers to directly interact with the physical network or when legacy applications require containers to have a unique MAC address and IP.
- **macvlan:** macvlan driver makes it possible to assign MAC addresses to a container.

Create a Macvlan network
$ docker network create -d macvlan --subnet=192.168.1.0/24 --gateway=192.168.1.1 my_macvlan_network

Run a container on a Macvlan network
$ docker run -d --name my_container --network my_macvlan_network my_image

6. ipvlan Network:

- **IPvLAN** is an advanced driver that offers precise control over the IPv4 and IPv6 addresses assigned to your containers, as well as layer 2 and 3 VLAN tagging and routing.
- Users have complete control over both IPv4 and IPv6 addressing by using the IPvlan driver.

Common Docker Networking Commands:

- List Networks:
  $ docker network ls
- Create a Network:
  $ docker network create --driver bridge my_bridge_network
- Inspect a Network (get detailed information about a network):
  $ docker network inspect my_bridge_network
- Connect a Container to a Network:
  $ docker network connect my_bridge_network my_container
- Disconnect a Container from a Network:
  $ docker network disconnect my_bridge_network my_container
- View Container's Network Information:
  $ docker inspect my_container

Exposing Ports for External Access:
In Docker, containers typically run in isolated networks and cannot be accessed externally unless specific ports are exposed. You can map container ports to host ports using the -p or --publish option.

Run a container and expose its port (e.g., 80 in container to port 8080 on the host)
$ docker run -d -p 8080:80 my_image
This allows you to access the container's service (running on port 80 inside the container) via the host machine's port 8080.

sudo docker network

How to create a docker network.
$ sudo docker network create --driver <driver-name> <bridge-name>

Using the “Connect” command, you can connect a running Docker Container to an existing Network.
sudo docker network connect <network-name> <container-name or id>

Using the Network Inspect command, you can find out the details of a Docker Network.
You can also find the list of Containers that are connected to the Network.
sudo docker network inspect <network-name>

The disconnect command can be used to remove a Container from the Network.
sudo docker network disconnect <network-name> <container-name>

You can remove a Docker Network using the rm command.
Note that if you want to remove a network, you need to make sure that no container is currently referencing the network.
sudo docker network rm <network-name>

To remove all the unused Docker Networks, you can use the prune command.
sudo docker network prune

Docker Networking – Basics, Network Types & Examples
https://spacelift.io/blog/docker-networking

Docker Volume and Bind Mounts:

Docker Volumes
Persist data outside containers:

- docker volume create my-data
- docker run -v my-data:/data alpine

In Docker, **volumes** and **bind mounts** are both used to persist data and share data between the host system and containers. **Docker volumes and bind mounts** are two ways to manage persistent data in Docker containers.
Here's an explanation of each:

1. Docker Volumes

A **Docker volume** is a specialized storage mechanism managed by Docker, designed for storing data that should persist even after containers are stopped, removed, or recreated. Volumes are stored in a specific location on the host filesystem, but Docker manages the underlying filesystem for the volume.

Key Features of Volumes:

- **Managed by Docker:** Volumes are stored outside the container filesystem, managed, and maintained by Docker.
- **Persistence**: Data stored in volumes persists even if a container is deleted and restarted. Volumes can be reused across multiple containers.
- **Isolation**: Volumes are independent of the host filesystem, making them more portable and secure. Docker handles the storage location.
- **Sharing Data**: Volumes can be shared and reused by multiple containers. For example, multiple containers can mount the same volume, enabling data sharing between them.
- **Backup and Restore**: Volumes are easier to back up and restore compared to bind mounts because Docker provides built-in tools.

Example:
Create a volume
$ docker volume create my_volume

Run a container with a volume mounted

$ docker run -d -v myvolume:/data myimage
$ docker run -d -v my_volume:/data my_container

2. Bind Mounts

Bind mounts allow you to mount a directory or file from the host system directly into a container. This means that changes made inside the container will be reflected on the host, and vice versa.

Bind mounts allow you to directly access and modify files and directories on the host machine from within the container.

Key Features of Bind Mounts:

- **Direct Host Access**: Bind mounts provide direct access to the host filesystem. You specify an exact path on the host (e.g., /path/on/host), and Docker mounts it to the container.
- **More Flexibility**: You can mount specific files or directories from the host into a container, allowing for custom configurations, shared logs, or easy development workflows.
- **Less Isolation**: Since bind mounts expose the host filesystem directly, they are less isolated than volumes, which may present security risks.
- **Performance**: Bind mounts can be faster for certain use cases, such as when you're working with large amounts of data and need direct access to the host filesystem.

Use Case:
Bind mounts are often used when you want a container to access files or directories that are located on the host system (e.g., source code during development or configuration files).

Example:
Run a container with a bind mount (host directory to container directory)
$ docker run -d -v /path/on/host:/data myimage
$ docker run -d -v /host/path:/container/path my_container

Comparison Between Docker Volumes and Bind Mounts

Feature	Docker Volumes	Bind Mounts
Storage Location	Managed by Docker (location depends on Docker setup)	Defined by the user on the host filesystem
Persistence	Data persists after container removal	Data persists unless the file or directory is deleted from the host
Backup and Restore	Easier, as volumes are managed by Docker	Backup and restore must be handled manually
Portability	Portable across hosts (if shared between containers)	Tied to the host filesystem
Security	More isolated from the host filesystem	Direct access to the host filesystem
Performance	May have slight overhead due to Docker management	Faster in some cases since it's a direct mount
Use Cases	Ideal for persistent storage (databases, logs, etc.)	Ideal for shared development files or custom configurations

---

When to Use Volumes vs Bind Mounts:

- **Use Volumes** when:
  - You need persistent, portable storage that is independent of the host filesystem.
  - You are running databases or applications that need reliable, managed storage.
  - You want Docker to handle storage management for backups, snapshots, and migration.
- **Docker Volumes** are typically preferred for production environments due to their portability, easier management, and Docker's built-in support for persistence and backup.

- **Use Bind Mounts** when:
  - You need to share files or directories directly between the host and the container (e.g., for development, configuration files, or logs).
  - You need more control over the location of the data on the host.
  - You want to mount specific files (e.g., a configuration file) into a container.

- **Bind Mounts** provide more flexibility and are useful for development or situations where you need direct access to the host filesystem.

Docker Volumes – Guide with Examples
https://spacelift.io/blog/docker-volumes

Docker Compose

Docker Compose is a tool that makes it easier to create and run multi-container applications. It automates the process of managing several Docker containers simultaneously, such as a website frontend, API, and database service.

Orchestrate multi-container apps with docker-compose.yml:

```yaml
version: '3.8'
services:
  web:
    image: nginx:alpine
    ports:
      - "80:80"
  db:
    image: postgres:13
    volumes:
      - db-data:/var/lib/postgresql/data
volumes:
  db-data:
```

Commands:

- docker-compose up -d # Start services in detached mode
- docker-compose down # Stop and remove containers

Dockerfile

```
# syntax=docker/dockerfile:1
FROM python:3.10-alpine
```

```
WORKDIR /code
ENV FLASK_APP=app.py
ENV FLASK_RUN_HOST=0.0.0.0
RUN apk add --no-cache gcc musl-dev linux-headers
COPY requirements.txt requirements.txt
RUN pip install -r requirements.txt
EXPOSE 5000
COPY . .
CMD ["flask", "run", "--debug"]
```

compose.yaml

```
services:
  web:
    build: .
    ports:
      - "8000:5000"
  redis:
    image: "redis:alpine"
```

- **docker compose up**
- **docker compose down**
- **docker compose stop**

Docker Compose – What is It, Example & Tutorial
https://spacelift.io/blog/docker-compose

Docker Security:

Docker security is essential for ensuring the safe operation of containers in both development and production environments. By applying these security practices and tools, you can minimize risks, protect the host system, and prevent attacks. Security should be an ongoing process, with regular updates, scans, and reviews to ensure Docker environments remain secure.

1. Image Security
Use Official Images: Official images on Docker Hub are often vetted for security issues. You should prefer official or trusted images over random, unverified ones.
Scan for Vulnerabilities: Docker images may contain vulnerabilities. You can use tools like Docker's docker scan (integrated with Snyk) to scan images for known vulnerabilities.
Minimize Base Image: Use minimal base images (e.g., alpine or scratch) to reduce the attack surface, avoiding unnecessary software in the image.

2. Container Isolation
Namespace Isolation: Docker uses namespaces to isolate containers from each other and from the host system. This helps ensure that one container cannot affect the others or the host system directly.

Control Groups (cgroups): Docker uses cgroups to control resources allocated to containers (like CPU, memory, and disk). This prevents one container from consuming too many resources and impacting others.
Seccomp Profiles:
AppArmor/SELinux:

3. User and Permissions Management
Least Privilege Principle: Containers should run with the least privileges required. This means avoiding running containers as the root user when unnecessary.
File Permissions: Properly manage file permissions in your container and on the host system to prevent unauthorized access.
User Namespaces:

4. Docker Daemon Security
Docker Daemon Socket: By default, the Docker daemon listens on a Unix socket (/var/run/docker.sock), which is accessible to users in the docker group. Restrict access to this socket to prevent unauthorized control over Docker.
Remote API Security: If you're using the Docker Remote API, ensure it is securely configured using TLS/SSL to encrypt communication. Access should be controlled with appropriate authentication mechanisms.
Limit Docker Daemon Privileges: Ensure that the Docker Daemon itself is running with the least privileges required, and limit its exposure to unnecessary services.

5. Networking Security
Network Segmentation: Use Docker's built-in networking capabilities (e.g., bridge, overlay) to isolate containers and limit network communication between them, based on their needs.
Secure Connections: Containers communicating over the network should use encryption (e.g., HTTPS, TLS) to prevent data from being intercepted.
Firewalls: Control network access to Docker containers using firewalls, either on the Docker host itself or within the container's network settings.

6. Logging and Monitoring
Log Container Activity:
Monitor Resources:
Audit Docker Commands:

7. Container Runtime Security
Runtime Security Tools:
Container Scanning at Runtime:

10. Vulnerability Patching
Regularly Update Images: Regularly pull the latest versions of images from official repositories to ensure you get security patches and updates.
Update Docker and Host Systems: Make sure that both Docker and the host system are kept up-to-date with the latest security patches and updates.

11. Security Tools for Docker

Trivy: A simple and comprehensive vulnerability scanner for containers, which checks images for vulnerabilities in OS packages and application dependencies.

12. Orchestration Security
When using orchestration systems like Docker Swarm or Kubernetes, consider the security of the cluster, such as secure communication (TLS), role-based access control (RBAC), and secrets management.

Image layers
what is the Base layers in docker file?
Latest version: 1.27.0-alpine
If the layers are more, then it can be easy to hack
Docker exec -it
we need to create new user to login into container.
It should username@container name.

trivy - to scan the images - it will teach in pipeline projects.

Docker ignore --
We should not use add command, this comes under security.

Add command can also download the files from url, because of this there might causes of hack.

Environmental variables, username and password.
Don't hard code the passwords and username.
User docker secretes.

Interview questions
1. which image have you used, base image or latest image?
2. which user have you user, either root user or different user?
3. don't provide the privileges for some users.
4. docker instructions commands
5. what is the Base layers in docker file?

Docker Troubleshooting:
Top
Stats
Logs
Logs -f
exce -it
inspect volume, network,
History

Docker compose and docker multi stage build.

Essential Docker Commands
Container Management

Command	Description
docker run -d -p 80:80 nginx	Run Nginx in detached mode, mapping port 80.
docker ps	List running containers.
docker ps -a	List all containers (including stopped).
docker stop <container>	Gracefully stop a container.
docker rm <container>	Delete a stopped container.
docker logs <container>	View container logs.

Image Management

Command	Description
docker pull nginx	Download an image from Docker Hub.
docker images	List local images.
docker rmi <image>	Delete an image.
docker build -t my-app .	Build an image from a Dockerfile.

Networking & Volumes

Command	Description
docker network ls	List networks.
docker volume create my-vol	Create a persistent volume.
docker run -v my-vol:/data	Mount a volume into a container.

Best Practices

✓ **Use** .dockerignore to exclude unnecessary files (like .gitignore).

✓ **Prefer small base images** (e.g., alpine over ubuntu).

✓ **Run one process per container**.
✓ **Use multi-stage builds** to reduce final image size.

Common Use Cases

- **Microservices**: Deploy isolated services.
- **CI/CD Pipelines**: Consistent build environments.
- **Local Development**: Replicate production setups.

Troubleshooting

- **Debug a crashing container**:
  ```
  docker logs <container>
  docker run -it --entrypoint sh <image>  # Override entrypoint
  ```
- **Clean up resources**:
  ```
  docker system prune -a  # WARNING: Deletes unused images/networks/volumes
  ```

Kubernetes

Kubernetes:

- Kubernetes is an open-source Container orchestration platform that automates the deployment, management, scaling, and networking of containers across the cluster.
- It is focused on managing the life cycle of containers. It schedules, run, manage isolated containers which are running on virtual/physical/cloud machine
- Kubernetes is a cluster. Cluster is a group of nodes, that run containerized applications.

Docker is container platform
Kubernetes is a container orchestration platform
Orchestration tool = Container Management tool

Docker
Docker has container runtime, it will allow to run container or manage the life cycle of the container.
Container is ephemeral - short life or lived, containers can die or revive anytime.

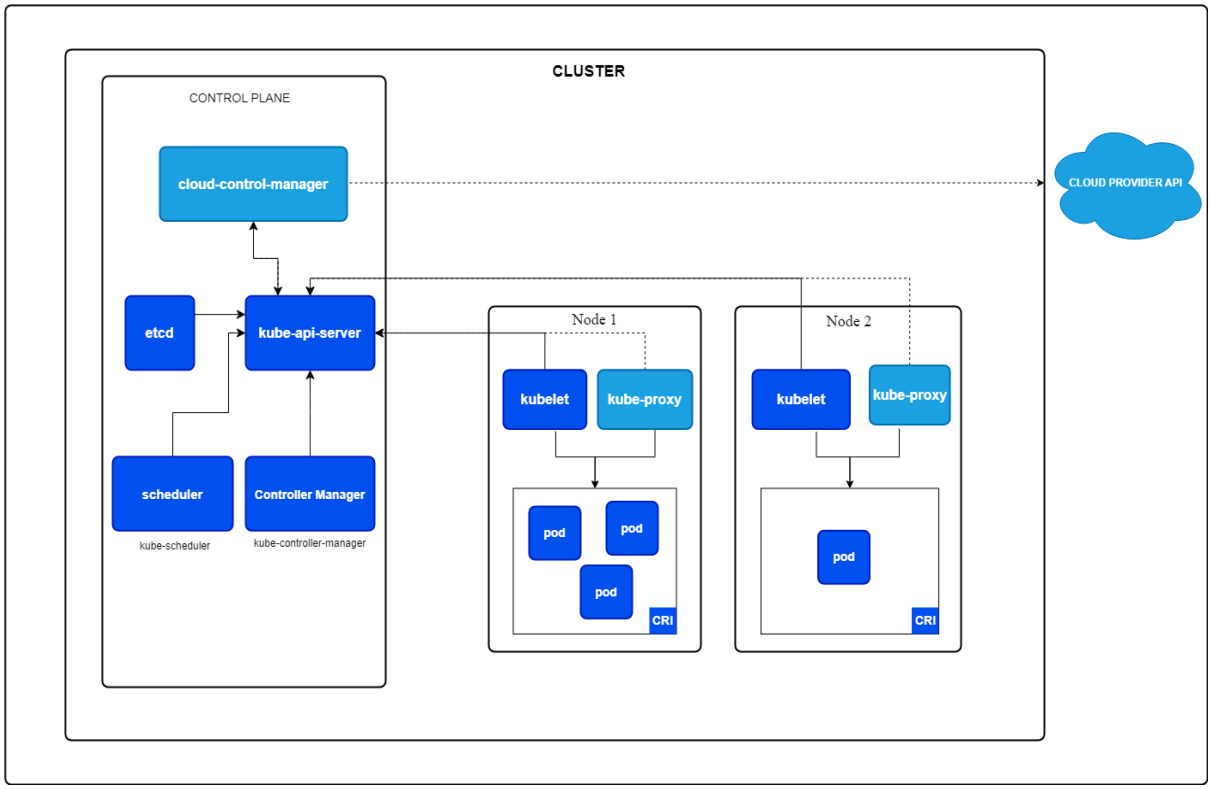
- Problem with scaling up the container:
- can't communicate with each other.
- Auto scaling and auto healing
- load balancing
- container had to be managed carefully.
- Single host nature of docker container
- **Enterprise level support**.
    - Auto scaling
    - Auto healing
    - Load balancer support
    - Firewall support
    - Api support gateways
    - White listing
    - Black listing

Advantages for k8s:

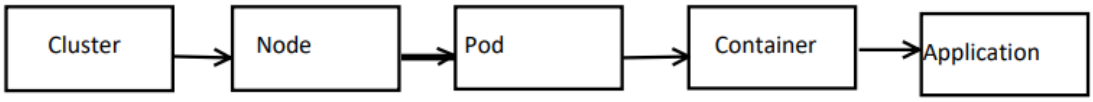
- **Container Orchestration:** It automates the management of containers running across a cluster of machines. Kubernetes ensures that containers are deployed, scaled, and maintained consistently.
- **Auto Scaling**: Kubernetes can automatically scale applications up or down based on resource utilization (like CPU or memory) or other custom metrics.
- **Auto Healing:** Kubernetes automatically replaces failed containers, restarts them, or reschedules them as necessary, ensuring the application remains available.
- **Load Balancing:** It automatically distributes incoming traffic to containers to ensure that no single container is overwhelmed, improving the overall performance and availability.
- **Service Discovery and Networking:** Kubernetes helps containers communicate with each other by providing a DNS-based service discovery system.
- **Platform independent (cloud/virtual/physical)**
- **Fault tolerance (node/pod failure)**
- **Rolling application upgrades and downgrades with zero downtime (Rolling back)**
- **Health Monitoring of pod**
- **Updates/new release/deployment**

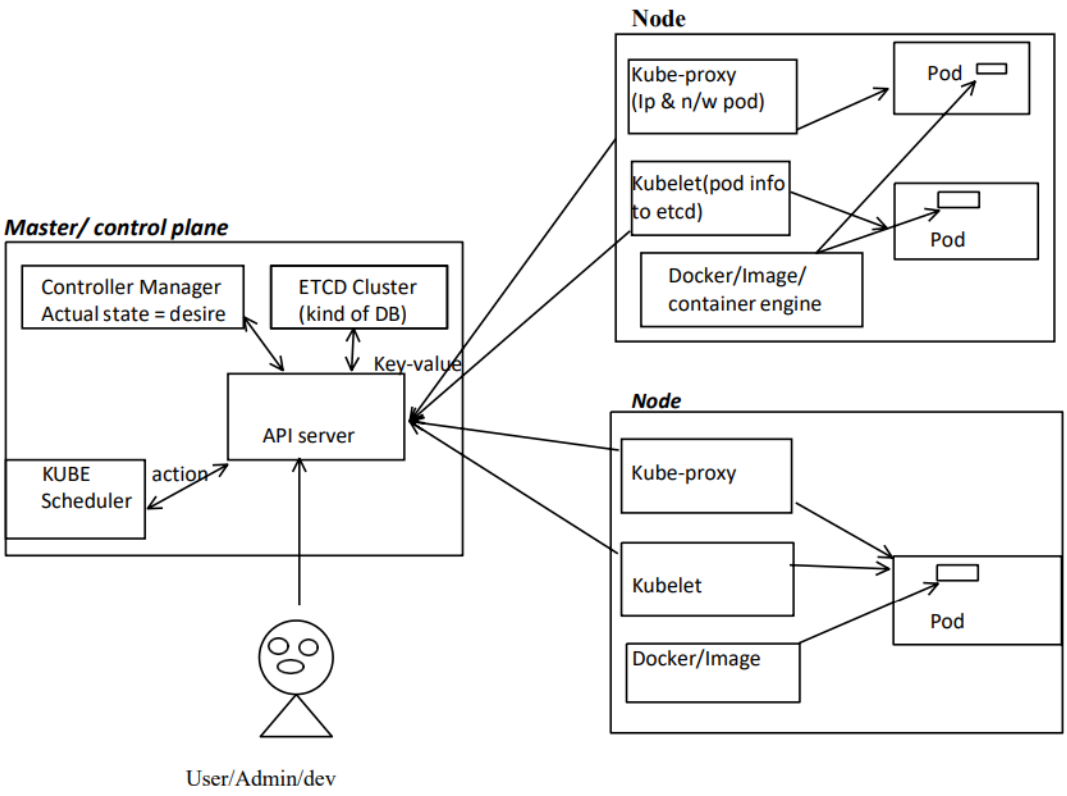
- **Secrete/config (master node)**

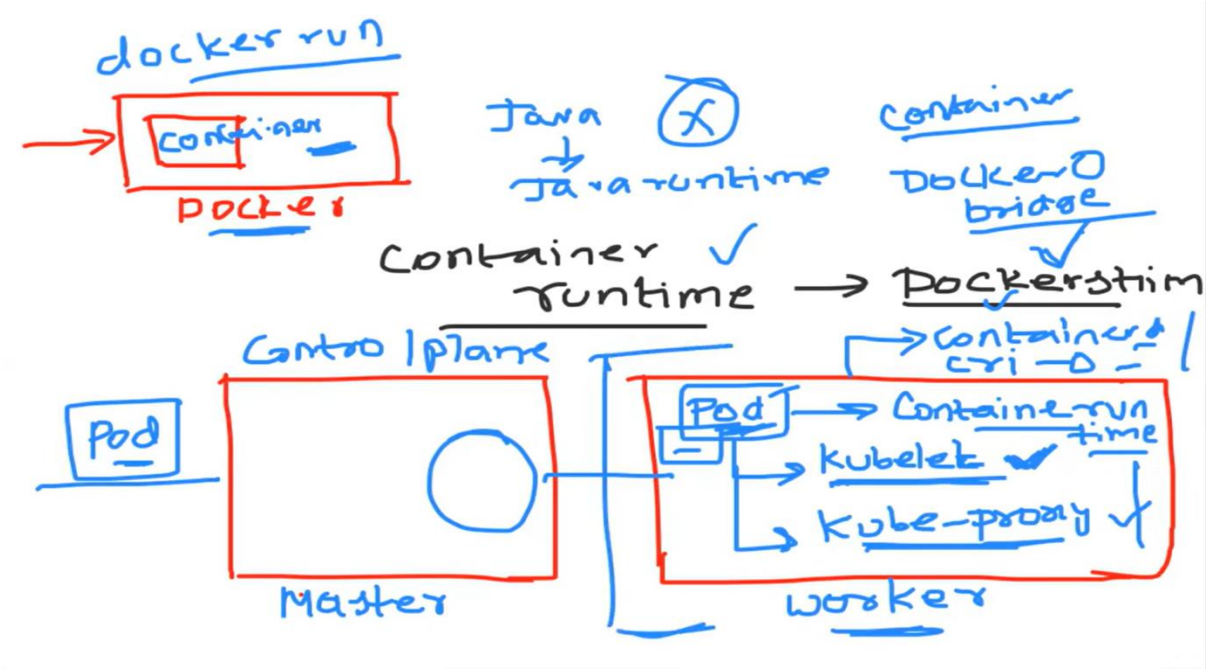
Kubernetes architecture:



Request flow High Level Diagram







Kubernetes architecture allows Kubernetes to provide a scalable, reliable, and flexible platform for managing containerized applications

Kubernetes Workflow:

1. **User interacts with the API server** (using kubectl or other tools).
2. **API server** processes the request and stores the data in etcd.
3. **Scheduler** assigns Pods to appropriate nodes based on resources and constraints.
4. **Kubelet** ensures that containers are running on the nodes.
5. **Kube Proxy** manages network traffic between services and Pods.

Role Of Master:

Kubernetes cluster runs on VM / BareMetal / cloud or mix.
1. K8s having one or more master and one or more workers.
2. The master is now going to run set of k8s process. These process with ensure smooth functioning of master these processes are called control plane
3. Can be multi master for high availability
4. Master runs control plane to run cluster smoothly.

Components Of master plane:

1. API Server
2. ETCD (not part of k8s but without this k8s won't work so consider this also a part of k8s)
3. Kube Scheduler
4. Kube Controller Manager
5. Cloud Controller Manager

1. API Server:

- The API server is a component of the Kubernetes control plane that exposes the Kubernetes API and it is responsible for **handling RESTful API requests**. The API server is the **front end** for the Kubernetes control plane.
- The API server authenticates and authorizes the request, and then sends the request to the relevant K8s components
- It validates and configures API objects (e.g., pods, services, deployments) via the kubectl command-line tool or client libraries.

2. ETC:

- It will **store the entire cluster information as a objects or key value pair.**
- It stores all Kubernetes objects (e.g., Pods, Deployments, Services) and ensures data consistency across the entire cluster.
- A key-value store that stores the configuration data of the cluster, including configurations, secrets, and state of the cluster information.

Features:

a) **Fully replicated:** entire state is available on every node of cluster
b) **Secure:** implements TLS with optional client-certificate authentication
c) **Fast:** benchmark at 10,000 writes per second

3. Kube Scheduler:

- The **Kube Scheduler** is responsible for scheduling the Kubernetes resources or pods on worker nodes.

- It will assign newly created Pods to nodes based on resource availability and policies **or [**based on resource requirements and other constraints (e.g., availability of resources, node affinity, taints/tolerations).**]**

4. Kube Controller Manager:

- The controller manager is responsible for ensuring that **the desired state of the cluster same as the actual state.**
- This component **runs controllers** that manage the state of the cluster. It **watches** the state of the cluster through the **API server** and makes changes to reach the desired state. Examples of controllers include the **Replication Controller** and **Deployment Controller**.
- **Controller** will ensure that the actual state in the yaml manifest is same as desired state.

  Controller Manager types:
  - Service controller
  - Pod controller
  - Ingress controller
  - Deployment controller
  - Replicaset controller
  - DaemonSet controller
  - Job Controller (Kubernetes Jobs)
  - CronJob Controller
  - endpoints controller
  - namespace controller
  - service accounts controller.
  - Node controller

- It manages all the controllers.
- You can extend Kubernetes with **custom controllers** associated with a custom resource definition.

Controller Components:

a) **Node Controller:** for checking of nodes that has detect in cloud after it's stop responding
b) **Route Controller:** Responsible to setting up n/w, route
c) **Service Controller:** Responsible for load balancing
d) **Volume Controller:** Managing Volumes

5. Cloud Controller Manager:

- This component integrates Kubernetes with cloud provider APIs to manage cloud specific resources (e.g., load balancers, storage, etc.)
- The cloud controller manager acts as a bridge between Cloud Platform APIs and the Kubernetes cluster.

Components Of Worker Plane:

1. Kube Proxy
2. Kubelet

3. Pods
4. Container Engine

1. Kube Proxy:

- The **Kube Proxy** is responsible for maintaining network rules for pod communication.
- **Kube Proxy** implements networking rules defined by the API server and ensures that network requests (traffic) are routed to the correct pods across different nodes.
- It manages load balancing and routing the network traffic between services in the cluster.
- It provides networking, IP address and load balancing capabilities to pods.
- This component will distribute to pods
- It runs on each node

2. Kubelet:

- It helps to interact with different Kubernetes services.
- This is responsible for creation of pods and ensuring that pods are in running state.
- **Kubelet** is an **agent** that runs on each worker node and ensures that **containers are running and healthy in a pod** as expected by communicating with the API server to receive instructions and report back the current state of pods.
- Kubelet will check the pods health status.
- The health of pods is checked using **liveness probes** and **readiness probes**. These probes are configured in the pod's definition and helps to ensure the application inside the pod is running properly and can handle requests.

3. Pods:

- Pods are the Kubernetes objects.
- Pods are the smallest deployable units in Kubernetes that can contain one or more containers, which share the same network and storage resources.
- Pod having it’s IP address but container don't have
- Auto scaling and auto healing by default not provided by pod. For this high level k8s object required

4. Container Engine or Runtime:

- The container runtime is responsible for running and managing containers on the worked node. Kubernetes supports several container runtimes, including Docker, containerd, CRI-O and docker shim (Docker runtime)
- Kubernetes interacts with the container runtime via the **Container Runtime Interface (CRI)**.

Kubernetes Cluster Addon Components

- Apart from the core components, the Kubernetes cluster needs addon components to be fully operational. Choosing an addon depends on the project requirements and use cases.

Following are some of the popular addon components that you might need on a cluster.

1. **CNI Plugin (Container Network Interface):** Manages networking for containers, ensuring seamless communication between pods.
2. **CoreDNS (For DNS server):** Acts as Kubernetes built-in DNS server, enabling **DNS-based service discovery** for pods and services.
3. **Metrics Server (For Resource Metrics):** This addon helps to collect performance data and resource usage of Nodes and pods in the cluster.
4. **Web UI (Kubernetes Dashboard):** This addon enables the Kubernetes dashboard to manage the object via web UI.

1. CNI Plugin

What is CNI?

- Container Networking Interface (**CNI**) is a **plugin-based architecture** with vendor-neutral specifications that provide networking capabilities for containers.
- It standardizes container networking across different **container orchestration platforms** such
  - Kubernetes
  - Mesos
  - CloudFoundry
  - Podman
  - Docker
- It was originally designed by the Cloud Native Computing Foundation (CNCF) and is **not specific to Kubernetes**.

🌐 Why Use CNI?

Container networking requirements vary across organizations—some may need advanced **isolation**, **security**, **encryption**, or **scalability**. As container technology evolved, many networking vendors built **CNI-based solutions** to address these varied needs. These solutions are known as **CNI Plugins**.

How CNI Works with Kubernetes

1. **Pod CIDR Assignment**
   - The **Kube-controller-manager** assigns a **pod CIDR** (a unique range of IP addresses) to each node.
2. **Pod Launch via Kubelet**
   - **Kubelet** interacts with the **container runtime** to launch scheduled pods.
   - The **CRI plugin** (part of the container runtime) communicates with the **CNI plugin** to configure pod networking.
3. **Pod-to-Pod Networking**
   - The **CNI Plugin** ensures networking between **pods across different nodes** using an overlay network.

🔐 Key Features of CNI Plugins

1. **Pod Networking**
   - Handles IP address allocation, routing, and connectivity.
2. **Network Security & Isolation**
   - Uses **Network Policies** to control traffic flow between pods and namespaces.

Popular CNI Plugins

- **Calico** – Provides high-performance **networking and security** using BGP.
- **Flannel** – A simple overlay network solution for Kubernetes clusters.
- **Weave Net** – Offers automatic encryption and **peer-to-peer networking**.
- **Cilium** – Uses **eBPF** for efficient network security and observability.
- **Amazon VPC CNI** – Optimized for **AWS Kubernetes clusters**.
- **Azure CNI** – Integrates with **Azure Virtual Networks** for Kubernetes networking.

Kubernetes Networking Based on Hosting Platforms

- **Single Cloud Deployment** → Use kubectl.
- **On-Premise Deployment** → Use kubeadm.
- **Hybrid/Federated Kubernetes** → Use kubefed.

The difference between an object and a resource in Kubernetes.

Object

Anything a **user creates and persists in Kubernetes is an object**. For example, a namespace, pod, Deployment configmap, Secret, etc.

Resource

In Kubernetes, everything is accessed through APIs.
a **resource** is a **specific API URL** used to access an object, and they can be accessed through HTTP verbs such as GET, POST, and DELETE.

https://devopscube.com/kubernetes-objects-resources/

Kubernetes Objects

- **Pod**
- **Services**
- **Deployments**
- **Volume**
- **Namespace**
- **ReplicaSets**
- **Replica Controller**
- **Secrete**
- **Config Maps**
- **StatefulSets**
- **Jobs**
- **Daemon Sets**
- **Label**
- **Ingress**
- **Network**

1) Pod: A thin wrapper around one or more containers.
2) Service: Maps a fixed IP address to a logical group of pods
3) Volume: a directory with data that is accessible across multiple containers in a Pod
4) Namespace: a way to organize clusters into virtual sub-clusters
5) ReplicaSets: Ensure high availability. Ensures a defined number of pods are always running.
6) Replica Controller: Ensures a defined number of pods are always running
7) Secrets: an object that contains a small amount of sensitive data such as a password, a tok1en, or a key
8) Config Maps: Manage app config. an API object that lets you store configuration for other objects to use
9) Deployments: Deployment-manage app updates.
10) StatefulSets: Manage stateful app the workload API object used to manage stateful applications.
11) Jobs: Run & scheduled jobs. Ensures a pod properly runs to completion and stop after process complete it's execution
12) Daemon Sets: Running on each node. Implements a single instance of a pod on all (or filtered subset of) worker node(s).
13) Label: Key/Value pairs used for association and filtering

1) Pod:

- Pods are the Kubernetes objects
- The smallest deployable units in Kubernetes that can contain one or more containers, which **share the same network and storage (volumes) resources.**
- Pods are often ephemeral.
- Each pod is assigned a unique IP address within the cluster.
- **K8s uses YAML file to describe the desired state** of the containers in a pod. This is also called a **Pod Spec**. These objects are passed to the kubelet through the API server.

Imperative vs Declarative commands

- Kubernetes API defines a lot of objects/resources, such as namespaces, pods, deployments, services, secrets, config maps etc.
- There are two basic ways to deploy objects in Kubernetes: **Imperatively and Declaratively**

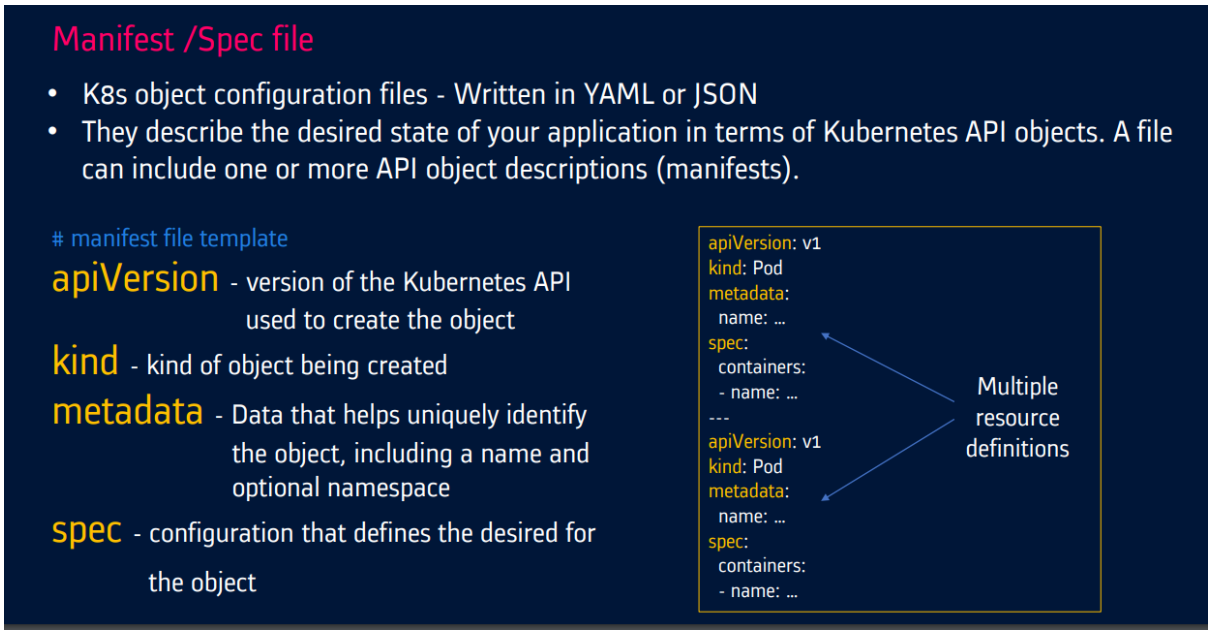
Imperatively Management:

- Involves using any of the verb-based commands like kubectl run, kubectl create, kubectl expose, kubectl delete, kubectl scale and kubectl edit
- Suitable for testing and interactive experimentation

Declaratively Management:

- Objects are written in **YAML files** and deployed using **kubectl create or kubectl apply**
- Best suited for production environments

Manifest /Spec file



Annotations

- **Annotations** are key-value pairs that provide metadata about objects. Unlike labels, which are used to select and organize resources.
- **Annotations** are used to **store non-identifying information** that can be used by tools and libraries.

Eg:
Pod example with annotations, multiple containers, and environment variables

```
apiVersion: v1
kind: Pod
metadata:
  name: Pod examples annotations, multiple containers, environment variables
# Basic Pod configuration with Pod name
  annotations:
    description: "This is an example Pod with annotations."
    config.checksum: "123456789"
    prometheus.io/scrape: "true"
    prometheus.io/port: "8080"
spec:
  containers:
  - name: main-container        # First container in the Pod
    image: nginx
    env:
    - name: MAIN_ENV_VAR
```

```
      value: "MainContainerValue"
  - name: sidecar-container     # Second container in the Pod
    image: busybox
    command: ["sh", "-c", "echo Hello from the sidecar container; sleep 3600"]
    env:                        # Pod Example with Environment Variable
    - name: SIDECAR_ENV_VAR
      value: "SidecarContainerValue"
```

Pod Lifecycle

1.Pending: The Pod is created but not yet running. This happens while Kubernetes schedules the Pod to a node.
2.Running: The Pod is successfully scheduled and all containers are running or in the process of starting.
3.Succeeded: All containers in the Pod have terminated successfully (exit code 0).
4.Failed: At least one container in the Pod has terminated with a non-zero exit code.
5.Unknown: The state of the Pod cannot be determined.

Pod Health check:

The health of pods is checked using **liveness probes** and **readiness probes**. These probes are configured in the pod's definition and help ensure the application inside the pod is running properly and can handle requests.

Liveness Probe

A liveness probe is used to **check if the application inside the pod is still running**. If the liveness probe fails, Kubernetes will restart the pod to try to recover the application.
Example of a liveness probe configuration:

```
livenessProbe:
  httpGet:
    path: /healthz
    port: 8080
  initialDelaySeconds: 3
  periodSeconds: 3
```

Readiness Probe

A readiness probe is used to **check if the application inside the pod is ready to handle requests**. If the readiness probe fails, the pod will be removed from the service's load balancer until it becomes ready again.
Example of a readiness probe configuration:

```
```

```
readinessProbe:
  httpGet:
    path: /ready
    port: 8080
  initialDelaySeconds: 3
  periodSeconds: 3
```

Types of Probes

Kubernetes supports three types of probes:

1. **HTTP Probes**: Perform an HTTP GET request against a specified endpoint.
2. **Command Probes**: Execute a command inside the container and check the exit code.
3. **TCP Probes**: Perform a TCP check against a specified port.

Example Configuration

Here is an example of a complete pod configuration with liveness and readiness probes:

```
apiVersion: v1
kind: Pod
metadata:
  name: example-pod
spec:
  containers:
  - name: example-container
    image: my-application:latest
    livenessProbe:
      httpGet:
        path: /healthz
        port: 8080
      initialDelaySeconds: 3
      periodSeconds: 3
    readinessProbe:
      httpGet:
        path: /ready
        port: 8080
      initialDelaySeconds: 3
      periodSeconds: 3
```

These probes help ensure that your application is running smoothly and can recover from failures automatically.

Pod contains single container or multiple containers.

Multiple containers

1. Init container.
2. Side-car container

By utilizing **init and sidecar containers**, we can create more robust and flexible deployments that meet the specific needs of your applications.

Init container.

- **Init containers** are special containers that **runs before the main application containers** in a pod.
- These containers are used to perform setup tasks (such as configuration, initialization, or data preparation) that need to be completed before the main application begins running.
- **Containers will delete, post complete the task** and only the main container will remain the same.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-with-init-container
spec:
  initContainers:
  - name: init-myservice
    image: busybox
    command: ['sh', '-c', 'echo Initializing; sleep 10']
  containers:
  - name: my-app-container
    image: nginx
```

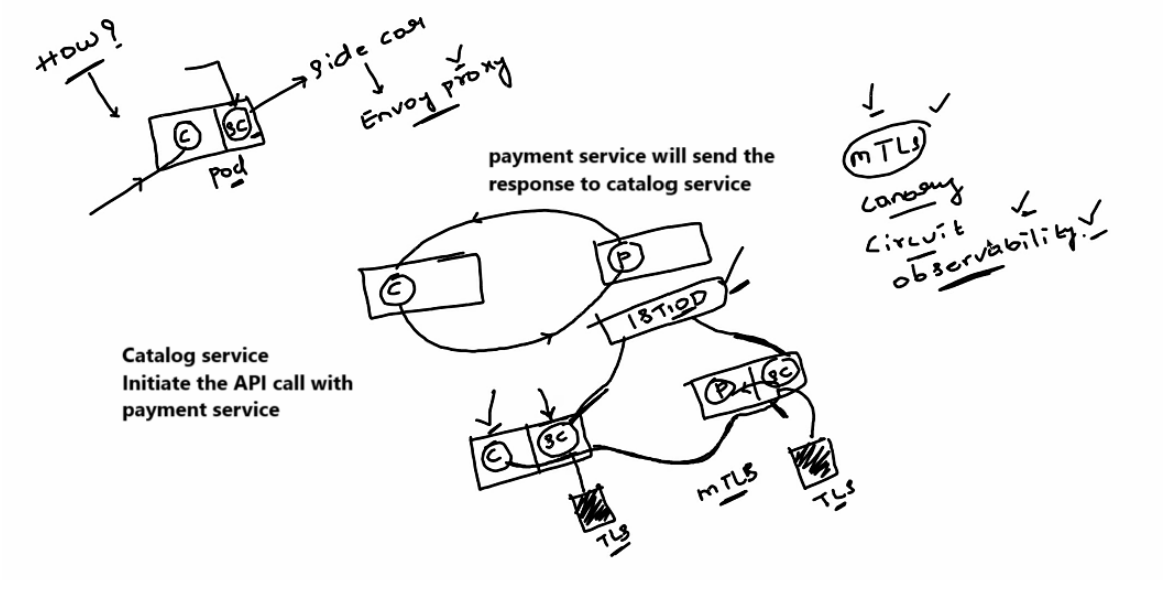
Use cases

- **Initializing shared volumes**
- Data Initialization
- Changing the file system before starting the app container
- Performing **automation backup** before starting an application.
- **Waiting for Dependencies to Be Ready**
  Scenario: A web application that depends on a database being initialized first.
- **Initializing Configurations or Secrets**: Pulling secrets from a vault and storing them in the application configuration file
  Scenario: A containerized application that needs to fetch secrets or configuration files from a centralized service (e.g., AWS SSM or HashiCorp Vault).
- **Preparing Data for the Main Application:**
  Scenario: A container that runs a web application that needs to download an initial set of data or files (like JSON or CSV files) from an external server or cloud storage.

Side-car container

- Sidecar containers are **secondary containers** within the same Pod that **runs alongside the main application container.**

- Sidecar containers extend the functionality of the main container by providing additional services, such as logging, monitoring, proxying, security, or data synchronization.
- Side car container contains envoy proxy application. It is proxy server it will handles the traffic management of pods.




```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-with-sidecar
spec:
  containers:
  - name: main-app
    image: nginx
  - name: sidecar-logging
    image: busybox
    command: ['sh', '-c', 'tail -f /var/log/nginx/access.log']
    volumeMounts:
        - name: log-volume
          mountPath: /logs
  volumes:
    - name: log-volume
      emptyDir: {}
```

Use Cases:

- **Logging (Fluentd, Elasticsearch)**: A sidecar container can be responsible for gathering logs from the main container and sending them to a logging system or processing them.
- **Monitoring (Metrics and Health Checks)**: A sidecar might collect metrics or health information from the main container for external monitoring purposes.
- **Proxying (Service Proxy or Service Mesh)**: A sidecar container can act as a proxy or a service mesh component (e.g., Istio sidecar) to manage inbound/outbound traffic for the main application container.
- **Security and Identity Management (Secret Injection and Identity Management)**: Sidecars can provide security features like injecting secrets into the environment of the main container.
- **Networking/Proxying (API Gateway/Proxying Requests):** Sidecar containers can serve as proxies or API gateways to route requests between services, for example, caching, rate limiting, or transforming requests.

When to Use Sidecar Containers

- **Sidecar Containers:** Use sidecar containers to add additional functionalities to your application, such as logging, monitoring, or communication proxies, without modifying the main application.

Feature	Init Containers	Sidecar Containers
Execution Time	Runs before the main container starts.	Runs alongside the main container during its lifecycle.
Primary Purpose	Initialization or setup tasks.	Auxiliary tasks that extend functionality (e.g., logging, proxying).
Example Use Cases	Waiting for dependencies, data migration.	Collecting logs, monitoring, proxying traffic.

Type of pods:

1. **Single-container Pods:**
   This is the simplest form of a Pod, containing only one container.
2. **Multi-container Pods:**
   These Pods contain **multiple containers** that need to work together.
3. **Static Pods:**
   Static pods are managed directly by the kubelet on a specific node, rather than through the API server. They are defined in the kubelet's configuration. **(kube-apiserver, etcd, kube-controller-manager, kube-scheduler)**
4. **Ephemeral Pods:**
   Ephemeral containers are used for troubleshooting running pods. They can be added to a pod without restarting it and are removed once the troubleshooting is complete.
5. **Guaranteed Pods:**
   These Pods are designed with **resource guarantees** (CPU and memory) in mind. Kubernetes will ensure that the requested resources are available.
6. **Pod Templates:**
   While not exactly a separate type of Pod, Pod templates are used to define a blueprint for creating Pods.

2) Service

Service:

- **Services:** Services in Kubernetes enables communication between Pods and external clients. They expose applications running inside Pods as **network services**.
- **Load Balancing and Health Monitoring:** A Service is a **round-robin load balancer** for Pods that match its labels or selector, and constantly monitors the Pods. If any Pod becomes unhealthy, the Service reroutes traffic to healthy Pods.
- **Stable Network Endpoint**: Services object provides a **stable network endpoint** to access a **set (group) of Pods**, along with **service discovery and load balancing**.
- Kubernetes **automatically distributes traffic between Pods** and provides **DNS resolution** for Service hostnames.
- Services provide **stable networking, load balancing, and service discovery**, ensuring **consistent communication within the cluster**, even when Pods are dynamically created, scaled, or replaced.
- Service objects is a logical bridge between pods and end user, which provide virtual IP
- **Scalability and Flexibility:** These features are designed to be **scalable, reliable**, and **flexible**, making it easier for developers to manage and orchestrate complex microservices architectures.
- **External Access:** Additional features like **Ingress** and **DNS-based service discovery** provide flexible external access to services and simplify service discovery within the cluster.
- **Networking plugins and configuration** options enable pod-to-pod communication and network isolation.
- Kubernetes uses a combination of **DNS-based service discovery** and **a built-in load balancer** called **kube-proxy**. Each Service is assigned a **unique DNS name**, which resolves to the cluster IP. The kube-proxy component load balances traffic across the Pods associated with the Service, distributing requests evenly.

Why Do We Need Services in Kubernetes?

If service is not available, due some issues, pod has deleted and created again because of auto healing. Pod IP address will change automatically, if IP address changes, we will not able to access the application with old IP address. To overcome this problem, we will create a service yaml file, it will interact with pods using labels and selectors. If any requested came, service file with communication with pods using the labels and selectors.

a) **Pods are Ephemeral:** Pods are temporary and can be destroyed or recreated for reasons like scaling, updates, or failures. Each new Pod gets a different IP address, making direct communication with Pods unreliable.

b) **Stable Communication:** Services provide a consistent way to access the Pods, regardless of changes in the underlying Pods IPs.

c) **Load Balancing:** Services distribute network traffic across multiple Pods.
d) **Service Discovery:** Simplifies communication between Pods by using stable IP addresses and DNS names.

Types of Kubernetes Services:

1. **ClusterIP (default):**
   - Exposes the Service on an internal IP address within the cluster.
   - It allows other Pods inside the cluster to communicate with it, but it's not accessible outside the cluster.
   - **Use case**: Internal communication between services within the cluster.

```yaml
kind: Deployment
apiVersion: apps/v1
metadata:
  name: httpddeployment
spec:
  replicas: 1
  selector: # tells the controller which pods to watch/belong to
    matchLabels:
      name: httpddeployment
  template:
    metadata:
      name: testpod1
      labels:
        name: httpddeployment
    spec:
      containers:
        - name: c00
          image: httpd
          ports:
            - containerPort: 80
---
kind: Deployment
apiVersion: apps/v1
metadata:
  name: ubuntudeployment
spec:
  replicas: 1
  selector: # tells the controller which pods to watch/belong to
    matchLabels:
      name: ubuntudeployment
  template:
    metadata:
      name: testpod2
      labels:
        name: ubuntudeployment
    spec:
```

```
      containers:
        - name: c01
          image: ubuntu
          command: ["/bin/bash", "-c", "while true; do echo Hello-sagar; sleep
5 ; done"]
---
kind: Service # Defines to create Service type Object
apiVersion: v1
metadata:
  name: demoservice
spec:
  ports:
    - port: 80 # Containers port exposed
      targetPort: 80 # Pods port
  selector:
    name: httpddeployment # Apply this service to any pods which has the
specific label
  type: ClusterIP # Specifies the service type i.e ClusterIP or NodePort
```

2. **NodePort**:
    - Exposes the Service on each Node's IP address at a static port.
    - Pods can accessible from outside the cluster using **<NodeIP>:<NodePort>.**
    - Expose the service on the same port of each selected node in the cluster using NAT.
    - It allows external traffic to access the service by connecting to **<NodeIP>:<NodePort>.**
    - **Use case**: When you need external access to your service (but not via LoadBalancer) and you can target specific Node IPs.

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: httpddeployment
spec:
  replicas: 1
  selector: # tells the controller which pods to watch/belong to
    matchLabels:
      name: httpddeployment
  template:
    metadata:
      name: testpod1
      labels:
        name: httpddeployment
    spec:
      containers:
        - name: c00
```

```
          image: httpd
          ports:
            - containerPort: 80
---
kind: Service # Defines to create Service type Object
apiVersion: v1
metadata:
  name: demoservice
spec:
  ports:
    - port: 80 # Containers port exposed
      targetPort: 80 # Pods port
  selector:
    name: httpddeployment # Apply this service to any pods which have this
specific label
  type: NodePort # Specifies the service type i.e ClusterIP or NodePort
```

3. **LoadBalancer**:
    - A service that distributes network traffic across multiple Pods.
    - Exposes the Service externally using an external (cloud provider's) load balancer.
    - This type of Service is accessible from outside the cluster, mainly via a public IP address.
    - **Use case**: To expose a service to the internet with automatic load balancing across Pods.

