Jenkins

1) Jenkins installation on Cloud and Server (VM) ?

Ans: For **Linux (Ubuntu/CentOS)**:

- I update the system, install Java (typically OpenJDK 11), then download and install Jenkins using the official Jenkins repo.
- I manage Jenkins as a **systemd service**, enabling it to auto-start on reboot.
- Commands

```
sudo apt update
sudo apt install openjdk-11-jdk -y
wget -q -O - https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
sudo sh -c 'echo deb https://pkg.jenkins.io/debian-stable binary/ >
/etc/apt/sources.list.d/jenkins.list'
sudo apt update
sudo apt install jenkins -y
sudo systemctl start jenkins
```

Jenkins Installation on **Cloud**

- AWS EC2 instances (manually and using automation tools like Terraform or Ansible).
- The installation process is nearly the same as on local VMs, but I ensure:
- Proper **security group/firewall rules** to allow port `8080` access.
- Set up **EBS volume (AWS)** or **managed disks (Azure)** for persistent Jenkins home

I always configure a **separate volume** for `/var/lib/jenkins` to back up job configurations.

- Use **Nginx or Apache** as a reverse proxy for TLS (HTTPS) setup.
- Secure Jenkins with **LDAP/SAML integration**, secrets management (Vault/SSM), and proper RBAC.

2) How do you **upgrade Jenkins**? Explain the steps and strategies (on On-Prem & vm) ?

Ans: When upgrading Jenkins (whether on an on-prem server or a VM), I follow a structured approach to **minimize downtime and ensure rollback is possible if needed**:

Step- 1: Take a Full Backup

- Backup the **entire Jenkins home directory**: /var/lib/jenkins/
- It contains jobs, plugins, configurations, credentials, and user data.
- Tools like `rsync`, `tar`, or Jenkins backup plugins can be used.

- Commands

  sudo systemctl stop jenkins

  sudo tar -czvf jenkins_backup_$(date +%F).tar.gz /var/lib/jenkins

  sudo systemctl start jenkins

Step 2: Note Current Version

- Record the current Jenkins version using:
- java -jar jenkins.war --version

Step 3: Check Plugin Compatibility

- Go to **Manage Jenkins** → **Plugin Manager** → **Updates**.
- Ensure critical plugins are compatible with the target Jenkins version.
- Upgrade important plugins first, especially Pipeline-related ones

Step 4: Download the Latest Jenkins

- manually download the new `.war` file if running Jenkins standalone:
- wget https://get.jenkins.io/war-stable/latest/jenkins.war

Step 5: Replace WAR File (if using WAR-based Jenkins)

- commands

  sudo systemctl stop jenkins
  sudo cp jenkins.war /usr/share/jenkins/jenkins.war
  sudo systemctl start jenkins

Step 6: Post-Upgrade Validation

- Access Jenkins UI.
- Verify:
  - Plugins are working
  - Jobs are intact
  - Credentials and users are retained
- Check logs:
- tail -f /var/log/jenkins/jenkins.log

Step- 7: Blue-Green Upgrade (Zero Downtime – Advanced)

- Spin up a new VM with the upgraded Jenkins version.
- Restore data from backup.
- Test and validate on the new instance.
- If successful, switch DNS or load balancer to point to the new server.

Step-8: In Case of Rollback

If issues are found post-upgrade:

- Stop Jenkins.
    - Restore from the tar backup.
    - Revert to previous WAR or reinstall the old version using `apt/yum`.

3) How Do You Take Backups in Jenkins (Server or VM), and What's the Process Post Backup for Jenkins Upgrade?

- When Jenkins is running on a standalone server or VM (not on managed cloud services), I follow this manual + automated backup strategy:
- What Do I Backup?
- The entire Jenkins Home Directory:
- Usually located at `/var/lib/jenkins`, which includes:
    - Job configurations
    - Build history
    - Plugins
    - Credentials (encrypted)
    - User configs
    - Secrets (`secrets/`, `credentials.xml`)
- Configuration files like:
    - `/etc/default/jenkins` (for port and environment settings)

    - `/etc/init.d/jenkins` (service script, if applicable)

- Stop Jenkins to avoid data corruption:

  sudo systemctl stop jenkins

- Take compressed backup:

  sudo tar -czvf jenkins-backup-$(date +%F).tar.gz /var/lib/jenkins

- Optionally back up plugin list:

  ls /var/lib/jenkins/plugins > plugin-list.txt

- Start Jenkins:

  sudo systemctl start jenkins

I have also used plugins like **ThinBackup** or **SCM Sync Configuration**, but for more control and safety, I prefer **filesystem-level backups**.

4) **What is the Difference Between Declarative and Scripted Pipeline in Jenkins?**

Ans:

1. Declarative Pipeline:

- **Introduced later** to simplify pipeline creation.
- Follows a **structured and predefined syntax**.
- Starts with a `pipeline {}` block.
- Easier to read, maintain, and version control.
- Enforces best practices and **validates syntax during compilation**.

2. Scripted Pipeline:

- The original format of Jenkins pipelines.
- Based entirely on Groovy scripting.

- Offers more flexibility and programmatic control (loops, conditionals, complex logic).
- Written inside a `node {}` block.
- Suitable for complex workflows or dynamic steps.

In most projects, I use Declarative Pipelines for their readability and standardization. But for advanced use cases like dynamically generating stages or handling external scripts, I switch to Scripted Pipelines or combine both using `script {}` blocks inside declarative pipelines.

5) **What is a Multibranch Pipeline in Jenkins, When Do We Use It, and What Do We Achieve?**

Ans:

A Multibranch Pipeline in Jenkins is a special type of pipeline project that:

- Automatically discovers, creates, and manages pipelines for each branch in a source control repository (like GitHub, GitLab, Bitbucket).
- Each branch can have its own Jenkinsfile, and Jenkins automatically builds each branch based on that file.

It eliminates the need to manually create separate pipeline jobs for every feature or release branch.

We use multibranch pipelines in:

- **Projects with multiple active branches** (e.g., `dev`, `qa`, `staging`, `main`, `feature/*`)
- **CI/CD automation for every branch**, so each team or developer can test code independently.
- **Pull Request builds** (GitHub/Bitbucket integration).
- When following **GitFlow or trunk-based development** where branches are actively pushed.

In my projects, I used **multibranch pipelines** to automate builds for multiple feature and release branches.

Jenkins automatically scanned the Git repo, detected new branches, and triggered builds whenever code was pushed.

This helped us maintain **branch-wise CI**, ensure **quality gates on PRs**, and allowed **environment-specific deployments** based on branch names — all with minimal manual effort.

6) **What Are Shared Libraries in Jenkins and How Do We Use Them?**

Ans:

Shared Libraries in Jenkins are a way to **reuse common pipeline code** (like functions, stages, steps) across multiple Jenkinsfiles or pipeline projects.

- They are **custom Groovy libraries** stored in a **separate Git repository** or a folder structure within an SCM.
- They allow teams to follow **DRY (Don't Repeat Yourself)** principles and **standardize CI/CD pipelines**.

We use shared libraries when:

- Multiple Jenkins pipelines have **common logic** (e.g., build, test, deploy steps).
- We want to centralize and **version control** pipeline functions.
- To maintain **consistency** across teams and reduce duplication.

The typical directory structure of a shared library looks like:

```
(root)
 └── vars/
    └── deployApp.groovy      # Declarative-style entry points (functions)
 └── src/
    └── org/company/Utils.groovy   # Helper classes (Java-style)
 └── resources/
    └── templates/email.html       # Groovy templates, files
```

└── README.md

I use Jenkins Shared Libraries to build reusable and standardized pipeline components across multiple projects.
This helps maintain consistency, reduces code duplication, and speeds up onboarding for new teams.
I usually keep the shared library in a separate Git repo, configure it globally in Jenkins, and call it using `@Library()` annotation inside Jenkinsfiles.

7) **write a groovy script showing different stages of pipeline, it should be prod kind of pipeline.**

Ans: in VS CODE

8) **What is Jenkins view?**

Ans:

A **Jenkins View** is a way to organize and group jobs (pipelines, freestyle projects, etc.) in your Jenkins dashboard.

