**Terraform**

**Terraform:**

Terraform is a product by Hashicorp that uses Infrastructure as Code (IaC) to provision cloud infrastructure.

It lets you define resources and infrastructure in human-readable, declarative configuration files, and manages your infrastructure's lifecycle.

**What is Terraform?**

Terraform is an IaC tool that allows users to provision and manage infrastructure resources across various cloud platforms and on-premises environments. It uses declarative configuration files, written in HashiCorp Configuration Language (HCL) or JSON, to define and automate the lifecycle of resources, ensuring predictability and consistency. Terraform’s extensible plugin-based architecture supports a wide range of providers, enabling seamless integration and management of diverse infrastructure environments.

**What is Infrastructure as Code with Terraform?**

Infrastructure as Code (IaC) tools allow you to manage infrastructure with configuration files rather than through a graphical user interface. IaC allows you to build, change, and manage your infrastructure in a safe, consistent, and repeatable way by defining resource configurations that you can version, reuse, and share.

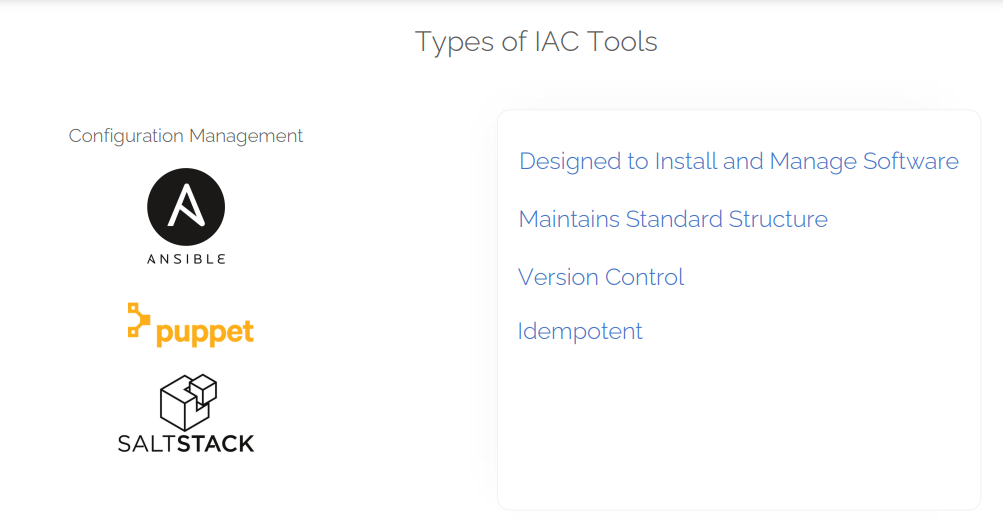
* Terraform can manage infrastructure on multiple cloud platforms.
* The human-readable configuration language helps you write infrastructure code quickly.
* Terraform's state allows you to track resource changes throughout your deployments.
* You can commit your configurations to version control to safely collaborate on infrastructure.

**Popular IaC Tools:**

1. **Terraform** An open-source declarative tool that offers pre-written modules to build and manage an infrastructure.  
   **2. Chef:** A configuration management tool that uses cookbooks and recipes to deploy the desired environment. Best used for Deploying and configuring applications using a pull-based approach.  
   **3. Puppet:** Popular tool for configuration management that follows a Client-Server Model. Puppet needs agents to be deployed on the target machines before the puppet can start managing them.  
   **4. Ansible:** Ansible is used for building infrastructure as well as deploying and configuring applications on top of them. Best used for Ad hoc analysis.  
   **5. Packer:** Unique tool that generates VM images (not running VMs) based on steps you provide. Best used for Baking compute images.  
   **6. Vagrant:** Builds VMs using a workflow. Best used for Creating pre-configured developer VMs within VirtualBox.

A screenshot of a computer

Description automatically generated

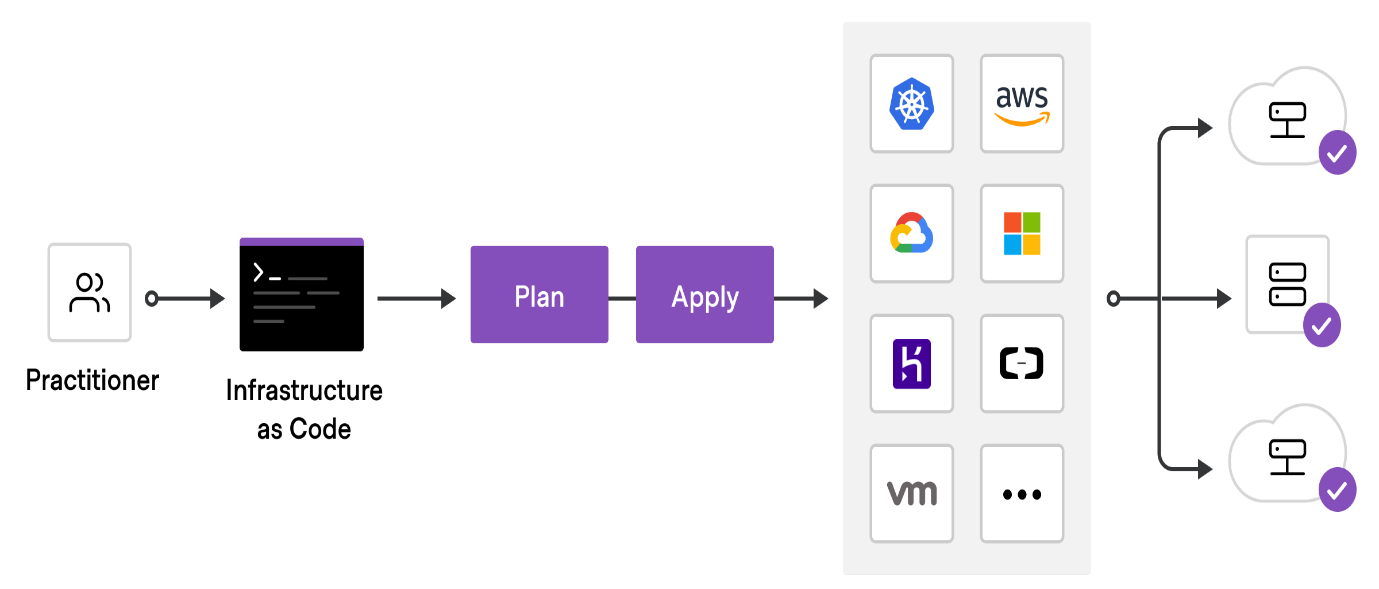


A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Terraform deployment workflow:** 

**Terraform Lifecycle:**

Terraform lifecycle consists of – init, plan, apply, and destroy.

* 1. **Terraform init** initializes the (local) Terraform environment. Usually executed only once per session.
  2. **Terraform plan**compares the Terraform state with the as-is state in the cloud, build and display an execution plan. This does not change the deployment (read-only).
  3. **Terraform apply**executes the plan. This potentially changes the deployment.
  4. **Terraform destroy**deletes all resources that are governed by this specific terraform environment.

