# **Containers**

## **Introduction to Containers?**

Containers are lightweight, standalone software packages that include everything needed to run an application—code, runtime, libraries, and dependencies—so that it functions consistently across different environments. They allow developers to package applications in a way that ensures they run the same whether on a local machine, a test server, or in production.

Containers are a foundational technology in modern computing that allow applications to be packaged along with their dependencies into lightweight, portable units. They help ensure that an application runs consistently in different environments—whether on a developer’s laptop, a test server, or in a production cloud environment.

Containers provide an isolated runtime environment where applications can execute without interference from the underlying system or other applications. Unlike traditional virtual machines (VMs), containers share the host operating system kernel but maintain their own libraries and dependencies, making them more efficient and lightweight.

Containers have gained popularity due to their ability to:

* Provide **portability** across different environments.
* Improve **efficiency** by using fewer system resources compared to VMs.
* Support **scalability**, making it easier to deploy and manage applications.
* Enhance **security** through process isolation.

### **Types of Containers**

There are several types of containers, each serving different purposes:

1. **Application Containers** – These hold and run individual applications with their dependencies, such as Docker containers.
2. **System Containers** – More like lightweight virtual machines, they provide full OS functionality and isolation.
3. **Process Containers** – Designed to run single processes in isolation, often used for security and resource management.
4. **Hybrid Containers** – A mix of application and system containers, balancing flexibility and isolation.

### **Comparison of Containers**

Containers differ from traditional VMs in several ways:

|  |  |  |
| --- | --- | --- |
| **Feature** | **Containers** | **Virtual Machines (VMs)** |
| Resource Usage | Lightweight, shares host OS | Heavy, requires full OS instance |
| Startup time | Quick, starts in seconds | Slow, takes minutes to boot |
| Portability | Highly portable | Less portable due to dependencies |
| Security | Isolated, but shares host kernel | Full isolation with separate OS |
| Scalability | Easy to scale and deploy | More complex scaling process |

### **Pros and Cons**

#### Pros:

**Efficiency:** Containers use fewer resources that VMs

**Portability:** They can run consistently across different environments

**Scalability:** Ideal for cloud deployments and microservices architectures.

**Isolation:** Reduce conflicts between applications.

#### Cons:

**Security Risks:** Since containers share the host kernel, security vulnerabilities can arise.

**Complex Management:** Requires orchestration tools like Kubernetes for large-scale deployments.

**Limited OS Support:** Some applications need full OS features that containers don’t provide.

## **Overview of Container Architecture**

Container architecture is a design approach that enables applications to run in isolation environments, ensuring consistency across different computing environments. It is widely used in cloud computing, microservices and DevOps practices.

Containers encapsulate an application and its dependencies into a single package, allowing it to run consistently across various environments. Unlike traditional virtual machines (VMs), containers share the host operating system kernel but maintain their own libraries and dependencies, making them lightweight and efficient.

### **Key Components of Container Architecture**

1. **Container Runtime:** The software responsible for running containers such as Docker or containerd.
2. **Container Images:** Pre-packaged applications with all necessary dependencies, stored in repositories like Docker Hub.
3. **Orchestration Tools:** Platforms like Kubernetes manage container deployment, scaling, and networking.
4. **Networking:** Containers communicate through virtual networks, ensuring secure and efficient data exchange.
5. **Storage:** Persistent storage solutions allow containers to retain data across restarts.

## **Container Orchestration**

Container Orchestration is the process of automating the deployment management, scaling, and networking of containers. It ensures that applications run efficiently across different environments without manual intervention.

### **Basic Introductions for Container Orchestration**

1. Choose an Orchestration Tool – Popular options include Kubernetes, Docker Swarm, and Apace Mesos
2. Define Your Containerized Application – Create container images using Docker or another containerization tool.
3. Set Up an Orchestration Environment – Deploy your chosen orchestration tool on a cloud platform or local infrastructure.
4. Configure Deployment – Define how containers should be deployed, including resource allocation and networking.
5. Implement Scaling Policies – Set rules for automatically scaling containers based on demand.
6. Monitor and Maintain – Use monitoring tools to track container health and performance.
7. Ensure Security – Apply security policies, role-based access control, and network segmentation.

### **Popular tools for Container Orchestration**

Container orchestration tools help manage the deployment, scaling, and operation of containerized applications efficiently. Here are some of the most popular ones:

1. **Kubernetes:** The most widely used container orchestration tool, offering automated deployment, scaling, and management of containerized applications.
2. **Docker Swarm:** A native clustering tool for Docker that simplifies container orchestration with easy setup and management.
3. **Apache Mesos:** A powerful tool that can handle container orchestration alongside other workloads like big data processing.
4. **Rancher:** A complete container management platform that integrates with Kubernetes and simplifies multi-cluster management.
5. **Amazon Elastic Kubernetes Service (EKS):** A managed Kubernetes service by AWS that simplifies Kubernetes deployment.
6. **Google Kubernetes Engine (GKE):** A manages Kubernetes service by Google Cloud, offering automated scaling and security features.
7. **Azure Kubernetes Service (AKS):** Microsoft’s managed Kubernetes service that integrates with Azure tools for seamless container management.

### **Cloud Orchestration Tools**

**Cloud Orchestration tools help manage cloud infrastructure efficiently:**

**AWS CloudFormation:** Automates infrastructure provisioning in AWS

**Terraform:** A widely used infrastructure-as-code tool for managing cloud resources

**Azure Logic Apps:** Helps automate workflows and integrate cloud services

**Google Dataflow:** A data orchestration tool for processing large-scale data

Each tool as its strengths depending on your needs.

## **Security Best Practices for Containers**

Securing containers is crucial to prevent vulnerabilities and ensure safe deployments. Here are some best practices to enhance container security.

1. **Secure Your Container Images**

* Use trusted base image from reputable sources
* Regularly scan images for vulnerabilities before deployment
* Keep images updated with the latest security patches

1. **Manage Secrets Securely**
   * Store sensitive data like API keys and passwords in secret management tools.
   * Avoid hardcoding credentials in container configurations
2. **Restrict Container Privilege**
   * Run containers with least privileges to minimize security risks
   * Use non-root users inside containers to prevent privileges escalation.
3. **Identify and Fix Misconfigurations**
   * Regularly audit container configuration for security flaws
   * Follow best practices for secure networking and storage
4. **Automate Vulnerability Scanning**
   * Implement continuous security scanning in CI/CD pipelines
   * Use tools like Trivy, Clair, or Anchore to detect vulnerabilities
5. **Enable Logging and Monitoring**
   * Set up real-time monitoring to detect suspicious activity.
   * Use logging tools to track container behavior and security incidents.
6. **Adopt “Shift Left” Security** 
   * Integrate security early in the development lifecycle.
   * Educate developers on secure coding practices for containers

# Docker

### Introduction to Docker

Docker is an open-source platform that enables developers to build, package and deploy application in containers. Containers are lightweight, portable, and ensure consistency across different environments, making Docker a popular choice for DevOps, Cloud Computing and Microservices architectures.

### **What is a Docker?**

Docker provides a way to package applications along with their dependencies into isolated environments called containers. These containers ensure that applications run consistently across different systems, whether on a developer’s laptop, a test server or in production.

### **Key Components of Docker**

1. **Docker Engine:** The core component responsible for running containers
2. **Docker Image:** Pre-packaged applications with all necessary dependencies
3. **Docker Container:** Running instance of a Docker Images
4. **Docker Hub:** A repository for storing and sharing container images
5. **Docker CLI:** A command line interface for managing Docker operations

### **Uses of Docker**

**Docker is widely used for**

* **Application Development**: Ensures applications run consistently across different environments
* **Microservices Architecture:** Helps break application into smaller manageable services.
* **CI/CD Pipeline:** Speeds up development and testing processes
* **Cloud Computing:** Works seamlessly with cloud providers like AWS, Azure and Google Cloud.
* **Resource Efficiency:** User Fewer system resources compared to traditional virtual machines.

### **Pros and Cons of Docker**

#### **Pros:**

* Portability: Runs consistently across different environments
* Efficiency: Uses fewer resources than virtual machines
* Scalability: Ideal for cloud-based applications
* Isolation: Prevents conflicts between applications
* Rapid Deployment: Containers start in seconds

#### **Cons:**

* Security Risks: Containers share the host kernel, increasing vulnerability
* Complex Management: Requires orchestration tools like Kubernetes for large-scale deployments
* Storage Limitations: Persistent storage management can be challenging
* Networking Complexity: Requires careful configuration for container communication.