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: httpddeployment
spec:
  replicas: 1
  selector: # tells the controller which pods to watch/belong to
    matchLabels:
      name: httpddeployment
  template:
    metadata:
      name: testpod1
      labels:
        name: httpddeployment
    spec:
      containers:
        - name: c00
          image: httpd
          ports:
            - containerPort: 80
```

```yaml
---
kind: Service # Defines to create Service type Object
apiVersion: v1
metadata:
  name: demoservice
spec:
  ports:
    - port: 80 # Containers port exposed
      targetPort: 80 # Pods port
  selector:
    name: httpddeployment
  type: LoadBalancer
```

4. **ExternalName**:
    - This Service type maps a service to an external DNS name (such as example.com), without exposing any Pods.
    - **Use case**: When you want Kubernetes to forward traffic to an external service by DNS name instead of managing Pods directly.

```yaml
apiVersion: v1
kind: Service
metadata:
  name: example-externalname-service
spec:
  type: ExternalName
  externalName: my.database.example.com
```

- **selector**: This defines which Pods the Service will route traffic to (those with label app=exmaple-app).
- **port**: The port on the Service (80 in this case).
- **targetPort**: The port on the Pods that the Service will forward traffic to (8080 in this case).

Feature	ClusterIP	NodePort	LoadBalancer
Exposition	Exposes the Service on an internal IP in the cluster.	Exposing services to external clients	Exposing services to external clients
Cluster	This type makes the Service only reachable from within the cluster	A NodePort service, each cluster node opens a port on the node itself (hence the name) and redirects traffic received on that port to the underlying service.	A LoadBalancer service accessible through a dedicated load balancer, provisioned from the cloud infrastructure Kubernetes is running on
Accessibility	It is **default** service and Internal clients send requests to a stable internal IP address.	The service is accessible at the internal cluster IP-port, and also through a dedicated port on all nodes.	Clients connect to the service through the load balancer's IP.
Yaml Config	`type: ClusterIP`	`type: NodePort`	`type: LoadBalancer`
Port Range	Any public ip form Cluster	30000 - 32767	Any public ip form Cluster

How Services work internally:

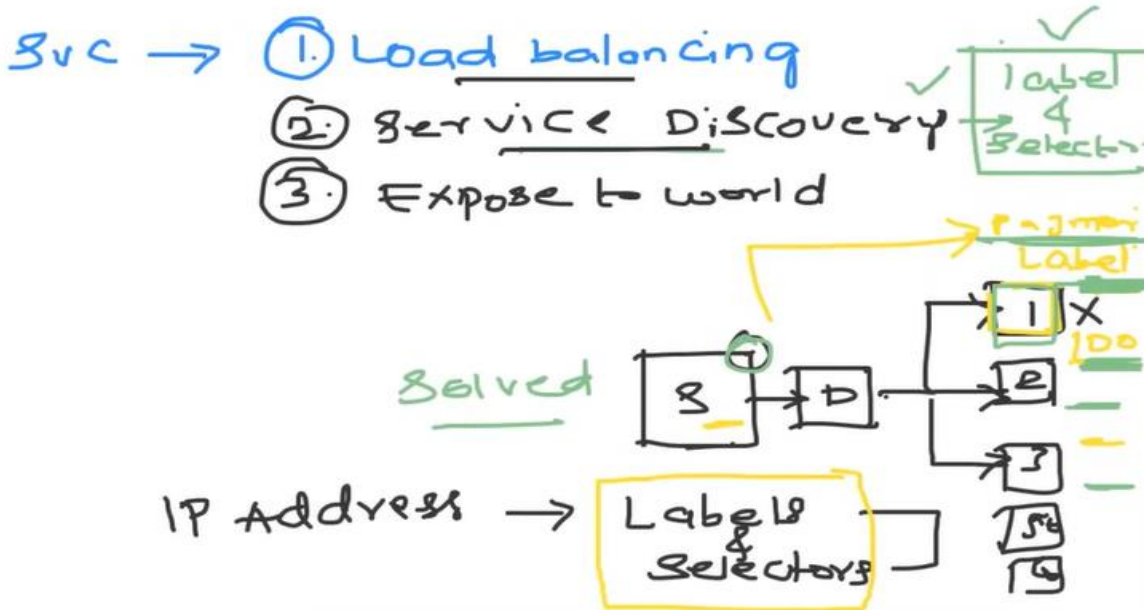
1. **Service Label Selector**: A Service identify the set of Pods using label selectors.
2. **End Points Object**: Kubernetes creates an Endpoints object, which keeps track of the IPs of the Pods selected by the label selector and Kubernetes automatically adjusts the endpoints when Pods are added or removed.
3. **Service Proxying (Routing)**: Kubernetes uses **kube-proxy** to route traffic to the Service and forward it to the appropriate Pod. **kube-proxy** uses methods like **iptables or IPVS for load balancing.**

Key Features of Kubernetes Services:

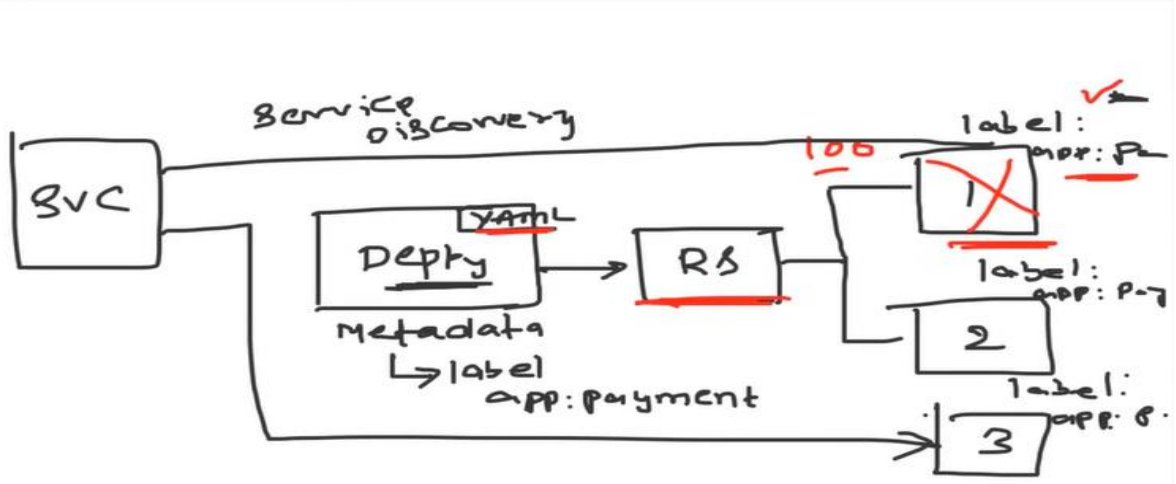
- **Stable Endpoint**: Services provide stable IP addresses and DNS names to access Pods.
- **Discovery and Load Balancing:** Kubernetes Services allow clients to discover and communicate with the right Pods using DNS-based service discovery and label selectors, while automatically distributing traffic across Pods through load-balancing mechanisms.
- **Selector and Labels:** A Service uses selectors to identify which Pods it should target. Pods with labels that match the selector will automatically become part of the Service.

Service responsibilities.

- Load balancing
- Service discovery mechanism (using labels and selectors)
- Expose to the external world.

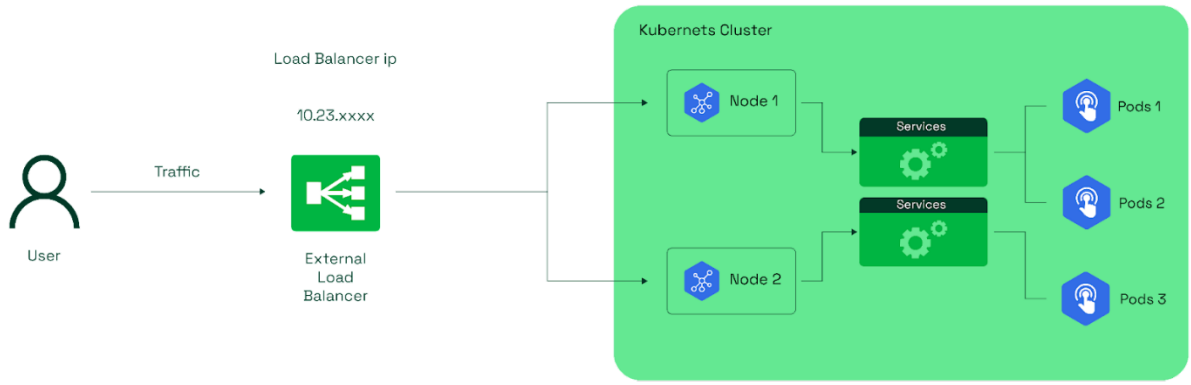


Service discovery



Load Balancer:

- A **LoadBalancer** service **provisions an external load balancer** to **expose applications** to **external traffic** and **distribute incoming network traffic** across multiple pods or nodes within the cluster, ensuring **reliability and scalability**.
- The Load Balancer will **forward the traffic** to the available nodes in the cluster on **the nodePort** assigned to the service
- Kubernetes offers **three types** of **load balancing algorithms** for Services, which distribute traffic based on **round-robin, least connections, or IP hash.**
- Load balancing is an essential part of Kubernetes networking, providing efficient and reliable traffic distribution across a cluster.



Eg:

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: httpddeployment
spec:
  replicas: 1
  selector: # tells the controller which pods to watch/belong to
    matchLabels:
      name: httpddeployment
  template:
    metadata:
      name: testpod1
      labels:
        name: httpddeployment
    spec:
      containers:
        - name: c00
          image: httpd
          ports:
            - containerPort: 80
---
kind: Service # Defines to create Service type Object
apiVersion: v1
metadata:
  name: demoservice
```

```yaml
spec:
  ports:
    - port: 80 # Containers port exposed
      targetPort: 80 # Pods port
  selector:
    name: httpddeployment
  type: LoadBalancer
```

LoadBalancer Use-cases in K8s

- Expose your applications to the public internet.
- Traffic distribution across Nodes and Pods

How Load Balancer works in K8s?

- A load balancer service is created, which identifies the cloud platform
- The cloud provider generates a load balancer with a unique IP address
- The load balancer distributes client requests to the appropriate nodes hosting the pods
- Configure LoadBalancer as Service
- Distribute traffic to external IP

Advantages of Load Balancer:

- **Automatic provisioning:** Simplifies exposing services externally.
- **Traffic distribution:** Automatically balances traffic across pods.
- **Managed service:** Especially useful in cloud environments where you don't need to manually configure or maintain the load balancer.

Types of LoadBalancer:

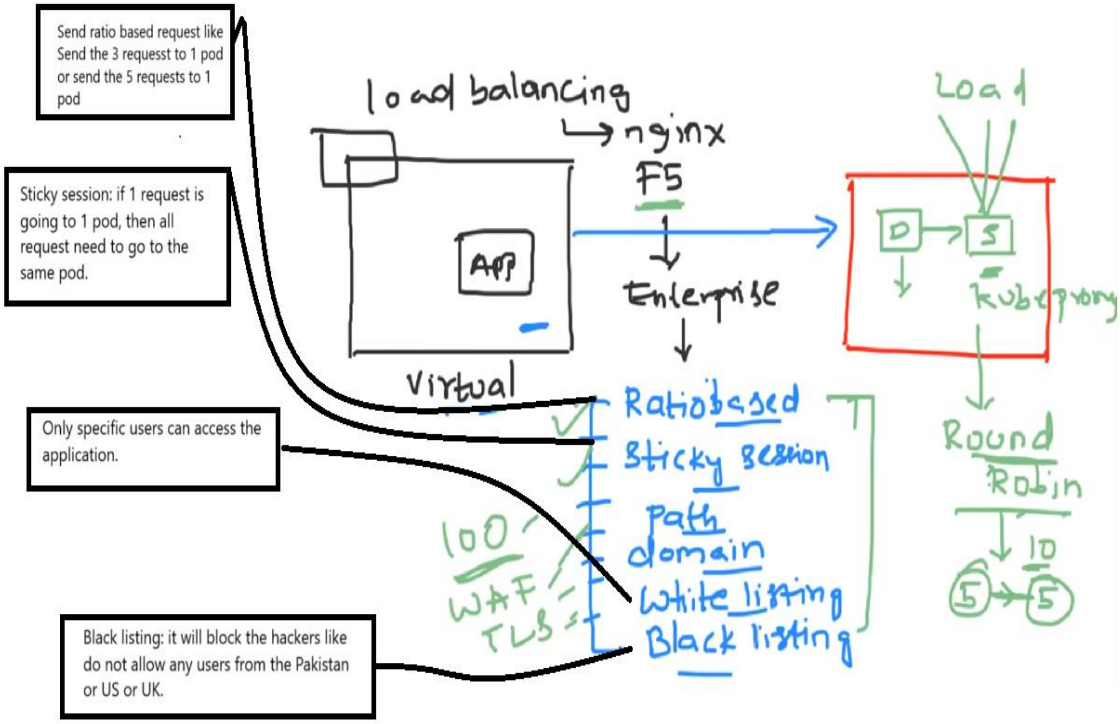
AWS: Elastic Load Balancer (ELB)

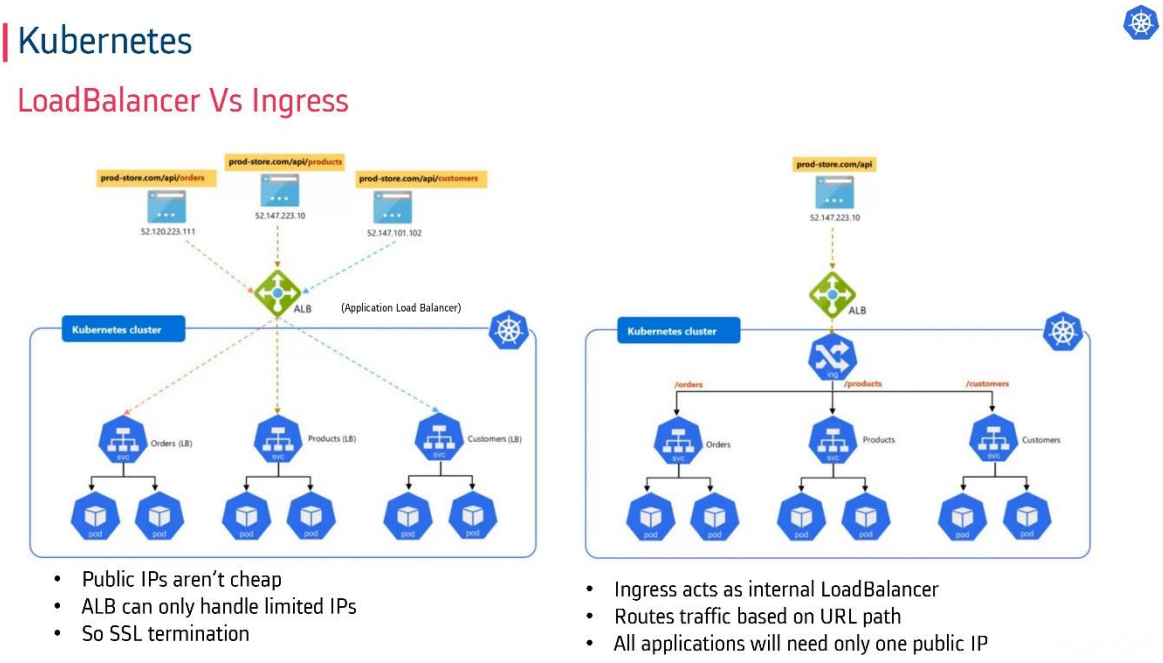
i) Application Load Balancer (ALB)
ii) Network Load Balancer (NLB)
iii) Classic Load Balancer (CLB).

Summary of Key Types:

- **Cloud Provider Managed Load Balancer:** Automatically provisions and manages external load balancers.
- **Internal Load Balancer:** Used for internal traffic within the cluster (cloud environment).
- **MetalLB:** A load balancer solution for bare-metal Kubernetes clusters.
- **Ingress Controller:** Manages routing of HTTP(S) traffic via rules and works with external load balancers.
- **Layer 4 Load Balancer:** Routes traffic based on IP address and port (TCP/UDP).
- **Layer 7 Load Balancer:** Routes traffic based on content of the request (HTTP/S).
- **DNS Load Balancer:** Distributes traffic via DNS resolution, often used for geo-distribution.
- **Global Load Balancer:** Distributes traffic across geographically distributed data centres.

In Virtual machines





Load balancer limitations:

- Limited URL routing
- Cloud provider dependent.
- Lacks SSL termination.

- It doesn't support URL rewriting and rate limiting.
- Enterprise level support and TLS Loadbalancer capabilities.
  (Ratio Based routing, Sticky, path, domain, writing listing and black listing-based routing.)
- Loadbalancer static IP address will be charged by cloud provider. if we created more loadbalancer static IP address

Ingress, Routes and Ingress Controllers:

Load Balancer Type Service

Q: Is Load Balancer service type only restricted to Cloud providers?
A: Bare Metal LB Implementation - https://github.com/metallb/metallb

Q: If Load Balancer service type can do the thing for you, why use an Ingress resource?

A. 1. If you have the large-scale ecommerce application, consider it has 200 to 300 services, if you want to user cloud provider load balancer, then you must create 200 to 300 static external IP addresses, which will cloud provider will charge huge amount. To overcome you can create ingress resource, it will manage all services with one static external IP address.

2. It defines routing for specific service using host base routing and path-based routing, session-based routing, or cookies-based routing etc.

Before 2015, in K8s v1.1, it provides only basic load balancer support. Ingress concept is not there.

Load balancing mechanism is providing simple round robin mechanism, If 10 request come, if you have 2 pods, then round robin mechanism distribute it equal to 2 to pods. 5 requests must go to 1 pod and another request must go to another pod.

Ingress:

What is a Kubernetes Ingress?

- **Kubernetes Ingress** is an **API object** that manages external access to services within a cluster. It is primarily used to configure and manage HTTP and HTTPS routing to services running inside the cluster.
- Ingress **exposes HTTP and HTTPS endpoints** to external users and **routes incoming traffic to internal services** based on **rules defined** in the **Ingress resource**.
- **Traffic routing** is controlled by **rules defined** in the **Ingress resource** based on hostnames and paths. **(**Specifying how external traffic should be directed to internal services within the Kubernetes cluster.**)**
- **The ingress controller** is responsible for routing HTTP(S) traffic based on defined rules
- **Ingress Controllers** mainly **work alongside a load balancer** (often a cloud-managed one or MetalLB) to handle HTTP(S) traffic.
- Once the **Ingress controller** is installed on a Kubernetes cluster, it continuously watches for Ingress resources (like nginx.conf, where all the routing details are updated) within the cluster. Along with the Ingress controller, NGINX applications are also deployed.

- Compared to **NodePort** or **LoadBalancer services**, **Ingress** offers advanced features like **path-based** or **host-based routing**, providing more flexible traffic management.
- Ingress allows exposing multiple services using a single external IP or domain, combining features of both a LoadBalancer and an API Gateway.

Key Features:

- Used for HTTP(S) traffic routing, mainly for web applications.
- Works well with SSL termination (decrypting) and path-based routing.
- Involves more advanced routing, including features like URL rewriting, traffic splitting, and authentication.

How ingress works?

- **The ingress controller** is responsible for routing traffic based on defined rules.
- The **Ingress Controller** routes incoming requests based on URL paths or hostnames (e.g., /app1, api.example.com). It often sits behind a load balancer to distribute the traffic across multiple Pods or services.
- Manages routing of HTTP(S) traffic via rules and works with external load balancers.
- NGINX Ingress Controller, Traefik, and AWS ALB Ingress

Examples of Ingress Advantages and Use Cases:

- **Path-based routing**: Routes requests to different services based on the URL path. For example:
  - example.com/api goes to the api-service.
  - example.com/web goes to the web-service.
- **Host-based routing**: Routes traffic based on the requested domain name (hostname). For example:
  - app1.example.com routes to service1.
  - app2.example.com routes to service2.
- **SSL/TLS termination**: Handles HTTPS traffic, terminating (decrypting) SSL connections, reducing the burden on backend services. You can configure Ingress to terminate SSL and forward traffic as HTTP. SSL termination
- **Why SSL Termination at LoadBalancer?**

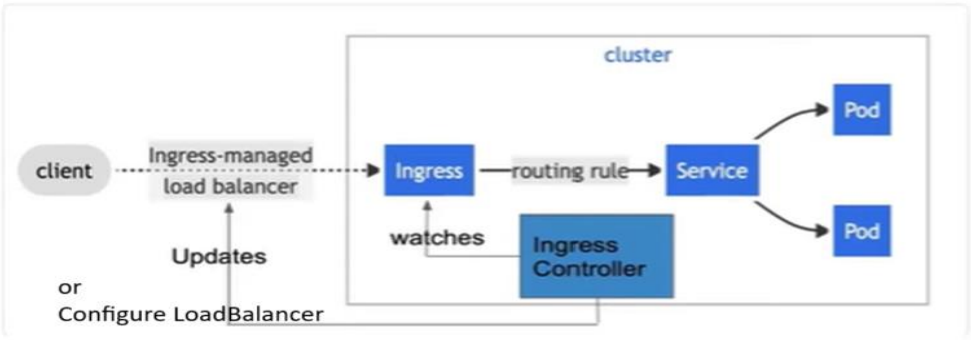
- **Traffic Load balancing**: Distributes incoming traffic across multiple instances (replicas) of a service for high availability and better resource utilization.
- **Rate Limiting and Security**: Limiting the number of requests or enforcing authentication at the Ingress level to prevent abuse or ensure secure access.

Why do we use Ingress?

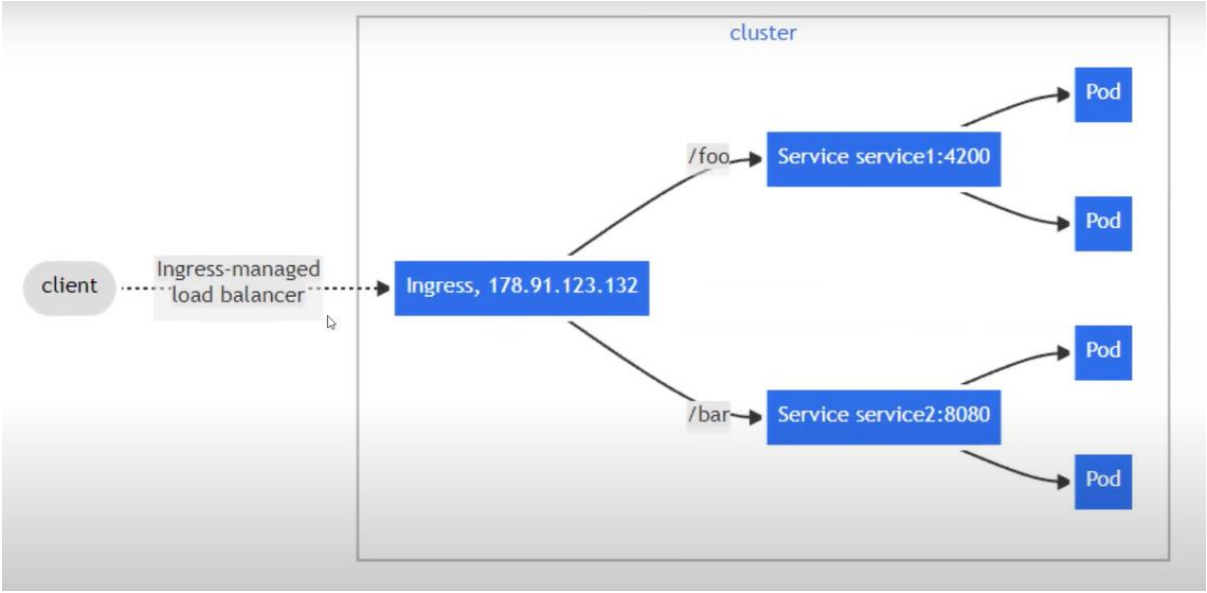
- Expose multiple microservices with domains and subdomains
- Centralized routing
- So ingress is best compared to LoadBalancer and NodePort

Ingress Controller

In order for the Ingress resource to work, the cluster must have an ingress controller running.



.




```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: nginx-ingress
  annotations:
    nginx.ingress.kubernetes.io/rewrite-target: /
spec:
  rules:
  - host: nginx.you_url.com
    http:
      paths:
      - path: /nginx
        pathType: Prefix
```

```yaml
      backend:
        service:
          name: nginx-loadbalancer-service
          port:
            number: 8080
            name: http
```

Sample Ingress

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: test-ingress
spec:
  defaultBackend:
    service:
      name: test
      port:
        number: 80
```

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress-no-auth
spec:
  rules:
  - host: foo.bar.com
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: http-svc
            port:
              number: 80
```

Host Based Routing

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress-with-auth
spec:
  rules:
  - host: foo.bar.com
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: http-svc
            port:
              number: 80
  - host: example.bar.com
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: meow-svc
            port:
              number: 80
```

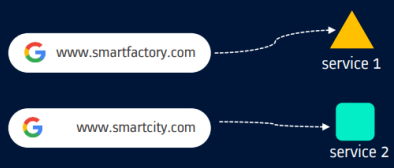
Path Based Routing

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress-with-auth
spec:
  rules:
  - host: foo.bar.com
    http:
      paths:
      - path: /first
        pathType: Prefix
        backend:
          service:
            name: http-svc
            port:
              number: 80
      paths:
      - path: /second
        pathType: Prefix
        backend:
          service:
            name: meow-svc
            port:
              number: 80
```

Kubernetes

Nginx Ingress Controller

- Ingress-nginx is an Ingress controller for Kubernetes using NGINX as a reverse proxy and load balancer
- Officially maintained by Kubernetes community
- Routes requests to services based on the request host or path, centralizing a number of services into a single entrypoint.
  Ex: www.mysite.com or www.mysite.com/stats



Deploy Nginx Ingress Controller

kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-0.32.0/deploy/static/provider/baremetal/deploy.yaml

https://github.com/kubernetes/ingress-nginx/blob/master/docs/deploy/index.md#bare-metal

Kubernetes

Ingress Rules

ingress-rules.yml

Path based routing

```
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress-rules
spec:
  rules:
  - host:
    http:
      paths:
      - path: /nginx
        backend:
          serviceName: nginx-service
          servicePort: 80
      - path: /flask
        backend:
          serviceName: flask-service
          servicePort: 80
```

Host based routing

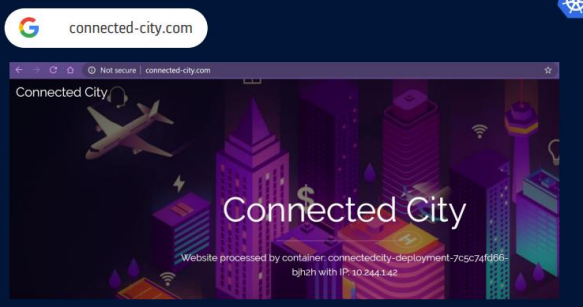
```
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress-rules
  annotations:
    nginx.ingress.kubernetes.io/rewrite-target: /
spec:
  rules:
  - host: nginx-app.com
    http:
      paths:
      - backend:
          serviceName: nginx-service
          servicePort: 80
  - host: flask-app.com
    http:
      paths:
      - backend:
          serviceName: flask-service
          servicePort: 80
```

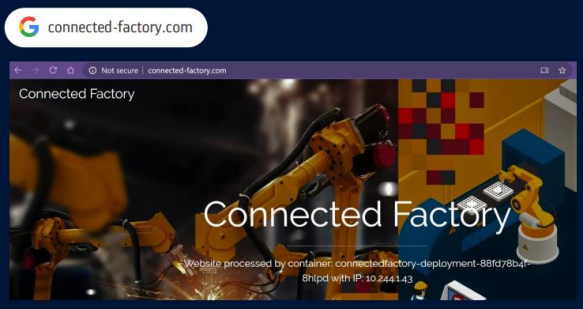
Ingress-controller executes these ingress-rules by comparing with the http requested URL in the http header

Kubernetes

Demo: Ingress

- 3VMs K8s Cluster + 1 VM for Reverse Proxy
- Deploy Ingress controller
- Deploy pods
- Deploy services
- Deploy Ingress rules
- Configure external reverse proxy
- Update DNS names
- Access applications using URLs
  - connected-city.com
  - connected-factory.com

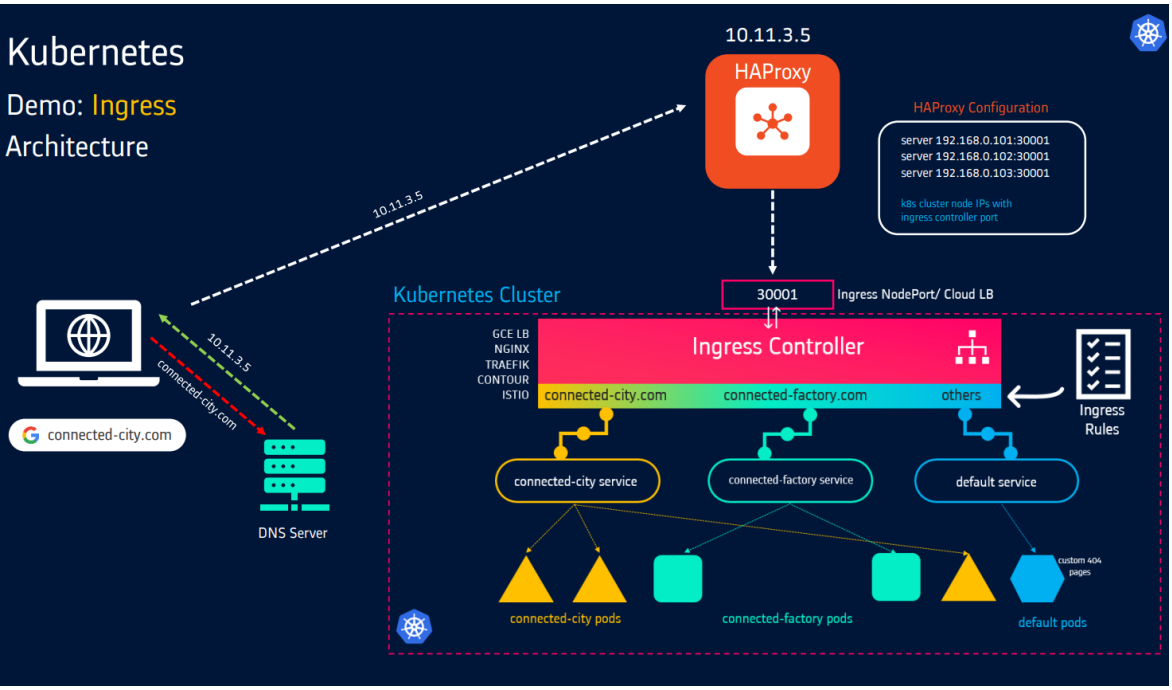




Kubernetes

Demo: Ingress

Architecture



Kubernetes

Demo: Ingress

1. Deploy Nginx Ingress Controller

kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-0.32.0/deploy/static/provider/baremetal/deploy.yaml

2. Deploy pods and services

kubectl apply –f <object>.yml

```yaml
apiVersion: v1
kind: Service
metadata:
  name: connectedcity-service
spec:
  ports:
  - port: 80
    targetPort: 5000
  selector:
    app: connectedcity
```

Application-1
Deployment + ClusterIP service

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: connectedcity-deployment
spec:
  replicas: 3
  selector:
    matchLabels:
      app: connectedcity
  template:
    metadata:
      labels:
        app: connectedcity
    spec:
      containers:
      - name: connectedcity
        image: kunchalavikram/connectedcity:v1
        ports:
        - containerPort: 5000
```

```yaml
apiVersion: v1
kind: Service
metadata:
  name: connectedfactory-service
spec:
  ports:
  - port: 80
    targetPort: 5000
  selector:
    app: connectedfactory
```

Application-2
Deployment + ClusterIP service

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: connectedfactory-deployment
spec:
  replicas: 3
  selector:
    matchLabels:
      app: connectedfactory
  template:
    metadata:
      labels:
        app: connectedfactory
    spec:
      containers:
      - name: connectedfactory
        image: kunchalavikram/connectedfactory:v1
        ports:
        - containerPort: 5000
```

Kubernetes

Demo: Ingress

3. Deploy ingress rules manifest file

- Host based routing rules
- Connects to various services depending upon the host parameter

kubectl apply –f <object>.yml

```yaml
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress-rules
  annotations:
    nginx.ingress.kubernetes.io/rewrite-target: /
spec:
  rules:
  - host: connected-city.com
    http:
      paths:
      - backend:
          serviceName: connectedcity-service
          servicePort: 80
  - host: connected-factory.com
    http:
      paths:
      - backend:
          serviceName: connectedfactory-service
          servicePort: 80
```

Kubernetes

Demo: Ingress

4. Deploy HA Proxy LoadBalancer

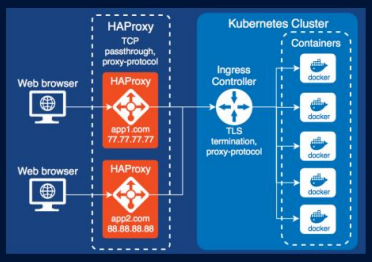
- Provision a VM
- Install HAProxy using package manager
  - apt install haproxy –y
- Restart HAProxy service after modifying the configuration
  - systemctl stop haproxy
  - add configuration to /etc/haproxy/haproxy.cfg
  - systemctl start haproxy && systemctl enable haproxy

10.11.3.5

/etc/haproxy/haproxy.cfg

```
# Configure HAProxy to listen on port 80
frontend http_front
   bind *:80
   default_backend http_back

# Configure HAProxy to route requests to swarm nodes on port 8080
backend http_back
   balance roundrobin
   mode http
   server srv1 192.168.0.101:32174
   server srv2 192.168.0.102:32174
   server srv3 192.168.0.103:32174
root@proxyserver:/home/osboxes#
```



Kubernetes

Demo: Ingress

5. Update dummy DNS entries

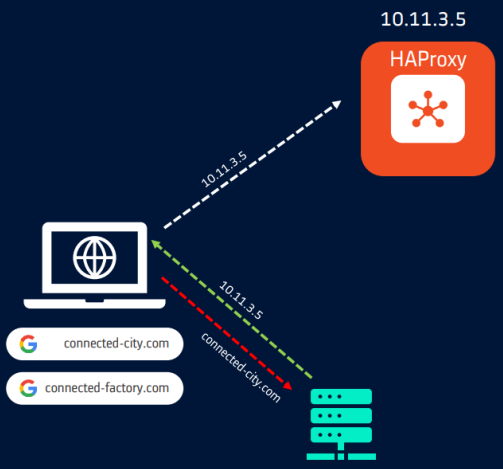
Both DNS names to point to IP of HAProxy server

windows

```
C:\Windows\System32\drivers\etc\hosts
192.168.0.105 connected-city.com
192.168.0.105 connected-factory.com
ipconfig /flushdns
```

linux

```
/etc/hosts
192.168.0.105 flask-app.com
```



Kubernetes

Demo: Ingress

6. Access Application through URLs

Ingress vs. LoadBalancer Services

- **Ingress**:
  - Provides a single-entry point for HTTP and HTTPS traffic.
  - Offers flexible routing based on hostnames, paths, and headers.
  - Can handle SSL/TLS termination.
  - Requires an Ingress controller to implement the Ingress resource.
- **LoadBalancer Service**:
  - Directly exposes a service to the internet using a cloud provider's load balancer.
  - Simpler to set up but less flexible in terms of routing rules.
  - Mainly used for non-HTTP/HTTPS traffic, like TCP and UDP.

Common Ingress Controllers:

1. **NGINX Ingress Controller**: One of the most widely used Ingress controllers, offering robust features like load balancing, SSL termination and path-based routing.
2. **Traefik**: A dynamic and modern reverse proxy, Traefik is highly adaptable and integrates seamlessly with Kubernetes.
3. **HAProxy Ingress**: A reliable and high-performance option, HAProxy supports advanced load balancing features.
4. **Istio**: Primarily a service mesh, Istio can also serve as an Ingress Controller with advanced routing, security, and observability features.
5. **Envoy**: A high-performance proxy used for microservices architectures, integrated with Kubernetes as an Ingress Controller for advanced traffic management.

Troubleshooting Common Ingress Configuration Errors:

1. **Ingress Not Routing Traffic Correctly**:
   - **Cause**: Incorrect path or host definitions.
   - **Solution**: Verify the path and host rules in the Ingress definition. Check for typos or mistakes in URL matching and ensure services are correctly defined under the rules.
2. **503 Service Unavailable Error**:
   - **Cause**: The Ingress controller cannot reach the backend service (often due to misconfigured service names or ports).
   - **Solution**: Check that the service specified in the Ingress resource exists, is exposed, and is properly configured with the correct port. Use **kubectl describe ingress** to check for errors related to backend services.
3. **SSL/TLS Errors (e.g., Certificate Mismatch)**:
   - **Cause**: A mismatch between the SSL/TLS certificate in the Ingress controller and the domain or expired certificates.
   - **Solution**: Ensure that the **TLS secret** associated with your Ingress has a valid certificate for the domain in question. Use **Cert-Manager** to automate certificate renewal.
4. **404 Not Found**:
   - **Cause**: The path or hostname in the request doesn't match any defined Ingress rules.

    - **Solution**: Verify that the Ingress paths and hostnames are correctly defined and that they match the incoming request. Check for correct service names and that the Ingress rules are pointing to the correct backend services.
5. **Incorrect Annotations or Configuration Settings**:
    - **Cause**: Misconfigured annotations or settings in the Ingress definition (e.g., missing or incorrect load balancing settings).
    - **Solution**: Review and validate the Ingress resource annotations. For example, NGINX has specific annotations like **nginx.ingress.kubernetes.io/rewrite-target** that must be configured correctly.
6. **Ingress Controller Not Running or Misconfigured**:
    - **Cause**: The Ingress controller might not be deployed or properly configured.
    - **Solution**: Ensure the Ingress controller pod is running by checking with kubectl get pods -n <namespace>. Check logs using kubectl logs <ingress-controller-pod-name> to look for errors.
7. **Timeout or Slow Response**:
    - **Cause**: The backend service might be slow or misconfigured, causing timeouts.
    - **Solution**: Investigate the backend service logs to ensure it is responsive. Increase timeout settings in the Ingress controller if necessary.
8. **Inconsistent Ingress Controller and Service Ports**:
    - **Cause**: Mismatch between the port configured on the Ingress and the port exposed by the service.
    - **Solution**: Ensure that the service port specified in the Ingress matches the actual service port.
9. **Check Logs**: Review the logs of the Ingress controller to identify any errors or misconfigurations.
10. **Validate Ingress Resources**: Ensure that Ingress resources are correctly defined and that annotations are valid.
11. **Inspect ConfigMaps**: Verify that ConfigMap keys and values are correctly configured.
12. **Health Checks**: Ensure that backend services are healthy and responding as expected.
13. **DNS Resolution**: Confirm that DNS resolution is working correctly and that the Ingress controller can resolve service names.
14. **Check Events**: Review Kubernetes events related to Ingress resources to identify any issues.

TLS:

TLS in Kubernetes: Secure Communication for Cluster Components

- **TLS (Transport Layer Security)** in Kubernetes is used to secure communication between components within the cluster and between external clients and Kubernetes services.
- TLS ensures that **data is encrypted**, **preventing unauthorized access** and **protects sensitive data.**

Where TLS is Used in Kubernetes?

- 🔹 **API Server –** TLS secures communication between the Kubernetes API server and clients (kubectl, controllers, etc.).
- 🔹 **etcd Database –** Data stored in etcd is encrypted using TLS to prevent unauthorized access.
- 🔹 **Kubelet & API Server –** TLS ensures **mutual authentication** between nodes and the control plane.
- 🔹 **Ingress Controller –** TLS enables HTTPS traffic for applications exposed externally.
- 🔹 **Service-to-Service Communication –** Applications within the cluster use TLS certificates for **secure pod-to-pod communication.**

TLS Certificates in Kubernetes

- ✅ **Self-Signed Certificates –** Default certificates generated for internal communication within Kubernetes.
- ✅ **Cert-Manager –** A Kubernetes tool that automates certificate issuance and renewal for TLS.
- ✅ **Let's Encrypt –** A popular service for issuing free TLS certificates for Kubernetes applications.

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: my-secure-ingress
  annotations:
    nginx.ingress.kubernetes.io/ssl-redirect: "true"
spec:
  tls:
  - hosts:
      - example.com
    secretName: tls-secret
  rules:
  - host: example.com
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: my-service
            port:
              number: 443
```

✅ **This Ingress configuration enables HTTPS using a TLS secret (tls-secret).**

Understanding SSL Passthrough, SSL Offloading, and SSL Bridging

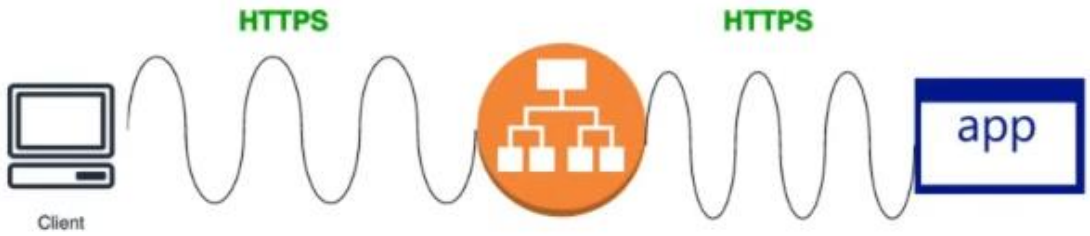
These are techniques used to handle **SSL/TLS encryption** in web applications, particularly within **load balancers, proxies, and Kubernetes ingress controllers**.

In Kubernetes, **SSL/TLS termination** can be handled in different ways depending on security and performance requirements. Here's a breakdown of **SSL Passthrough, SSL Offloading (Termination), and SSL Bridging (Re-Encryption)**, along with their use cases in Kubernetes (especially with Ingress Controllers like Nginx, Traefik, or HAProxy).

1. SSL Passthrough

- **Definition:** The load balancer (**Ingress Controller) forwards encrypted HTTPS traffic** directly to the backend server **without decrypting it**.
- The backend service (e.g., a Pod running a web server) is responsible for **SSL termination** (handles decryption and serves the request).
- **Use case:** Best for **security-sensitive applications**, since the encryption remains **intact end-to-end**.

Pros	Cons
End-to-end encryption	Backend must handle TLS (decryption)
No decryption at Ingress	Harder to debug (traffic stays encrypted)
Good for compliance	Higher workload on backend



Load Balancer capabilities are merely used.
Attacker can pass hacking codes in the traffic and will be directly passed to the backend server.
SSL Passthrough is also a costly process. Might require more CPU.

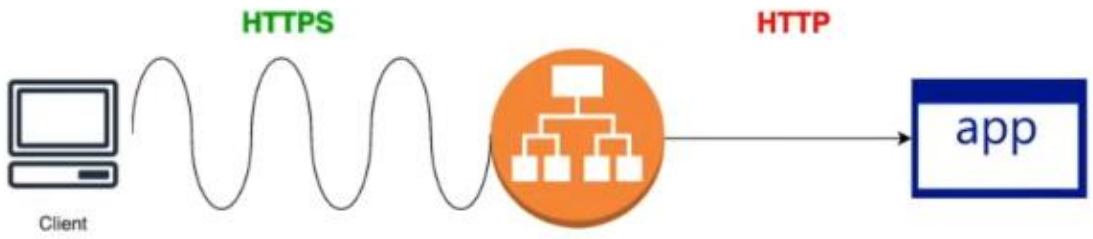
```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  annotations:
    nginx.ingress.kubernetes.io/ssl-passthrough: "true"  # Enables passthrough
spec:
  tls:
  - hosts:
    - myapp.example.com  # Client-facing domain
  rules:
```

```
  - host: myapp.example.com
    http:
      paths:
      - path: /
        backend:
          service:
            name: my-service
            port:
              number: 443  # Backend must handles HTTPS
```

2. SSL Offloading

- **Definition:** The load balancer (**Ingress Controller) decrypts all HTTPS traffic** and forwards it as **plain HTTP** to the backend servers.
- The load balancer handles **SSL termination** to improve backend performance.
- **Use case:** AWS Application Load Balancer (**ALB**) uses **SSL Offloading** to handle HTTPS requests efficiently. (**Layer 7 routing**)

Pros	Cons
Reduces backend workload	Traffic is unencrypted between Ingress and Pods
Easier to debug	Requires network policies to secure internal traffic
Supports advanced routing	Not compliant for strict end-to-end encryption



Vulnerable to data theft, man-in-the-middle attacks.
Faster

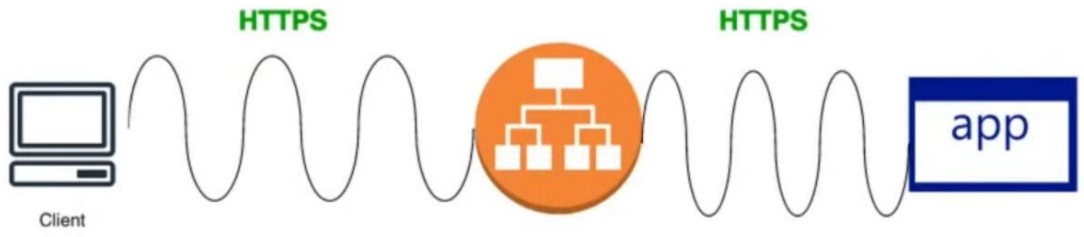
```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ssl-offload-ingress
spec:
  tls:
  - hosts:
```

```
    - myapp.example.com
    secretName: my-tls-secret  # Cert stored in a Secret
  rules:
  - host: myapp.example.com
    http:
      paths:
      - path: /
        backend:
          service:
            name: my-service
            port:
              number: 80  # Backend receives HTTP
```

3. SSL Bridging

- **Definition:** The load balancer (**Ingress Controller) decrypts TLS traffic** (like SSL Offloading) but then **re-encrypts it** before sending it to the backend.
- **How it works:** Maintains **end-to-end encryption** while allowing traffic inspection.
- **Use case:** When **internal traffic must also be encrypted** (e.g., multi-tenant clusters).

Pros	Cons
Internal traffic stays encrypted	Slightly higher latency
Allows L7 inspection	More complex setup
Good for compliance	Needs backend TLS certs



E2E encrypted and validated for malware attacks by Load Balancer.
More secure more costly in processing as server has to decrypt the traffic.

