Assignment 3

Q:1 Different type of cloud storage

Ans: Sure, there are various types of cloud storage services, each offering different features and catering to different needs. Here are some common types:

1. Public Cloud Storage: These are services provided by third-party vendors over the internet. Users can store and access their data through web-based interfaces or APIs. Examples include Google Drive, Dropbox, and OneDrive.

2. Private Cloud Storage: These are cloud storage services that are dedicated to a single organization. The infrastructure may be maintained either on-premises or by a third-party provider. Private cloud storage offers more control and security over data compared to public cloud storage.

3. Hybrid Cloud Storage: This involves a combination of public and private cloud storage solutions. It allows organizations to store sensitive data in a private cloud while leveraging the scalability and cost-effectiveness of public cloud storage for less critical data.

4. Object Storage: This type of storage organizes data as objects rather than files or blocks. Each object typically includes data, metadata, and a unique identifier. Object storage is highly scalable

and used for storing large amounts of unstructured data, such as media files, backups, and archives. Examples include Amazon S3 (Simple Storage Service) and Google Cloud Storage.

5. Block Storage: Block storage involves dividing data into blocks and storing them as separate pieces. It's commonly used for storing data that requires frequent access and low latency, such as databases and virtual machine disks. Examples include Amazon EBS (Elastic Block Store) and Azure Disk Storage.

6. File Storage: This type of storage organizes data into a hierarchical structure of files and folders, similar to how data is organized on traditional file systems. File storage is suitable for shared access and collaboration among multiple users or applications. Examples include NFS (Network File System) and SMB (Server Message Block) shares.

7. Cold Storage: Cold storage is designed for long-term retention of data that is accessed infrequently. It typically offers lower storage costs but longer retrieval times compared to other types of storage. Examples include Amazon Glacier and Google Cloud Storage Nearline.

Q:2 What is role base access control and identity and access management and MFA

Ans: Role-Based Access Control (RBAC) is a method of restricting network access based on the roles of individual users within an organization. It assigns permissions to roles rather than to individual users. In an RBAC system, roles are created for various job functions within an organization, and access permissions to resources are then assigned to these roles. Users are assigned to appropriate roles, and through those roles, they gain access to the resources they need to perform their tasks.

RBAC offers several advantages, including simplifying administration, improving security by reducing the potential for human error, and facilitating compliance with regulations by enforcing the principle of least privilege.

Identity and Access Management (IAM) is a framework of policies and technologies for ensuring that the right individuals have the appropriate access to resources within an organization. IAM encompasses processes such as user provisioning, authentication, authorization, and access management.

Q: 3 What is physical and virtual host allocation?

Ans: Physical and virtual host allocation refer to the process of assigning computing resources, specifically server hardware, to different tasks or applications within a computing environment. Here's a breakdown of each:

1. Physical Host Allocation:

In physical host allocation, computing tasks or applications are run on dedicated physical servers. Each physical server has its own hardware resources, including CPU, memory, storage, and network bandwidth. Tasks or applications are installed directly onto these servers, and they utilize the resources exclusively allocated to them.

2. Virtual Host Allocation:

In virtual host allocation, computing resources are abstracted from the underlying physical hardware and allocated to virtual machines (VMs) or containers. Multiple VMs or containers can run concurrently on a single physical server, sharing its resources while remaining isolated from each other.

Q:4 How to access resource of cloud computing?

Ans: Accessing resources in cloud computing typically involves several steps, depending on the specific service or resource you want to access. Here's a general overview:

1. Choose a Cloud Service Provider (CSP): Start by selecting a cloud service provider that offers the services and resources you need.

Major CSPs include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others.

2. Sign Up and Create an Account: Register for an account with your chosen cloud service provider. This usually involves providing some basic information and setting up authentication credentials.

3. Choose a Deployment Model: Decide whether you want to deploy your resources in a public cloud, private cloud, hybrid cloud, or multi-cloud environment, depending on your requirements for security, scalability, and control.