**Terraform Core Concepts**

**1. Variables**: Terraform has input and output variables, it is a key-value pair. Input variables are used as parameters to input values at run time to customize our deployments. Output variables are return values of a terraform module that can be used by other configurations.  
Read our blog on [**Terraform Variables**](https://k21academy.com/terraform-iac/variables-in-terraform/)

**2. Provider**: Terraform users provision their infrastructure on the major cloud providers such as AWS, Azure, OCI, and others. A *provider* is a plugin that interacts with the various APIs required to create, update, and delete various resources.  
Read our blog to know more about [**Terraform Providers**](https://k21academy.com/terraform-iac/terraform-providers-overview/)

**3. Module**: Any set of Terraform configuration files in a folder is a *module*. Every Terraform configuration has at least one module, known as its ***root module.***

**4. State**: Terraform records information about what infrastructure is created in a Terraform *state* file. With the state file, Terraform is able to find the resources it created previously, supposed to manage and update them accordingly.

**5. Resources**: Cloud Providers provides various services in their offerings, they are referenced as Resources in Terraform. Terraform resources can be anything from compute instances, virtual networks to higher-level components such as DNS records. Each resource has its own attributes to define that resource.

**6. Data Source**: Data source performs a read-only operation. It allows data to be fetched or computed from resources/entities that are not defined or managed by Terraform or the current Terraform configuration.

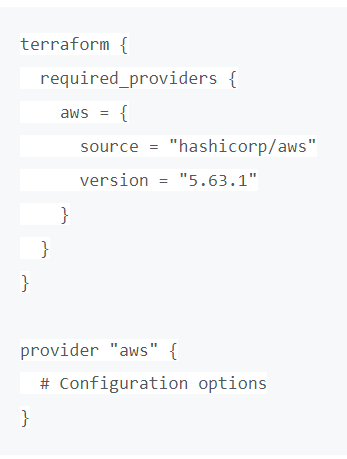
**7. Plan**: It is one of the stages in the Terraform lifecycle where it determines what needs to be created, updated, or destroyed to move from the real/current state of the infrastructure to the desired state.

**8. Apply**: It is one of the stages in the Terraform lifecycle where it applies the changes real/current state of the infrastructure in order to achieve the desired state.

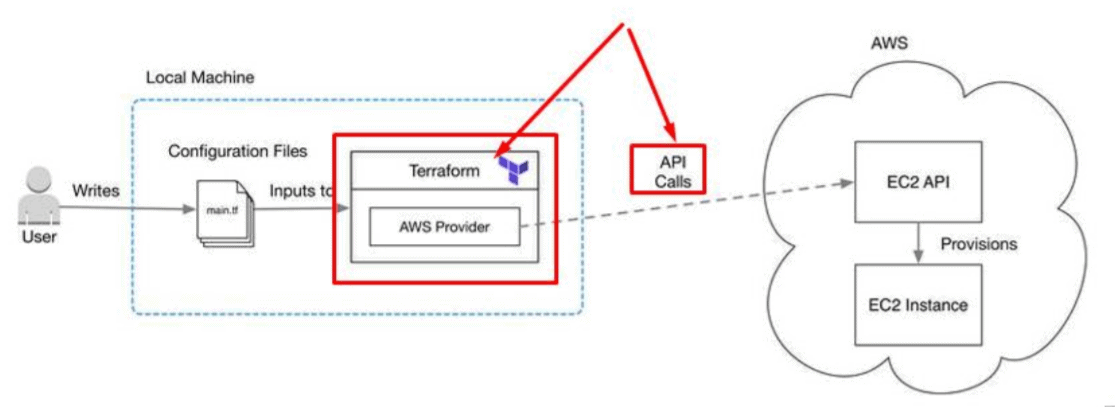
**Check Out:**Our previous blog post on [**Terraform Cheat Sheet**](https://k21academy.com/terraform-iac/terraform-cheat-sheet/).

**Terraform Providers:**

**Aws Provider**

****

A provider is responsible for understanding API interactions and exposing resources. It is an executable plug-in that contains code necessary to interact with the API of the service. Terraform configurations must declare which providers they require so that Terraform can install and use them.

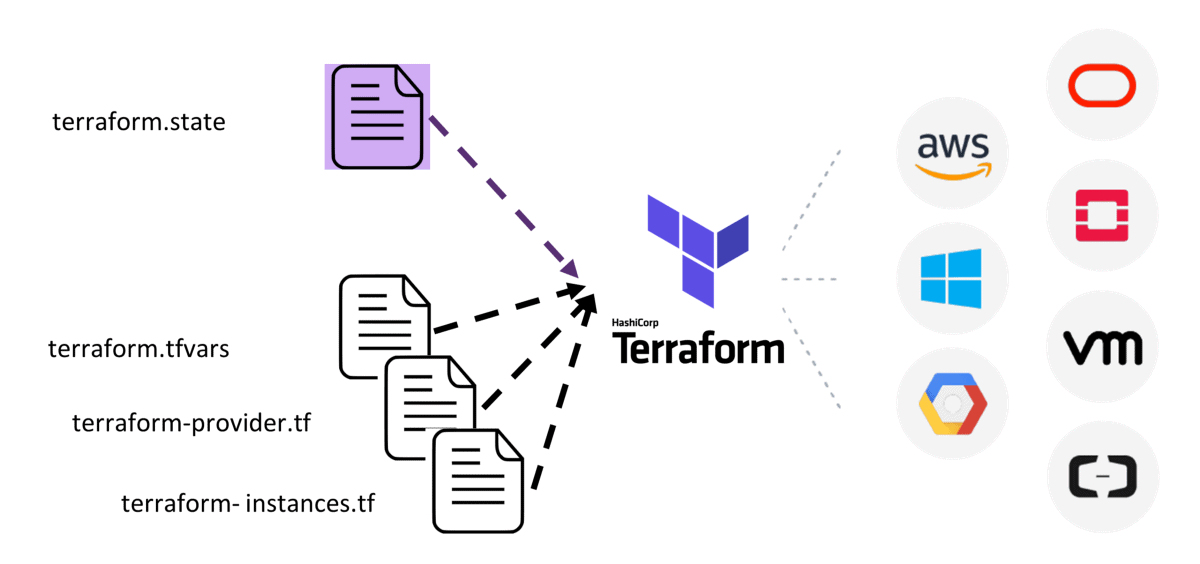


Terraform has over a hundred providers for different technologies, and each provider then gives terraform user access to its resources. So through AWS provider, for example, you have access to hundreds of AWS resources like EC2 instances, the AWS users, etc.

**Read More:**About [**Terraform Workflow**](https://k21academy.com/terraform-iac/terraform-workflow-and-its-use-case/).

**Terraform Configuration Files**

Configuration files are a set of files used to describe infrastructure in Terraform and have the file extensions **.tf** and **.tf.json**. Terraform uses a declarative model for defining infrastructure. Configuration files let you write a configuration that declares your desired state. Configuration files are made up of resources with settings and values representing the desired state of your infrastructure.



A Terraform configuration is made up of one or more files in a directory, provider binaries, plan files, and state files once Terraform has run the configuration.