### **Docker Installation**

Installing Docker is a straight forward process, but it varies depending on the operating system. Here’s a step-by-step guide to installing Docker on Windows, macOS and Linux

#### **Installing Docker on Windows**

1. **Download Docker Desktop**

Visit the Docker Website and download Docker Desktop for Windows

1. **Run the Installer**

* Open the downloaded file and follow the setup wizard
* Select WSL 2 as the backend (recommended)

1. **Launch Docker Desktop**

* Open Docker Desktop and wait for it to initialize

1. **Verify Installation**

* Open Command Prompt or PowerShell and run:

docker --version

If Docker is installed correctly, it will display the version number.

#### **Installing Docker on macOS**

1. **Download Docker Desktop**
   * Visit the Docker website and download the correct version for Apple Silicon or Intel Macs
2. **Install Docker**
   * Open the .dmg file and drag Docker to the Application Folder.
3. **Launch Docker**
   * Open Docker from the Applications folder and grant necessary permissions.
4. **Verify Installation**
   * Open Terminal and run:

docker –version

If Installed correctly, it will display the Docker version

#### **Installing Docker on Linux**

1. **Update System Packages**
   * Run the following commands to update your package index:

sudo apt update && sudo apt upgrade -y **# For Debian/Ubuntu**

sudo dnf update -y **# For Fedora**

1. **Install Docker**

For Ubuntu/Debian:

sudo apt install docker.io -y

For Fedora:

sudo dnf install docker -y

For CenOS:

sudo yum install docker -y

1. **Start and Enable Docker**

Run the following command to start Docker:

sudo systemctl start docker

sudo systemctl enable docker

1. **Verify Installation**

Check the installed version:

docker –version

Test Docker by running:

sudo docket run hello-world

If successful, you will see a message confirming that Docker is running.

**Post-Installation (Linux Users)**

By default, Docker requires sudo to run. To allow running Docker without sudo:

sudo usermod -aG docker $USER

Log out and log back in for changes to take effect.

### **Docker Architecture**

Docker follows a Client-Server Architecture that enables efficient containerization, allowing applications to run in isolated environments. Below is a detailed breakdown of Docker’s architecture.

#### **Docker Engine**

Docker Engine is the core component responsible for running containers. It consists of

* **Docker Daemon (dockerd):** Manages containers, images, networks, and storage.
* **Docker CLI:** A command line tool for interacting with Docker
* **REST API:** Allows communication between Docker components and external applications.

#### **Docker Images**

Docker images are pre-packaged applications that contain all dependencies needed to run a container. Key points:

* Images are read-only and act as templates for containers
* Stored in Docker Hub or private registries
* Built using Dockerfiles, which define the image structure

#### **Docker Containers**

Containers are running instances of Docker images. They provide:

* **Isolation:** Each container runs independently.
* **Portability:** Can run on any system with Docker Installed.
* **Efficiency:** Uses fewer resources than virtual machines.

#### **Docker Registers**

Docker registers store and distribute images. There are:

**Public Registries:** Docker Hub, GitHub Container Registry

**Private Registries:** Used for enterprise security

#### **Docker Networking**

Docker provides multiple networking options:

* **Bridge Network:** Default network for containers.
* **Host Network:** Containers share the host’s network.
* **Overlay Network:** Used in multi-host environments.
* **Macvlan Network:** Assigns MAC addresses to containers

#### **Docker Storage**

Docker supports different storage mechanisms

* **Volumes:** Persistent storage for containers
* **Bind Mounts:** Directly link host directories to containers
* **Tmpfs Mounts:** Temporary storage in memory

#### **Docker Orchestration**

For managing multiple containers, Docker integrates with:

* **Kubernetes:** Industry standard orchestration tool
* **Docker Swarm:** Native Clustering solutions for Docker

### **Step by Step Guide to Run a Docker Container**

#### **Step-1: Pull a Docker Image**

Docker Images are prebuilt application environments. Let’s pull the **hello-world** image as an example.

docker pull hello-world

This command downloads the image from Docker Hub

#### **Step-2: Run a Container from the image**

Now that we have an image, let’s run it as a container

docker run hello-world

#### **Step-3: Understanding the Output**

When you run the above command, Docker:

* Creates a new container from the hello-world image.
* Executes it
* Displays a welcome message indicating that everything is set up correctly

#### **Step-4: Listing Running Container**

To See active containers, use:

docker ps

For all containers (even stopped ones), run:

docker ps – a

#### **Step-5: Removing a Container**

After running a container, you might want to clean up unused ones:

docker rm <container\_id>

To remove the hello-world container, get its ID using docker ps -a and then remove it.

#### **Step-6: Running a Custom Application in a Container**

Let’s run a more useful container – a simple nginx web server:

1. Pull the nginx image:

docker pull nginx

1. Run the container

docker run -d -p 8080:80 nginx

-d runs the container in detached mode (in the background)

-p 8080:80 maps port 80 to the container to port 8080 on your machine.

1. Open your browser and go to:

<http://localhost:8080>

You should see the default nginx welcome page.

#### **Step-7: Stopping a Running Container**

If you want to stop the nginx container

docker stop <container\_id>

To remove it completely

docker rm <continer\_id>

## **Docker Networking**

Docker networking is a crucial topic that enables containers to communicate with each other and the outside world. Docker provides multiple networking modes depending on your application’s requirements.

### **Bridge Network (Default)**

* + This is Docker’s default network when you run a container without specifying a network
  + Containers within the same bridge network can communicate with each other via their container names.

docker network create my\_bridge\_network

docker run --network=my\_bridge\_network --name container1 -d nginx

docker run --network=my\_bridge\_network –-name container2 -d nginx

Now, container1 can ping container2 using its name

#### Example-1: Step by Step Guide to ping container2 from container1

* + 1. **Access container1’s Terminal**

Run the following command to enter the interactive terminal of container1

docker exec -it container1 /bin/sh

This will open a shell inside container1

* + 1. **Ping container2 by Name**

Since both containers are on the same bridge network, you can directly ping container2 using

ping container2

You should see replies from container2, confirming that the connection is working. Incase you get an error indicating that ping not found. You need to update and install iputils-ping

* Ensure both containers are in the same network:

docker network inspect my\_bridge\_network

* If ping is missing inside the container, install it using:

apt update && apt install -y iputils-ping

This should help you test container-to-container communication within your Docker bridge network

* + 1. **Ping container2 by IP**

If you want to ping container1 using its IP address:

* + First, find its IP address:

Then, insider container1, ping it using:

docker inspect -f '{{range.NetworkSettings.Networks}}{{.IPAddress}}{{end}}' container2

This will return the IP of container1 (e.g., 172.18.0.2)

* + Then, inside container1, ping it using

ping 172.18.0.2

#### Example-2: Step by Step Guide for the following usecase: Run a MySQL & Web Server in Bridge Networking 🔹 Set up a simple REST API using Python in containers 🔹 Simulate multi-container app communication

* + 1. **Verify Docker Installation**

docker --version

* + 1. **Check default Bridge Network**

docker network ls

* + 1. **Create a Custom Bridge Network**

docker network create myapp-network

* + 1. **Create a Python REST API**

Build a simple Flask-based REST API that connects to MySQL

* **Create Project Structure**

mkdir docker-app

cd docker-app

mkdir app

touch app/main.py app/requirements.txt Dockerfile docker-compose.yml

* **Write the REST API (app/mail.py):**

from flask import Flask, jsonify

import mysql.connector

from mysql.connector import Error

app = Flast(\_\_name\_\_)

def get\_db\_connection():

try:

connection = mysql.connetor.connect(

host = ‘mysql’ , # Container name of MySQL

database = ‘testdb’,

user = ‘root’

password = ‘password’

)

@app.route(‘/users’, methods=[‘GET’])

def get\_users():

conn = get\_db\_connection()

if conn is None:

return jsonify({“Error”: “Database connection failed”), 500

cursor = conn.cursor(dictionary=TRUE)

cursor.execute(“SELECT \* FROM users”)

users = cursor.fetchall()

cursor.close()

conn.close()

return jsonify(users)

if \_\_name\_\_ == ‘\_\_main\_\_’:

app.run(host=’0.0.0.0’, port= 5000)

* **Define Dependencies (app/requirements.txt):**

flask == 2.3.2

mysql-connector-python==8.0.33

* **Create Dockerfile for the Web Server:**

FROM python:3.0-slim

WORKDIR /app

COPY requirements.txt .

RUN pip install –no-cache-dir -r requirements.txt

COPY ..

EXPOSE 5000

CMD[“python”, “main.py”]

Test the Flask app locally to ensure it runs (python app/main.py)

Note: The program will fail to connect to MySQL until the database container is set up.

* + 1. **Set up MySQL Container**

Run a MySQL container in the same bridge network as the web server.

* Pull the MySQL image:

docker pull mysql:8.0.