```
apiVersion: traefik.containo.us/v1alpha1
kind: IngressRoute
metadata:
  name: ssl-bridge-route
spec:
  entryPoints:
    - websecure
```

```yaml
routes:
- match: Host(`myapp.example.com`)
  services:
  - name: my-service
    port: 443
    scheme: https  # Forces HTTPS to backend
    tls: {}       # Enables re-encryption
tls:
  secretName: my-tls-secret  # Cert for client-side
```

Pros and Cons !!

SSL Passthrough	SSL-Offloading/Termination	SSL-Bridge/Re-encrypt
Costly in processing for Server	Fast in processing	Costly in processing for Server
Secure in many cases	Insecure	Secure
L4 (TCP) Load Balancing	L7 Load Balancing	L7 Balancing
Choose when you don't bother about access rules, blocking, cookie e.t.c.,.	When you want less latency and can compromise on security.	When you need security and advanced load balancer capabilities.
No Load Balancer Inspection.	Load Balancer Inspects the packets.	Load Balancer Inspects the packets.
Recommended*	Highly unrecommended.	Recommended

OpenShift Routes

SSL Offloading == Edge Termination

SSL Bridge == Re-encrypt Termination

SSL Passthrough == Passthrough Termination

```yaml
apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: hello-openshift
spec:
  host: hello-openshift-hello-openshift.
  port:
    targetPort: 8080
  to:
    kind: Service
    name: hello-openshift
```

Secure Routes

*Routes does not support storing the TLS certs in secrets - Issue

Routes are simple, you cannot add multiple services, paths or hosts in a single route.

Service mesh

Service mesh

- It will help to manage the traffic between services in cluster. Mainly (East-West traffic).

- **East-West traffic** refers to **communication between Pods within the cluster**—basically, Pod-to-Pod communication inside Kubernetes.
  For example, a frontend Pod calling a backend Pod or database Pod.
- **North-South traffic** means **traffic entering or leaving the cluster**—communication between Pods and external clients or services outside the cluster.
  For example, user requests coming into your app from the internet, or your app calling an external API.

Why service mesh needs?

- A **service mesh** enhances **service-to-service communication** within a cluster and supports features like **mTLS** (Mutual TLS) for secure communication.
- It will also add the advanced capabilities such as **deployment strategies** (Canary / A-B / Blue Green)
- **Observabilities** – Kiali – it will keeps a track of service to service communication information. It will helps to understand how services are behaving and metrics health of services.
- **Circuit breaking** – it can helps to split traffic splitting

In **Kubernetes**, a **Service Mesh** is an infrastructure layer that manages **service-to-service communication** within a cluster. It provides advanced features like **traffic control, observability, security**, and **reliability** without requiring changes to your application code.

🔧 What Does a Service Mesh Do?

1. **Traffic Management**
   - Controls how requests are routed between services.
   - Supports features like retries, timeouts, and circuit breakers.
2. **Security**
   - Implements **mTLS (Mutual TLS)** to encrypt traffic and authenticate services.
   - Ensures secure communication between microservices.
3. **Observability**
   - Provides metrics, logs, and tracing for service interactions.
   - Helps monitor performance and troubleshoot issues.
4. **Policy Enforcement**
   - Allows defining access control and rate-limiting policies.

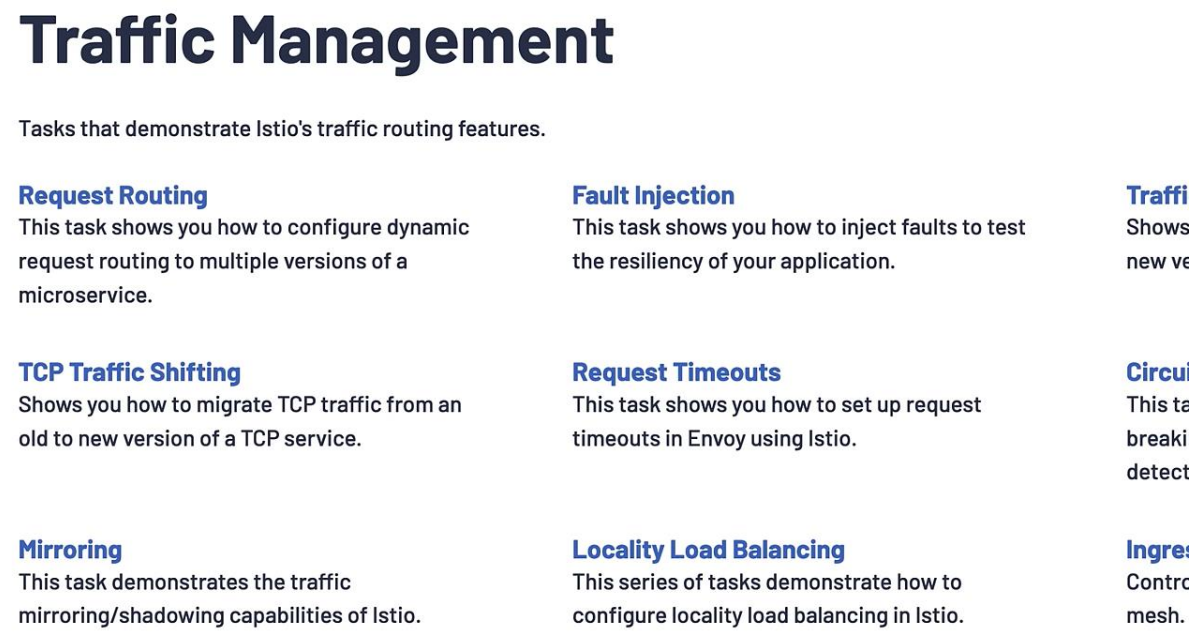
🧱 How It Works in Kubernetes

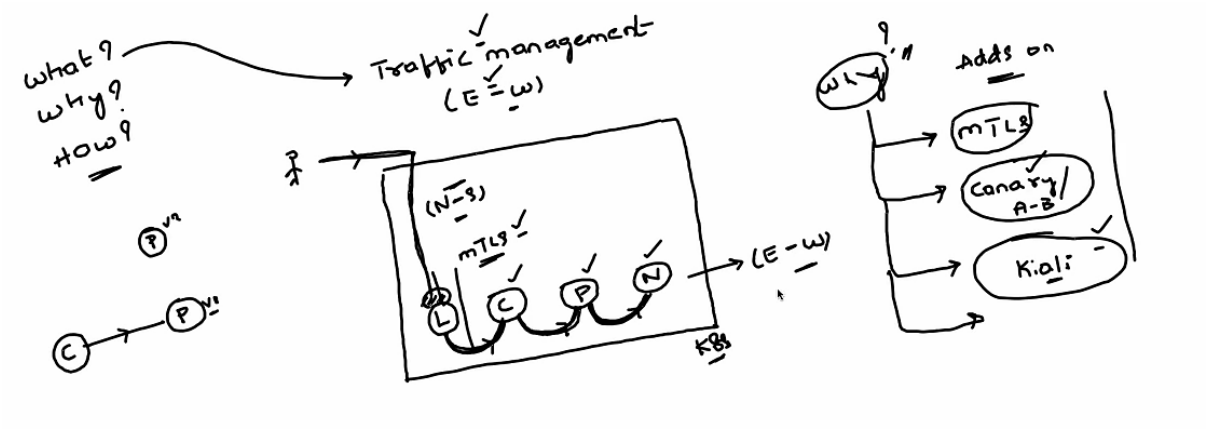
A service mesh typically uses **sidecar proxies** (like Envoy) that are injected into each pod. These proxies handle all incoming and outgoing traffic for the service, enabling the mesh to manage communication transparently.

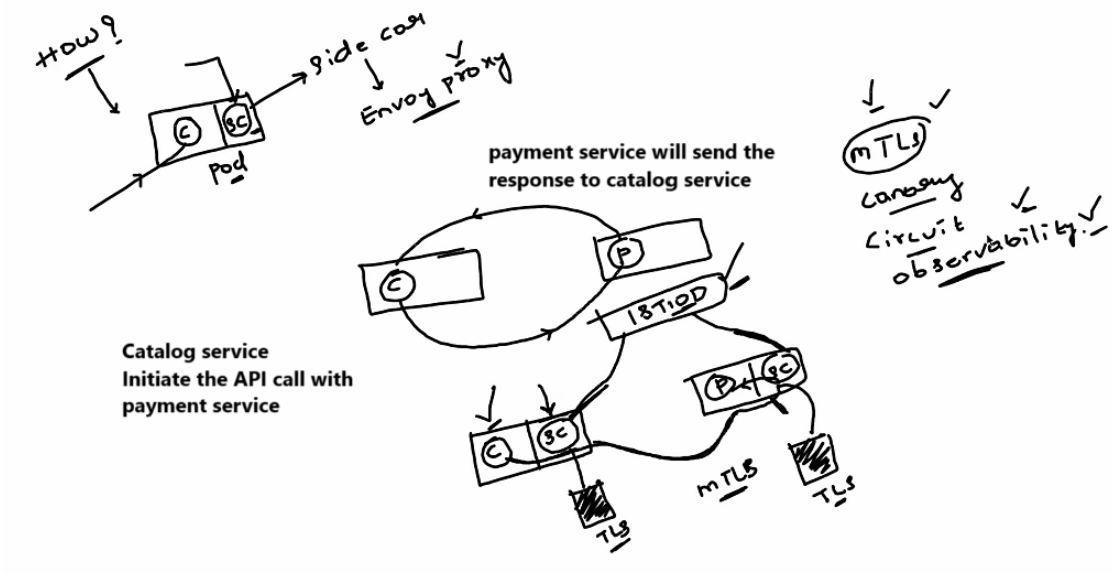
📌 Example Use Case

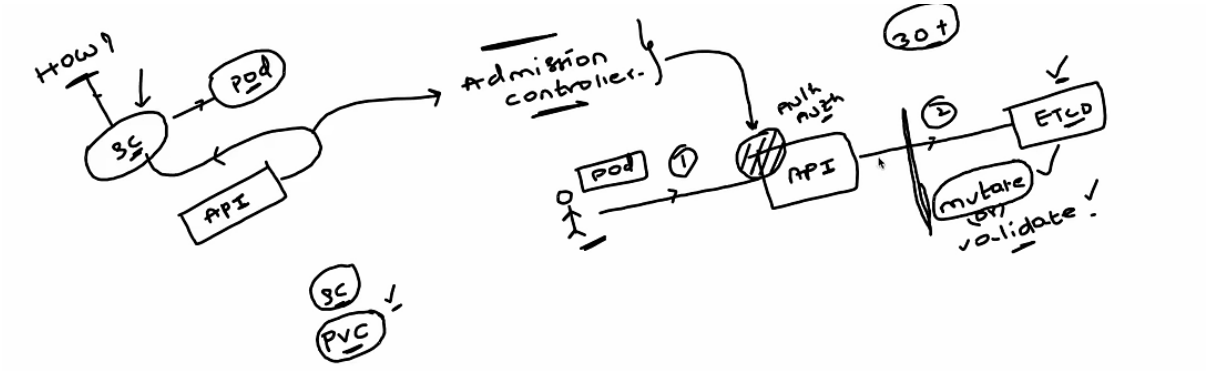
Imagine you have three microservices: **frontend**, **backend**, and **database**. A service mesh can:

- Encrypt traffic between them using mTLS.
- Automatically retry failed requests.
- Monitor latency and error rates.
- Apply policies like "only frontend can talk to backend."









Admission controller
It will validate and mutate the authenticated and authenticated user request

- Mutate
- Validate

3) Replicaset

ReplicaSets:

- **A ReplicaSet** is a Kubernetes object that ensures that the exact number of pods(replicas) are always running in the cluster by replacing any failed pods with new ones. It's primarily used to maintain **high availability** and **scalability** of applications.
- The replica count is controlled by the replicas field in the resource definition file
- **Replicaset** uses **set-based selectors** whereas **replicacontroller** uses **equality-based selectors**

🔁 **What Does a ReplicaSet Do?**

- **Ensures desired state**: If a pod crashes or is deleted, the ReplicaSet automatically creates a new one to maintain the desired number.
- **Supports rolling updates**: Often used behind the scenes by **Deployments** to manage updates.
- **Scales applications**: You can increase or decrease the number of replicas easily.

🧱 **Key Components**

- **replicas**: Number of pod copies you want running.
- **selector**: Labels used to identify which pods the ReplicaSet should manage.
- **template**: The pod specification (like image, ports, etc.).

ReplicationController:

A **ReplicationController** is an older Kubernetes resource with a similar purpose to ReplicaSets. It ensures that a specified number of pod replicas are running at all times.

Differences between ReplicaSet and ReplicationController:

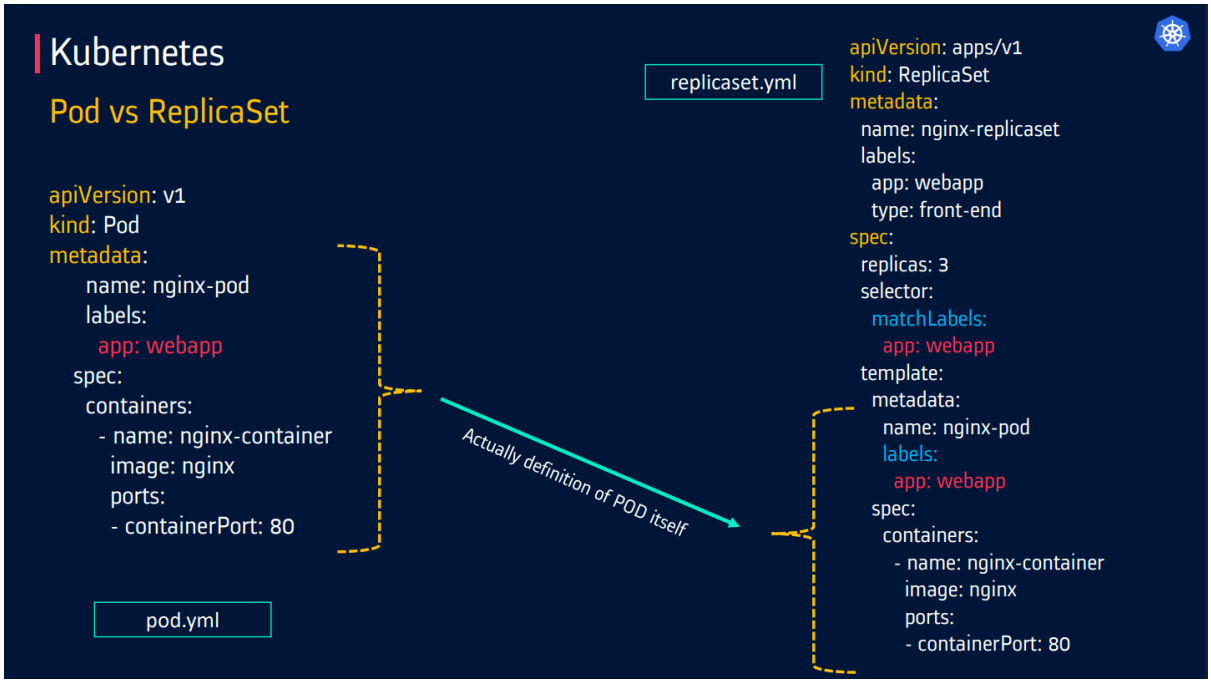
➢ **Replicaset:**

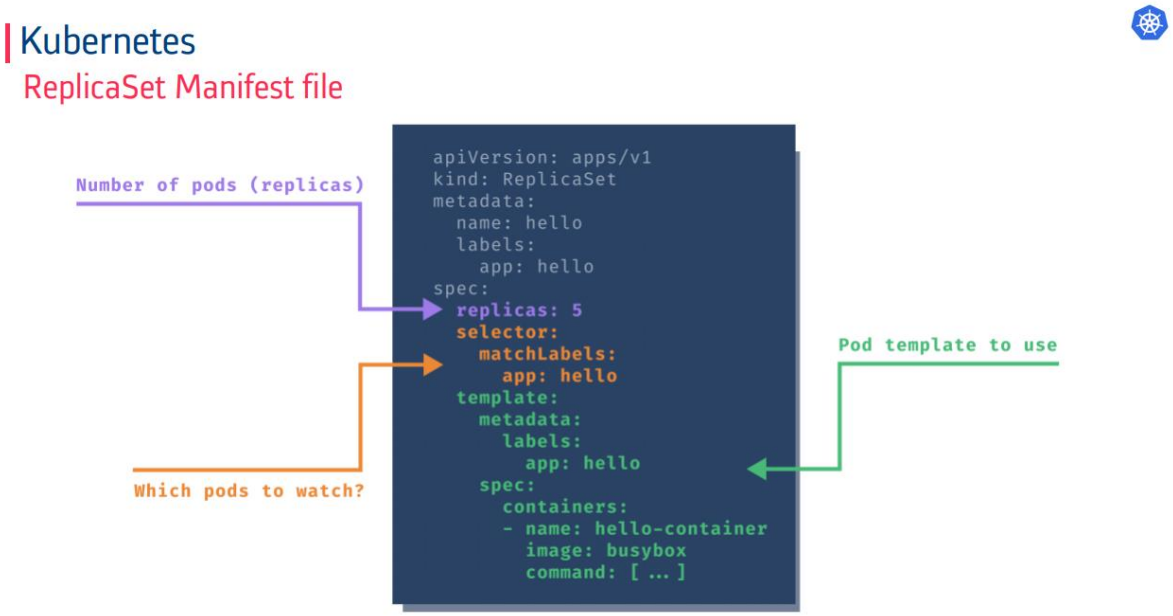
- **Selectors:** Supports set-based selectors (more flexible).
- **Use Case:** Used with Deployments for modern applications.
- **Efficiency:** More advanced and flexible.

➢ **ReplicationController**

- **Selectors:** Supports only equality-based selectors.
- **Use Case:** Considered legacy, replaced by ReplicaSet.
- **Efficiency:** Limited to basic replication tasks.

Example:





Example:

```yaml
apiVersion: apps/v1
kind: ReplicaSet
metadata:
  name: frontend
  labels:
    app: guestbook
    tier: frontend
spec:
  replicas: 3  # modify replicas according to your case
  selector:
```

```
    matchLabels:
      tier: frontend
  template:
    metadata:
      labels:
        tier: frontend
    spec:
      containers:
        - name: php-redis
          image: gcr.io/google_samples/gb-frontend:v3
```

4) Deployments

Deployments:

- A **Deployment** is a Kubernetes object used to manage Pods and ReplicaSets through a declarative configuration. It defines the desired state of an application including the number of Pods, deployment strategies, container images and manages the rollout and rollback of changes.
- The **Deployment Controller** ensures the actual state matches the desired state by replacing failed pods.
- Deployments support several **deployment strategies** like "**recreate**" and "**rolling update**" and can be customized for advanced methods such as blue/green or canary deployments.
- A **Deployment** provides replication functionality and **auto-healing** and **auto-scaling** features with the help of ReplicaSets.
- It also facilitates **rolling out** and **rolling back** changes effectively.

Key Features of Deployments

1. **Declarative Management:** You describe the desired state in a YAML or JSON file. Kubernetes takes care of the changes.
2. **Rolling Updates:** Gradually replaces old pods with new ones, ensuring zero downtime
3. **Rollback Capability:** Kubernetes can revert to previous versions if an update fails.
4. **Self-healing:** Automatically replaces failed or deleted pods.

Command to rollout and rollback

1. **Monitor the Update Progress:**
   Check Deployment status: **kubectl rollout status deployment/my-app**
   View update history: **kubectl rollout history deployment/my-app**
2. **Rollback if Needed:** If the update causes issues,
   rollback to the previous version:
   kubectl rollout undo deployment/my-app
   You can also specify a specific revision to rollback to:
   kubectl rollout undo deployment/my-app --to-revision=2
3. **Blue-Green Deployment (Optional)**

Instead of a rolling update, you can create a new Deployment with the updated version and use a Service to switch traffic between the old and new versions.

4. **Canary Deployment (Optional)**
   This approach deploys the new version to a small subset of users first, allowing testing in a production-like environment. Gradually, the new version replaces the old one.

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.14.2
        ports:
        - containerPort: 80
```

Explanation of the YAML:

- **spec:** The specifications of the Deployment.
  - **replicas:** Defines the number of Pods to run (e.g., 3).
  - **selector:** Defines the label selector to match the Pods managed by this Deployment.
  - **template:** Defines the template for the Pods that will be created by the Deployment. It includes the metadata and spec for the Pods (such as the container image and port to expose).

Failed Deployment:

Your Deployment may get stuck trying to deploy its newest ReplicaSet without ever completing. This can occur due to some of the following factors:

- Insufficient quota
- Readiness probe failures
- Image pull errors
- Insufficient permissions

• Limit ranges
• Application runtime misconfiguration

Deployment Strategy:

In **Kubernetes**, a **Deployment Strategy** defines **how updates** to your application are rolled out. It controls **how new versions of pods replace old ones**, ensuring minimal downtime and maximum reliability.

🚀 Common Deployment Strategies

1. Rolling Update (Default)

- Gradually replaces old Pods with new ones, **one-by-one or in batches**.
- Ensures **zero downtime** by keeping at least some Pods running during the update.

Key Features:

- **Controlled Scaling**:
  - **maxSurge:** How many extra Pods can be created during the update (default: 25%).
  - **maxUnavailable:** How many Pods can be unavailable during the update (default: 25%).
- **Smooth Transition**:
  - New Pods are started before old ones are terminated.
- **Automatic Rollback**:
  - If new Pods fail health checks, Kubernetes reverts to the previous version.

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  replicas: 3
  strategy:
    type: RollingUpdate
    rollingUpdate:
      maxSurge: 1       # Allows 1 extra Pod during update
      maxUnavailable: 0 # Ensures all Pods remain available
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.25
```

```
    ports:
    - containerPort: 80
```

- **RollingUpdate:** release a new version on a rolling update fashion, one after the other. **It's the default strategy in K8s. No application downtime is required.**
- **Blue/green:** release a new version alongside the old version then switch traffic

```
spec:
  replicas: 10
strategy:
    type: Recreate
```

```
spec:
  replicas: 10
strategy:
    type: RollingUpdate
    rollingUpdate:
      maxSurge: 2
      maxUnavailable: 0
```

Kubernetes

Rolling Update Strategy

- By default, deployment ensures that only 25% of your pods are unavailable during an update and does not update more that 25% of the pods at a given time
- It does not kill old pods until/unless enough new pods come up
- It does not create new pods until a sufficient number of old pods are killed
- There are two settings you can tweak to control the process: maxUnavailable and maxSurge. Both have the default values set - 25%
- The maxUnavailable setting specifies the maximum number of pods that can be unavailable during the rollout process. You can set it to an actual number(integer) or a percentage of desired pods

  Let's say maxUnavailable is set to 40%. When the update starts, the old ReplicaSet is scaled down to 60%.
  As soon as new pods are started and ready, the old ReplicaSet is scaled down again and the new ReplicaSet is scaled up. This happens in such a way that the total number of available pods (old and new, since we are scaling up and down) is always at least 60%.
- The maxSurge setting specifies the maximum number of pods that can be created over the desired number of pods

  If we use the same percentage as before (40%), the new ReplicaSet is scaled up right away when the rollout starts. The new ReplicaSet will be scaled up in such a way that it does not exceed 140% of desired pods. As old pods get killed, the new ReplicaSet scales up again, making sure it never goes over the 140% of desired pods

Kubernetes

Deployments

- kubectl create deployment nginx --image nginx --dry-run -o yaml
- kubectl create -f deployment.yml --record (--record is optional, it just records the events in the deployment)

```
root@k-master:/home/osboxes# kubectl create -f deployment.yml
deployment.apps/nginx-deployment created
root@k-master:/home/osboxes#
```

- kubectl get deployments

```
root@k-master:/home/osboxes# kubectl get deployments -o wide
NAME               READY   UP-TO-DATE   AVAILABLE   AGE    CONTAINERS
nginx-deployment   5/5     5            5           117s   nginx-container
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 10
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx-container
        image: nginx
        ports:
        - containerPort: 80
```

Kubernetes

Deployments

- kubectl describe deployment <deployment-name>

```
root@k-master:/home/osboxes# kubectl describe deployment nginx-deployment
Name:                   nginx-deployment
Namespace:              default
CreationTimestamp:      Tue, 19 May 2020 03:40:19 -0400
Labels:                 app=nginx
Annotations:            deployment.kubernetes.io/revision: 1
                        kubernetes.io/change-cause: kubectl create --filename=deployment.yml
Selector:               app=nginx
Replicas:               5 desired | 5 updated | 5 total | 5 available | 0 unavailable
StrategyType:           RollingUpdate
MinReadySeconds:        0
RollingUpdateStrategy:  25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginx
  Containers:
   nginx-container:
    Image:        nginx
    Port:         80/TCP
    Host Port:    0/TCP
    Environment:  <none>
    Mounts:       <none>
  Volumes:        <none>
Conditions:
  Type           Status  Reason
  ----           ------  ------
  Available      True    MinimumReplicasAvailable
  Progressing    True    NewReplicaSetAvailable
OldReplicaSets:  <none>
NewReplicaSet:   nginx-deployment-96577bc6d (5/5 replicas created)
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 10
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx-container
        image: nginx
        ports:
        - containerPort: 80
```

Kubernetes

Deployments

- kubectl get pods –o wide

```
root@k-master:/home/osboxes# kubectl get pods -o wide
NAME                               READY   STATUS    RESTARTS   AGE     IP            NODE
TES
nginx-deployment-96577bc6d-2hkpk   1/1     Running   0          3m34s   10.244.2.20   k-slave02
nginx-deployment-96577bc6d-h5gdv   1/1     Running   0          3m34s   10.244.2.19   k-slave02
nginx-deployment-96577bc6d-nqtn6   1/1     Running   0          3m34s   10.244.2.22   k-slave02
nginx-deployment-96577bc6d-pd4cg   1/1     Running   0          3m34s   10.244.2.21   k-slave02
nginx-deployment-96577bc6d-tphhh   1/1     Running   0          3m34s   10.244.2.23   k-slave02
root@k-master:/home/osboxes#
```

- kubectl edit deployment <deployment -name> - perform live edit of deployment
- kubectl scale deployment <deployment -name> --replicas2
- kubectl apply –f deployment.yml – redeploy a modified yaml file; Ex: replicas changed to 5, image to nginx:1.18

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 10
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx-container
        image: nginx
        ports:
        - containerPort: 80
```

Kubernetes

Deployments

- kubectl rollout status deployment <deployment -name>

```
root@k-master:/home/osboxes# k rollout status deployment.apps/nginx-deployment
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 3 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 4 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 4 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 4 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 4 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 4 out of 5 new replicas have been updated...
Waiting for deployment "nginx-deployment" rollout to finish: 2 old replicas are pending termination...
Waiting for deployment "nginx-deployment" rollout to finish: 1 old replicas are pending termination...
Waiting for deployment "nginx-deployment" rollout to finish: 1 old replicas are pending termination...
Waiting for deployment "nginx-deployment" rollout to finish: 1 old replicas are pending termination...
Waiting for deployment "nginx-deployment" rollout to finish: 4 of 5 updated replicas are available...
deployment "nginx-deployment" successfully rolled out
```

- kubectl rollout history deployment <deployment -name>

```
root@k-master:/home/osboxes# k rollout history deployment.apps/nginx-deployment
deployment.apps/nginx-deployment
REVISION  CHANGE-CAUSE
1         kubectl create --filename=deployment.yml --record=true
2         kubectl create --filename=deployment.yml --record=true
```

2. Recreate

- **Terminates all old Pods first**, then creates new ones.
- Causes **downtime**, but ensures a clean start.

Key Features:

- **Simple but disruptive**:
  - No overlap between old and new Pods.
- **Useful for non-version-tolerant apps**:
  - E.g., databases or apps that can't run multiple versions simultaneously.
  - Useful when old and new versions **can't run together** (e.g., database schema changes).

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: mysql-deployment
spec:
  replicas: 1
  strategy:
    type: Recreate  # All old Pods are killed before new ones start
  selector:
    matchLabels:
      app: mysql
  template:
    metadata:
      labels:
        app: mysql
    spec:
      containers:
      - name: mysql
        image: mysql:8.0
        env:
```

```
        - name: MYSQL_ROOT_PASSWORD
          value: "password"
```

Blue/Green and **Canary** deployments are advanced deployment strategies used in Kubernetes and DevOps to release new versions of applications **safely and with minimal risk**.

3. Blue/Green Deployment 🔵🟢

Concept:

- Two identical environments **(Blue = current, Green = new)** run simultaneously.
- Traffic switches all at once from Blue to Green after testing.
- Zero downtime, but requires double the resources during the transition.
- Tools: Service meshes (Istio), Kubernetes Services with label switching.

How it works:

1. Deploy the new version to the **Green** environment.
2. Test it thoroughly.
3. Switch traffic from **Blue** to **Green** (usually via a load balancer).
4. If something goes wrong, you can quickly roll back to **Blue**.

Pros:

- Instant rollback.
- No downtime during switch.

Cons:

- Requires double the infrastructure (two environments).

Implementation in Kubernetes

Using Services & Selectors

1. Deploy **v1 (Blue)** and **v2 (Green)** with different labels:

```
# Blue (v1)
apiVersion: apps/v1
kind: Deployment
metadata:
  name: app-v1
spec:
  replicas: 3
  selector:
    matchLabels:
      app: myapp
      version: v1
  template:
    metadata:
      labels:
        app: myapp
        version: v1
```

```
    spec:
      containers:
      - name: app
        image: myapp:v1

# Green (v2)
apiVersion: apps/v1
kind: Deployment
metadata:
  name: app-v2
spec:
  replicas: 3
  selector:
    matchLabels:
      app: myapp
      version: v2
  template:
    metadata:
      labels:
        app: myapp
        version: v2
    spec:
      containers:
      - name: app
        image: myapp:v2
```

2. Use a **Service** to switch traffic:

```
apiVersion: v1
kind: Service
metadata:
  name: myapp-service
spec:
  selector:
    app: myapp
    version: v1  # Initially points to Blue (v1)
  ports:
    - protocol: TCP
      port: 80
      targetPort: 8080
```

3. **Cutover to Green (v2)** by updating the Service selector:

```
kubectl patch service myapp-service -p '{"spec":{"selector":{"version":"v2"}}}'
```

4. 🐤 Canary Deployment

Concept:

- Gradually roll out the new version to a small subset of users before a full rollout.

How it works:

1. Deploy the new version to a small percentage of users (e.g., 5%). **Gradually shifts traffic** (e.g., 5% → 20% → 100%) to the new version.
2. **Monitors metrics** (errors, latency) before full rollout. [Monitor for errors or performance issues.]
3. Gradually increase traffic to the new version.
4. If stable, complete the rollout; if not, roll back.
5. **Reduces risk** by testing in production with a small subset of users.

Pros:

- Safer, controlled rollout.
- Real-world testing with minimal risk.

Cons:

- More complex monitoring and traffic routing setup.

When to Use?

✓ **A/B testing** (e.g., UI changes).
✓ **High-risk updates** (e.g., major version upgrades).

Implementation in Kubernetes

Using Nginx Ingress (Traffic Splitting)

1. Deploy **v1 (stable)** and **v2 (canary)**:

```yaml
# Stable (v1)
apiVersion: apps/v1
kind: Deployment
metadata:
  name: app-v1
spec:
  replicas: 3
  selector:
    matchLabels:
      app: myapp
  template:
    metadata:
      labels:
        app: myapp
        version: v1
    spec:
      containers:
      - name: app
        image: myapp:v1

# Canary (v2)
apiVersion: apps/v1
kind: Deployment
metadata:
```

```
  name: app-v2
spec:
  replicas: 1  # Fewer replicas = less traffic
  selector:
    matchLabels:
      app: myapp
  template:
    metadata:
      labels:
        app: myapp
        version: v2
    spec:
      containers:
      - name: app
        image: myapp:v2
```

2. Configure **Ingress** to split traffic:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: myapp-ingress
  annotations:
    nginx.ingress.kubernetes.io/canary: "true"
    nginx.ingress.kubernetes.io/canary-weight: "10"  # 10% to v2
spec:
  rules:
  - host: myapp.example.com
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: myapp-service
            port:
              number: 80
```

3. **Gradually increase traffic**:

```
kubectl annotate ingress myapp-ingress nginx.ingress.kubernetes.io/canary-
weight="50" --overwrite
```

5) DaemonSet

DaemonSet is a Kubernetes object that ensures that a specific pod runs on every node in a cluster. It is useful for running background tasks, system monitoring, or log collection on every node.

How DaemonSet Works?

1. **Node Addition** → If a new node joins, the DaemonSet **automatically schedules a Pod** on it.
2. **Node Removal** → If a node is deleted, its Pod is **garbage-collected**.
3. **Manual Scaling?** → No, it's **node-dependent** (unlike Deployments).

Example YAML:

```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  name: fluentd
  namespace: logging
  labels:
    app: fluentd-logging
spec:
  selector:
    matchLabels:
      name: fluentd
  template:
    metadata:
      labels:
        name: fluentd
    spec:
      containers:
      - name: fluentd-elasticsearch
        image: quay.io/fluentd_elasticsearch/fluentd:v2.5.2
        resources:
          limits:
            memory: 200Mi
          requests:
            cpu: 100m
            memory: 200Mi
        volumeMounts:
        - name: varlog
          mountPath: /var/log
      terminationGracePeriodSeconds: 30
      volumes:
      - name: varlog
        hostPath:
          path: /var/log
```

Key Components:

1. tolerations → Allows Pods to run on master nodes (if needed).
2. hostPath **volumes** → Access node files (e.g., logs).
3. selector.matchLabels → Ensures only DaemonSet-managed Pods are controlled.

🔧 Common Use Cases

Use Case	Description
Log collection	Run agents like Fluentd or Logstash on every node.
Monitoring	Deploy Prometheus Node Exporter or Datadog agents.
Networking	Run CNI plugins or kube-proxy on each node. (Calico, Weave)
Security	Install security agents or scanners on all nodes.

How DaemonSets Differ from Other Controllers

- **Deployment**: Focuses on stateless applications and scalable services, with pods distributed across nodes based on resource needs.
- **StatefulSet**: Manages stateful applications where stable pod identities and persistent storage are required.
- **DaemonSet**: Ensures pods are deployed uniformly across all (or selected) nodes, mainly for system-level tasks.

6) StatefulSet

StatefulSet:

- A **StatefulSet** is a Kubernetes controller designed to **manage and deploy stateful applications** that require **persistent storage**, **stable network identity**, and **ordered deployment or scaling.**
- It ensures each Pod has a **unique and stable identity** (like pod-0, pod-1) and a **dedicated persistent storage volume** that persists even during scaling, node failures, or replacements.
- Unlike **Deployments** used for **stateless applications**, **StatefulSets** are specifically built for **stateful workloads** where the **order of Pod creation**, **deletion**, and **stable identities** are crucial.
- They are ideal for running **databases** and **clustered applications** (e.g., MongoDB, Kafka, Cassandra).
- StatefulSets are defined using a YAML manifest that includes:
    - A **Pod template**
    - A **Headless Service** (clusterIP: None) for stable DNS
    - A **VolumeClaimTemplate** to create PVCs per Pod

A **StatefulSet** is a Kubernetes workload API object used to manage **stateful applications** that require:

- Stable, unique network identifiers
- Persistent storage
- Ordered, graceful deployment and scaling

A **StatefulSet** ensures that:

- Each pod has a **unique, stable name** (e.g., web-0, web-1, web-2).
  Pattern **<statefulset-name>-<ordinal>.**
- Each pod gets its own **persistent volume**, which is **not shared** and **not deleted** when the pod is removed.
- Pods are **created, updated, and deleted in order**.

🔧 Key Features

Feature	Description
Stable Identity	Each pod keeps the same name and network identity. (pod-0, pod-1 etc.)
Persistent Storage	Each pod gets a dedicated volume that persists across restarts.
Ordered Operations	Pods are started, updated, and terminated in a defined order. (0→1→2)
Use Case	Databases (MySQL, Cassandra), Kafka, Zookeeper, etc.

🧠 When to Use StatefulSet?

✓ Databases (MySQL, PostgreSQL, MongoDB)
✓ Message queues (Kafka, RabbitMQ)
✓ Any application requiring:

- Stable network identity
- Requires **persistent storage** tied to each pod.
- Must be **started or stopped in a specific order**. (Ordered deployments)

Example YAML:

```yaml
apiVersion: v1
kind: Service
metadata:
  name: redis
  namespace: default
  labels:
    app: redis
spec:
  ports:
  - port: 6379
    protocol: TCP
  selector:
    app: redis
  type: ClusterIP
  clusterIP: None
```

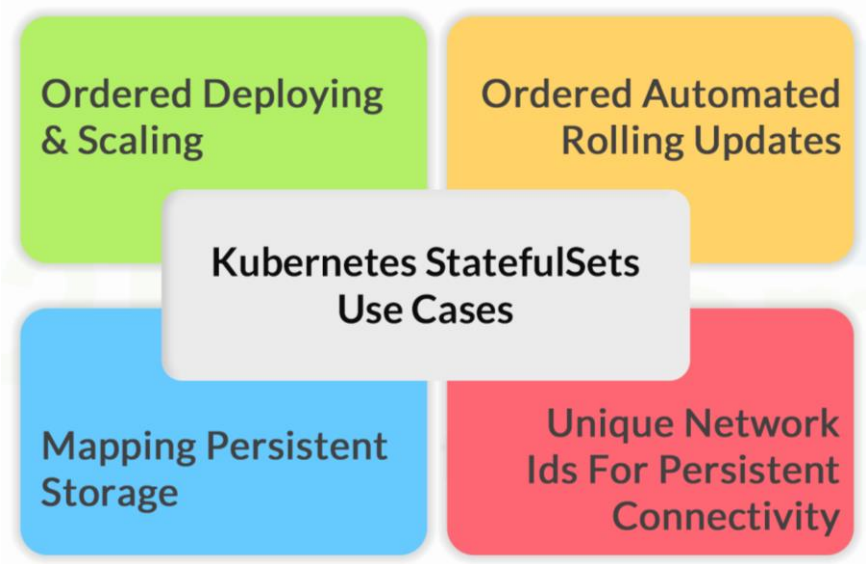
```yaml
---
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: redis
spec:
  selector:
    matchLabels:
      app: redis
  serviceName: "redis"
  replicas: 1
  template:
    metadata:
      labels:
        app: redis
    spec:
      containers:
      - name: redis
        image: redis:5.0.4
        command: ["redis-server"]
        ports:
        - containerPort: 6379
          name: web
        volumeMounts:
        - name: redis-aof
          mountPath: /data
  volumeClaimTemplates:
  - metadata:
      name: redis-aof
    spec:
      accessModes: [ "ReadWriteOnce" ]
      storageClassName: "gp2"
      resources:
        requests:
          storage: 1Gi
```

Explanation:

1. **Pod Naming**:
    - Pods are named sequentially, like mongodb-0, mongodb-1, mongodb-2.
2. **Persistent Volumes (volumeClaimTemplates)**:
    - Dynamically provisions PVs for each pod.
    - Ensures data persistence across pod even if a pod is recreated. its data is retained.
3. **Order Pod Management**:
    - Pods are created one after another (from mongodb-0 to mongodb-2) and terminated in reverse order.

Common Use Cases for StatefulSets

1. **Databases**:
   - Applications like MySQL, PostgreSQL, MongoDB, or Cassandra, where data consistency is critical.
2. **Distributed File Systems**:
   - Systems like Ceph or GlusterFS require persistent storage and stable network identities.
   - Elasticsearch, Cassandra, ZooKeeper
3. **Message Queues**:
   - Services like Kafka or RabbitMQ that rely on ordered operations.



Kubernetes Deployment VS StatefulSet:

1. Overview

Feature	Deployment	StatefulSet
Purpose	Stateless applications	Stateful applications
Pod Identity	No stable identity (interchangeable)	Stable hostname + ordinal number
Scaling	Seamless scaling up/down	Ordered scaling (0→1→2...)
Storage	Ephemeral or shared volumes	Persistent, pod-specific volumes
Networking	Random service endpoints	Stable DNS names (pod-0, pod-1)
Rollout Strategy	Rolling updates (default)	Ordered updates (or rolling)

Feature	Deployment	StatefulSet
Use Cases	Web servers, APIs, microservices	Databases (MySQL, Kafka, etc.)

2. Key Differences Explained

A. Pod Identity & Naming

- **Deployment**:
  - Pods get random names (e.g., nginx-7dfd6c7b9c-abc12).
  - No guaranteed order during restarts.
- **StatefulSet**:
  - Pods get **stable, predictable names** (e.g., mysql-0, mysql-1).
  - Each pod retains its identity even after rescheduling.

B. Scaling Behavior

- **Deployment**:
  - Pods are **scaled arbitrarily** (no order).
  - Deleting a pod creates a new one with a random name.
- **StatefulSet**:
  - Scaling follows **strict order** (0→1→2...).
  - Downscaling deletes pods in **reverse order** (2→1→0).

C. Storage (Persistent Volumes)

- **Deployment**:
  - Typically uses **emptyDir** or **shared volumes** (all pods write to the same storage).
- **StatefulSet**:
  - Each pod gets **its own PersistentVolume (PV)** via volumeClaimTemplates.
  - Example (MySQL StatefulSet):

```
volumeClaimTemplates:
- metadata:
    name: mysql-data
  spec:
    accessModes: ["ReadWriteOnce"]
    resources:
      requests:
        storage: 10Gi
```

D. Networking (DNS & Service Access)

- **Deployment**:
  - Accessed via a **single Service** (load-balanced).
  - No individual pod DNS.
- **StatefulSet**:
  - Each pod gets a **stable DNS name** (e.g., mysql-0.mysql.default.svc.cluster.local).
  - Requires a **headless Service** (clusterIP: None).

---

3. When to Use Which?

Use Deployment If:
✓ Running **stateless apps** (e.g., Nginx, APIs).
✓ Need **rolling updates** with zero downtime.
✓ Pods are **interchangeable** (no persistent data).

Use StatefulSet If:
✓ Running **stateful apps** (e.g., MySQL, MongoDB, Kafka).
✓ Need **stable pod names and storage**.
✓ Require **ordered scaling** (e.g., primary-replica databases).

Final Recommendation

- **Use** Deployment **for stateless, scalable microservices.**
- **Use** StatefulSet **for databases, queues, and clustered stateful apps.**

7) Jobs

Jobs:

- **A Job** is a Kubernetes controller used to **run a specific task to completion or batch job**. It is designed for one-time or on-demand tasks that terminate automatically after completion.
- Jobs are ideal for **short-lived tasks** such as batch processing, data analysis, or backups.
- A Job creates **one or more pods** to run the task and **monitor their completion status**. If a pod fails, the Job automatically replaces it to ensure the task is successfully completed.
- Jobs are configured using a **YAML manifest** that includes:
  - A **Pod template**
  - **Completion criteria** (completions, parallelism)
  - Optional retry settings (backoffLimit)

A **Job** creates one or more Pods to run a **specific task to completion**.

🔧 **Key Features**

Feature	Description
One-time execution	Runs a task once and exits. like data processing or backups.
Retry on failure	Automatically retries failed pods. If a pod fails during job execution, Kubernetes automatically retries the job until it succeeds or meets the set limit.
Parallelism	Can run multiple pods in parallel.
Completion tracking	Tracks how many pods have completed successfully, even if Pods fail.

Feature	Description
Automatic cleanup	Once the task is finished, the Job and its Pods are removed.

Example YAML:

```yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: kubernetes-parallel-job
  labels:
    jobgroup: jobexample
spec:
  completions: 6
  parallelism: 2
  template:
    metadata:
      name: kubernetes-parallel-job
      labels:
        jobgroup: jobexample
    spec:
      containers:
      - name: c
        image: devopscube/kubernetes-job-demo:latest
        args: ["100"]
      restartPolicy: OnFailure
```

Explanation:

1. **completions**: Specifies how many times the job needs to complete successfully (here, 1 time).
2. **parallelism**: Sets the number of pods to run simultaneously (here, 1 pod).
3. **restartPolicy**: Ensures the pod doesn't restart on completion (Never).
    - **Never:** Pod won't restart after failure
    - **OnFailure:** Pod will restart if fails

Job Lifecycle

1. **Created** → Job object created
2. **Pod Creation** → Kubernetes creates Pod(s)
3. **Running** → Pod executes task
4. **Completion** → Pod exits successfully
5. **Cleanup** → Completed Pods remain for debugging (by default)

Common Use Cases for Jobs

1. **Batch Processing**: Process large datasets (e.g., image or video processing).

2. **Data Backups**: Perform database dumps and store them securely.
3. **Maintenance Tasks**: Automate cleanup tasks like deleting outdated resources.
4. **Analytics**: Run complex analytics computations on datasets.
5. **Migrations**: When you need to run **one-time tasks** such as database migrations or batch processing.

- Run **data processing** batches or **ETL tasks**.
- Perform **database migrations**.
- Backup operations
- CI/CD pipeline tasks
- Execute **scheduled tasks** (with CronJobs).
- Run **one-time scripts** or **maintenance tasks**.

8) CronJobs

CronJobs:

- A CronJob is a Kubernetes resource that schedules Jobs to run periodically based on a specified schedule. It's like a time-based trigger that initiates Jobs at predefined intervals.
- In Kubernetes, a **CronJob** is a specialized resource used to **schedule and run Jobs at specific time intervals or recurring schedules.**
- A **CronJob** runs **Jobs on a schedule** similar to Linux cron.

A **CronJob** creates **Jobs on a time-based schedule** (similar to Unix/Linux cron).

🔧 **Key Features**

Feature	Description
Scheduled execution	Runs at specific times using cron syntax.
Automatic retries	Retries failed jobs based on configuration.
History Retention	Keeps track of successful/failed jobs.
Concurrency Control	Manages how concurrent jobs are handled
Job Creation	Creates Job objects at scheduled times
Recurring Tasks	Automates repetitive tasks, such as backups, cleanup operations, log rotation, or data synchronization

Cron Expression Format:

The schedule for a CronJob is defined using a cron expression, which consists of five fields:

```
* * * * *
| | | | |
| | | | +--- Day of the week (0 - 7, both 0 and 7 represent Sunday)
| | | +----- Month (1 - 12)
| | +------- Day of the month (1 - 31)
| +--------- Hour (0 - 23)
+----------- Minute (0 - 59)
```

For example:

- `"*/5 * * * *": Runs every 5 minutes.`
- `"0 0 * * *": Runs daily at midnight.`

Examples:

- 0 * * * * - Every hour at :00
- 30 3 * * * - Daily at 3:30 AM
- 0 0 * * 0 - Weekly on Sunday midnight

Example YAML:

```yaml
apiVersion: batch/v1
kind: CronJob
metadata:
  name: kubernetes-cron-job
spec:
 schedule: "*/5 * * * *" # Every 5 minutes
 jobTemplate:
   spec:
    template:
     metadata:
       labels:
         app: cron-batch-job
     spec:
       restartPolicy: OnFailure
       containers:
       - name: kube-cron-job
         image: busybox:1.28
         command: ["echo", "Hello, Kubernetes CronJobs!"]
```

Explanation:

1. **schedule:** Defines when the CronJob should run using a cron expression.

2. **jobTemplate:** Specifies the template for the job that the CronJob will create.
3. **restartPolicy:** Ensures that the pod doesn't restart after completion (Never).
4. **concurrencyPolicy**
    - Allow (default): Concurrent jobs allowed
    - Forbid: Skip new job if previous still running
    - Replace: Cancel current job and start new one

Common Use Cases for CronJobs

1. **Data Backups**: Automating regular backups of databases, filesystems, or applications.
2. **Log Rotation/Cleanup**: Automate deleting old logs files or temporary files to save disk space.
3. **Data synchronization:** Keeping data consistent across different systems or databases
4. **Scheduled Emails**: Send periodic notifications or updates.
5. **Monitoring and alerting:** Running scripts to monitor system health and send alerts.
6. **Recurring Reports generation**: Generating reports at regular intervals.

- **Recurring health checks**

✓ Daily database backups
✓ Hourly log analysis
✓ Weekly report generation
✓ Monthly data archiving
✓ Any recurring task with a fixed schedule

How Jobs and CronJobs Work Together:

1. CronJob Scheduling: The CronJob controller monitors the cluster for CronJob objects. When a CronJob's schedule matches the current time, it creates a new Job.
2. Job Execution: The Job controller creates Pods to execute the task defined in the Job spec.
3. Task Completion: The Pods run the task and report their status to the Job controller.
4. Job Completion: Once all Pods associated with the Job complete successfully, the Job is considered finished.
5. Cleanup: The Job and its Pods are automatically deleted.

By effectively utilizing Jobs and CronJobs, you can automate routine tasks, optimize resource utilization, and ensure the reliability and efficiency of your Kubernetes applications.

Feature	Job	CronJob
Purpose	Executes tasks once or until complete.	Schedules recurring tasks.
Trigger	Manually or programmatically triggered.	Runs on a defined schedule (cron syntax).
Use Case	Database migration, file processing.	Nightly backups, scheduled reports.
Retries	Supports retries on failure.	Inherits retries from the Job template.

Feature	Pod	ReplicaSet	Deployment	DaemonSet	StatefulSet	Job	CronJob
Main Purpose	Runs a single container	Maintains a fixed number of pods	Manages app updates & scaling	Runs a pod per node	Manages stateful apps	Runs a task once	Runs scheduled tasks
Self-healing?	No	Yes	Yes	Yes	Yes	No	No
Scaling?	No	Yes	Yes	No	Yes	No	No
Persistent Storage?	No	No	No	No	Yes	No	No
Use Case	Simple apps	Ensures pod count	Web apps, APIs	Logging, Monitoring	Databases, Kafka	Data processing	Scheduled tasks

9) Namespace in Kubernetes

Namespace:

- **A Kubernetes Namespace** is a virtual cluster within a Kubernetes cluster. It provides a way to organize and isolate resources such as Pods, Services, Deployments, and other objects within the cluster. Namespaces allow different teams or projects to use the same cluster without affecting each other's resources, ensuring resource isolation and access control.

A **Namespace** in Kubernetes is a virtual cluster within a physical cluster.

A Namespace is used to:

- **Organize and isolate resources (like pods, services, deployments).**
- Apply different policies (like resource limits or access control).
- Support multi-tenancy in a single cluster.
- Access control boundaries

📦 Default Namespaces in Kubernetes

Namespace	Purpose
default	Used when no other namespace is specified. resources are created in the default namespace.
kube-system	Contains system components like kube-dns, kube-proxy, scheduler, controller manager.
kube-public	Readable by all users (used for cluster info). This namespace is generally reserved for cluster usage like cluster-info ConfigMap
kube-node-lease	Tracks node heartbeats for node health monitoring.

Key Features of Namespaces:

- **Resource Isolation:** Namespaces allows isolation of environments for different teams or projects to use the same cluster without interference.
- **Resource Quota Management:** It defines limits (e.g., CPU, memory) for resources within a namespace to avoid resource contention.
- **Access Control:** Kubernetes uses Role-Based Access Control (RBAC) to restrict access to specific users or teams in different namespaces.
- **Network Isolation (Policies):** Namespaces are used to control communication between resources in different namespaces. However, by default, Pods in different namespaces can communicate with each other.
- **Default Namespace**
- **Ease of Management**

🧠 When to Use Namespaces?

- Separate environments (e.g., dev, staging, prod).
- Isolate teams or projects.
- Apply different resource quotas or RBAC rules.

Important Considerations

⚠ **Not all objects are namespaced**

- Nodes, PersistentVolumes, ClusterRoles are cluster-scoped

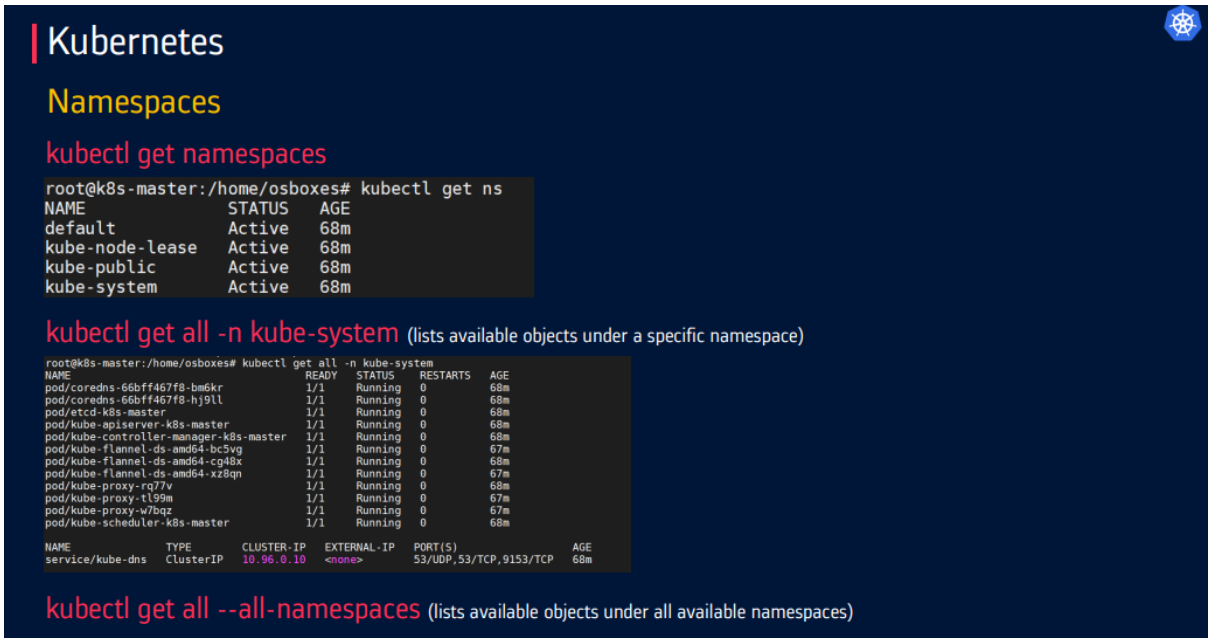
⚠ **Scoping Resources:**

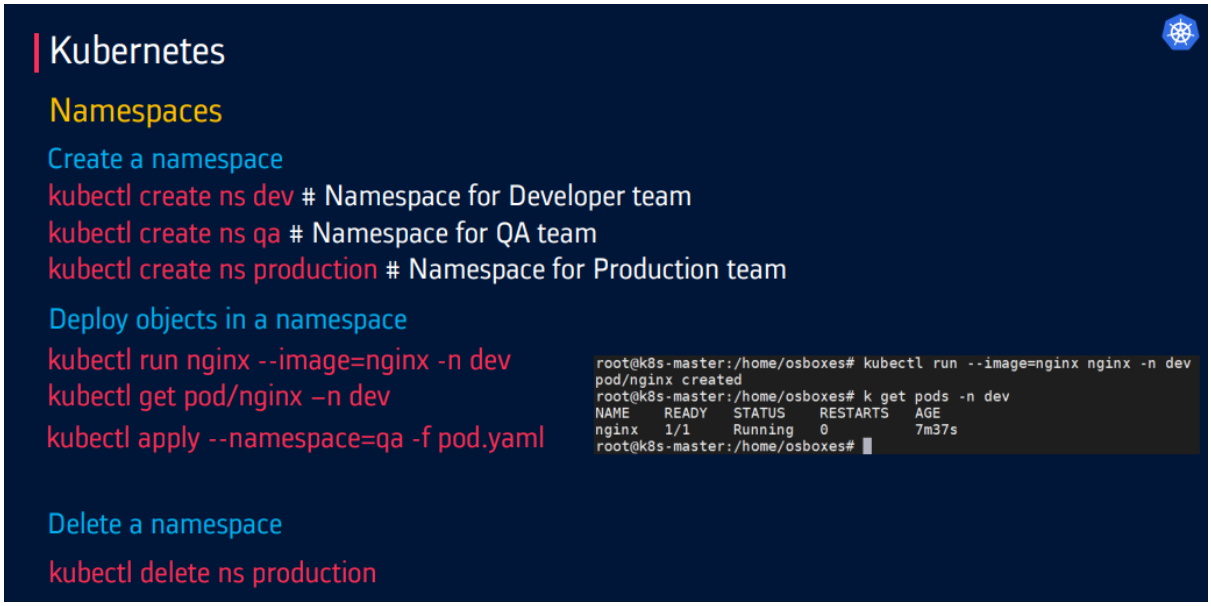
- Resources like Pods, Services, ConfigMaps, and Secrets are created within a specific namespace.