By default, Jenkins shows **all jobs** in the **"All" view**, but you can create custom views to:

- Group related jobs (e.g., by team, environment, service)
- Filter jobs by name or status
- Apply different display settings or columns

View Type	Description
List View	Most common; lets you manually or dynamically select jobs
My View	Personalized view for logged-in users
Nested View *(plugin)*	Organize views in folders/subfolders
Pipeline View *(plugin)*	Visualizes pipeline stages (via Build Pipeline or Blue Ocean)

9) **how to add a custom plugin to Jenkins ?**

ANS:

To add a **custom plugin** to Jenkins, you can either install it via the UI (if it's published) or manually upload a `.hpi` or `.jpi` file if it's a custom-built plugin.

1. Upload via Jenkins UI (for custom `.hpi/.jpi` files)

2. Manually Place Plugin in File System

    Place your `.hpi` or `.jpi` file into Jenkins' plugin directory:

    /var/lib/jenkins/plugins/

3. Set proper ownership/permissions (if needed):

    chown jenkins:jenkins /var/lib/jenkins/plugins/your-plugin.hpi

4. Restart Jenkins:

    systemctl restart jenkins

Kubernetes

1) **What is authentication and Authorization and how it happens in k8s cluster, explain it step by step.**

Ans:

When a request is made to the Kubernetes API Server (e.g., `kubectl get pods`), the following steps are executed:

Step 1: Authentication – Who Are You?

The API Server first checks who is making the request by validating credentials such as:

- **X.509 client certificate** (used in kubeconfig)
- **Bearer Token** (used by service accounts or external OIDC)
- **Static token files**
- **OpenID Connect (OIDC)** – integrates with external identity providers like Azure AD, Okta, Google
- **Webhook token authentication**

📌 **If authentication fails**, the API server returns `401 Unauthorized`.

Step 2: Authorization – What Can You Do?

Once authenticated, the API server checks if the identity has permission to perform the requested action using:

- **RBAC (Role-Based Access Control)** → most widely used.
- **ABAC (Attribute-Based Access Control)** → legacy.
- **Webhook authorization** → custom external logic.

📌 The request is evaluated against:

- **Verb**: get, list, create, delete, update
- **Resource**: pods, deployments, secrets
- **Namespace**: where the resource resides
- **User identity** (User or ServiceAccount)

📌 **If authorization fails**, it returns `403 Forbidden`.

Step 3: Admission Controllers – Should We Allow It?

After the request is authenticated and authorized, admission controllers run to:

- Mutate the request (add labels, enforce policies)
- Validate request against custom rules (e.g., no privileged containers)

Examples:

- `NamespaceLifecycle`, `LimitRanger`, `PodSecurity`, `MutatingAdmissionWebhook`

📌 If the request fails here, it is rejected before resource creation.

Real-World Example:

When I run `kubectl get pods -n dev`:

1. The kubeconfig token or client cert is sent → Authentication
2. K8s checks if this user/service account has `get` access to `pods` in `dev` namespace → Authorization
3. If a Pod creation, admission controllers might mutate or validate the spec → Admission Control

In Kubernetes, authentication verifies who you are, authorization checks what you're allowed to do, and admission controllers enforce cluster policies.

I usually work with RBAC, and manage access via ServiceAccounts, Roles, and RoleBindings, ensuring least privilege principle and using tools like OPA Gatekeeper or Kyverno for policy enforcement.

2) Is it necessary to use openshift if we already have EKS and AKS.? difference between in details.

Ans:

No, it's not necessary to use OpenShift if you already use managed Kubernetes services like **EKS (AWS)** or **AKS (Azure)**.

OpenShift is an enterprise Kubernetes platform with additional features on top of upstream Kubernetes, while **EKS and AKS** are **vanilla Kubernetes** services managed by their respective cloud providers.

However, there are key **differences in features, flexibility, and use cases** that can help decide **when to use OpenShift**.

Feature	OpenShift (Red Hat)	EKS (AWS) / AKS (Azure)
Kubernetes Base	Uses Kubernetes + enhancements	Uses upstream vanilla Kubernetes
Managed By	Red Hat (or self-managed)	AWS (EKS), Azure (AKS)
Installation	Complex (unless using OpenShift Dedicated or ROSA)	Fully managed (1-click cluster creation)
Web Console (UI)	Built-in developer/admin console	Minimal or none (AKS has basic dashboard)

Integrated CI/CD	Has OpenShift Pipelines (Tekton-based)	No built-in CI/CD (you use GitHub Actions, CodePipeline, Azure DevOps)
Security / RBAC	Built-in **SecurityContextConstraints (SCC)**, stricter policies	Standard Kubernetes RBAC only
Container Registry	Comes with **integrated image registry**	You integrate ECR (EKS) or ACR (AKS)
Developer Tools	Source-to-Image (S2I), Developer Catalog, Templates	Not built-in; you need external tooling
Upgrades & Maintenance	Managed by Red Hat (ROSA/OpenShift Online) or self-managed	AWS or Azure manages upgrades
Cost	OpenShift license required (for self/ROSA)	Pay-as-you-go for compute and services only
Ecosystem Flexibility	More opinionated stack	More flexibility, bring your own tools
Support for Custom Workloads	Might be restricted by SCC/PodSecurity	More open and flexible for workload customization

OpenShift is **not necessary** if you're using EKS or AKS, but it's a **powerful enterprise platform** when you need **built-in CI/CD, tighter security controls**, and **pre-integrated developer tools**.

I choose between them based on project needs — if I need flexibility, I go with EKS/AKS; if I need security, governance, and full-stack enterprise support, I consider OpenShift.

3) Tell me about operators and use case, how do we manage operators in openshift?

Ans:

An Operator is a Kubernetes-native application controller that extends Kubernetes capabilities to manage complex stateful or custom applications.

It codifies operational knowledge (installing, configuring, upgrading, recovering) into a Kubernetes-native custom controller, using CRDs (Custom Resource Definitions).

How Operators Work (Simple Explanation):

- The operator defines a CRD like `PostgresCluster`.
- You apply a custom resource (YAML) that describes the desired state.
- The Operator watches that resource and performs all actions needed to bring it to life — install, scale, backup, restore, upgrade, etc.

OpenShift has a dedicated GUI and CLI support for managing Operators.

OperatorHub (GUI):

- **Navigate to:** *Operators* > *OperatorHub* (in OpenShift Console)
- Browse certified, community, and custom operators
- Click to **Install**, choose:
    - Target namespace or cluster-wide
    - Manual or automatic updates
- It creates CRDs + deploys Operator controller

OpenShift uses **OLM** to:

- Install, upgrade, and manage Operators
- Handle versioning and dependency resolution
- Auto-update operators (if configured)

Operators in OpenShift are Kubernetes-native controllers that manage complex applications automatically.

I use them to deploy tools like **PostgreSQL, Prometheus, ArgoCD**, etc., with custom configurations, scaling, and recovery logic.

In OpenShift, we manage operators via **OperatorHub (UI)** or the **`oc` CLI**, and **Operator Lifecycle Manager** ensures smooth updates and version control.

4) How our Kubernetes cluster authenticate with docker hub or other container registry, how will you manage password change for docker and manage secrets and make sure authentication does not fail, also maintaining creds as secure ?

ANS:

Why Authentication is Needed-

Kubernetes needs to pull images from private registries (e.g., Docker Hub, AWS ECR, Azure ACR).

When pulling from a private repository, Kubernetes must authenticate using valid credentials (username/password or token).

How Authentication Works with Docker Hub -

You create a Docker Registry Secret of type `kubernetes.io/dockerconfigjson`.

```
kubectl create secret docker-registry regcred \
  --docker-username=<your-docker-username> \
  --docker-password=<your-docker-password> \
  --docker-email=<your-email> \
  --namespace=your-app-namespace
```

This stores the credentials securely in Kubernetes.

- You attach the secret in your pod spec using `imagePullSecrets`.

- Now Kubernetes uses the `regcred` secret to authenticate with Docker Hub when pulling the image.

I automate Docker credential rotation using external secret stores like **AWS Secrets Manager or Vault**, combined with a shell script or Kubernetes CronJob that updates Kubernetes secrets across namespaces.

This ensures that when passwords change, the cluster always has the latest credentials securely — reducing downtime and manual intervention.

Automate Image Pull Secrets with ServiceAccounts

- Automate Image Pull Secrets with ServiceAccounts
- If multiple pods in a namespace need the same image pull secret: then we use serviceaccount for that to reference secret.

What If Docker Password Changes?

To pull private images, Kubernetes uses `docker-registry` type secrets which store the Docker Hub or container registry credentials.

I manage these using `kubectl create secret`, attach them using `imagePullSecrets`, and rotate credentials via automation when passwords change.

For security and scale, I prefer **external secret managers** (Vault, AWS Secrets Manager) and GitOps tools like **Sealed Secrets** to avoid exposing sensitive data in plaintext or Git.