* Run MySQL container manually to test

Docker run –name mysql -d \

--network myapp-network \

-e MYSQL\_ROOT\_PASSWORD=password \

-e MYSQL\_DATABASE=testdb \

mysql:8.0

* Access MySQL to create a sample table:

docker exec -it mysql mysql -uroot -ppassword

Inside MySQL:

USE testdb;

CREATE TABLE users (id INT AUTO\_INCREMENT PRIMARY KEY, name VARCHAR(255);

INSER INTO users (name) VALUES (‘Alice’), (‘Bob’)

SELECT \* FROM users:

EXIT;

Verify MySQL is running

docker ps

Confirm its in your custom network:

docker network inspect myapp-network

* + 1. **Run the Web Server Container**

Build and run Flask app in a container, connecting to MySQL

Steps:

* Build the web server image

cd docker-app

docker build -t myapp-web .

* Run the web server container:

docker run –name web -d \

--network myapp-network \

-p 5000:5000 \

Myapp-web

* Test the API:

Open a browser httpp://localhost:5000/users

Expected output [{“id”:1, “name”: “Alice”},{“id”:2, “name”:”Bob”}]

* + 1. **Simplify with Docker Compose**

Use Docker compose to manage both containers in one configuration

* + - * **Create docker-compose.yml:**

version: '3.8'

services:

mysql:

image: mysql:8.0

environment:

MYSQL\_ROOT\_PASSWORD: password

MYSQL\_DATABASE: testdb

networks:

- myapp-network

volumes:

- mysql-data:/var/lib/mysql

web:

build: .

ports:

- "5000:5000"

### **Host Network**

Docker Host Network is a networking mode in Docker that allows a container to use the network stack of the host machine directly. This means that the container doesn’t have its own isolated network and instead shares the host’s IP address and network interfaces.

**Key Features of Docker Host Network**

* + **Not Network Isolation:** The container runs directly on the host’s network interface, bypassing the Docker bridge network.
  + **Low Latency:** Since there is no need for NAT (Network Address Translation), network performance is improved.
  + **Same Network configuration as Host:** Containers can directly access the host’s network services as if they were running on the host itself.
  + **Suitable for Performance-Sensitive Applications:** Host networking is useful for applications that require high network performance, like databases or monitoring tools.
  + Useful when performance is critical or when handling networking-intensive tasks.
  + Example:

docker run -–network=host -d nginx

The Nginx server will run directly on the host’s network, without separate container IP

**Considerations:**

* **Port Conflicts:** Since containers share the host’s network, they might interface with processes running on the host that use the same ports.
* **Security Risks:** Containers using the host network don’t have the isolation benefits of Docker’s bridge network, increasing potential vulnerabilities.
* **Linux-only Feature**: Host networking is only available on Linux-based systems; it doesn’t work the same way on Windows or MacOS.

**Practical use cases for Docker Host Network**

1. **High-Performance Applications**

Applications like databases, monitoring tools or streaming services often require low latency and high-speed communication. Using the host network removes the overhead of Docker’s virtual network, leading to better performance.

1. **Running Network Utilities**

If you need to run network utilities like tcpdump, traceroute, or ping inside a container, using the host network ensures that the tools interact with the real network interfaces without interference.

1. **Simplifying Configuration**

Some applications require direct access to services running on the host without additional network setup. Using the host network eliminates the need to expose ports manually or configure complex networking rules.

1. **Containers That Need to Discover Services**

Some service discovery mechanisms, like multicast-based discovery, don’t work well in Docker’s bridge network. Using the host network allows the container to participate in service discovery without restrictions.

1. **Running a Web Server**

If you’re deploying a web server like Nginx, Apache, or reverse proxy, using the host network allows it to serve requests without needing Docker’s networking layer.

### **Overlay Network (For Multi-Host communication)**

* + User in Docker Swarm for connecting services across different hosts
  + Allows containers to communicate securely across multiple machines
  + Exampe:

docker network create -d overlay my\_overlay\_network

Containers on different nodes can now talk using this overlay network

### **Macvlan Network (For Direct Physical Network Access)**

* + Assigns a MAC address to the container so it appears as a Physical device in the network
  + Useful when containers need direct communication with the external network
  + Example:

docker network create -d mcvlan –subnet=192.168.1.0/24 my\_mcvlan

### **None Network (Completely Isolated)**

* + Removes all networking capabilities – ideal for strict security use cases.
  + Example:

docker run –network=none -d busybox

This container won’t have internet or local network access

### **Custom Networks & DNS**

* + When using custom networks, Docker provides a built-in DNS resolver so containers can communicate by name instead of IP
  + You can inspect networks using:

docker network inspect my\_bridge\_network

**Connecting a Running Container to a Different Network**

If a container is running but you need to connect it wot another network

docker network connect my\_bridge\_network container1

## **Building Docker Images**

Docker is a platform that enables developers to build, package, and deploy applications as containers, ensuring consistency across different environments. Docker building refers to the process of creating a Docker image from a Dockerfile, which is a script containing instruction to define the application environment and its dependencies.

Building Docker images is a core process in containerization, enabling developers to package applications with their dependencies into portable, reproducible units.

Below is a detailed, Step-by-Step explanation of the Docker building process, assuming you have Docker installed on your system.

### **Step by Step Guild to Docker Building**

#### **Step-1: Understand the Components**

Before building Docker image, familiarize yourself with the key components:

**Dockerfile:** A text file with instructions to build Docker image. It specifies the base image dependencies, environment setup and commands to run the application.

**Docker Image:** A lightweight, portable, and executable package that includes everything needed to run an application (code, runtime, libraries, and dependencies)

**Docker Container:** A running instance of Docker Image

**Docker Engine:** The runtime that builds and runs Docker container.

#### **Step-2: Set up Your Project Directory**

Create a directory for your Docker project to keep your files organized.

1. Open a terminal and create a project folder:

mkdir my-docker-app

cd my-docker-app

1. Inside this directory, you will place all your application code and the Dockerfile

#### **Step-3: Create a Dockerfile**

The Docker file defines how the Docker image is built. Create a file named Dockerfile (no extension) in your project directory.

touch Dockerfile

Open the Dockerfile in a text editor and add instructions. Below is an example for a simple Node.js application:

**# Step 1: Specify the base image**

FROM node:18

**# Step 2: Set the working directory inside the container**

WORKDIR /app

**# Step 3: Copy package.json and install dependencies**

COPY package\*.json ./

RUN npm install

**# Step 4: Copy the rest of the application code**

COPY . .

**# Step 5: Expose the port the app runs on**

EXPOSE 3000

**# Step 6: Define the command to run the application**

CMD ["npm", "start"]

**Explanation of Instructions:**

**FROM:** Specifies the base image (e.g., node:18 for a Node.js environment)

**WORKDIR:** Sets the working directory inside the container for subsequent commands

**COPY:** Copies files from the host machine to the container (e.g., package .json and application code).

**RUN:** Executes commands during the build process (e.g., installing dependencies)

**EXPOSE:** Documents the port the application will use (does not actually publish the port)

**CMD:** Specifies the default command to run when the container starts

#### **Step-4: Create Your Application**

For this example, assume you are building a simple Node.js application. Create the following files in your my-docker-app directory:

1. **package.json:**

{

“name”: ”my-docker-app”,

“version”: “1.0.0”,

“scripts”: {

“start”: “node index.js”

},

“dependencies”: {

“express”: “^4.18.2”

}

}

1. **index.js (a simple Express Server):**

const express = require(‘express’);

const app = express();

const port = 3000;

app.get (‘/’, (req, res) => {

res.send(“Hello From Docker!”);

});

app.listen (port, () => {

console.log(‘Server running at http://localhost:${port}”);

});

These files define a basic Node.js application using Express Sever that listens on port 3000

#### **Step-5: Build the Docker Image**

With the Dockerfile and application files ready, build the Docker image using the docker build command.

1. In the terminal, ensure you are in the my-docker-app directory
2. Run the build command

docker build -t my-docker-app:latest .

1. Docker will execute instruction in the Dockerfile:
   1. Pull the base image (node:18) if not already present
   2. Create intermediate container to execute RUN commands
   3. Copy files into the image as specified
   4. Create the file image with the specific configuration
2. Monitor the terminal output to see the progress of each step. If successful, you will see a message like:

#### **Step-6: Verify the Image**

docker images

This lists all images on your system. You should see my-app:latest (or whatever name/tag you used).

#### **Step-7: Run a Container from the Image**

docker run -p 3000:3000 my-app:latest

* + -p: Maps port 3000 on the host to port 3000 in the container (based on the EXPOSE instruction).
  + The container starts, and the application should be accessible at http://localhost:3000.

#### **Step-8: Test the Application**

http://localhost:3000.