Namespace vs Cluster

Feature	Namespace	Cluster
Scope	Virtual partition	Physical cluster

Feature	Namespace	Cluster
Isolation	Logical	Physical
Resources	Shares cluster resources	Dedicated resources
Access Control	RBAC per namespace	Cluster-wide policies





10) Volumes

Volumes:

- In Kubernetes, **Volumes** are used to manage **persistent storage** to containers. Pods are temporary, but **Volumes help keep the data alive** even if the Pod dies or restarts.
- a Volume is a directory accessible to containers in a Pod that allows data to persist beyond the container's lifecycle.

Volumes are used to manage **persistent or shared storage for containers** running in Pods. Unlike the ephemeral storage inside a container, volumes provide a way to persist data across container restarts or share data between containers in the same Pod.

🔹 Key Concepts of Kubernetes Volumes

1. **Ephemeral vs Persistent Storage**
   - Ephemeral: Data is lost when the container restarts.
   - Persistent: Data is retained using volumes, even if the container restarts.
2. **Volume Lifecycle**
   - A volume exists as long as the Pod exists.
   - For longer persistence, use Persistent Volumes (PVs) and Persistent Volume Claims (PVCs).

Key Components:

PV (PersistentVolume)
A pre-provisioned storage resource in the cluster, like a hard disk.
A piece of storage in the cluster provisioned by an admin or dynamically.
PVC (PersistentVolumeClaim)
A request made by a Pod to use storage (i.e., "I need 5Gi of space").

A request for storage by a user.
StorageClass
Defines **how storage is created,** including type (like SSD, HDD), speed, etc. It enables **dynamic provisioning** of storage.

Key Volume Features

Feature	Description
Lifecycle	Tied to Pod lifecycle (unless using PersistentVolumes)
Sharing	Multiple containers in a Pod can access same volume
Types	Many storage backends supported (local, cloud, network, etc.)
Persistence	Some types persist beyond Pod lifetime

Types of Kubernetes Volumes

There are different types of volumes you can use in a Kubernetes pod:

- ❑ **Node-local memory** (emptyDir and hostPath)
- ❑ **Cloud volumes** (e.g., awsElasticBlockStore, gcePersistentDisk, and azureDiskVolume)
- ❑ **File-sharing volumes,** such as Network File System (NFS)
- ❑ **Distributed-file systems** (e.g., CephFS and GlusterFS)
- ❑ **Special volume types** such as PersistentVolumeClaim, secret, configmap and gitRepo

1. Ephemeral Volumes
- Exist only while Pod runs
- Examples: emptyDir, configMap, secret
- Types like emptyDir or configMap last only for the lifecycle of a pod.

2. Persistent Volumes
- Survive Pod restarts
- Examples: persistentVolumeClaim, awsElasticBlockStore, nfs

3. Special Purpose Volumes
- For specific use cases
- Examples: downwardAPI, projected

🔸 Types of Volumes

Volume Type	Description
Ephemeral emptyDir	Temporary storage shared between containers in a Pod. Deleted when the Pod is removed. (Temporary directory created when Pod starts)
hostPath	Mounts a file or directory from the host node's filesystem into the pod.

Volume Type	Description
configMap	Mounts configuration data as files.
secret	Mounts sensitive data like passwords or tokens.
persistentVolumeClaim	**PVC:** A request for PV by a pod to claim storage resources. **PV:** Pre-provisioned storage in the cluster, independent of pods.
Nfs (Network File System)	Mounts a remote Network File System share. Allows multiple pods across nodes to access shared storage on an NFS server.
CSI (Container Storage Interface)	Enables Kubernetes to integrate with external storage systems.
awsElasticBlockStore, gcePersistentDisk, azureDisk	Cloud provider-specific persistent storage.

Persistent Volume (PV) & PVC Workflow

1. **Admin provisions PV** (storage resource in cluster)
2. **User creates PVC** (storage request)
3. **Kubernetes binds PVC to PV**
4. **Pod uses PVC**

Example Volume Configuration

Here's an example of a pod with a PersistentVolume and PersistentVolumeClaim:

PersistentVolume (PV):

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: my-pv
spec:
  capacity:
    storage: 1Gi
  accessModes:
    - ReadWriteOnce
  hostPath:
    path: /mnt/data
```

PersistentVolumeClaim (PVC):

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
```

```yaml
metadata:
 name: my-pvc
spec:
 accessModes:
  - ReadWriteOnce
 resources:
  requests:
   storage: 1Gi
```

Pod Using PVC:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
spec:
  volumes:
  - name: my-volume
    persistentVolumeClaim:
      claimName: my-pvc
  containers:
  - name: my-container
    image: busybox
    volumeMounts:
    - mountPath: /data
      name: my-volume
    command: ["sh", "-c", "echo Hello Kubernetes > /data/hello.txt && sleep 3600"]
```

AWS EBS Example

```yaml
volumes:
- name: ebs-volume
  awsElasticBlockStore:
    volumeID: "vol-123456"
    fsType: "ext4"
```

AWS EBS Volume Example

1. StorageClass (Dynamic Provisioning)

```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ebs-sc
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp3  # gp2, gp3, io1, io2, sc1, st1
```

```
  fsType: ext4
  encrypted: "true"  # Enable EBS encryption
volumeBindingMode: WaitForFirstConsumer  # Recommended for EBS
reclaimPolicy: Delete  # Or Retain for persistent data
```

2. PersistentVolumeClaim (PVC)

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: ebs-pvc
spec:
  accessModes:
    - ReadWriteOnce  # EBS only supports RWO
  storageClassName: ebs-sc
  resources:
    requests:
      storage: 10Gi
```

3. Pod Using the EBS Volume

```
apiVersion: v1
kind: Pod
metadata:
  name: ebs-pod
spec:
  containers:
  - name: app
    image: nginx
    volumeMounts:
    - name: ebs-storage
      mountPath: "/usr/share/nginx/html"
  volumes:
  - name: ebs-storage
    persistentVolumeClaim:
      claimName: ebs-pvc
```

4. Static Provisioning (Existing EBS Volume)

If you need to use an **existing EBS volume** (instead of dynamic provisioning):

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: ebs-pv
spec:
  capacity:
    storage: 10Gi
  accessModes:
```

```
    - ReadWriteOnce
  awsElasticBlockStore:
    volumeID: vol-1234567890abcdef0  # Your EBS volume ID
    fsType: ext4
  storageClassName: ebs-sc  # Optional: Match to StorageClass
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: ebs-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 10Gi
  volumeName: ebs-pv  # Explicitly bind to existing PV
```

Key AWS-Specific Parameters

Parameter	Values	Description
type	gp2, gp3, io1, io2, sc1, st1	EBS volume type
iopsPerGB	e.g., "10"	Required for io1/io2 types
encrypted	"true"/"false"	Enable EBS encryption
kmsKeyId	AWS KMS key ARN	Custom encryption key

Verification Commands

```
# Check StorageClass
kubectl get storageclass ebs-sc

# Verify PVC status
kubectl get pvc ebs-pvc

# Check PV (auto-created for dynamic provisioning)
kubectl get pv

# Verify Pod mounted the volume
kubectl describe pod ebs-pod | grep -A 5 "Volumes"
```

When to Use Volumes

- Database storage
- Configuration files

- Shared cache between containers
- SSL certificates
- Application logs

Access Modes

Mode	Description
ReadWriteOnce (RWO)	Read-write by single node (EBS, GCE PD)
ReadOnlyMany (ROX)	Read-only by many nodes. Some file/NFS systems
ReadWriteMany (RWX)	Read-write by many nodes. NFS, CephFS, AzureFile
ReadWriteOncePod (RWOP)	Read-write by single pod. CSI drivers supporting this

Reclaim Policy (For PVs)

Policy	**What Happens When PVC is Deleted**	**Use Case**
Retain	Volume is kept (not deleted)	Critical data that should never be automatically deleted
Delete	Volume is automatically deleted	Temporary or easily reproducible data
Recycle (Deprecated)	Volume is wiped and made available again	Older clusters (not recommended)

11) ConfigMaps and Secrets in Kubernetes

ConfigMaps and **Secrets** are used to manage **configuration data and sensitive information** for applications running within the cluster.

1. ConfigMaps

- A **ConfigMap** is used to **store non-sensitive configuration data** as **key-value pairs**. This can include things like:
  - Application settings
  - Environment variables
  - Command-line arguments
  - Configuration files

Key Features of ConfigMaps:

- Store configuration separate from application code

- Can be mounted as files or exposed as environment variables
- **Application Environment Variables**: Pass configuration details as environment variables or volume mounts.

Example of ConfigMap:

Create a ConfigMap

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: app-config
data:
  ENV: production
  LOG_LEVEL: info
  API_URL: https://api.example.com
```

Use ConfigMap in a Pod (as Environment Variables)

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-app
spec:
  containers:
    - name: app-container
      image: myapp:latest
      env:
        - name: ENV
          valueFrom:
            configMapKeyRef:
              name: app-config
              key: ENV
        - name: LOG_LEVEL
          valueFrom:
            configMapKeyRef:
              name: app-config
              key: LOG_LEVEL
```

Use ConfigMap as a File (Mounted Volume)

```yaml
volumes:
  - name: config-volume
    configMap:
      name: app-config
containers:
  - name: app
    volumeMounts:
      - name: config-volume
        mountPath: /etc/config
```

2. Create a ConfigMap to store application settings:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: app-config
data:
  APP_ENV: production
  LOG_LEVEL: debug
```

Use the ConfigMap in a Pod:

```
apiVersion: v1
kind: Pod
metadata:
  name: example-pod
spec:
  containers:
  - name: example-container
    image: busybox
    env:
    - name: APP_ENV
      valueFrom:
        configMapKeyRef:
          name: app-config
          key: APP_ENV
    - name: LOG_LEVEL
      valueFrom:
        configMapKeyRef:
          name: app-config
          key: LOG_LEVEL
```

Explanation:

- **APP_ENV:** The environment variable is set to production from the ConfigMap.
- **LOG_LEVEL:** Configures the logging level as debug.

Inside your container, the config will appear as files:

- /etc/config/ENV
- /etc/config/LOG_LEVEL

Types of ConfigMaps

There's **no official "type" field**, but there are **ways to create ConfigMaps**:

A. **From Literal Values**
   kubectl create configmap my-config --from-literal=ENV=prod

B. **From a File**

kubectl create configmap my-config --from-file=config.properties

C. **From a Directory**
kubectl create configmap my-config --from-file=./config-dir/

Each file or line in the directory becomes a key in the ConfigMap.

Common Use Case:
Dynamically update the environment configuration for a web application without rebuilding or redeploying its containers.

- **Dynamic Updates**:
  - **If used as environment variables:** changes **won't reflect** unless the Pod is restarted.
  - **If mounted as a volume:** changes **can auto-refresh** (depending on how Kubernetes is set up).
- 📦 **Helm + ConfigMaps**: In production, you often manage ConfigMaps using Helm charts for templating and versioning.
- 🔁 **Rolling Updates**: You can trigger a rolling update by modifying the ConfigMap and restarting the Pods.

2. Secrets

- **A Secret** is used to **store sensitive data** like**:**
  - **Passwords**
  - **API keys**
  - **Tokens**
  - **SSH keys**
  - **TLS certificates**

- Secrets are **base64-encoded** and can be **encrypted at rest** by the Kubernetes API server.

✅ **Use Cases:**

- Storing credentials securely
- Injecting secrets into containers as environment variables or mounted files

🧱 **Types of Secrets**

Type	Description
Opaque (default)	Generic key-value pairs (most common)
kubernetes.io/tls	TLS cert and private key
kubernetes.io/dockerconfigjson	Docker registry credentials for private image pulls
kubernetes.io/basic-auth	For username/password pairs
kubernetes.io/ssh-auth	SSH keys

Example of Secrets:

Create a Secret to store database credentials:

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: db-credentials
type: Opaque
stringData:
  username: admin
  password: SuperSecretPass123
```

Use the Secret in a Pod:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: db-pod
spec:
  containers:
  - name: db-container
    image: busybox
    env:
    - name: DB_USERNAME
      valueFrom:
        secretKeyRef:
          name: db-credentials
          key: username
    - name: DB_PASSWORD
      valueFrom:
        secretKeyRef:
          name: db-credentials
          key: password
```

Explanation:

- **DB_USERNAME:** Retrieves the username admin from the Secret.
- **DB_PASSWORD:** Retrieves the password SuperSecretPass123.

2. Create a Secret YAML

This stores a DB username and password (values must be base64 encoded):

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: db-secret
type: Opaque
data:
```

```
  username: YWRtaW4=       # base64 for "admin"
  password: cGFzc3dvcmQ=   # base64 for "password"
```

Use Secret in a Pod as Environment Variables

```
apiVersion: v1
kind: Pod
metadata:
  name: secret-demo
spec:
  containers:
    - name: app
      image: myapp:latest
      env:
        - name: DB_USER
          valueFrom:
            secretKeyRef:
              name: db-secret
              key: username
        - name: DB_PASS
          valueFrom:
            secretKeyRef:
              name: db-secret
              key: password
```

Use Secret as a File (Mounted Volume)

```
volumes:
  - name: secret-volume
    secret:
      secretName: db-secret
containers:
  - name: app
    volumeMounts:
      - name: secret-volume
        mountPath: "/etc/secret-data"
```

📁 **Now inside the container:**

- **/etc/secret-data/username will contain admin**
- **/etc/secret-data/password will contain password**

Applying ConfigMaps and Secrets

Use the following commands:

- **Apply ConfigMap:** kubectl apply -f configmap.yaml
- **Apply Secret:** kubectl apply -f secret.yaml

Example: WordPress with ConfigMap and Secret

```yaml
# ConfigMap for non-sensitive config
apiVersion: v1
kind: ConfigMap
metadata:
  name: wordpress-config
data:
  WORDPRESS_DB_HOST: mysql-service
  WORDPRESS_TABLE_PREFIX: wp_

# Secret for database credentials
apiVersion: v1
kind: Secret
metadata:
  name: wordpress-secret
type: Opaque
data:
  WORDPRESS_DB_USER: YWRtaW4=
  WORDPRESS_DB_PASSWORD: UzNjcjN0IQ==

# Deployment using both
apiVersion: apps/v1
kind: Deployment
metadata:
  name: wordpress
spec:
  template:
    spec:
      containers:
      - name: wordpress
        image: wordpress
        envFrom:
        - configMapRef:
            name: wordpress-config
        - secretRef:
            name: wordpress-secret
```

🌎 Real-Time Use Cases

Scenario	How Secrets Help
🔑 Database Access	Store DB credentials securely
🔐 API Authentication	Store API keys or tokens
🔐 TLS/SSL Certificates	Store TLS certs and private keys for HTTPS
📲 Third-party services	Keep credentials for services like AWS, Stripe, etc.

💉 **CI/CD Integration**	**Inject secrets into build pipelines safely**

12) Resource Limits in Kubernetes

Resource Limits:

- In Kubernetes, **Resource Limits** are used to control how much **CPU and memory (RAM)** a container can **use**.
- This helps ensure efficient **resource distribution, prevents resource hogging (**starvation**)**, and improves cluster performance.

🔹 Why Use Resource Limits?

- Prevent a single container from consuming all node resources.
- Ensure high availability and performance.
- Enable Kubernetes to make better scheduling decisions.
- Protect against memory leaks or runaway processes.

🔸 Key Terms

Term	Description
Requests	Minimum amount of CPU/memory guaranteed for the container. Used by the scheduler to place Pods.
Limits	Maximum amount of CPU/memory a container can use. If exceeded, the container may be throttled or killed.

Types of Resources

Kubernetes allows specifying limits for two primary resources:

1. **CPU** (measured in cores or millicores, e.g., 0.5 CPU or 500m)
2. **Memory** (measured in bytes, e.g., 256Mi, 1Gi)

Consequences of Exceeding Limits (CPU and Memory)

- **CPU Throttling**: If a container exceeds CPU limits, Kubernetes throttles (slowed down), its CPU usage.
- **OOM Kill**: If a container exceeds memory limits, Kubernetes terminates it (OOMKilled).

Key Features of Resource Limits

1. **Requests**: Define minimum resources (CPU & memory) to a container needs to run.
2. **Limits**: Specify the maximum resources a container is allowed to use.
3. **Quality of Service (QoS)**: Kubernetes uses resource requests and limits to categorizes Pods based on their resource settings:
    - **Guaranteed**: Requests = Limits → Stable & reliable performance
      Both requests and limits are equal, ensuring reliable performance.

- **Burstable**: Limits > Requests → Can use extra resources if available
  Pods with higher limits than requests can use extra resources when available.
- **BestEffort**: No requests or limits → May get less priority
  No requests or limits are defined, so resource allocation is uncertain.

Real-Time Example of Resource Limits

Define resource limits for a container running a web server:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: resource-limits-example
spec:
  containers:
  - name: nginx
    image: nginx:latest
    resources:
      requests:
        memory: "128Mi"
        cpu: "500m"
      limits:
        memory: "256Mi"
        cpu: "1"
```

Explanation:

- **Requests**:
  - memory: "128Mi": Guarantees the container will have at least 128MB of memory.
  - cpu: "500m": Ensures the container gets 0.5 CPU cores minimum.
- **Limits**:
  - memory: "256Mi": Caps memory usage to 256MB.
  - cpu: "1": Caps CPU usage to 1 full core.

2. Define CPU & Memory Resource Requests and Limits

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: resource-demo
spec:
  containers:
    - name: app
      image: myapp:latest
      resources:
        requests:
          memory: "128Mi"
          cpu: "250m"
        limits:
          memory: "256Mi"
          cpu: "500m"
```

🔹 This means:

- The container **requests** 128Mi memory and 250 millicores of CPU
- The container can **use up to** 256Mi memory and 500 millicores of CPU

Quality of Service Classes

Based on the above example:

- Pods will be classified as **Burstable** because requests (128Mi) are lower than limits (256Mi).

Real-Time Scenario

Imagine a production environment with:

- **Critical Services** (e.g., payment gateway): Use Guaranteed QoS to ensure reliable performance with equal requests and limits.
- **Batch Jobs** (e.g., video processing): Use Burstable QoS with lower requests to allow flexible allocation when the system has idle resources.
- **Testing Pods** (e.g., debugging tools): Use BestEffort QoS without requests or limits to avoid impacting critical workloads.

Monitoring Resource Usage

Use Kubernetes tools like:

1. **kubectl describe pod**: View resource requests and limits for a pod.
2. **Metric Server**: Monitor live resource usage via kubectl top pod.
3. **Prometheus**: Collect and analyze resource metrics for detailed insights.

You can also set limits on **Ephemeral Storage**:

```
requests:
  ephemeral-storage: "500Mi"
limits:
  ephemeral-storage: "1Gi"
```

✅ Default Resource Limits (LimitRange)

You can set **default limits** at the namespace level:

```
apiVersion: v1
kind: LimitRange
metadata:
  name: mem-limit-range
  namespace: dev
spec:
  limits:
  - default:
      memory: 256Mi
    defaultRequest:
      memory: 128Mi
    type: Container
```

So even if a developer forgets to set resource values, defaults will apply.

⚖️ Resource Quotas

You can combine Resource Limits with **Resource Quotas** to control the **total amount of resources** used by all Pods in a namespace:

```yaml
apiVersion: v1
kind: ResourceQuota
metadata:
  name: dev-quota
spec:
  hard:
    requests.cpu: "2"
    requests.memory: "1Gi"
    limits.cpu: "4"
    limits.memory: "2Gi"
```

🔧 Best Practices

- Always set both **requests** and **limits**.
- Use **resource quotas** at the namespace level to control total usage.
- Monitor usage with tools like **Prometheus**, **Grafana**, or **Kubernetes Metrics Server**.

13) Custom Resource Definitions (CRDs), Custom Resources (CRs) in Kubernetes and Custom Controllers

Custom Resource Definitions (CRDs) allow users to extend Kubernetes by defining their own resource types, while **Custom Resources (CRs)** are instances of those resource types. These mechanisms empower developers to create domain-specific abstractions that suit their application needs.

🔸 1. Custom Resource Definition:

- A **Custom Resource Definitions (CRDs)** is a way to **extend Kubernetes** by defining a new **kind** of resource, just like built-in ones (like Pods, Services, etc.).

✅ Purpose:

- Extend the Kubernetes API without modifying the core code.
- Define your own objects (e.g., MyApp, Database, BackupJob or LogCollector).

Key Features of CRDs

1. **API Extension**: CRDs allow users to extend Kubernetes' API dynamically by creating new resource types like Database or Backup.
2. **Declarative Resource Management**: Custom Resources (CRs) can be created, updated, and deleted like native Kubernetes objects.
3. **Custom Controllers**: Controllers can manage CRs, ensuring the desired state of the system.

🔸 2. Custom Resources (CRs)

A **Custom Resource (CR)** is an instance of a CRD. (like how a Pod is an instance of the Pod kind).
Once a CRD is created, you can create and manage CRs just like any other Kubernetes object.

🔸 3. Custom Controllers (Operators)

A Custom Controller watches for changes to Custom Resources and performs actions in response. It ensuring the cluster state matches the desired state.

How It Works:

1. **Watches** for changes **(create/update/delete)** to CRs
2. **Reconciles** the actual state with the desired state.
3. **Takes actions** (e.g., creating Pods, Deployments, etc.).
4. **Automate complex operations** (e.g., backups, scaling, healing).

Key Points:

- You can write a controller/operator to watch your custom resource and act on it.
- Example: When a Database CR is created, the controller could:
  - Create a StatefulSet
  - Configure a PVC
  - Set up a Service
  - Update CR status

🔁 How They Work Together

1. **CRD defines a new resource type.**
2. **CR is an instance of that type.**
3. **Controller watches the CR and acts accordingly.**

Real-Time Example of CRD and CR

Step 1: Define a CRD and Use it

Let's define a Database resource type:

```yaml
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  name: databases.example.com
spec:
  group: example.com
  names:
    kind: Database
    plural: databases
    singular: database
    shortNames:
    - db
  scope: Namespaced
  versions:
  - name: v1
    served: true
```

```
    storage: true
    schema:
      openAPIV3Schema:
        type: object
        properties:
          spec:
            type: object
            properties:
              type:
                type: string
              version:
                type: string
              storage:
                type: string
```

Explanation:

- **group:** Specifies the API group for the custom resource (example.com).
- **names:** Defines how the resource will be identified (e.g., Database with shorthand db).
- **scope:** Indicates whether the resource is namespaced or cluster-wide (Namespaced here).
- **schema:** Defines the structure of the resource's specification, including fields like type, version, and storage.

Step 2: Creating a Custom Resource (CR)

With the Database CRD defined, we can create an instance (CR) of it:

```
apiVersion: example.com/v1
kind: Database
metadata:
  name: my-database
spec:
  type: MySQL
  version: "8.0"
  storage: "10Gi"
```

Explanation:

- **type:** Specifies the type of the database (e.g., MySQL).
- **version:** Defines the version of the database (e.g., 8.0).
- **storage:** Requests 10Gi of storage for the database.

Step 3: Applying the CRD and CR

1. Apply the CRD: kubectl apply -f database-crd.yaml
2. Apply the CR: kubectl apply -f my-database.yaml

📜 Step 1: Define a Custom Resource Definition (CRD)

```
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  name: databases.mycompany.com
```

```yaml
spec:
  group: mycompany.com
  names:
    kind: Database
    plural: databases
    singular: database
  scope: Namespaced
  versions:
    - name: v1
      served: true
      storage: true
      schema:
        openAPIV3Schema:
          type: object
          properties:
            spec:
              type: object
              properties:
                engine:
                  type: string
                version:
                  type: string
                storage:
                  type: string
```

📜 Step 2: Create a Custom Resource Based on the CRD

```yaml
apiVersion: mycompany.com/v1
kind: Database
metadata:
  name: my-database
spec:
  engine: postgres
  version: "14"
  storage: "20Gi"
```

Now you can run:
kubectl get databases
And see your custom object!

✅ Custom Controller (Optional)

A controller can be written to monitor and manage Database Custom Resources (CRs). The controller ensures the desired state, such as provisioning database instances or managing backups.

Common Use Cases for CRDs

1. **Domain-Specific Resources**:
    - Example: Creating resources like Database, Backup, or MonitoringRule to model application-specific abstractions.
2. **Simplify Complex Applications**:
    - Example: Automate lifecycle management for applications like databases or machine-learning models using controllers and CRDs.
3. **Integration with Kubernetes Ecosystem**:
    - Example: Create CRDs to integrate third-party services like cloud databases or monitoring tools.

🌍 **Real-Time Use Cases**

Use Case	Example
🧩 **Databases as a service**	Create a Database CRD to manage Postgres/MySQL instances
📦 **Custom Deployments**	Create a WebApp resource with auto-scaling and config built-in
🔁 **Backups**	Define a Backup CRD that automates snapshots for PVCs or DBs
📊 **Monitoring/Logging**	Use LogCollector or MetricsJob CRDs to define monitoring pipelines

14) Plugins in Kubernetes: CNI, CSI, and CRI

Plugins in Kubernetes enhance its functionality by enabling seamless networking, storage, and container runtime management.

The three key plugin interfaces are:

1. **CNI (Container Network Interface)** – Manages pod networking.
2. **CSI (Container Storage Interface)** – Manages persistent storage.
3. **CRI (Container Runtime Interface)** – Manages container execution.

1. Container Network Interface (CNI)

- CNI is responsible for **managing network connectivity** for Kubernetes pods.
- It provides a way to configure networking resources dynamically when a container is created.
- CNI plugins manage **networking for containers** in Kubernetes. It handles:
    - **Pod IP assignment (**allocation**)**
    - **Enable Pod-to-pod communication** or **(**Enables communication between Pods and services.)
    - **Network policies**

- Ensures pods can communicate within the cluster and with external services.

How It Works

1. When a pod is created, the **kubelet** calls the CNI plugin.
2. The plugin assigns an IP, sets up networking, and connects the pod to the cluster network.
3. When the pod is deleted, the CNI plugin cleans up the network resources.

📄 Example YAML (Network Policy using CNI)

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: deny-all
  namespace: default
spec:
  podSelector: {}
  policyTypes:
    - Ingress
    - Egress
```

➡️ This denies all traffic unless explicitly allowed.

Example: Using Flannel as a CNI Plugin

Flannel is a simple CNI implementation for overlay networks.

- Deploy Flannel using:

kubectl apply -f https://raw.githubusercontent.com/flannel-io/flannel/master/Documentation/kube-flannel.yml

Real-Time Use Case:

- **Flannel** creates an overlay network that enables pods on different nodes to communicate seamlessly. It's commonly used in clusters hosted on bare-metal or cloud providers.

🧱 Popular CNI Plugins:

- **Calico** – (Networking + Network Policies) Adds network policies for security and granular control **and routing.**
- **Weave** – (**Peer-to-peer mesh networking.)** Offers automatic encryption for cluster networking. (**Automatic IP address management.**)
- **Flannel** – Simple overlay networking
- **Cilium** – Powered by eBPF, very fast and secure

2. Container Storage Interface (CSI)

- CSI standardizes the integration of external storage systems with Kubernetes.
- It allows storage vendors to create plugins that manage their resources directly.

- CSI plugins manage **storage for containers.** in Kubernetes. It allows:

- Manages **persistent storage** (dynamic provisioning, attaching volumes, mounting volumes).
- Allows integration with cloud storage (EBS, Azure Disk, GCE PD) and on-prem solutions (Ceph, NFS).
- Working with block/file storage.

How It Works

1. A **StorageClass** defines the provisioner (CSI driver).
2. When a **PersistentVolumeClaim (PVC)** is created, the CSI driver provisions storage.
3. The volume is attached to the node and mounted into the pod.

Example: Using AWS EBS CSI Driver

Create a PersistentVolume with the EBS CSI plugin:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: ebs-pvc
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ebs-sc
  resources:
    requests:
      storage: 10Gi
```

- Apply the plugin: kubectl apply -f ebs-csi-plugin.yaml

2. YAML (Persistent Volume Claim using CSI)

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mypvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
  storageClassName: standard
```

➡️ The CSI driver (like AWS EBS) handles provisioning and attaching the volume.

Real-Time Use Case:

- CSI simplifies the management of persistent storage for stateful applications like databases. For example, using CSI, you can dynamically allocate Amazon EBS volumes for pods running MySQL.

🧱 **Popular CSI Drivers:**

- **AWS EBS CSI**
- **GCP PD CSI**
- **Azure Disk/File CSI**
- **CephFS / Rook**

3. Container Runtime Interface (CRI)

- **Container Runtime Interface (CRI)** is the API that allows Kubernetes to communicate with container runtimes like **containerd** and **CRI-O**. It helps Kubernetes run and manage containers efficiently, without being tied to a specific runtime.
- Kubernetes doesn't run containers itself — it uses a runtime to do that. **CRI** is the "**translator**" between kubelet and container runtimes.

- It is used to manages container runtimes.
    - Allows Kubernetes to communicate with **container runtimes** like containerd or CRI-O.
    - Abstracts the container runtime implementation.
    - Allows swapping runtimes (Docker → containerd → CRI-O) without modifying kubelet.
    - Enables lightweight and efficient container execution.

How It Works

1. The **kubelet** communicates with the **CRI runtime** (e.g., containerd).
2. The runtime pulls images, starts/stops containers, and manages storage.

📄 No YAML Needed

CRI is configured on the **Kubelet side**, not at the Pod level.

Example: Using CRI-O

CRI-O is a lightweight container runtime designed specifically for Kubernetes.

- Configure kubelet to use CRI-O:
  kubelet --container-runtime=remote --runtime-request-url=/var/run/crio/crio.sock

Real-Time Use Case:

- A Kubernetes cluster running CRI-O improves performance for workloads where runtime efficiency is critical, such as in high-throughput microservices environments.

🧱 **Popular CRI Runtimes:**

- **containerd** – **Lightweight, production-grade container runtime.**
- **CRI-O** – Lightweight runtime used by OpenShift. (Kubernetes-native container runtime.)
- **gVisor** – Sandboxed, secure containers
- **Kata Containers** – Lightweight VMs for strong isolation

Comparing CNI, CSI, and CRI

Real-World Scenario

Imagine you're running a Kubernetes cluster for a cloud-based e-commerce application:

1. Use **CNI (Calico)** for pod networking with granular security policies.
2. Use **CSI (AWS EBS)** to allocate storage dynamically for databases.
3. Use **CRI (containerd)** for lightweight container execution.

🧩 Summary Table

Plugin Type	Interface	Purpose	Examples
CNI	**Networking**	**Pod-to-Pod and external communication**	**Calico,** Flannel, Cilium
CSI	**Storage**	**Persistent volume management**	**AWS EBS,** Ceph, OpenEBS
CRI	**Runtime**	**Container lifecycle management**	**containerd,** CRI-O

15) Service Accounts and RBAC in Kubernetes

Kubernetes uses **Service Accounts** for intra-cluster authentication and **Role-Based Access Control (RBAC)** for authorization. Together, they ensure secure access to Kubernetes resources.

1. Service Accounts

- **A Service Account** is an identity used by Pods to interact with the Kubernetes API.
- A **Service Account** in Kubernetes is used to provide an **identity for pods** to **authenticate** with the Kubernetes API server and access cluster resources securely.
- It allows pods to securely interact with the Kubernetes API and access resources in the cluster.
- Unlike **regular user accounts** (designed for human interaction), **service accounts** are for non-human entities such as pods, **apps, controllers, and jobs** to authenticate and perform actions inside the cluster.

✅ Purpose:

- Allow Pods to **authenticate** to the Kubernetes API.
- Automatically mounted into Pods as a **token**.
- Unlike user accounts (for humans), service accounts are for machines/automation.
- Used by controllers, jobs, and other system components.

Key Concepts

- **Default Service Account**: Every namespace has a default service account.
- **Tokens**: Mounted into pods at /var/run/secrets/kubernetes.io/serviceaccount.
- **Automounting**: Pods automatically use the default service account unless specified otherwise.

Key Features of Service Accounts

1. **Secure API Access**: Provides pods with unique credentials to access the Kubernetes API.
2. **Namespace Scope**: Service accounts are scoped to a specific namespace.
3. **Automatic Creation**: Each namespace has a default service account created automatically.
4. **Customization**: You can create custom service accounts with specific permissions.

Real-Time Example of Service Accounts

Creating a Service Account

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: custom-service-account
  namespace: default
```

Apply the service account:

kubectl apply -f service-account.yaml

Using the Service Account in a Pod

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: example-pod
spec:
  serviceAccountName: custom-service-account
  containers:
  - name: example-container
    image: busybox
    command: ["sh", "-c", "echo Hello from custom ServiceAccount!"]
```

Explanation:

- **serviceAccountName:** Tells the pod to use the custom-service-account for API access.

📜 **Step 1: Create a Service Account**

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: my-app-sa
  namespace: dev
```

📜 **Step 2: Use It in a Pod**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
```

```
  namespace: dev
spec:
  serviceAccountName: my-app-sa
  containers:
    - name: my-container
      image: myapp:latest
```

This tells Kubernetes:

📣 "Run this Pod using my-app-sa, so the app inside can access only what it's allowed to."

🔐 Service Account Tokens

A **JWT token** is created for each SA and mounted in the Pod at:

- /var/run/secrets/kubernetes.io/serviceaccount/token

🧰 Bind SAs to Roles using RBAC

To allow only limited actions:

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-pods-binding
  namespace: dev
subjects:
- kind: ServiceAccount
  name: my-app-sa
  namespace: dev
roleRef:
  kind: Role
  name: pod-reader
  apiGroup: rbac.authorization.k8s.io
```

Common Use Cases of Service Accounts

1. **Pods Accessing Secrets**:
    - **Example:** A pod requires access to a **Secret** for database credentials. A service account enables controlled access.
2. **External Authentication**:
    - **Example:** Applications that need to interact with external services securely using Kubernetes authentication.

2. Role-Based Access Control (RBAC)

- **Role-Based Access Control (RBAC) in** Kubernetes is a security mechanism that **restricts access** to **cluster resources** based on **the roles assigned to users, service accounts or groups.**
- It provides fine-grained control over access to cluster resources.
- Define roles, role bindings, and service accounts to grant or restrict access to specific resources and actions within the cluster.

Purpose

- Controls **who (users/service accounts) can do what (verbs) on which resources**.
- Uses **Roles** (namespace-scoped) and **ClusterRoles** (cluster-scoped).
- Binds them using **RoleBindings** or **ClusterRoleBindings**.

Key Components

Component	Scope	Description
Role	Namespaced	Defines a set of permissions within a namespace.
ClusterRole	Cluster-wide	Defines permissions across the cluster (including non-namespaced resources)
RoleBinding	Namespaced	Binds a Role/ClusterRole to a user/group/service account in a namespace.
ClusterRoleBinding	Cluster-wide	Binds a ClusterRole to a user/group/service account across the cluster.

Real-Time Example of RBAC

Creating a Role

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```

Explanation:

- **apiGroups:** Empty string indicates core Kubernetes resources (e.g., pods, services).
- **resources:** Specifies the resources the role applies to (e.g., pods).
- **verbs:** Defines the actions allowed (e.g., get, list).

Binding the Role to a Service Account

Create a RoleBinding to link the pod-reader role with the custom-service-account:

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: read-pods-binding
  namespace: default
subjects:
```

```
- kind: ServiceAccount
  name: custom-service-account
  namespace: default
roleRef:
  kind: Role
  name: pod-reader
  apiGroup: rbac.authorization.k8s.io
```

Explanation:

- **subjects:** Specifies the entity (service account) to bind to the role.
- **roleRef:** References the pod-reader role created earlier.

📜 **Step 1: Create a Role (Namespace-scoped)**

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: dev
  name: pod-reader
rules:
  - apiGroups: [""]
    resources: ["pods"]
    verbs: ["get", "list", "watch"]
```

➡️ This Role allows reading Pods in the dev namespace.

📜 **Step 2: Create a RoleBinding (Assign Role to a User)**

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: read-pods-binding
  namespace: dev
subjects:
  - kind: User
    name: dev-user
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: pod-reader
  apiGroup: rbac.authorization.k8s.io
```

➡️ This binds the pod-reader Role to the user dev-user.

📜 **Cluster-wide Role Example (ClusterRole + ClusterRoleBinding)**

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
```

```
  name: admin-role
rules:
  - apiGroups: ["*"]
    resources: ["*"]
    verbs: ["*"]
```

ClusterRoleBinding

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: admin-binding
subjects:
  - kind: User
    name: admin-user
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: admin-role
  apiGroup: rbac.authorization.k8s.io
```

➡️ Gives full admin access to the user admin-user across the entire cluster.

Common Use Cases of RBAC

1. **Restricting Access**:
    - **Example**: Allow developers to only view pods without making changes.
2. **Separate Dev/Test/Prod Access**
    - **Example**: Developers can access only their namespace.
3. **Granular Resource Management**: **CI/CD Pipelines**
    - **Example**: Grant CI/CD pipelines access to deploy applications but restrict access to secrets.
4. **Service Account Scoping**:
    - **Example**: Bind service accounts to roles for specific tasks, like accessing only storage-related resources.

⚙️ Additional Functionalities

✅ Predefined ClusterRoles

- view → Read-only access (no secrets).
- edit → Modify resources (no RBAC changes).
- admin → Full namespace control.
- cluster-admin → Superuser (cluster-wide).

✅ Integration with Authentication

- RBAC works **after authentication**. Auth systems (like OIDC, Active Directory, etc.) confirm identity → RBAC decides what they're allowed to do.

Best Practices

✅ **Least Privilege Principle**: Grant only necessary permissions.
✅ **Avoid** default **Service Account**: Create dedicated service accounts.
✅ **Use** ClusterRole **Sparingly**: Prefer Role for namespace-scoped access.
✅ **Audit RBAC Rules**: Regularly check unused roles/bindings.

Summary

Feature	Service Account	RBAC
Purpose	Authenticate pods to access Kubernetes APIs.	Define and enforce resource permissions.
Scope	Namespace-specific	Namespace or cluster-wide
Real Time Use Case	Pod accessing external APIs	Developer with read-only access to pods

16) Metrics Server in Kubernetes and Horizontal Pod Autoscaler (HPA)

Kubernetes **Horizontal Pod Autoscaler (HPA)** automatically scales the number of pods in a deployment or replica set based on observed **resource usage like** CPU/memory usage or custom metrics.
The **Metrics Server** provides the necessary resource usage data for HPA to make scaling decisions.

1. Metrics Server

- The **Metrics Server** collects **resource usage data** (**CPU and memory**) from **nodes and pods** within a Kubernetes cluster. These **metrics** are used by **HPA** and other components.

Purpose

- Collects and aggregates (compiles or gathers) **resource metrics** (CPU/memory) from Kubernetes nodes and pods.
- Acts as a lightweight, in-memory monitoring solution.
- Required for **HPA** and **kubectl top commands**.

Key Features

- **Lightweight and scalable**: No persistent storage (unlike Prometheus).
- **Cluster-wide Metrics**: Provides CPU/memory usage for nodes and pods.
- **Kubernetes-native**: Integrates with the Kubernetes API.

Installing Metrics Server

1. Deploy the Metrics Server:
   kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml

2. Verify the installation:
   kubectl get apiservices | grep metrics

Troubleshooting

If **kubectl top fails**:

1. Check logs:
   kubectl logs -n kube-system deployment/metrics-server
2. Common issue:
   SSL/TLS errors (**add --kubelet-insecure-tls flag in deployment args**).

Common Use Cases of Metrics Server

1. Provides resource usage data for tools like HPA.
2. Monitors pod and node performance metrics using kubectl top:
   kubectl top pod
   kubectl top node

Key Considerations

- The Metrics Server must be installed and running for HPA to work with resource metrics.
- Use custom metrics for advanced autoscaling logic (e.g., scaling based on request count or latency).
- Configure resource requests and limits for all containers to avoid unpredictable scaling.

Real-World Scenario

Consider a **cluster hosting** an **API backend** with **unpredictable traffic**:

1. **Deploy Metrics Server** to collect **CPU and memory metrics**.
2. Use **HPA to scale** the **API backend** deployment from 2 to 20 pods **during traffic spikes.**
3. Monitor scaling decisions using: kubectl get hpa

2. Horizontal Pod Autoscaler (HPA)

- The **Horizontal Pod Autoscaler (HPA)** automatically adjusts the **number of Pods** in a Deployment, ReplicaSet, or StatefulSet based on observed **CPU utilization** or **custom metrics**.
- It helps maintain application performance during traffic spikes while optimizing resource usage during idle periods.

Purpose

- Automatically **scales pods horizontally** (increases/decreases replicas) based on:
  - **CPU/Memory usage** (default).
  - **Custom metrics** (e.g., requests per second, queue length).

How HPA Works

1. **Metrics Server** collects CPU/memory usage.
2. **HPA Controller** checks metrics against **defined thresholds**.

3. **Scaling Decision**:
    - If usage > target → **Increase replicas**.
    - If usage < target → **Decrease replicas**.

✅ **Key Features:**

- Scales Pods horizontally (adds/removes replicas).
- Uses metrics like CPU, memory, or custom metrics.
- Helps maintain performance and optimize resource usage.

🔁 **How Metric server and HPA Work Together**

1. Metrics Server collects real-time resource usage.
2. HPA queries the Metrics Server.
3. Based on the metrics, HPA adjusts the number of Pods.

Real-Time Example of HPA

Step 1: Create a Deployment

Start with a deployment:

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: example-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app: example
  template:
    metadata:
      labels:
        app: example
    spec:
      containers:
      - name: example-container
        image: nginx
        resources:
          requests:
            cpu: 200m
          limits:
            cpu: 400m
```

Step 2: Enable HPA

Create an HPA resource to auto-scale the deployment based on CPU usage:

```yaml
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: example-hpa
spec:
```

```yaml
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: example-deployment
  minReplicas: 2
  maxReplicas: 10
  metrics:
  - type: Resource
    resource:
      name: cpu
      target:
        type: Utilization
        averageUtilization: 50
```

Explanation:

- **scaleTargetRef:** Links the HPA to the example-deployment.
- **minReplicas:** Ensures a minimum of 2 replicas are running at all times.
- **maxReplicas:** Caps the scaling to 10 replicas.
- **averageUtilization:** Targets 50% CPU usage. If CPU usage exceeds 50%, the HPA scales up the pods.

Applying the HPA

1. Apply the deployment: kubectl apply -f deployment.yaml
2. Apply the HPA: kubectl apply -f hpa.yaml
3. Monitor scaling: kubectl get hpa

2. Let's create a Horizontal Pod Autoscaler for a **Deployment** based on **CPU usage**.

📜 **Step 1: Define the Deployment**

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  replicas: 1
  selector:
    matchLabels:
      app: my-app
  template:
    metadata:
      labels:
        app: my-app
    spec:
      containers:
        - name: my-container
          image: myapp:latest
          resources:
            requests:
              cpu: "200m"
```

```
            limits:
              cpu: "500m"
```

- Here, the app starts with **1 replica**, and we've defined CPU **requests** and **limits** for the container.

📜 **Step 2: Define the Horizontal Pod Autoscaler (HPA)**

```yaml
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: my-app-hpa
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: my-app
  minReplicas: 1
  maxReplicas: 10
  metrics:
  - type: Resource
    resource:
      name: cpu
      target:
        type: Utilization
        averageUtilization: 50
```

Key points of the HPA YAML:

- **scaleTargetRef**: Points to the Deployment (the object we want to scale).
- **minReplicas**: The minimum number of Pods to maintain (1 in this case).
- **maxReplicas**: The maximum number of Pods to scale to (10 in this case).
- **metrics**: Defines that we are scaling based on CPU utilization. In this example, the target CPU utilization is **50%**.

Troubleshooting HPA

Issue	Solution
HPA shows `<unknown>	Check if Metrics Server is running (**kubectl top pods**).
No scaling happens	Verify **resources.requests** are set in the deployment.
Too frequent scaling	Adjust **behavior.stabilizationWindowSeconds**.

Common Use Cases of HPA

1. **E-commerce Web Applications Traffic Spikes**:
    - Example: Scale an e-commerce app to handle traffic spikes during sales.
2. **Processing Pipelines**:

    - Example: Scale data processing pods during peak workloads.
3. **APIs**:
    - Example: Scale API servers dynamically based on the number of incoming requests.
4. **Microservices:**
    - In microservices architectures, each service can scale independently based on its needs (e.g., scaling a payment service during high load).

🧱 Types of Metrics in HPA

🎛️ 1. Resource Metrics (CPU & Memory)

- **CPU Utilization**: Autoscale based on the CPU usage of Pods.
- **Memory Usage**: Autoscale based on the memory usage of Pods.

🧩 2. Custom Metrics (v2)

- Allows scaling based on application-specific metrics (e.g., number of requests, queue length, latency).
- For custom metrics, you'll need **Prometheus** or another monitoring solution to expose those metrics.

📊 3. External Metrics (v2)

- Scale based on metrics from outside Kubernetes, such as queue length in a messaging system (e.g., RabbitMQ), or request counts from an external API.
- This requires integration with external monitoring systems.

Best Practices

✅ **Set Resource Requests**: HPA needs resources.requests to calculate utilization.
✅ **Avoid Too Aggressive Scaling**: Use behavior to stabilize scaling.
✅ **Monitor HPA Events**:

17) Cluster Autoscaling

Cluster Autoscaling

- **Cluster Autoscaling** in Kubernetes automatically adjusts the number of **nodes** in a cluster based on resource demands.
- Cluster Autoscaling automatically adjusts the size of Kubernetes **node pool** (adding or removing worker nodes).
- This helps optimize resource utilization and costs.

Scaling Triggers

- **Scale-Up**: When pods fail to schedule due to:
    - Insufficient CPU/memory.
    - Node affinity/taint constraints.
- **Scale-Down**: When nodes are underutilized (configurable threshold).

How Cluster Autoscaler Works

1. **Scale Up** – It watches **unschedulable** pods and adjusts node count.

2. **Scale Down** – When nodes are **underutilized** for a certain period, they are removed.
   Node Group Integration – Integrate with **cloud-specific autoscaling groups** to manage instances dynamically.
   Defines min/max size for scaling (e.g., **AWS Auto Scaling Groups**).
3. **Cloud Provider API** – Integrates with AWS/GCP/Azure to manage nodes.

Key Features of Cluster Autoscaler

1. **Automatic Scaling** – Adds or removes nodes based on pod scheduling requirements.
2. **Cost Optimization** – Adds or removes nodes in **node pools** based on pending pods or underutilized nodes to save costs in cloud environments.
3. **Works with Node Groups** – Integrates with cloud providers like AWS, Azure, and GCP.
4. **Improves High Availability** – Ensures pods have enough compute resources to run smoothly.
5. **Pod Scheduling Awareness** – Reacts to unallocated or pending pods by provisioning nodes.

📄 Example YAML Code for Cluster Autoscaler

Step 1: Cluster Autoscaler Deployment YAML

The Cluster Autoscaler is typically deployed as a **Deployment** or **Pod** in your cluster.

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cluster-autoscaler
  namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      app: cluster-autoscaler
  template:
    metadata:
      labels:
        app: cluster-autoscaler
    spec:
      serviceAccountName: cluster-autoscaler
      containers:
        - name: cluster-autoscaler
          image: registry.k8s.io/autoscaling/cluster-autoscaler:v1.21.0
          command:
            - ./cluster-autoscaler
            - --v=4
            - --cloud-provider=aws
            - --nodes=1:10:k8s-nodepool
            - --scale-down-enabled=true
            - --scale-down-unneeded-time=10m
            - --stderrthreshold=info
            - --skip-nodes-with-local-storage=false
```

```
            - --expander=least-waste # Prefer node pool with least wasted
resources
            - --node-group-auto-discovery=asg:tag=k8s.io/cluster-
autoscaler/enabled,k8s.io/cluster-autoscaler/my-eks-cluster
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 200m
              memory: 256Mi
```

Key Points:

- **cloud-provider=aws**: Specifies that the Cluster Autoscaler is set to run on **AWS Cloud (AWS)**.
- **--nodes=1:10:k8s-nodepool**: Specifies the **node pool** (k8s-nodepool) and sets the **minimum** (1 node) and **maximum** (10 nodes) number of nodes.
- **--scale-down-enabled=true**: Enables automatic scaling down of unused nodes.
- **--scale-down-unneeded-time=10m**: A node is removed only if it's unused for at least 10 minutes.

2. Tag Your Auto Scaling Group (ASG)

- Add tags to your ASG:
  - Key: **k8s.io/cluster-autoscaler/enabled** → Value: **true**
  - Key: **k8s.io/cluster-autoscaler/<CLUSTER-NAME>** → Value: **owned**

3. Verify Autoscaler Logs

kubectl logs -n kube-system deployment/cluster-autoscaler

Step 2: Example of ConfigMap (Optional)

Cluster Autoscaler often uses a ConfigMap to configure specific settings. Here's how you can use a ConfigMap to configure the behavior of Cluster Autoscaler:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-autoscaler-config
  namespace: kube-system
data:
  cluster-autoscaler.cfg: |
    scale-down-unneeded-time=10m
    scale-down-delay-after-add=10m
    scale-up-from-zero=true
```

- **scale-down-unneeded-time=10m**: Ensures that a node is only scaled down after being unused for 10 minutes.
- **scale-up-from-zero=true**: Allows scaling the cluster from zero nodes if required.

