Training Day 8 Report

04 July 2025

Core Cloud Components

In this week, we explore the core components that form the foundation of cloud computing. These include compute power, storage solutions, networking, and security. Understanding these elements is essential for working with cloud platforms like AWS, Azure, and GCP. The following sections cover important topics such as compute services, storage types, cloud networking, and cloud security, with real-world examples.

1.Compute Services (e.g., VMs, EC2, GCE)

Compute services in cloud computing refer to the virtual resources that provide processing power for applications. These services allow users to create, manage, and scale virtual machines and computing environments.

Virtual Machines (VMs): Emulated computing environments that run on physical hardware. They include their own operating systems and applications.

Amazon EC2 (Elastic Compute Cloud): AWS's compute service that allows users to launch scalable virtual servers.

Google Compute Engine (GCE): Google Cloud's infrastructure-as-a-service (IaaS) offering that provides VMs on demand.

Compute services are used for hosting applications, websites, databases, and running workloads that require flexible computing capacity.

2. Storage Services (e.g., Object, Block, File Storage)

Cloud storage services allow data to be stored remotely and accessed over the internet. Depending on the use case, cloud providers offer various storage types:

Object Storage:

Ideal for unstructured data such as media files, backups, and logs.

Each file is stored as an object with metadata.

Examples: Amazon S3, Google Cloud Storage.

Block Storage:

Data is split into blocks and stored in volumes.

Commonly used for system drives and database storage.

Examples: Amazon EBS, Google Persistent Disk.

File Storage:

Data is stored in a file and folder hierarchy.

Suitable for shared access and traditional applications.

Examples: Amazon EFS, Google File store .

Each storage type is designed for specific performance, durability, and access requirements.

3.Networking in Cloud (VPC, Subnets, IPs, DNS)

Cloud networking ensures secure and efficient communication between cloud resources and external systems.

VPC (Virtual Private Cloud):

A private network space within a cloud provider's infrastructure.

Users can define custom IP ranges and configure route tables.

Subnets:

Subdivisions within a VPC used to organize and isolate resources.

IP Addresses:

Unique identifiers for resources.

Public IPs are used for internet access, while private IPs are used for internal communication.

DNS (Domain Name System):

Resolves human-friendly domain names into machine-readable IP addresses.

Networking setup is essential for managing traffic flow, securing services, and integrating with other systems.

4.Security in Cloud (IAM, Firewalls, Encryption)

Security is a critical aspect of cloud computing to protect data and ensure compliance with regulations.

IAM (Identity and Access Management):

A service for controlling user access to cloud resources.

Enables role-based and policy-based access control.

Firewalls:

Used to monitor and filter network traffic to and from cloud services based on defined rules.

Encryption:

Protects data by converting it into a secure format.

Supported for both data in transit and at rest.

Cloud providers offer various tools and services to help organizations implement strong security practices and meet compliance standards.

By: Asha Rani URN: 2302485 CRN: 2315029