7) What Are the Common Errors You Face During Deployment with Pods and Containers in Kubernetes?

ANS:

In real-world Kubernetes deployments, I've encountered **various pod and container-level errors**. These usually occur due to **misconfigurations, image issues, resource constraints, or missing dependencies**.

Below are **common categories of deployment errors**, their causes, how I debug them, and how I fix them.

1. ImagePullBackOff / ErrImagePull

💬 Description: Pod fails to pull the image from registry.

🔍 Causes:

- Incorrect image name or tag
- Image doesn't exist in the registry
- No access to private registry (auth missing)
- Wrong or missing `imagePullSecrets`

🛠️ Fixes:

- Check image path: `docker.io/org/app:tag`
- Verify `kubectl describe pod` → check event logs
- Recreate `imagePullSecrets`
- Ensure internet access in private clusters

2. CrashLoopBackOff

Description: Container starts → crashes → Kubernetes restarts it → repeat

🔍 Causes:

- App exits due to unhandled exceptions
- Bad environment variables or missing config
- Database not ready / service dependency down
- Wrong command or entrypoint in Dockerfile

🛠️ Fixes:

- Use `kubectl logs <pod>` to debug crash
- Run locally with `docker run` to test

- Add `livenessProbe` and `readinessProbe` properly
- Add `sleep` or retry logic in the app startup

3. ContainerCreating (Stuck Pod)

💬 **Description:** Pod is stuck in "ContainerCreating" status

🔍 **Causes:**

- Volume mount issues (PVC not bound)
- Image pull delay
- Network or CNI plugin not working
- Node resource pressure

🛠️ **Fixes:**

- Check with `kubectl describe pod`
- Check PV/PVC status using `kubectl get pvc`
- Ensure CNI plugin is healthy (`kube-flannel`, `calico`)
- Check node disk/memory with `kubectl describe node`

4. Pending Pod

💬 **Description:** Pod is stuck in "Pending" state

🔍 **Causes:**

- No available nodes match resource requests
- Node selector/taints mismatch

- Insufficient CPU or memory on nodes
- PVC not bound

🛠️ **Fixes:**

- Check with `kubectl describe pod`
- Validate taints, tolerations, node selectors
- Scale up nodes or reduce resource limits
- Ensure PVC is bound to a PV

5. OOMKilled (Out of Memory Killed)

💬 **Description:** Container exceeded memory limits and was killed by the system

🔍 **Causes:**

- Memory leak in app
- `resources.limits.memory` too low
- Heavy operations during startup

🛠️ **Fixes:**

- Review container memory usage: `kubectl top pod`
- Increase memory limit
- Optimize app memory usage

6. Readiness Probe / Liveness Probe Failed

💬 **Description:** Health check fails → container restarted or not added to service

🔍 **Causes:**

- Wrong path/port in `readinessProbe`
- App takes too long to start
- Probe response is not 200 OK

🛠️ **Fixes:**

- Tune `initialDelaySeconds`, `timeoutSeconds`
- Validate probe path manually (e.g., `curl localhost:8080/health`)
- Add logging in probe handler

7. VolumeMount Errors

💬 **Description:** Pod fails due to missing or misconfigured volume mounts

🔍 **Causes:**

- PVC not bound
- Wrong mount path
- Access denied or permission error on mounted directory

🛠️ **Fixes:**

- Check PVC status and storage class
- Ensure file permissions are correct
- Validate volume definitions in pod spec

8. Node Affinity / Taints Errors

💬 **Description:** Pod can't be scheduled to any node due to taints or affinity rules

🔍 **Causes:**

- Tolerations missing in pod spec
- Node affinity rules too restrictive

🛠️ **Fixes:**

- Add matching tolerations
- Review affinity rules and relax constraints if needed

9. DNS Resolution Failure

💬 **Description:** App fails to resolve internal service names

🔍 **Causes:**

- CoreDNS pods not running
- Wrong service name
- App not using internal cluster DNS format

🛠️ **Fixes:**

- Restart `coredns` deployment
- Check `resolv.conf` inside container
- Use proper DNS name like `myservice.my-namespace.svc.cluster.local`

8) explain more about secret management securely and insecurely in k8s?

ANS:

Kubernetes Secrets are objects used to store sensitive data, such as:

- Passwords
- API keys

- TLS certificates
- Docker registry credentials

They are base64-encoded and mounted into pods as environment variables or volumes.

- **Apply RBAC policies so only specific service accounts or namespaces can access them.**
- **Instead of storing secrets inside the cluster, fetch them securely from external tools:**

In Kubernetes, secrets are base64-encoded and can be easily mismanaged if not protected properly.

I use **RBAC**, **encryption at rest**, and tools like **External Secrets Operator** or **Sealed Secrets** to handle secrets securely.

I avoid storing raw secrets in Git and follow the principle of **least privilege** when exposing secrets to pods.

9) How Would You Troubleshoot an Application Failing to Connect to a Third-Party Service Due to Certificate Issues?

1. Identify the Error Clearly

- Check logs of the application or container:

  kubectl logs <pod-name>

Look for typical certificate-related errors like:

- `x509: certificate signed by unknown authority`
- `SSL certificate problem: unable to get local issuer certificate`
- `certificate has expired or is not yet valid`
- `hostname mismatch` or `untrusted CA`

2. Validate the Remote Service Certificate

Use `openssl` or `curl` to inspect the service certificate from a test

Check for:

- Expired certificate
- Self-signed certificate
- Certificate chain issues
- Hostname mismatch

If certificate expired or hostname mismatch:

- Contact 3rd-party vendor to issue a valid certificate.
- Use correct FQDN (not IP) to avoid hostname mismatch.

If the app runs in Kubernetes:

- **Mount custom CA as a secret or configMap**:

When troubleshooting TLS/certificate issues, I first examine the exact error from logs, then validate the remote service certificate using `openssl` or `curl`.

I check if the certificate chain is trusted by the app's runtime, and if not, I import the CA cert to the appropriate trust store.

In Kubernetes, I use configMaps or rebuild images with updated trust stores, and validate connectivity from debug pods.

This structured approach helps prevent downtime and ensures secure connections.

10) How do you manage TLS certificates for apps in Kubernetes?

ANS:

TLS certificates in Kubernetes are crucial for securing in-cluster and external communication (HTTPS, mTLS). I use multiple approaches depending on the use case:

- I manage TLS in Kubernetes primarily using **cert-manager**, which automates certificate issuance, renewal, and storage using Let's Encrypt or internal CAs.
- For manually managed certs, I store them in **Kubernetes TLS secrets** and mount them securely to apps or Ingress.
- I also implement **RBAC and automatic rotation policies**, and make sure apps or ingress reload the certs dynamically to avoid downtime.

10) How do you know if a certificate used by your app has expired or is about to expire?

1. If Using `cert-manager` (Best Practice)

- **cert-manager** maintains TLS certificates using `Certificate` and `CertificateRequest` resources.
- You can track certificate status and expiry directly via CRDs.

kubectl describe certificate myapp-cert -n my-namespace

What to look for:

- `NotAfter` (expiration date)
- `Renewal Time`
- `Ready: False` (means expired or failed renewal)

2. Query Secret and Decode Certificate

If cert is stored in a Kubernetes TLS Secret (e.g., `myapp-tls`), you can manually decode and inspect expiry.

kubectl get secret myapp-tls with grep command

4. External Health Checks (Ingress)

If cert is used in an Ingress (like NGINX or Traefik), you can:

- Use `curl` or `openssl` from inside or outside the cluster:

I monitor certificate expiration in Kubernetes using `cert-manager`'s status fields and Prometheus metrics.

For manual TLS secrets, I decode the certificate using `openssl` to check the `Not After` date.

I also automate alerts using Prometheus rules or custom scripts/CronJobs to ensure we are alerted before expiry — typically 30 days in advance to ensure smooth renewals or rotations.

14) How does helm pull artifacts from nexus artifactory, how the authentication happens and how its pulls artifactory artifact and puts it in K8s cluster ?

ANS:

Helm pulls packaged application charts (`.tgz`) from a Helm repository.

If your **Nexus Artifactory** is configured as a **Helm repository**, you can host and retrieve Helm charts from it just like any remote Helm repo (e.g., Bitnami, ArtifactHub, etc.).

