===================== Shell scripts ==============

How to find a directory and then list the files inside it?

```
find . -type d -name "target_dir" -exec ls -l {} \;
```

How back up all .log files from a directory and move them to a backup folder with a timestamp?

```
#!/bin/bash
# Define source and backup directories
SRC_DIR="/home/user/logs"
BACKUP_DIR="/home/user/backup"
DATE=$(date +%Y%m%d)
# Create backup directory if it doesn't exist
mkdir -p "$BACKUP_DIR"
# Loop through each .log file in the source directory
for file in "$SRC_DIR"/*.log; do
    filename=$(basename "$file" .log)
    cp "$file" "$BACKUP_DIR/${filename}_$DATE.log"
    echo "Backed up $file to $BACKUP_DIR/${filename}_$DATE.log"
done
```

How to find all log files that have been modified within the last 5 hours?

```
find /path/to/search -name "*.log" -mmin -300
```

Write a shell script to Searches the pattern "error" from the log file created within 5hrs and generate a output   filename:line_number:error_line_text ?

```
#!/bin/bash
SEARCH_DIR=${1:-.}                    # $1 is unset or empty, use . (current directory) as the default
TIME_RANGE_MINUTES=300
find "$SEARCH_DIR" -type f -name "*.log" -mmin -"$TIME_RANGE_MINUTES" | while read -r logfile; do
    # Search for 'error' in the file, case-insensitive, print filename, line number, and the line
    grep -i -n "error" "$logfile" | sed "s|^|$logfile:|"
done
```

Write a program to check the health of the server using python script?

```
import requests
servers = ['http://192.168.1.10', 'http://192.168.1.11']
for server in servers:
    try:
        r = requests.get(server, timeout=5)
        if r.status_code == 200:
            print(f"{server} is up!")
        else:
            print(f"{server} returned status: {r.status_code}")
    except requests.RequestException:
        print(f"{server} is down or unreachable.")
```

How to take the terraform.tfstate file backup using python?

```
import os
import shutil
from datetime import datetime
def backup_tfstate(tfstate_path='terraform.tfstate', backup_dir='tfstate_backups'):
    # Ensure the tfstate file exists
    if not os.path.isfile(tfstate_path):
        print(f"Error: '{tfstate_path}' not found.")
        return
    # Create backup directory if it doesn't exist
    os.makedirs(backup_dir, exist_ok=True)

    # Create a timestamped backup filename
    timestamp = datetime.now().strftime('%Y%m%d_%H%M%S')
    backup_filename = f"terraform_{timestamp}.tfstate"
    backup_path = os.path.join(backup_dir, backup_filename)

    # Copy the tfstate file to the backup location
    shutil.copy2(tfstate_path, backup_path)

    print(f"Backup created: {backup_path}")

backup_tfstate()
```

===================== git and jenkins =============

Explain the Git Branching Strategy that you used in your company.

```
master
|
├── dev──────────feature
|        |                ├── feature1
|        ├── qa           ├── feature2 ( merge f1 and f2 to dev , qa testing is success )
|        ├── release  (create a tag/version, stage testing if success go for pre-prod deployment and testing )
|                |                 ( if pre-prod deployment and testing success merge to master )
|
├────────────────────deploy to pre-prod and test if success go to production
         ├──hotfix ( do same stage and pre-prod testing success merge to release and master )
```

Explain 3 challenges that you faced with Git during your work experience.

Explain the recent challenge that you faced with Git and how did you address it

Have you ever used Git tags ? If yes, why ?

To versioning the build we use git tag.

git tag -a v1.0.0 -m "Release version v1.0.0"

How do you combine Multiple commits into a Single commit ?

git rebase -i HEAD~3 ------- last 3 commit combine to single commite

A teammate accidentally committed a Kubernetes Secret (base64 encoded) to Git. What you will do ?

ANS-> Alert the team that a secret has been exposed.

Find which commit introduced it ---> git log -p -S "<part-of-secret>"

Removes the file from all commits in Git history using git filter-repo

git filter-repo --path k8s/secret.yaml --invert-paths

then git push origin --force --all and git push origin --force --tags

next Everyone need to re-clone or hard reset their local repos.

Update the Kubernetes secret:

kubectl delete secret <secret-name>

kubectl create secret generic <secret-name> --from-literal=key=value

now Update the value wherever it's used (apps, CI/CD pipelines, etc.)

Replace credentials or regenerate API keys if the secret was cloud-based (e.g., AWS, GCP, Stripe).

Not to repeate the same error we install pre-commit package pip install pre-commit

Write a script to detect conflict automatically, if there is no conflict merge the code?

Step 1 - Fetch latest branches
step 2 - Try merging dev into QA
step 3 - Abort if conflict is detected

```bash
#!/bin/bash

set -e

# Setup
git checkout QA
git pull origin QA
git fetch origin dev

# Attempt to merge
if git merge origin/dev --no-commit --no-ff; then
    echo "Merge successful, pushing to QA"
    git commit -m "Automated merge of dev into QA"
    git push origin QA
else
    echo " Merge conflict detected between dev and QA!"
    git merge --abort
    # Optional: send a notification or create a GitHub issue
fi
```

how to run two stage simaltaniously in jenkins?

```groovy
pipeline {
    agent any

    stages {
        stage('Parallel Stage') {
            parallel {
                stage('Stage A') {
                    steps {
                        echo 'Running Stage A'
                        // Your commands here
                    }
                }
                stage('Stage B') {
                    steps {
                        echo 'Running Stage B'
                        // Your commands here
                    }
                }
            }
        }
    }
}
```

I have 3 parallel jenkins stage if one will fail it should continue?

in the stage you mention the below

```groovy
steps {
    catchError(buildResult: 'SUCCESS', stageResult: 'FAILURE') {
         echo 'Running Task A'
         sh 'exit 1' // simulate failure
```

}

===================== Docker ====================

Port is Not Accessible on localhost even after Port mapping in Docker

execute docker run -p 8080:80 myimage or docker-compose.yml
check errors from docker logs <container_id_or_name>
check docker ps
0.0.0.0:8080->80/tcp ----------> if output is not like this then your port mapping isn't in effect
Test Connectivity
curl http://localhost:8080 and from container curl http://localhost:80

What is the purpose of EXPOSE in Dockerfile ?

