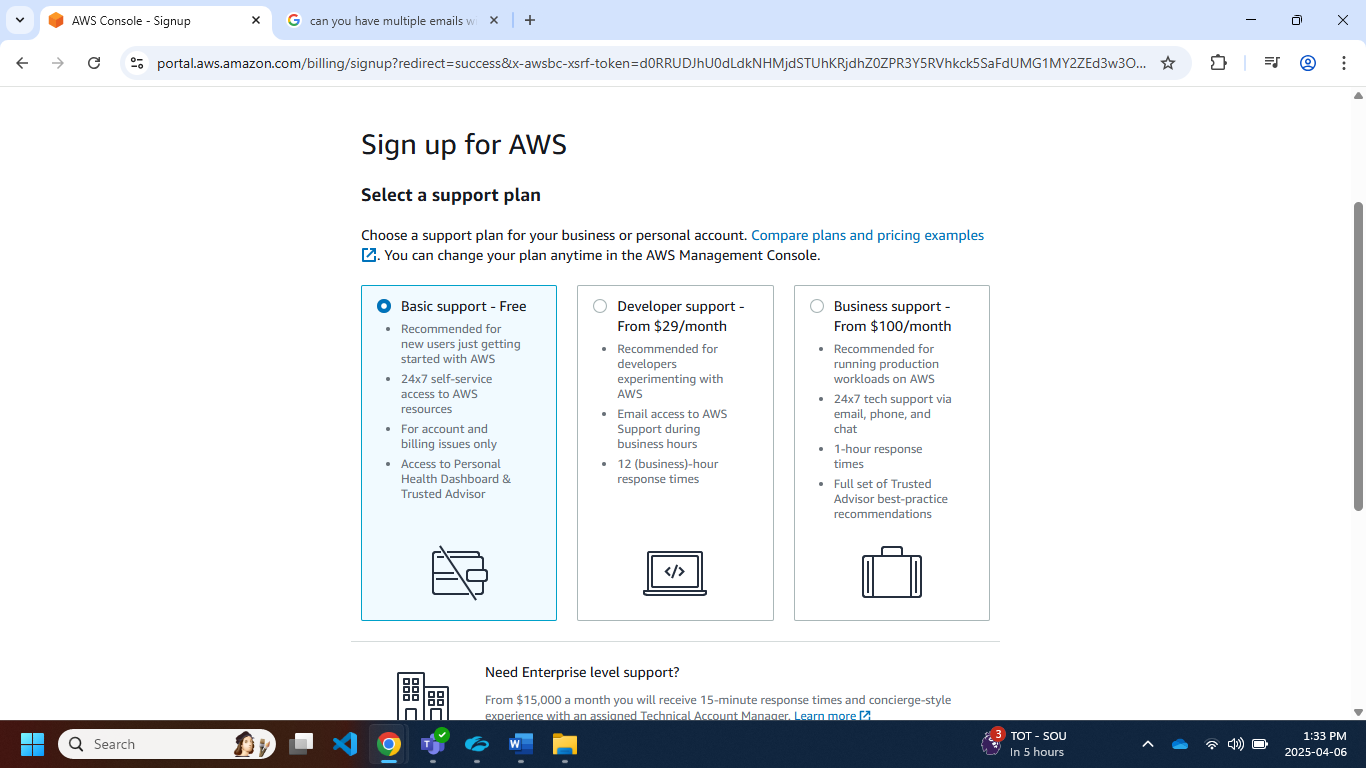
AWS-CERTIFIED-CLOUD-PRACTITIONER

UDEMY: <https://fiserv.udemy.com/course/aws-certified-cloud-practitioner-new/learn/lecture/19891628#labs>

Creating an AWS Account

Registration: <https://signin.aws.amazon.com/signup?request_type=register>



**IT Terminology**

• Network: cables, routers and servers connected with each other

• Router: A networking device that forwards data packets between computer networks. They know where to send your packets on the internet!

• Switch: Takes a packet and send it to the correct server / client on your network

**Problems with traditional IT approach**

• Pay for the rent for the data center

• Pay for power supply, cooling, maintenance

• Adding and replacing hardware takes time

• Scaling is limited

• Hire 24/7 team to monitor the infrastructure • How to deal with disasters? (earthquake, power shutdown, fire…

**Cloud**:

Cloud is a platform which provides infrastructure to build an application.

Before cloud came into picture, we had on premise infrastructure to host our application or website.

**Cloud computing**

Cloud computing is to store, process and access data on remote server.