Pod not schedulable.

1. **Node Selector - will update details in pod yml**
2. **Node Affinity - will update details in pod yml**
3. **Taints - will update configure in nodes**
4. **Tolerations**

Troubleshooting

Issue	Solution
Autoscaler not scaling up	Check ASG tags, IAM permissions, and pod resource requests.
Autoscaler not scaling down	Verify scale-down-utilization-threshold and pod eviction constraints.
Nodes stuck in "NotReady"	Ensure termination hooks and drain operations work.

Combining HPA + Cluster Autoscaler

- **HPA** scales pods horizontally.
- **Cluster Autoscaler** scales nodes to fit the pods.

Example Workflow:

1. HPA increases pod replicas due to high CPU.
2. If no nodes have capacity, Cluster Autoscaler adds a new node.
3. When load decreases, HPA scales down pods.
4. Cluster Autoscaler removes underutilized nodes.

📜 **Example Use Case**

- You have a Deployment with HPA that scales Pods from 2 to 20.
- If the current nodes can't handle 20 Pods, the Cluster Autoscaler will **add more nodes**.
- When traffic drops and fewer Pods are needed, it will **remove unused nodes**.

Best Practices

✅ **Set Pod Resource Requests/ Limits** → Ensures accurate scaling decisions.
✅ **Use Pod Disruption Budgets (PDBs)** → Prevent scale-down from disrupting critical pods.
✅ **Avoid Overlapping Node Pools** → Use separate pools for different workloads (e.g., GPU vs CPU).
✅ **Monitor Autoscaler Events** → Check logs and Kubernetes events. **Prometheus**, **Grafana**,

18) Node Selector

✅ Node Selector:

- A **Node Selector** is **used to schedule Pods onto specific nodes** in a Kubernetes cluster based on **node labels**.
- If no node matches, the Pod will not be scheduled.

🧩 How It Works:

1. **Nodes are labeled** with key-value pairs (e.g., disk=ssd, gpu=true).
2. In the **Pod/Deployment spec**, use nodeSelector to match node labels.
3. Kubernetes **schedules the pod only on nodes** that match the specified labels.

✅ Purpose

- Control **where** a Pod runs.
- Ensure Pods are scheduled only on nodes that meet specific criteria (e.g., hardware, region, OS).

📄 Example YAML for Node Selector

The nodeSelector field in a Pod specification is used to define which nodes the Pod can be scheduled on.

1. Example: Node Selector to Schedule Pod on Specific Nodes

This example shows how to use a Node Selector to schedule a Pod on nodes with a specific label (e.g., zone=us-west-1).

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
spec:
  nodeSelector:
    zone: us-west-1
  containers:
    - name: my-container
      image: nginx
```

Explanation:

- **nodeSelector**: A key-value pair where the key is zone and the value is us-west-1.
- This configuration ensures that the Pod will only be scheduled on nodes that are labeled with zone=us-west-1.

Example of Node Labeling:

- For this nodeSelector to work, the nodes in your cluster need to have a matching label, like:
  kubectl label nodes <node-name> zone=us-west-1

This command adds the label zone=us-west-1 to the specified node. Now, the Pod in the previous YAML can be scheduled on this node.

2. Example with Multiple Node Selectors:
You can specify multiple label selectors in the nodeSelector field, but all conditions must match exactly. Here's an example:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
spec:
  nodeSelector:
    zone: us-west-1
    hardware: gpu
  containers:
    - name: my-container
      image: nginx
```

In this case, Kubernetes will only schedule the Pod on nodes that have both zone=us-west-1 **and** hardware=gpu labels.

3. Example
Step 1: Label a node

- **kubectl label nodes node-1 disktype=ssd**

Step 2: Use nodeSelector in your Pod

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: ssd-pod
spec:
  containers:
    - name: my-container
      image: nginx
  nodeSelector:
    disktype: ssd
```

This Pod will only be scheduled on nodes labeled with disktype=ssd.

Troubleshooting

Issue	Solution
Pod Pending	Check node labels and capacity (kubectl describe pod <pod-name>).
Label Missing	Verify node labels (kubectl get nodes --show-labels).

Differences Between Node Selector and Node Affinity

- **Node Selector**:
  - Simple key-value pair.
  - No flexibility or complex rule-based matching.

    - Only exact matches are allowed.
- **Node Affinity**:
    - More complex and flexible.
    - Can use operators like In, NotIn, Exists, and DoesNotExist.
    - Allows **preferred** and **required** rules for scheduling.

For more complex scheduling needs, **Node Affinity** or **Node Anti-Affinity** might be a better choice.

🛠️ Other Functionalities and Considerations

Taints and Tolerations with Node Selector

- **Node Selector** can be combined with **taints and tolerations** for advanced scheduling.
- **Taints** are applied to nodes to **prevent Pods** from **being scheduled** on c**ertain nodes** unless they have a matching **toleration**.

For example, a node may have a taint like this:
kubectl taint nodes <node-name> dedicated=high-performance:NoSchedule

Then, the Pod must include a toleration to be scheduled on that node:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
spec:
  nodeSelector:
    hardware: gpu
  tolerations:
    - key: "dedicated"
      operator: "Equal"
      value: "high-performance"
      effect: "NoSchedule"
  containers:
    - name: my-container
      image: nginx
```

This configuration ensures the Pod is only scheduled on nodes labeled with hardware=gpu and can tolerate the dedicated=high-performance:NoSchedule taint.

✅ Use Cases:

- Ensuring pods run on nodes with specific hardware (e.g., GPU, SSD).
- Separating workloads by environment (e.g., env=prod vs. env=dev).
- Managing licensing or resource constraints.

⚠️ Limitations:

- Only supports **exact match only** (no expressions or complex logic).
- **Static**: You must manually label nodes and update selectors.

🔄 Alternatives for More Flexibility

Feature	Description
Node Affinity	More expressive (supports operators like In, NotIn, Exists).
Label Missing	Prevent Pods from being scheduled unless they tolerate the node's taint.
Pod Affinity/Anti-Affinity	Schedule Pods based on other Pods' locations.

19) Node Affinity and Anti-Affinity

✅ Node Affinity and Anti-Affinity

- **Node Affinity** and **Node Anti-Affinity** are advanced scheduling features that control pod scheduling by defining rules based on node labels
- They provide fine-grained control beyond simple nodeSelector rules.

1. Node Affinity:

- **Node Affinity** is used to **schedule pods** on **specific nodes** based on **node labels**, similar to **Node Selector**, but offers more flexibility.
  (**e.g.**, "run this Pod on a node labeled as zone=us-west-1").

✳️ Types of Node Affinity Rules:

1. **requiredDuringSchedulingIgnoredDuringExecution (Hard Rule)**
   - Pod **must** be scheduled on Node matching the rule.
   - If no match exists, pod remains unscheduled or pending**.**
2. **preferredDuringSchedulingIgnoredDuringExecution (Soft Rule)**
   - Kubernetes **prefers** to schedule Pods on matching Nodes.
   - If no match exists, Pod is placed elsewhere.

Example YAML for Node Affinity

This example demonstrates how to use node affinity to ensure that a Pod is scheduled only on nodes with a specific label.

Example: Node Affinity to Schedule Pod on Specific Nodes

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
```

```
        nodeSelectorTerms:
          - matchExpressions:
              - key: "zone"
                operator: In
                values:
                  - us-west-1
  containers:
    - name: my-container
      image: nginx
```

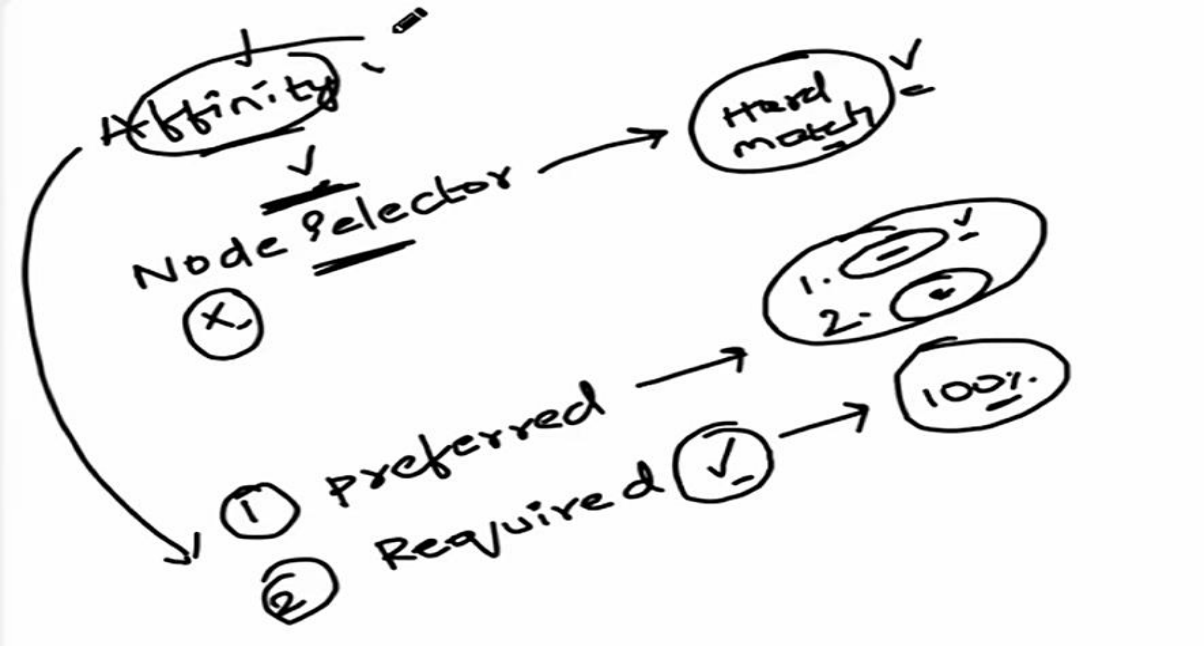
Explanation:

- **nodeSelectorTerms**: Specifies the conditions that the node must meet.
- **key: "zone":** The node must have a label with the key zone.
- **operator: In:** The value of the node's zone label must be in the specified set (here, "us-west-1").

This configuration ensures that the Pod is scheduled only on nodes labeled with zone=us-west-1.

2. Node Anti-Affinity:

- **Node Anti-Affinity prevents pods** from **being scheduled** on **nodes with specific labels.** It's used to **spread pods across nodes** or **to avoid scheduling** on certain types of nodes.
- (e.g., "don't run this Pod on a node labeled as zone=us-west-1").



Types of Node Anti-Affinity

Similar to node affinity, anti-affinity has two types:

1. **requiredDuringSchedulingIgnoredDuringExecution**:
    - **Strict enforcement**: Pods **will not be scheduled** unless the anti-affinity rule is satisfied.

    - **Example**: "I do not want to run this Pod on a node with zone=us-west-1."
2. **preferredDuringSchedulingIgnoredDuringExecution**:
    - The scheduler will try to find a node that meets the anti-affinity rules, but if it cannot find one, the pod will still be scheduled on a node that does not meet the rules.
    - **Example**: "I prefer not to run this Pod on nodes in the us-west-1 zone, but it's not strictly required."

Node Anti-Affinity Example:

This example shows how to use **node anti-affinity** to avoid scheduling Pods on nodes with specific labels.

Example: Node Anti-Affinity to Avoid Certain Nodes

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-pod
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: "zone"
                operator: NotIn
                values:
                  - us-west-1
  containers:
    - name: my-container
      image: nginx
```

Explanation:

- **operator: NotIn**: Specifies that the zone label on the node should **not** be one of the listed values.
- **values: ["us-west-1"]**: The Pod should **not** be scheduled on nodes labeled zone=us-west-1.

This configuration ensures that the Pod **won't** be scheduled on any nodes in the "us-west-1" zone.

Key Operators

Operator	Description
In	Label value is in the specified list.
NotIn	Label value is **not** in the list.

Operator	Description
Exists	Label key exists (values ignored).
DoesNotExist	Label key **does not** exist.

Troubleshooting

Issue	Solution
Pod Stuck in Pending	Check affinity rules and Node labels.
Unexpected Scheduling	Verify weight in soft rules.

⚙️ Other Functionalities of Node Affinity and Anti-Affinity

Advanced Matching

- **matchExpressions**: You can combine multiple conditions to refine scheduling decisions.
    - **Example**: "Pod must be scheduled on a node labeled with zone=us-west-1 and environment=production."
- **matchFields**: You can use **field selectors** to match other attributes, like node name or status.
    - **Example**: "Pod should only be scheduled on nodes with status=Ready."

Combining Affinity with Taints and Tolerations

- You can combine **Node Affinity** with **taints and tolerations** for even more fine-grained control over Pod scheduling.

20) Pod Affinity and Anti-Affinity

- **Pod Affinity** and **Pod Anti-Affinity** are advanced scheduling rules that control **how Pods are placed relative to other Pods** in the cluster.

They help optimize:

- **High Availability** (spread Pods across zones/nodes)
- **Co-location** (group related Pods together)
- **Workload Isolation** (prevent Pods from sharing nodes)

✅ Pod Affinity:

- **Pod Affinity** rules ensure that a **pod is scheduled on the same node** (or in the same zone) as other specified pods, based on labels.

🔹 **Use Case**:

- Used for applications that benefit from **low latency** or **better communication** (e.g., microservices that frequently interact).
- Ensuring Pods that share data are on the same node or zone.

🔧 YAML Examples

✅ Pod Affinity Example: Place Pods together

This Pod wants to run on a node **where another Pod with label app=nginx** is already running.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web-app
spec:
  affinity:
    podAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
              - key: app
                operator: In
                values:
                  - nginx
          topologyKey: "kubernetes.io/hostname"
  containers:
    - name: web
      image: nginx
```

📝 **Explanation**:

- podAffinity: Means "I want to be close to..."
- requiredDuringSchedulingIgnoredDuringExecution: A **hard rule** for scheduling.
- topologyKey: kubernetes.io/hostname: Means Pods should be on the **same node**.

❌ Pod Anti-Affinity:

- **Pod Anti-Affinity** rules **prevent** pods from being scheduled **on the same node (or zone)** as other specified pods, based on labels.
- This is useful for **high availability** or to reduce resource contention.

🔹 **Use Case**:

- Improved **High availability** and **redundancy** (spread replicas across nodes).
- Avoiding resource contention.

❌ Pod Anti-Affinity Example: Place Pods apart

This Pod should **not** run on the same node as another Pod with app=nginx.

```yaml
apiVersion: v1
kind: Pod
```

```yaml
metadata:
  name: web-app
spec:
  affinity:
    podAntiAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
              - key: app
                operator: In
                values:
                  - nginx
          topologyKey: "kubernetes.io/hostname"
  containers:
    - name: web
      image: nginx
```

📝 **Explanation**:

- podAntiAffinity: Means "I want to stay away from..."
- Keeps high-availability workloads separated across nodes.

You can use one or both in a Pod spec depending on how strict you want the rule to be.

🔑 **Key Concepts**

- **topologyKey**: Defines the domain over which the rule applies (e.g., node, zone).
  - Common values: kubernetes.io/hostname, topology.kubernetes.io/zone
- **requiredDuringSchedulingIgnoredDuringExecution**:
  - **Hard rule**: Pod won't be scheduled if the condition isn't met.
- **preferredDuringSchedulingIgnoredDuringExecution**:
  - **Soft rule**: Scheduler tries to meet it, but may ignore if necessary.

Troubleshooting

Issue	Solution
Pod stuck in Pending	Check affinity conflicts with kubectl describe pod.
Unexpected co-location	Verify topologyKey and label selectors.
High churn during scaling	Prefer preferredDuringScheduling over hard rules.

21) Taints and Tolerations

- **Taints and Tolerations** work together to ensure that Pods are only scheduled onto appropriate nodes. They prevent Pods from being scheduled on certain nodes unless the Pods explicitly tolerate the taint. They are essentially the inverse of affinity rules.

They work together but serve opposite roles:

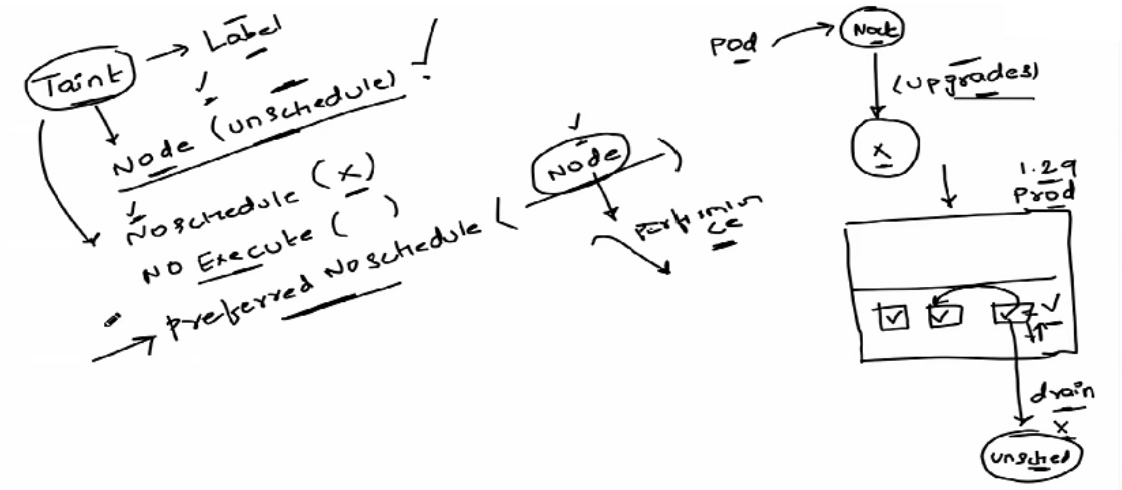
- **Taints** are applied to **Nodes** to prevent (repel) Pods.
- **Tolerations** are applied to **Pods** to allow them to ignore taints.

✅ Taints:

- A **taint** is applied to a **Node** and **prevents Pods** from being scheduled on it unless those Pods have a matching toleration.
- It tells Kubernetes:
  "**Don't schedule any Pod here** unless it can tolerate this taint."

Use Case:

- Prevent regular workloads from running on specialized nodes (e.g., GPU nodes, storage-heavy nodes).



Taint Components

Each taint has three parts:

1. **Key** (e.g., gpu)
2. **Value** (e.g., true)
3. **Effect**:
   - **NoSchedule** → Pods without matching toleration **won't be scheduled**.
   - **PreferNoSchedule** → Kubernetes tries to avoid scheduling but not strictly required.
   - **NoExecute** → Don't schedule and **Evicts existing Pods** without matching toleration

✅ Tolerations:

- **Tolerations** are applied to Pods to allow them to be scheduled on Nodes with matching taints.
- It tells Kubernetes:
  "This Pod is **okay to run on** a node with this specific taint."
  So, taints repel Pods, and tolerations let Pods tolerate (i.e., ignore) that taint.

- A **toleration** is added to a Pod to let it **bypass a Node's taint**.

Use Case:

- Allow certain workloads, like system-critical services, to run on specific nodes despite taints.

Toleration Components

Tolerations match taints using:

- **key, value, and operator (Equal or Exists).**

🔑 Key Features

Feature	Description
🚫 Prevent unwanted scheduling	Taints can block certain Pods from running on sensitive or special nodes.
✅ Allow only specific Pods	Only Pods with matching tolerations can run on tainted nodes.
🎯 Node-level control	Taints are applied per node.

📜 Example:

Add a taint to a node

kubectl taint nodes node1 key=value:NoSchedule

This means: "Do not schedule any Pod on node1 unless it tolerates this taint."

Example YAML + Commands

🧱 Step 1: Add a taint to a node

- kubectl taint nodes <node-name> key=value:NoSchedule

📝 Example:

- kubectl taint nodes worker1 env=prod:NoSchedule

This tells Kubernetes: ❌ "Don't schedule Pods here unless they tolerate env=prod."

📦 Step 2: Pod with a matching toleration

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-prod-pod
spec:
  tolerations:
    - key: "env"
      operator: "Equal"
      value: "prod"
      effect: "NoSchedule"
  containers:
    - name: nginx
      image: nginx
```

✅ This Pod says: “I tolerate the env=prod taint, so it's okay to schedule me there.”

📜 **More Examples**

⛔ **NoExecute Taint Example**

- kubectl taint nodes worker2 key=value:NoExecute

Pods **without toleration** are evicted immediately.

Toleration with Duration

```yaml
tolerations:
  - key: "key"
    operator: "Equal"
    value: "value"
    effect: "NoExecute"
    tolerationSeconds: 60
```

⏱️ This Pod will be evicted **after 60 seconds** if the taint is added.

Troubleshooting

Issue	Solution
Pod stuck in Pending	Check kubectl describe pod for taint conflicts.
Unexpected evictions	Verify NoExecute taints on nodes.

📌 Use Cases

- **Dedicated nodes** for specific workloads (e.g., GPU, high-memory).
- **Node isolation** for security or compliance.
- **Graceful eviction** of Pods during maintenance.
- **Node Maintenance:** Drain nodes without deleting Pods**.**
- **Spot Instance Handling:** Prevent critical Pods from running on spot nodes**.**

📘 Summary Table

Component	Description
Taint	Applied to a node to reject unwanted Pods
Toleration	Applied to a Pod to allow it to run on tainted nodes
Effect Types	NoSchedule, PreferNoSchedule, NoExecute
Use Cases	Node isolation, special workloads, critical systems
Commands	kubectl taint nodes for tainting, tolerations go in Pod YAML

💡 **Pro Tips**

- You can **remove a taint** using this command:
  kubectl taint nodes <node-name> env=prod:NoSchedule-
- Taints and tolerations don't **guarantee** Pod placement — they just **allow** or **prevent** it.
- Combine with **nodeSelector** or **nodeAffinity** for stricter control.

22) Network Policies

- **Network Policies** are Kubernetes are used to control **traffic flow between Pods** and **external client**
- It helps **secure communication** inside the cluster by restricting or allowing connections based on labels, namespaces, and IP blocks.
- They act like **firewall rules** for Pods, allowing you to define **which Pods can communicate with each other** and with external endpoints.

🧠 In simple words:
It's like a **firewall for Pods** — it allows or deny traffic **based on labels, ports, and namespaces**.
By default, **all Pods can communicate** with each other. Network Policies let you **lock that down**.

✅ Purpose

- Improve **security** by restricting unwanted traffic.
- Enforce **least privilege** networking.
- Control **ingress** (incoming) and **egress** (outgoing) traffic.

📌 Key Concepts

Term	Description
podSelector	Selects which Pods the policy applies to.
ingress	Rules for incoming traffic to Pods.
egress	Rules for outgoing traffic from Pods.
policyTypes	Specifies whether the policy applies to ingress, egress, or both.

How Network Policies Work

1. **Pods are labeled** to identify their traffic rules.
2. **Network Policies define allowed or restricted communication** between labeled pods.
3. **Only pods matching the policy can send or receive traffic**, ensuring controlled access.

Key Features of Network Policies

1. **Pod-to-Pod Traffic Control** – Define which pods can communicate with each other.
2. **Namespace-Level Isolation** – Restrict traffic between namespaces for better security.

3. **Ingress and Egress Rules** – Control incoming and outgoing network traffic.
4. **Label-Based Rules** – Apply policies dynamically using pod labels.
5. **Works with CNI Plugins** – Requires a networking provider that supports policies (e.g., Calico, Cilium, Weave).

🔀 Types of Network Policies

Type	Description
Ingress	Controls incoming traffic to a Pod
Egress	Controls outgoing traffic from a Pod
Both	You can define both at once

📄 Example YAMLs

✅ a. Allow traffic from specific Pods (Ingress)

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-frontend
spec:
  podSelector:
    matchLabels:
      app: my-backend
  ingress:
    - from:
        - podSelector:
            matchLabels:
              role: frontend
```

🔐 Only Pods with label role: frontend can access Pods labeled app: my-backend.

✅ b. Allow traffic only from a specific Namespace

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-namespace
spec:
  podSelector:
    matchLabels:
      app: secure-api
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              team: dev
```

🔐 Only Pods from the namespace with label team: dev can access the secure-api Pods.

✅ **c. Allow outgoing traffic only to a specific IP (Egress)**

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: restrict-egress
spec:
  podSelector:
    matchLabels:
      app: myapp
  egress:
    - to:
        - ipBlock:
            cidr: 10.0.0.0/24
```

🔐 myapp Pods can only send traffic to IPs in 10.0.0.0/24.

Troubleshooting

Issue	Debugging Command
Policy not enforced	kubectl describe networkpolicy <name>
Unexpected blocked traffic	Check CNI plugin logs (e.g., Calico logs).
DNS failures	Ensure egress to CoreDNS Pods (kube-system namespace).

🚨 Important Notes

- **By default, all traffic is allowed**. Once you apply a Network Policy to a Pod, **only allowed traffic is permitted**.
- **You must label your Pods properly** for policies to work.
- **Test carefully**! It's easy to accidentally block traffic you need.

23) Kustomize

- **Kustomize** is a tool built into kubectl that helps customize Kubernetes YAML files for different environments (like dev, staging, and prod) without duplicating the files
- It helps to reuse, override, and patch YAML files in a clean, structured way — like templates, but **without using Helm or templating engines**.
- It's great for managing different environments like **dev, staging, and prod** using the same base YAML files.

How Kustomize Works

- **Base**: Original YAML files (common across environments. e.g., Deployment, Service).
- **Overlay**: Environment-specific customizations (patches, replacements. e.g, dev, pods)

- **Generates final YAML (kustomization.yaml)** by merging bases + overlays.

No Templating!
Unlike Helm, Kustomize **doesn't use templates** ({{ .Values }}). Instead, it:

- **Patches** existing YAML (JSON Merge Patch, Strategic Merge Patch).
- **Modifies fields** (e.g., replicas, labels, env vars).

✅ **Key Features**

- No need for templating languages (like Helm).
- Layered configuration using **overlays**.
- Supports **patching**, **variable substitution**, and **resource composition**.
- Built into kubectl (kubectl apply -k).
- **Generators**: Auto-generate ConfigMaps and Secrets

📁 **Folder Structure and YAML Examples**
Let's say you want different configs for dev and prod using a single base.
📂 **File Structure:**

```
my-app/
├── base/
│   ├── deployment.yaml
│   ├── service.yaml
│   └── kustomization.yaml
├── overlays/
   ├── dev/
   │   ├── kustomization.yaml
   │   └── patch.yaml
   └── prod/
       ├── kustomization.yaml
       └── patch.yaml
```

📦 **Base Deployment (base/deployment.yaml)**

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  replicas: 2
  template:
    metadata:
      labels:
        app: my-app
    spec:
      containers:
        - name: my-container
          image: my-app:latest
```

📄 **Base Kustomization (base/kustomization.yaml)**

```yaml
resources:
  - deployment.yaml
  - service.yaml
```

🧪 **Dev Overlay (overlays/dev/kustomization.yaml)**

```yaml
resources:
  - ../../base
patchesStrategicMerge:
  - patch.yaml
```

🧪 **Dev Patch (overlays/dev/patch.yaml)**

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  replicas: 1
  template:
    spec:
      containers:
        - name: my-container
          image: my-app:dev
```

📜 **Example Patch**

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  replicas: 2
```

This patch overrides the number of replicas in the base deployment.

🛠️ **Apply Dev Config with Kustomize**

- kubectl apply -k overlays/dev

Troubleshooting

Issue	Solution
Patch not applied	Verify kustomization.yaml references the patch file.

Issue	Solution
Name collisions	Use namePrefix or nameSuffix.

🧩 Extra Functionalities

Feature	Description
images:	Override container images
namePrefix:	Add prefixes to resource names (like dev-)
namespace:	Set all resources to a specific namespace
commonLabels:	Add labels to all resources
configMapGenerator / secretGenerator	Auto-create ConfigMaps and Secrets from files or literals

Example:

```
namespace: dev
namePrefix: dev-
commonLabels:
  env: dev
```

Kustomize vs. Helm

Feature	Kustomize	Helm
Approach	Declarative patching	Templating ({{ .Values }})
Learning Curve	Low (YAML-only)	Medium (Go templates)
Secrets Management	Built-in (secretGenerator)	Requires external tools
Community Plugins	Limited	Extensive (charts)

🍼 Bonus: Common Commands

```
kubectl kustomize .              # See the output YAML
kubectl apply -k overlays/dev    # Apply dev config
kubectl apply -k overlays/prod   # Apply prod config
```

24) Logs

🔎 Fluentd

- **Fluentd** is an **open-source log processor**. In Kubernetes, it's commonly used to **collect, filter, transform, and forward logs** from all Pods and nodes to a log storage system like **Elasticsearch, Splunk, or Cloud Logging**.

  🧠 Think of Fluentd as a **log router**. It reads logs from the system, changes them if needed, and sends them where you want.

📄 How Fluentd Works in Kubernetes

- Logs are written to /var/log/containers on each node.
- **Fluentd (as a DaemonSet)** reads those logs.
- It then filters and formats the logs.
- Sends logs to **a central location** (like Elasticsearch or a cloud logging service).

📁 Example YAML (Fluentd as DaemonSet)

```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  name: fluentd
  namespace: kube-system
spec:
  selector:
    matchLabels:
      name: fluentd
  template:
    metadata:
      labels:
        name: fluentd
    spec:
      containers:
      - name: fluentd
        image: fluent/fluentd:v1.14-1
        env:
        - name: FLUENTD_ARGS
          value: "--no-supervisor -q"
        volumeMounts:
        - name: varlog
          mountPath: /var/log
        - name: varlibdockercontainers
          mountPath: /var/lib/docker/containers
          readOnly: true
      volumes:
      - name: varlog
        hostPath:
          path: /var/log
      - name: varlibdockercontainers
        hostPath:
```

```
          path: /var/lib/docker/containers
```

📝 This sets up Fluentd on **every node**, pulling logs from Docker containers and system logs.

📌 Fluentd Config Example (fluent.conf)

conf

```
<source>
  @type tail
  path /var/log/containers/*.log
  format json
  tag kube.*
</source>

<match kube.**>
  @type elasticsearch
  host elasticsearch.logging.svc.cluster.local
  port 9200
  logstash_format true
</match>
```

🔄 This config reads logs from containers and forwards them to **Elasticsearch**.

🔗 Types / Plugins

Fluentd doesn't have "types" like Services do, but it has **input, filter, and output plugins**.

Plugin Type	Example	Purpose
Input	tail, http, syslog	Collect logs
Filter	record_transformer, grep	Modify logs
Output	elasticsearch, s3, gcs	Send logs somewhere

🔚 Summary

Item	Info
Tool	Fluentd
Purpose	Log aggregation, transformation, and forwarding
Runs As	DaemonSet
Used With	Elasticsearch, Splunk, Cloud Logging
Config File	fluent.conf
Key Use Case	Centralized and enriched logging for Kubernetes clusters

Scaling in Kubernetes

Kubernetes supports two types of scaling:
1. Horizontal Pod Autoscaling (HPA): Dynamically adjusts the number of pod replicas for a deployment or replica set. It monitors metrics like CPU, memory, or custom application metrics.Adds or removes pod replicas based on thresholds.
2. Node Scaling: Adding or removing nodes to/from the cluster. Managed manually or automatically using tools like Cluster Autoscaler. Cluster Autoscaler integrates with cloud providers to add remove virtual machines dynamically.

Managing Workloads in Kubernetes
Workloads: Workloads are the applications or services running on Kubernetes. It is defined in Kubernetes using manifests (YAML or JSON files).

Types of Workloads:
Deployments: For stateless applications; supports scaling and updates.
StatefulSets: For stateful applications that require unique identities and stable storage (e.g., databases).
DaemonSets: Ensures a copy of a pod runs on every node (e.g., log collectors).
Jobs and CronJobs: For running one-time or scheduled tasks.

Other Features:
Load Balancing: Kubernetes ensures workloads are balanced across the cluster using Services and Ingress.
Monitoring and Logging: Tools like Prometheus, Grafana, and ELK Stack (Elasticsearch, Logstash, Kibana) help monitor workloads and log activities.
High Availability and Resilience: Kubernetes automatically restarts failed pods and reschedules them to healthy nodes.

SECURE KUBERNETES

1. Secure API server
2. RBAC
3. Network policies
4. Encrypted at rest (ETCD)
5. Secure Container Images
6. Cluster monitoring
7. upgrades.

🔐 Encryption at Rest

- Secrets are stored base64 encoded by default.
- For better security, enable encryption at rest in your cluster using KMS or a custom encryption provider.

Networking:

- Networking plugins and configuration options also facilitate pod-to-pod communication and network isolation

What is AWS RDS?

AWS RDS (Relational Database Service) is a fully managed relational database service that simplifies database management tasks like provisioning, patching, backups, scaling and failover. It supports popular database engines:

- MySQL
- PostgreSQL
- MariaDB
- Oracle
- Microsoft SQL Server

Key Features:

- Automated backups & patching
- Storage and compute scaling
- High availability with Multi-AZ
- Read replicas for scaling
- Automatic failover
- Secure and VPC-integrated networking

How to Use AWS RDS with Kubernetes

AWS RDS runs outside the Kubernetes cluster. Application pods in Kubernetes access it over the network, using securely stored credentials.

High-Level Steps for Production Integration:

1. **Create an RDS Instance**
2. **Store Credentials Securely in Kubernetes Secrets**
3. **Deploy Application to Kubernetes with RDS Access**
4. **Secure Communication with Proper VPC and Security Groups**
5. **Monitor and Scale the RDS Instance**
6. **Expose Application via Kubernetes Service**

Step 1: Create an AWS RDS Instance

Use the AWS Management Console or AWS CLI to create an RDS instance.
Example (PostgreSQL via CLI):

```
aws rds create-db-instance \
  --db-instance-identifier myprod-db \
  --db-instance-class db.m5.large \
  --engine postgres \
  --allocated-storage 100 \
  --master-username adminuser \
  --master-user-password adminpassword \
  --backup-retention-period 7 \
  --multi-az \
  --vpc-security-group-ids sg-0123456789abcdef0
```

Step 2: Configure Secrets in Kubernetes

Store database credentials securely:

```
kubectl create secret generic mydb-credentials \
  --from-literal=DB_USER=adminuser \
  --from-literal=DB_PASSWORD=adminpassword \
  --from-literal=DB_HOST=myprod-db.c1h1h3d22dkk.us-east-1.rds.amazonaws.com \
  --from-literal=DB_PORT=5432 \
  --from-literal=DB_NAME=mydatabase
```

Step 3: Deploy an Application that Connects to RDS

Define your app deployment to connect to RDS:

Deployment Example (Node.js-based App):

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: webapp-deployment
spec:
  replicas: 3
  selector:
    matchLabels:
      app: webapp
  template:
    metadata:
      labels:
        app: webapp
    spec:
      containers:
      - name: webapp
        image: myapp-image:latest
        env:
        - name: DB_USER
          valueFrom:
            secretKeyRef:
              name: mydb-credentials
              key: DB_USER
        - name: DB_PASSWORD
          valueFrom:
```

```
            secretKeyRef:
              name: mydb-credentials
              key: DB_PASSWORD
        - name: DB_HOST
          valueFrom:
            secretKeyRef:
              name: mydb-credentials
              key: DB_HOST
        - name: DB_PORT
          valueFrom:
            secretKeyRef:
              name: mydb-credentials
              key: DB_PORT
        - name: DB_NAME
          valueFrom:
            secretKeyRef:
              name: mydb-credentials
              key: DB_NAME
        ports:
        - containerPort: 80
```

Step 4: Secure Communication between Kubernetes and RDS

Ensure secure access between RDS and Kubernetes:

- Use the **same VPC** or set up **VPC peering**.
- Configure **RDS Security Groups** to allow access from Kubernetes worker nodes on the DB port (e.g., 5432 for PostgreSQL).

Example security group rule:

```
aws ec2 authorize-security-group-ingress \
  --group-id sg-0123456789abcdef0 \
  --protocol tcp --port 5432 \
  --source-group sg-0987654321abcdef0
```

Step 5: Monitor and Scale RDS

- **CloudWatch** for metrics
- **Performance Insights** for diagnostics
- **Enhanced Monitoring** for real-time stats
- Use modify-db-instance to scale:

```
aws rds modify-db-instance \
  --db-instance-identifier myprod-db \
  --db-instance-class db.m5.2xlarge \
  --apply-immediately
```

Step 6: Expose the Application

Use a LoadBalancer service to make the app accessible externally:

```
apiVersion: v1
kind: Service
```

```yaml
metadata:
  name: webapp-service
spec:
  selector:
    app: webapp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  type: LoadBalancer
```

Example Application Connection Code (Node.js)

javascript

```javascript
const mysql = require('mysql');

const connection = mysql.createConnection({
  host: process.env.DB_HOST,
  user: process.env.DB_USER,
  password: process.env.DB_PASSWORD,
  database: process.env.DB_NAME
});

connection.connect(err => {
  if (err) {
    console.error('Connection error:', err.stack);
    return;
  }
  console.log('Connected as id', connection.threadId);
});
```

Summary

Benefits of Using AWS RDS with Kubernetes:

- Offloads database management tasks
- Enhances scalability and availability
- Simplifies Kubernetes deployments
- Ensures production readiness with monitoring, backups, and HA

How to set up SSO for application inside the kubernetes pods and with examples

To set up **Single Sign-On (SSO)** for an application running inside Kubernetes pods, you need to integrate an **Identity Provider (IdP)** that supports **OAuth2** or **OIDC (OpenID Connect)**. In this example, I will show you how to integrate **OIDC** for SSO

using **AWS Cognito** as the IdP, which is one of the popular choices for managing authentication and user access.

The general approach will involve:
1. Configuring **AWS Cognito** as the **IdP**.
2. Setting up the **application** to use **OIDC** for authentication.
3. Deploying the application in a **Kubernetes cluster**.
4. Setting up appropriate configurations in the application to handle authentication through Cognito.

Steps to Set Up SSO for Application Inside Kubernetes Pods

Prerequisites
1. **AWS Cognito** set up as the IdP for managing users.
2. Kubernetes cluster running with **Ingress** configured for external access to the app.
3. A sample application running in Kubernetes (e.g., a web application like **Node.js**, **Spring Boot**, **Express.js**).
4. OAuth2 or OpenID Connect integration in your application.

Step 1: Configure AWS Cognito for Authentication

1. **Create a Cognito User Pool**:
   - Go to the **Cognito Console** in AWS and create a **User Pool** for your application.
   - Configure attributes like **email**, **username**, **password policies**, etc.

2. **Create an App Client**:
   - Inside the **User Pool**, go to **App clients** and create a new **App Client**.
   - Ensure that **OAuth 2.0** flows like **Authorization Code Grant** are enabled.
   - Note down the **App Client ID** and **App Client Secret** (for use in your application).

3. **Configure Cognito App Client Settings**:
   - Set the **Callback URL** (where Cognito will redirect the user after login, e.g., `http://your-app/callback`).
   - Set the **Sign-out URL** (where users will be redirected after signing out).
   - Enable **OAuth 2.0** scopes: `openid`, `email`, `profile`.

4. **Configure Domain**:
   - Set up a **Domain** for your Cognito instance so it can provide the login page (e.g., `https://<your-cognito-domain>.auth.us-west-2.amazoncognito.com`).

5. **Enable the OIDC Settings**:
   - You'll need the **Issuer URL** for the OIDC configuration, which will look something like:
     ```
     https://cognito-idp.us-west-2.amazonaws.com/us-west-2_XXXXXXXXX
     ```
   - This URL will be used to integrate the authentication mechanism into your app.

Step 2: Integrating OIDC into Your Application

Let's assume you are using a **Node.js** application, but the general process applies to other frameworks (e.g., **Spring Boot**, **Express**, **Flask**).

1. **Install OIDC Authentication Library**:
   Use libraries like **passport.js** for Node.js to handle OAuth2 or OIDC authentication.
   For Node.js with **passport.js**:
   npm install passport passport-oidc express-session

2. **Configure OIDC Authentication**:
   In your **Node.js** application, configure **passport-oidc** to authenticate users using AWS Cognito.

   Example of `server.js` with OIDC authentication:

   ```javascript
   const express = require('express');
   const passport = require('passport');
   const session = require('express-session');
   const OIDCStrategy = require('passport-oidc').Strategy;

   const app = express();

   passport.use(
     new OIDCStrategy(
       {
         issuer: 'https://cognito-idp.us-west-2.amazonaws.com/us-west-2_XXXXXXXXX',
         authorizationURL: 'https://<your-cognito-domain>.auth.us-west-2.amazoncognito.com/oauth2/authorize',
         tokenURL: 'https://<your-cognito-domain>.auth.us-west-2.amazoncognito.com/oauth2/token',
         clientID: '<your-app-client-id>',
         clientSecret: '<your-app-client-secret>',
         callbackURL: 'http://localhost:3000/callback',
       },
       function (issuer, profile, done) {
         return done(null, profile);
       }
     )
   );

   app.use(session({ secret: 'secret', resave: true, saveUninitialized: true }));
   app.use(passport.initialize());
   app.use(passport.session());

   app.get('/login', (req, res) => {
     passport.authenticate('oidc')(req, res);
```

```
});

app.get('/callback', (req, res) => {
  passport.authenticate('oidc', { failureRedirect: '/' })(req, res, function () {
    res.redirect('/');
  });
});

app.get('/', (req, res) => {
  if (req.isAuthenticated()) {
    res.send(`Hello, ${req.user.displayName}!`);
  } else {
    res.send('Hello, guest! Please <a href="/login">login</a>');
  }
});

app.listen(3000, () => {
  console.log('App is listening on port 3000');
});
```

3. **Start the Application Locally** (for testing):
   Run the app locally first to verify that the authentication flow works before deploying to Kubernetes.

```
node server.js
```

   Visit `http://localhost:3000` and test the SSO login flow with AWS Cognito.

Step 3: Deploy the Application in Kubernetes

1. **Containerize the Application**:

   Create a `Dockerfile` for your application.

   Example `Dockerfile` for a Node.js app:

   dockerfile

```
FROM node:16
WORKDIR /app
COPY package.json package-lock.json ./
RUN npm install
COPY . .
EXPOSE 3000
CMD ["node", "server.js"]
```

   Build and push the image to a container registry (e.g., DockerHub, AWS ECR).

```
docker build -t my-app .
docker tag my-app:latest <your-dockerhub-username>/my-app:latest
docker push <your-dockerhub-username>/my-app:latest
```

2. **Create Kubernetes Deployment YAML**:

Define your Kubernetes deployment (`deployment.yaml`).

Example:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  replicas: 1
  selector:
    matchLabels:
      app: my-app
  template:
    metadata:
      labels:
        app: my-app
    spec:
      containers:
        - name: my-app
          image: <your-dockerhub-username>/my-app:latest
          ports:
            - containerPort: 3000
          env:
            - name: CLIENT_ID
              valueFrom:
                secretKeyRef:
                  name: cognito-credentials
                  key: client-id
            - name: CLIENT_SECRET
              valueFrom:
                secretKeyRef:
                  name: cognito-credentials
                  key: client-secret
```

3. **Create Kubernetes Service and Ingress (optional)**:

Expose your app using a **Service** and optionally an **Ingress**.