It tells users and other developers which ports the application expects to be accessed on.
EXPOSE 80 --------- in docker file
or docker run -d -p 8080:80 myimage   manually

Docker Container Exits Immediately, how will you troubleshoot ?

docker ps -a ----- container id
docker logs <container_id or name> ---> see the container output before exiting.
check the Command specified in CMD or ENTRYPOINT is valid or not

difference between CMD or ENTRYPOINT?

ENTRYPOINT – Defines the main executable that will always run.
CMD – Sets the default command to run when the container starts, but can be overridden at runtime.

```
FROM ubuntu
ENTRYPOINT ["echo"]
CMD ["Hello from CMD"]
```

docker run myimage ------------------> Output: Hello from CMD

docker run myimage World ------------> # Output: World

EX 2

```
FROM python:3.11
ENTRYPOINT ["python"]
CMD ["app.py"]
```

------------> This will always run python app.py by default.

but if we do   docker run myimage -m venv venv   ----> it will execute python -m venv venv

You made change in your code, rebuilt the image, but the change isn't reflected?

Ensure your Dockerfile has copied your changed code
docker history your-image-name   --------> You can inspect the built image to confirm layers
remove the image and recreate

Difference between copy and add in docker file

copy and add will copy the file from source to destination
but in add it also extract the file from tar file after copying

ex

```
# Copy files into the container  COPY app.py /app/app.py
# Automatically extracts app.tar.gz into /app   ADD app.tar.gz /app/
```

App Crashes with "Permission Denied" in Container but works fine on localhost?

check container log → docker logs <container_id_or_name> or

```
    docker exec -it <container_id_or_name> /bin/sh    ---> cd /app/logs ---> tail -f app.log
```

Check File permissions Use chmod and chown if need to change the permissions

In dockerfile change the user to root (USER root) and try

Check the Volume mounts and check mapping permissions in docker-compose file

```
        volumes:
            - ./data:/app/data
```

Security configsConsider SELinux/AppArmor restrictions

```
    -v ./data:/app/data:z
```

Docker host is running out of disk space. How do you clean up?

docker system df check the space used

docker system prune remove the Stopped containers , Unused networks , Build cache

docker system prune -a -f removes all unused images

docker volume ls and docker volume inspect <volume_name> Check volume usage

delete the contents of a Docker volume without deleting the volume itself, after archiving

```
    docker run --rm \
        -v <volume_name>:/volume \
        -v $(pwd):/backup \
        alpine \
        tar czf /backup/<volume_name>.tar.gz -C /volume .

    docker run --rm \
        -v <volume_name>:/volume \
        alpine \
        sh -c "rm -rf /volume/* /volume/.[!.]* /volume/..?* || true"
```

How to optimize a Java build image that's currently 1.5 GB, even though you're already using a lightweight base image?

1. Use a Multi-Stage Build (for Docker)

first dockerfile

```
    FROM maven:3.9.6-eclipse-temurin-17 AS builder
    WORKDIR /app
    COPY . .
    RUN mvn clean package -DskipTests
```

2nd dockerfile

```
    FROM eclipse-temurin:17-jre-alpine
    WORKDIR /app
    COPY --from=builder  /app/target/your-app.jar .
```

2. exclude unnecessary dependencies, Logs or files from jar

```
    COPY --from=builder /app/target/myapp.jar app.jar
    ENTRYPOINT ["java", "-jar", "app.jar"]
```

How to filter stopped containers?

```
docker ps -a --filter "status=exited"
```

How will you Debug a Live Container ?

```
Check logs:                    docker logs --tail <number_of_lines> -f <container_id_or_name>
Inspect container metadata:  docker inspect <container_id_or_name>
```

when will you forcefully remove a container and how ?

The container is stuck or unresponsive

```
kubectl get pods  # Look for CrashLoopBackOff, Error
kubectl describe pod <pod_name>  # See events and termination reason
kubectl logs <pod_name> --previous  # Get logs from the previous instance (crashed)
```

to clean up zombie containers

```
docker container prune -f
```

to remove container ---> docker ps -a -f status=exited -q | xargs docker rm

================= Ansible ===============

Ansible ensures repeated executions produce the same result by only applying changes when needed? / How does Ansible handle idempotency?

example --> If Nginx is already installed, the task is skipped.

```
- name: Ensure Nginx is installed
    apt:
        name: nginx
        state: present
```

Example --> If the user "sumanta" already exists, Ansible skips the task

```
- name: Ensure 'sumanta' user exists
    user:
        name: sumanta
        state: present
```

Example --> If the service is already running and enabled, Ansible skips the task.

```
- name: Ensure Nginx is running and enabled
    service:
        name: nginx
        state: started
        enabled: yes
```

What is the purpose of Ansible Handlers?

A handler task in Ansible will not execute on its own, it will only run if a previous task use notify.
Example --> If the config file changes, the copy task will notify the restart nginx handler, otherwise the file didn’t change, the handler is not run.

```
- name: Ensure Nginx config is present
    copy:
        src: nginx.conf
        dest: /etc/nginx/nginx.conf
    notify: restart nginx

handlers:
    - name: restart nginx
        service:
            name: nginx
            state: restarted
```

=================K8S ===================

Applicaton access in a networks range in k8s ?

using ipBlock applicaton access in a networks range

```
ingress:
- from:
   - ipBlock:
        cidr: 192.168.0.0/16
```

how you can secure an application in k8s?