2. Hosting Helm Charts on Nexus

In Nexus (Sonatype Nexus 3.x+ or JFrog Artifactory), you:

- Create a Helm repository (hosted or proxy)
- Upload your `.tgz` Helm charts
- Nexus auto-generates an `index.yaml` file for the repo

When using Helm with Nexus Artifactory, I add the Helm repo via authenticated `helm repo add`, which pulls Helm charts (`.tgz`) hosted on Nexus.

Helm authenticates using basic auth or tokens, downloads the chart, renders it into Kubernetes YAMLs, and deploys them to the cluster using `kubectl`.

I always use token-based auth, and automate this via CI/CD for consistent, secure deployments.

15) Deployed an app in k8s cluster, how do you troubleshoot, give realtime issues what you have faced and why you faced those issues?

When I deploy an app to Kubernetes, I follow a systematic approach to troubleshoot issues:

1 . Check Deployment & Pod Status

- kubectl get pods -o wide -n my-namespace

  Whether pods are running or stuck (e.g., `CrashLoopBackOff`, `ImagePullBackOff`, `Pending`)

2. Check Logs

- If pods are running but not working as expected:

  kubectl logs <pod-name> -n my-namespace 0r kubectl logs <pod-name> -c container-name

Issue 1: `ImagePullBackOff` or `ErrImagePull`

Reason: Wrong image name, invalid tag, or private image repo without credentials.

Fix:

- Corrected the image name/tag.

Created a `docker-registry` secret:

bash
CopyEdit

```
kubectl create secret docker-registry regcred --docker-username=xxx
--docker-password=xxx ...
```

-
- Added `imagePullSecrets` to deployment.

⚠️ **Issue 2: `CrashLoopBackOff`**

Reason: App failed to start repeatedly due to:

- Missing environment variable

- Wrong DB credentials
- Service dependency not ready

Fix:

- Used `kubectl logs` to check crash stack trace.
- Validated environment variables in the `deployment.yaml`.
- Used readiness/liveness probes to delay traffic until app was ready.

⚠️ Issue 3: `Pending` Pods

Reason: Pod couldn't be scheduled due to:

- No node with enough resources
- Taint/toleration mismatch

Fix:

- Checked pod events: `kubectl describe pod`
- Scaled up the cluster or adjusted resource requests/limits.
- Updated tolerations or nodeSelector if required.

⚠️ Issue 4: Readiness Probe Failed

Reason: Application took time to boot up, and Kubernetes considered it unhealthy.

Fix:

- Increased `initialDelaySeconds` in readiness probe.

- Changed the probe path to actual working `/health` endpoint.
- Added retry logic in the app startup to wait for DB or cache.

⚠️ Issue 5: Service Not Reachable

Reason: Misconfigured `service` or wrong port mapping

Fix:

- Verified `targetPort` matched container port.
- Checked `kubectl describe svc` and compared with pod's container spec.
- Used a debug pod (`kubectl run -it busybox`) to `curl` the internal service.

⚠️ Issue 6: Ingress Not Routing Properly

Reason: Wrong host in ingress or certificate misconfiguration.

Fix:

- Checked ingress status: `kubectl describe ingress`
- Verified DNS points to LoadBalancer IP
- Ensured TLS secret existed and was valid

⚠️ Issue 7: PVC Stuck in `Pending`

Reason: No PersistentVolume matched PVC request (wrong size, storage class mismatch)

Fix:

- Described PVC and saw "no matching PV".

- Updated PVC to match available PV.
- Added storage class annotations.

16) Explain about kubelet and what is the purpose of it in k8s?

ANS:

Kubelet is the node agent in Kubernetes that ensures containers are running as expected.

It communicates with the control plane, receives pod specs, and manages pod lifecycles by interacting with the container runtime.

Without kubelet, the node cannot run or manage workloads — it is a critical component of the Kubernetes architecture.

17) Explain more about probes in Kubernetes, like startup, liveliness and readiness?

ANS:

In Kubernetes, **probes** are used by the **kubelet** to check the health and availability of containers in a pod. They determine when a container:

- Is ready to serve traffic
- Is still running as expected
- Is just starting up and needs time

Probe Type	Purpose	Impact on Pod/Service
✅ Readiness	Checks if the container is **ready to serve traffic**	Controls whether pod receives traffic via Services

✅ Liveness	Checks if the container is **still alive/running**	Restarts the container if the check fails
✅ Startup	Checks if the container **startup is complete**	Delays other probes until the app is fully started

🧪 Real Example Scenario

In one project, a Spring Boot app took ~90 seconds to start, but the liveness probe started too early and restarted the container repeatedly.

Fix: Added a `startupProbe` with proper delay, so liveness was paused until the app booted fully.

In Kubernetes, probes help ensure app stability and availability.

I use **readiness probes** to control service traffic, **liveness probes** to restart unhealthy containers, and **startup probes** to delay checks for slow-starting apps.

Correct probe tuning is essential to avoid false failures and unnecessary restarts, especially in production environments.

18) Even If Liveness, Readiness, and Startup Probes Show Healthy — But the App Fails, What Should You Do?

Ans:

This is a real-world problem: the probes return `200 OK`, but the application is functionally broken or degraded internally.

1. Check Application-Level Logs

Even though Kubernetes thinks the container is "healthy", the app might be:

- Throwing internal exceptions
- Returning `500` to real clients

- Stuck due to unresponsive external services

```
kubectl logs <pod-name>
```

🔹 2. Improve Your Probe Design

The default health endpoints (`/health`, `/status`) often return `200 OK` for basic checks only.

✅ Modify them to:

- Check database connectivity
- Verify dependent services are reachable
- Run a functional test (e.g., mock query)

Example:

java

CopyEdit

```
GET /healthz → should check:
- DB
- Redis
- External API
```

🔹 3. Add Application Metrics/Monitoring

Use Prometheus + Grafana to monitor:

- Application error rate
- Latency

- Queue size
- Custom metrics

Alert on business-level failures, not just infra-level health.

🔹 4. Check for Stateful Failures

The app might pass health checks but be internally broken due to:

- Memory leaks
- Deadlocks
- Disk full
- Thread exhaustion

Use:

- `kubectl top pod`
- APM tools like Datadog, New Relic, Dynatrace

🔹 5. Enable Better Observability

Add:

- Structured logging
- Tracing (`OpenTelemetry`)
- External synthetic tests (e.g., ping app from outside)

🟡 Summary (Interview Style)

Even if probes show green, apps can still be broken. I enhance probe endpoints to test critical dependencies like DB/API, and add Prometheus alerts and logs.
Health checks only tell Kubernetes that the container is alive—not that it's functionally correct.

19) What Are CRDs in Kubernetes? How Do You Manage and Use Them?

What Are CRDs (Custom Resource Definitions)?

CRDs are a way to extend Kubernetes by defining custom resources.

- Kubernetes natively has resources like `Pod`, `Service`, `Deployment`.
- With CRDs, you can create your own like:
    - `KafkaTopic`
    - `MySQLBackup`
    - `PrometheusRule`

These are managed like any K8s resource:

bash

CopyEdit

```
kubectl get kafkatopics

kubectl describe mysqlbackup my-backup
```

🧱 CRD = Schema + Controller

Component	Role

CRD	Defines the schema (YAML structure)
Controller	Watches the CRD and takes action

For example:

- `cert-manager` uses CRDs like `Certificate`, `Issuer`
- `ArgoCD`, `Prometheus`, `Istio`, `OpenShift` all use CRDs

CRDs allow me to extend Kubernetes with custom resource types. I've used them in tools like cert-manager and Prometheus, and I manage them like any other K8s resource via GitOps and RBAC.

I ensure schema validation and pair them with controllers to automate resource behavior effectively.

19) I have load balancer created in eks, issue is even though ALB controller and everything is available, external ip is not visible or in pending, what could be the reasons?

Ans:

i) ALB Controller Installed but Missing IAM Permissions

= Make sure the **IAM role (IRSA)** assigned to the ALB controller pod has the correct **IAM policy** attached.

Example: it should have permissions like `elasticloadbalancing:CreateLoadBalancer`, `ec2:DescribeSubnets`, etc.

Check : " **kubectl -n kube-system logs deploy/aws-load-balancer-controller**"

2. **Your Service Type Is Not Supported**

If you're using a `Service` of type `LoadBalancer`, that is handled by the default Kubernetes cloud controller (not the ALB controller). The AWS Load Balancer Controller works with Ingress resources, not Service objects directly.

- Define an **Ingress** using the `alb.ingress.kubernetes.io/*` annotations.
- Ensure `IngressClass` is set to the ALB controller.