Example `service.yaml`:

```
apiVersion: v1
kind: Service
metadata:
  name: my-app-service
spec:
  selector:
    app: my-app
  ports:
    - protocol: TCP
      port: 80
```

```
    targetPort: 3000
```

Example `ingress.yaml` for exposing the service via Ingress:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: my-app-ingress
spec:
  rules:
  - host: my-app.example.com
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: my-app-service
            port:
              number: 80
```

4. **Deploy to Kubernetes:**

Apply the Kubernetes resources (`deployment.yaml`, `service.yaml`, `ingress.yaml`) to deploy the app:

```
kubectl apply -f deployment.yaml
kubectl apply -f service.yaml
kubectl apply -f ingress.yaml
```

Step 4: Verify the SSO Flow in Kubernetes

1. **Access the application** via the Ingress URL or external IP (e.g., `http://my-app.example.com`).
2. **Test the login flow** by accessing the login page, which should redirect to AWS Cognito for authentication.
3. After successful login, Cognito will redirect back to the callback URL (`/callback`), and your application should be authenticated.

Step 5: Manage Secrets for Sensitive Information

For sensitive information like the **Client ID** and **Client Secret**, store them in **Kubernetes Secrets** instead of hardcoding them in the app code. Here's how to create a

Kubernetes Secret:

```
apiVersion: v1
kind: Secret
metadata:
  name: cognito-credentials
type: Opaque
```

data:
  client-id: <base64-encoded-client-id>
  client-secret: <base64-encoded-client-secret>

Apply the Secret:
kubectl apply -f secret.yaml

Conclusion
Setting up **SSO** for an application inside Kubernetes involves configuring an **Identity Provider** (e.g., AWS Cognito) and integrating your application to authenticate via **OIDC** or **OAuth2**. Once integrated, deploy the app inside Kubernetes and configure **Ingress** or **Service** for external access. Ensure **Kubernetes Secrets** are used for managing sensitive credentials securely. This will enable **SSO** authentication for your users in the application running in Kubernetes.

AWS

AWS IAM

- **AWS IAM (Identity and Access Management)** is a web service helps to control access to AWS resources securely. It enables management of users, security credentials, and permissions that that determine which AWS resources users and applications can access.
- **IAM** allows you to create and manage users, groups, and roles.

Core IAM Components

1. Users

- **Users**: IAM users represent individual people or entities (such as applications or services) that interact with AWS resources.
- Each user has a **unique name and security credentials** (password or access keys) used for authentication and access control.

2. Groups

- **Groups** are collections of users that share the same permissions.
- Simplifies permission management (assign permissions to group rather than individual users)

3. Roles

- **Roles:** IAM roles are used to grant temporary access to AWS resources.
- Often used by AWS services or for cross-account access
- Generate temporary security credentials instead of permanent ones
- A Role can be assigned to a federated user who signed in from an external Identity Provider.

4. Policies

- **Policies:** IAM policies are JSON documents that define permissions.
- Policies can be attached to users, groups, or roles to control access.
- Two main types:
    - Identity-based policies (attached to IAM identities users, groups, or roles)
    - Resource-based policies (attached to AWS resources like S3 buckets)

AMI:

AMI Stands for Amazon Machine Image.
● AMI decides the OS, installs dependencies, libraries, data of your EC2 instances.
● Multiple instances with the same configuration can be launched using a single AMI.

In AWS (Amazon Web Services), **AMI** stands for **Amazon Machine Image**. It's a template that contains the software configuration (operating system, application server, and applications) required to launch an instance (a virtual server) in the EC2 (Elastic Compute Cloud) environment.

Key Components of an AMI:

1. **A root volume**: Typically includes the OS and installed applications.
2. **Launch permissions**: Control which AWS accounts can use the AMI to launch instances.
3. **Block device mapping**: Specifies the volumes to attach to the instance when it's launched.

Types of AMIs:

- **Public AMIs**: Provided by AWS or shared by the community.
- **Private AMIs**: Created by users for internal use.
- **AWS Marketplace AMIs**: Provided by third-party vendors, often with pre-installed software.

Security Group:

In AWS, a Security Group acts as a virtual firewall for your EC2 instances to control inbound and outbound traffic.

A Security group acts as a virtual firewall for your EC2 Instances.
● It decides the type of port and kind of traffic to allow**.**
● **Security groups** are active at **the instance level** whereas **Network ACLs** are active at the **subnet level.**
● Security Groups can only allow but can’t deny the rules.
● The Security group is considered **stateful**.
● By default, in the outbound rule all traffic is allowed and needs to define the inbound rules.

Key Pair:
A key pair, consisting of a private key and a public key, is a set of security credentials that you can use to prove your identity while connecting to an instance.
● Amazon EC2 instances use two keys, one is the public key which is attached to your EC2 instance.
● Another is the private key which is with you. You can get access to the EC2 instance only if these keys get matched.
● Keep the private key in a secure place.

AWS EC2

What is AWS EC2?
Amazon EC2 (Elastic Compute Cloud) is a core service in AWS that provides **resizable compute capacity in the cloud**. It allows you to run virtual servers (called **instances**) on-demand, making it ideal for hosting applications, websites, databases, and more.

AWS EC2 (Amazon Elastic Compute Cloud) is a core service within Amazon Web Services (AWS) that provides scalable virtual servers (instances) in the cloud.

Launching an EC2 Instance
Steps to launch an EC2 instance:

1. **Choose an AMI** (Amazon Machine Image) – Preconfigured OS templates.
2. **Select Instance Type** (e.g., t3.micro, m5.large).
3. **Configure Network (VPC, Subnet, Security Group)**.
4. **Add Storage (EBS volumes or instance store)**.
5. **Set Tags & Review**.
6. **Launch (Select or create a key pair for SSH access)**.

Storage Options

- **EBS (Elastic Block Store)**: Persistent, network-attached storage (SSD/HDD).
- **Instance Store**: Temporary, high-speed local storage (ephemeral).
- **EFS (Elastic File System)**: Shared NFS storage for multiple instances.

Networking & Security

- **VPC (Virtual Private Cloud)**: Isolated network for your instances.
- **Security Groups**: Virtual firewalls controlling inbound/outbound traffic.
- **Key Pairs**: SSH key authentication for Linux/Windows instances.
- **IAM Roles**: Assign permissions to instances without storing credentials.

Auto Scaling & Load Balancing

- **Auto Scaling**: Automatically adjust the number of instances based on demand.
- **ELB (Elastic Load Balancing)**: Distribute traffic across instances.

Instance Store:

- Instance store is the ephemeral block-level storage for the EC2 instance

- Instance stores can be used for faster processing and temporary storage of the application.

AWS EBS (Elastic Block Store) Volumes

Amazon **EBS (Elastic Block Store)** provides persistent block storage volumes for use with **EC2 instances**. Unlike instance store (ephemeral) storage, EBS volumes persist independently of the instance lifecycle, making them ideal for databases, file systems, and applications requiring durable storage.
It is the block-level storage that is assigned to your single EC2 Instance.

Amazon EBS (Elastic Block Store) is a scalable, high-performance block storage service designed for use with **Amazon EC2** instances. It provides persistent storage that remains available even after the instance is stopped or terminated.

2. EBS Volume Types

AWS offers several EBS volume types optimized for different workloads:

Volume Type	Description	Use Case	Max IOPS/Throughput
gp3 (SSD)	General Purpose SSD (default)	Boot volumes, apps, dev environments	16,000 IOPS, 1,000 MB/s
io1/io2 (SSD)	High-performance, low-latency	Databases (RDS, Oracle, SAP)	64,000 IOPS (io2 Block Express: 256K IOPS)
st1 (HDD)	Throughput-optimized HDD	Big data, log processing	500 MB/s
sc1 (HDD)	Cold HDD (lowest cost)	Infrequently accessed data	250 /s

---

3. EBS vs. Instance Store

Feature	EBS Volume	Instance Store (Ephemeral)
Persistence	Survives instance termination	Lost on stop/termination
Performance	Network-attached (varies by type)	Direct-attached (very high speed)
Use Case	Databases, long-term storage	Temp data, cache, scratch disks
Scalability	Can resize (with limitations)	Fixed size per instance type

---

4. Key Operations

a) Creating & Attaching an EBS Volume

1. **AWS Console → EC2 Dashboard → Volumes → Create Volume**.
2. Select **type, size, AZ, and encryption**.
3. Attach to an EC2 instance (must be in the same AZ).

b) Expanding an EBS Volume

1. **Increase volume size** (via Console/CLI).
2. **Extend the file system** (for Linux: resize2fs or xfs_growfs).

c) Taking Snapshots

- Snapshots are **incremental** (only changed blocks are stored).
- Can **copy snapshots across regions** for disaster recovery.
- Used to **create new volumes** or **AMI images**.

d) Restoring from a Snapshot

1. Create a new volume from a snapshot.
2. Attach it to an instance.

---

5. Performance Optimization

- **Use Provisioned IOPS (**io1/io2**)** for high-performance databases.
- **RAID 0 (striping)** for higher throughput (combine multiple volumes).
- **EBS-optimized EC2 instances** ensure dedicated bandwidth.
- **Monitor with CloudWatch** (VolumeReadOps, VolumeWriteOps).

AWS VPC

What is AWS VPC?

Amazon Virtual Private Cloud (VPC) is a service that allows users to create a virtual dedicated network for resources.

Amazon VPC (Virtual Private Cloud) is a foundational AWS service that lets you **provision a logically isolated network** within the AWS cloud. It gives you full control over your virtual networking environment, including IP address ranges, subnets, route tables, internet gateways, and more.

🌐 **Key Concepts in VPC:**

Component	Description
VPC	**A virtual network dedicated to your AWS account.**
Subnets	**Segments of a VPC's IP address range. Can be public or private.**
Route Tables	**Control traffic routing within the VPC.**
Internet Gateway (IGW)	**Enables internet access for resources in public subnets.**

Component	Description
NAT Gateway	**Allows instances in private subnets to access the internet securely.**
Security Groups	**Instance-level firewalls.**
Network ACLs	**Subnet-level firewalls.**
VPC Peering	**Connects two VPCs for private communication.**
Endpoints	**Connect to AWS services privately without using the internet.**

Example Architecture:

- **Public Subnet**: Contains a load balancer and NAT gateway.
- **Private Subnet**: Contains EC2 instances and databases.
- **Route Tables**: Direct traffic to IGW or NAT as needed.
- **Security Groups**: Allow HTTP/HTTPS to the load balancer, and internal traffic to the backend.

Security Groups:
Default Security Groups:-
Inbound rule - Allows all inbound traffic
Outbound rule - Allows all outbound traffic
Custom Security Groups:- (by default)
Inbound rule - Allows no inbound traffic
Outbound rule - Allows all outbound traffic

Network ACLs (access control list):
Default Network ACL:-
Inbound rule - Allows all inbound traffic
Outbound rule - Allows all outbound traffic
Custom Network ACL:- (by default)
Inbound rule - Denies all inbound traffic
Outbound rule - Denies all outbound traffic

AWS VPC (Virtual Private Cloud) - Complete Guide
Amazon **VPC (Virtual Private Cloud)** is a logically isolated network within AWS where you can launch AWS resources (EC2, RDS, Lambda, etc.) in a **private, secure, and customizable cloud environment**.

---

1. Key Features of AWS VPC
✅ **Isolated Networking** – Your own virtual network inside AWS.
✅ **Subnet Segmentation** – Divide your VPC into public/private subnets.

✅ **Internet Connectivity** – Control inbound/outbound traffic via **Internet Gateways (IGW)** and **NAT Gateways**.
✅ **Security** – Use **Security Groups** (instance-level firewall) and **Network ACLs** (subnet-level firewall).
✅ **Hybrid Cloud** – Connect to on-premises data centers via **VPN** or **AWS Direct Connect**.
✅ **Scalability** – Automatically scales with your AWS resources.

---

2. Core Components of a VPC

a) VPC & CIDR Block

- A VPC is defined by an **IPv4/IPv6 CIDR block** (e.g., 10.0.0.0/16).
- **Max size**: /16 (65,536 IPs) to /28 (16 IPs).
- **Private IP ranges** (RFC 1918):
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

b) Subnets

- Subnets are **segments within a VPC** (e.g., 10.0.1.0/24).
- **Public Subnet**: Has a route to the internet (via **Internet Gateway**).
- **Private Subnet**: No direct internet access (uses **NAT Gateway** for outbound traffic).
- **Availability Zones (AZs)**: Subnets must reside in a single AZ.

c) Route Tables

- Determine **how traffic is routed** within the VPC.
- Every subnet is associated with a **route table**.
- Example route for a public subnet:

text
Copy
Download
Destination: 0.0.0.0/0 → Target: igw-12345 (Internet Gateway)

d) Internet Gateway (IGW)

- Allows **public subnets** to communicate with the internet.
- **1 IGW per VPC**.

e) NAT Gateway / NAT Instance

- Allows **private subnets** to access the internet (for updates, downloads) without exposing them.
- **NAT Gateway** (AWS-managed) is preferred over **NAT Instance** (self-managed EC2).

f) Security Groups (SGs) & Network ACLs (NACLs)

Feature	Security Group (SG)	Network ACL (NACL)
Scope	Instance-level	Subnet-level
Stateful?	Yes (return traffic allowed automatically)	No (stateless, explicit rules needed)
Rule Evaluation	Allow rules only	Allow + Deny rules

Feature	Security Group (SG)	Network ACL (NACL)
Order of Rules	All rules evaluated	Evaluated in order (lowest rule # first)

g) VPC Peering

- Connects **two VPCs** (same/different AWS accounts/regions).
- **No transitive peering** (must be direct).
- **CIDR blocks must not overlap**.

h) VPC Endpoints (PrivateLink)

- Privately connect to AWS services (S3, DynamoDB) **without internet/NAT**.
- **Types**:
  - **Interface Endpoint** (uses ENI, powered by PrivateLink).
  - **Gateway Endpoint** (only for S3 & DynamoDB).

i) VPN & Direct Connect

- **Site-to-Site VPN**: Securely connect on-premises network to AWS via IPsec.
- **AWS Direct Connect**: Dedicated private network connection (lower latency).

---

3. Default vs. Custom VPC

Feature	Default VPC	Custom VPC
CIDR Block	172.31.0.0/16	User-defined
Subnets	One per AZ	Manually created
Internet Access	Enabled (public subnets)	Configurable
Deletion	Can be deleted & restored	Permanent deletion

---

4. Creating a VPC (Step-by-Step)

1. **Define CIDR Block** (e.g., 10.0.0.0/16).
2. **Create Subnets** (public/private, e.g., 10.0.1.0/24 in us-east-1a).
3. **Set Up Internet Gateway (IGW)** and attach to VPC.
4. **Configure Route Tables** (public route: 0.0.0.0/0 → IGW).
5. **Launch EC2 Instances** in subnets with proper Security Groups.

---

5. Best Practices

✓ **Use multiple AZs** for high availability.
✓ **Private subnets for databases** (no direct internet access).
✓ **VPC Flow Logs** to monitor traffic.
✓ **Avoid overlapping CIDR blocks** in peering.
✓ **Use Security Groups for granular access control**.

---

6. Use Cases

- **Multi-tier applications** (web, app, DB layers).

- **Hybrid cloud** (connect on-premises to AWS).
- **Isolated environments** (dev/test/prod).
- **Secure access to AWS services** (via VPC endpoints).

AWS Security: Security Groups (SGs) vs. Network ACLs (NACLs)

Security Groups (SGs) and Network Access Control Lists (NACLs) are two fundamental **firewall** mechanisms in AWS that control traffic to and from your resources. While both provide security, they operate at **different layers** and have **different rule structures**.

---

1. Security Groups (SGs) - Instance-Level Firewall

Key Features

✅ **Stateful** – Return traffic is automatically allowed.
✅ **Operates at the instance level** (applied to ENIs, EC2, RDS, Lambda, etc.).
✅ **Supports "allow" rules only** (no explicit deny).
✅ **Evaluates all rules before allowing traffic**.
✅ **Default behavior**:
- **No inbound traffic allowed** (unless explicitly permitted).
- **All outbound traffic allowed** (can be restricted).

Example Security Group Rules

Type	Protocol	Port Range	Source/Destination	Use Case
Inbound	TCP	80 (HTTP)	0.0.0.0/0	Allow web traffic
Inbound	TCP	22 (SSH)	203.0.113.1/32	Allow SSH from a specific IP
Outbound	TCP	443 (HTTPS)	0.0.0.0/0	Allow outbound HTTPS

Best Practices for Security Groups

✓ **Follow the principle of least privilege** (only allow necessary ports).
✓ **Use descriptive names & tags** (e.g., web-sg, db-sg).
✓ **Reference other security groups** (not just IPs) for tighter security.
✓ **Avoid using** 0.0.0.0/0 unless absolutely necessary.

---

2. Network ACLs (NACLs) - Subnet-Level Firewall

Key Features

✅ **Stateless** – Return traffic must be explicitly allowed.
✅ **Operates at the subnet level** (applies to all instances in the subnet).
✅ **Supports both "allow" and "deny" rules**.
✅ **Rules are evaluated in order (lowest rule # first)**.
✅ **Default behavior**:
- **New custom NACLs deny all inbound/outbound traffic**.
- **Default NACL allows all inbound/outbound traffic**.

Example NACL Rules

Rule #	Type	Protocol	Port Range	Source/Destination	Allow/Deny	Use Case
100	Inbound	TCP	80 (HTTP)	0.0.0.0/0	ALLOW	Allow HTTP
110	Inbound	TCP	22 (SSH)	203.0.113.1/32	ALLOW	Allow SSH from a specific IP
120	Inbound	ALL	ALL	0.0.0.0/0	DENY	Block all other inbound
100	Outbound	TCP	443 (HTTPS)	0.0.0.0/0	ALLOW	Allow HTTPS outbound
110	Outbound	ALL	ALL	0.0.0.0/0	DENY	Block all other outbound

Best Practices for NACLs

✓ **Use NACLs for broad subnet-level filtering** (e.g., block known malicious IPs).
✓ **Order rules carefully** (lower-numbered rules take precedence).
✓ **Explicitly allow ephemeral ports** (e.g., 1024-65535) for return traffic.
✓ **Use NACLs for compliance requirements** (e.g., deny certain countries).

---

3. Security Groups vs. NACLs (Comparison)

Feature	Security Group (SG)	Network ACL (NACL)
Scope	Instance-level	Subnet-level
Stateful?	Yes (return traffic allowed automatically)	No (must explicitly allow return traffic)
Rule Types	Allow only	Allow + Deny
Rule Evaluation	All rules evaluated	Processed in order (lowest rule # first)

Feature	Security Group (SG)	Network ACL (NACL)
Default Behavior	Deny all inbound, allow all outbound	Default NACL: Allow all; Custom NACL: Deny all

---

4. When to Use Security Groups vs. NACLs?
Use Security Groups When:

- You need **instance-level security**.
- You want **automatic return traffic handling** (stateful).
- You need **granular control per instance** (e.g., different rules for web and DB servers).

Use NACLs When:

- You need **subnet-wide traffic control**.
- You want to **explicitly block certain IPs or ports**.
- You need **compliance-mandated deny rules**.

---

5. Example Security Architecture
Multi-Tier Web Application

1. **Public Subnet (Web Tier)**
    - **SG**: Allow HTTP/80, HTTPS/443 from the internet.
    - **NACL**: Allow HTTP/80, HTTPS/443 inbound; deny everything else.
2. **Private Subnet (DB Tier)**
    - **SG**: Allow MySQL/3306 only from the Web Tier SG.
    - **NACL**: Allow inbound from Web Tier subnet, deny all else.

🔐 Security Groups (SGs)

Feature	Description
Level	Instance-level (attached to EC2 instances)
Stateful	Yes – return traffic is automatically allowed
Rules	Only allow rules (no deny rules)
Applies to	EC2 instances, ENIs (Elastic Network Interfaces)
Evaluation	All rules are evaluated together (OR logic)
Default behavior	Deny all inbound, allow all outbound

🌐 Network ACLs (NACLs)

Feature	Description
Level	Subnet-level (applies to all resources in a subnet)

Feature	Description
Stateful	No – return traffic must be explicitly allowed
Rules	Allow and deny rules
Applies to	All traffic entering or leaving a subnet
Evaluation	Rules are evaluated in order (lowest number first)
Default behavior	Allow all inbound and outbound (modifiable)

🧠 **Key Differences:**

Aspect	Security Group	Network ACL
Scope	Instance	Subnet
Traffic Direction	Inbound/Outbound	Inbound/Outbound
Rule Type	Allow only	Allow and Deny
Statefulness	Stateful	Stateless
Use Case	Fine-grained control	Broad subnet-level control

✅ **When to Use What?**

- Use **Security Groups** for **instance-level** access control (e.g., allow SSH to a specific EC2).
- Use **NACLs** for **subnet-level** filtering, especially when you need **deny rules** or want an extra layer of security.

AWS Beanstalk

What is Amazon Elastic Beanstalk?

● Beanstalk is a compute service for deploying and scaling applications developed in many popular languages.

AWS Elastic Beanstalk supports two types of Environment:

● Web Tier Environment

● Worker Environment

AWS Elastic Beanstalk - Complete Guide

AWS Elastic Beanstalk is a **Platform-as-a-Service (PaaS)** offering that simplifies deploying, managing, and scaling web applications. It supports multiple programming languages (Java,

Python, Node.js, PHP, etc.) and automatically handles infrastructure provisioning, load balancing, and scaling.

---

1. Key Features of AWS Elastic Beanstalk

✅ **Fully Managed** – AWS handles servers, load balancing, and scaling.
✅ **Multi-Language Support** – Java, .NET, Python, Node.js, PHP, Ruby, Go, Docker.
✅ **Easy Deployment** – Upload code via CLI, Git, or AWS Management Console.
✅ **Auto-Scaling & Load Balancing** – Adjusts capacity based on traffic.
✅ **Customizable** – Modify underlying AWS resources (EC2, RDS, etc.).
✅ **Monitoring & Logging** – Integrated with CloudWatch and access to instance logs.

---

2. Core Components of Elastic Beanstalk

a) Application

- The **top-level container** for your environments (e.g., my-web-app).
- Can have **multiple environments** (dev, staging, prod).

b) Environment

- A **running version** of your application (e.g., my-web-app-dev).
- Consists of:
  - **EC2 instances** (auto-scaled).
  - **Load Balancer** (optional).
  - **Auto Scaling Group**.
  - **Database (optional, e.g., Amazon RDS)**.

c) Application Version

- A **specific release** of your code (e.g., v1.0.0).
- Stored in **S3** as a .zip or .war file.

d) Environment Tier

- **Web Server Tier** (HTTP/HTTPS traffic).
- **Worker Tier** (for background tasks using Amazon SQS).

---

3. How Elastic Beanstalk Works

1. **Upload Code** (via CLI, Git, or Console).
2. **Beanstalk Provisions Infrastructure** (EC2, ASG, ELB, etc.).
3. **Deploys Application** and manages dependencies.
4. **Auto-Scaling & Monitoring** (adjusts capacity based on demand).

What is AWS Lambda?

AWS Lambda is a **serverless compute service** provided by Amazon Web Services that lets you run code **without provisioning or managing servers**. You simply upload your code, and Lambda takes care of everything required to run and scale it with high availability.

⚙️ **How AWS Lambda Works:**

1. **You write a function** in a supported language (e.g., Python, Node.js, Java).
2. **You upload the code** to AWS Lambda or write it directly in the console.
3. **You define a trigger**, such as:

- An HTTP request via API Gateway
- An S3 event (e.g., file upload)
- A DynamoDB stream
- A scheduled event (cron job)

4. **Lambda executes the code** in response to the trigger.
5. **You pay only for the compute time** your code uses (measured in milliseconds).

AWS Lambda is a serverless compute service that lets you run code in response to events.
● AWS Lambda is a serverless compute service through which you can run your code without provisioning any Servers.
● It only runs your code when needed and also scales automatically when the request count increases.
● AWS Lambda follows the Pay per use principle – it means there is no charge when your code is not running.
● Lambda allows you to run your code for any application or backend service with zero administration.
● Lambda can run code in response to the events. Example – update in DynamoDB Table or change in S3 bucket.
● You can even run your code in response to HTTP requests using Amazon API Gateway.

AWS Lambda: The Complete Guide
AWS **Lambda** is a **serverless compute service** that lets you run code without provisioning or managing servers. You pay only for the compute time you consume—there's no charge when your code isn't running.
Key Features
✅ **Event-Driven Execution** – Runs code in response to triggers (e.g., S3 uploads, API calls).
✅ **Automatic Scaling** – Handles from a few requests to thousands per second.
✅ **No Server Management** – AWS handles infrastructure, patching, and scaling.
✅ **Pay-Per-Use Pricing** – Billed by **millisecond** of execution time.
✅ **Multi-Language Support** – Node.js, Python, Java, C#, Go, Ruby, and custom runtimes.

---

1. How AWS Lambda Works
Basic Flow
1. **Upload Code** (ZIP file or container image).
2. **Configure Trigger** (e.g., S3, API Gateway, DynamoDB).
3. **Lambda Executes** when the trigger event occurs.
4. **Automatic Scaling** – Spins up instances as needed.

Example Use Cases
- **Real-time file processing** (e.g., resize images uploaded to S3).
- **Backend APIs** (via API Gateway).
- **Cron jobs** (using CloudWatch Events).
- **Data processing** (e.g., transform logs from CloudWatch).

---

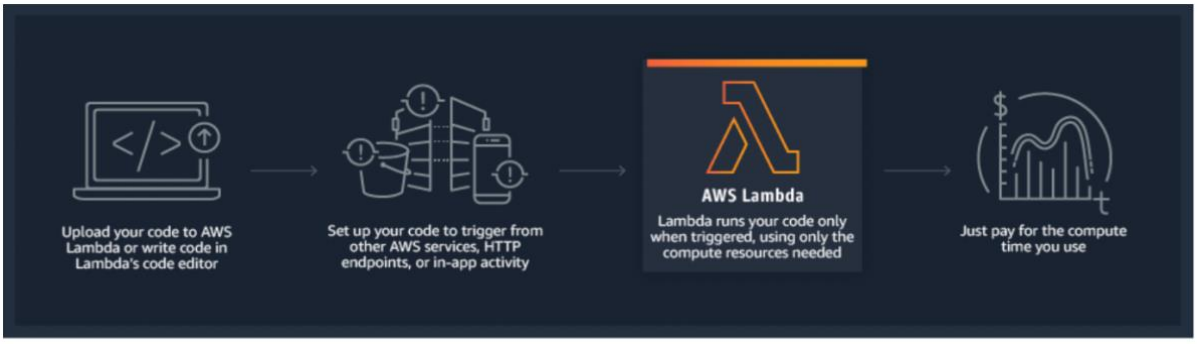
2. Lambda Components

Component	Description
Function	Your actual code (e.g., Python script).
Trigger	What invokes Lambda (e.g., S3, API Gateway).
Runtime	Language environment (Python, Node.js, etc.).
Execution Role	IAM permissions for the Lambda function.
Layers	Shared code/libraries across functions.
Concurrency	Controls how many instances run simultaneously.

What is Serverless computing?
● Serverless computing is a method of providing backend services on a pay per use basis.
● Serverless/Cloud vendor allows you to write and deploy code without worrying about the underlying infrastructure.
● Servers are still there, but you are not managing them, and the vendor will charge you based on usage.

When do you use Lambda?
● When using AWS Lambda, you are only responsible for your code.
● AWS Lambda manages the memory, CPU, Network, and other resources.
● It means you cannot log in to the compute instances or customize the operating system.
● If you want to manage your own compute resources, you can use other compute services such as EC2, Elastic Beanstalk.
● There will be a level of abstraction which means you cannot log in to the server or customize the runtime.

How does Lambda work?



Lambda Functions
● A function is a block of code in Lambda.

● You upload your application/code in the form of single or multiple functions.
● You can upload a zip file, or you can upload a file from the S3 bucket as well.
● After deploying the Lambda function, Lambda automatically monitors functions on your behalf, reporting metrics through Amazon CloudWatch

AWS Fargate
What is AWS Fargate?
AWS Fargate is a serverless compute service that is used for containers by Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).
● It eliminates the tasks required to provision, configure, or scale groups of virtual machines like Amazon EC2 to run containers.
● It packages the application in containers, by just specifying the CPU and memory requirements with IAM policies. Fargate task does not share its underlying kernel, memory resources, CPU resources, or elastic network interface (ENI) with another task.
● It does not support all the task definition parameters that are available in Amazon ECS tasks. Only a few are valid for Fargate tasks with some limitations.
● Kubernetes can be integrated with AWS Fargate by using controllers. These controllers are responsible for scheduling native Kubernetes pods onto Fargate.
● Security groups for pods in EKS can not be used when pods running on Fargate.
● The following storage types are supported for Fargate tasks:
○ Amazon EFS volumes for persistent storage
○ Ephemeral storage for nonpersistent storage

Amazon Elastic Kubernetes Service(EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) is a **managed Kubernetes service** that makes it easy to run Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control plane or nodes.

🧰 **Basic Workflow:**
1. **Create an EKS cluster** (via Console, CLI, or IaC like Terraform).
2. **Provision worker nodes** (EC2 or Fargate).
3. **Configure kubectl** to connect to the cluster.
4. **Deploy applications** using Kubernetes manifests (yaml files).
5. **Monitor and scale** using CloudWatch, HPA, and other tools.

What is Amazon Elastic Kubernetes Service(EKS)?
Amazon Elastic Kubernetes Service (Amazon EKS) is a service that enables users to manage Kubernetes applications in the AWS cloud or on-premises. Any standard Kubernetes application can be migrated to EKS without altering the code.

The EKS cluster consists of two components:
● Amazon EKS control plane
● Amazon EKS nodes

Amazon EKS (Elastic Kubernetes Service) - Complete Guide
AWS **Elastic Kubernetes Service (EKS)** is a **managed Kubernetes service** that simplifies deploying, managing, and scaling containerized applications using **Kubernetes** on AWS.

---

1. Key Features of Amazon EKS

✅ **Managed Control Plane** – AWS handles Kubernetes master nodes (API server, etcd, scheduler).
✅ **High Availability** – Runs across multiple AZs by default.
✅ **Integrates with AWS Services** (VPC, IAM, ALB, RDS, etc.).
✅ **Supports EC2 & Fargate** (serverless containers).
✅ **Kubernetes Compliance** – Certified conformant by the CNCF.
✅ **Security** – IAM integration, encryption (EBS, secrets), and private cluster support.

---

2. Core Components of EKS

a) EKS Cluster

- **Control Plane** (Managed by AWS, runs in AWS-owned VPC).
- **Worker Nodes** (EC2 or Fargate, run in your VPC).

b) Node Groups

- A group of **EC2 instances** running Kubernetes workloads.
- Can be **managed** (AWS handles scaling) or **self-managed**.

c) Kubernetes Add-ons

- **CoreDNS** (DNS-based service discovery).
- **kube-proxy** (Network traffic routing).
- **VPC CNI Plugin** (AWS-native networking).

d) Fargate Profiles

- Run **serverless containers** without managing EC2 instances.
- Good for **batch jobs, microservices**.

---

3. EKS vs. Self-Managed Kubernetes vs. ECS

Feature	EKS	Self-Managed K8s (kops, Kubeadm)	ECS
Management	AWS manages control plane	You manage everything	AWS manages orchestration
Scaling	Auto-scaling via Cluster Autoscaler	Manual/DIY	Auto-scaling
Networking	Uses AWS VPC CNI	Custom (Calico, Flannel)	AWS VPC
Best For	Enterprise K8s workloads	Full customization	Simple container apps

---

4. How EKS Works

1. **Create an EKS Cluster** (Control Plane).

2. **Launch Worker Nodes** (EC2 or Fargate).
3. **Deploy Kubernetes Manifests** (Pods, Deployments, Services).
4. **Use AWS Integrations** (ALB Ingress, IAM Roles for Service Accounts).

Troubleshooting Common Issues

- **Nodes not joining cluster?** → Check IAM roles & aws-auth ConfigMap.
- **Pod networking issues?** → Verify VPC CNI plugin.
- **Ingress not working?** → Check AWS Load Balancer Controller.

Amazon Elastic Container Service

What is Amazon ECS?

Amazon Elastic Container Service (Amazon ECS) is a regional container orchestration service like Docker that allows to execute, stop, and manage containers on a cluster. A container is a standard unit of software development that combines code, its dependencies, and system libraries so that the application runs smoothly from one environment to another.

Amazon Elastic Container Service (Amazon ECS) is a **fully managed container orchestration service** provided by AWS. It allows you to easily run, scale, and secure **Docker containers** on a cluster of virtual machines.

ECS Launch Types:

1. **EC2 Launch Type**:
    - You manage the EC2 instances (cluster capacity).
    - More control over the infrastructure.
2. **Fargate Launch Type**:
    - Serverless – no need to manage EC2 instances.
    - You only define the container specs; AWS handles the rest.

🧰 **Basic ECS Workflow:**

1. **Create a Task Definition**: Define container settings (image, CPU, memory, ports).
2. **Create a Cluster**: Logical grouping of resources.
3. **Run a Task or Service**: Launch containers using EC2 or Fargate.
4. **Monitor and Scale**: Use CloudWatch and Auto Scaling.

Amazon ECS (Elastic Container Service) - Complete Guide

Amazon **ECS (Elastic Container Service)** is a fully managed **container orchestration service** that helps you run, scale, and manage Docker containers on AWS. It integrates with other AWS services like **EC2, Fargate, ECR, and Load Balancers** for seamless deployments.

---

1. Key Features of Amazon ECS

✅ **Supports Docker Containers** – Run any Dockerized application.
✅ **Serverless Option** – Use **AWS Fargate** to avoid managing servers.
✅ **High Scalability** – Auto-scaling for containers and clusters.

✅ **Integration with AWS Ecosystem** – Works with ALB, CloudWatch, IAM, and VPC.
✅ **Cost-Effective** – Pay only for resources used (EC2 or Fargate).

---

2. Core Concepts in ECS

Term	Description
Cluster	Logical group of EC2 instances or Fargate tasks.
Task Definition	Blueprint for your application (container images, CPU, memory, networking).
Task	A running instance of a Task Definition (can be 1+ containers).
Service	Maintains a desired number of Tasks (supports auto-scaling).
Container Agent	Runs on EC2 instances to manage tasks.

---

3. ECS Launch Types

a) EC2 Launch Type

- You **manage EC2 instances** where containers run.
- Good for **cost control** (use Spot Instances for savings).
- Best for **long-running workloads** with predictable resource needs.

b) Fargate Launch Type

- **Serverless** – No EC2 management, AWS handles infrastructure.
- Pay per **vCPU & memory** used by tasks.
- Ideal for **bursty workloads** or microservices.

Feature	EC2 Launch Type	Fargate Launch Type
Server Management	Yes (you manage EC2)	No (fully serverless)
Cost Model	Pay for EC2 instances	Pay per task (vCPU/memory)
Scaling	Auto Scaling Groups	Auto-configured scaling
Networking	Supports all EC2 networking modes	Only AWS VPC (no host mode)

---

4. ECS vs. EKS vs. Lambda

Feature	ECS	EKS (Kubernetes)	Lambda
Orchestration	AWS-native	Kubernetes	Serverless (no orchestration)

Feature	ECS	EKS (Kubernetes)	Lambda
Use Case	Docker microservices	Complex K8s apps	Event-driven functions
Management	Medium (easier than EKS)	High (K8s expertise needed)	None (fully managed)
Scaling	Auto-scaling	Auto-scaling (via K8s)	Automatic

---

5. How ECS Works (Step-by-Step)

1. **Create a Task Definition** (specify Docker image, CPU, memory).
2. **Launch a Cluster** (EC2 or Fargate-based).
3. **Run Tasks/Services** (manually or via auto-scaling).
4. **Integrate with ALB/NLB** (for load balancing).

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) is a **fully managed Docker container registry** provided by AWS. It allows you to **store, manage, and deploy container images** securely and at scale.

🔄 **Basic Workflow:**

1. **Create a repository** in ECR.
2. **Authenticate Docker** to ECR using the AWS CLI.
3. **Tag your image** with the ECR repository URI.
4. **Push the image** to ECR.
5. **Pull the image** from ECR in your ECS/EKS/Lambda deployments.

What is Amazon Elastic Container Registry?
Amazon Elastic Container Registry (ECR) is a managed service that allows users to store, manage, share, and deploy container images and artifacts. It is mainly integrated with Amazon Elastic Container Service (ECS), for simplifying the production workflow.

Features:
● It stores both the containers which are created, and any container software bought through AWS Marketplace.
● It is integrated with Amazon Elastic Container Service (ECS), Amazon Elastic Kubernetes Service (EKS), and AWS Lambda, and AWS Fargate for easy deployments.
● AWS Identity and Access Management (IAM) enables resource-level control of each repository within ECR.
● It supports public and private container image repositories. It allows sharing container applications privately within the organization or publicly for anyone to download.
● A separate portal called Amazon ECR Public Gallery, helps to access all public repositories hosted on Amazon ECR Public.

● It stores the container images in Amazon S3 because S3 provides 99.999999999% (11 9's) of data durability.
● It allows cross-region and cross-account replication of the data for high availability applications.
● Encryption can be done via HTTPS while transferring container images. Images are also encrypted at rest using Amazon S3 server-side encryption or by using customer keys managed by AWS KMS.
● It is integrated with continuous integration and continuous delivery and also with third-party developer tools.
● Lifecycle policies are used to manage the lifecycle of the images

Amazon Elastic Container Registry (ECR) - Complete Guide
Amazon ECR is a **fully managed Docker container registry** that makes it easy to store, manage, and deploy Docker container images. It integrates seamlessly with **Amazon ECS, EKS, and AWS Fargate**.

1. Key Features of Amazon ECR

✅ **Fully Managed** - No servers to maintain
✅ **Secure** - Integrated with AWS IAM and encrypted by default
✅ **High Performance** - Backed by Amazon S3 for durability
✅ **Integrated with AWS Services** - Works with ECS, EKS, Lambda, Batch
✅ **Vulnerability Scanning** - Built-in image scanning (via AWS Inspector)
✅ **Lifecycle Policies** - Automate image cleanup

2. Core Concepts

a) Registry

- A regional container image storage service (one per AWS account per region)
- Example format: 123456789012.dkr.ecr.us-east-1.amazonaws.com

b) Repository

- Stores Docker images (similar to folders in S3)
- Can apply fine-grained IAM permissions per repository

c) Image

- A versioned Docker container image (tagged with latest, v1.0, etc.)

9. Troubleshooting

🔹 **"no basic auth credentials" error** → Re-run aws ecr get-login
🔹 **403 Forbidden** → Check IAM permissions
🔹 **Slow pushes** → Check network connectivity to ECR

Amazon S3

Amazon S3 (Simple Storage Service) is a **scalable, durable, and secure object storage service** offered by AWS. It's designed to store and retrieve **any amount of data from anywhere** on the web.

🧰 **Basic Workflow:**

1. **Create a bucket** (a container for your objects).
2. **Upload objects** (files) to the bucket.
3. **Set permissions** (public/private, IAM roles, bucket policies).
4. **Access objects** via a URL or programmatically using the AWS SDK/CLI.

What is Amazon S3?
S3 stands for Simple Storage Service.
Amazon S3 is object storage that allows us to store any kind of data in the bucket. It provides availability in multiple AZs, durability, security, and performance at a very low cost.
Any type of customer can use it to store and protect any amount of data for use cases, like static and dynamic websites, data analytics, and backup.
Basics of S3?
● It is object-based storage.
● Files are stored in Buckets.
● The bucket is a kind of folder.
● Folders can be from 0 to 5 TB.
● S3 bucket names must be unique globally.
● When you upload a file in S3, you will receive an HTTP 200 code if the upload was successful.
● S3 offers Strong consistency for PUTs of new objects, overwrites or delete of current object and List operations.
● By Default, all the Objects in the bucket are private.

Permissions & Management.
● **Access Control List**: ACLs used to grant read/write permission to another AWS Account.
● **Bucket Policy:** It uses JSON based access policy advance permission to your S3 Resources.
● **CORS**: CORS stands for Cross-Origin Resource Sharing. It allows cross-origin access to your S3 Resources.

Amazon S3 (Simple Storage Service) - Complete Guide
Amazon **S3 (Simple Storage Service)** is a **scalable, secure, and highly durable object storage** service designed for storing and retrieving any amount of data from anywhere.

---

1. Key Features of Amazon S3
✅ **Unlimited Storage** – Store any amount of data (files, images, backups, logs).
✅ **High Durability (99.999999999%)** – Data is replicated across multiple AZs.
✅ **Security & Compliance** – Supports **encryption (SSE-S3, SSE-KMS, SSE-C)**, IAM policies, and access logging.
✅ **Scalability** – Handles millions of requests per second.
✅ **Cost-Effective** – Pay only for what you use (no minimum fee).
✅ **Integrations** – Works with **Lambda, CloudFront, ETL tools, and more**.

---

2. Core Concepts in S3

Term	Description
Bucket	A container for objects (globally unique name, region-specific).
Object	A file + metadata (Key, Value, Version ID, Metadata).
Key	The object's filename (e.g., images/profile.jpg).
Versioning	Keeps multiple versions of an object (protects against deletes).
Storage Class	Different tiers for cost optimization (Standard, Intelligent-Tiering, Glacier).

4. S3 Security & Access Control

- **Bucket Policies** (JSON-based rules for bucket-level access).
- **IAM Policies** (Granular user/role permissions).
- **ACLs (Legacy)** – Basic read/write permissions (avoid if possible).
- **Encryption**
  - **SSE-S3** (S3-managed keys).
  - **SSE-KMS** (AWS KMS-managed keys).
  - **SSE-C** (Customer-provided keys).
  - **Client-Side Encryption** (Encrypt before uploading).

---

5. S3 Data Management Features

✓ **Versioning** – Keep multiple versions of files (protects against accidental deletes).
✓ **Lifecycle Policies** – Automatically transition objects to cheaper storage classes.
✓ **Cross-Region Replication (CRR)** – Copy objects to another region.
✓ **Event Notifications** – Trigger Lambda, SQS, or SNS on file uploads.
✓ **S3 Select & Glacier Select** – Retrieve only parts of files (cost-saving).

AWS EBS - Elastic Block Store

Amazon EBS (Elastic Block Store) is a **block storage service** designed for use with **Amazon EC2** instances. It provides **persistent, high-performance storage** that can be attached to EC2 instances, similar to how a hard drive works with a physical server.

Key Characteristics of EBS:

Feature	Description
Persistent	**Data remains intact even after the EC2 instance is stopped or terminated.**
Block-level storage	**Ideal for databases, file systems, and applications requiring low-latency access.**

Feature	Description
Attachable	**Can be attached to one EC2 instance at a time (except for multi-attach volumes).**
Encrypted	**Supports encryption at rest and in transit.**
Snapshot support	**Back up volumes to Amazon S3 using snapshots.**

📦 **EBS Volume Types:**

Volume Type	Use Case	Key Traits
gp3	**General-purpose**	**Customizable IOPS and throughput**
gp2	**General-purpose (legacy)**	**Baseline performance with burst**
io2/io1	**IOPS-intensive apps**	**High-performance, durable**
st1	**Throughput-optimized HDD**	**Big data, log processing**
sc1	**Cold HDD**	**Infrequent access, lowest cost**

What is AWS EBS?
Amazon Elastic Block Store (AWS EBS) is a persistent block-level storage (volume) service designed to be used with Amazon EC2 instances. EBS is AZ specific & automatically replicated within its AZ to protect from component failure, offering high availability and durability.

Features:
● High Performance (Provides single-digit-millisecond latency for high-performance)
● Highly Scalable (Scale to petabytes)
● Offers high availability (guaranteed 99.999% by Amazon) & Durability
● Offers seamless encryption of data at rest through Amazon Key Management Service (KMS).
● Automate Backups through data lifecycle policies using EBS Snapshots to S3 Storage.
● EBS detached from an EC2 instance and attached to another one quickly.

EBS vs Instance Store
Instance Store (ephemeral storage) :
● It is ideal for temporary block-level storage like buffers, caches, temporary content
● Data on an instance store volume persists only during the life of the associated instance. (As it is volatile storage - lose data if stop the instance/instance crash)
● Physically attached to ec2 instance - hence, the lowest possible latency.
● Massive IOPS - High performance
● Instance store backed Instances can be of maximum 10GiB volume size

● Instance store volume cannot be attached to an instance, once the Instance is up and running.
● Instance store volume can be used as root volume.
● You cannot create a snapshot of an instance store volume.

EBS :
● Persistent Storage.
● Reliable & Durable Storage.
● EBS volume can be detached from one instance and attached to another instance.
● EBS boots faster than instance stores.

AWS EBS (Elastic Block Store) - Complete Guide
AWS Elastic Block Store (EBS) provides persistent block storage volumes for use with Amazon EC2 instances. Unlike ephemeral instance store volumes, EBS volumes persist independently of the life of an instance.
Key Features of EBS
✅ **Durable & Persistent** - Data persists even after instance termination
✅ **High Performance** - SSD-backed options for I/O intensive workloads
✅ **Scalable** - Resize volumes on-the-fly (with some limitations)
✅ **Snapshots** - Point-in-time backups stored in S3
✅ **Encryption** - AES-256 encryption at rest (using AWS KMS)
✅ **Multi-Attach** - Some volumes can connect to multiple instances

EBS Volume Types Comparison

Volume Type	Description	Best For	Max IOPS	Max Throughput
gp3 (General Purpose SSD)	Default balanced SSD	Boot volumes, dev environments	16,000	1,000 MB/s
io2/io1 (Provisioned IOPS SSD)	High-performance SSD	Databases (Oracle, SAP)	64,000 (io2 Block Express: 256K)	4,000 MB/s
st1 (Throughput Optimized HDD)	Low-cost HDD	Big data, log processing	500	500 MB/s
sc1 (Cold HDD)	Lowest cost HDD	Infrequently accessed data	250	250 / s

EBS vs Instance Store

Feature	EBS Volume	Instance Store
Persistence	Survives instance stop/termination	Lost on instance stop/termination
Performance	Network-attached (varies by type)	Direct-attached (extremely high speed)
Cost	Persistent storage pricing	Free (included with instance)
Use Case	Databases, persistent storage	Cache, temporary data, scratch disks

Key Operations

1. **Creating & Attaching Volumes**
    - Create in same AZ as EC2 instance
    - Attach to instances as /dev/sdf through /dev/sdp
2. **Modifying Volumes**
    - Increase size (can be done without stopping instance for most types)
    - Change volume type (gp2→gp3, etc.)
3. **Taking Snapshots**

bash
Copy
Download
aws ec2 create-snapshot --volume-id vol-12345 --description "My backup"

    - Snapshots are incremental (only changed blocks stored)
    - Can create AMIs from snapshots
4. **Encryption**
    - Enabled by default for new volumes in many regions
    - Uses AWS KMS (Customer Master Keys)

AWS EFS - Elastic File Storage

Amazon EFS (Elastic File System) is a **fully managed, scalable, and elastic NFS (Network File System)** file storage service provided by AWS. It allows multiple EC2 instances to **simultaneously access a shared file system**, making it ideal for workloads that require shared access to data.

🧰 **Basic Workflow:**

1. **Create an EFS file system** in the AWS Console or CLI.
2. **Configure mount targets** in your VPC subnets.
3. **Mount the file system** on EC2 instances using the NFS protocol.
4. **Read/write files** as you would with a local file system.

🔄 **EFS vs. EBS vs. S3:**

Feature	EFS	EBS	S3
Type	File storage	Block storage	Object storage
Access	Multiple EC2s	Single EC2 (or multi-attach)	Web/API
Use Case	Shared file systems	Databases, OS volumes	Backups, static assets
Scalability	Auto-scales	Manual	Auto-scales

What is AWS EFS?
Amazon Elastic File System (Amazon EFS) provides a scalable, fully managed elastic distributed file system based on NFS. It is persistent file storage & can be easily scaled up to petabytes. It is designed to share parallelly with thousands of EC2 instances to provide better throughput and IOPS. It is a regional service automatically replicated across multiple AZ's to provide High Availability and durability.

Amazon EFS (Elastic File System) - Complete Guide
Amazon EFS is a **fully managed, scalable, cloud-native NFS file system** for AWS workloads. It provides **shared file storage** that can be accessed by multiple EC2 instances, containers, and serverless applications simultaneously.

1. Key Features of Amazon EFS

✅ **Fully Managed** - No hardware to provision
✅ **Elastic Scaling** - Grows and shrinks automatically
✅ **Shared Access** - Multiple instances can access files concurrently
✅ **High Availability** - Replicates across AZs (Standard storage class)
✅ **Security** - Supports IAM, VPC security groups, encryption at rest/in-transit
✅ **Multi-Protocol** - Supports NFS v4.1 (Linux) and soon Amazon S3 access

2. Core Components

a) File System

- The primary EFS resource (similar to an EBS volume but shared)
- Can be mounted on multiple EC2 instances simultaneously

b) Mount Targets

- ENIs (Elastic Network Interfaces) in each AZ that allow EC2 access
- Each mount target gets its own IP address

c) Access Points

- Application-specific entry points with custom:
  - POSIX user/group permissions
  - Root directory restrictions
  - IAM policies

3. EFS Performance Modes

Mode	Description	Best For
General Purpose	Low latency (ms)	Web servers, CMS
Max I/O	Higher throughput, higher latency	Big data, media processing

4. Storage Classes

Class	Description	Cost
Standard	Frequently accessed files	Higher
Infrequent Access (IA)	90% cost savings for rarely accessed files	Lower

6. EFS Security

- **Network Security**:
  - VPC security groups on mount targets
  - Can enable VPC endpoints for private access
- **File System Security**:
  - POSIX permissions (user/group/others)
  - IAM policies for API-level control
- **Encryption**:
  - At-rest (KMS)
  - In-transit (TLS 1.2+)

AWS Snowball

What is AWS Snowball?

● AWS Snowball is a storage device used to transfer a large amount of data ranging from 50TB - 80TB between Amazon Simple Storage Service and onsite data storage location at high speed.

AWS Storage Gateway

What is the AWS Storage Gateway?

AWS Storage Gateway is a hybrid cloud storage service that allows your on-premise storage & IT infrastructure to seamlessly integrate with AWS Cloud Storage Services. It Can be AWS Provided Hardware or Compatible Virtual Machine.

Amazon Aurora

What is Amazon Aurora?

Aurora is the fully managed RDS services offered by AWS. It's only compatible with PostgreSQL/MySQL. As per AWS, Aurora provides 5 times throughput to traditional MySQL and 3 times throughput to PostgreSQL.

Amazon DocumentDB

What is Amazon DocumentDB?

DocumentDB is a fully managed document database service by AWS which supports MongoDB workloads. It is highly recommended for storing, querying, and indexing JSON Data.

Amazon DynamoDB

Amazon DynamoDB is a **fully managed NoSQL database service** provided by AWS that delivers **single-digit millisecond performance at any scale**. It's designed for applications that require consistent, low-latency data access and can scale to support millions of requests per second.

📦 **Data Model:**

- **Tables**: Collections of items.
- **Items**: Individual records (like rows).
- **Attributes**: Fields within an item (like columns).
- **Primary Key**: Uniquely identifies each item (can be simple or composite).
- **Secondary Indexes**: Enable querying on non-key attributes.

What is DynamoDB?

● AWS DynamoDB is a Key-value and DocumentDB database by Amazon.
● It delivers a single Digit millisecond Latency.
● It can handle 20 million requests per second and 10 trillion requests a day.
● It is a Serverless Service; it means no servers to manage.
● It maintains the performance by managing the data traffic of tables over multiple servers.

Amazon DynamoDB - Complete Guide

Amazon DynamoDB is a **fully managed NoSQL database** service that provides **single-digit millisecond performance** at any scale. It's a key-value and document database that delivers **seamless scalability, high availability, and low latency**.

1. Key Features of DynamoDB

✅ **Serverless** - No servers to manage, automatic scaling
✅ **High Performance** - Single-digit millisecond latency
✅ **Highly Available** - Multi-AZ by default with 99.999% SLA
✅ **Flexible Data Models** - Key-value + document store
✅ **Durable** - Replicated across 3 AZs
✅ **Security** - Encryption at rest, VPC endpoints, IAM integration

2. Core Concepts

a) Tables

- The top-level container for your data (similar to a database in SQL)

b) Items

- A single data record (similar to a row in SQL)
- Can contain **up to 400KB** of data

c) Attributes

- Key-value pairs that make up an item (similar to columns in SQL)
- Supports **scalar** (string, number, binary), **document** (list, map), and **set** types

d) Primary Key

- **Partition Key (HASH key)**: Single attribute that determines partition
- **Composite Key (Partition + Sort Key)**: Enables richer queries

3. DynamoDB vs. Traditional Databases

Feature	DynamoDB	RDS (SQL)
Data Model	Key-value + document	Relational
Scaling	Automatic, unlimited	Manual, limited
Performance	Predictable low latency	Variable
Management	Fully managed	Requires maintenance
Schema	Flexible	Rigid

Amazon RDS

Amazon RDS (Relational Database Service) is a **fully managed relational database service** by AWS that makes it easy to set up, operate, and scale a relational database in the cloud. It automates time-consuming tasks like provisioning, patching, backups, and scaling.

🧰 **Basic Workflow:**

1. **Choose a database engine (e.g., PostgreSQL).**
2. **Configure instance settings (vCPU, memory, storage).**
3. **Set up networking and security (VPC, security groups).**
4. **Launch the DB instance.**
5. **Connect to the database using standard tools (e.g., psql, mysql, JDBC).**

What is Amazon RDS?

RDS (Relational Database System) in AWS makes it easy to operate, manage, and scale in the cloud. It provides scalable capacity with a cost-efficient pricing option and automates manual administrative tasks such as patching, backup setup, and hardware provisioning.

MySQL

● It is the most popular open-source DB in the world.
● Amazon RDS makes it easy to provision the DB in AWS Environment without worrying about the physical infrastructure.
● In this way, you can focus on application development rather than Infra. Management.

Amazon RDS (Relational Database Service) - Complete Guide

Amazon RDS is a **managed relational database service** that simplifies database setup, operation, and scaling in the cloud. It supports multiple database engines with automated backups, patching, and high availability.

1. Key Features of Amazon RDS

✅ **Fully Managed** - AWS handles provisioning, patching, backups
✅ **Multi-Engine Support** - MySQL, PostgreSQL, Oracle, SQL Server, MariaDB, Aurora
✅ **High Availability** - Multi-AZ deployments for failover
✅ **Scalability** - Vertical scaling (instance size) & read replicas
✅ **Automated Backups** - Point-in-time recovery (up to 35 days)
✅ **Security** - Encryption at rest/in-transit, IAM integration, VPC isolation

2. Supported Database Engines

Engine	Use Cases	Special Features
MySQL	Web apps, CMS	Compatible with open-source MySQL
PostgreSQL	Geospatial, JSON docs	Advanced extensions (PostGIS, pgvector)
Aurora	High-performance apps	5x faster than MySQL, auto-scaling
SQL Server	Enterprise .NET apps	License included (License Included mode)
Oracle	Enterprise applications	Bring Your Own License (BYOL) option
MariaDB	MySQL-compatible alternative	Enhanced storage engines

3. Core Components

a) DB Instance

- The basic building block (e.g., db.m6g.large)
- Compute + Memory + Storage combination

b) Multi-AZ Deployment

- **Synchronous standby replica** in another AZ
- Automatic failover (<2 min downtime)

c) Read Replicas

- **Asynchronous copies** for read scaling (up to 15 per master)
- Available for MySQL, PostgreSQL, MariaDB, Aurora

d) Parameter Groups

- Manage database configuration settings
- Customize memory allocation, timeouts, etc.

e) Option Groups

- Enable additional features like Oracle APEX or SQL Server TDE

4. Creating an RDS Database

Via AWS Console:

1. Navigate to RDS → "Create database"
2. Select engine (e.g., PostgreSQL)
3. Choose template (Production, Dev/Test)
4. Configure:
    - DB instance size
    - Storage type (GP3, IOPS-optimized)
    - VPC & security groups
5. Set master username/password

5. Backup & Recovery
Automated Backups

- Daily full backups + transaction logs
- Retention period (1-35 days)
- Restore to any second within retention

Manual Snapshots

- User-initiated (persist until deleted)
- Can copy across regions

AWS Secrets Manager

AWS Secrets Manager is a **secure and fully managed service** that helps you **store, manage, and retrieve sensitive information**, such as:

- Database credentials
- API keys
- OAuth tokens
- SSH keys
- Other application secrets

🧰 **Basic Workflow:**

1. **Create a secret** in the AWS Console or CLI.
2. **Store key-value pairs** (e.g., username, password).
3. **Grant access** using IAM policies.
4. **Retrieve the secret** in your application using the AWS SDK or CLI.

What is AWS Secrets Manager?
AWS Secrets Manager is a service that replaces secret credentials in the code like passwords, with an API call to retrieve the secret programmatically. The service provides a feature to rotate, manage, and retrieve database passwords, OAuth tokens, API keys, and other secret credentials. It ensures in-transit encryption of the secret between AWS and the system to retrieve the secret. Secrets Manager can easily rotate credentials for AWS databases without any additional programming. Though rotating the secrets for other databases or services requires Lambda function to instruct how Secrets Manager interacts with the database or service.

Accessing Secrets Manager:
● AWS Management Console

○ It stores binary data in secret.
● AWS Command Line Tools
○ AWS Command Line Interface
○ AWS Tools for Windows PowerShell
● AWS SDKs
● Secrets Manager HTTPS Query API

Secret rotation is available for the following Databases:
● MySQL on Amazon RDS
● PostgreSQL on Amazon RDS
● Oracle on Amazon RDS
● MariaDB on Amazon RDS
● Amazon DocumentDB
● Amazon Redshift
● Microsoft SQL Server on Amazon RDS
● Amazon Aurora on Amazon RDS

Features:
● It provides security and compliance facilities by rotating secrets safely without the need for code deployment.
● With Secrets Manager, IAM policies and resource-based policies can assign specific permissions for developers to retrieve secrets and passwords used in the development environment or the production environment.
● Secrets can be secured with encryption keys managed by AWS Key Management Service (KMS).
● It integrates with AWS CloudTrail and AWS CloudWatch to log and monitor services for centralized auditing.

Use cases:
● Store sensitive information as part of the encrypted secret value, either in the SecretString or SecretBinary field.
● Use a Secrets Manager open-source client component to cache secrets and update them only when there is a need for rotation.
● When an API request quota exceeds, the Secrets Manager throttles the request and returns a 'ThrottlingException' error. To resolve this, retry the requests.
● It integrates with AWS Config and facilitates tracking of changes in Secrets Manager.

AWS Secrets Manager - Complete Guide
AWS Secrets Manager is a **secure secrets management service** that helps you protect access to your applications, services, and IT resources by enabling you to **store, rotate, and retrieve secrets** programmatically.

1. Key Features
✅ **Secure Secret Storage** - Encrypted at rest using AWS KMS
✅ **Automatic Rotation** - Built-in support for RDS, Redshift, DocumentDB
✅ **Fine-Grained Access Control** - Integrated with AWS IAM

✅ **Cross-Account Access** - Share secrets across AWS accounts
✅ **Audit Trail** - Logs all access via AWS CloudTrail

2. What Can You Store?

- Database credentials (RDS, MySQL, PostgreSQL, etc.)
- API keys (3rd party services)
- OAuth tokens
- Encryption keys (though KMS is better for crypto keys)
- Any plaintext/key-value pairs (up to 10KB per secret)

3. Core Concepts

a) Secret

A container for your sensitive data that contains:

- Secret values (key/value pairs)
- Rotation configuration
- Metadata (description, tags, etc.)

b) Secret Rotation

Automatically updates credentials on a schedule (e.g., every 30 days)

c) KMS Integration

All secrets are encrypted using AWS Key Management Service (KMS)

4. Getting Started

Creating a Secret (Console)

1. Go to AWS Secrets Manager
2. Choose "Store a new secret"
3. Select secret type (e.g., "RDS database credentials")
4. Enter credentials and configure rotation (if needed)
5. Set permissions via IAM

6. Secret Rotation

Supported Services

- Amazon RDS (MySQL, PostgreSQL, Oracle, SQL Server, MariaDB)
- Amazon DocumentDB
- Amazon Redshift

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) is a **fully managed service** that helps you **provision, manage, and deploy SSL/TLS certificates** for use with AWS services and your internal connected resources. It simplifies the process of securing websites and applications by handling the complexity of certificate management.

🧰 **Basic Workflow:**

1. **Request a certificate** (public or private).
2. **Validate domain ownership** (via DNS or email).
3. **Deploy the certificate** to services like:
    - Elastic Load Balancer (ELB)

- Amazon CloudFront
- Amazon API Gateway

4. **Monitor and renew** automatically (for public certs issued by ACM).

What is AWS Certificate Manager?
AWS Certificate Manager is a service that allows a user to provide, manage, renew and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) X.509 certificates. The certificates can be integrated with AWS services either by issuing them directly with ACM or importing third-party certificates into the ACM management system.

SSL Server Certificates:
● HTTPS transactions require server certificates X.509 that bind the public key in the certificate to provide authenticity.
● The certificates are signed by a certificate authority (CA) and contain the server's name, the validity period, the public key, the signature algorithm, and more.

The different types of SSL certificates are:
● Extended Validation Certificates (EV SSL) - most expensive SSL certificate type
● Organization Validated Certificates (OV SSL) - validate a business' creditably
● Domain Validated Certificates (DV SSL) - provide minimal encryption
● Wildcard SSL Certificate - secures base domain and subdomains
● Multi-Domain SSL Certificate (MDC) - secure up to hundreds of domain and subdomains
● Unified Communications Certificate (UCC) - single certificate secures multiple domain names.

Ways to deploy managed X.509 certificates:
1. AWS Certificate Manager (ACM) - useful for large customers who need a secure web presence.
● ACM certificates are deployed using Amazon API Gateway, Elastic Load Balancing, Amazon CloudFront.
2. ACM Private CA - useful for large customers building a public key infrastructure (PKI) inside the AWS cloud and intended for private use within an organization.
● It helps create a certificate authority (CA) hierarchy and issue certificates to authenticate users, computers, applications, services, servers, and other devices.
● Private certificates by Private CA for applications provide variable certificate lifetimes or resource names.

ACM certificates are supported by the following services:
● Elastic Load Balancing
● Amazon CloudFront
● AWS Elastic Beanstalk
● Amazon API Gateway
● AWS Nitro Enclaves (an Amazon EC2 feature)
● AWS CloudFormation

AWS Certificate Manager (ACM) - Complete Guide

AWS Certificate Manager (ACM) is a **managed SSL/TLS certificate service** that simplifies provisioning, deploying, and renewing certificates for AWS services and internal resources.

1. Key Features of ACM

✅ **Free SSL/TLS Certificates** - No cost for public certificates
✅ **Automatic Renewal** - No manual renewal needed
✅ **Integrated with AWS Services** - Works with ALB, CloudFront, API Gateway
✅ **High Availability** - Certificates are regionally distributed
✅ **Private CA Support** - For internal PKI infrastructure

2. Supported Certificate Types

Type	Description	Use Case
Public Certificates	Domain-validated (DV) certificates	Public websites (example.com)
Private Certificates	Issued by your Private CA	Internal apps (.internal)
Wildcard Certificates	Covers *.example.com	Multiple subdomains
Multi-Domain (SAN) Certificates	Multiple domains in one cert	example.com + api.example.com

3. ACM Integration with AWS Services

- **Elastic Load Balancing (ALB/NLB)**
- **Amazon CloudFront**
- **API Gateway**
- **AWS Elastic Beanstalk**
- **AWS CloudFormation**

4. Requesting a Public Certificate

Via AWS Console

1. Navigate to **ACM > Request a certificate**
2. Choose **Public certificate**
3. Add domain names (e.g., example.com, *.example.com)
4. Select validation method:
    - **DNS validation** (recommended, creates CNAME record)
    - **Email validation** (manual approval)
5. **Validate** domain ownership

6. Deploying ACM Certificates

On ALB

1. Create/update load balancer
2. Select ACM certificate from dropdown

On CloudFront

1. Create distribution
2. Select certificate from **US East (N. Virginia)** region

AWS Auto Scaling

AWS Auto Scaling is a service that helps you **automatically adjust the capacity of your AWS resources** to maintain performance and optimize costs. It can scale **EC2 instances**, **ECS services**, **DynamoDB tables**, and **Aurora Replicas** based on demand.

🧱 **Components of EC2 Auto Scaling:**

1. **Launch Template/Configuration**: Defines how new instances are launched (AMI, instance type, etc.).
2. **Auto Scaling Group (ASG)**: Manages a group of EC2 instances.
3. **Scaling Policies**:
    - **Target tracking** (e.g., keep CPU at 50%)
    - **Step scaling** (scale by steps based on thresholds)
    - **Scheduled scaling** (scale at specific times)

What is AWS Auto Scaling?

● AWS Auto Scaling keeps on monitoring your Application and automatically adjusts the capacity required for steady and predictable performance.
● By using auto scaling it's very easy to set up the scaling of the application automatically with no manual intervention.
● It allows you to create scaling plans for the resources like EC2 Instances, Amazon EC2 tasks, Amazon DynamoDB, Amazon Aurora Read Replicas.
● It balances Performance Optimization and cost.

Monitoring:

● **Health Check:** Keep on checking the health of the instance and remove the unhealthy instance out of Target Group.
● **CloudWatch Events:** AutoScaling can submit events to Cloudwatch for any type of action to perform in the autoscaling group such as a launch or terminate an instance.
● **CloudWatch Metrics:** It shows you the statistics of whether your application is performing as expected.
● **Notification Service:** Autoscaling can send a notification to your email if the autoscaling group launches or the instance gets terminated.

AWS Auto Scaling - Complete Guide

AWS Auto Scaling automatically adjusts your compute resources to maintain performance while optimizing costs. It ensures you have the right number of Amazon EC2 instances (or other resources) available to handle your application load.

Key Features

✅ **Automatic Scaling** - Adds/removes instances based on demand
✅ **Multiple Scaling Strategies** - Target tracking, step scaling, simple scaling
✅ **Multi-Resource Scaling** - EC2, ECS, DynamoDB, Aurora
✅ **Cost Optimization** - Maintains performance at lowest cost
✅ **Integration** - Works with ELB, CloudWatch, Route 53

Core Components

1. Auto Scaling Groups (ASG)

- Logical group of EC2 instances
- Defines:

- Minimum/maximum/desired capacity
- Launch templates/configurations
- Availability Zone distribution
- Health check settings

2. Launch Templates/Configurations

- Blueprint for new instances (AMI, instance type, key pair, IAM role, etc.)
- Launch Templates (newer) support versioning

3. Scaling Policies

Policy Type	Description	Use Case
Target Tracking	Maintains a specific metric value	CPU at 40% utilization
Step Scaling	Adds/removes instances in increments	Gradual response to load changes
Simple Scaling	Single adjustment with cooldown period	Simple applications

How Auto Scaling Works

1. **Monitors Metrics** (CPU, memory, network, custom)
2. **Triggers Scaling** when thresholds are breached
3. **Launches/Terminates** instances to match demand
4. **Maintains Health** - Replaces unhealthy instances

Monitoring & Optimization

- **CloudWatch Metrics**: CPUUtilization, RequestCount
- **Scaling History**: View past scaling events
- **Cost Explorer**: Analyze scaling impact on costs

AWS CloudFormation

AWS CloudFormation is a **service that enables you to model, provision, and manage AWS infrastructure as code**. You define your infrastructure in a **template file** (written in YAML or JSON), and CloudFormation takes care of provisioning and configuring those resources automatically.

🔧 **Basic Workflow:**

1. **Write a template** in YAML or JSON.
2. **Upload it** to the AWS Console, CLI, or SDK.
3. **Create a stack** from the template.
4. **CloudFormation provisions** the resources.
5. **Manage updates** using change sets or stack updates.

What is AWS CloudFormation?
AWS CloudFormation is a service that collects AWS and third-party resources and manages them throughout their life cycles, by launching them together as a stack. A template is used to create, update, and delete an entire stack as a single unit, without managing resources individually. It provides the capability to reuse the template to set the resources easily and repeatedly. It can be integrated with AWS IAM for security. It can be integrated with CloudTail to capture API calls as events.

Templates - A JSON or YAML formatted text file used for building AWS resources.
Stack - It is a single unit of resources.
Change sets - It allows checking how any change to a resource might impact the running resources. Stacks can be created using the AWS CloudFormation console and AWS Command Line Interface (CLI).
Stack updates: First the changes are submitted and compared with the current state of the stack and only the changed resources get updated.

There are two methods for updating stacks:
- **Direct update** - when there is a need to quickly deploy the updates.
- **Creating and executing change sets** - they are JSON files, providing a preview option for the changes to be applied.

StackSets are responsible for safely provisioning, updating, or deleting stacks. Nested Stacks are stacks created within another stack by using the AWS::CloudFormation::Stack resource. When there is a need for common resources in the template, Nested stacks can be used by declaring the same components instead of creating the components multiple times. The main stack is termed as parent stack and other belonging stacks are termed as child stack, which can be implemented by using ref variable '! Ref'.

AWS CloudFormation Registry helps to provision third-party application resources alongside AWS resources. Examples of third-party resources are incident management, version control tools.

AWS CloudFormation - Complete Guide
AWS **CloudFormation** is an **Infrastructure-as-Code (IaC)** service that allows you to model, provision, and manage AWS resources using **declarative JSON or YAML templates**. It automates the deployment of cloud infrastructure in a repeatable and scalable way.

---

1. Key Features of AWS CloudFormation
✅ **Infrastructure as Code (IaC)** – Define AWS resources in templates (YAML/JSON).
✅ **Automated Deployment** – Create, update, and delete stacks in a controlled manner.
✅ **Dependency Management** – Automatically handles resource creation order.
✅ **Rollback & Change Sets** – Safely test changes before applying them.
✅ **Drift Detection** – Identify manual changes to deployed resources.
✅ **Cross-Account & Cross-Region Deployments** – Use **StackSets** for large-scale deployments.

---

2. Core Concepts

Term	Description
Template	JSON/YAML file defining AWS resources and configurations.
Stack	A collection of AWS resources created from a template.
Change Set	Preview of changes before updating a stack.
StackSets	Deploy stacks across multiple accounts/regions.
Parameters	Dynamic inputs (e.g., instance type, VPC ID).
Outputs	Return values from a stack (e.g., public IP).
Nested Stacks	Break large templates into reusable components.

---

3. CloudFormation vs. Terraform vs. CDK

Feature	CloudFormation	Terraform	AWS CDK
Language	YAML/JSON	HCL (Hashicorp)	TypeScript, Python, etc.
Provider	AWS-only	Multi-cloud	AWS-only (CDK generates CF templates)
State Management	Managed by AWS	Self-managed (Terraform state file)	Managed by AWS
Best For	AWS-native deployments	Hybrid/multi-cloud	Developers who prefer coding ov

Amazon CloudWatch

Amazon CloudWatch is a **monitoring and observability service** provided by AWS that helps you collect, visualize, and analyze **metrics, logs, and events** from AWS resources, applications, and services in real time.

Key Features of Amazon CloudWatch:

Feature	Description
Metrics	Collect and track performance data (e.g., CPU usage, memory, disk I/O).

Feature	Description
Logs	Centralized logging from EC2, Lambda, ECS, and custom apps.
Alarms	Trigger actions (e.g., notifications, Auto Scaling) based on metric thresholds.
Dashboards	Visualize metrics and logs in customizable dashboards.
Events (EventBridge)	Respond to changes in your AWS environment with automated workflows.
CloudWatch Synthetics	Monitor endpoints using canary scripts.
CloudWatch Logs Insights	Query and analyze log data interactively.

What is Amazon CloudWatch?
Amazon CloudWatch is a service that helps to monitor and manage services by providing data and actionable insights for AWS applications and infrastructure resources. It monitors AWS resources such as Amazon RDS DB instances, Amazon EC2 instances, Amazon DynamoDB tables, and, as well as any log files generated by the applications.

Amazon CloudWatch can be accessed by the following methods:
- Amazon CloudWatch console
- AWS CLI
- CloudWatch API
- AWS SDKs

Amazon CloudWatch is used together with the following services:
- Amazon Simple Notification Service (Amazon SNS)
- Amazon EC2 Auto Scaling
- AWS CloudTrail
- AWS Identity and Access Management (IAM)

Amazon CloudWatch - Complete Guide
Amazon CloudWatch is AWS's **monitoring and observability** service that provides data and actionable insights for AWS, hybrid, and on-premises resources and applications.
1. Key Features of CloudWatch
✅ **Metrics Collection** - System and custom metrics
✅ **Logs Management** - Centralized log storage and analysis
✅ **Alarms & Notifications** - Real-time alerting
✅ **Dashboards** - Custom visualization of metrics

✅ **Events (EventBridge)** - Automated responses to changes
✅ **Synthetics** - Automated canary testing
✅ **ServiceLens** - End-to-end application monitoring

2. Core Components
a) CloudWatch Metrics
- **Standard Metrics**: Collected automatically from AWS services (EC2 CPU, S3 requests)
- **Custom Metrics**: Push your own application metrics
- **Dimensions**: Metric attributes (InstanceId, AutoScalingGroup)
- **Namespaces**: Containers for metrics (AWS/EC2, Custom/App)

b) CloudWatch Logs
- **Log Groups**: Collection of log streams
- **Log Streams**: Sequence of log events
- **Metric Filters**: Extract metrics from logs
- **Insights**: SQL-like log queries

c) CloudWatch Alarms
- Monitor metrics and trigger actions
- States: **OK**, **ALARM**, **INSUFFICIENT_DATA**
- Can notify via SNS, Auto Scaling, EC2 actions

d) CloudWatch Dashboards
- Custom views of metrics and logs
- Shareable across accounts
- Supports both AWS and custom metrics

3. Getting Started
Viewing Basic Metrics
1. Open CloudWatch Console
2. Navigate to **Metrics**
3. Browse by service (e.g., EC2, Lambda)

Amazon CloudFront

Amazon CloudFront is a **fast, secure, and programmable content delivery network (CDN)** service from AWS. It delivers your content—such as websites, APIs, video streams, and other web assets—to users globally with **low latency and high transfer speeds**.

🧰 **Basic Workflow:**
1. **Create a CloudFront distribution**
   - Choose an origin (e.g., S3 bucket, EC2, ALB).
2. **Configure cache behavior**
   - Set TTLs, allowed HTTP methods, and viewer protocol policies.
3. **Deploy the distribution**
   - CloudFront assigns a domain name (e.g., d1234.cloudfront.net).
4. **Use the CloudFront URL** or map it to your custom domain with Route 53.

🔐 **Example: Secure S3 Content with CloudFront**
- Store files in a **private S3 bucket**.

- Create a **CloudFront distribution** with the S3 bucket as the origin.
- Use **Origin Access Control (OAC)** to allow CloudFront to access the bucket.
- Enable **signed URLs** to restrict access to authorized users.

What is Amazon CloudFront?
Amazon CloudFront is a content delivery network (CDN) service that securely delivers any kind of data to customers worldwide with low latency, low network and high transfer speeds. It uses edge locations (a network of small data centers) to cache copies of the data for the lowest latency. If the data is not present at edge locations, the request is sent to the source server, and data gets transferred from there.

Amazon CloudFront - Complete Guide
Amazon CloudFront is a **global Content Delivery Network (CDN)** service that securely delivers data, videos, applications, and APIs to customers worldwide with **low latency and high transfer speeds**.

1. Key Features of Amazon CloudFront

✅ **Global Edge Network** - 400+ Points of Presence (PoPs) worldwide
✅ **High Performance** - Low latency content delivery
✅ **Security** - DDoS protection, HTTPS support, AWS WAF integration
✅ **Flexible Origin Options** - S3, EC2, ALB, MediaStore, or any custom HTTP server
✅ **Cost-Effective** - Pay-as-you-go pricing with free data transfer out to the internet

2. Core Components

a) Distribution

- The main CloudFront configuration unit
- Two types:
  - **Web Distribution** (for websites and HTTP content)
  - **RTMP Distribution** (for media streaming, now deprecated)

b) Edge Locations

- AWS data centers where content is cached
- Located globally for low-latency access

c) Origins

- The source of your content:
  - **S3 buckets**
  - **EC2 instances**
  - **Elastic Load Balancers**
  - **Custom origins** (any HTTP server)

d) Behaviors

- Define how CloudFront processes requests:
  - Path patterns (/images/*)
  - Cache settings
  - Origin selection

3. How CloudFront Works

1. User requests content (e.g., example.com/image.jpg)
2. DNS routes request to nearest Edge Location
3. If cached → served immediately
4. If not cached → fetched from origin, then cached for future requests

4. Creating a CloudFront Distribution

Step 1: Create Distribution via Console

1. Open CloudFront console → **Create Distribution**
2. Select origin (e.g., S3 bucket)
3. Configure settings:
    - **Default Cache Behavior** (TTL, headers)
    - **Distribution Settings** (Price class, SSL cert)
4. Deploy (takes 5-15 minutes)

AWS Transit Gateway

What is AWS Transit Gateway?

AWS Transit Gateway is a network hub used to interconnect multiple VPCs. It can be used to attach all hybrid connectivity by controlling your organization's entire AWS routing configuration in one place.

Transit Gateway vs. VPC peering:

Transit Gateway

It has an hourly charge per attachment in addition to the data transfer fees. Multicast traffic can be routed between VPC attachments to a Transit Gateway. It provides Maximum bandwidth (burst) of 50 Gbps per Availability Zone per VPC connection. Security groups feature does not currently work with Transit Gateway.

VPC peering

It does not charge for data transfer. Multicast traffic cannot be routed to peering connections. It provides no aggregate bandwidth. Security groups feature works with intra-Region VPC peering.

Amazon Route 53

Amazon Route 53 is a **highly available and scalable Domain Name System (DNS) web service** from AWS. It's designed to route end-user requests to internet applications hosted on AWS or elsewhere, and it also supports **domain registration** and **health checking**.

What is Amazon Route 53?

Route53 is a managed DNS (Domain Name System) service where DNS is a collection of rules and records intended to help clients/users understand how to reach any server by its domain name. Route 53 hosted zone is a collection of records for a specified domain that can be managed together. There are two types of zones:

● Public host zone – It determines how traffic is routed on the Internet.

● Private hosted zone – It determines how traffic is routed within VPC. Route 53 TTL (seconds):

● It is the amount of time for which a DNS resolver creates a cache information about the records and reduces the query latency.
● Default TTL does not exist for any record type but always specifies a TTL of 60 seconds or less so that clients/users can respond quickly to changes in health status.

Amazon Route 53 - Complete Guide
Amazon Route 53 is AWS's **highly available and scalable Domain Name System (DNS) web service** that provides reliable domain registration, DNS routing, and health checking.

1. Key Features of Route 53

✅ **Domain Registration** - Buy and manage domains
✅ **DNS Service** - Ultra-reliable DNS resolution (100% SLA)
✅ **Traffic Routing** - Advanced routing policies
✅ **Health Checking** - Monitor endpoints and failover
✅ **DDoS Protection** - Integrated with AWS Shield
✅ **Private DNS** - For VPCs and hybrid clouds

2. Core Components

a) Hosted Zones

- **Public Hosted Zone**: Routes internet traffic
- **Private Hosted Zone**: Routes traffic within VPCs

b) Record Sets

- Define how traffic is routed for a domain
- Common record types:
  - **A** (IPv4 address)
  - **AAAA** (IPv6 address)
  - **CNAME** (Canonical name)
  - **MX** (Mail exchange)
  - **TXT** (Text records)

c) Routing Policies

Policy	Use Case	Example
Simple	Basic routing	example.com → 192.0.2.1
Weighted	Split traffic	70% US, 30% EU
Latency	Lowest latency	Route to nearest region
Failover	Active-passive setup	Primary → Backup
Geolocation	Location-based routing	US users → US servers
Multi-Value	Random healthy endpoint	Load balancing

5. Integrations
With EC2/ELB

- Point domains to load balancers
- Use Alias records for zero-latency updates

With S3 Static Websites

bash
Copy
Download