**1. Configuration file (\*.tf files):** Here we declare the provider and resources to be deployed along with the type of resource and all resources specific settings

**2. Variable declaration file (variables.tf or variables.tf.json):** Here we declare the input variables required to provision resources

**3. Variable definition files (terraform.tfvars):** Here we assign values to the input variables

**4. State file (terraform.tfstate):** a state file is created once after Terraform is run. It stores state about our managed infrastructure.

**Also Read:**Our blog post on [**Terraform Create VM**](https://k21academy.com/terraform-iac/terraform-automate-aws-vm/).

For more information:  
https://k21academy.com/terraform-iac/terraform-beginners-guide/

**Terraform resources:**

**A computer screen with text

Description automatically generated**

**Terraform variables:**

Variables introduce the flexibility and dynamism needed to manage larger sets of infrastructure.

There are mainly three types of variables in Terraform – local, input, and output.

**Local variables:**

These are locally declared variables.

They provide a way to name any attribute value that needs to be used throughout the Terraform code. [Local variables](https://spacelift.io/blog/terraform-locals) are particularly useful when you need to reference the same values in multiple places within your Terraform configuration.

variables.tf main.tf

A computer screen shot of a program code

Description automatically generated

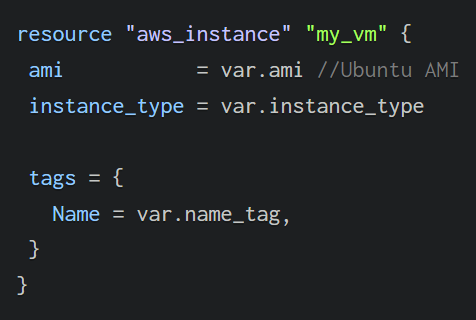
**A computer screen with text and symbols

Description automatically generated with medium confidence**

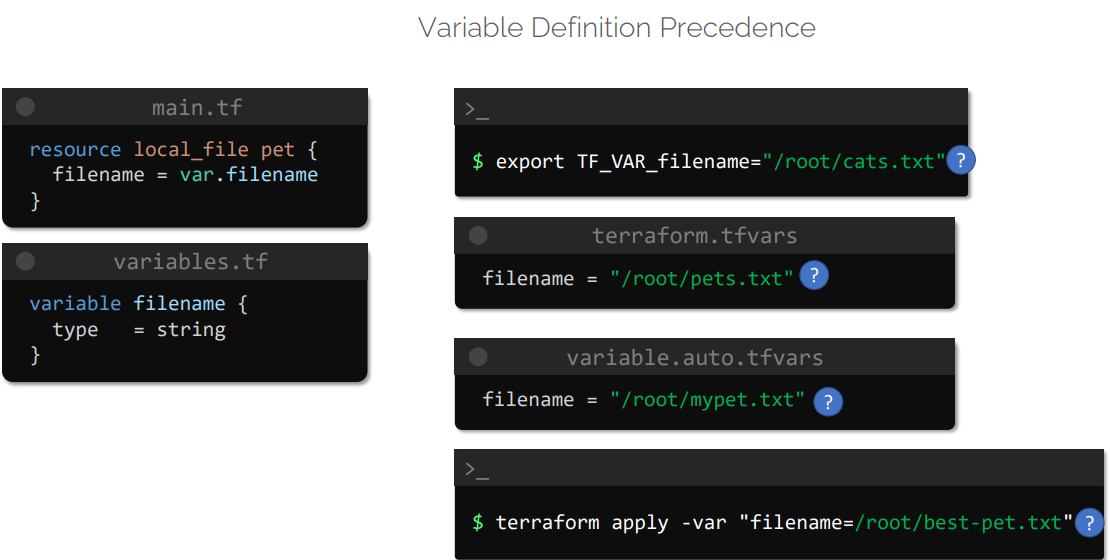
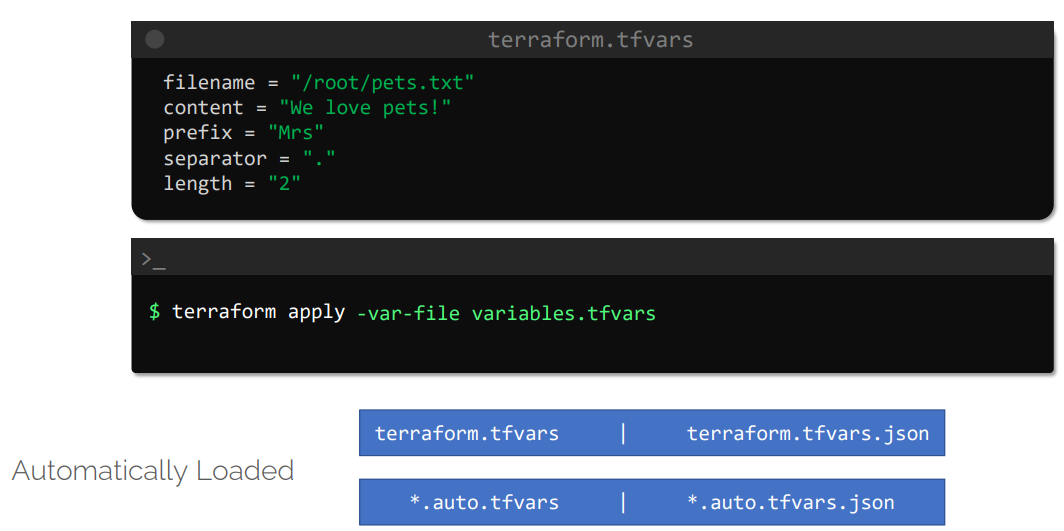
**Input variables**

