Module 5

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

Ans:

1. Selecting the Right Cloud Service Model:

Public Cloud: Offers scalability and cost-effectiveness, but requires stringent security controls.

Private Cloud: Provides more control over security and privacy but can be more expensive.

Hybrid Cloud: Combines both public and private clouds, offering a balance between cost and security.

2. Implementing Security Measures:

Identity and Access Management (IAM)

Use Strong Authentication: Implement multi-factor authentication (MFA) for accessing cloud services.

Role-Based Access Control (RBAC): Assign permissions based on roles to limit access to sensitive information.

Data Encryption

Encryption at Rest and in Transit: Encrypt sensitive data both when it is stored and when it is being transmitted.

Key Management Services (KMS): Use secure key management services provided by cloud providers to manage encryption keys.

3. Ensuring Compliance and Privacy

Regulatory Compliance

Understand Legal Requirements: Be aware of regulations such as GDPR, HIPAA, and CCPA that apply to your industry.

Compliance Audits: Regularly conduct audits to ensure compliance with relevant regulations.

Data Privacy

Data Minimization: Collect and retain only the necessary data.

Anonymization and Pseudonymization: Use techniques to anonymize or pseudonymize data to protect individual privacy.

4. Maintaining Security and Privacy

Continuous Monitoring

Security Information and Event Management (SIEM): Implement SIEM systems to monitor and analyze security events.

Threat Intelligence: Use threat intelligence services to stay updated on the latest security threats.

Q:2 What is portability in cloud?

Ans: Portability in the cloud is the ability to move applications, data, and workloads between different cloud environments with ease.

This includes switching between public, private, or hybrid clouds without significant changes.

Q: 3 What is Reliability and high Availability in cloud?

Ans:

Reliability: The ability of cloud services to perform consistently and correctly over time without failures.

High Availability: Ensuring cloud services are continuously operational and accessible with minimal downtime.

Q:4 Describe Mobility Cloud Computing.

Ans: It refers to the ability to access cloud resources and services from anywhere, using any internet-enabled device.

It allows users to work, collaborate, and access data seamlessly regardless of their location or the device they are using.

Q:5 Describe AWS, Azure, Google cloud Platforms

Ans: **AWS (Amazon Web Services):** AWS is a comprehensive cloud computing platform offered by Amazon.

It provides a wide range of services including computing power, storage, databases, machine learning, analytics, and more.

Microsoft Azure: Azure is a cloud computing platform provided by Microsoft.

It offers a wide array of services for computing, storage, networking, databases, artificial intelligence (AI), Internet of Things (IoT), and more.

Google Cloud Platform: GCP is a cloud computing platform provided by Google.

Q:6 Accessing AWS, Azure and Google cloud Platforms

Ans: **AWS: 1. Creating an Account:** Sign up for an account on the respective cloud platform's website.

2. Console Access: Each platform provides a web-based console/dashboard where you can manage your resources. After creating an account, you can log in to the console using your credentials.

3. Command-Line Interface (CLI): Install the CLI tool provided by the cloud platform. This allows you to interact with the platform via the command line, enabling automation and scripting.

4. Software Development Kits (SDKs): Download and install SDKs for your preferred programming languages. SDKs provide libraries and APIs for integrating your applications with cloud services.

5. Access Keys: Generate access keys or credentials to authenticate API requests made from your applications or tools.

Q:7 Create compute, create network, create storage on AWS

Ans: **AWS (Amazon Web Services):**

Compute (EC2 Instance):

1. Access AWS Console: Log in to the AWS Management Console.
2. Navigate to EC2: Go to the EC2 Dashboard.
3. Launch Instance: Click on "Launch Instance" to start the instance creation wizard.
4. Choose AMI: Select an Amazon Machine Image (AMI) for your instance.
5. Choose Instance Type: Choose the instance type based on your requirements.
6. Configure Instance: Set instance details like network, storage, and security groups.
7. Add Storage: Specify the storage volumes for your instance.

8. Configure Security Group: Define the security group rules for inbound and outbound traffic.
9. Review and Launch: Review the configuration and launch the instance.
10. Access Instance: Access the instance using SSH (Linux) or RDP (Windows).

Network (VPC):

1. Navigate to VPC: Go to the VPC Dashboard.
2. Create VPC: Click on "Create VPC" and specify details like CIDR block.
3. Create Subnets: Define subnets within the VPC, specifying the CIDR blocks and availability zones.
4. Configure Route Tables: Set up route tables to control traffic within the VPC.
5. Configure Security Groups: Create security groups to control inbound and outbound traffic.
6. Attach Internet Gateway: If needed, attach an internet gateway to enable internet access.
7. Review and Create: Review the configuration and create the VPC.

Storage (S3 Bucket):

1. Navigate to S3: Go to the S3 Dashboard.
2. Create Bucket: Click on "Create bucket" and specify the bucket name and region.

