1. **Key Recovery**

Ans:- In AWS we can recover the key in two ways

1. **custom image**: In this method we have to replace the server . we have to create custom image of the server , need to know private ip , subnet , and vpc . In Ec2 creation time using AMI have to use previous private IP only , so we have to terminate the lost key Ec2 instance
2. **volume method** : No need to replace the server but we required one more server for recover the key . first we have to create a launch a new ec2 instance with same key pair. Then stop the lost key serve server then detach the root volume and attached with the new server. Connect the new ec2 instance and check the volume by the command

# lsblk

Create a new directory

# mkdir /recovery

Mount the volume

# mount nouuid /dev/sdb1 /recovery

Copy the key to the directory

# cp -p /home/ec2-user/.ssh/authorized\_key /recovery

Then unmount it

# umount /recovery

**Note**: we recover the key if the key is lost from the server side . And if key is lost from the aws side or from oue local pc we can not recover the key. For this we have to create the new key pair .

**2. S3 Cross Account Access**

**3. Role and Policy association using IAM to user and service**

**Ans:- IAM policy :** policy associate with the user

**IAM Role**: IAM Role associate with the AWS services .

When we want to communicate two aws services without involving the user we use IAM Role .

IAM Role cannot be associate with the user.

**4. How many ways we can generate the IAM Policy**

**Ans:- There are many ways**

1. AWS managed policy
2. customer managed policy
3. Inline policy (IAM🡪IAM user🡪permission🡪Add Inline policy)
4. Policy generator tool

**5. How many ways we can connect VM**

**Ans:-** We can connect the vm by

1. RDP
2. AWS System Manager
3. EC2 intance connect
4. Mobaextream
5. Putty
6. Ssh

**6. How to extend disk/partition**

**Ans:-** To extend the disk partition we have to modify EBS volume size

EC2🡪Volume🡪Select the volume🡪Action🡪Modify volume

Step2: Extend the partition and filesystem inside the EC2 instance .

# lsblk

# growpart /dev/xvda1 (Grow the partition)

# resize2fs /dev/xvda1 (resize the filesystem for ext4)

**7. How to configure backup**

**8. Your VM is not booting how to troubleshoot**

**9. How 22 traff will come into your VM**

Ans:- You (MobaXterm)

│

▼

Internet

│

▼

Internet Gateway (IGW)

│

▼

Route Table (0.0.0.0/0 → IGW)

│

▼

Network ACL (allows 22)

│

▼

Security Group (allows 22)

│

▼

EC2 Instance (sshd running)

**10. Difference between IGW AND NGW**

Ans:- **Internet Gateway vs NAT Gateway**

**Internet Gateway (IGW)**

An Internet Gateway allows resources in a VPC (e.g., EC2 instances in public subnets) to connect to the internet and enables incoming connections from the internet.

**Key Features:**

* **Bidirectional Traffic**: Supports both inbound and outbound traffic between your VPC and the internet.
* **Attached to VPC**: Must be attached to the VPC for the resources to access the internet.
* **Public IP/Elastic IP Required**: Instances must have a public or Elastic IP for internet communication.
* **Free Service**: AWS does not charge for using an Internet Gateway.

**Use Case:**

* Hosting publicly accessible resources, such as websites or APIs, where external users need access.

**NAT Gateway (NGW)**

A NAT (Network Address Translation) Gateway allows instances in private subnets to access the internet or other AWS services **without exposing themselves to inbound internet traffic**.

**Key Features:**

* **Outbound Traffic Only**: Supports outbound connections (e.g., downloading updates, accessing APIs) but blocks inbound traffic from the internet.
* **Private Subnets Only**: Used for instances in private subnets to access the internet securely.
* **Charged Service**: AWS charges for NAT Gateway usage based on data transfer and hourly costs.

**Use Case:**

* Allowing private EC2 instances to access the internet.

**11. How your private VM will communicate with internet**

**Ans:-** private vm don’t have public ip to communicate with the internet. To communicate the private vm to the internet we have to create NAT GATWAY (NGW) in public subnet and we have to add the route of the NAT GATWAY in the route table .

**12. How to connect your S3 with VM privately**

Ans:- Steps to Connect S3 Privately to a VM (EC2)

1. Ensure EC2 and S3 Are in the Same Region

* Your EC2 instance and S3 bucket must be in the same AWS region.