Use minimal base images

Scan images for vulnerabilities

```
jfrog xr scan docker-local/myapp:1.0 --format=json > xray-report.json
```

Store sensitive data in Kubernetes Secrets.

```
kubectl create secret generic my-secret \
        --from-literal=username=admin \                ------- from lietral
        --from-literal=password=secret123
                or
kubectl create secret generic my-secret \
--from-file=./mySecretFile.txt                         ------- from file
```

Set security contexts in k8 manifest file:

```
spec:
        securityContext:
                runAsNonRoot: true
        containers:
                - name: secure-container
                  image: busybox
                  command: [ "sh", "-c", "sleep 3600" ]
                  securityContext:
                        readOnlyRootFilesystem: true
                        allowPrivilegeEscalation: false
                        runAsNonRoot: true
```

Use NetworkPolicies to restrict communication between pods.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-frontend-to-backend
spec:
  podSelector:
        matchLabels:
                app: backend
  ingress:
        - from:
                - podSelector:
                        matchLabels:
                                app: frontend
  policyTypes:
        - Ingress
```

apply Ingress Security ---------- Advance topic

Use HTTPS for all traffic (TLS termination).

Enable Web Application Firewall (WAF) if supported (e.g., in cloud load balancers).

Set strict ingress rules to control which traffic reaches your services.
Add rate limiting, IP whitelisting, and header validation.

```
annotations:
    nginx.ingress.kubernetes.io/ssl-redirect: "true"            ---- Enforce HTTPS
    nginx.ingress.kubernetes.io/limit-connections: "20"                  ----  Rate limiting to protect abusing the system ( ex Only allow 20 requests per minute from each user.
    nginx.ingress.kubernetes.io/whitelist-source-range: "203.0.113.0/24" ---- Only devices with those IP addresses/ in group can access it
```

how to run a pod in a particular node?

nodeAffinity and preferredDuringSchedulingIgnoredDuringExecution and requiredDuringSchedulingIgnoredDuringExecution

what is readenessprob and livenessProbe?

Liveness Probe checks if the container is still running. If it fails, the container will be restarted.

Readiness Probe checks if the container is ready to handle traffic.
If it fails, Kubernetes will stop routing traffic to that pod. so the pod is removed from the service endpoints (url).

how to rollback k8 deployment from jenkins?

```
sh '''
   kubectl rollout undo deployment/your-deployment-name --to-revision=2 -n your-namespace
'''
```

What are the storage array you worked on?

We work on AWS EBS (elastic block storage), S3
io2 type EBS --> Critical business applications for databases like Oracle, SQL Server
gp3 type EBS --> For development/test environments / Web servers / App servers

how you create volume where the pod will run in same AZ (availability zone)?

Use volumeBindingMode: WaitForFirstConsumer ----> it will create the volume where the pod will be scheduled.

if you use volumeBindingMode: Immediate ----> it will create the volume without knowing where the pod will be scheduled. (mostly not recommended)

What is reclaimPolicy and how it is used in k8s? / How to manage lifecycle storage in cloud?

reclaimPolicy defines what happens to the PV when the PVC is deleted. So reclaimPolicy manage lifecycle for storage.

reclaimPolicy: Retain or reclaimPolicy: Delete

reclaimPolicy: Delete --> when you delete the PersistentVolume (PV)the data can not be retain

reclaimPolicy: Retain --> it keeps the PersistentVolume (PV) and delete the PVC so the data can be retain

What is storageClass in k8?

StorageClass defines the type of storage that can be dynamic provisioning of storage.
StorageClass defines the type of storage dynamically using
reclaimPolicy and volumeBindingMode
There is different storageClassName (fast, slow, standard) provided by the cloud provider.

storageClassName: fast --> usually refers to the storage with better performance , like SSD-backed volumes

storageClassName: slow --> this refers Cheaper, lower performance disks
storageClassName: standard --> general-purpose storage (e.g., magnetic or standard HDD)

How you can provision the storage dynamicaly in Kubernetes?

Define a StorageClass with a specific provisioner (e.g., AWS EBS)
Create PVC using that StorageClass.
Kubernetes automatically provisions a PV that matches the PVC using the StorageClass's configuration.
The PVC is bound to the newly created PV
A pod mounts the volume using the PVC.

Define storageClass

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: fast
provisioner: kubernetes.io/aws-ebs   # Or use CSI like ebs.csi.aws.com for containerized workloads
parameters:
    type: gp3
    fsType: ext4
    iops: "6000"          # Custom IOPS (minimum: 3000, maximum: 16000)
    throughput: "250"     # MB/s (max: 1000)
reclaimPolicy: Delete
volumeBindingMode: WaitForFirstConsumer
allowVolumeExpansion: true  # Enables `kubectl edit pvc` to resize
```

create PVC

```
    apiVersion: v1
    kind: PersistentVolumeClaim
    metadata:
        name: mypvc
    spec:
        accessModes:
            - ReadWriteOnce
    resources:
        requests:
            storage: 10Gi
    storageClassName: fast
```

Use the PVC in a Pod

```
apiVersion: v1
kind: Pod
metadata:
    name: mypod
spec:
    containers:
        - name: app
          image: nginx
          volumeMounts:
            - mountPath: "/usr/share/nginx/html"
              name: myvolume
    volumes:
```

```
                                    - name: myvolume
                                      persistentVolumeClaim:
                                      claimName: mypvc
```

Your team deployed a PersistentVolumeClaim (PVC) on EKS, but it remains in Pending state. The storageClassName is set to gp2. What could be the issue?

check available storage classes --- kubectl get storageclass
AWS deprecated gp2. So we need to use gp3 storageClassName or create a gp2 StorageClass manually

Your pod fails to start due to an EBS volume mounting error. Logs show AZ mismatch. What's wrong?