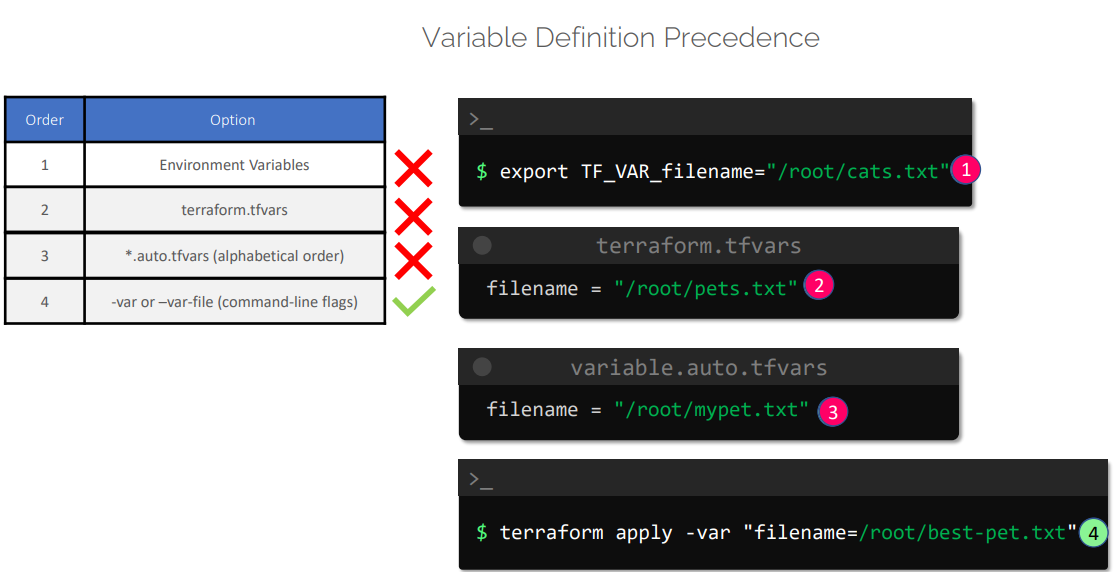
variables.tf main.tf

A screen shot of a computer program

Description automatically generated

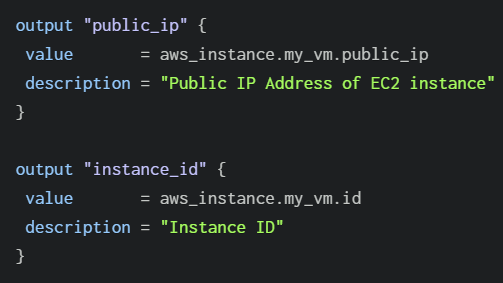
**Terraform.tfvars:**

A better way to manage these default values is to create another file named terraform.tfvars. Terraform automatically interprets tfvars as a group of key-value pairs and maps them with the declared variables in the variables.tf file. 



**Output Variables**

[Output Variables](https://spacelift.io/blog/terraform-output) provide a way to retrieve the details we are interested in directly in the CLI terminal. Additionally, output variables “return” values to the parent modules for further processing.



**Terraform Commands:**

1. **terraform validate**
2. **terraform fmt**
3. **terraform show**
4. **terraform providers**
5. **terraform output**
6. **terraform refresh**
7. **terraform graph**

**Terraform State management:**

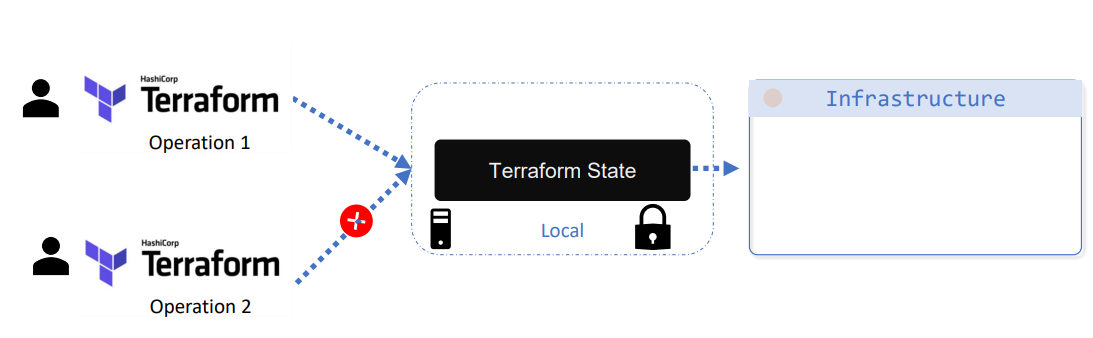
State management in Terraform is one of the crucial things to know and learn about especially when working with teams

1. terraform.tfstate
2. terraform.tfstate.backup

**State lock file**

There is one more file involved in all of this – .terraform.tfstate.lock.info.

**State Locking**

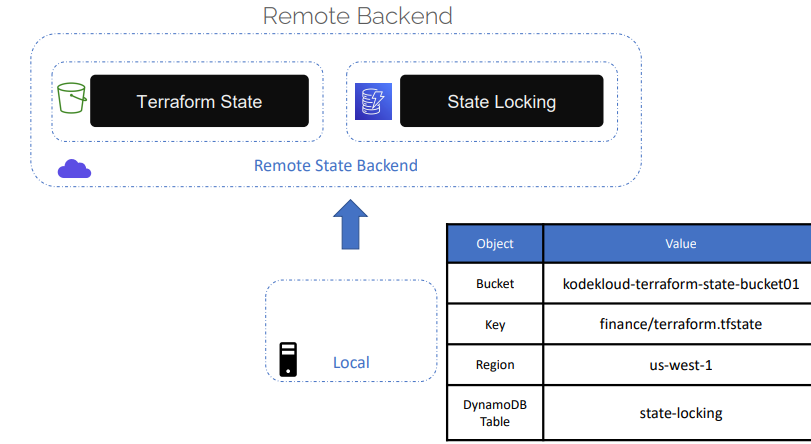


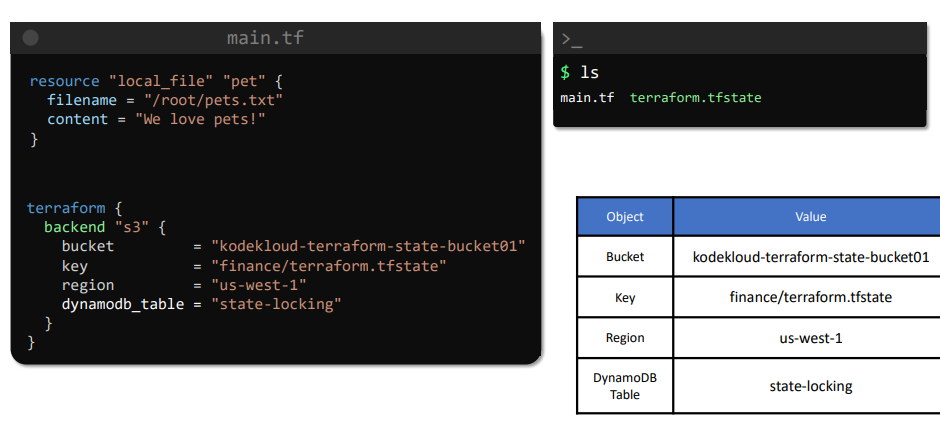
A screenshot of a computer

Description automatically generated

A screenshot of a state locking system

Description automatically generated





A screenshot of a computer program

Description automatically generated

A computer screen with text on it

Description automatically generated

**Terraform Taint**

**Debugging:**

Log Levels

**#export TF\_LOG=TRACE**

**Terraform Import**

**Data Source:**

****

**Terraform Modules:**

Modules are containers for multiple resources that are used together. A module consists of a collection of .tf and/or .tf.json files kept together in a directory.

Modules are the main way to package and reuse resource configurations with Terraform.

**Terraform AWS modules**

<https://registry.terraform.io/namespaces/terraform-aws-modules>

<https://github.com/terraform-aws-modules>

**Terraform Functions:**

|  |  |
| --- | --- |
| **Function Type** | **Description** |
| **String** | **String related operations (format, join, split)** |
| **Numeric** | **Numeric related operations (min, max, pow)** |
| **Collection** | **Functions that manipulate lists, tuples, sets and maps (length, lookup, merge)** |
| **Date and Time** | **Manipulate date and time (formatdate, timestamp)** |
| **Crypto and Hash** | **Crypto and Hash functions (base64sha512, bcrypt)** |
| **Filesystem** | **File system operations (file, filexists, abspath)** |
| **Ip Network** | **Network Cidr functions (cidrsubnet, cidrhost)** |
| **Encoding** | **Encoding and decoding functions (base64decode, base64encode, jsonencode)** |
| **Type Conversion** | **Functions that convert data types (tobool, tomap, tolist)** |

Please follow the below link for more details.

