**\* \* \* AWS Session \* \* \***

**01-27-Aws-27-DEC-24**

------------------------------------------------------------------------------------------------------------------

1) What is IT infrastructure ?

2) Challenges with On-Prem infrastructure

3) What is Cloud Computing

4) Cloud Service Models

5) Cloud Providers

6) AWS Introduction

7) AWS Services Overview

**=============================**

**What is IT Infrastructure ?**

**=============================**

=> To run a software company then we need to purchase below resources

a) machines

b) network

c) power

d) storage

e) backup

f) security

=> The above resources are called as IT infrastructure.

=> We can maintain infrastructure in 2 ways

a) On-Prem infrastructure

b) Cloud infrastructure

**==================================**

**What is On-Prem Infrastructure ?**

**==================================**

=> On-Prem means we need to purchase and we need to maintain our resources to run our business.

=> We have several challenges with On-Prem infrastructure

1) Lot of money investment

2) Lot of man power

3) Scalability (increase / decrease)

4) Availability

5) Network issues

6) Security issues

=> To overcome the problems of on-prem infrastructure companies are preferring Cloud Infrastructure.

**===========================**

**What is Cloud Computing ?**

**===========================**

=> The process of delivering IT resources over the internet on demand basis is called as Cloud Computing.

=> We have below advantages with cloud computing.

- Pay as you go

- Less cost

- Scalability

- Availability

- Security

- Backup

Note: Cloud computing works based on pay as you go model.

**================**

**Cloud Providers**

**================**

=> The companies which are providing IT infrastructure based on "pay as you go" model are called as Cloud Providers.

1) Amazon (AWS)

2) Microsoft (Azure)

3) Google (GCP)

4) Salesforce

5) Ali Baba

6) Digital Ocean

**=======================**

**Cloud Service Models**

**=======================**

=> We have 3 types cloud service models

1) IAAS

2) PAAS

3) SAAS

**=============**

**What is IaaS**

**=============**

=> IAAS stands for infrastructure as a service

=> Provider will give infrastructure for us

Ex: Machines, Network, Storage

=> As a customer we need to prepare platform to run our application

Ex: install required softwares + setup web servers + deploy application.

**=============**

**What is PaaS**

**=============**

=> PaaS stands for Platform as a service

=> Provider will give ready made platform to run our application directley.

=> As a customer we need to take care of only our application deployment.

**=================**

**What is SaaS**

**=================**

=> SaaS stands for software as a service

-> Cloud Provider will give their application to run our business.

Ex: zoom, google drive, dropbox, microsoft teams, jira ...

**===========**

**AWS Cloud**

**===========**

=> AWS stands for Amazon webservices.

=> AWS providing cloud services from 2006 onwards

=> AWS works based on Pay as you go model

=> 190+ countries using AWS cloud services to run their businesses

=> AWS having global infrastructure

34 - Regions

108 - Availability Zones

**===============**

**AWS Services**

**===============**

=> We have 200+ Services.....

1) EC2 : To Create Virtual Machines (Hourly Billing)

2) S3 : Unlimited storage

3) RDS : Relational Database service

4) EFS : Elastic File System (shared file system)

5) IAM : Identity & Access Management

6) VPC : Virtual Private Cloud

7) Elastic Beanstack : End to end web-application mgmt (PaaS)

8) Lambdas : Serverless computing

9) Route 53 : Domain Mapping (DNS)

10) ECS : Elastic Container Service

11) EKS : Elastic Kubernetes Service

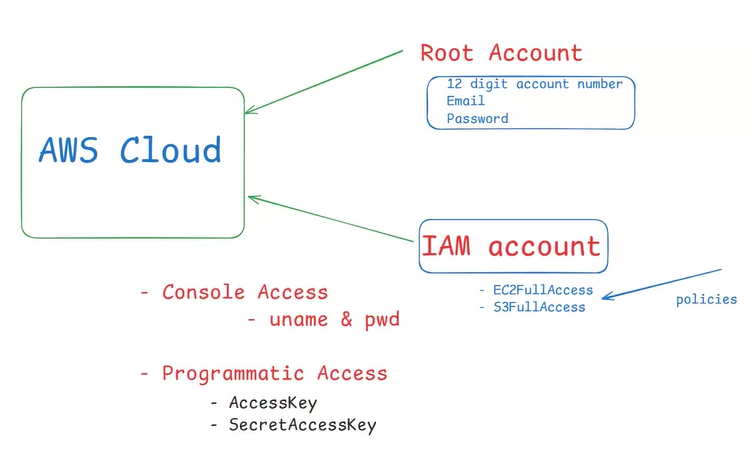
12) Cloud Watch : Monitoring

13) SNS : Simple Notification Service .....

**=====**

**IAM 02-27-Aws-30-DEC-24**

**=====**

****

=> Identity and Access management

=> It is used to manage users, groups, policies and roles

=> IAM is a free service

=> In AWS cloud platform we will have 2 types of accounts

1) Root Account

2) IAM Account

Note: When we signup in aws website then by default it will consider that as root account.

=> Root account is very powerfull account with no restrictions.

=> If we login with Root user credentials, we can access everything in AWS cloud.

Note-1 : We shouldn't use root account for day to day activities.

Note-2 : We shouldn't share root account credentials with anyone.

Note-3: Company will not provide root account credentials for team members.

Note-4: It is recommended to enable MFA for root account.

MFA : Multi Factor Authentication

**===================================**

**Multi Factor Authentication (MFA)**

**===================================**

-> It is used to provide additional security for root account.

-> Enable MFA for root account using Google Authenticator app.

-> After enabling MFA, logout and login into root account and check behaviour.

**============**

**IAM Account**

**============**

=> For team members IAM accounts will be created with limited access

=> For daily activities in aws cloud we should use IAM account only

=> For IAM user we can provide below types of accesses

1) Console Access (web login)

- uname & pwd

2) Programmatic Access

- AccessKey and SecretAccessKey

**Note: To communicate with AWS cloud using terraform then IAM user should have programmatic access**.

1) Create IAM account and attach policies (RDSFullAcces, S3FullAccess)

2) Login into IAM account and check EC2 service (can't access because no permission)

**=================**

**IAM User Group**

**=================**

**Note - Policies are only applicable for users and group level only.**

=> When we want to provide some permissions for multiple users then we can create IAM user group and we can add users to that group and we can attach policies to group.

1) Create User Group

2) Attach Policies to group

3) Add Users to group

**=========**

**IAM Role**

**=========**

**=> IAM role nothing but set of permissions**

Ex-1: EC2 VM wants to create EKS cluster, Then EC2 VM should have IAM Role with EKS permissions.

1. create IAM role with all EKS policies

2) Attach IAM role to ec2 vm

**Note – AWS policies will be saved in the JSON format.**

**If one service want to communicate with the another service then IAM role comes into the picture.**

**============**

**IAM Summary**

**============**

1) What is IAM

2) What is Root Account

3) How to enable MFA

4) What is IAM account

5) Console Access Vs Programmatic Access

6) Users Creation

7) User Groups

8) Policies / Permissions

9) Roles

10) Working with Custom Policies