EBS volume created in one AZ cannot be attached to a node in another AZ.
So ensure your cluster uses WaitForFirstConsumer in the StorageClass.

```
volumeBindingMode: WaitForFirstConsumer
```

You need to retain an EBS volume for manual backup even if a PVC is deleted. How can this be achieved via StorageClass?
Use reclaimPolicy: Retain in your StorageClass

You're upgrading your cluster to use the AWS EBS CSI driver instead of the in-tree provisioner.
What changes must be made to StorageClasses?
Update your StorageClasses to use the new CSI provisioner

```
provisioner: ebs.csi.aws.com
```

On EKS you created a new StorageClass gp3-fast but PVCs still use gp3. How can you change the default StorageClass?
Patch the new class to be default

```
kubectl patch storageclass gp3-fast -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

================ AWS & Terraform =================

What are Policies?
what actions are allowed or denied on which AWS resources. Policy use to grant user access to resources/services
What are Roles?
A role uses policies to define what it can do. Role use to grant access between two services/resources

how you can insert ec2 from one region to another region in aws?

In the source region where the EC2 instance already exist:
Go to the EC2 Dashboard. --> Select the instance you want to move. --> Click Actions --> Image and templates --> Create image. --> Fill in the image name and click Create image.
The image (AMI) which you have created copy the AMI to the target region
Go to EC2 → AMIs in the source region --> Select your AMI → Actions → click Copy AMI --> Choose the destination region --> Rename it --> Click Copy AMI
Launch EC2 in the new region using the coped AMI

If you need certain volumes (EBS) then follow below as well,
you can Create a snapshot of the Source volume --> Copy the snapshot to another region --> Create a new volume from that snapshot. ---> Attach it to a new instance.
Go to the AWS EC2 Console ---> In the left-hand menu, click Volumes under "Elastic Block Store" --->

Select the volume attached to the source EC2 instance --> Click Actions → Create snapshot --> Fill in a name --> create

To Copy the Snapshot to Another Region ---> Go to Snapshots in the EC2 menu (under "Elastic Block Store")

--> Select the snapshot you just created --> Click Actions → Copy snapshot --> Choose the destination region --> Click Copy snapshotCreate a New Volume from the Snapshot

Create a New Volume from the Snapshot --> go to EC2 → Snapshots --> Find the copied snapshot --> --> click Actions → Create volume ---> Choose the Availability Zone where your new EC2 instance is ---> Select the volume type and size if needed → Create volume

Attach the New Volume to a New (or Existing) EC2 Instance ---> Go to EC2 → Volumes --> Select the new volume

--> Click Actions → Attach volume --> Choose the EC2 instance to attach it to --> -->Choose a device name (/dev/sdf)--> Click Attach volume.

What is ploicies?

Policies in AWS define the permissions what actions are allowed or denied on which resources (Ec2 , S3).

How to create policy in terraform?

Step 1 --> Create a datasource which use to retrive data from AWS

```
data "aws_iam_policy_document" "s3_read_only" {
        statement {
                effect = "Allow"

                actions = [
                        "s3:GetObject",
                        "s3:ListBucket"
                ]

                resources = [
                        "arn:aws:s3:::my-example-bucket",
                        "arn:aws:s3:::my-example-bucket/*"
                ]
        }
}
```

Step 2 --> create a policy which can be used for a role or user

```
resource "aws_iam_policy" "s3_read_only" {
        name   = "S3ReadOnlyPolicy"
        policy = data.aws_iam_policy_document.s3_read_only.json
}
```

what is IAM role?

An IAM role is a set of permissions in AWS that defines what actions are allowed or denied for a trusted entity such as a user, service(ec2), or application to perform specific actions on AWS resources

How to create a Role in IAM for Account A in AWS?

AWS Console → IAM → Roles → Create role → Choose trusted entity (ec2 , S3) → Attach permissions policies (S3ReadOnly , get)

→ Add tags (Key = Environment, Value = Production) → Name the role (ex-: EC2S3AccessRole) → Create role

How to create Role using terraform? / How to attach this policy to a role or user?

```
resource "aws_iam_role" "ci_cd_role" {
	name = "ci-cd-deploy-role"
	assume_role_policy = data.aws_iam_policy_document.assume_role_policy.json
}
```

What is IAM USER?

IAM users are individual identities in AWS assigned with credentials and permissions to access AWS services and resources securely

How to create IAM user in AWS? How to create user access key and secret key in AWS?

AWS console ---- IAM ---- add user ---- provide user name , aws access type --- attach policy ---- provide tag ---- click on create user

Now you will get the user name, access key, secret access key for that user and you can download the csv fie and save it.

How to enforce least privilege and secure access without manual intervention for user?

step 1--> create user

```
resource "aws_iam_user" "user" {
	name = "least-privilege-user"
	force_destroy = true  # Allows destroying user with keys attached
}
```

step 2 --> create policies and impose policy to the user

```
resource "aws_iam_user_policy" "readonly_s3" {
	name = "readonly-s3-policy"
	user = aws_iam_user.user.name
	policy = data.aws_iam_policy_document.s3_read_only.json
}
```

step 3 --> generating access keys via Terraform

```
resource "aws_iam_access_key" "user_key" {
	user = aws_iam_user.user.name
}
```

step 4 --> Enforce password reset at next login if you want console access

```
resource "aws_iam_user_login_profile" "login" {
	user   = aws_iam_user.user.name
	password_reset_required = true
	pgp_key  = "keybase:username"  # encrypt password automatically
}
```

How do you enforce least privilege (Minimal Permissions)access control in IAM AWS.

1 Apply permissions (s3:GetObject, ec2:StartInstances)only to specific resources (e.g., one S3 bucket, not all buckets)

2 Assign role to the user

3 Different roles for differnt activity (one role manages infrastructure, another deploys applications)

How can IAM policy deployment be terraform?

create IAM policy in Terraform using aws_iam_policy.

```
resource "aws_iam_policy" "example_policy" {
	name        = "MyExamplePolicy"
	description = "A test policy created by Terraform"
	policy      = data.aws_iam_policy_document.s3_read_only.json
}
```

How can IAM policy deploy as part of infrastructure code?

In terraform we can use " aws_iam_policy " for IAM policy.