<https://spacelift.io/blog/terraform-functions-expressions-loops>

<https://developer.hashicorp.com/terraform/language/functions>

**Terraform Workspaces:**

****

Refer the below link for more information:

<https://spacelift.io/blog/terraform-workspaces>

**Terraform Project**

**1.  Terraform Project with Aws resources.**

Q. Create AWS EC2 instance by supplying arguments with variables and use data source to grab the AMI (Latest ami of amazon linux) from the aws. Access the html file in the shell scripting and run  it( add data file to access shell script) and also add security groups with inbound rules as http?

A.

**main.tf:**

**#terraform provider.**

terraform {

required\_providers {

aws = {

source = "hashicorp/aws"

version = "5.64.0"

}

}

}

provider "aws" {

region = var.region

}

**#aws ec2 instance block**

resource "aws\_instance" "web" {

ami = data.aws\_ami.linux.id

instance\_type = var.Instance\_type

tags = {

Name = "Linux"

}

}

**#Data resource block to grab the latest ami**

data "aws\_ami" "linux" {

most\_recent = true

owners = ["amazon"]

filter {

name = "architecture"

values = ["arm64"]

}

filter {

name = "name"

values = ["amzn2-ami-hvm-\*-x86\_64-gp2"]

filter {

name = “virtualization”

values= [“hvm”]

}

}

#allow security groups with inbound rules

resource "aws\_security\_group" "example" {

# ... other configuration ...

ingress {

description = "HTTPS ingress"

from\_port = 443

to\_port = 443

protocol = " tcp"

cidr\_blocks = ["0.0.0.0/0"]

ipv6\_cidr\_blocks = ["::/0"]

}

egress {

from\_port = 0

to\_port = 0

protocol = "-1"

cidr\_blocks = ["0.0.0.0/0"]

ipv6\_cidr\_blocks = ["::/0"]

}

}

**#local file to call shell script.**

resource "local\_file" "foo" {

content = "foo!"

filename = "${path.module}/foo.bar"

}

**variables.tf:**

**#variable block**

variable " region" {

type = string

default = “us-east-1 "

}

variable “Instance\_type” {

type= string

default=”t2.micro”

}

**shellscript.sh:**

**#shell script**

Q. Create S3 buckets with policy and enable the static website host and enable versioning.

A.

#create s3 bucket

resource "aws\_s3\_bucket" "example" {

bucket = "my-tf-test-bucket"

}

}

Q. Create VPC using modules.

    Add 2 availability zone and 2 public and private subnets and create database subnets

    Attach internet and nat gateway and also use tfvars file for giving the variable?

Q. Create RDS and use null resources and also use locals and use environment variables?

**Docker**

Docker is containerization technology tool.

Kubernetes is container orchestration tool.

**Docker is a container runtime.**

**Containerization:**  
 Its all about deploy application with required dependencies is known as containerization.

**Kubernetes:**

Kubernetes is a platform for running and managing container for many(100’s of) containers runtimes.

**Virtualization:**

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

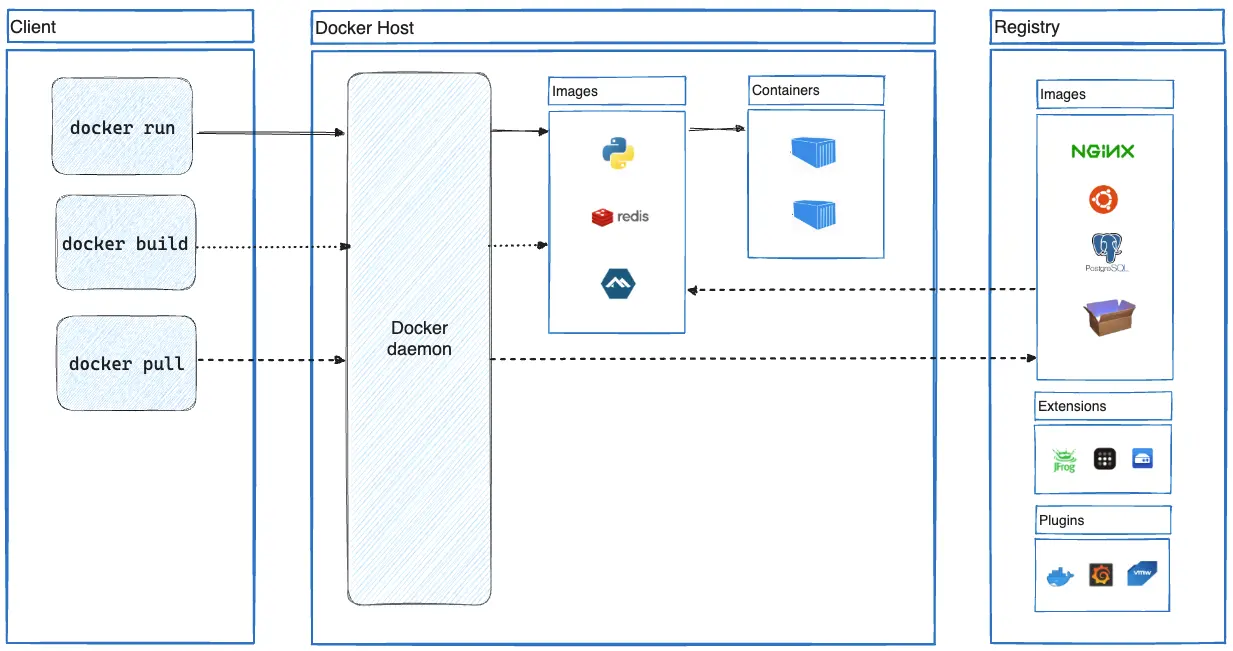
**Container Engine:**

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

Tool:

Docker, Jail, Crio.

**Docker Architecture:**



**Docker CLI/Client:**

Docker client is used to interact with docker hub to interact with images or containers.

* **Docker pull :** It helps to get the images from docker hub into the server.
* **Docker build:** To create docker images.
* **Docker run:** To create the containers from the images.

**Docker Daemon (Docker service):**

Docker daemon manages all the services by communicating with other daemons. 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**

A Docker host is a type of machine that is responsible for running more than one container. It comprises the Docker daemon, Images, Containers, Networks, and Storage.

**Docker Registry**

All the docker images are stored in the docker registry.

**Registry** : It is a collection of all dependencies and docker container images

**Docker pull:** It helps to download the images or dependencies from registry on to the docker host.

Docker pull <image name:version>

**Docker Images**

An image contains instructions for creating a docker container. It helps to create container from docker images and it is used to store and ship applications.

**Docker Containers**

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 have to follow 3 steps (or) activities.

1. Start the docker services.

Ex: service docker start

1. Enable docker services at boot time.

chkconfig docker on

1. 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 >

1. 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 layer 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"]

1. Excute it (Image build process)

Commad:

Docker image build –tag <image\_name > <docker file path>

1. Result: docker ps
2. Then push to docker hub.

**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.
* **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.

For more information about docker installations:

<https://docs.docker.com/get-started/docker-concepts/building-images/writing-a-dockerfile/>

**Docker Networking**

Docker Networking allows you to create a Network of Docker Containers managed by a master node called the manager.   
A network is a group of two or more devices that can communicate with each other either physically or virtually.

