

Cloud Security Essentials

1.How to configure, develop and maintain Security and Privacy in cloud?

ANS: Cloud security and privacy are ensured through a combination of **technical controls, policies, and continuous monitoring.**

A. Configure Security:

- Use **Identity and Access Management (IAM)** to control user access
- Apply **least privilege principle**
- Configure **firewalls / security groups / network ACLs**
- Enable **encryption at rest and in transit**
- Enable **logging and monitoring**

B. Develop Security:

- Secure application development (DevSecOps)
- Use secure APIs and authentication mechanisms
- Implement secure key management (KMS)
- Design private networks (VPC, subnets)

C. Maintain Security:

- Regular **patching and updates**
- Continuous **monitoring and auditing**
- Vulnerability scanning and penetration testing
- Backup and disaster recovery planning
- Compliance with regulations (GDPR, ISO, SOC)

2.What is Portability in cloud?

ANS: **Portability** in cloud refers to the ability to **move applications, data, or workloads from one cloud platform to another** with minimal changes.

Examples:

- Moving an application from AWS to Azure
- Running containers on any cloud using Docker and Kubernetes

Benefits:

- Avoids vendor lock-in
- Increases flexibility
- Improves disaster recovery options

3.What is Reliability and high Availability in cloud?

ANS:

Reliability:

Reliability ensures that **cloud services perform consistently without failure.**

- Achieved through fault-tolerant systems
- Automatic failure detection and recovery

High Availability (HA):

High Availability ensures **services remain available even during failures**.

Techniques:

- Multiple servers (redundancy)
- Load balancing
- Multiple availability zones
- Automatic scaling

Example:

If one server fails, traffic is redirected to another without downtime.

4.Describe Mobility Cloud Computing

ANS: Mobility Cloud Computing allows users to **access cloud services from mobile devices** such as smartphones, tablets, and laptops.

Key Features:

- Anywhere, anytime access
- Internet-based service delivery
- Device independence

Examples:

- Google Drive
- Microsoft OneDrive
- Cloud-based mobile apps

Benefits:

- Increased productivity
- Real-time data access
- Supports remote work

5.Describe AWS, Azure, Google cloud Platforms**ANS:****Amazon Web Services (AWS):**

- Market leader in cloud computing
- Offers compute, storage, networking, AI, security services
- Global infrastructure with many regions

Microsoft Azure:

- Strong integration with Microsoft products
- Popular in enterprise environments
- Supports hybrid cloud solutions

Google Cloud Platform (GCP):

- Known for data analytics and machine learning
- High-performance networking
- Used heavily for big data workloads

6.Accessing AWS, Azure and Google cloud Platforms (any one portal)

ANS:

Steps to Access AWS:

1. Go to AWS Management Console
2. Create an AWS account
3. Login using email and password
4. Access services like EC2, S3, VPC from the dashboard

Access Methods:

- Web Console
- Command Line Interface (CLI)
- SDKs (Python, Java, etc.)

7.Create compute, create network, create storage on AWS , Azure and GCP

ANS:

A. AWS:

- **Compute:** EC2 instance
- **Network:** VPC, Subnets, Security Groups
- **Storage:** S3 (object), EBS (block)

B. Azure:

- **Compute:** Virtual Machine (VM)
- **Network:** Virtual Network (VNet)
- **Storage:** Blob Storage, Disk Storage

C. Google Cloud:

- **Compute:** Compute Engine
- **Network:** VPC Network

8.Compare Cloud pricing of resources and services on all platform Amazon Web Services (AWS):

ANS:

Feature	AWS	Azure	GCP
Pricing Model	Pay-as-you-go	Pay-as-you-go	Pay-as-you-go
Free Tier	12 months	12 months	\$300 credit
Compute Pricing	Instance-based	VM-based	Per-second billing
Storage Cost	Moderate	Moderate	Slightly lower
Discounts	Reserved Instances	Reserved VMs	Sustained Use Discounts
Best For	General purpose	Enterprise	Data analytics