```
resource "aws_iam_policy" "example_policy" {
  name        = "DescribeEC2Policy"
  description = "Allows describing EC2 instances"
  policy      = file("${path.module}/policy.json")
}
```

uses tags (attributes) to control access to resources

What is IAM Identity Center?

IAM Identity Center formerly known as AWS Single Sign-On to AWS accounts.

How to enable centralized user provisioning automatically?

Automated access can be managed using:

SCIM (System for Cross-domain Identity Management)

Attribute-based access control (ABAC) ----> uses tags (attributes --> Department = "Engineering") to control access to resources (ec2, S3)

Pre-configured permission sets mapped to roles across accounts ----> The company has many departments /accounts like Finance ,IT, HR and some departments (like IT) have sub-teams, like: IT Support , IT Development

What is (SCIM) System for Cross-domain Identity Management and how you could do it in terraform?

For an example your HR system (IT team) already keeps a list of who works at the company.
but you want all those people get access to AWS services automatically also update the access
when someone is hired, leaves, or changes roles.

```
aws-iam-hr-sync/
        │
        ├── scripts/
        │   └── hr_sync.py           # Script to pull user data from HR system
        │
        ├── data/
        │   └── example_hr_data.json    # Sample HR data (for dev/testing , team add data to this property file)
        │
        ├── main.tf                 # Main Terraform config
        ├── variables.tf             # Variable definitions
        ├── outputs.tf               # Output definitions
        ├── provider.tf              # AWS provider setup
        │
        ├── iam/
        │   ├── groups.tf            # IAM groups and policies per role
        │   ├── users.tf            # IAM user creation logic
        │   └── memberships.tf        # IAM user-to-group mapping
        │
        │
        ├── terraform.tfvars          # Values for variables (e.g., region)
        ├── .gitignore
        └── ci/
              └── Jenkinsfile      # (Or Jenkins, etc.) CI/CD automation
```

===== hr_sync.py ======

```
import json
```

```
        # Simulate HR system API
        employees = [
            {"username": "john.doe", "role": "developer"},
            {"username": "jane.smith", "role": "hr"},
            {"username": "jane.smith", "role": "IT"}
        ]

        # Transform to desired format / as a dictonary
        output = {}
        for idx, emp in enumerate(employees, start=1):
            key = f"user{idx}"
            output[key] = {
                "username": emp["username"],
                "role": emp["role"]
            }

        # Write JSON to a file
        with open("result.json", "w") as f:
            json.dump(output, f, indent=4)
```

==== example_hr_data.json ====

```
    {
        "users": {
            "john.doe": {
                "role": "developer"
            },
            "jane.smith": {
                "role": "hr"
            }
        }
    }
```

====main.tf==== external data source from scripts/hr_sync.py

```
        data "external" "hr_users" {
            program = ["python3", "${path.module}/scripts/hr_sync.py"]
        }
```

====variables.tf==== variables like region, default policy ARNs

```
    variable "default_policy_arn" {
        type    = string
        default = "arn:aws:iam::aws:policy/ReadOnlyAccess"
    }
```

==== groups.tf====   Defines IAM groups for roles like developer, hr, admin

```
    resource "aws_iam_group" "developer" {
        name = "DeveloperGroup"
    }
```

==== users.tf ====   Creates IAM users dynamically based on HR data

```
    resource "aws_iam_user" "users" {
        for_each = data.external.hr_users.result["users"]
        name = each.key
    }
```

==== memberships.tf ====== Maps IAM users to the appropriate IAM group

```
    resource "aws_iam_user_group_membership" "group_membership" {
        for_each = data.external.hr_users.result["users"]

        user   = aws_iam_user.users[each.key].name
        groups = [aws_iam_group.${each.value["role"]}.name]
```

```
}
```

How to provide access to the resources to the users in IAM?

we can provide access to the resource using Attribute-Based Access Control (ABAC).

Step 1 --> Tag IAM Users with Department Attribute

```
resource "aws_iam_user" "developer" {
	name = "dev-user"

	tags = {
		Department = "Engineering"
	}
}
```

Step 2 --> Tag AWS Resources (e.g., S3 Buckets)

```
resource "aws_s3_bucket" "dev_bucket" {
	bucket = "engineering-bucket-123"

	tags = {
		Department = "Engineering"
	}
}
```

Step 3 --> Create IAM Policy with ABAC Rules for resource

```
data "aws_iam_policy_document" "s3_abac_policy" {
	statement {
		effect = "Allow"

		actions = [
		"s3:GetObject",
		"s3:PutObject",
		"s3:ListBucket"
		]

		resources = [
		"arn:aws:s3:::*"
		]

		condition {
		test     = "StringEquals"
		variable = "s3:ResourceTag/Department"
		values   = ["${aws_iam_user.developer.tags["Department"]}"]
		}
	}
}
```

Step 4 --> Attach Policy to IAM User (Now User 'dev-user' can only access buckets that have the same 'Department' tag)