```
aws route53 change-resource-record-sets \
 --hosted-zone-id Z1PA6795UKMFR9 \
 --change-batch '{
  "Changes": [{
   "Action": "CREATE",
   "ResourceRecordSet": {
    "Name": "static.example.com",
    "Type": "A",
    "AliasTarget": {
     "HostedZoneId": "Z3AQBSTGFYJSTF",
     "DNSName": "s3-website-us-east-1.amazonaws.com",
     "EvaluateTargetHealth": false
    }
   }
  }]
 }'
```

With CloudFront

- Route traffic to CDN endpoints

6. Security

- **DDoS Protection**: AWS Shield Standard (free)
- **IAM Policies**: Control who can manage DNS
- **Private DNS**: Isolate internal traffic

AWS SNS (Simple Notification Service)

Amazon SNS (Simple Notification Service) is a **fully managed messaging service** that enables you to **send messages or notifications** to a large number of subscribers or other AWS services. It supports **pub/sub (publish-subscribe)** messaging and **mobile push notifications**, making it ideal for decoupling microservices and sending alerts.

🧰 **Basic Workflow:**

1. **Create a topic** (e.g., OrderUpdates).
2. **Subscribe endpoints** (e.g., email, Lambda, SQS).
3. **Publish messages** to the topic.
4. **Subscribers receive** the messages in real time.

What is AWS SNS?

Amazon Simple Notification Service (Amazon SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud. It provides developers with a highly scalable, flexible, and cost-effective approach to publish messages from an application and deliver them to subscribers or other applications. It provides push notifications directly to mobile devices and delivers notifications by SMS text messages, email to Amazon Simple Queue Service (SQS), or any HTTP client. It allows developers to group multiple recipients using topics. It consists of topics and subscribers.

Amazon SNS (Simple Notification Service) - Complete Guide
Amazon SNS is a **fully managed pub/sub messaging service** that enables you to send notifications to distributed systems and mobile devices. It supports multiple protocols and provides high-throughput, push-based messaging.

1. Key Features of Amazon SNS
✅ **Pub/Sub Messaging** - Decouple senders (publishers) and receivers (subscribers)
✅ **Multiple Protocols** - HTTP(S), Email (SMTP), SMS, AWS Lambda, SQS, Mobile Push
✅ **High Availability** - Built on AWS's reliable infrastructure
✅ **Serverless Integration** - Directly trigger Lambda functions
✅ **Message Filtering** - Route messages selectively to subscribers
✅ **Message Encryption** - KMS integration for data security

2. Core Concepts
a) Topics
- Logical access points for communication (like a "channel")
- Unique ARN format: arn:aws:sns:region:account-id:topic-name

b) Subscriptions
- Endpoints receiving messages from a topic:
  - **Email** (JSON/text)
  - **SMS** (text messages)
  - **HTTP/HTTPS** (webhooks)
  - **AWS Lambda** (direct invocation)
  - **SQS** (queues for async processing)
  - **Mobile Push** (APNs, FCM, etc.)

c) Publishers
- Services/applications sending messages (e.g., EC2, Lambda, CloudWatch)

3. How SNS Works
1. **Publisher** sends a message to an **SNS Topic**
2. **SNS** replicates the message to all **subscribers**
3. **Subscribers** receive the message via their preferred protocol

4. Creating an SNS Topic & Subscription
Via AWS Console:
1. Go to **SNS → Topics → Create Topic**
2. Choose **Standard** (unlimited throughput) or **FIFO** (ordered delivery)
3. Add **Subscriptions** (e.g., email, Lambda, SQS)

5. SNS vs. SQS

Feature	SNS (Pub/Sub)	SQS (Queue)
Messaging Model	Broadcast (1:N)	Point-to-point (1:1)
Message Retention	No retention (immediate delivery)	Up to 14 days
Use Case	Fan-out notifications	Decoupled task processing
Ordering	Standard (unordered) or FIFO	Standard or FIFO
Polling Required?	No (push-based)	Yes (pull-based)

Amazon Simple Queue Service (SQS)

Amazon SQS (Simple Queue Service) is a **fully managed message queuing service** that enables **decoupling and scaling** of microservices, distributed systems, and serverless applications. It allows components of an application to communicate and coordinate by sending messages through queues.

What is Amazon Simple Queue Service (SQS)?
Amazon Simple Queue Service (SQS) is a serverless service used to decouple (loose couple) serverless applications and components. The queue represents a temporary repository between the producer and consumer of messages. It can scale up to 1-10000 messages per second. The default retention period of messages is four days and can be extended to fourteen days. SQS messages get automatically deleted after being consumed by the consumers. SQS messages have a fixed size of 256KB.

There are two SQS Queue types:

Standard Queue -
- The unlimited number of transactions per second.
- Messages get delivered in any order.
- Messages can be sent twice or multiple times. FIFO Queue -
- 300 messages per second.
- Support batches of 10 messages per operation, results in 3000 messages per second.
- Messages get consumed only once.

Amazon Simple Queue Service (SQS) - Complete Guide
Amazon SQS is a **fully managed message queuing service** that enables you to decouple and scale microservices, distributed systems, and serverless applications.
1. Key Features
✅ **Fully Managed** - No infrastructure to provision or manage
✅ **Highly Scalable** - Handles any volume of messages
✅ **Reliable** - Messages stored redundantly across multiple AZs

✅ **Secure** - Encryption, IAM policies, and VPC endpoints
✅ **Low Cost** - Pay only for what you use

2. Core Concepts
a) Queue Types

Type	Standard Queue	FIFO Queue
Ordering	Best-effort	Exactly-once, First-In-First-Out
Throughput	Nearly unlimited	Up to 3,000 messages/second
Duplicates	Possible	No duplicates
Use Cases	Most applications	Transactions, banking, ordering systems

b) Message Components

- **Body** (Up to 256KB text - can reference larger data in S3)
- **Attributes** (Metadata like timestamps)
- **ID** (Unique identifier)
- **Receipt Handle** (Used for deletion)

c) Visibility Timeout

- Duration (0-12 hours) that a message is hidden after being received
- Default: 30 seconds

Jenkins

Here is a comprehensive overview of Jenkins, covering its core concepts, architecture, usage, and best practices:

Jenkins Overview

Jenkins is an open-source automation server widely used for continuous integration (CI) and continuous delivery (CD). It helps automate the parts of software development related to building, testing, and deploying, facilitating CI/CD practices.

Key Concepts
1. Continuous Integration (CI):
CI is a development practice where developers integrate code into a shared repository frequently, preferably several times a day.
Jenkins helps to automate the build and test process every time a developer commits code, ensuring early detection of issues.

- **Definition:** Integrating the live changes of source code into master/production/central repository after being validated and tested.
  (or)
- Continuous Integration is a software development practice where developers regularly merge their code changes into a central repository after being validated and tested.

2. Continuous Delivery (CD):
CD is a practice where code changes are automatically built, tested, and prepared for release to production.
Jenkins can automate the deployment of applications, making it easier to deliver updates quickly and consistently.

- **Definition:** Continuous Delivery is a software development practice where source code changes are automatically built, tested, and prepared for release to production, but the actual release to production is done manually.

Continuous Deployment (CD):

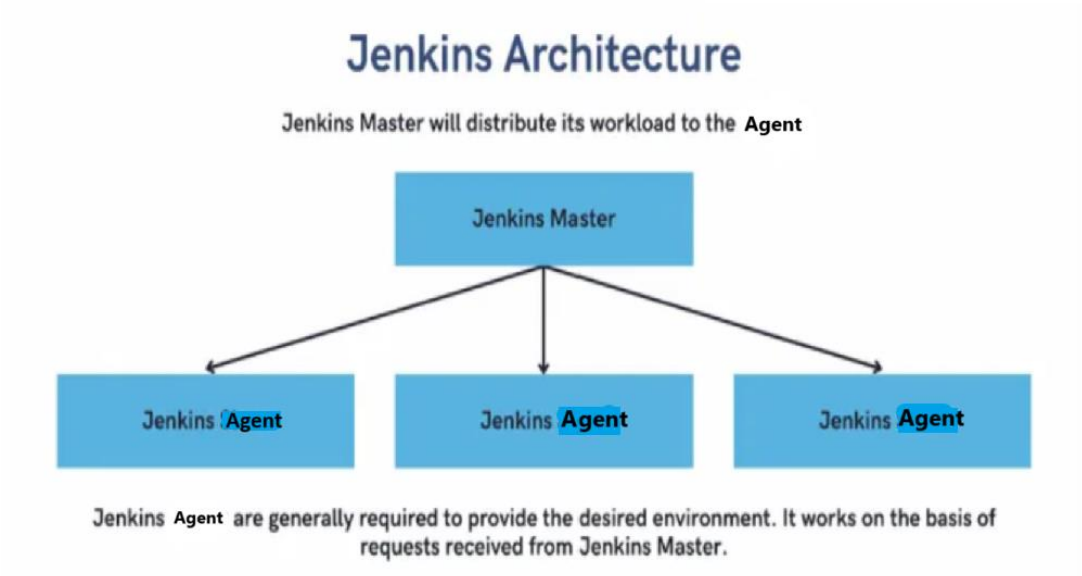
- **Definition:** "Continuous Deployment (CD) is a software development practice where source code changes are automatically built, tested, and released to production without manual intervention.

3. Pipeline:
A pipeline in Jenkins defines the entire workflow of building, testing, and deploying applications.
Jenkins pipelines can be scripted (Declarative or Scripted pipelines) using a domain-specific language (DSL).

Pipeline:
Devops pipeline is a set of automated tools and processes that helps developer and operation professionals work together to build and deploy code to production environments.

4. Plugins:
Jenkins is highly extensible through plugins.
Plugins allow Jenkins to integrate with various development, testing, and deployment tools like Git, Maven, Docker, Kubernetes, etc.

Jenkins Architecture



1. Master-Agent Architecture:
Jenkins Master: The main Jenkins server, responsible for scheduling jobs, dispatching builds to Agent, and monitoring the state of agents.
Jenkins agent: Agents that execute jobs dispatched by the master.

2. Jobs/Builds:
Jenkins jobs or builds define tasks like compiling code, running tests, or deploying applications.

Types of Jenkins jobs:
Freestyle Projects: Basic jobs that allow a wide variety of build configurations.

Pipeline Projects: More advanced, script-based jobs.

Feature	Freestyle Project	Pipeline Project
Configuration	Form-based (UI)	Code-based (Jenkinsfile)
Complexity	Simple, limited flexibility	Highly flexible, supports complex workflows
Multi-stage Builds	Limited support	Full support for multi-stage workflows
Version Control	Not easily versioned	Version-controlled (via Jenkinsfile in SCM)
Parallel Execution	Limited, requires plugins	Full support using parallel step
Error Handling & Conditionals	Basic error handling	Advanced error handling, retries, conditionals
Reusability	Not easily reusable across projects	Can be reused and stored in version control
UI/Visualization	Basic visualization	Advanced pipeline visualization
Use Case	Simple, individual tasks	Complex workflows, multi-stage, large projects

In summary:

- **Freestyle Projects** are great for simple, one-off tasks where you don't need complex workflows or configurations.
- **Pipeline Projects** are more suitable for larger projects that require flexible, maintainable, and versioned CI/CD pipelines with multiple stages, parallel execution, and advanced error handling.

3. Workspace:
Each Jenkins job has a workspace directory on the Jenkins agents, where it performs build operations.

Setting Up Jenkins

1. Installation:

Jenkins can be installed on various platforms, including Windows, macOS, and Linux.
Installation methods include direct download of Jenkins WAR file, Docker image, or package managers like apt or yum.

2. Initial Configuration:

Post-installation, Jenkins requires setting up the administrator password and installing plugins.
Configure Jenkins URL, manage credentials, and connect to version control systems like Git.

Configuring Jenkins
1. Global Tool Configuration:
Set up JDK, Maven, Ant, and other build tools required by Jenkins jobs.

2. Creating a Job:
Define the source code repository (Git, SVN, etc.).
Set up build triggers (e.g., polling the repository or receiving webhooks).
Define the build steps (e.g., execute shell commands, invoke Ant, or run a Maven target).
Post-build actions (e.g., publish reports or send notifications).

3. Pipelines:

Declarative Pipeline:

```
pipeline {
    agent any
    stages {
        stage('Build') {
            steps {
                sh 'mvn clean install'
            }
        }
```

```
        stage('Test') {
            steps {
                sh 'mvn test'
            }
        }
        stage('Deploy') {
            steps {
                sh 'mvn deploy'
            }
        }
    }
}
```

Scripted Pipeline:

```
node {
    stage('Build') {
        sh 'mvn clean install'
    }
    stage('Test') {
        sh 'mvn test'
    }
    stage('Deploy') {
        sh 'mvn deploy'
    }
}
```

Best Practices

1. Use Pipelines:
Prefer pipelines over freestyle projects for better scalability and maintainability.
2. Modular Jobs:
Create modular jobs with shared libraries to reduce code duplication.
3. Security:
Enable Role-Based Access Control (RBAC) for better security.
Manage credentials securely using Jenkins' credentials management.
4. Monitoring and Maintenance:
Regularly update Jenkins and its plugins.
Monitor Jenkins performance and scale Jenkins by adding more slave nodes if necessary.
5. Backup and Recovery:
Regularly back up Jenkins configuration and job configurations.
Use plugins like **ThinBackup** for automated backups.

In Jenkins, the **Manage Jenkins** section is the central place for administering the Jenkins server. Here's an explanation of the different options you typically find under Manage Jenkins:

1. System Configuration

Configure System:

Allows configuring global Jenkins settings, such as environment variables, default paths, email notifications, JDK, Git installations, and other tools.

Global Tool Configuration:

Used to set up global tools like JDKs, Maven, Ant, Gradle, Git, and others that are used across different jobs.

2. Security

Manage Users:

Used to create, update, delete, or manage user accounts within Jenkins.

Configure Global Security:

Controls overall security settings like enabling/disabling security, configuring authentication methods (LDAP, Jenkins' own database, etc.), and authorization strategies (e.g., Matrix-based security, Role-based security).

Credentials:

A centralized location to manage credentials like SSH keys, tokens, passwords, which can be used in jobs and pipelines.

3. System Maintenance

Manage Nodes and Clouds:

Allows you to manage Jenkins agents (nodes). You can configure, connect, or disconnect agent nodes and clouds for distributed builds.

Reload Configuration from Disk:

Reloads Jenkins configuration from disk, useful when making manual changes to configuration files.

Prepare for Shutdown:

Gracefully stops Jenkins from accepting new builds and waits for ongoing builds to finish before shutting down.

4. Monitoring and Logs

System Log:

Displays and manages Jenkins logs. You can add custom loggers for different components.

Load Statistics:

Shows system load statistics, such as the number of executors busy, build queue length, etc.

Monitor Jenkins:

Provides an overview of the Jenkins system's health and status, often with suggestions for improving performance.

5. Plugins Management

Manage Plugins:

This is where you can install, update, disable, or remove plugins. The plugin management interface has tabs for:

Updates: Displays available plugin updates.
Available: Shows plugins that can be installed.
Installed: Lists already installed plugins.
Advanced: Provides options to upload plugins manually or manage plugin repositories.

6. Tools and Actions

Script Console:

A powerful tool that allows administrators to run Groovy scripts to perform administrative tasks programmatically.

Manage Old Data:

Used to manage obsolete data that might be left behind by old or removed plugins.

System Information:

Displays detailed information about the Jenkins environment, such as JVM properties, environment variables, and system properties.

Jenkins CLI:

Provides details on how to use Jenkins Command Line Interface (CLI) to automate various tasks.

7. Backup and Restore

ThinBackup (if installed):

A plugin that provides options for backing up and restoring Jenkins configurations.

8. Miscellaneous

About Jenkins:

Displays the Jenkins version and information about the project.

New Item:

Shortcut to create a new Jenkins job or pipeline.

Manage Credentials:

Same as the Credentials option mentioned above, it provides a direct route to managing stored secrets.

9. Advanced Options

Reload from Disk:

Reloads the Jenkins configuration from the file system. This is useful if you manually edit the configuration files outside the Jenkins UI.

Restart Jenkins:

Provides an option to restart Jenkins from the UI.

Jenkins Notes from Scratch

https://media.licdn.com/dms/document/media/v2/D561FAQH2BicVz0RBrg/feedshare-document-pdf-analyzed/feedshare-document-pdf-analyzed/0/1731904562911?e=1736985600&v=beta&t=xOoI1hda7w5TyTQnZMJCuhADelpTP6AK7yw_iTSEAbw

SonarQube

SonarQube architecture

Set the some rule on java code.

Generate the sonarqube reports

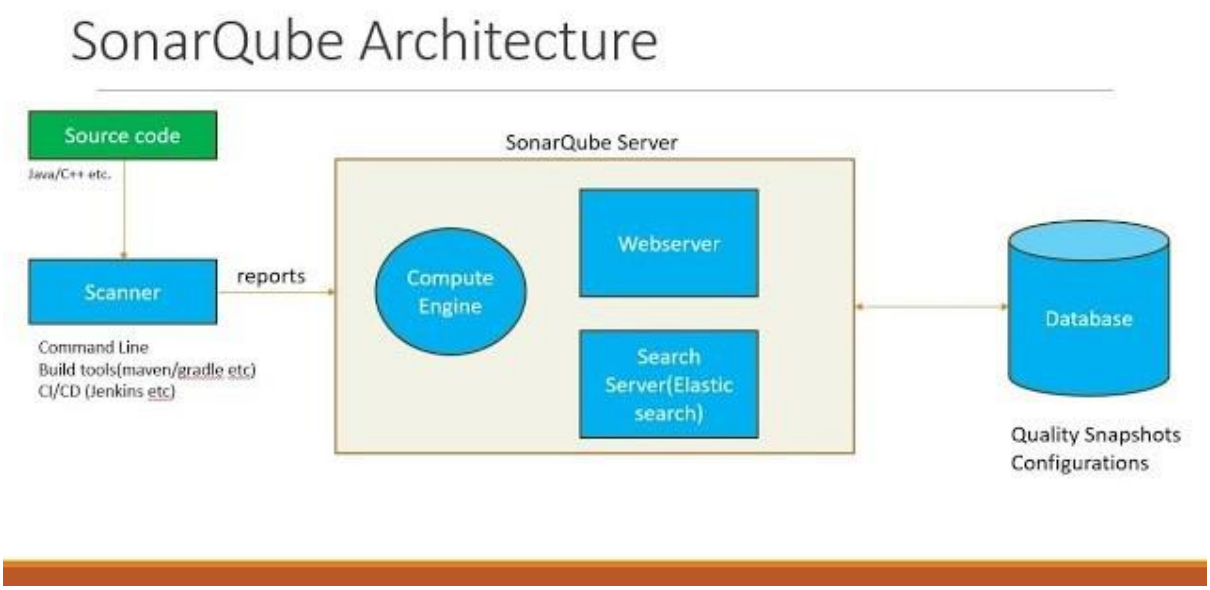
User sonar scanner plugin

SonarQube is a Code Quality Assurance tool that collects and analyzes source code, and provides reports for the code quality of project. It combines static and dynamic analysis tools and enables quality to be measured continually over time

Sonarqube architecture

Architecture

Concept	Definition
Analyzer	A client application that analyses the source code to compute snapshots.
Database	Stores configuration and snapshots
Server	Web interface that is used to browse snapshot data and make configuration changes



Code Quality
Sonarqube:
Advantages:
It acts as a quality management tool.

- Code analysis
- Test reports
- Code coverage, etc

Component of sonarqube

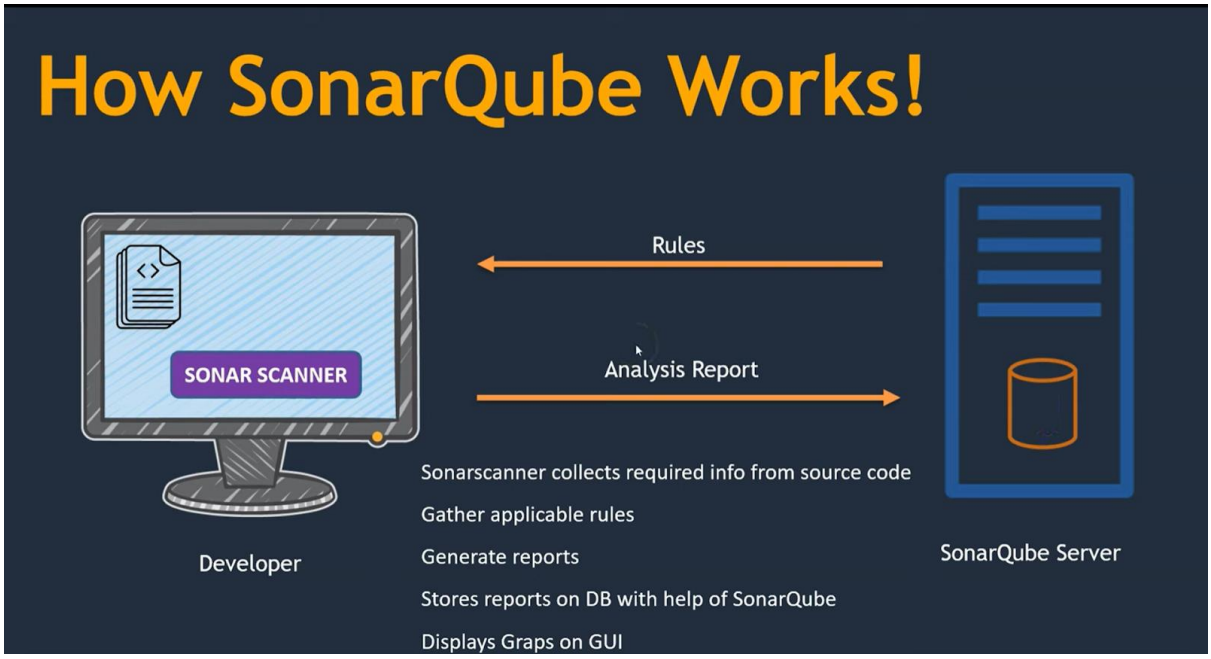
1. SonarQube server.
   - **Rules :** Rules are instructions need to follow while writing the code.
   - **Database :** Database will store the analysis reports.

- **Web Interface:** Once analysis reports are stored in the database through the web interface, then we can see and understand easily.
- **Elastic search:** it helps to search required data from sonarqube database.

2. SonarScanner:

- Source code.

Sonar Scanner is a service or agent which runs on the system where source code exists.
Once sonar scanner run the scan, it is going to gather the report and that will be published into the sonarqube server



- Sonarscanner collects required info from source code
- Gather applicable rules from sonarqube server
- Generate reports
- Stores reports on DB with help of SonarQube
- Displays Graphs on GUI

To create a quality gate in SonarQube

navigate to the "Quality Gates" section within your SonarQube instance, click "Create", give your quality gate a name, and then add conditions by selecting metrics, operators, and thresholds that define when the quality gate will pass or fail based on your desired code quality standard.

Key steps:

- **Access Quality Gates:** Go to the "Quality Gates" tab in your SonarQube dashboard.
- **Create a new Quality Gate:** Click "Create" to start building a new quality gate.
- **Name your Quality Gate:** Provide a descriptive name for your quality gate.
- **Add Conditions:**
    - Select a metric you want to evaluate (e.g., code coverage, complexity, number of issues).
    - Choose a comparison operator (e.g., greater than, less than, equals).

    - Set a threshold value.
- **Define Scope (optional):** Specify whether the conditions should apply to new code only or the entire codebase.

I understand now! You're looking for all the individual tool configurations and scripts that support a full production environment. You want to see the code for each of the different tools involved, such as **Dockerfile**, **Helm charts**, **Kubernetes configurations**, and so on, in a production environment. Let's take an example of a **Java-based application** with **Docker**, **Helm**, **Kubernetes**, and **GitOps** tools in the CI/CD pipeline.

---

1. Dockerfile (for Java-based application)
In the **CI pipeline**, we build a Docker image. Here's an example of a **Dockerfile** for a Java-based application:

```
# Use an official Java runtime as a parent image
FROM openjdk:11-jdk-slim

# Set the working directory in the container
WORKDIR /app

# Copy the local jar file into the container
COPY target/your-app.jar /app/your-app.jar

# Set the command to run the app
ENTRYPOINT ["java", "-jar", "your-app.jar"]

# Expose the port the app will run on
EXPOSE 8080
```

Explanation:

- **FROM openjdk:11-jdk-slim**: Pulls the OpenJDK 11 image as the base image.
- **COPY target/your-app.jar**: Copies the built application JAR file from the local target/ directory to the container.
- **ENTRYPOINT ["java", "-jar", "your-app.jar"]**: Specifies the command to run the application when the container starts.
- **EXPOSE 8080**: Exposes port 8080, which is typically used by web applications.

---

2. Helm Chart (for deploying application to Kubernetes)

For the **CD pipeline**, we deploy the application using Helm. Here's an example of a **Helm Chart** (with **values.yaml**, **deployment.yaml**, and **service.yaml**) that deploys the Java application to a Kubernetes cluster.

Helm Chart Structure:

```
your-app-helm/
├── charts/
├── templates/
│   ├── deployment.yaml
│   └── service.yaml
├── values.yaml
└── Chart.yaml
```

Chart.yaml:

```
apiVersion: v2
name: your-app
description: A Java-based application for Kubernetes
version: 0.1.0
appVersion: "1.0"
```

values.yaml (where we specify configurations such as the Docker image):

```
image:
  repository: your-docker-registry.com/your-app
  tag: latest  # This will be replaced by the pipeline with the correct image tag
  pullPolicy: Always

replicaCount: 3

service:
  type: ClusterIP
  port: 8080

resources: {}
```

deployment.yaml:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: {{ .Release.Name }}
  labels:
```

```
    app: {{ .Release.Name }}
spec:
  replicas: {{ .Values.replicaCount }}
  selector:
    matchLabels:
      app: {{ .Release.Name }}
  template:
    metadata:
      labels:
        app: {{ .Release.Name }}
    spec:
      containers:
        - name: {{ .Release.Name }}
          image: "{{ .Values.image.repository }}:{{ .Values.image.tag }}"
          ports:
            - containerPort: {{ .Values.service.port }}
          resources: {{ .Values.resources | toYaml | nindent 12 }}
```

service.yaml:

```
apiVersion: v1
kind: Service
metadata:
  name: {{ .Release.Name }}
spec:
  selector:
    app: {{ .Release.Name }}
  ports:
    - protocol: TCP
      port: {{ .Values.service.port }}
      targetPort: {{ .Values.service.port }}
  type: {{ .Values.service.type }}
```

Explanation:

- **values.yaml**: Contains the values to be used in the Helm templates (e.g., Docker image repository and tag).
- **deployment.yaml**: Defines the Kubernetes deployment, including the Docker image, replicas, and resource settings.
- **service.yaml**: Exposes the application as a Kubernetes service on port 8080.

---

3. Kubernetes Configuration (for setting up the cluster)

For deploying the app, the **Kubernetes configuration** includes a **kubeconfig** file (typically set up in Jenkins or other CI/CD tools to interact with the Kubernetes cluster). A typical **kubeconfig** looks like this:

kubeconfig.yaml:

```
apiVersion: v1
clusters:
```

```
- cluster:
    server: https://<K8S_API_SERVER>
    certificate-authority-data: <CA_CERTIFICATE>
  name: your-cluster
contexts:
- context:
    cluster: your-cluster
    user: your-user
  name: your-context
current-context: your-context
kind: Config
preferences: {}
users:
- name: your-user
  user:
    client-certificate-data: <CERTIFICATE_DATA>
    client-key-data: <CLIENT_KEY>
```

Explanation:

- **server**: The Kubernetes API server endpoint.
- **certificate-authority-data**, **client-certificate-data**, **client-key-data**: TLS certificates for secure communication with the Kubernetes cluster.

---

4. GitOps (for syncing the application state in Git)

To maintain the declarative state, the **GitOps pipeline** works by updating the Git repository that holds the Helm values. Here's an example of the **GitOps values.yaml** file and the necessary commands to update it.