The Ingress resource must match the controller's class name (default is `alb`). If it's not defined or mismatched, ALB won't be created.

Check: **kubectl get ingressclass**

spec:

ingressClassName: alb

4. **Subnet Tagging Is Missing or Incorrect**

ALB controller looks for subnets with specific tags to place the load balancer.

Key: kubernetes.io/cluster/<cluster-name> | Value: shared

Key: kubernetes.io/role/elb | Value: 1

For **private** subnets (for internal ALBs):

Key: kubernetes.io/role/internal-elb | Value: 1

6. **Security Group Conflicts**

The security groups attached to your EKS worker nodes or load balancer subnets might block incoming traffic (ports 80/443).

Check:

- Inbound HTTP/HTTPS (80/443) to the ALB
- ALB to reach backend pods

21) Headless service

A Headless Service in Kubernetes is a special type of service that does not have a ClusterIP and is used to directly expose the IPs of the backing pods — typically for stateful applications like databases or for DNS-based service discovery.

In a regular Kubernetes service, the service gets a **cluster IP**, and traffic is load-balanced among the pods. But in a **headless service**, you tell Kubernetes **not to assign a cluster IP**, by setting:

spec:

clusterIP: None

Instead of routing traffic through a load balancer, **DNS returns individual pod IPs**, enabling clients to talk directly to specific pods.

Headless services **do not provide load balancing**.

Useful for **direct pod discovery via DNS**.

Ideal with **StatefulSets** to give each pod a **stable DNS identity**.

`clusterIP: None` is **mandatory** to declare a headless service.

SHELL

1) **How Do You Install a Package on an Isolated Linux Server (No Internet, No Bastion, No NAT Gateway)?**

ANS:

There are two approaches — one without S3 and one with S3, depending on what access is available inside the private environment.

Option 1: Without S3 or Any Public Access

You can manually download dependencies, move them into the server, and install them offline.

Approach A: Create an Offline Package Bundle

For YUM-based systems (RHEL/CentOS/Amazon Linux):

bash

CopyEdit

```
# On an internet-connected machine:

yum install --downloadonly --downloaddir=./offline-nginx nginx


# Transfer the .rpm files using a secure USB or encrypted EBS

scp *.rpm ec2-user@localhost:/tmp/


# On the isolated server:

sudo yum localinstall *.rpm
```

For APT-based systems (Ubuntu/Debian):

bash

CopyEdit

```
# On a connected machine:

apt-get download <package-name>

apt-cache depends <package-name> | grep Depends


# Move .deb files and install:

sudo dpkg -i *.deb
```

> 🔁 You can automate the dependency resolution using `apt-offline` or `yumdownloader`.

Approach B: Create a Local Repo on a USB or Volume

1. Download all `.rpm` or `.deb` files
2. Use `createrepo` (YUM) or `dpkg-scanpackages` (APT)
3. Mount it on the target server as a local repo

Example (RHEL):

bash

CopyEdit

```
mount /dev/xvdf /mnt

createrepo /mnt

echo "[local-repo]

name=Local Repo

baseurl=file:///mnt
```

```
enabled=1

gpgcheck=0" > /etc/yum.repos.d/local.repo

yum install nginx
```

For isolated Linux servers, I use two main approaches.

Without S3 or internet, I prepare offline `.rpm` or `.deb` packages on a connected machine and transfer them via EBS, USB, or AMI customization.

With S3 access via a VPC endpoint, I upload the packages and use `aws s3 cp` to dynamically pull them at runtime and install them via `yum localinstall` or `dpkg`.

This ensures clean, secure, and automated package installation in air-gapped environments.

2) Count how many times each ip address is present in a file (ip's are given in either list, or array or dictionary). ?

Example File Content (`ips.txt`):

["192.168.1.1", "10.0.0.1", "192.168.1.1"]

{"server1": "10.0.0.1", "server2": "172.16.0.1"}

192.168.1.1

10.0.0.1

```
#!/bin/bash

# File name containing the IPs

FILE="ips.txt"

# Extract all IPv4 addresses using grep and regex

grep -oE '\b([0-9]{1,3}\.){3}[0-9]{1,3}\b' "$FILE" |

 sort |

 uniq -c |

 sort -nr
```

What This Does:

- `grep -oE`: Extracts only the IP addresses from each line (even inside JSON, lists, arrays, or text)
- `sort`: Sorts them so `uniq` can count duplicates
- `uniq -c`: Counts occurrences of each unique IP
- `sort -nr`: Sorts the result by descending count

3) Using Istio or in Istio how do you expose endpoints externally.?

In Istio, we expose services externally using the Istio Ingress Gateway, which acts as a layer 7 load balancer (similar to a reverse proxy) for incoming traffic into the mesh.

🔹 Key Resources Used to Expose Services Externally in Istio:

Resource	Purpose

`Gateway`	Defines how incoming traffic is received (host, port, TLS, etc.)
`VirtualService`	Routes traffic from the gateway to the correct service in the mesh
`Service`	The internal Kubernetes service

🧱 Basic Architecture Flow

External client → Istio Ingress Gateway → VirtualService → Internal K8s Service → Pod

21) How do you implement Pod Security Standards (PSS) or Pod Security Policies in Kubernetes?

Pod Security Standards (PSS) are built-in security policies in Kubernetes v1.23+. They replace deprecated PodSecurityPolicies (PSP). PSS enforce pod-level security based on predefined levels: privileged, baseline, and restricted. You can enforce them using namespace labels or Gatekeeper/OPA for advanced policies.

22) How does Kubernetes RBAC work and how do you audit access and permission issues?

RBAC (Role-Based Access Control) defines roles and bindings to control user access. You audit access by enabling the audit logs in the API server and inspecting events, or using tools like `kubectl auth can-i`.

23) What is the difference between a ValidatingAdmissionWebhook and a MutatingAdmissionWebhook?

ValidatingAdmissionWebhook validates the request and can deny it. MutatingAdmissionWebhook can modify the request (e.g., inject sidecars) before it's persisted. They run at different stages in the admission process.

24) How does OpenShift handle security differently from vanilla Kubernetes?

OpenShift uses Security Context Constraints (SCCs), integrates OAuth for login, and restricts container privileges by default. It enforces a more secure-by-default approach compared to vanilla Kubernetes.

25) How does OpenShift handle security differently from vanilla Kubernetes?

OpenShift uses Security Context Constraints (SCCs), integrates OAuth for login, and restricts container privileges by default. It enforces a more secure-by-default approach compared to vanilla Kubernetes.

26) How do you enforce image policies in OpenShift and Kubernetes clusters?

In Kubernetes, you can use OPA/Gatekeeper or Kyverno. In OpenShift, ImagePolicies and ImageStreams can restrict image sources and enforce trusted registries

27) Explain how Multi-Tenancy is implemented in Kubernetes and OpenShift.

Multi-tenancy is managed via namespaces, RBAC, and NetworkPolicies. OpenShift extends this with stricter SCCs and integrated user authentication and quotas per project (namespace).

28) What are NetworkPolicies and how do you implement them securely?

NetworkPolicies control traffic between pods. You define ingress and egress rules using labels. Secure implementation involves default deny policies and explicit allow rules.

29) How do you troubleshoot CrashLoopBackOff and ImagePullBackOff errors?

Check pod logs (`kubectl logs`), describe the pod, and inspect init containers or config issues. For ImagePullBackOff, check image name, tag, registry authentication, or network access.

30) How do you manage Kubernetes upgrades without downtime?

Use a blue-green or rolling deployment approach. Upgrade control plane and nodes in a phased manner, drain nodes safely, and ensure HA components are available.

31) How does the Kubernetes scheduler work and how can you influence its behavior?

It assigns pods to nodes based on resource requests, taints/tolerations, affinity/anti-affinity, and custom schedulers. Influence it via constraints and priorities.

32) What is etcd, how is it secured, and what happens if it becomes corrupted?

etcd is the key-value store backing Kubernetes. It's secured via TLS, encryption, and snapshots. If corrupted, restore from a recent snapshot and verify quorum.

33) How do you configure audit logging in Kubernetes?

Enable `--audit-policy-file` in kube-apiserver and specify audit log paths. Use policy rules to capture events and analyze logs for auditing access.

34) Explain the role and lifecycle of a Kubernetes Certificate (TLS bootstrapping).

Kubernetes uses client and server TLS certs for authentication. TLS bootstrapping allows kubelets to get a cert via kube-controller-manager. Certificates expire and need renewal via `cert-manager` or automation.

35) How do you backup and restore a Kubernetes cluster?