The Docker network is a virtual network created by Docker to enable communication between Docker containers.

If two containers are running on the same host they can communicate with each other without the need for ports to be exposed to the host machine.

**Network Drivers:**

There are several default network drivers available in Docker.

Command to check docker networks list.

**docker network ls**

**Types of Network Drivers:**

**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.

**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.

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

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

**ipvlan:** Users have complete control over both IPv4 and IPv6 addressing by using the IPvlan driver.

**macvlan:** macvlan driver makes it possible to assign MAC addresses to a container.

Network Drivers

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.

**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**

**Kubernetes**

**Kubernetes:**

Docker is container platform

Kubernetes is a container orchestration platform

**Docker**

Docker has container runtime, which will allows you to run container or manage the life cycle of the container.

**Container is ephemeral** - short life, containers can die or revive anytime.

**Auto healing** - Auto-healing refers to the capability of a system to automatically detect and recover from failures, ensuring continuous operation with minimal manual intervention.

1. **Single host nature of docker container** - it might causes containers will not respond or die
2. **Auto healing** is not available in docker
3. **Auto scaling** - missing
4. **Enterprise level support**.

* Auto scaling
* Auto healing
* Load balancer support
* Firewall support
* Api support gateways
* White listing
* Black listing

**Kubernetes**

Kubernetes is a cluster.

Cluster is a group of nodes.

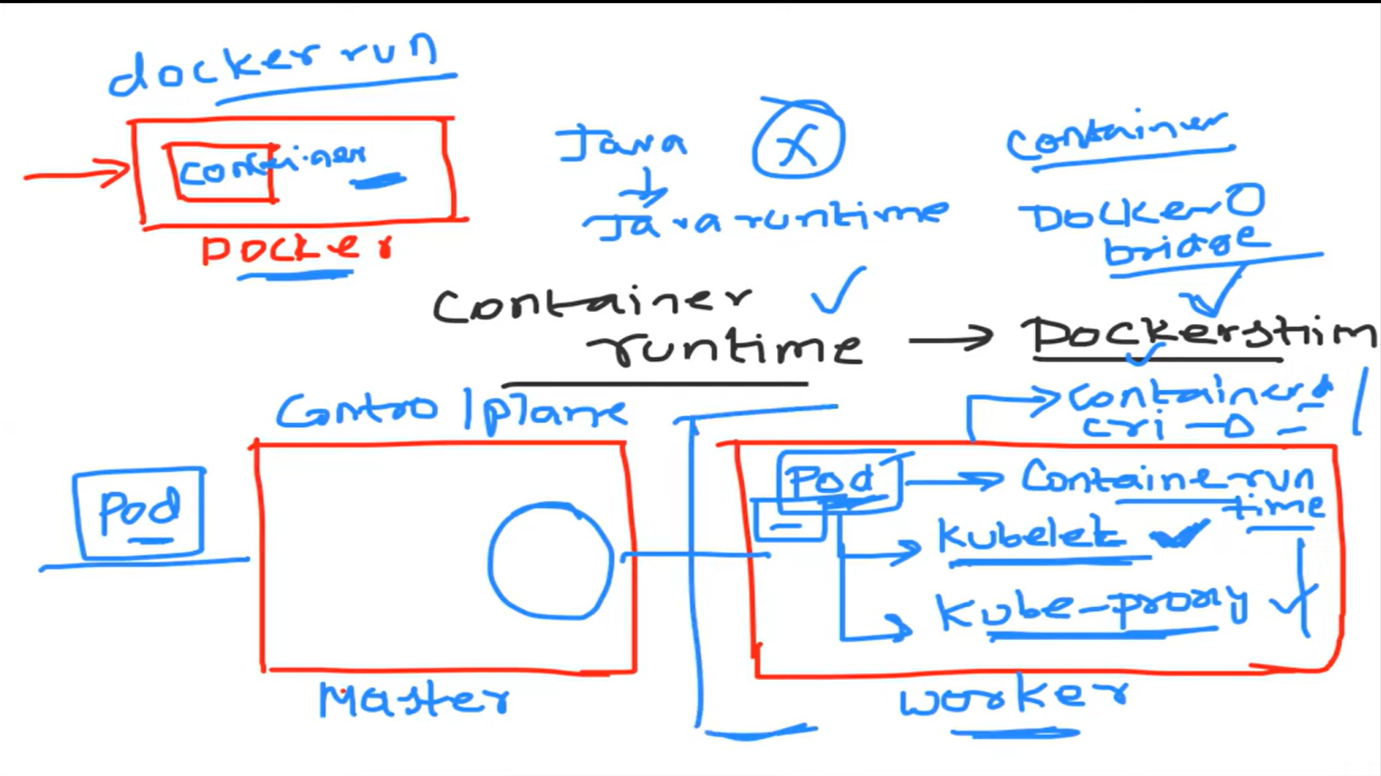
In production Kubernetes is installed as cluster.

1. If 1 pod or container is affecting because of another node, kubernetes will put the affected node into another node.
2. Using replicas set, we can achieve the auto scaling, it can be horizontal or vertical scaling.
3. Auto healing - if one container does down, whenever api server received the signal container is going down, immediately api server will create new container or roll out the new container.
4. Enterprise level support.

**Kubernetes architecture:**

A diagram of a computer

Description automatically generated



**Node Components**

**Kubelet:**

This is responsible for creation of pods and ensuring that pods are in running state.

An agent that runs on each node, ensuring that containers are running in a pod.

**Container Runtime:**

It will run the containers or pods

Manages the lifecycle of containers. Kubernetes supports container runtimes like containerd and CRI-O or docker shim (Docker runtime)

**kube-proxy:**

It is similar like docker default network- bridge network.

Kube-proxy is basically about configureing the network rules on each of the node in cluster.

Kube-proxy works by maintaining a set of network rules on nodes, allowing network communication to your pods.

It provides networking, IP address and load balancing capabilities to pods

This component will distribute to pods

Linux has concept called IP tables.

We can configure kube-proxy in different modes, but by default one is kube-proxy updates the IP tables, so when ever somebody access the application, let's say your service is on node port mode.

So if they access the URL or if they hit the URL, node port : (colon) port number. the kube proxy because it has configured the IP tables. The request is sent from that specific node IP colon port to the pod. Okay. So this entire routing is done using the kernel and the IP tables. So you can also use ipvs and other things. But by default mode is ip tables in Kubernetes.

**Control Plane Components**

The brain of Kubernetes, managing the whole system.

1. **kube-apiserver**: The central management entity that exposes the Kubernetes API. It handles all REST operations to manage the cluster.

It will exposes to external world. It will take the request from external.

It will decided in which node pod should create.

It will gives the information.

For eg: user want to create a pod,

First API server will receive the request and it will decide in which node pod should create or it will check which node is free and it inform to create a specific node.

1. **etcd**: A consistent and highly-available key-value store used for all cluster data.

It will store the entire cluster information as objects or key value pair.

1. **kube-scheduler**: Assigns newly created pods to nodes based on resource requirements and other constraints.