#### **Step-9: Optimize the Build (Optional)**

**To make builds faster and images smaller:**

Use Multi-Stage Builds: Separate build and runtime environments to exclude unnecessary build tools from the final image.

Example:

# Build stage

FROM node:18 AS builder

WORKDIR /app

COPY package\*.json ./

RUN npm install

COPY . .

RUN npm run build

**# Runtime stage**

FROM node:18-slim

WORKDIR /app

COPY --from=builder /app/dist ./dist

COPY package\*.json ./

RUN npm install --production

EXPOSE 3000

CMD ["node", "dist/index.js"]

* **Minimize Layers:** Combine related commands (e.g., multiple RUN commands) to reduce the number of layers.
* **Use Smaller Base Images**: Use lightweight base images like node:18-slim or alpine.
* **Leverage Cache**: Order instructions from least to most frequently changed (e.g., copy package.json before source code to reuse cached dependency layers).

#### **Step-10: Push the image to Registry (Optional)**

**To share or deploy the image, push it to a container registry like Docker Hub, AWS ECR, or GitHub Container Registry**

1. **Log into the Registry**

docker login

1. **Tag the Image (if needed)**

docker tag my-app:lates <registry-username>/my-app:latest

1. **Push the Image:**

docker push <registry-username>/my-app:latest

#### **Step-11: Clean Up (Optional)**

### **Common Issues and Troubleshooting**

**Build Context Too Large:** Use a .dockerignore file to exclude unnecessary files

**Cache Issues:** If the Cache is outdated, force a rebuild with

docker build –no—cache -t my-app:latest .

**Permission Errors:** Ensure the Docker Daemon is running and you have appropriate permissions.

**Image Size:** Check the image size with docker images and optimize using multi-stage builds or smaller base images.

### **Key Concepts in Docker Building**

**Build Context:** The set of files and directories sent to the Docker daemon during the build (usually the directory containing the Dockerfile)

**Layers:** Each instruction in the Dockerfile creates a layer in the image. Layers are cached and reused to speed up builds

**Image Immutability:** Once built, images are immutable. Changes require rebuilding the image.

**Multi-Stage Builds:** For advanced use cases, you can use multi-stage builds to create smaller images by separating build and runtime environments.

## **Docker Compose**

Docker Compose is a tool for defining and running multi-container Docker applications using a YAML file to configure services, networks and volumes. It simplifies the process of managing complex applications by allowing you to orchestrate multiple containers that work together, with a single command to start, stop or rebuild them. It’s particularly useful for development, testing and staging environments.

Key Concepts of Docker Compose

1. Services: Containers running a specific image, defined with configurations like port environment variables and dependencies.
2. Networks: Communication channels between container, automatically created customized.
3. Volumes: Persistent storage for containers to retain data across restarts
4. YAML File: The docker-compose.yml file where you define the entire application stack.
5. CLI: The docker-compose command line tool to manage the application lifecycle (e.g., up, down, build)

**Benefits:**

* Simplifies multi-container setups
* Ensures consistent environments across machines
* Supports dependency management between services
* Integrates with Docker’s ecosystem

Step-by-Step Explanation with Example:

Lets create a simple web application using Docker Compose with two services: A Python Flask Web server and a Redis Database. The Flask app will use Redis to store a visit counter.

### **Step-1: Install Docker Compose**

Ensure Docker and Docker Compose are installed:

Docker: Required for Running Containers

Docker Compose: Usually included with Docker Desktop (Windows/Mac) or installed separately on Linux (sudo apt-get install docker-compose-plugin or equivalent).

Verify installation:

docker-compose –version

### **Step-2: Create Project Directory**

Create a directory for the project:

mkdir flask-redis-app

cd flask-redis-app

### **Step-3: Create Application Code**

Create a file app.py for the Flask application:

from flask import Flask

from redis import Redis

import os

app = Flask(\_\_name\_\_)

redis = Redis(host=’redis’, post= 6379)

@app.route(‘/’)

def hello():

count = redis.incr(‘hits’)

return f’hello!, this page has been visited {count} times.’

If \_\_name\_\_ == ‘\_\_main\_\_’:

app.run(host=’0.0.0.0’, port=5000)

### Step-4: Create Requirements File

Create requirments.txt for Python Dependencies

flask==2.3.3

redis==5.0.1

### **Step-5: Create Dockerfile**

Create a Dockerfile to build the Flask app image:

FROM python:3.9-slim

WORKDIR /app

COPY requjirements.txt

RUN pip install --no—cache-dir -r requirements.txt

COPY ..

EXPOSE 5000

CMD[“python”, “app.py”]

### **Step-6: Create Docker Compose File**

Create docker-compose.yml to define the services:

Yaml file contents:

Version: ‘3.8’

Services:

web:

build: .

ports:

* “5000:5000”

Depends\_on:

* Redis

Environment:

* FLASK\_ENV = development

redis:

image: redis:7.0-alpine

ports:

* “6379:6379”

Volumes:

* redis-data:/data

volumes:

redis-data

networks:

default:

name: flask-redis-network

**Explanation of docker-compose.yml:**

**version:** Specifies the Docker Compose file format (3.8 is widely used)

**services:**

* web: The Flask app service, built from the local Dockerfile. Maps port 5000 on the host to 5000 in the container. Depends on the redis service.
* Redis: Uses the official Redis image. Maps port 6379 and persists data in a volume

**volumes:** Defines a named volume redis-data for Redis persistence.

**networks:** Creates a custom network flask-redis-network for service communication

### **Step-7: Run Docker Compose**

Start the application:

docker-compose up –build

--build : Builds the images if they don’t exist or if changes are detected

This command builds the Flas app image, pulls the Redis image, creates the network and volume, and starts both containers

### **Step-8: Access the application**

Open the browser and navigate to http://localhost:5000 . You should see

Hello! This page has been visted 1 times

Refresh the page to increment the counter.

### Step-9: Stop the Application

Stop and remove the containers

docker-compose down

To also remove volumes

docker-compose down -v

### **Step-10: Explore Additional Commands**

**View Running services:** docker-compose ps

**View logs:** docker-compose logs

**Rebuild services:** docker-compose build

**Start in detached mode:** docker-compose up -d

**Directory Structure**

flask-redis-app/

|--------app.py

|--------Dockerfile

|--------docker-compose.yml

|--------requirements.txt

### **Advanced Features:**

**Scaling:** Run multiple instances of a service (e.g., docker-compose up –scale web=3)

**Environment Files:** Use .env files for variables (e.g., DB\_HOST=redis)

**Health Checks:** Add healthcheck in docker-compose.yml to monitor service health

**Profiles:** Use profiles to run subsets of services (e.g., docker-compose –profile dev up)

### **Common Issues and Solutions:**

**Port Conflicts:** Ensure ports 5000 and 6379 are free or change them in docker-compose.yml

**Redis connection Errors:** Verify the redis service name matches in app.py and the network is correctly set up.

**Image Build failures:** Check Dockerfile and requirements.txt for errors

This example demonstrates Docker Compose’s power to orchestrate a multi-container application with minimal setup. You can extend it by adding Databases, message Queues or other services as needed.

## **Scaling in Docker**

Scaling in Docker Compose allows you to run multiple instances (containers) of a specific service defined in your docker-compose.yml file. This is useful for load balancing, improving performance, or testing distributed systems in development enviroments. The –scale option with docker-compose up command lets y ou specify the number of containers for a particular service.

### **Key Points about scaling in Docker Compose.**

Purpose: Run multiple containers of the same service to handle increased load or simulate a production like environment

Mechanism: Each scaled container runs the same image and configuration but is assigned a unique name (e.g., web\_1, web\_2, web\_3).

Networking: Scaled containers share the same Docker network, allowing communications between them and other services.

#### **Limitations:**

Docker compose scaling is primarily for development and testing, not production-grade orchestration (use Kubernetes or Docker Swarm for production)

You must ensure services are stateless or properly configured to handle multiple instances (e.g., shard storage for stateful services)

Port mappings can cause conflicts if not handled properly

#### **How Scaling Works**

When you use docker-compose up – scale <service>=<number>, Docker Compose:

1. Starts the specified number of containers for the given service
2. Assigns unique container names (e.g., <project-name>\_<service-name>\_<index>)
3. Ensures all containers share the same configuration (image, environment variables, volumes, etc) as defined in the docker-compose.yml
4. Places all containers in the same network for inter-service communication.

### Example: Scaling the Web Service

Using the previous Flask-Redis Example, lets scale the web service (Flask app) to run 3 instances.