4. Select the Required Services: Identify the specific services and resources you need, such as virtual machines, storage, databases, networking, machine learning, analytics, etc.

5. Provision Resources: Use the cloud provider's management console, command-line interface (CLI), or application programming interface (API) to provision the desired resources. This typically involves specifying configurations such as resource type, size, region, and other settings.

6. Access Resources: Once the resources are provisioned, you can access them using various methods:

- Web Console: Many cloud providers offer web-based management consoles where you can view and manage your resources through a graphical user interface (GUI).

- Command-Line Interface (CLI): Cloud providers usually provide command-line tools that allow you to interact with their services and resources via a terminal or command prompt.

- APIs: You can programmatically access cloud resources using APIs provided by the cloud provider. This allows for automation and integration with other systems and applications.

- SDKs: Software Development Kits (SDKs) are available for various programming languages, which provide libraries and tools for interacting with cloud services programmatically.

7. Secure Access: Ensure that access to your cloud resources is secured using best practices such as strong authentication, access controls, encryption, and monitoring.

8. Manage Resources: Regularly monitor and manage your cloud resources to optimize performance, cost, and security. This may involve scaling resources up or down based on demand, implementing automated workflows, and managing access permissions...

Q:5 Type of backup in cloud?

Ans: In cloud computing, various types of backup strategies can be employed to protect data and ensure business continuity. Here are some common types of backups used in the cloud:

1. Full Backup:

- A full backup involves copying all data from a source system to a backup location. In the cloud, this typically means transferring all files, databases, or virtual machine images to cloud storage.

- Full backups provide complete data protection but can consume significant storage space and network bandwidth.

2. Incremental Backup:

- Incremental backups only copy data that has changed since the last backup, reducing storage and bandwidth requirements.

- In cloud environments, incremental backups often involve identifying and transferring only the modified or new files or data blocks since the last backup.

3. Differential Backup:

- Differential backups capture all changes made since the last full backup. Unlike incremental backups, they do not rely on the previous backup.

- In cloud environments, a differential backup involves copying all data that has changed since the last full backup, which can be more efficient than incremental backups for some use cases.

4. Snapshot:

- Snapshots capture the state of a system or data at a specific point in time. They provide a quick and efficient way to create backups without interrupting ongoing operations.

- In cloud computing, snapshots are commonly used for virtual machine disks, databases, and other storage volumes.

5. Cloud-to-Cloud Backup:

- Cloud-to-cloud backup involves replicating data from one cloud service to another, providing redundancy and protection against data loss caused by cloud service outages, accidental deletions, or malicious attacks.

- This type of backup is particularly relevant for Software-as-a-Service (SaaS) applications hosted in the cloud, such as email, collaboration tools, and customer relationship management (CRM) systems.

6. Archival Backup:

- Archival backups are used for long-term retention of data that is not frequently accessed but may need to be retained for compliance, legal, or historical purposes.

- Cloud storage services offer cost-effective archival options with features such as infrequent access storage tiers and lifecycle policies for data retention.

7. Disaster Recovery Backup:

- Disaster recovery backups are designed to facilitate the rapid restoration of data and systems in the event of a disaster, such as hardware failures, natural disasters, or cyberattacks.

- Cloud-based disaster recovery solutions replicate data and systems to geographically diverse cloud regions or data centers, providing high availability and resilience.

Q:6 What is disaster recovery?

Ans: Disaster recovery (DR) is the process of planning for and recovering from events that have the potential to disrupt or damage an organization's IT infrastructure, systems, applications, and data. These events, often referred to as disasters, can include natural disasters (e.g., earthquakes, floods, hurricanes), human-made disasters (e.g., cyberattacks, data breaches, power outages), or other unexpected incidents.

The goal of disaster recovery is to minimize the impact of such events on the organization's operations and ensure business continuity by quickly restoring critical IT services and data to a functional state.