```
resource "aws_iam_policy" "s3_abac" {
	name       = "ABACPolicy"
	policy     = data.aws_iam_policy_document.s3_abac_policy.json
}

resource "aws_iam_user_policy_attachment" "dev_user_policy" {
	user       = aws_iam_user.developer.name
	policy_arn = aws_iam_policy.s3_abac.arn
}
```

How do you secure pipeline identities accessing AWS resources?

Use IAM roles with limited session duration (session_duration = "PT4H")

Avoid long-lived credentials (max_session_duration = 14400)
Enable MFA for human access
Use Audit logging via CloudTrail to monitor access

What is a secure pattern for deploying to multiple AWS accounts using a CI/CD pipeline? /
Use cross-account role assumption with trust policies?

If your Jenkins setup includes Folders, you can :
Create a folder. --- Move the job into the folder. --- Apply Folder-level authorization / Role-Based Plugin on target folder

How do you audit and validate access control in automated pipelines?
Use AWS Access Analyzer for policy validation
AWS Console -- IAM -- Add a New User -- Configure User Details and AWS access type --
Check "Access key and Check "Password -- Next -- Attach policies directly -- Add Tags --
-- Review and Create user
Now use IAM Access Analyzer to validate policy
IAM --> Policies --> Click on the name of the policy attached to your user ---> choos "Policy actions" dropdown
and select "Validate policy".
or
IAM > Users --> click on the user whcih you have created --> Permissions tab --> click on the policy name from policy list
--> click "Validate policy" using Access Analyzer

Run IAM Access Advisor and IAM Policy Simulator
The IAM Access Advisor shows which AWS services a user has accessed and when

How do you rotate credentials and secrets automatically?
AWS Secrets Manager or SSM Parameter Store with automatic rotation.
AWS Console — Secrets Manager — Store a new secret -- Select secret type -- Provide secret key-value pairs
(e.g., username, password) -- Click Next -- Secret name -- add description and tags
-- Enable automatic rotation -- Set rotation interval (e.g., every 30 days) -- Click Next -- Click Store

How do you rotate credentials and secrets automatically using terraform?

How would you secure an S3 bucket?

Block public access settings ==> S3 Console -- Click on your bucket name. -- "Permissions" tab.-- "Block public access
Use bucket policies ==> S3 Console -- Click on your bucket name. -- Properties -- Permissions -- Bucket Policy

Enable encryption (SSE) ==> S3 Console -- Click on your bucket name. -- Properties -- Scroll down to "Default encryption

IAM policies for least privilege ==> Go to IAM > Users or Roles -- Assign policies on the bucket

Enable logging and monitoring

What is S3 pre-signed URL and how it is used?
A pre-signed URL is a URL that includes:
The bucket name and object key.

AWS access credentials (embedded securely).
An expiration time.
A signature
ex --> https://my-bucket.s3.amazonaws.com/docs/invoice.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=...

What is S3 event?

S3 event refers to a notification that is triggered by a specific action in an Amazon S3 bucket.
s3:ObjectCreated:* – Triggered when a new object is uploaded.
Includes subtypes like Put, Post, Copy, and CompleteMultipartUpload
s3:ObjectRemoved:* – Triggered when an object is deleted.
Includes Delete, DeleteMarkerCreated
s3:ObjectRestore:* – Triggered when an object is restored from Glacier.
s3:ReducedRedundancyLostObject – Triggered when an RRS object is lost.

How to create event in S3?

S3 Console -- your bucket name -- Properties -- Event notifications -- Create event notification
-- name , Event types: (e.g., All object create events) , Destination: Choose Lambda, SNS topic, or SQS queue
-- Click Save

How to create event in S3 using terraform?

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

# --- 1. Create an S3 bucket ---
resource "aws_s3_bucket" "example" {
        bucket = "my-example-s3-bucket-12345"
}

# --- 2. Create a Lambda function --- / use Lambda function already exists
data "aws_lambda_function" "existing_lambda" {          ||
        function_name = "my-existing-lambda"            ||---- use Lambda function already exists
}                                        ||

# --- 3. Allow S3 to invoke the Lambda function ---
resource "aws_lambda_permission" "allow_s3" {
        statement_id  = "AllowS3Invoke"
        action        = "lambda:InvokeFunction"
        function_name = data.aws_lambda_function.existing_lambda.function_name
        principal     = "s3.amazonaws.com"
        source_arn    = aws_s3_bucket.example.arn
}

# --- 4. Configure S3 Event Notification ---
resource "aws_s3_bucket_notification" "bucket_notification" {
bucket = aws_s3_bucket.example.id

lambda_function {
        lambda_function_arn = data.aws_lambda_function.existing_lambda.arn
        events              = ["s3:ObjectCreated:*"]
        filter_prefix       = "uploads/"
        filter_suffix       = ".jpg"
}
```

```
    depends_on = [aws_lambda_permission.allow_s3]
    }
```

where terrafrom is installed in your organization? and how you are accessing it?

Terraform is installed on a remote internal server.

To access it login to jump server ---> login remote machine ---> access terrafrom (using terrafrom init / plan /apply)

create 3 instance with differnt aim usign for_each loop?

```
    variable "instances" {
        default = {
            instance1 = {
            aim = "web-server"
            ami = "ami-0c55b159cbfafe1f0"
            instance_type = "t2.micro"
            }
            instance2 = {
            aim = "database"
            ami = "ami-0c55b159cbfafe1f0"
            instance_type = "t2.medium"
            }
            instance3 = {
            aim = "cache"
            ami = "ami-0c55b159cbfafe1f0"
            instance_type = "t2.small"
            }
        }
    }

    resource "aws_instance" "example" {
        for_each = var.instances

        ami           = each.value.ami
        instance_type = each.value.instance_type

        tags = {
            Name = each.key
            Aim  = each.value.aim
        }
    }

    output "instance_ids" {
        value = { for k, inst in aws_instance.example : k => inst.id }
    }

    output "instance_aims" {
        value = { for k, inst in aws_instance.example : k => inst.tags["Aim"] }
    }
```

What are the componets of vpc?

```
     VPC
      |---Subnets (VPC IP range)      --- create ips
          |          |----- public ips
          |          |----- private ips
```

```
|---Route Tables                                --- to access internet
|           |----- Public subnets → Route Table with NAT Gateway                    <--------|
|           |----- Private subnet → Route Table with NAT Gateway access    ------|  ( Nat gateway help to access internet )
|           |----- Private subnet  ------ without NAT gateway acess
|---Internet Gateway (IGW)
|---NAT Gateway / NAT Instance
|---Security Groups
|             |----- ssh
|             |----- http
|             |----- tcp
|---Network Access Control Lists (NACLs) --- to Control traffic in and out of subnets
|---VPC Peering  ---- Communication across two or more VPCs
|---VPN Gateway  ---- Secure connection between on-premise network and VPC over the internet
|---Elastic IP Addresses
|---DHCP Option Sets ---- Assign domain names, DNS servers, etc.
```

How Nat gateway work? / How a private subnet access internet?