3. Configure Options: Set additional options like versioning, logging, and encryption.
4. Set Permissions: Define access permissions using bucket policies and access control lists (ACLs).
5. Review and Create: Review the configuration and create the S3 bucket.

Azure: Compute (Virtual Machine):

1. Access Azure Portal: Log in to the Azure Portal.
2. Navigate to Virtual Machines: Go to the Virtual Machines section.
3. Create VM: Click on "Create virtual machine" and follow the creation wizard.
4. Choose Image: Select an image from the Azure Marketplace or your own custom image.
5. Configure VM: Specify details like size, region, networking, and storage.
6. Configure Networking: Set up networking options like virtual network, subnet, and public IP address.
7. Configure Storage: Define storage options like disk type and size.
8. Configure Security: Set up security options like NSG (Network Security Group) rules.
9. Review and Create: Review the configuration and create the VM.
10. Access VM: Access the VM using Remote Desktop Protocol (RDP) or SSH.

Network (Virtual Network):

1. Navigate to Virtual Networks: Go to the Virtual Networks section.
2. Create Virtual Network: Click on "Add" to create a new virtual network.
3. Configure Details: Specify details like name, address space, and subscription.
4. Configure Subnets: Define subnets within the virtual network, specifying the address range.
5. Configure Security: Set up network security groups and route tables.
6. Review and Create: Review the configuration and create the virtual network.

Storage (Storage Account):

1. Navigate to Storage Accounts: Go to the Storage Accounts section.
2. Create Storage Account: Click on "Add" to create a new storage account.
3. Configure Details: Specify details like name, account kind, replication, and subscription.
4. Set Advanced Options: Configure advanced settings like access tier and network access.
5. Review and Create: Review the configuration and create the storage account.

Google Cloud Platform: Compute (Compute Engine):

1. Access GCP Console: Log in to the Google Cloud Console.
2. Navigate to Compute Engine: Go to the Compute Engine section.
3. Create VM Instance: Click on "Create instance" to create a new VM instance.
4. Configure Instance: Specify details like machine type, boot disk, and networking.
5. Configure Networking: Set up networking options like VPC network, subnet, and external IP.
6. Configure Firewall Rules: Define firewall rules to control incoming and outgoing traffic.
7. Review and Create: Review the configuration and create the VM instance.
8. Access VM: Access the VM using SSH.

Network (VPC Network):

1. Navigate to VPC Network: Go to the VPC Network section.
2. Create VPC Network: Click on "Create VPC network" and specify details like name and subnet mode.
3. Configure Subnets: Define subnets within the VPC network, specifying the IP range.
4. Configure Firewall Rules: Set up firewall rules to control traffic within the network.

5. Review and Create: Review the configuration and create the VPC network.

Storage (Cloud Storage):

1. Navigate to Cloud Storage: Go to the Cloud Storage section.
2. Create Bucket: Click on "Create bucket" to create a new storage bucket.
3. Specify Bucket Name: Choose a unique name for the bucket and specify the storage class.
4. Configure Advanced Settings: Set up options like location, storage class, and access control.
5. Set Permissions: Define access permissions using IAM policies.
6. Review and Create: Review the configuration and create the storage bucket.

Q:8 Compare Cloud pricing of resources and services on all platform.

Ans: **1. Service Usage:**

Different cloud providers offer a wide range of services with varying pricing structures. It's crucial to understand which services your applications require and how they are priced on each platform. For example, compute instances, storage solutions, databases,

networking, and machine learning services may have different pricing models and rates across AWS, Azure, and GCP.

2. Region:

Cloud providers have data centers located in multiple regions worldwide, and pricing can vary depending on the region. Factors such as infrastructure costs, taxes, and regulations may influence pricing differences between regions. It's important to consider the geographic locations where your users are located and choose regions that offer the best balance of performance and cost.

3. Discounts:

Each cloud provider offers various discount options to help reduce costs for long-term commitments and specific usage patterns. These discounts may include Reserved Instances (RIs), Committed Use Discounts (CUD), volume discounts, and sustained use discounts. Understanding the discount options available and how they apply to your usage patterns can significantly impact your overall cloud spending.

4. Free Tier:

Many cloud providers offer free tier offerings or trial credits for new customers to explore their services. It's essential to take advantage of these free tiers to experiment with different services and understand their capabilities and costs before committing to paid usage. Be sure to review the limitations and duration of the free tier offerings to avoid unexpected charges.

5. Additional Costs:

In addition to the base service prices, there may be additional costs associated with data transfer, storage, network egress, and other usage-related fees. These costs can vary depending on factors such as data volume, geographic regions, and traffic patterns. Understanding these additional costs and optimizing usage to minimize them can help control overall cloud expenses.

6. Custom Pricing:

Large enterprise customers may have the opportunity to negotiate custom pricing agreements with cloud providers based on their specific usage volumes and business requirements. These negotiated agreements may include volume discounts, special terms, and tailored support options. It's important to explore these possibilities if your organization has significant cloud usage and negotiating leverage.