Use etcd snapshots for control plane state. Backup manifests, PV data, and secrets. Tools like Velero can backup apps and volume data.

36) How do you debug issues with CoreDNS or kube-dns in Kubernetes?

Check logs of CoreDNS pods, validate `kube-dns` service, use `nslookup` or `dig` inside pods, and inspect NetworkPolicies or ConfigMaps.

37) What is the difference between Helm and Operator Lifecycle Manager (OLM)?

Helm is a templating tool for deploying applications. OLM manages Operator installation and upgrades, providing a declarative model for lifecycle management.

38) How does OpenShift ImageStream differ from Kubernetes image pulls?

ImageStreams abstract the image source and allow OpenShift to trigger builds and deployments automatically when a new image is pushed.

39) How does OpenShift handle route and ingress differently from Kubernetes?

OpenShift uses Routes (built-in) instead of Ingress by default, supporting advanced TLS, path-based routing, and edge/reencrypt/ passthrough termination types.

40) How do you monitor a production Kubernetes or OpenShift cluster?

Use Prometheus, Grafana, Alertmanager, and tools like kube-state-metrics. OpenShift includes these via Cluster Monitoring Operator

41) What is the purpose of SCC (Security Context Constraints) in OpenShift?

SCCs control pod permissions like running as root, privileged containers, volume types, etc. They enhance pod-level security.

42) How do you troubleshoot a stuck pod in Terminating state?

Check if the pod is blocked by finalizers or volume unmount. Force delete it using `kubectl delete pod --grace-period=0 --force`.

43) What is KEDA and how can it be used in OpenShift/K8s?

KEDA is Kubernetes-based Event Driven Autoscaler. It scales pods based on events (like queue length, custom metrics). Useful for microservices and serverless apps.

44) How would you handle secrets rotation automatically in a K8s/OpenShift environment?

Use tools like Vault with Kubernetes Auth method, cert-manager for TLS secrets, and operators to handle config reload and rotation.

45) Explain Horizontal Pod Autoscaler vs Vertical Pod Autoscaler vs Cluster Autoscaler.

HPA adjusts pod count based on metrics. VPA adjusts CPU/memory of pods. Cluster Autoscaler adjusts node count in the cluster based on pending pods.

46) How would you debug a node that is NotReady?

Check `kubectl describe node`, kubelet logs, system services (e.g., container runtime), and disk/memory status. Also verify network connectivity and certificates.

To fix a `NotReady` node in Kubernetes, first run `kubectl describe node <node-name>` to check the conditions. SSH into the node and restart the kubelet (`systemctl restart kubelet`). Verify Docker/CRI status, disk space (`df -h`), and certificate expiration. Ensure the node can reach the API server over the network.

47) How would you tune etcd performance and ensure its HA?

Place etcd on SSDs, separate from workload, monitor latency, use 3-5 member clusters, secure with TLS, and take regular snapshots.

48) How do you secure inter-pod communication (e.g., mTLS with Istio)?

Use Istio to inject sidecars, enforce strict mTLS, and configure DestinationRules and PeerAuthentication policies.

49) . Explain the architecture and usage of OpenShift GitOps (ArgoCD).?

OpenShift GitOps uses ArgoCD to sync Kubernetes manifests from Git repositories to the cluster. It enforces declarative CD and auditability

50) What is a service mesh and how does OpenShift integrate it (e.g., with Istio)?

A service mesh like Istio provides traffic control, security (mTLS), observability, and retries. OpenShift Service Mesh (based on Istio) manages this with Kiali, Jaeger, and Grafana integration.

51) What are the differences between OpenShift 3.x, 4.x, and upstream Kubernetes?

OpenShift 3.x was based on Kubernetes 1.x and used Docker and Ansible. 4.x uses CRI-O, Operators, and runs on CoreOS. Upstream Kubernetes lacks built-in UI, SCC, OAuth, etc.

Terraform

What is the `lifecycle` block in Terraform used for?

- The `lifecycle` block allows you to control how Terraform handles resource creation, destruction, and changes. It includes settings like `create_before_destroy`, `prevent_destroy`, and `ignore_changes`.

What does `prevent_destroy` do in Terraform?

- It prevents Terraform from destroying a resource unless the setting is removed. Useful for critical resources like databases or production servers.

What does `create_before_destroy` mean?

- Ensures that a new resource is created before the old one is destroyed—important for avoiding downtime.

What is the use of `ignore_changes` in Terraform lifecycle?

- It tells Terraform to ignore certain attributes if they change outside of Terraform (e.g., manually via console or another tool).

Give an example of when you would use `ignore_changes`.

- When an EC2 instance's `user_data` or `tags` are managed by another system (e.g., Ansible), and you don't want Terraform to constantly update or overwrite them.

What happens if you set `prevent_destroy = true` and try to destroy the resource?

- Terraform will throw an error and block the destroy plan until you manually remove the `prevent_destroy` line.

Can we use `lifecycle` on data sources?

- No. The `lifecycle` block applies only to resources, not to data sources.

What happens if `create_before_destroy` is set but both resources can't exist at the same time (e.g., same name)?

- Terraform will fail with an error, as it cannot satisfy both constraints. In such cases, consider not using `create_before_destroy`.

In which scenario would you use `create_before_destroy` with `depends_on`?

- When you have a dependency (e.g., DNS record depends on a load balancer), and you want the new load balancer to be created before the DNS record is updated.

How does `ignore_changes` impact Terraform state?

- Terraform still tracks the full state, but during a plan/apply, it will skip changes to specified attributes, so no diffs or updates will be attempted.

Can you combine `prevent_destroy` and `ignore_changes` together?

- Yes. You might want to protect a resource from being destroyed **and** tell Terraform to ignore certain updates, especially for manually managed resources.

What lifecycle behavior would you recommend for managing database resources in production?

```
lifecycle {

  prevent_destroy = true

  ignore_changes = [backup_retention_period]

}
```

    - This avoids accidental deletion and ignores operational changes like backups.

13. How do you override `prevent_destroy` during a destroy operation?

- You must remove or comment out the `prevent_destroy` line in the Terraform code, re-apply, and then destroy.
- How do lifecycle rules affect the `terraform plan` and `terraform apply`?

- Lifecycle rules change the behavior of the plan and apply steps. For example, `ignore_changes` might show no changes in plan even if something has changed in reality.

15. What is the default behavior of Terraform when replacing a resource without lifecycle rules?

- Terraform destroys the old resource and then creates the new one — can lead to downtime.

16 . for each and count ?

`count` is used to create multiple identical copies of a resource by specifying how many instances you want.

Interview-question:

1) i want to create 3 ec2 instance with 3 different name, how can i create using terraform

The count parameter allows you to create multiple resources by iterating a fixed number of times. You can use a list to assign unique names for each instance.

```
resource "aws_instance" "web" {
  count         = 3
  ami           = "ami-0abcdef1234567890"
  instance_type = "t2.micro"

  tags = {
    Name = "web-${count.index}"
  }
}
```

`count = 3` → creates 3 EC2 instances.

You can access the instances using:

- `aws_instance.web[0]`

- `aws_instance.web[1]`
- `aws_instance.web[2]`

`${count.index}` gives you `0`, `1`, `2` respectively.

`for_each` lets you create resources from a **map or a set of strings**, giving each a **unique identity** using `each.key` and `each.value`.

```
variable "ec2_instances" {
  default = {
    "web1" = "t2.micro"
    "web2" = "t2.small"
    "web3" = "t3.micro"
  }
}

resource "aws_instance" "web" {
  for_each      = var.ec2_instances
  ami           = "ami-0abcdef1234567890"
  instance_type = each.value

  tags = {
    Name = each.key
  }
}
```

`for_each` iterates over a **map**.

`each.key` → `"web1"`, `"web2"`, `"web3"`

`each.value` → `"t2.micro"`, `"t2.small"`, `"t3.micro"`

Terraform will create 3 EC2 instances, each with a **unique name and instance type**.

Terraform - interview questions"

==========

Types of blocks in terraform:
1) resource block - Defines the creation and configuration of a specific resource.
2) variable block - Declares variables to make the configuration dynamic and reusable.
3) output block - Outputs information after the plan or apply stages.
4) provider block - Specifies the provider to interact with cloud services.
5) data block - Retrieves information about existing resources or infrastructure.
6) module block - Encapsulates reusable configurations in a separate directory or repository.
7) locals block - Defines local values to simplify expressions and reduce duplication.
8) provisioner block - Executes scripts or commands on resources during creation or destruction.