2. Create a VPC Gateway Endpoint for S3

📍 Go to AWS Console > VPC > Endpoints

* Click "Create Endpoint"
* Service Category: AWS Services
* Service Name: com.amazonaws.<region>.s3
* Type: Gateway
* VPC: Select your VPC
* Route Tables: Select the route tables of the subnets where your EC2 instance resides
* Click "Create Endpoint"

3. Update Route Table

When you attach the gateway endpoint, it adds a route like:

Destination: pl-xxxxxxxx (S3 prefix list) → Target: vpce-xxxxxxx

This makes S3 reachable without internet.

4. Remove Internet Dependency (Optional)

* If you want completely private access, do NOT associate an Internet Gateway (IGW) or remove the S3 call from NAT.
* Ensure there's no 0.0.0.0/0 via IGW or NAT Gateway for S3 traffic.

5. IAM Role or Instance Profile

Ensure your EC2 instance has an IAM role with the right permissions:

{

"Effect": "Allow",

"Action": "s3:\*",

"Resource": "arn:aws:s3:::your-bucket-name/\*"

}

6. Test Access from EC2

Once all is set:

aws s3 ls s3://your-bucket-name --region your-region

This will work without internet access if the endpoint is set up correctly**.**

**13. What is the use case of EFS**

Ans:- Amazon EFS (Elastic File System) is a fully managed, scalable, shared file storage service for use with Linux-based workloads in the AWS Cloud. It's a Network File System (NFS) that multiple EC2 instances can mount simultaneously.

**14. Your VM is not able to mount the EFS how to troubleshoot**

**15. You are not able to SSH into VM how to fix**

Ans:- (i)First check the pinging of the client system. If it is not pinging then check the IP address of the client system. If client system and sever system are in different domains or networks it will not ping. So, bring the client system into the network of the server system. Check the network is working or not and also check whether the network cable is connected or not.

(ii)If both systems are pinging then check whether the **openssh** package is installed or not. If not installed then install that package and configure ssh on the client system and restart the sshd deamon.

(iii)Check the client <IP address or hostname> in **/etc/hosts.deny** files. If there is an entry of the client system in this file, then remove that entry and restart the sshd deamon.

(iv) Finally open the ssh configuration file by # vim /etc/ssh/sshd\_config and see any client user name is present or not and check other lines for client entries in this file, if present remove those entries, save that file and restart the sshd service.

(v) Finally check whether the client user is there in the server or not, if not create the client user, assign the password share those details to client. If user is there then check whether the client user's password is locked, account expired and any other or not, if locked then remove the lock, if client account is expired then activate that account, assign the password and make the ssh trusting between client and server systems.

**16. How will you patch the servers**

**17. How many servers are there in your environment**

Ans:- there are 150 servers.

**18. How many linux and windows servers are there**

Ans:- there are arount 60-70 is linux and rest of them are windows

**19. How many environment are there**

Ans:- There are three environment

1. Prod
2. Non-prod
3. Testing

**20. What is the use of Elastic IP**

Ans:- A elastic IP address is static IPv4 address designed for dynamic cloud computing.

**21. What is WAF**

**22. What is LB and how to setup**

Ans:- LB (Load Balancer) is a system that distributes incoming network traffic across multiple targets (like EC2 instances)

**Step 1️⃣: Create Target Group**

1. Go to **EC2 Console → Target Groups**
2. Choose:
   * **Target Type**: Instances or IP
   * **Protocol**: HTTP or HTTPS
   * **Port**: 80 (or your app port)
3. Register your EC2 instances in the target group.

**Step 2️⃣: Create Load Balancer**

1. Go to **EC2 Console → Load Balancers**
2. Choose **Application Load Balancer**
3. Set:
   * Name
   * Scheme: Internet-facing or Internal
   * IP address type: IPv4
4. Select **Availability Zones** and **subnets**

**Step 3️⃣: Configure Listener**

* Default: HTTP on port 80
* Forward request to the **target group** you created

**Step 4️⃣: Set Security Groups**

* Allow HTTP (port 80) or HTTPS (port 443)
* Optional: Add rules for health checks

**Step 5️⃣: Test the Load Balancer**

* Use the **DNS name** given by AWS (e.g., my-alb-123456.elb.amazonaws.com)
* You should see traffic being load balanced across registered EC2s.

**22. what is the difference between ALB and NLB**

**23. What is ASG and how to setup**

**24. What is the use case of SSM**

**Ans**:- AWS system manager is service that’s helps you to manage , control and automate your server (ec2 and on-prem) from one place.

Main feature of AWS system manager:

* 1. **Session manager**: connect EC2 (like ssh)without key pair or opening port 22 .
  2. **Run Command:** Run shell scripts or command on multiple EC2 from one place
  3. **Parameter Store** : store and manage secrets or config data (like password , DB name)
  4. **Pach Manager** : Automate install update or patches on EC2
  5. **Inventory** : collect software and configuration info from your instance
  6. **Automation :** create workflows to automate command task (like reboot , backup etc) .