#### **Step-1: Review the docker-compose.yml**

Here is the relevant part of the docker-compose.yml from the Flask-Redis example:

version: '3.8'

services:

web:

build: .

ports:

- "5000:5000"

depends\_on:

- redis

environment:

- FLASK\_ENV=development

redis:

image: redis:7.0-alpine

ports:

- "6379:6379"

volumes:

- redis-data:/data

volumes:

redis-data:

networks:

default:

name: flask-redis-network

#### **Step-2: Address Port Conflicts**

The web service maps port 5000 on the host to 5000 in the container. If you scale to multiple instances, all containers will try to bind to the same host port (5000), causing a conflict. To avoid this, you have two options:

1. Remove Host Port Mapping: Omit the host port in ports (e.g. ports: - “5000”) to let Docker assign random host ports. You can check assigned ports with docker-compose ps
2. Use a Load Balancer: Introduce a reverse proxy (e.g., Nginx) to route traffic to scaled containers. For simplicity, we will use the first approach.

Modify the web service in docker-compose.yml

web:

build: .

ports:

- "5000" # No host port specified

depends\_on:

- redis

environment:

- FLASK\_ENV=development

#### **Step-3: Scaling the Service**

Run the following command to start three instances of the web service:

docker-compose up –scale web=3

#### **Step-4: Verify Scaled Containers**

Check the running Containers

Docker-compose ps

Output:

Name Command State Ports

--------------------------------------------------------------------------------

flask-redis-app\_redis\_1 docker-entrypoint.sh redis ... Up 0.0.0.0:6379->6379/tcp

flask-redis-app\_web\_1 python app.py Up 0.0.0.0:49153->5000/tcp

flask-redis-app\_web\_2 python app.py Up 0.0.0.0:49154->5000/tcp

flask-redis-app\_web\_3 python app.py Up 0.0.0.0:49155->5000/tcp

Three web containers (web\_1, web\_2, web\_3) are running

Each is assigned a random host port (e.g., 49153, 49154, 49155) mapped to container port 5000

The redis remains single instance

#### **Step-5: Test the Application**

Access the Flask appl by visiting the assigned ports in your browser (e.g., <http://localhost:49153>, <http://localhost:49154>, <http://localhost:49155>). Each instance will respond, and the Redis counter will increment consistently because all web containers connect to the same Redis Service.

#### **Step-6: Stop the Application**

Stop and remove the containers

docker-compose down

#### **Using a Load Balancer (Optional)**

For a more production-like setup, you can add an Nginx service to load-balance traffic across scaled web containers. Here is how:

Modify docker-compose.yml

Add an Nginz service:

Yaml

version: '3.8'

services:

web:

build: .

expose:

- "5000" # Expose port for internal network, no host mapping

depends\_on:

- redis

environment:

- FLASK\_ENV=development

redis:

image: redis:7.0-alpine

ports:

- "6379:6379"

volumes:

- redis-data:/data

nginx:

image: nginx:1.25-alpine

volumes:

- ./nginx.conf:/etc/nginx/nginx.conf:ro

ports:

- "80:80"

depends\_on:

- web

volumes:

redis-data:

networks:

default:

name: flask-redis-network

**Create nginx.conf**

Create a file nginx.conf in the project directory:

events {}

http {

upstream web {

server web\_1:5000;

server web\_2:5000;

server web\_3:5000;

}

server {

listen 80;

location / {

proxy\_pass http://web;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

}

}

}

This configuration load-balances traffic across the web containers.

**Scale and Run**

Start the application with scaled web instances:

docker-compose up –scale web=3

Access the app at http://localhost Nginx distributes requests across the three web containers.

**Consideration for Scaling**

**Stateless Services:** Ensures the service is stateless or uses shared storage (e.g., Redis database) to avoid inconsistent state across instances.

**Resource Usage:** Scaling increases CPU/Memory usage. Monitor with docker stats

**Service Discovery:** Container communicate using service names (e.g., redis, web\_1).

Docker’s DNs resolves these within the network

**Production Scaling:** For Production, use Docker Swarm, Kubernetes, or cloud services for advanced orchestration, health checks and auto-scaling.

**Example Behavior**

In the Flask-Redis App:

1. Each web container handles http request independently
2. All containers share the same Redis instance, so the visit counter is consistent
3. Without Nginx, you manually access random host ports. With Nginx, a single port (80) load-balances requests.

This demonstrates how Docker Compose’s --scale option enables running multiple instances of a service, with or without a load balancer, for development and testing purposes.

## **Docker Swarm**

Docker Swarm is a native orchestration tool for Docker that allows you to manage and deploy a cluster of Docker nodes as a single virtual system. It provides features like service discovery, load balancing, scaling and rolling updates for containerized applications. Below I will explain Docker Swarm in detail, step by step with an example of setting up a simple web application.

### **What is Docker Swarm?**

Docker Swarm is a clustering and orchestration solution for Docker containers. It enables you to:

1. Create a swarm (a group of Docker hosts) that work together
2. Deploy Services (Containerized applications) across the swarm
3. Scale services up or down, manage load balancing and ensure high availability
4. Perform rolling updates and rollbacks for services

Swarm operates in a manager-worker architecture:

**Manage Nodes:** Manage the swarm, maintain the cluster state, and schedule tasks

**Worker Nodes:** Run the container (tasks) assigned by the manager

### **Key Concepts in Docker Swarm**

1. **Node:** A docker host participating in the Swarm (either a manager or a Worker)
2. **Service:** A definition of task to execute (e.g., run a specific container image with a given configuration)
3. **Task:** A single container running as part of a service

### Step-by-Step Guide to Using Docker Swarm

Lets walk through setting up a docker swarm cluster and deploying a simple web application (e.g., an Nginx web server) with scaling and load balancing.

**Prerequisites**

* Docker installed on all machines (nodes), you will use in the swarm
* Basic understanding of Docker containers and networking
* At least two machines (physical or virtual) to simulate a multi-node setup. For this example we will assume three machines

Manager Node: 192.168.1.100

Worker Node1: 192.168.1.101

Worker Node2: 192.168.1.102

#### **Step-1: Initialize the Swarm**

1. **Choose a Manager Node:**

One of the machine you want to designate as the manager (192.168.1.100), initialized the swarm:

docker swarm init –advertise—addr 192.168.1.100

The –advertise-addr sepecifies the IP address for Swarm communication

This command outputs a docker swarm join command with a token, which you will use to add worker nodes.

**Example Output:**

Swarm initialized: current node (abc123...) is now a manager.

To add a worker to this swarm, run the following command:

docker swarm join --token SWMTKN-1-xyz... 192.168.1.100:2377

1. **Verify the Swarm**

On the manager node, check the swarm status:

docker node ls

**Output:**

ID HOSTNAME STATUS AVAILABILITY MANAGER STATUS

abc123... manager1 Ready Active Leader

#### **Step-2: Add Worker Nodes**

1. On each worker node (192.168.1.101 and 192.168.1.102), run the docker swarm join command provided by the manager.

docker swarm join --token SWMTKN-1-xyz... 192.168.1.100:2377

**Output:**

This node joined a swarm as a worker.

1. On the manager node, verify that the workers have joined:

docker node ls

**Output**

ID HOSTNAME STATUS AVAILABILITY MANAGER STATUS

abc123... manager1 Ready Active Leader

def456... worker1 Ready Active

ghi789... worker2 Ready Active

#### **Step-3: Create on Overlay Network**

To allow containers on different nodes to communicate, create an overlay network:

docker network create –driver overlay my-app-network

The overlay driver enables cross-node communication

Verify the network

docker network ls

#### **Step-4: Deploy a Service**

Lets deploy an Nginx web server as a service in the swarm

1. **Create a Service:**

On the manager node, create a service named web using Nginx image:

docker service create \

--name web \

--replicas 3 \

--publish published=80,target=80 \

--network my-app-network \

nginx:latest

* --name web: Names the service.
* --replicas 3: Runs three instances (tasks) of the container.
* --publish published=80,target=80: Maps port 80 on the swarm to port 80 in the container.
* --network my-app-network: Attaches the service to the overlay network.
* nginx:latest: The container image to use.

1. **Verify the Service:**

Check the service status:

docker service ls

**Output:**

ID NAME MODE REPLICAS IMAGE PORTS

xyz123... web replicated 3/3 nginx:latest \*:80->80/tcp

List the tasks (containers) running for the service:

docker service ps web

**Output:**

ID NAME IMAGE NODE DESIRED STATE CURRENT STATE

aaa111... web.1 nginx:latest manager1 Running Running 5 minutes ago

bbb222... web.2 nginx:latest worker1 Running Running 5 minutes ago

ccc333... web.3 nginx:latest worker2 Running Running 5 minutes ago

#### **Step-5: Test the service:**

1. Access the Nginx service by opening a browser or using curl to any node’s IP address on port 80:

curl <http://192.168.1.100>

You should see the default Nginx welcome page HTML

1. Swarm’s built-in load balancer distributes requests across the three replicas. Try accessing other nodes (192.168.1.101 or 192.168.1.102) to verify

#### **Step-6: Scale the Service**

1. Scale the service to 5 replicas:

docker service scale web=5

1. Verify the updated service:

docker service ps web

You will see two additional tasks scheduled on available nodes.

