ALM-3

2100031820

M.Himani

1. What are policies and what are the different types of policies?

Ans:

In the context of Amazon Web Services (AWS), policies refer to sets of permissions that define what actions are allowed or denied on AWS resources. These policies are written in JSON (JavaScript Object Notation) format and are associated with AWS Identity and Access Management (IAM) entities such as users, groups, and roles. Policies help you control access to AWS services and resources securely.

Bucket Policies

Access Control Lists (ACLs)

IAM (Identity and Access Management) Policies

Pre-Signed URLs

S3 Access Points

VPC Endpoints for S3

Use HTTPS

Server-Side Encryption (SSE)

Versioning

Logging and Monitoring

2. What are different types of instances?

Ans:

Amazon EC2 (Elastic Compute Cloud) instances come in various types, each designed to serve different use cases based on computing power, memory, storage, and networking requirements.

General Purpose Instances

Compute Optimized Instances

Memory Optimized Instances

Storage Optimized Instances

Accelerated Computing Instances:

Bare Metal Instances

Graviton Instances

Infrequent Access Instances

3. What is VPC?

Ans:

Amazon Virtual Private Cloud (Amazon VPC) is a service provided by Amazon Web Services (AWS) that enables you to create a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network. With Amazon VPC, you have control over your virtual networking environment, including IP address ranges, subnets, route tables, and network gateways.

4. What are NAT Gateways?

Ans:

A NAT Gateway (Network Address Translation Gateway) is a managed service provided by Amazon Web Services (AWS) that enables instances in a private subnet to connect to the internet or other AWS services, while preventing unsolicited inbound traffic from reaching those instances.

5. How can you control the security to your VPC?

Ans:

Controlling the security of your Virtual Private Cloud (VPC) in Amazon Web Services (AWS) involves implementing various mechanisms and services to ensure that your resources are protected from unauthorized access. Here are key components and practices for controlling the security of your VPC:

Network Access Control Lists (NACLs)

Security Groups

Subnet Design

Internet Gateways

NAT Gateways or NAT Instances

Virtual Private Gateways (VPGs) and VPNs

VPC Peering

Flow Logs

Endpoint Services

IAM Policies

DNS Resolution and Hostnames

Regular Auditing and Monitoring