Cloud

Agenda

1. Introduction to the Cloud
2. Security Management in AWS (30 mins Hands-on)
3. What are Cloud Providers and Discussion more on AWS
4. Comparison between AWS, Azure and GCP
5. Talking about Providers AWS, Azure and GCP
6. Types of Cloud - Public, Private and Hybrid
7. Load Balancing and Route S3 on AWS (30 mins Hands-on)
8. Management Console
9. Access Management

INTRODUCTION

Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online.

With Cloud Computing users can access database resources via the internet from anywhere for as long as they need without worrying about any maintenance or management of actual resources.

What is Cloud?

The term **Cloud** refers to a **Network** or **Internet**.
In other words, we can say that Cloud is something, which is present at remote location.
Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN.
Applications such as **e-mail, web conferencing, customer relationship management (CRM),** all run in cloud.

What is Cloud Computing?

Cloud Computing refers to **manipulating, configuring,** and **accessing** the applications online. It offers online data storage, infrastructure and application.

Cloud Computing is both a combination of software and hardware based computing resources delivered as a network service.

What are Cloud Providers and Discussion more on AWS

A cloud service provider, or CSP, is an IT company that provides on-demand, scalable computing resources like computing power, data storage, or applications over the internet.

Typically, cloud-based service models are defined as IaaS (infrastructure as a service), PaaS (platform as a service), or SaaS (software as a service).

Cloud service provider definition

A CSP (cloud service provider) is a third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services.

Types of cloud providers

CSPs offer a variety of services, but typically they fall under three types of cloud service providers:

IaaS providers

IaaS solutions provide access to IT infrastructure components that you would normally have in your data center, eliminating the need to procure, configure, or manage your own. This includes resources like compute, networks, storage, data management, virtualization, and operating systems. While the IaaS model increases flexibility, lowers costs, and speeds up times to market, customers are still responsible for managing and maintaining their own applications and responding to issues.

PaaS providers

PaaS solutions build off IaaS, providing tools and services to create and deploy applications. PaaS incorporates operating systems, middleware, and runtime environments into the application stack and also manages any hardware or other assets related to the underlying infrastructure.

SaaS providers

SaaS solutions are perhaps the most familiar and make up the fastest growing services in the cloud market. CSPs deliver ready-to-use applications and are responsible for maintaining and managing everything, from hardware and maintenance to development, scaling, and delivery. For example, you probably use many of the SaaS productivity applications in Google Workspace every day, such as Gmail, Calendar, Docs, and Drive.

While these are the most common categories, they do not fully describe all of the types of services currently offered by CSPs. Many top cloud service providers are continuously developing new cloud-based services around emerging technologies like containerization, edge computing, machine learning, and Kubernetes.

Cloud service provider examples

The CSP market includes cloud providers of all shapes and sizes. The big three—Google Cloud, Microsoft Azure, and Amazon Web Services (AWS)—are considered the established leaders. However, there are a host of other smaller or niche players that offer cloud services as well, including IBM, Alibaba, Oracle, Red Hat, DigitalOcean, and Rackspace.

Comparison between AWS, Azure and GCP

AWS, Azure, and GCP are the largest cloud providers in the market today, but each has their own nuances and background. Here's some basic information about each provider before we dive into the specifics around how they differ:

Amazon Web Services (AWS) is the cloud infrastructure provider from Amazon. AWS was founded in 2006 and is now the leading cloud provider in the world, with a market share of 32% in Q1 2023. AWS offers a wide range of services, including compute, storage, networking, databases, analytics, machine learning, and artificial intelligence. AWS is used by a wide range of businesses, from small businesses to large enterprises.

Microsoft Azure, which was first launched in 2010 from the Microsoft Corporation, is the second-largest cloud provider in the global cloud market, with a market share of 23% in Q1 2023. Azure offers a wide range of services, similar to AWS, but specializes in Windows-based compute and works well with other Microsoft services.

Google Cloud Platform (GCP) was started by Google in 2011 and is the third-largest cloud provider in the world, with a market share of 9% in Q1 2023. GCP offers a wide range of services, similar to AWS and Azure, however has fewer data centers than AWS and Azure and has solutions that are considered friendly for DevOps.

Types of Cloud - Public, Private and Hybrid

PUBLIC CLOUD : The **Public Cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

PRIVATE CLOUD : The **Private Cloud** allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

COMMUNITY CLOUD : The **Community Cloud** allows systems and services to be accessible by group of organizations.