1. Scale down to 2 repicas

docker service scale web=2

#### **Step-7: Perform a Rolling update**

Lets update the service to use a different Nginx version (e.g., nginx:1.20)

1. Update the service

docker service update \

--image nginx:1.20 \

--update-delay 10s \

Web

* --image nginx:1.20: Updates the image to version 1.20.
* --update-delay 10s: Waits 10 seconds between updating each replica (rolling update).

1. Monitor the update

docker service ps web

#### **Step-8: Clean Up**

1. Remove the service

docker service rm web

1. Remove the overlay network

docker network rm my-app-network

1. Leave the swarm (on worker nodes)

docker swarm leave

1. Dissolve the swarm (on the manger node):

docker swarm leave –force

**Example Summary**

In this example, we:

* Initialized a Docker Swarm with one Manager and two Worker Nodes
* Created an overlay network for communication
* Deployed an Nginx web service with three replicas
* Tested load balancing by accessing the service on different nodes
* Scaled the service up and down
* Performed a rolling update to new Nginx version
* Cleaned up the resources

**Additional Notes:**

**High Availability**: If a node fails, Swarm reschedules tasks to healthy nodes

**Security:** Swarm uses TLS for secure communication between nodes

Storage: For Persistent data, use Docker volumes or bind mounts with Swarm

**Comparison with Kubernetes:** Sware is simpler and tightly integrated with Docker but less feature-rich than Kubernetes for complex orchesteration.

# **Kubernetes**

## **Introduction to Kubernetes**

Overview: Kubernetes, often abbreviated as K8s, is an open-source platform designed to automate the deployment, scaling, and management of containerized applications. Initially developed by Google, it was donated to the Cloud Native Computing Foundation (CNCF) in 2014. Kubernetes provides a robust framework for running distributed systems resiliently, handling tasks like load balancing, service discovery, and automated rollouts and rollbacks.

## **Why Kubernetes?**

Modern applications are increasingly built using containers – lightweight, portable units that package code and dependencies together. Containers enable consistent development, testing, production environments. However, managing hundreds or thousands of containers manually is impractical. Kubernetes addresses this by orchestrating containers cross a cluster of machines, ensuring high availability, scalability, and efficient resource utilization.

## **Key Benefits**

**Portability**: Runs on various environments, including public clouds, private clouds, and on premises infrastructure.

**Scalability:** Automatically scale applications based on demand, from a single cluster to thousands.

**Resilience:** Self-handling capabilities restart failed containers, reschedule them, and ensure desired application states.

**Extensibility:** Supports a rich ecosystem of tools and plugins for monitoring, logging, and CI/CD integration.

**Declarative Configuration:** Define application states using YAML or JSON manifests, allowing version-controlled infrastructure as code.

## **Core Concepts**

Kubernetes operates on a cluster-based architecture, with a control plane managing worker nodes. Below are the fundamental components and concepts:

### **Cluster**

A Kubernetes cluster consists of:

**Control Plane:** Manages the cluster’s state, including scheduling and API interactions. Key components include:

**kube-apiserver:** The API entry point for all Operations

**etcd:** A distributed key-value store for cluster data

**kube-scheduler:** Assigns workloads to nodes based on resource needs and constraints

**kube-controller-manager:** Runs controllers to maintain desired states (e.g., replication)

**Worker Nodes:** Machines (physical or virtual) that run containerized applications. Each node includes:

**kubelet:** An agent that communicates with the Control plane and manages containers

**kube-proxy:** Handles networking, enabling communication between services

**Container Runtime:** Software (e.g., Docker, containerd) that runs containers

### **Pods**

A pod is the smallest deployable unit in Kubernetes, typically containing one or more containers that share storage, networking, and a specification for how to run. Pods are ephemeral and managed by higher-level controllers.

### **Controllers**

Controllers ensure the desired state of the cluster. Common types include:

**Deployment:** Manages stateless applications, handling updates and rollbacks.

**StatefulSet:** Manages stateful applications, ensuring stable identities and persistent storage.

**DaemonSet:** Runs a pod on every node (e.g., for logging or monitoring)

**Job/CronJob:** Manages one-time or scheduled tasks

### **Services**

A service defines a logical set of pods and policy to access them, providing stable networking endpoints. Types include:

**ClusterIP:** Internal access within the cluster (default)

**NodePort:** Exposes the service on a node’s IP and static port.

**LoadBalance:** Expose the service externally via a cloud provider’s load balancer.

**ExternalName:** Maps a service to an external DNS name.

### **Ingress**

Ingress manages external HTTP/HTTPS traffic, providing load balancing, SSL termination, and name based virtual hosting. It requires an Ingress controller (e.g., NGINX, Traefik).

### **ConfigMaps and Secrets**

**ConfigMaps:** Store non-sensitive configuration data (e.g., environment variables, command-line arguments)

**Secrets:** Store sensitive data (e.g., passwords, API Keys), in an encoded format.

### **Namespaces**

Namespace provide virtual clusters within a physical cluster, enabling resource isolation for teams, projects or environments (e.g., dev, prod)

### **Storage**

Kubernetes supports persistent storage through:

**Volumes:** Provides storage tied to a pod’s lifecycle

**Persistent Volumes (PV):** Cluster-wide storage resources

**Persistent Volume Claims (PVC):** Requests for storage by users

**Storage Classes:** Define storage types (e.g., SSD, HD) for dynamic provisioning

## **Architecture:**

### **Kubernetes follows a Master-Worker model:**

The **control plane (master)** handles cluster-wide decisions, such as scheduling and responding to events.

**Worker Nodes** executes application workloads, managed by the control plane.

Communication occurs via Kubernetes API, with tools like kubectl (CLI) or client libraries interacting with the kube-apiserver

#### **Control Plane Components**

The Control Plane is responsible for maintaining the desired state of the cluster. It runs on Master Nodes and consists of several that work together to manage the cluster.

##### **API Server (kube-apiserver)**

**Function:** The Front-end for the Kubernetes control plane. It exposes the Kubernetes API, which is used by users, CLI tools like (kubectl), and other components to interact with the cluster.

**Details:**

* Processes RESTful API requests (e.g., create, update, delete resources like pods, services).
* Validates and stores object in etcd
* Acts as a communication hub between all components

Example: When you run kubectl apply -f deployment.yaml, the API server processes the request and updates the cluster state.

##### **etcd**

**Function:** A highly available, distributed key-value store that holds the cluster’s configuration data and state.

**Details:**

* Stores all Kubernetes objects (e.g., Pods, Deployments, ConfigMaps)
* Provides a single source of truth for the cluster
* Uses a watch mechanism to notify components of state changes
* Typically deployed as a stack of etcd instances for high availability

Example: If a pod is scheduled, its metadata (e.g., name, namespace, status) is stored in etcd.

##### **Scheduler (kube-scheduler)**

**Function:** Assigns Pods to worker nodes based on resource requirements, policies, and constraints.

**Details:**

* Monitors the API server for unscheduled Pods
* Evaluates factors like resource availability (CPU, memory), node affinity/anti-affinity, taints and tolerations.
* Places Pods on suitable nodes and updates the Pod’s node assignment in etcd via the API server

Example: A pod requiring 2 CPU cores is scheduled on a node with sufficient available resources.

##### **Controller Manager (kube-controller-manager)**

**Function:** Runs controllers that monitor the cluster’s state and take corrective action to achieve the desired state.

**Details:**

Includes multiple controllers, such as:

* **Replication Controller:** Ensures that correct number of Pod replicas are running
* **Deployment Controller:** Manages rollouts and rollbacks of application updates
* **StatefulSet Controller:** Manages stateful applications
* **Node Controller:** Monitors node health and evicts Pods from failed nodes

Each controller watches etcd via the API server and reconciles the current state with the desired state.

Example: If a Pod in a deployment crashes, the Deployment Controller creates a new Pod to replace it.

##### **Cloud Controller Manager (cloud-controller-manager)**

**Function:** Integrates Kubernetes with Cloud Providers (e.g., AWS, GCP, Azure) for cloud-specific operations.

**Details:**

* Manages cloud resources like load balancers, storage volumes and node metadata
* Separates cloud-specific logic from core Kubernetes components

Example: Provisions an AWS Elastic Load Balancer when Kubernetes Service of Type LoadBalancer is created.