It is responsible for scheduling the resources or pods in the cluster.

For eg: user want to create a pod,

First API server will receive the request and it will decide in which node pod should create or it will check which node is free and it inform to create a specific node.

Second Scheduler will do the action on specific node.

1. **kube-controller-manager**: Runs controller processes to regulate the state of the cluster, such as node and job controllers.

To automate it has controllers.

For eg: Replica set - it is maintaining state of pods

**Controller** will ensure that the actual state in the yaml manifest is same as desired state.

1. **cloud-controller-manager**: Integrates with cloud provider APIs to manage cloud-specific resources.

**Kubernetes pods:**

**What is pod?**

 Definition of how to run containers.

Pod contains single container or multiple containers.

**Multiple containers**

1. Init container.
2. Side-car container

Consider 2 containers inside the pod.

If multiple containers are inside the pod, the kubernetes will ensure that both of the containers have the advantages

Advantages:

1. Shared the network.
2. Shared storage

With the help of cluster IP address we can access containers inside pods.

Kube proxy will assign the cluster IP address to pod.

**Interview:**

1. How do you debug pod or applications issue in Kubernetes

* Kubectl describe pod <pod\_name>
* Kubectl logs <pod\_name>

1. Why do we need deployment?

* Pod yaml files doesn’t supports the auto healing and auto scaling features.
* Deployment has replica set it will helps to auto healing and auto scaling features.

1. What is difference container, pod and deployment?
2. What is difference between deployment and replica set?

* Replica set is Kubernetes controller that is the one implementing the auto scaling and auto healing feature of pods by saying the actual state in the deployment yaml manifest are the desired state in the deployment yaml manifest should be same on the cluster.

1. How to list out all the resources that are available in a particular namespace.

* Kubectl get all
* Kubectl get all -A (To list all namespaces.)



**Kubernates Service:**

[**https://www.harness.io/blog/kubernetes-services-explained**](https://www.harness.io/blog/kubernetes-services-explained)

**Kubernetes**[**Services**](https://kubernetes.io/docs/concepts/services-networking/service)**are API objects that enable network exposure for one or more cluster Pods.**

Kubernetes Services are resources that map network traffic to the Pods in your cluster. You need to create a Service each time you expose a set of Pods over the network, whether within your cluster or externally.

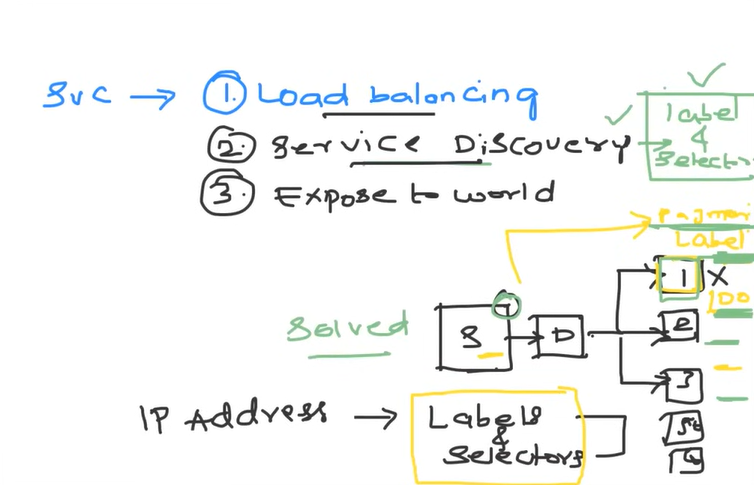
For each deployment yaml file we will create the service yaml file.

**Why service is required in the kubernates?**

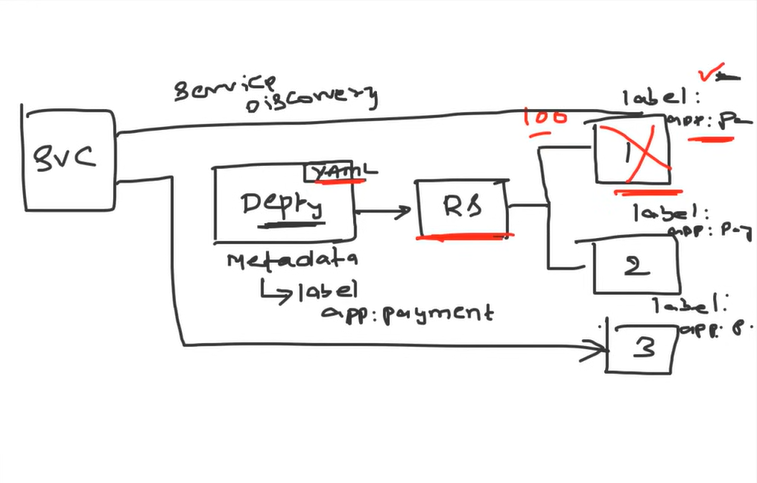
If service is not available, due some issues, pod has deleted and created again becuaseof auto healing. Pod ip address will change automatically, if ip address changes, we will not able to access the application with old ip address. In order to overcome this problem, we will create a service yaml file,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

**Service responsibilities.**

* Load balancing
* Service descovery machanism (using lables and selectors)
* Expose to the external world.



**Service discovery**

****

**Networking in K8s**

1. ClusterIP
2. NodePort Pull up for precise seeking
3. Load Balancer

**ClusterIP**

1. ClusterIP is the default type of service in Kubernetes.
2. This service type allows communication between different components inside the cluster.

* **Internal-only:** Not accessible from outside the cluster.
* **Automatic load balancing:** ClusterIP service automatically balances traffic between the pods it manages.
* **Default service type:** If no other type is specified, Kubernetes creates a ClusterIP service.

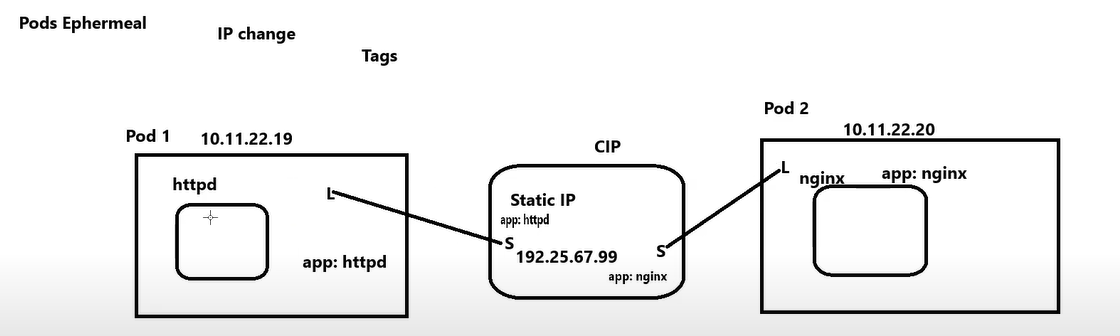
**ClusterIP Use Cases**

* Internal Communication Between Microservices
* **Example**: In an e-commerce application, a front-end service might need to communicate with a back-end API, and they can do so securely using ClusterIP.
* Database Access Within the Cluster
* Communication Between Pods in Different Namespaces