GitOps values.yaml:

This file represents the source of truth for the cluster's application state, stored in a Git repository.

```
image:
  repository: your-docker-registry.com/your-app
  tag: latest  # This will be updated in the GitOps pipeline with the new image tag
```

GitOps Pipeline Example:

Here's the **Jenkins pipeline** script to update the GitOps repository:

```
pipeline {
    agent any
    environment {
        GIT_REPO = 'https://github.com/your-org/your-gitops-repo.git'
        GIT_BRANCH = 'main'
        IMAGE_TAG = "${env.BUILD_NUMBER}"  // This will be passed from the CI pipeline
        APP_NAME = 'your-app'
        DOCKER_REGISTRY = 'your-docker-registry.com'
        HELM_VALUES_FILE = 'path/to/values.yaml'  // GitOps values file
    }
    stages {
        stage('Checkout GitOps Repo') {
            steps {
```

```
            git branch: "${GIT_BRANCH}", url: "${GIT_REPO}"
        }
      }
      stage('Update Helm Values') {
        steps {
          script {
            sh """
            sed -i 's|image: .*|image: ${DOCKER_REGISTRY}/${APP_NAME}:${IMAGE_TAG}|'
${HELM_VALUES_FILE}
            """
          }
        }
      }
      stage('Commit and Push Changes') {
        steps {
          script {
            sh """
            git config user.email "ci-cd@example.com"
            git config user.name "Jenkins CI/CD"
            git add ${HELM_VALUES_FILE}
            git commit -m "Update image tag to ${IMAGE_TAG}"
            git push origin ${GIT_BRANCH}
            """
          }
        }
      }
    }
    post {
      success {
        echo 'GitOps repository updated successfully!'
      }
      failure {
        echo 'Failed to update GitOps repository.'
      }
    }
}
```

Explanation:

- **GitOps**: This pipeline checks out the GitOps repository, updates the Helm values file with the new image tag, commits, and pushes it back to the repository.
- **sed command**: Dynamically updates the Docker image tag in the Helm values file.

5. Jenkins Pipeline Configuration (for CI/CD)

For Jenkins, you would need to define **credentials** (such as Docker registry and Kubernetes credentials) and pipeline settings. Here's an example of how to configure the Jenkinsfile for CI/CD.

Jenkinsfile for CI/CD:

```
pipeline {
    agent any
```

```
    environment {
        DOCKER_REGISTRY = 'your-docker-registry.com'
        APP_NAME = 'your-app'
        IMAGE_TAG = "${env.BUILD_NUMBER}"
        KUBE_CONFIG = '/path/to/kubeconfig'
        HELM_RELEASE_NAME = 'your-app-release'
        HELM_CHART_PATH = './helm/your-app'
        NAMESPACE = 'production'
    }
    stages {
        stage('Checkout Code') {
            steps {
                git branch: 'main', url: 'https://github.com/your-org/your-repo.git'
            }
        }
        stage('Build Application') {
            steps {
                sh 'mvn clean package -DskipTests'
            }
        }
        stage('Build Docker Image') {
            steps {
                sh "docker build -t ${DOCKER_REGISTRY}/${APP_NAME}:${IMAGE_TAG} ."
            }
        }
        stage('Push Docker Image') {
            steps {
                withDockerRegistry([credentialsId: 'docker-credentials', url:
"https://${DOCKER_REGISTRY}"]) {
                    sh "docker push ${DOCKER_REGISTRY}/${APP_NAME}:${IMAGE_TAG}"
                }
            }
        }
        stage('Deploy with Helm') {
            steps {
                withEnv(["KUBECONFIG=${KUBE_CONFIG}"]) {
                    sh """
                    helm upgrade --install ${HELM_RELEASE_NAME} ${HELM_CHART_PATH} \
                    --namespace ${NAMESPACE} \
                    --set image

.repository=${DOCKER_REGISTRY}/${APP_NAME}
 --set image.tag=${IMAGE_TAG} """ } } } } }
```

Summary of Tools and Configurations:

- Dockerfile: For building a Docker image.

- Helm Chart: For deploying the application on Kubernetes.
- Kubernetes Config (kubeconfig): For accessing the Kubernetes cluster.
- GitOps: For declarative configuration management using Git repositories.
- Jenkins Pipeline: For orchestrating the CI/CD process, integrating Docker, Helm, and GitOps.

This is the full set of tools and configurations you would typically use in a production environment to automate the process of building, testing, and deploying an application with Docker, Helm, Kubernetes, and GitOps.

What are type of pod crashes in kubernates?

Kubenates
Errors:
CrashLoopBackOff:

In Kubernetes, pods can crash for various reasons, and understanding the types of crashes can help with troubleshooting. Here are some common types of pod crashes:

1. CrashLoopBackOff
- Description: This occurs when a pod fails to start, crashes, and then is restarted repeatedly within a short time frame.
- Symptoms: The pod's status is `CrashLoopBackOff`, meaning it keeps crashing and Kubernetes is trying to restart it.
- Common Causes: Application errors, misconfigurations, dependency failures.

2. Error
- Description: The container inside the pod exits with a non-zero exit code.
- Symptoms: The pod may show `Error` status in `kubectl get pods`.
- Common Causes: Runtime errors in the application, missing environment variables, or incorrect command-line arguments.

3. OOMKilled
- Description: This occurs when the pod is killed by the system because it exceeds its memory limits.
- Symptoms: The pod's exit reason will show `OOMKilled` in the events.
- Common Causes: Insufficient memory allocation, memory leaks in the application.

4. Completed
- Description: This status indicates that the pod has finished executing its tasks successfully but is no longer running.
- Symptoms: The pod will show as `Completed` in the status.
- Common Causes: Job or batch processing that completes its execution as intended.

5. Crash Due to Resource Limits
- Description: If the pod hits its CPU limits, it may be throttled, causing it to crash or become unresponsive.
- Symptoms: The application may perform poorly or crash under load.
- Common Causes: Underestimating resource requirements.

6. Application-Specific Crashes
- Description: Applications can crash for various reasons specific to their logic or runtime environment.
- Symptoms: Specific error messages or stack traces in logs.
- Common Causes: Bugs in the application code, exceptions that aren't handled properly.

7. Failed Scheduling
- Description: This occurs when a pod cannot be scheduled due to lack of resources or node availability.
- Symptoms: The pod status shows `Pending` with events indicating scheduling issues.
- Common Causes: Insufficient resources in the cluster, unsatisfied node selectors or taints.

8. Misconfiguration
- Description: Errors related to incorrect configurations such as invalid environment variables, secrets, or config maps.
- Symptoms: Pods may crash during startup.
- Common Causes: Typographical errors, missing configurations.

Summary

Understanding these crash types can help you diagnose issues effectively. Always start by checking the pod's status, logs, and events to determine the specific cause of the crash. If you need assistance with a particular case, feel free to share details!

https://cmakkaya.medium.com/argo-cd-1-understanding-installing-and-using-argo-cd-as-a-gitops-continuous-delivery-tool-0ec0b4e00a77

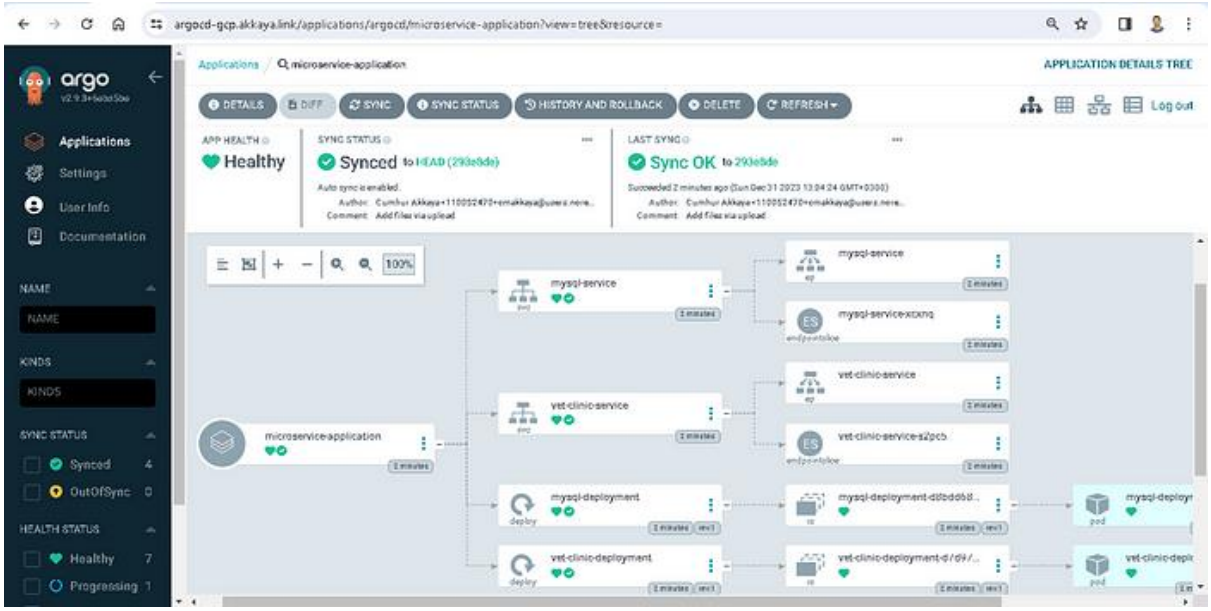
1. What is Argo CD

Argo CD is implemented as a Kubernetes controller which continuously monitors running applications and compares the current, live state against the desired target state

Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes.
With Argo CD, applications are automatically and continuously distributed to the target environments. It provides ease of deployment and management to multiple Kubernetes Clusters. User definitions and authorization procedures can be performed. SSO integration is possible. Rollback can be made to any commit in the Git repo. Kubernetes objects can be synchronized manually or automatically to the desired state specified in the Git repo. Also included is the Argo CD CLI for Continuous Integration automation.

ArgoCD functions as a Kubernetes controller that **continuously monitors a Git repository for changes to application configurations, and then automatically applies those changes to the live Kubernetes**

cluster, ensuring the cluster state always aligns with the desired state defined in the Git repository, essentially acting as a "**pull-based**" continuous delivery (CD) tool based on the **GitOps principle where Git is the single source of truth for application** deployments; meaning any updates to your application are made through Git commits, which ArgoCD then detects and automatically applies to the cluster, keeping it synchronized with the latest version in the Git repo.



How ArgoCD works in practice:

1. Developer commits changes:

A developer makes changes to their application configuration files (Kubernetes manifests) and commits them to the Git repository.

2. ArgoCD detects changes:

ArgoCD continuously monitors the Git repository and detects the new commit.

3. Comparison with live state:

ArgoCD compares the new configuration in Git with the current state of the application running on the Kubernetes cluster.

4. Apply changes if needed:

If differences are found, ArgoCD applies the necessary changes to the cluster to match the desired state defined in Git.

1. **Define**: Write Kubernetes manifests (or Helm/Kustomize configs) in Git.
2. **Review**: Submit a pull request for changes (new deployments or updates).
3. **Merge**: After review, merge the PR into the main branch.
4. **Sync**: GitOps controller (ArgoCD/Flux) detects the change and applies it to the cluster.
5. **Reconcile**: The controller continuously compares the cluster state with Git and auto-corrects any drift.

We can easily do these with argo CD;

- Application definitions, configurations, and environments; It is done in a declarative and version-controlled manner.

- Application deployment and lifecycle management; It is automated, auditable, and easily understandable.

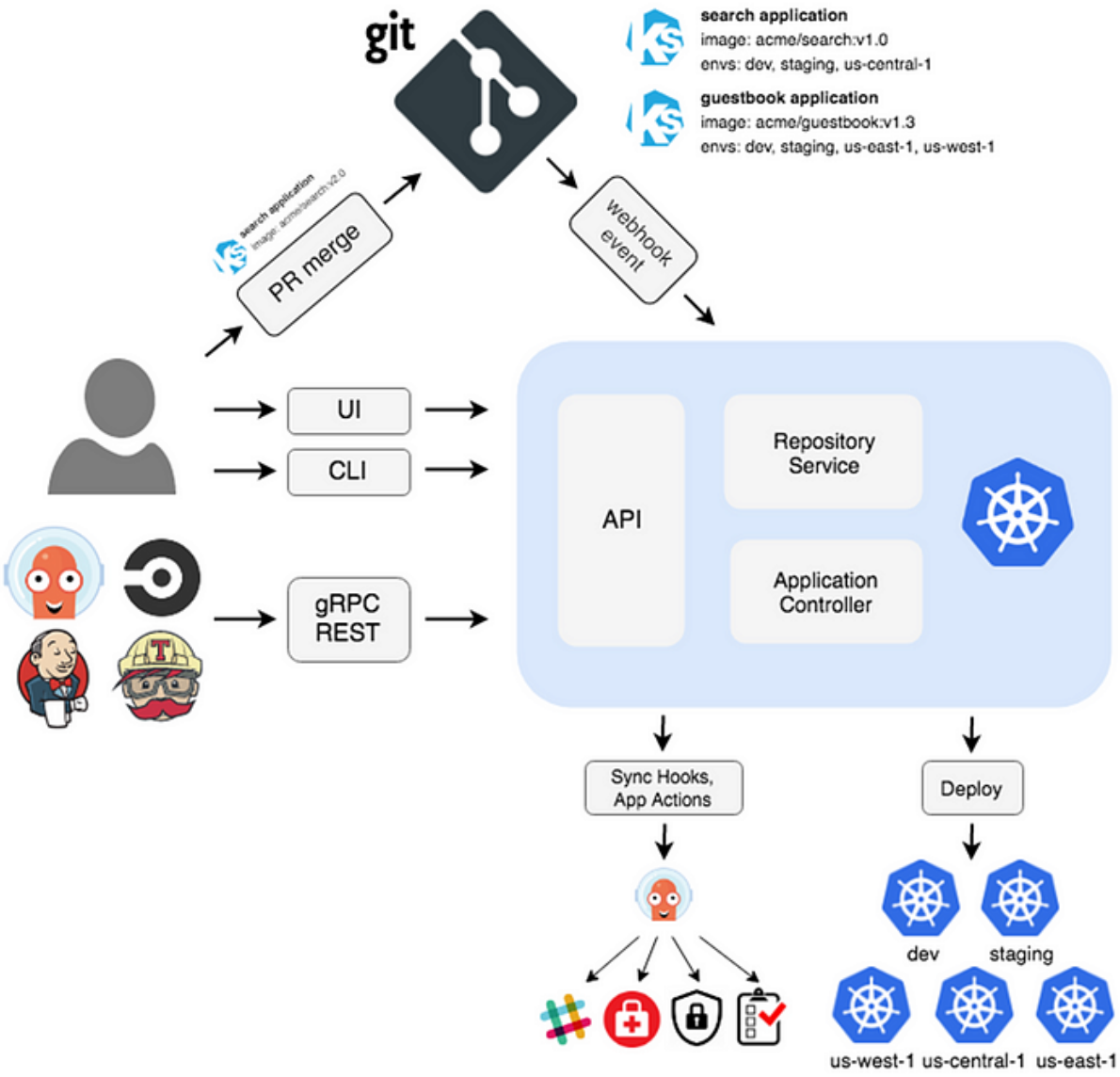
Argo CD is composed of three main components as seen in the picture below; (1)

- **API Server:** Exposes the API for the WebUI / CLI / CICD Systems
- **Repository Server:** Internal service that maintains a local cache of the git repository holding the application manifests
- **Application Controller:** Kubernetes controller which controls and monitors applications continuously and compares that current live state with the desired target state (specified in the repository). If a OutOfSync is detected, it will take corrective actions.

Architecture Diagram

To visualize the architecture:

1. Git Repository serves as the source of truth for application configurations.
2. API Server communicates with users via CLI/Web UI.
3. Repository Server processes manifests from the Git repository.
4. Controller performs reconciliation by applying changes to Kubernetes clusters.
5. Kubernetes Cluster contains the deployed resources, which are monitored by Argo CD.



Argo CD Architecture

The architecture of Argo CD is designed to manage Kubernetes resources declaratively. Below is a breakdown of its key components:

1. User Interface

- **Web UI:** A user-friendly dashboard for managing applications, clusters, and sync operations.
- CLI: Command-line interface for executing all actions programmatically.

2. Core Components

- **API Server:** Exposes REST API endpoints to interact with Argo CD.
- **Repository Server:** Fetches manifests from Git repositories and handles Helm chart rendering.

- Controller: Watches applications and syncs Kubernetes clusters with the desired state.

3. Data Stores
- Git Repository: Stores the desired state of the application in manifest files or Helm charts.
- Cluster State: Argo CD fetches the live state of resources from Kubernetes clusters.

4. Kubernetes Integration
- Custom Resource Definitions (CRDs): Argo CD uses CRDs such as `Application` and `ApplicationSet` to define application configurations.
- Namespaces: Applications are deployed into specified namespaces.

5. Sync Mechanism
- Declarative Sync: Ensures the live state matches the desired state defined in Git repositories.
- Automated Sync Policies: Automatically syncs resources and performs self-healing.

Argo CD Commands List

Here's a list of commonly used Argo CD CLI commands:

1. Login and Configuration
- Login to Argo CD server
```
argocd login <ARGOCD_SERVER> --username <USERNAME> --password <PASSWORD>
```

- Set default project or cluster context
```
argocd context --set <CONTEXT_NAME>
```

- List current contexts
```
argocd context
```

2. Application Management
- Create an application
```
argocd app create <APP_NAME> \
  --repo <REPO_URL> \
  --path <PATH_IN_REPO> \
  --dest-server <K8S_CLUSTER_URL> \
  --dest-namespace <NAMESPACE>
```

- List all applications
```
argocd app list
```

- Get details of an application
```
argocd app get <APP_NAME>
```

- Sync an application
```
argocd app sync <APP_NAME>
```

- Delete an application

argocd app delete <APP_NAME>

3. Application Operations
- Pause automated sync
argocd app pause <APP_NAME>

- Resume automated sync
argocd app resume <APP_NAME>

- Check the sync status
argocd app sync-status <APP_NAME>

- Force sync
argocd app sync <APP_NAME> --force

4. Cluster Management
- Add a Kubernetes cluster
argocd cluster add <K8S_CLUSTER_CONTEXT>

- List all clusters
argocd cluster list

- Remove a cluster
argocd cluster rm <K8S_CLUSTER_CONTEXT>

5. Projects Management
- Create a new project
bash
argocd proj create <PROJECT_NAME>

- List all projects
bash
argocd proj list

- Add a destination to a project
bash
argocd proj add-destination <PROJECT_NAME> <SERVER_URL> <NAMESPACE>

- Delete a project
bash
argocd proj delete <PROJECT_NAME>

6. Repository Management
- Add a Git repository
argocd repo add <REPO_URL> --username <USERNAME> --password <PASSWORD>

- List all repositories
argocd repo list

- Remove a repository
  argocd repo rm <REPO_URL>

Let me know if you'd like a detailed diagram or explanation for specific components!
Here’s a concise version of the notes with YAML code for quick reference:

1. Deploying with Kubernetes Manifest Files

YAML Example:
yaml
```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: nginx-manifests
  namespace: argocd
spec:
  project: default
  source:
    repoURL: https://github.com/your-repo/nginx-k8s-manifests
    targetRevision: HEAD
    path: manifests
  destination:
    server: https://kubernetes.default.svc
    namespace: nginx
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
```

2. Deploying with Helm Charts

a. From a Git Repository
YAML Example:
yaml
```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: nginx-helm
  namespace: argocd
spec:
  project: default
  source:
    repoURL: https://github.com/your-repo/nginx-helm-chart
```

```
    targetRevision: HEAD
    path: charts/nginx
    helm:
      parameters:
        - name: replicaCount
          value: "3"
        - name: service.type
          value: LoadBalancer
  destination:
    server: https://kubernetes.default.svc
    namespace: nginx
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
```

b. From a Helm Repository

YAML Example:

yaml

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: nginx-helm-repo
  namespace: argocd
spec:
  project: default
  source:
    repoURL: https://charts.bitnami.com/bitnami
    chart: nginx
    targetRevision: 13.2.8
    helm:
      parameters:
        - name: replicaCount
          value: "2"
        - name: service.type
          value: ClusterIP
  destination:
    server: https://kubernetes.default.svc
    namespace: nginx
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
```

3. Deploying Across Multiple Clusters

Add Target Cluster
bash
argocd cluster add <target-cluster-context>
argocd cluster list

Deploy Application to Target Cluster
YAML Example:
yaml
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: nginx-app
  namespace: argocd
spec:
  project: default
  source:
    repoURL: https://github.com/your-repo/nginx-app
    targetRevision: HEAD
    path: manifests
  destination:
    server: https://<target-cluster-server-url>
    namespace: nginx
  syncPolicy:
    automated:
      prune: true
      selfHeal: true

4. Blue-Green Deployment with Argo CD

ApplicationSet YAML Example:
yaml
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: nginx-bluegreen
spec:
  generators:
    - list:
        elements:
          - cluster: blue
            namespace: nginx-blue
            values:

```
          version: "1.21.6-blue"
        - cluster: green
          namespace: nginx-green
          values:
            version: "1.21.6-green"
  template:
    metadata:
      name: nginx-{{ cluster }}
    spec:
      project: default
      source:
        repoURL: https://github.com/your-repo/nginx-bluegreen
        targetRevision: HEAD
        path: manifests/{{ cluster }}
      destination:
        server: https://kubernetes.default.svc
        namespace: nginx-{{ namespace }}
      syncPolicy:
        automated:
          prune: true
          selfHeal: true
```

Switch Traffic

Modify the Kubernetes service selector to change traffic between blue and green environments:

yaml

```
apiVersion: v1
kind: Service
metadata:
  name: nginx-service
  namespace: default
spec:
  selector:
    app: nginx-blue # Change to nginx-green after verification
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  type: LoadBalancer
```

5. Sync and Verify Deployments

- Sync Application:

  bash

  ```
  argocd app sync nginx-app
  ```

- Verify Resources:
  bash
  kubectl get all -n <namespace>

Let me know if you'd like further clarifications!

GitOps

https://www.linkedin.com/comm/pulse/gitops-demystified-why-your-kubernetes-should-follow-git-agnihotri-ld4xc?lipi=urn%3Ali%3Apage%3Aemail_email_series_follow_newsletter_01%3BOcdQzJxaRR2c3Lifb8MapA%3D%3D&midToken=AQEToR-trJbPgQ&midSig=2sJryMsxGn6rM1&trk=eml-email_series_follow_newsletter_01-newsletter_content_preview-0-readmore_button_&trkEmail=eml-email_series_follow_newsletter_01-newsletter_content_preview-0-readmore_button_-null-kr7ymj~ma85cb5y~u3-null-null&eid=kr7ymj-ma85cb5y-u3&otpToken=MTMwNzFiZTUxMjJhY2RjMmI1MjcwZmViNDExYWUxYjY4OGNjZDE0MjkwYWU4ZTZjN2JjZjA2NmM0NzViNThmMGYwZDdkMGU5NmVlOGU2Yzk0ZWZkZGJjMzA5Yzg4ZWIxMzM0NWM3Mzk0Y2FhNWNmOWFiOTA4ZDBlLDEsMQ%3D%3D

1. GitOps Fundamentals

- **Definition**: GitOps is a methodology where Git is the **single source of truth** for infrastructure and application deployments.
- **Principles**:
  - Declarative configuration (YAML/Helm/Kustomize).
  - Git as the central repository for desired state.
  - Automated synchronization (ArgoCD reconciles Git with the cluster).
  - Immutable infrastructure (changes only via Git commits).

---

2. ArgoCD Core Concepts

- **What is ArgoCD?**: A declarative, GitOps-based **Kubernetes** continuous delivery (CD) tool.
- **Key Features**:
  - Syncs Kubernetes manifests from Git to clusters.
  - Supports **multi-environment** deployments (dev/staging/prod).
  - Provides a **web UI** and CLI for monitoring.
  - **Automated or manual sync** strategies.
  - **Health checks** (e.g., pod status, readiness probes).
  - **Rollback** to previous Git revisions.

---

3. How ArgoCD Works

- **Components**:
  - **Application CRD**: Defines source (Git repo, branch, path) and destination (Kubernetes cluster/namespace).

    - **ArgoCD Server**: Manages sync operations and UI.
    - **Repo Server**: Fetches manifests from Git.
    - **Controller**: Compares Git state with cluster state.
- **Sync Process**:
    - Polls Git for changes (or uses webhooks).
    - Detects drift (differences between Git and cluster).
    - Applies changes (if auto-sync is enabled).

---

4. Key Interview Topics

A. Setup & Configuration

- Installing ArgoCD (Helm, kubectl).
- Configuring **RBAC** (role-based access control).
- Connecting Git repos (SSH, HTTPS, private repos).

B. Application Deployment

- Creating an **Application** YAML:

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: my-app
spec:
  project: default
  source:
    repoURL: https://github.com/user/repo
    targetRevision: main
    path: manifests/
  destination:
    server: https://kubernetes.default.svc
    namespace: my-namespace
  syncPolicy:
    automated: {}
```

C. Sync Strategies

- **Automated vs. Manual Sync**:
    - Automated: ArgoCD applies changes immediately.
    - Manual: Requires user approval (safer for production).
- **Sync Waves**: Order of resource deployment (e.g., databases before apps).

D. Advanced Features

- **Helm/Kustomize Support**: How ArgoCD handles Helm charts or Kustomize overlays.
- **Secrets Management**: Integration with **Sealed Secrets**, **Vault**, or **SOPS**.
- **Multi-Cluster Deployments**: Managing apps across clusters.
- **Metrics & Alerts**: Prometheus integration for monitoring.

E. Troubleshooting

- **Common Issues**:
    - Sync failures (e.g., permissions, network issues).
    - Drift detection (cluster state differs from Git).
    - Resource health (stuck deployments).

- **Debugging Tools**:
    - argocd app get <app-name> (status check).
    - argocd app sync <app-name> (force sync).
    - Logs (kubectl logs -n argocd <argocd-server-pod>).

---

5. Comparison to Other Tools

- **ArgoCD vs. Flux**: Both are GitOps tools, but ArgoCD has a UI and stronger multi-cluster support.
- **ArgoCD vs. Jenkins**: Jenkins is CI/CD (imperative), while ArgoCD is GitOps (declarative).

---

6. Sample Interview Questions

1. **"How does ArgoCD ensure cluster state matches Git?"**
   → It continuously polls Git and reconciles differences (like a control loop).
2. **"How would you handle secrets in a GitOps workflow?"**
   → Use **Sealed Secrets** (encrypt secrets in Git) or **Vault** (external secrets).
3. **"What happens if someone manually edits a resource in the cluster?"**
   → ArgoCD will detect the drift and revert it (if auto-sync is enabled).
4. **"How do you rollback a deployment in ArgoCD?"**
   → Revert the Git commit or use argocd app set --history-id <commit-hash>.
5. **"How does ArgoCD manage dependencies between resources?"**
   → Sync waves (argocd.argoproj.io/sync-wave annotation) or Helm hooks.

---

1. What is GitOps?

GitOps is a modern approach to continuous deployment and infrastructure automation that uses **Git as the single source of truth**. It allows developers to manage infrastructure and application configurations in the same way they manage code: through pull requests and version control.

- **Definition**: GitOps is a methodology where Git is the **single source of truth** for infrastructure and application deployments.
- It automates deployments by synchronizing the actual state of the system (e.g., Kubernetes clusters) with the desired state defined in Git repositories.

---

2. The Core Principles Behind GitOps

GitOps is founded on four key principles:

1. **Declarative Descriptions**: The system's desired state is described declaratively (e.g., YAML files).
2. **Versioned and Immutable Storage**: Desired states are stored in Git, ensuring traceability and auditability.
3. **Automated Delivery**: Automated systems (like ArgoCD or Flux) sync the desired state from Git to the environment.
4. **Continuous Reconciliation**: A controller continuously monitors the system to ensure it matches the Git state.

---

3. How GitOps Works (With Real-Life Analogy)

Analogy: Think of GitOps like a **recipe book (Git)** for a restaurant kitchen (**production environment**).

- The head chef (**GitOps controller**) reads the recipes and ensures each dish (deployment) matches exactly what's written.
- If a cook adds a different ingredient (manual change), the head chef spots it and corrects the dish.
- All recipe updates go through a review process (pull requests), ensuring everyone agrees before cooking changes.

---

4. GitOps Workflow in Kubernetes

6. **Define**: Write Kubernetes manifests (or Helm/Kustomize configs) in Git.
7. **Review**: Submit a pull request for changes (new deployments or updates).
8. **Merge**: After review, merge the PR into the main branch.
9. **Sync**: GitOps controller (ArgoCD/Flux) detects the change and applies it to the cluster.
10. **Reconcile**: The controller continuously compares the cluster state with Git and auto-corrects any drift.

---

5. GitOps vs Traditional CI/CD

Feature	**GitOps**	**Traditional CI/CD**
Source of Truth	Git repository	CI/CD tool state
Deployment Trigger	Git change	CI/CD pipeline execution
Rollback	Git revert (versioned state)	Manual or scripted rollback
Drift Detection	Continuous monitoring	Limited or none
Security	Git-based audit, access control	Tool-based, often fragmented

---

1. **What is GitOps?**

GitOps is a modern approach to infrastructure and application management that uses **Git as the single source of truth** for declarative infrastructure and applications. It automates deployments by synchronizing the actual state of the system (e.g., Kubernetes clusters) with the desired state defined in Git repositories.

- **Key Idea**: "If it’s not in Git, it doesn’t exist."
- **Origin**: Coined by Weaveworks in 2017, built around DevOps best practices.

---

2. **The Core Principles Behind GitOps**

Four pillars define GitOps:

1. **Declarative Configuration**: The entire system state (apps, infra, policies) is declared in Git (e.g., YAML/Helm charts).
2. **Version Control**: Git tracks all changes, enabling audit trails, rollbacks, and collaboration.

3. **Automated Delivery**: A GitOps operator (e.g., ArgoCD) auto-reconciles the live state with Git.
4. **Closed-Loop Feedback**: Observability tools alert on drift between Git and runtime.

---

3. **How GitOps Works (With Real-Life Analogy)**

Analogy: Think of GitOps like a **self-driving car**.

- **Git Repository**: The GPS route (desired destination).
- **GitOps Operator**: The car's autopilot (continuously compares actual position to the route).
- **Kubernetes Cluster**: The car itself (adjusts speed/direction to match the route).

Process:

1. A developer commits a change to Git (e.g., new app version).
2. The GitOps tool detects the change and deploys it to Kubernetes.
3. If the cluster drifts (e.g., manual change), the tool reverts it to match Git.

---

4. **GitOps Workflow in Kubernetes**

1. **Developers** push code/app manifests to Git.
2. **CI Pipeline** builds artifacts (container images) but **does not deploy**.
3. **GitOps Operator** (e.g., ArgoCD) monitors Git and:
    - Pulls changes (no push-based access to clusters).
    - Applies updates using Kubernetes controllers.
4. **Monitoring** tools (Prometheus) alert on deviations.

Example:

yaml
Copy
Download

```
# Git repo (desired state)
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx
spec:
  replicas: 3  # ArgoCD ensures exactly 3 pods run.
```

---

5. **GitOps vs Traditional CI/CD**

Aspect	GitOps	Traditional CI/CD
Source of Truth	Git repository	CI server (Jenkins, CircleCI)
Deployment	Pull-based (operator-driven)	Push-based (CI-triggered)
Security	Minimal cluster access (read-only)	Requires cluster write permissions
Rollbacks	Git revert (atomic)	Manual/intervention-heavy

---

6. **Key Benefits of GitOps**

- **Auditability**: Full change history in Git.
- **Consistency**: No "snowflake environments."
- **Security**: No direct cluster access needed.
- **Disaster Recovery**: Rebuild clusters from Git.
- **Collaboration**: Developers use familiar Git workflows.

✅ Core Concepts of GitOps

Understand what GitOps is:

- **GitOps = Git + Ops**: A model where Git is the single source of truth for declarative infrastructure and application definitions.
- **Declarative infrastructure**: All infrastructure and app state is defined in Git (YAML, Helm, Kustomize).
- **Automation**: Changes are made by committing to Git; tools like Argo CD automatically sync Git state to the cluster.
- **Reconciliation loop**: GitOps tools continuously monitor and reconcile the cluster to match the Git state.

Key Benefits:

- Version control
- Auditability
- Rollbacks via Git history
- Continuous delivery without scripts

🔧 Argo CD Essentials

1. What is Argo CD?

- A declarative, GitOps continuous delivery tool for Kubernetes.
- Syncs Git repositories to Kubernetes clusters automatically or manually.

---

2. How Argo CD Works

- **Git repository** (source of truth) contains YAML/Helm/Kustomize manifests.
- **Argo CD application** defines:
  - repo URL
  - target revision (branch/tag)
  - destination cluster and namespace
  - path in the repo where manifests reside
- Argo CD monitors the repo and syncs the state to the cluster.

---

3. Key Argo CD Concepts

- **Application**: Core object that links Git repo to the cluster.
- **Sync status**:
  - *Synced*: Cluster state matches Git
  - *OutOfSync*: Cluster state differs from Git
- **Health status**:
  - *Healthy*, *Degraded*, etc., depending on app readiness.
- **Sync strategies**:
  - Manual sync

    - Auto-sync (optional pruning and self-healing)
- **Hooks**: PreSync, Sync, PostSync hooks (like Helm lifecycle events)
- **RBAC**: Role-based access control for team management

---

4. Configuration Tools Support
Argo CD supports:

- **Plain YAML**
- **Helm**
- **Kustomize**
- **Jsonnet**

You should know how Argo CD integrates with these.

---

5. Important CLI/Commands
You might be asked to demonstrate:

- argocd login
- argocd app create
- argocd app get <app-name>
- argocd app sync <app-name>
- argocd app delete <app-name>

🎯 **Interview Prep Tips**
1. Know how to:

- Deploy a basic app using Argo CD
- Explain what happens when you update the Git repo
- Describe how Argo CD reacts to drift (cluster != Git)

2. Be ready to answer:

- Difference between GitOps and traditional CI/CD
- How Argo CD differs from FluxCD or Jenkins X
- Pros and cons of using Argo CD

3. Bonus topics:

- Integrating Argo CD with CI tools (e.g., GitHub Actions triggers Git commit)
- Handling secrets (e.g., using **Sealed Secrets**, **SOPS**, **External Secrets**)
- Multi-cluster deployments using Argo CD

Useful References:

- **Official GitOps Website**
- **Argo CD Documentation by**
- **Flux Documentation**
- **GitOps Working Group (CNCF)**

Linux

what is difference between root user and sudo user in linux?

The **root user** has full, unrestricted access to the system, while a **sudo user** is a regular user granted temporary root privileges to execute certain administrative tasks.
Using sudo is generally safer and more manageable than working directly as the root user.

Users & Groups.

User:
Some Important Points related to Users:

- Users and groups are used to control access to files and resources
- Users login to the system by supplying their username and password
- Every file on the system is owned by a user and associated with a group
- Every process has an owner and group affiliation, and can only access the resources its owner or group can access.
- Every user of the system is assigned a unique user ID number (the UID) Users name and UID are stored in /etc/passwd /etc/pa
- User's password is stored in /etc/shadow in encrypted form.
- Users are assigned a home directory and a program that is run when they login (Usually a shell)
- Users cannot read, write or execute each other's files without permission.

Whenever a user is created in Linux things created by default:

- A home directory is created(/home/username)
- A mail box is created(/var/spool/mail)
- unique UID & GID are given to user

Passwd file
/etc/passwd

Group file
The file /etc/group stores group information. Each line in this file stores one group entry.

1. **/etc/group**

ADD USER, SET PASSWORD & SWITCH TO USER

2. **Id user/group**

ADD USER, GROUP & USER INTO GROUP

3. **The /etc/shadow file**

This file stores users' password and password related information. Just like /etc/passwd file, this file also uses an individual line for each entry.
1. Username
2. Encrypted password
3. Number of days when password was last changed
4. Number of days before password can be changed
5. Number of days after password must be changed

6. Number of days before password expiry date to display the warning message
7. Number of days to disable the account after the password expiry
8. Number of days since the account is disabled
9. Reserved field

File permissions

Viewing Permissions from the Command-Line
File permissions may be viewed using **Is -l**
$ ls -1/bin/login
-rwxr-xr-x 1 root root 19080 Apr 1 18:26 /bin/login
Four symbols are used when displaying permissions:
• **r:** permission to read a file or list a directory's contents
• **w:** permission to write to a file or create and remove files from a directory
• **x:** permission to execute a program or change into a directory and do a long listing of the directory
• **-:** no permission (in place of the r, w, or x)

Changing File Ownership
• Only root can change a file's owner
• Only root or the owner can change a file's group
• Ownership is changed with **chown:**
  • **chown [-R] user_name file directory ...**
Examples:
  • **chown username:groupname file.txt**
  • **chown -R username:groupname /path/to/directory**

• Group-Ownership is changed with **chgrp:**
  • **chgrp [-R] group_name file directory**
Examples:
  • **chgrp admins /path/to/directory**
  • **chgrp -R developers /path/to/directory**

Changing Permissions - Symbolic Method
To change access modes:
  • **chmod [-OPTION]... mode[, mode]** filel directory ...
mode includes:
  • **u, g** or **o** for user, group and other
  • **+ -** or for grant, deny or set
  • **or, wor x** for read, write and execute
Options include:
  • **-R** Recursive
• **-v** Verbose
• **--reference** Reference another file for its mode
Examples:
• **chmod ugo+r file**: Grant read access to all for file
• **chmod o-wx dir**: Deny write and execute to others for dir

Changing Permissions - Numeric Method
Uses a three-digit mode number
- first digit specifies owner's permissions
- second digit specifies group permissions
- third digit represents others' permissions

Permissions are calculated by adding:
- 4 (for read)
- 2 (for write)
- 1 (for execute)

Example:
- chmod 640 myfile

Change owner
chown sam.sam devopstools
chown sam.sam vpdir/ -R

Interview

https://chatgpt.com/share/6745db0c-8660-8002-a8fb-d2ae956853af

Linux
https://linuxjourney.com
What is awk command in Linux
The awk command's main purpose is to make information retrieval and text manipulation easy to perform in Linux. This Linux command works by scanning a set of input lines in order and searches for lines matching the patterns specified by the user.
 # awk 'pattern { action }' input-file

Shell Scripting Tutorial Beginners To Advanced
https://safiakhatoon.hashnode.dev/shell-scripting-tutorial-beginners-to-advanced

https://learnshell.org/

Sonarqube dashboard compenents, like vern
Helm chat creation, templates, values default, custom values, commands, history, roll back,
Secreats,

Argocd Application sets

Helm Chart

Helm Chart
Helm is the **package manager for Kubernetes cluster**, and Helm Charts are its packaging format.
We can install, upgrade, and delete helm chart
It simplifies the deployment and management of applications on Kubernetes by using Helm charts, which are pre-configured templates for Kubernetes resources.

1. What is a Helm Chart?
A Helm Chart is a **collection of YAML files** organized in a specific directory structure that defines:

- Kubernetes manifests (Deployments, Services, etc.)
- Configurable parameters (via values.yaml)
- Dependencies on other charts
- Versioning and metadata

Analogy: If Docker containers package single applications, Helm Charts package entire Kubernetes applications (often multiple containers working together).

2. Helm Chart Structure
A typical chart directory looks like this:

3. Helm structure

- Char.yaml
- Templates
- Values.yaml

```
mychart/                # Chart name
 ├── Chart.yaml         # Contains metadata about the chart (name, version, dependencies)
 ├── values.yaml        # Default configuration values that users can override
 ├── charts/            #  Subcharts/dependencies - Stores dependencies that your chart requires.
 ├── templates/         # Kubernetes manifests templates (Go templating for dynamic values)
|    ├── deployment.yaml
|    ├── service.yaml
|    ├── ingress.yaml
|    └── _helpers.tpl      # Helper templates
 ├── templates/NOTES.txt  # OPTIONAL - Post-install notes
 ├── .helmignore        # Lists files to exclude when packaging the chart (similar to .gitignore).
└── README.md           # Documentation explaining:
```

3. Key Components
A. Chart.yaml
Contains metadata about the chart:
apiVersion: v2
name: myapp
description: A Helm chart for MyApp

```
version: 1.0.0
dependencies:
  - name: postgresql
    version: "~12.0"
    repository: "https://charts.bitnami.com/bitnami"
```

B. values.yaml
Default configuration that users can override:

```
replicaCount: 3
image:
  repository: nginx
  tag: "1.23"
service:
  type: ClusterIP
  port: 80
```

helm install <release-name> <chart-path> -f custom.values.yaml

C. templates/
Kubernetes manifests with **Go templating** for dynamic values:

```
# templates/deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: {{ .Release.Name }}-myapp
spec:
  replicas: {{ .Values.replicaCount }}
  template:
    spec:
      containers:
      - name: myapp
        image: "{{ .Values.image.repository }}:{{ .Values.image.tag }}"
```

4. How Helm Works

1. **User runs**:

```
helm install myapp ./mychart --values=myvalues.yaml
```

2. **Helm**:
    - Combines templates/ + values.yaml + user overrides
    - Provide final Kubernetes manifests
    - Deploys them to your cluster

5. Why Use Helm Charts?

Benefit	Explanation
Reusability	Deploy the same app across environments (dev/stage/prod) with different values.

Benefit	Explanation
Versioning	Track versions of your Kubernetes applications (like Docker image tags).
Dependency Management	Bundle databases, caches, or other services your app needs.
Rollbacks	helm rollback myapp 1 reverts to version 1.

Common Helm Commands

Command	Description
helm install myapp ./mychart	Deploys a chart
helm upgrade myapp ./mychart	Updates a release
helm uninstall myapp	Removes a release
helm list	Shows installed charts
helm repo add bitnami https://charts.bitnami.com/bitnami	Adds a chart repository
helm dependency update	Updates sub-charts

Real-World Example: Deploying WordPress

```
# Add the Bitnami repo
helm repo add bitnami https://charts.bitnami.com/bitnami

# Install WordPress with Helm
helm install my-wordpress bitnami/wordpress \
  --set mariadb.primary.persistence.enabled=true \
  --set service.type=LoadBalancer
```

This single command deploys:

- WordPress (PHP) container
- MariaDB database
- Persistent volumes
- LoadBalancer service

Prometheus and Grafana

Prometheus and Grafana are open-source tools that work together to monitor and visualize applications and systems. Prometheus collects metrics, while Grafana displays them.

Prometheus

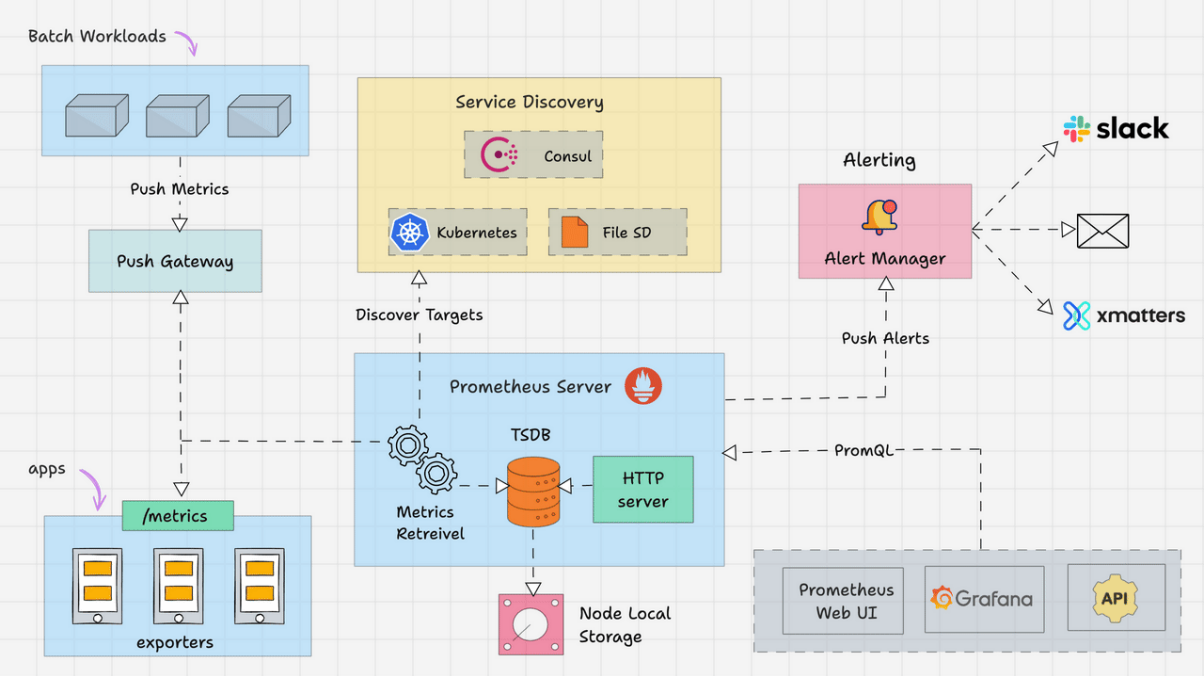
- **Collects and stores metrics in a time-series data** and runs queries
- Includes a querying language
- Supports exporters for monitoring services like MySQL, Kubernetes, and Kafka
- Offers alerting

Grafana
It is a very powerful **visualisation tool** which can used for all sorts of dashboard and monitoring requirements.

- Transforms metrics into visualizations
- Works with multiple data sources, including Prometheus
- Allows users to create dashboards

Prometheus

Prometheus is a time series database. Prometheus is designed to monitor targets. Servers, databases, standalone virtual machines, pretty much everything can be monitored with Prometheus. It will collect the CPU, Disk and network utilization logs of pods/deployments/replicas. It will send these logs to Grafana.
Prometheus Architecture



Components

- **Prometheus Server**: The core component that collects metrics, stores them in a time series database (TSDB), and runs queries
- **Exporters**: Tools that expose metrics from third-party systems so Prometheus can collect them.

- **Alert manager**: Manages alerts by deduplicating, grouping, and routing them to notification channels
- **Pushgateway**: Allows ephemeral (short-lived) jobs to send metrics to Prometheus
- **Service Discovery**: Automatically discovers targets to collect metrics from.
- **Client Libraries**: "Allow application developers to expose custom metrics for Prometheus to collect.

How Prometheus works
Prometheus uses a pull-based approach to collect data from predefined HTTP endpoints. It applies rules to the data to create new time series or alert users.

Grafana:

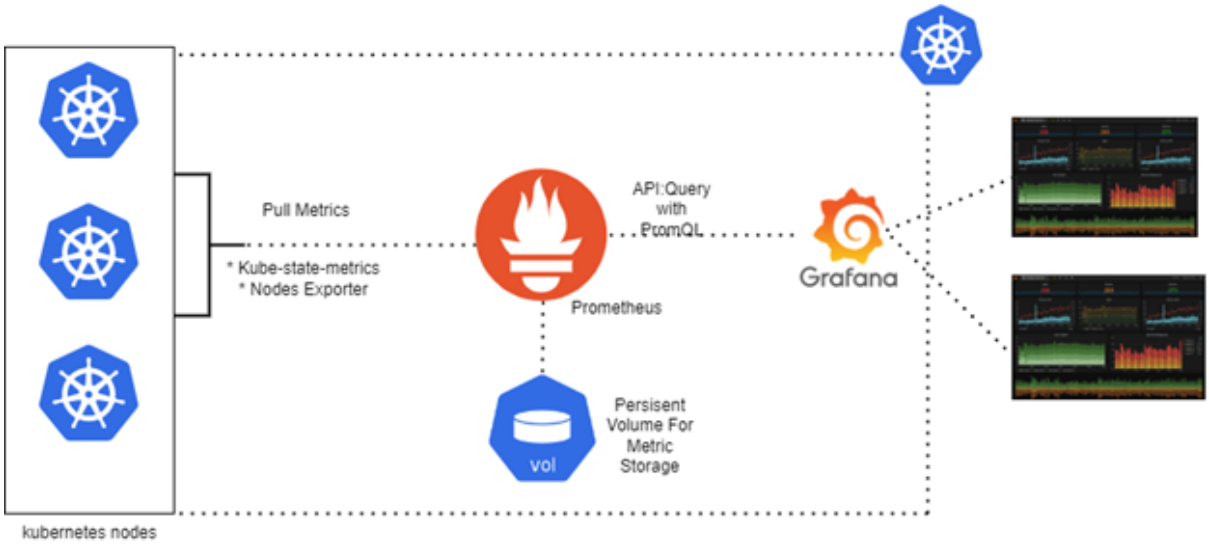
Grafana is a web-based application that uses a microservices-based architecture to **monitor and visualize data in DevOps.** It's designed to help teams understand their systems and applications, and to troubleshoot issues.

What is Grafana?
Grafana is a multi-platform open-source analytics and interactive visualization web application. **It provides charts, graphs, and alerts when connected to supported data sources.** It is expandable through a plug-in system. End users can create complex monitoring dashboards using interactive query builders.

It provides: ✓ Charts ✓ Graphs ✓ Alerts

Grafana Features: Visualize Grafana has a plethora of visualization options to help you understand your data, beautifully Alert Seamlessly define alerts where it makes sense | while you're in the data Unify Grafana supports dozens of databases, natively. Mix them together in the same Dashboard Open Source Grafana's completely open source, and backed by a vibrant community
Extend Discover hundreds of dashboards and plugins in the official library Collaborate Bring everyone together, and share data and dashboards across teams
Create the dashboards in Grafana
Alerting
How it works

- Grafana alerting periodically queries data sources and evaluates the condition defined in the alert rule
- If the condition is breached, an alert instance fires
- Firing instances are routed to notification policies based on matching labels
- Notifications are sent out to the contact points specified in the notification policy



Components

- **Grafana Mimir**: A microservices-based architecture that can run components in parallel
- **Backend**: Interacts with various data sources, such as Prometheus and Loki
- **Frontend**: Renders visualizations for users, such as charts and graphs

Features

- **Central monitoring**: Consolidates data from multiple sources into dashboards
- **Alerting**: Sends out alerts when metrics hit certain thresholds
- **Collaboration**: Sharing dashboards and data views enhances team communication
- **Integration**: Works with a range of DevOps tools

Use cases

- **Monitoring application performance**: Tracks key performance indicators (KPIs) and sets up alerts
- **Monitoring server performance**: Provides insights into CPU usage, memory consumption, and more
- **Monitoring application logs**: Consolidates and visualizes logs to identify issues
- **Request tracing**: Visualizes the end-to-end flow of requests through multiple services
- **Error tracking**: Correlates logs and metrics to identify and diagnose errors

Seamens Interview

Intro
Ansible configuration- why required as your are creating the infrastructure in Kubernetes (application deployed in K8S).
ArgoCD: Process how it works
K8s architecture and components
AWS resources - 20
Terraform code - vpc and eks code components (code)
Kubernates: Difference between statefull set and deployment.

How volumes will attach to