#### **Worker Node Component**

Worker nodes are the machines (Physical or Virtual) that run the application workloads. Each worker node hosts the following components:

##### **Kubelet**

**Function:** An agent that runs on each worker node and ensures containers are running as expected

**Details:**

* Communicates with the API server to receive Pod specifications
* Interacts with the container runtime (e.g., Docker, containerd) to start, stopor restart containers
* Monitors Pod health and reports status back to the API server
* Manages Pods created directly or via controllers (e.g., Deployments)

Example: If a container crashes, the Kubelet restarts it based on the Pod’s restart policy.

##### **Kube-Proxy**

**Function**: Manages network connectivity of Pods and Services on the worker node.

**Details:**

* Runs on every node and maintains network rules (e.g., iptables IPVS) to enable communication between Pods, Services and External clients.
* Support Service discovery and load balancing for Services.
* Implements Service Types like ClusterIP, NodePort or LoadBalancer

Example: For a Service with three pods, kube-proxy ensures client traffic is load-balanced across the pods.

##### **Container Runtime**

**Function:** The software responsible for running containers

**Details:**

* Kubernetes supports multiple container runtimes, such as Docker, containerd, or CRI-O.
* The Kubelet uses the container runtime to manage container lifecycle (e.g., pull images, start/stop containers)
* Must conform to the Container Runtime Interface (CRI)

**Example:** Pull a container image from registry like Docker Hub and starts it as a container.

## **Setting up a Kubernetes Cluster**

Setting up a Kubernetes cluster with one master node and two worker nodes involves installing and configuring the necessary software on each node, initializing the control plane on the master node, joining the worker nodes to the cluster, and verifying the setup.

Below is a detailed, step-by-step guide to accomplish this using **Ubuntu 22.04 LTS** as the operating system, **kubeadm** as the cluster bootstrap tool, and containerd as the container runtime. This guide assumes you have basic Linux knowledge and access to three machines (physical or virtual).

### **Prerequisites**

**1. Hardware/VM Requirements:**

- Master Node: 2 CPUs, 2 GB RAM, 20 GB disk space.

- Worker Nodes: 1 CPU, 1 GB RAM, 20 GB disk space.

- Example: Three VMs running Ubuntu 22.04 LTS.

**2. Network Requirements:**

- All nodes must be on the same network with static IP addresses.

- Example IPs:

- Master Node: `192.168.1.100`

- Worker Node 1: `192.168.1.101`

- Worker Node 2: `192.168.1.102`

- Full network connectivity between nodes (ports like 6443, 10250, etc., must be open; see Kubernetes port requirements).

**3. Software Requirements:**

- Ubuntu 22.04 LTS installed on all nodes.

- SSH access to all nodes.

- `sudo` privileges for the user on each node.

**4. Tools:**

- `kubeadm`, `kubectl`, `kubelet` for cluster setup and management.

- `containerd` as the container runtime.

- A Container Network Interface (CNI) plugin (e.g., Calico) for Pod networking.

### **Step-by-Step Setup**

#### **Step 1: Prepare All Nodes**

Perform the following steps on **all three nodes** (Master, Worker 1, Worker 2) to configure the base environment.

**1. Update the System:**

```bash

sudo apt update && sudo apt upgrade -y

```

**2. Set Hostnames:**

Set unique hostnames for each node to avoid conflicts.

**- On Master Node:**

```bash

sudo hostnamectl set-hostname master-node

```

**- On Worker Node 1:**

```bash

sudo hostnamectl set-hostname worker-node1

```

**- On Worker Node 2:**

```bash

sudo hostnamectl set-hostname worker-node2

```

**3. Update `/etc/hosts`:**

Add entries to resolve node names to IPs.

```bash

sudo nano /etc/hosts

```

Add the following lines:

```

192.168.1.100 master-node

192.168.1.101 worker-node1

192.168.1.102 worker-node2

```

Save and exit.

**4. Disable Swap:**

Kubernetes requires swap to be disabled for performance and stability.

```bash

sudo swapoff -a

sudo sed -i '/ swap / s/^\(.\*\)$/#\1/g' /etc/fstab

```

**5. Load Kernel Modules:**

Enable required kernel modules for container networking.

```bash

cat <<EOF | sudo tee /etc/modules-load.d/containerd.conf

overlay

br\_netfilter

EOF

sudo modprobe overlay

sudo modprobe br\_netfilter

```

**6. Configure Sysctl Parameters:**

Enable networking settings for Kubernetes.

```bash

cat <<EOF | sudo tee /etc/sysctl.d/99-kubernetes-cri.conf

net.bridge.bridge-nf-call-iptables = 1

net.ipv4.ip\_forward = 1

net.bridge.bridge-nf-call-ip6tables = 1

EOF

sudo sysctl --system

```

**7. Install containerd:**

Install and configure `containerd` as the container runtime.

```bash

sudo apt install -y containerd

sudo mkdir -p /etc/containerd

containerd config default | sudo tee /etc/containerd/config.toml

```

Edit the `config.toml` to enable the `SystemdCgroup` driver for Kubernetes compatibility:

```bash

sudo nano /etc/containerd/config.toml

```

Find the `[plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc.options]` section and set:

```toml

SystemdCgroup = true

```

Save and exit. Restart containerd:

```bash

sudo systemctl restart containerd

sudo systemctl enable containerd

```

**8. Install Kubernetes Components:**

Install `kubeadm`, `kubelet`, and `kubectl`.

```bash

sudo apt update

sudo apt install -y apt-transport-https ca-certificates curl

curl -fsSL https://pkgs.k8s.io/core:/stable:/v1.29/deb/Release.key | sudo gpg --dearmor -o /etc/apt/keyrings/kubernetes-apt-keyring.gpg

echo 'deb [signed-by=/etc/apt/keyrings/kubernetes-apt-keyring.gpg] https://pkgs.k8s.io/core:/stable:/v1.29/deb/ /' | sudo tee /etc/apt/sources.list.d/kubernetes.list

sudo apt update

sudo apt install -y kubelet kubeadm kubectl

sudo apt-mark hold kubelet kubeadm kubectl

```

- This installs Kubernetes version 1.29 (adjust the version if needed).

- `apt-mark hold` prevents accidental upgrades.

#### **Step 2: Initialize the Control Plane on the Master Node**

Perform these steps \*\*only on the Master Node\*\* (`master-node`).

**1. Initialize the Cluster with kubeadm:**

Initialize the control plane, specifying the Pod network CIDR (required for the CNI plugin).

```bash

sudo kubeadm init --pod-network-cidr=192.168.0.0/16 --apiserver-advertise-address=192.168.1.100

```

- `--pod-network-cidr=192.168.0.0/16`: Defines the IP range for Pods (used by Calico).

- `--apiserver-advertise-address=192.168.1.100`: The master node’s IP.

- Output: The command generates a join command for worker nodes, which looks like:

```

kubeadm join 192.168.1.100:6443 --token <token> --discovery-token-ca-cert-hash sha256:<hash>

```

Save this command for Step 4.

**2. Set Up kubectl for the User:**

Configure the `kubectl` command-line tool to interact with the cluster.

```bash

mkdir -p $HOME/.kube

sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config

sudo chown $(id -u):$(id -g) $HOME/.kube/config

```

**3. Verify the Control Plane:**

Check that the control plane components are running.

```bash

kubectl get pods -n kube-system

```

- You’ll see Pods like `kube-apiserver`, `kube-controller-manager`, `kube-scheduler`, and `etcd`, but the cluster isn’t fully functional yet because networking is missing.

#### **Step 3: Install a CNI Plugin (Calico) on the Master Node**

Kubernetes requires a network plugin to enable Pod-to-Pod communication. We’ll use Calico.

**1. Apply Calico Manifests:**

```bash

kubectl apply -f https://raw.githubusercontent.com/projectcalico/calico/v3.26.1/manifests/calico.yaml

```

- This deploys Calico Pods and configures the Pod network.

**2. Verify Networking:**

Wait for Calico Pods to be in the “Running” state.

```bash

kubectl get pods -n kube-system

```

- Look for Pods like `calico-node` and `calico-kube-controllers`.

- This may take a few minutes as images are pulled.

**3. Check Cluster Status:**

Verify that the master node is ready.

```bash

kubectl get nodes

```

- Output:

```

NAME STATUS ROLES AGE VERSION

master-node Ready control-plane 5m v1.29.0

```

---

#### **Step 4: Join Worker Nodes to the Cluster**

Perform these steps on Worker Node 1 (`worker-node1`) and Worker Node 2 (`worker-node2`).

**1. Run the Join Command:**

Use the `kubeadm join` command from Step 2. For example:

```bash

sudo kubeadm join 192.168.1.100:6443 --token <token> --discovery-token-ca-cert-hash sha256:<hash>

```

- Replace `<token>` and `<hash>` with the values from the `kubeadm init` output.