The private instance can access the internet using Nat gateway,
but the internet cannot access the private instance directly.
Nat gateway does not allow inbound connections from the internet to the private instance.
NAT Gateway, which knows how to route the response, So the response from the internet comes back to the NAT Gateway, then to the private instance.

A private EC2 instance (e.g. backend EC2) wants to access the internet (e.g., to download a package)sends a request through route table. Route table routes (0.0.0.0/0) request to the NAT Gateway.
The request goes to the NAT Gateway, which lives in a public subnet.
NAT Gateway receives the traffic, and translates the source IP from the private EC2 IP (e.g., 10.0.2.15) to its own Elastic IP (e.g., 18.234.56.78)   (Elastic IP attached to nat gateway)
Note ---> NAT Gateway + Elastic IP = One-Way Internet Access
Then NAT Gateway forwards the request to the Internet Gateway.
The response from the internet comes back to the NAT Gateway, then to the private instance.

Your private EC2 instance cannot access the internet, even though a NAT Gateway is set up in the public subnet. What could be the issue?

The route table associated with the private subnet doesn't have a route to the NAT Gateway (no 0.0.0.0/0 to NAT GW).
NAT Gateway is not properly associated with the Elastic IP (required for internet access)
Network ACLs/Security Groups are blocking outbound traffic.
NAT Gateway is in an Availability Zone that's different from the private subnet and there's no route between them.

How can you reduce NAT Gateway data transfer charges?

Use VPC Endpoints (S3, DynamoDB): Avoid routing traffic through the NAT Gateway for AWS services.
Minimize unnecessary outbound internet traffic (e.g., OS updates, telemetry).
Aggregate data transfers (e.g., through a single instance or batch processing).

You set up a new NAT Gateway in a public subnet, but none of the private EC2 instances can reach the internet. What might be misconfigured?

NAT Gateway is in a public subnet (must have a route to the Internet Gateway).
Private subnet has a route to the NAT Gateway (0.0.0.0/0 → NAT GW).
Security Groups allow outbound traffic (usually default allows all).
The Elastic IP is associated and not released.
NACLs do not block the traffic.

How you Ensure NAT Gateway is in a Public Subnet and route to an Internet Gateway (IGW)?

Go to VPC Console → public Subnets where the NAT Gateway is deployed -- Check the Route Table -- Select the associated route table → Edit routes -- fill (Destination: 0.0.0.0/0 and Target: Internet Gateway) -- save

How you will confirm Private Subnet Routes to NAT Gateway?

VPC Console → private Subnet which need to connect internet -- Route Table -- Ensure there is a route (Destination: 0.0.0.0/0 → Target: NAT Gateway)

How you Ensure the private subnet has a security group whcih allowing outbound traffic?

EC2 Console → private EC2 Instances -- click Security Group -- Outbound rules (Type: HTTP, HTTPS, and Destination: 0.0.0.0/0)

How to ensure that an Elastic IP (EIP) is attached and not released for your NAT Gateway?

VPC Console -- NAT Gateways -- In the NAT Gateway details, look for the Elastic IP address

If Elastic IP address is not present, then nat gateway is not attach to Elastic IP

To add Elastic ip

Open the EC2 Console -- choose Elastic IPs under Network & Security -- Allocate Elastic IP address -- Allocate
Then select newly created Elastic IP -- Click Actions → Associate Elastic IP address -- Choose NAT Gateway -- Click Associate.

You created two NAT Gateways in different Availability Zones (AZs) for high availability.
Still, your private subnet traffic isn't failing over during AZ issues. Why?

Use multiple NAT Gateways (one per AZ) and assign AZ-specific route tables.

A private EC2 instance needs to download patches from the internet during maintenance. There is no NAT Gateway set up.
How can you enable temporary access?
Temporarily move the instance to a public subnet and assign an Elastic IP.
Add a NAT Instance (manual, but quick if NAT Gateway not preferred).
Create a temporary NAT Gateway, route the subnet to it, then delete after use.

How to Move the Instance to a Public Subnet?
Stop the EC2 instance in private subnet
Create an AMI from the instance (right-click → Create Image)
Launch a new EC2 instance in a public subnet, using newly created AMI
then do your work and then erminate the original instance if no longer needed.

A NAT Gateway is created, but it is still not passing any traffic. What should you check in the public subnet?
The subnet has a route to the Internet Gateway.
The NAT Gateway is associated with an Elastic IP.
The public subnet's route table must allow outbound access.
The NAT Gateway's ENI (Elastic Network Interface) is active and in the correct AZ.

Can NAT Gateway be used to allow inbound traffic to private subnets?
No, NAT Gateway only allows outbound internet traffic from private subnets.
For inbound access, use: Load Balancer in public subnet routing to private instances / Application Load Balancer

How to configure Route table in AWS?
VPC Dashboard -- Route Tables > Create route table -- Enter a name and select your VPC -- Create route table

Select your new route table -- click Edit routes -- Add routes
|----- Add 0.0.0.0/0 → Internet Gateway (IGW) |
|----- 10.0.2.0/24 → if other VPC Peered (the ip is for other VPC)|
-- Click Save-- Click Subnet Associations > Edit subnet associations -- Select the subnets that should use this route table --- Click Save

A host in a local network can communicate with other hosts in the same subnet but cannot reach any external websites.
What could be the issue in the routing table?

The most likely issue is that the default route (0.0.0.0/0) is either missing or incorrectly configured in the routing table. This default route is essential for directing traffic destined for external networks e.g., the internet) to the default gateway.

For 192.168.1.0/24 via Router A and 192.168.1.0/25 via Router B which one has more specific (longer) subnet? Which route will be chosen, and why?