---

5. Data Block

A Data Block in Terraform is used to fetch information about existing resources or configurations. This is particularly useful when you need to retrieve data from resources created outside Terraform or by another module, without creating new resources.

* Non-destructive: Fetches data without modifying the infrastructure.
* Supports various providers like AWS, Azure, GCP, etc.
* Can be used as inputs to other resources, locals, or modules.

Example:

```
# Fetch the most recent Amazon Linux 2 AMI
data "aws_ami" "new_ami" {
  most_recent = true
  owners = ["amazon"]
  filter {
   name = ubuntu
   values = ["ubuntu_20"]
 }
}

resource "aws_instance" "ubuntu" {
  ami = data.aws_ami.new_ami.id
  instance_type = "t2.micro"
}
```

---

7. Local Block

The Locals Block defines local values within a configuration. These values are immutable and calculated once during the plan phase. Locals simplify complex expressions and reduce repetition

* Can reference variables, resource attributes, data sources, or other locals.
* Improves readability and maintainability of Terraform configurations.

```
# Define locals
locals {
  instance_type = "t3.large"
  tags = {
    Name        = "example-instance"
    Environment = var.environment
  }
}

# Use locals in a resource
resource "aws_instance" "example" {
  ami           = "ami-12345678"
  instance_type = local.instance_type
  tags          = local.tags
}
```

---

8. provisioner block

The Provisioner Block runs scripts or commands on a resource after it has been created or before it is destroyed. It is typically used for bootstrapping, installing software, or configuring the resource.

Two main types:
* Remote-exec: Executes commands on the remote resource.
* Local-exec: Executes commands on the machine running Terraform.

Can be used with creation_time and destruction_time.

Example: remote-exec

```
resource "aws_instance" "example" {
  ami           = "ami-12345678"
  instance_type = "t2.micro"
```

```
  provisioner "remote-exec" {
    inline = [
      "sudo apt-get update",
      "sudo apt-get install -y nginx"
    ]

    connection {
      type     = "ssh"
      user     = "ubuntu"
      private_key = file("~/.ssh/id_rsa")
      host     = self.public_ip
    }
  }
}
```

example: Local-exec

```
resource "aws_instance" "example" {
  ami           = "ami-12345678"
  instance_type = "t2.micro"

  provisioner "local-exec" {
    command = "echo ${self.public_ip} >> instance_ips.txt"
    when    = destroy
  }
}
```

Use Case: Delete temporary files created during the lifecycle of an instance.

```
resource "aws_instance" "example" {
  ami           = "ami-12345678"
  instance_type = "t2.micro"

  provisioner "remote-exec" {
    when    = destroy
    inline = [
      "rm -rf /tmp/my-app-data"
    ]
```

```
    connection {
      type        = "ssh"
      user        = "ubuntu"
      private_key = file("~/.ssh/id_rsa")
      host        = self.public_ip
    }
  }
}
```

Passing userdata in terraform :

```
resource "aws_instance" "example" {
  ami           = "ami-12345678"
  instance_type = "t2.micro"

  # Load script from a file
  user_data = file("init.sh")
}
```

Triggers for null resource:

The triggers argument in null_resource is used to force the recreation of the resource based on certain conditions.

```
resource "null_resource" "example" {
  triggers = {
    timestamp = "${timestamp()}" # Forces recreation on every run
  }

  provisioner "local-exec" {
    command = "echo 'Resource recreated due to triggers!'"
  }
}
```

* The resource is recreated every time Terraform is applied because timestamp() changes dynamically.

Interview-question:

1) i want to create 3 ec2 instance with 3 different name, how can i create using terraform

The count parameter allows you to create multiple resources by iterating a fixed number of times. You can use a list to assign unique names for each instance.

```
variable "instance_names" {
  default = ["instance1", "instance2", "instance3"]
}

resource "aws_instance" "example" {
  count         = length(var.instance_names)
  ami           = "ami-12345678"  # Replace with your AMI ID
  instance_type = "t2.micro"

  tags = {
    Name = var.instance_names[count.index]
  }
}
```

Steps to Configure S3 Backend for Terraform

* Terraform Code to Create the S3 Bucket

```
resource "aws_s3_bucket" "tf_state" {
  bucket = "my-terraform-state-bucket" # Replace with a globally unique name
  acl    = "private"

  versioning {
    enabled = true
  }
```

```
  lifecycle {
    prevent_destroy = true
  }

  tags = {
    Name        = "Terraform State Bucket"
    Environment = "Production"
  }
}
```

*** Create a DynamoDB Table (Optional, for State Locking)**

```
resource "aws_dynamodb_table" "tf_lock" {
  name         = "terraform-lock-table"
  billing_mode = "PAY_PER_REQUEST"
  hash_key     = "LockID"

  attribute {
    name = "LockID"
    type = "S"
  }

  tags = {
    Name        = "Terraform Lock Table"
    Environment = "Production"
  }
}
```

*** Configure the S3 Backend in Terraform**

```
terraform {
  backend "s3" {
    bucket         = "my-terraform-state-bucket" # Replace with your bucket name
    key            = "path/to/my/terraform.tfstate" # Path within the bucket
    region         = "us-east-1"                 # Replace with your bucket's region
    dynamodb_table = "terraform-lock-table"       # Optional, for state locking
    encrypt        = true                        # Encrypt state at rest
  }
}
```

Some of the most useful Terraform commands are:

* terraform init - initializes the current directory
* terraform refresh - refreshes the state file
* terraform output - views Terraform outputs
* terraform apply - applies the Terraform code and builds stuff
* terraform destroy - destroys what has been built by Terraform
* terraform graph - creates a DOT-formatted graph
* terraform plan - a dry run to see what Terraform will do
* terraform validate - check whether the configuration is valid

---

3) Null resource:

In Terraform, null resources are resources that do not represent any actual infrastructure but can be used to execute provisioners or other operations

```
resource "null_resource" "example" {
  triggers = {
    app_version = var.app_version
  }

  provisioner "local-exec" {
    command = "echo 'App version updated to ${self.triggers.app_version}'"
  }
}
```

---

4) What are sentinel policy

Sentinels are a powerful way to implement a variety of policies in Terraform

* Restrict how modules are used in the Private Module Registry
* Enforce explicit ownership in resources

5) What are the various levels of Sentinel enforcement?

Sentinel has three enforcement levels - advisory, soft mandatory, and hard mandatory.

* Advisory - Logged but allowed to pass. An advisory is issued to the user when they trigger a plan that violates the policy.
* Soft Mandatory - The policy must pass unless an override is specified. Only administrators have the ability to override.
* Hard Mandatory - The policy must pass no matter what. This policy cannot be overridden unless it is removed. It is the default enforcement level in Terraform.

---

5) Terraform workspaces:

Terraform workspaces allow you to manage multiple instances of a Terraform configuration within the same working directory. By default, Terraform uses a workspace called "default". However, additional workspaces can be created to separate environments (e.g., dev, staging, prod) or manage multiple configurations for the same infrastructure.

* Each workspace has its own state file. This helps you isolate and manage infrastructure changes for different environments or purposes.

```
# List all workspaces
terraform workspace list

# Create a new workspace
terraform workspace new dev

# Switch to an existing workspace
terraform workspace select dev

# Create another workspace (e.g., prod)
terraform workspace new prod
```

```
provider "aws" {
  region = "us-east-1"
}

resource "aws_s3_bucket" "example" {
  bucket = "my-bucket-${terraform.workspace}"
```

```
  acl    = "private"
}
```

If you're in the dev workspace, the bucket name will be my-bucket-dev.
In the prod workspace, it will be my-bucket-prod.

terraform init
terraform workspace select dev
terraform apply

---

6) State File Not Backed Up or Deleted with No Backup

Re-Import Resources: Use the terraform import command to manually re-associate resources with your configuration.

= terraform import aws_instance.example i-0abcd1234efgh5678

Although Terraform does not natively support bulk imports, you can automate the process using third party tool. Here's how:

= terraformer import aws --resources=ec2,s3 --regions=us-east-1

---

7) To use the output of one module as input to another module in Terraform:

* Define an Output: In the first module, declare an output for the value you want to share.

* Call the First Module: Use the first module in your root configuration, so its output becomes available.

* Pass the Output to the Second Module: Reference the output from the first module and pass it as an input to the second module.

* Declare the Input in the Second Module: In the second module, define a variable to accept the value.