- If the token has expired (valid for 24 hours), generate a new one on the master node:

```bash

kubeadm token create --print-join-command

```

**2. Repeat for Worker Node 2:**

Run the same `kubeadm join` command on `worker-node2`.

#### **Step 5: Verify the Cluster**

Perform these steps on the \*\*Master Node\*\*.

**1. Check Node Status:**

Verify that all nodes are in the “Ready” state.

```bash

kubectl get nodes

```

- Expected output:

```

NAME STATUS ROLES AGE VERSION

master-node Ready control-plane 10m v1.29.0

worker-node1 Ready <none> 2m v1.29.0

worker-node2 Ready <none> 1m v1.29.0

```

**2. Check Pods in kube-system Namespace:**

Ensure all control plane and networking Pods are running.

```bash

kubectl get pods -n kube-system

```

- Look for Pods like `kube-apiserver`, `kube-scheduler`, `calico-node`, etc., in the “Running” state.

**Step 6: Deploy a Test Application**

To confirm the cluster is functional, deploy a simple Nginx application.

**1. Create a Deployment:**

```bash

kubectl create deployment nginx --image=nginx --replicas=3

```

**2. Expose the Deployment:**

Create a Service to access the Nginx Pods.

```bash

kubectl expose deployment nginx --port=80 --type=NodePort

```

**3. Verify the Deployment:**

Check the Pods and Service.

```bash

kubectl get pods

kubectl get svc

```

- Output for Pods:

```

NAME READY STATUS RESTARTS AGE

nginx-6799fc88d8-abcde 1/1 Running 0 2m

nginx-6799fc88d8-fghij 1/1 Running 0 2m

nginx-6799fc88d8-klmno 1/1 Running 0 2m

```

- Output for Service:

```

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE

nginx NodePort 10.96.123.456 <none> 80:31234/TCP 1m

```

**4. Access the Application:**

Find the NodePort (e.g., 31234) and access Nginx on any worker node’s IP.

```bash

curl http://192.168.1.101:31234

```

- You should see the Nginx welcome page HTML.

---

#### **Step 7: (Optional) Install a Dashboard**

To visualize the cluster, install the Kubernetes Dashboard.

**1. Deploy the Dashboard:**

```bash

kubectl apply -f https://raw.githubusercontent.com/kubernetes/dashboard/v2.7.0/aio/deploy/recommended.yaml

```

**2. Create an Admin User:**

Create a file `dashboard-admin.yaml`:

```yaml

apiVersion: v1

kind: ServiceAccount

metadata:

name: admin-user

namespace: kubernetes-dashboard

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRoleBinding

metadata:

name: admin-user

roleRef:

apiGroup: rbac.authorization.k8s.io

kind: ClusterRole

name: cluster-admin

subjects:

- kind: ServiceAccount

name: admin-user

namespace: kubernetes-dashboard

```

Apply it:

```bash

kubectl apply -f dashboard-admin.yaml

```

**3. Get an Access Token:**

```bash

kubectl -n kubernetes-dashboard create token admin-user

```

**4. Access the Dashboard:**

Start a proxy:

```bash

kubectl proxy

```

Open a browser and navigate to:

```

http://localhost:8001/api/v1/namespaces/kubernetes-dashboard/services/https:dashboard-kubernetes-dashboard:/proxy/

```

Log in using the token from the previous step.

---

#### **Troubleshooting Tips**

**- Nodes Not Ready:**

- Check `kubectl get nodes` and `kubectl describe node <node-name>` for errors.

- Verify `containerd` and `kubelet` services: `sudo systemctl status containerd kubelet`.

**- Networking Issues:**

- Ensure Calico Pods are running: `kubectl get pods -n kube-system`.

- Check firewall rules or cloud security groups for required ports (e.g., 6443 for API Server).

**- Join Command Expired:**

- Generate a new join command: `kubeadm token create --print-join-command`.

**- Pod Scheduling Issues:**

- Ensure the CNI plugin is installed and Pods have IPs: `kubectl get pods -o wide`.

#### **Summary of Cluster Components**

**- Master Node (`master-node`):**

- Runs control plane components: `kube-apiserver`, `kube-controller-manager`, `kube-scheduler`, `etcd`.

- Runs `kubelet`, `kube-proxy`, and `containerd`.

- Hosts Calico Pods for networking.

**- Worker Nodes (`worker-node1`, `worker-node2`):**

- Run `kubelet`, `kube-proxy`, and `containerd`.

- Host application Pods (e.g., Nginx) and Calico Pods.

#### **Next Steps**

**- High Availability:** For production, set up multiple master nodes for control plane redundancy.

**- Monitoring:** Deploy Prometheus and Grafana for cluster monitoring.

**- Storage:** Configure a storage class for persistent volumes.

**- Ingress:** Set up an Ingress controller (e.g., NGINX) for advanced routing.

# Comparison between Docker and Kubernetes

Docker and Kubernetes are both essential tools in the world of containerization and cloud-native applications, but they serve different purposes. Below is a detailed comparison:

## **Overview**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Docker** | **Kubernetes** |
| Primary Role | Container runtime (build, ship, run containers) | Container orchestration (managing cluster of containers) |
| Developed By | Docker Inc | Google (later donated to CNCF – Cloud Native Computation Foundation) |
| Release Year | 2013 | 2014 |
| Key Purpose | Create and run containers | Automate deployment scaling and management of containers |

## **Core Functionality**

**Docker**

**Containerization:** Packages applications and dependencies into lightweight, portable containers.

**Docker Engine:** Runtime that builds and runs containers

**Dockerfile:** Defines how to build a container image

**Docker Hub:** Registry for sharing container images

**Single-Node Focus:** Works on a single machine (though Docker Swarm provides clustering)

**Kubernetes**

**Orchestration:** Manages multiple containers across multiple hosts

**Cluster Management:** Handles scheduling, scaling, failover and load balancing

**Declarative Configuration:** Uses YAML/JSON files to define desired state

**Multi-Node Focus:** Designed for distributed systems (cloud/on-prem clusters)

## **Key Features**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Docker** | **Kubernetes** |
| Container Management | Manages individual containers | Manages clusters of containers |
| Scaling | Limited (Docker Swarm can scale) | Auto-scaling (horizontal & Vertical) |
| Load Balancing | Basic (via Docker Swarm) | Advanced (Services, Ingress) |
| Networking | Docker-native networking | Plugins (CNI) for advanced Networking |
| Storage | Volumes for local storage | Persistent Volumes (PVs) for distributed storage |
| Self-Healing | Limited (restart policies) | Auto-replacement of failed containers |
| Rollouts & Rollbacks | Manual (Docker Swarm supports rolling updates) | Automated (Deployments, StatefulSets) |
| Service Discovery | Basic (via Docker Swarm) | Built-in (DNS-based) |

## **Architecture**

**Docker**

**Docker Daemon:** Background service managing containers

**Docker Client:** CLI for interacting with the daemon

**Docker Images:** Immutable templates for containers

**Docker Swarm:** Native Clustering (less popular than K8s)

**Kubernetes**

**Control Plane:** Manages cluster (API Server, Scheduler, Controller Manager, etcd)

**Worker Nodes:** Run containers via kubelet

**Pods:** Smallest deployable units (one or more containers)

**Services:** Expose Pods as network services

**Ingress:** Manages external access to services

## **When to use which?**

|  |  |  |
| --- | --- | --- |
| **Use Case** | **Docker** | **Kubernetes** |
| Local Development | Best for local testing | Overkill |
| Single-Node Deployment | Simple Deployments | Not Needed |
| Microservice at Scale | Limited orchestration | Best choice |
| CI/CD Pipeline | Build & Test containers | Deploy & Mange in Production |
| Hybrid/Cloud Deployments | Nees Swarm | Cloud-native support |

## **Can they work together?**

Yes! Docker creates containers, Kubernetes manages them.

Docker can run inside a Kubernetes cluster (though Kubernetes also supports other runtimes like containerd)

Docker Desktop includes a lightweight Kubernetes Cluster for local testing

## **Alternatives**

|  |  |  |
| --- | --- | --- |
| **Category** | **Docker Alternatives** | **Kubernetes Alternatives** |
| Competitors | Podman, containerd, LXC | Docker Swarm, Nomad, Mesos |
| Cloud Services | AWS, ECS, Azure Container Instances | AWS EKS, GKE, AKS |
|  |  |  |

## **Conclusion**

Docker is ideal for building and running containers on a single host.

Kubernetes is best for orchestrating containers across clusters in production.

They complement each other: Docker handles containerization, while Kubernetes manages deployment and scaling.