**25. What is ACM**

**Ans:** ACM stands for AWS Certificate Manager.

It is a managed service that helps you provision, manage, and deploy SSL/TLS certificates easily and securely on AWS services**.**

**26. What is SSL Certificate.**

**27. How to renew the SSL Certificate**

**28. Suppose if two servers are supporting one application how will you patch those servers without down the application**

**29. What is 3/3 Checks on VM**

**Ans**:- When we create a instance AWS perform two health checkup by using cloudwatch matrices

* 1. **System status check** : AWS backend virtual infra means it will check the hardware side .
  2. **Instance status check (os level helth check):** Here AWS will check the connectivity grom hypervisor to instance
  3. **Application Health check**: This is a user-defined health check (common in Auto Scaling Groups, ELB, or monitoring tools) to verify whether the application running on the VM is healthy.

**30. Difference between SG nd NACL and what is the usecase**

**Ans:- SG:**

* + It’s a virtual firewall to filter the traffic .
  + It’s a instance level firewall
  + It’s a state full firewall: only one side traffic will check either inbound or outbound
  + We can allow the rule , we can not deny the rule

**NACL:**

* It’s a subnet level firewall
* It’s a state less firewall: NACL never maintain session table means no record of inbound and outbound that’s why it will check each and every direction
* We can allow as well as deny also to any traffic.

**31. What is Route Table and what is the use case**

Ans:- Route Table define how traffic will route within the vpc or outside the the vpc.

A route table contains a set of rules, called routes that are used to determine where network traffic is directed.

**32. For which purpose you are using S3**

**Ans:- 1. Data Backup and Restore**

* Storing backups of servers, databases, and applications.
* Disaster recovery planning.

**2. Logging and Monitoring**

* Storing logs from AWS services like CloudTrail, ELB, or Lambda.
* Centralized log storage for security and audit.

**4. Logging and Monitoring**

* Storing logs from AWS services like CloudTrail, ELB, or Lambda.
* Centralized log storage for security and audit.

**33. How to host web application in S3**

**34. What is the gateway endpoint**

Ans:- In AWS for the private communication between two aws services we use Gateway endpoint

**35. What is cloudwatch**

Ans:-cloudwatch is a AWS Infra or resourese monitoring tool .

**36. How to setup alert using cloudwatch**

**Ans:-** ✅ Step 1: Open CloudWatch Console

* Go to: In Alarm section

✅ Step 2: Choose Metrics

* In the left menu, click "Metrics"
* Browse by:
  + EC2 → Per-Instance Metrics (for CPU, Network, etc.)
  + Or select other services like RDS, Lambda, etc.

✅ Step 3: Select a Metric

* For example: CPUUtilization of a specific EC2 instance
* Click the checkbox next to the metric
* Click "Create Alarm"

✅ Step 4: Define the Alarm

* Metric Name: (e.g., CPUUtilization)
* Threshold: For example:
  + "Whenever CPUUtilization is greater than 80% for 5 minutes"
* Set the Period, Evaluation Period, and Statistic (e.g., Average, Maximum)

✅ Step 5: Set Notification (SNS)

* Choose an existing SNS topic or create a new one
  + To send email alerts, create an SNS topic with your email address as a subscriber
* Confirm the subscription via email (first time only)

✅ Step 6: Name and Create

* Give your alarm a name like: High-CPU-Alert
* Review and click Create Alarm

**37. Which monitoring tool your are using**

Ans:- we are using Grafana for monitoring

**38. Which metrics are you monitoring**

Ans:- cpu utilization , Memory utilization , Disk utilization

**39. What is vpc endpoint ?**

Ans:- A **VPC Endpoint** is a feature in AWS that enables you to **privately connect your Virtual Private Cloud (VPC)** to supported AWS services and **VPC endpoint services** **without using an Internet Gateway (IGW), NAT Gateway, or VPN**.

**40. How to solve the issue if the cpu utilization is High?**

Ans:-first we check which process and who execute that process is consuming more CPU Utilization or memory utilization by executing the command **top**

Then inform to those users who execute the process

If those users not present or responding then we have to change the priority of the process by the by the command renice

**renice -n 10 PID**

**41. How to troubleshoot if the memory utilization is full ?**

Ans:- 1. First check which process and who execute that process id consuming more memory by the command #top

2.Try to kill or disable or stop the unnecessary services

3.If all these are not possible then we have to increase the memory