/25 is a more specific (longer) subnet than /24, because it uses more bits for the network portion and allows fewer hosts.

In IPv4, an IP address is 32 bits long (8bit + 8bit + 8bit + 8bit ---- for ip address)
/25 means the first 25 bits are used for the network portion. (11111111.11111111.11111111.10000000)
7 bits (32 - 25) for the host portion.
2^7 = 128 no of total IP addresses.

but for /24 -- total ip addresses is 2^8 = 256

In this case it will choose Router B because it is more specific (longer subnet mask).

In AWS, an EC2 instance in a private subnet can't access the internet, even though it has a NAT gateway.
What should you check in the route table?

Verify the private subnet's route table has a route like:
0.0.0.0/0 → NAT Gateway ID
If this route is missing or incorrect, internet-bound traffic will not reach the NAT gateway.

What are the storage array you worked on?

I worked on AWS EBS, S3
io2 type EBS --> Critical business applications for databases like Oracle, SQL Server
gp3 type EBS --> For development/test environments / Web servers / App servers

You have a VPC with two subnets: one public and one private. You launch a web server in the public subnet and a database server in the private subnet. The web server needs internet access; the DB must not. How do you configure this?

Step 1 - Attach an Internet Gateway (IGW) to the VPC.

VPC Dashboard → Internet Gateways -> Create internet gateway → Name it -> Click Create internet gateway
-> Select your new IGW → Click Actions → Attach to VPC -> Choose your VPC -> Click Attach internet gateway

Step 2 - Route the public subnet's traffic to the IGW via a route table.

VPC Dashboard → Route Tables -> Find associate it with your VPC or create a route table -> associate with public subnet

Select that route table → Go to Routes tab → Click Edit routes → Add route

Destination: 0.0.0.0/0

Target: Choose your Internet Gateway

Save the route

Go to the Subnet associations tab → Edit subnet associations → Select your public subnet → Save

Step 3 - Ensure the public subnet has an auto-assigned public IP or Elastic IP.

VPC Dashboard → Subnets → Select your public subnet -> Click Actions → Modify auto-assign IP settings

-> select Enable auto-assign public IPv4 address → Save

or

EC2 Dashboard → Elastic IPs → Allocate Elastic IP address -> select Elastic IP address ->

-> Allocate your EC2 instance in the public subnet

Step 4 - The private subnet has no route to the IGW — only to internal VPC traffic.

Go to Route Tables in the VPC dashboard -> Select the private subnet's route table -> ensure there's no

route to 0.0.0.0/0 for no IGW route -> Has only the local route

Step 5 - Use security groups to allow HTTP/HTTPS to the web server and allow only internal traffic to the DB.

For public Subnet -> EC2 Dashboard → Security Groups → Create or select security group ->Inbound rules

-> HTTP , HTTPS , SSH is enable

for private subnet -> EC2 Dashboard → Security Groups → Create or select security group ->Inbound rules

-> TCP (specify your required port) -> No outbound

You have two VPCs in the same AWS region. You want instances in VPC-A to talk to instances in VPC-B securely. How do you do it?

Create a VPC Peering Connection between VPC-A and VPC-B from both sides.

VPC Dashboard -> click Peering Connections -> Create Peering Connection -> fill Requester VPC and Accepter VPC

After creation, go back to Peering Connections -> Find and Select the new connection -> Click Actions → Accept Request.

Update route tables in both VPCs to route traffic to each other's CIDR blocks via the peering connection from both side.

VPC dashboard, go to Route Tables -> Find the route table associated with VPC-A -> Click Edit Routes → Add Route

-> Destination: VPC-B's -> Target: Select the Peering Connection ID -> save

Ensure security groups allow traffic from the peer VPC's CIDR.

in VPC-A -> Go to Security Groups -> Select the Security Groups -> Click Inbound Rules → Edit Inbound Rules → Add Rule

-> Type: Custom TCP , Source: CIDR block of VPC-B (e.g., 10.1.0.0/16) -> save

Do the above all steps in VPC-B

You have a private subnet where EC2 instances need to access the internet for updates (e.g., apt-get), but you don't want them to be publicly accessible. How do you achieve this?

Launch a NAT Gateway in a public subnet.
Assign an Elastic IP to the NAT Gateway.
Update the route table of the private subnet to send 0.0.0.0/0 traffic to the NAT Gateway.
The NAT Gateway forwards requests to the internet and returns the responses, while instances remain private

What's the difference between a Security Group and a Network ACL in VPC?
NACLs to block IP ranges across an entire subnet; use SGs for app-specific access.
Go to VPC Dashboard → Network ACLs ; Go to EC2 Dashboard → Security Groups

You want your EC2 instances in private subnets to access S3 without going through the internet. How do you do that?

Create a VPC Endpoint of type Gateway for S3.
Select the appropriate route table(s) and subnets.
Add an entry in the route table:
Destination: S3 prefix list → Target: VPC Endpoint.
Now traffic to S3 stays within AWS and doesn't need a NAT Gateway or Internet Gateway.

You need to set up a custom VPC with high availability. What's a standard best-practice layout?

VPC with at least 2 public and 2 private subnets, spread across 2 Availability Zones.
Internet Gateway attached to VPC.
NAT Gateway in each public subnet for private subnet internet access.
Route tables per subnet type.
Use Security Groups, NACLs, and CloudWatch Logs for security and monitoring.

What is PreSigned URL for an S3 Object and how to Create a PreSigned URL for an S3 Object via AWS Console?

A Pre-Signed URL in Amazon S3 is a temporary, secure link that gives anyone limited access to an S3 object (file)
without AWS credentials.

'S3' service -> Click on the bucket -> Select the Object -> Click on the Actions -> Share with a pre-signed URL
-> Select the minutes/ hours -> click Generate Presigned URL

example of a pre-signed url --> https://focus_allstate.s3.amazonaws.com/searchRetrive/