HYBRID CLOUD : The **Hybrid Cloud** is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

Management Console

The AWS Management Console is a web-based application that lets users access the broad range of services included in the Amazon Web Services (AWS) platform. It also provides easy navigation and centralized access to these services.

The built-in interface of the AWS Management Console enables customers to perform certain AWS-related tasks such as provisioning resources, launching instances, setting up load balancers and creating or managing Amazon Simple Storage Service (S3) buckets. Users can customize the Console Home page by adding, removing and rearranging widgets, such as "Recently visited," "AWS Health" and "AWS Trusted Advisor."

Access Management

Identity and Access Management (IAM) manages Amazon Web Services (AWS) users and their access to AWS accounts and services. It controls the level of access a user can have over an AWS account & set users, grant permission, and allows a user to use different features of an AWS account. Identity and access management is mainly used to manage users, groups, roles, and Access policies The account we created to sign in to Amazon web services is known as the root account and it holds all the administrative rights and has access to all parts of the account. The new user created an AWS account, by default they have no access to any services in the account & it is done with the help of IAM that the root account holder can implement access policies and grant permission to the user to access certain services.


AWS Identity and Access Management
Apply Fine-Grained Permissions to AWS Services and Resources
Who
Workforce Users and Workloads with IAM
Can Access
Permissions with IAM Policies
What
Resources within your AWS Organization

How IAM Works?

IAM verifies that a user or service has the necessary authorization to access a particular service in the AWS cloud. We can also use IAM to grant the right level of access to specific users, groups, or services. For example, we can use IAM to enable an EC2 instance to access S3 buckets by requesting fine-grained permissions.

What Does IAM Do?

With the help of IAM, we perform the following

IAM Identities

IAM Identities assists us in controlling which users can access which services and resources in the AWS Console and also we can assign policies to the users, groups, and roles. The IAM Identities can be created by using the Root user

IAM Identities Classified As

IAM Users

IAM Groups

IAM Roles

Root user

The root user will automatically be created and granted unrestricted rights. We can create an admin user with fewer powers to control the entire Amazon account.

IAM Users

We can utilize IAM users to access the AWS Console and their administrative permissions differ from those of the Root user and if we can keep track of their login information.

Example

With the aid of IAM users, we can accomplish our goal of giving a specific person access to every service available in the Amazon dashboard with only a limited set of permissions, such as read-only access. Let’s say user-1 is a user that I want to have read-only access to the EC2 instance and no additional permissions, such as create, delete, or update. By creating an IAM user and attaching user-1 to that IAM user, we may allow the user access to the EC2 instance with the required permissions.

IAM Groups

A group is a collection of users, and a single person can be a member of several groups. With the aid of groups, we can manage permissions for many users quickly and efficiently.

Example

Consider two users named user-1 and user-2. If we want to grant user-1 specific permissions, such as the ability to delete, create, and update the auto-calling group only, and if we want to grant user-2 all the necessary permissions to maintain the auto-scaling group as well as the ability to maintain EC2, we can create groups and add this user to them. If a new user is added, we can add that user to the required group with the necessary permissions.

IAM Roles

While policies cannot be directly given to any of the services accessible through the Amazon dashboard, IAM roles are similar to IAM users in that they may be assumed by anybody who requires them.

By using roles, we can provide AWS Services access rights to other AWS Services.

Example

Consider Amazon EKS. In order to maintain an autoscaling group, AWS eks needs access to EC2 instances. Since we can’t attach policies directly to the eks in this situation, we must build a role and then attach the necessary policies to that specific role and attach that particular role to EKS.

IAM Policies

IAM Policies can manage access for AWS by attaching them to the IAM Identities or resources IAM policies defines permissions of AWS identities and AWS resources when a user or any resource makes a request to AWS will validate these policies and confirms whether the request to be allowed or to be denied.

AWS policies are stored in the form of Jason format the number of policies to be attached to particular IAM identities depends upon no.of permissions required for one IAM identity. IAM identity can have multiple policies attached to them.

IAM Features

Shared Access to your Account: A team working on a project can easily share resources with the help of the shared access feature.

Free of cost: IAM feature of the Aws account is free to use & charges are added only when you access other Amazon web services using IAM users.

Have Centralized control over your Aws account: Any new creation of users, groups, or any form of cancellation that takes place in the Aws account is controlled by you, and you have control over what & how data can be accessed by the user.

Grant permission to the user: As the root account holds administrative rights, the user will be granted permission to access certain services by IAM.

Multifactor Authentication: Additional layer of security is implemented on your account by a third party, a six-digit number that you have to put along with your password when you log into your accounts.