HELM

1) **helm chart, how do we package our helm chart, publish and install in our k8s cluster?**

ANS:

To package, publish, and install a Helm chart in your Kubernetes cluster, you typically follow these steps

To create helm chart

- helm create <app-name>
- ls <app name>

Your Helm chart should have this structure:

```
mychart/
  Chart.yaml          # Chart metadata
  values.yaml         # Default configuration values
  templates/          # K8s manifest templates (Deployment, Service, etc.)
  charts/             # Subcharts (optional)
  .helmignore         # Files to ignore when packaging
```

Package the Helm Chart

Navigate to the directory containing the chart:

cd mychart
helm package .

This will create a `.tgz` file like `mychart-0.1.0.tgz`.

— Push to a Helm Repository (e.g., ChartMuseum, S3, GitHub Pages)

helm push mychart-0.1.0.tgz oci://myregistry.example.com/helm-charts

—- Add the Helm Repo

helm repo add myrepo https://yourusername.github.io/helm-charts
helm repo update

— Install the Chart into Kubernetes

helm install myrelease myrepo/mychart --values custom-values.yaml

— Upgrade or Uninstall

helm upgrade myrelease myrepo/mychart --values new-values.yaml

helm uninstall myrelease

---

2) Helpers.tpl explain?

ANS: The `helpers.tpl` file in a Helm chart is a **special template file** used to define **reusable template functions (helpers)** using Go templating syntax.

Purpose of `helpers.tpl`

- **Avoid repetition** in templates (e.g., labels, resource names)
- Centralize logic so that changes need to be made in only one place

Use helpers for:

- Naming resources
- Labels/annotations
- Conditional blocks (e.g., ingress class)

- Helm Components

a) Chart -

* is a collection of files contains all instructions that Helm needs to know to be able to create collection of objects that we need in our k8s cluster.

* using charts we can install applications into our cluster

b) Release -

* when a chart is applied to the cluster a release is created.

* A release is a single installation of an application using helm chart

* With each release can have multiple revisions

* each revision is like snapshot of the application
(any changes to deploy, pod, service etc, new revision is created)

c) metadata -

* keeps tracks of charts installed, revision state, to save data

* stores in Kubernetes as secrets

---

verify helm chart -- for error in syntax

1) lint -- helm lint ./nginx-chart
2) template -- helm template ./nginx-chart # shows the custom values from the custom-values.yaml or final template of deployment etc
   or
   -- helm template ./nginx-chart --debug
3) Dry run -- helm template ./nginx-chart --dry-run

CHART HOOKS

1) pre-upgrade

we use jobs to take backup before update like "backup.sh"

* we will have a file in templates directory as backup-job.yaml

* we should add annotations - "helm.sh/hook": pre-upgrade
* we can cleanup the hook using "helm.sh/hook-delete-policy": before-hook-creation

helm.sh/hook: pre-upgrade ensures the job runs before an upgrade.
helm.sh/hook-delete-policy: before-hook-creation cleans up the job if it already exists.

2) post-upgrade

A post-upgrade hook runs after the release is successfully upgraded. For example, you can run a script to verify that everything was upgraded correctly.

"helm.sh/hook": post-upgrade
"helm.sh/hook-delete-policy": hook-succeeded

3) pre-install & post-install

"helm.sh/hook": pre-install

"helm.sh/hook-delete-policy": hook-succeeded

4) pre-delete & post-delete

"helm.sh/hook": pre-delete
"helm.sh/hook-delete-policy": hook-succeeded

5) pre-rollback & post-rollback

"helm.sh/hook": pre-rollback
"helm.sh/hook-delete-policy": hook-succeeded

---

commands:

1) helm search hub <chartname>
2) helm repo add bitnami https:// charts.bitnami.com/bitnami
3) helm install <my-release name> bitnami/wordpress
4) helm list
5) helm unistall <release>
6) helm repo update
7) helm upgrade <my-release> bitnami/nginx --version 13
8) helm show values <chart> > values.yaml
9) helm pull bitnami/wordpress
10) helm pull --untar bitnami/wordpress # to get achieve of chart

Helm Lifecycle commands -

1) helm install my-release bitnami/wordpress --version x.x.x
2) helm upgrade my-release bitnami/wordpress
3) helm list
4) helm history
5) helm rollback <revision number>

AWS

1. VPC Peering

- VPC Peering is a network connection between two VPCs, allowing traffic to flow privately between them using private IPs.
- Peering can be:
    - Intra-region or Inter-region
    - One-to-one only (no transitive peering)
- Use case: Microservices in different VPCs or accounts.

2. VPC Flow Logs

- VPC Flow Logs capture IP-level traffic metadata (source, dest, port, accept/reject) for:
    - VPCs
    - Subnets
    - ENIs (Elastic Network Interfaces)
- Use case: Security monitoring, troubleshooting, and cost optimization.
- Can be stored in CloudWatch Logs or S3.

3. S3 Data Transfer

- S3 supports data transfer over:
    - Public Internet (default)
    - VPC Endpoint (PrivateLink) for private access from VPCs.
- Use case: Upload/download data, backups, data lake ingest.

4. S3 Object Locking

- S3 Object Lock protects objects from deletion or modification for a fixed time or indefinitely.
- Two modes:
    - Governance – Can be overridden by privileged users.
    - Compliance – Cannot be overridden (even by root).
- Use case: Regulatory compliance (e.g., WORM storage for financial data).

5. Direct Connect

- AWS Direct Connect provides a dedicated, private network link from your on-premises data center to AWS.
- Benefits:
    - Lower latency
    - Higher bandwidth
    - Secure (not via internet)
- Use case: Hybrid cloud setup, constant large data transfers.

✅ 6. Gateway Interface

This might refer to two services — let me explain both for clarity:

a. VPC Gateway Endpoint

- For S3 or DynamoDB only.
- Routes traffic within AWS network, without going over the internet.
- Uses route tables and does not require NAT.

b. Interface Endpoint (PrivateLink)

- Connects to AWS services or your own services over ENI (Elastic Network Interface).
- Works at network interface level.
- Use case: Accessing services like SSM, Secrets Manager securely in VPC.

ANSIBLE

1. **How would you manage secrets in Ansible during a CI/CD deployment pipeline?**

ANS:

Use **Ansible Vault to encrypt secrets** and store them securely in version control. Decrypt them at runtime using a CI/CD secret manager (e.g., GitLab secrets, Jenkins credentials). Avoid hardcoding secrets in playbooks.

2. **You have 10,000 servers to patch. How would you scale your Ansible execution?**

ANS:

Use **Ansible Tower/AWX** or **Ansible Automation Platform** for parallel execution and control.
Split inventory into batches and use `serial`, `forks`, or dynamic inventory to manage large-scale execution efficiently.

3. **How do you handle different OS families (Debian vs RedHat) in the same playbook?**

ANS:

Use conditionals like `when: ansible_os_family == 'RedHat'` and `when: ansible_os_family == 'Debian'` to apply specific tasks. You can also use variable files in `vars/RedHat.yml` and `vars/Debian.yml`.

4. **A playbook fails halfway during execution. How would you resume it safely?**

ANS:

Use `--start-at-task` to rerun the playbook from the failed task. Alternatively, use idempotent tasks so rerunning the playbook is safe without causing duplicate changes.

5. **How would you debug a playbook that randomly fails on certain hosts?**

ANS:

Use `-vvv` for verbose logging. Add `debug` or `register` statements to inspect variables. Use `serial: 1` to isolate hosts and examine patterns or flaky infrastructure issues.

6. **How do you use dynamic inventory with cloud platforms like AWS or Azure?**

ANS:

Use the AWS or Azure dynamic inventory plugins. Configure them in `ansible.cfg` and use cloud tags or filters to target specific groups.

7. **How would you enforce that only one host at a time runs a particular task (e.g., database migration)?**

ANS:

Use `serial: 1` in the play and lock the task using a `delegate_to: localhost` or `run_once: true` pattern.

8. **You want to update 100 nodes, but only 10 at a time. How would you do that in Ansible?**

ANS:

Use `serial: 10` in the playbook to limit the number of hosts being processed simultaneously. This helps control risk during rollouts.

9. **You need to deploy a file to different paths based on hostname. How would you structure your playbook?**

ANS:

Use host-specific variables in `host_vars/` and reference the path using `{{ file_path }}` in the task. Or, use a `when` condition with `inventory_hostname`.

10. **You’re using Ansible to provision infrastructure and apps. How do you separate these concerns?**

ANS:

Use separate playbooks or roles for infrastructure and application. Maintain different inventories or tags to run only the necessary parts.