**How ClusterIP works**

Only internal, not external

For external we have NodePort and Load Balancer



**LoadBalancer:**

A diagram of a service

Description automatically generated

LoadBalancer is typically used in cloudenvironments to expose a serviceexternally

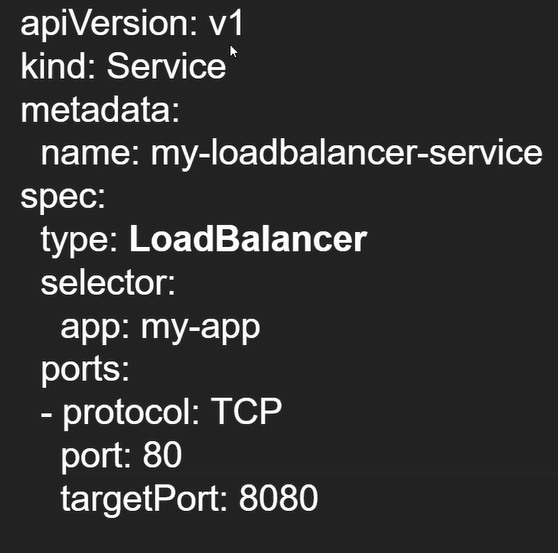
* LoadBalancer automatically provisions the external address to access your services outside the cluster.
* It works on AWS, GCP and Azure where you provision as external LoadBalancer
* On-premises may need provision manually.

**LoadBalancer Use-cases in K8s**

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

**How Load Balancer works in K8s?**

* Configure LoadBalancer as Service
* Distribute traffic to external IP

Eg:

**Advanatages of LoadBalancer:**

* **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.

**Ingress**:

* **Ingress** as a resource that manages external HTTP(S) access to services within a Kubernetes cluster
* Unlike NodePort or LoadBalancer services, Ingress offers more advanced features like path-based or host-based routing.
* Expose multiple services using a single external IP or domain

**Why do we use Ingress?**

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

**How ingress works?**

* **The ingress controller** is responsible for routing traffic based on defined rules.
* Routes external traffic to the correct internal service based on hostnames or paths.
* NGINX Ingress Controller, Traefik, and AWS ALB Ingress

A diagram of a diagram

Description automatically generated

A screenshot of a computer

Description automatically generated

Helm

Helmfile

Helmfile doesn’t come along with the installation.

We need to install helmfile using utilities separately.

Objects in kubernetes

Kubernetes objects are persistence entities in kubernetes system. Means if any pods will die, it will create new pods. Kubernetes will check every time whether the object or resources are running or not using API server.

Interview Questions

1. What is the **difference Docker and Kubernetes?**
   1. Docker is a container platform where as Kubernetes is a container orchestration environment that offers capabilities like Auto healing, Auto Scaling, Clustering and Enterprise level support like Load balancing.
2. What are the main **components of Kubernetes architecture?**

**A.** On a broad level, you can divide the kubernetes components in two parts

**1. Control Plane** (API SERVER, SCHEDULER, Controller Manager, C-CM, ETCD)

**2. Data Plane** (Kubelet, Kube-proxy, Container Runtime)

1. What are the main **differences between the Docker Swarm and Kubernetes?**
2. Kubernetes is better suited for large organisations as it offers more scalability,

networking capabilities like policies and huge third party ecosystem support.

1. What is the **difference between Docker container and a Kubernetes pod ?**
2. A pod in kubernetes is a runtime specification of a container in docker. A pod provides more declarative way of defining using YAML and you can run more than one container in a pod.
3. What is a **namespace in Kubernetes**?
4. In Kubernetes namespace is a logical isolation of resources, so that multiple project teams in a company can work on the same kubernetes cluster, but each of them will have a dedicated namespace, so that noboady will interrupt the work of the other people or other projects.

In Kubernetes namespace is a logical isolation of resources, network policies, rbac and everything. For example, there are two projects using same k8s cluster. One project can use ns1 and other project can use ns2 without any overlap and authentication problems.

1. What is the **role of kube proxy**?
2. Kube-proxy works by maintaining a set of network rules on each node in the cluster, which are updated dynamically as services are added or removed. When a client sends a request to a service, the request is intercepted by kube-proxy on the node where it was received. Kube-proxy then looks up the destination endpoint for the service and routes the request accordingly.

Kube-proxy is an essential component of a Kubernetes cluster, as it ensures that services can communicate with each other

1. What are the **different types of services within Kubernetes**?
2. There are three different types of services that a user can create.

1. Cluster IP Mode

2. Node Port Mode

3. Load Balancer Mode

1. What is the **difference between NodePort and Load Balancer type service**?
2. When a **service is created a** **NodePort type**, The kube-proxy updates the IP Tables with Node IP address and port that is chosen in the service configuration to access the pods.

Where as if you create a **Service as type Load Balance**r, the cloud control manager creates a external load balancer IP using the underlying cloud provider logic in the C-CM. Users can access services using the external IP

1. What is the role of **Kubelet**?
2. Kubelet manages the containers that are scheduled to run on that node. It ensures that the containers are running and healthy, and that the resources they need are available.

Kubelet communicates with the Kubernetes API server to get information about the containers that should be running on the node, and then starts and stops the containers as needed to maintain the desired state. It also monitors the containers to ensure that they are running correctly, and restarts them if necessary.

1. **What are the day to day activities on Kubernetes?**
2. As part of the devops engineer role we manage kubernetes clusters for our organization and we also ensure that you know the applications are deployed onto the kubernetes cluster and there are no issues with the application so we have set up monitoring on our Kubernetes cluster we ensure that whenever there are bugs on the kubernetes cluster for example uh the developers are not able to troubleshoot some issue with respect to pods developers are not able to troubleshoot with respect to Services they are not able to you know uh route the traffic in inside the Kubernetes cluster so in such cases as subject matter expertise on the Kubernetes Clusters we coming to picture and we solve their problems but apart from that we also do a lot of Maintenance activities for example uh we have kubernetes clusters with three Master nodes and 10 worker nodes so we have to do some continuous maintenance activities on this worker nodes probably uh you know upgrading the versions of this worker nodes or installing some default mandatory packages ensuring that these worker nodes are not uh security uh exposed to security vulnerabilities so all of these things are our day-to-day activities on Kubernetes apart from that we also serve as subject matter expertise on kubernetes so if anyone in the organization has any issues with kubernetes they create a jeera items for us or you know they create tickets for us and we will help them in solving or making them understand the concept of kubernetes so this is how you can explain so it is a very simple answer it's a very straightforward answer you don't have to you know get scared about this question so these are the 10 questions that I have for today and let us see how many people were able to get all the 10 questions correct because you know most of the questions we have covered I think eight questions we already covered in the previous videos so let us see what is the uh scorecard and uh yeah in future videos we will learn about Ingress we will learn about the Practical implementation of services we'll also talk about custom resources definitions we will see a few things about Helm so it's going to be four or five videos more on kubernetes and after that we'll also do a Kubernetes interview questions part two so if you like the video click on the like button and if you feel that someone who is not following our 45 days of devops course please share these videos with them so that they'll also get benefit out of the videos thank you so much I'll see in the next video take care everyone bye