Store data/apps on remote servers

Process data/apps on remote servers

Access data/apps on remote servers

**Types of cloud computing:**

|  |  |  |
| --- | --- | --- |
| Private Cloud: | Public Cloud: | Hybrid Cloud: |
| A private cloud refers to cloud computing resources used exclusively by a single business or organisation. A private cloud can be physically located on the company’s on-site datacentre.  • Cloud services used by a single organization, not exposed to the public.  • Complete control  • Security for sensitive applications  • Meet specific business needs | • Cloud resources owned and operated by a third-party cloud service provider delivered over the Internet.  (AWS,GCP,AZURE ETC) | • Keep some servers on premises and extend some capabilities to the Cloud  • Control over sensitive assets in your private infrastructure  • Flexibility and costeffectiveness of the public cloud |

**The Five Characteristics of Cloud Computing**

1. On-demand self-service: Users can provision resources and use them without human interaction from the service provider
2. Broad network access: Resources available over the network, and can be accessed by diverse client platforms
3. Multi-tenancy and resource pooling: Multiple customers can share the same infrastructure and applications with security and privacy. Multiple customers are serviced from the same physical resources
4. Rapid elasticity and scalability: Automatically and quickly acquire and dispose resources when needed. Quickly and easily scale based on demand
5. Measured service: Usage is measured, users pay correctly for what they have used

Six Advantages of Cloud Computing

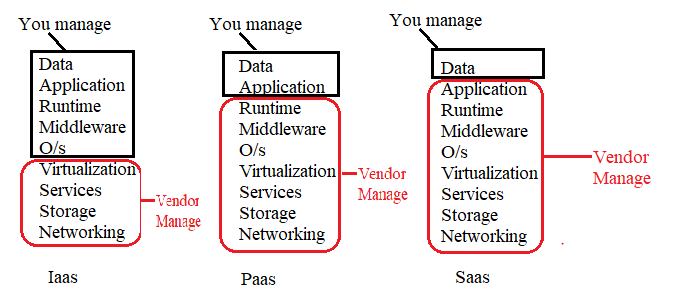
1. Trade capital expense (CAPEX) for operational expense (OPEX): Pay On-Demand: don’t own hardware • Reduced Total Cost of Ownership (TCO) & Operational Expense (OPEX)
2. Benefit from massive economies of scale: Prices are reduced as AWS is more efficient due to large scale
3. Stop guessing capacity: Scale based on actual measured usage
4. Increase speed and agility
5. Stop spending money running and maintaining data centers
6. Go global in minutes: leverage the AWS global infrastructure

Problems solved by the Cloud

1. Flexibility: change resource types when needed
2. Cost-Effectiveness: pay as you go, for what you use
3. Scalability: accommodate larger loads by making hardware stronger or adding additional nodes
4. Elasticity: ability to scale out and scale-in when needed
5. High-availability and fault-tolerance: build across data centers
6. Agility: rapidly develop, test and launch software application

**Cloud service types:** Cloud resources cover wide range of resources that a service provider delivers to customer via internet

1. Infrastructure as a Service (IaaS): IaaS contains the basic building blocks for cloud IT. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives you the highest level of flexibility and management control over your IT resources. It is most like the existing IT resources with which many IT departments and developers are familiar.
2. Platform as a Service (PaaS): PaaS removes the need for you to manage underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. This helps you be more efficient as you don’t need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.
3. Software as a Service (SaaS): SaaS provides you with a complete product that is run and managed by the service provider. In most cases, people referring to SaaS are referring to end-user applications (such as web-based email). With a SaaS offering, you don’t have to think about how the service is maintained or how the underlying infrastructure is managed. You only need to think about how you will use that software.



AWS Global Infrastructure

1. AWS Regions
2. AWS Availability Zones
3. AWS Data Centers
4. AWS Edge Locations / Points of Presence

https://infrastructure.aws

**AWS Region**

* Geographically separated area where AWS has set up its resources. (cluster of data centers)
* Each Region is independent of each other
* In India –Mumbai and Hyderabad (coming soon)

<https://aws.amazon.com/about-aws/global-infrastructure/>

How to choose an AWS Region

* Compliance with data governance and legal requirements: data never leaves a region without your explicit permission
* Proximity to customers: reduced latency
* Available services within a Region: new services and new features aren’t available in every Region
* Pricing: pricing varies region to region and is transparent in the service pricing page

**Availability Zone (AZ)**

* AZ’s are isolated, multiple and physically separated data center of each region.
* AZ’s are data center
* They’re separate from each other, so that they’re isolated from disasters
* They’re connected with high bandwidth, ultra-low latency networking
* Each region has many availability zones (usually 3, min is 3, max is 6).

Example: • ap-southeast-2a • ap-southeast-2b • ap-southeast-2c

**Edge Location (AWS Points of Presence)**

* These are small data center where end user access services located at AWS
* Frequently used data will be stored in cache, helps to access fast.
* AWS will not disclose where AZ’s and edge location

Tour of the AWS Console

**AWS has Global Services:**

• Identity and Access Management (IAM)

• Route 53 (DNS service)

• CloudFront (Content Delivery Network)

• WAF (Web Application Firewall) •

Most AWS services are Region-scoped:

Amazon EC2 (Infrastructure as a Service)

Elastic Beanstalk (Platform as a Service)

Lambda (Function as a Service)

Rekognition (Software as a Service)

Region Table: https://aws.amazon.com/about-aws/global-infrastructure/regional-product-service

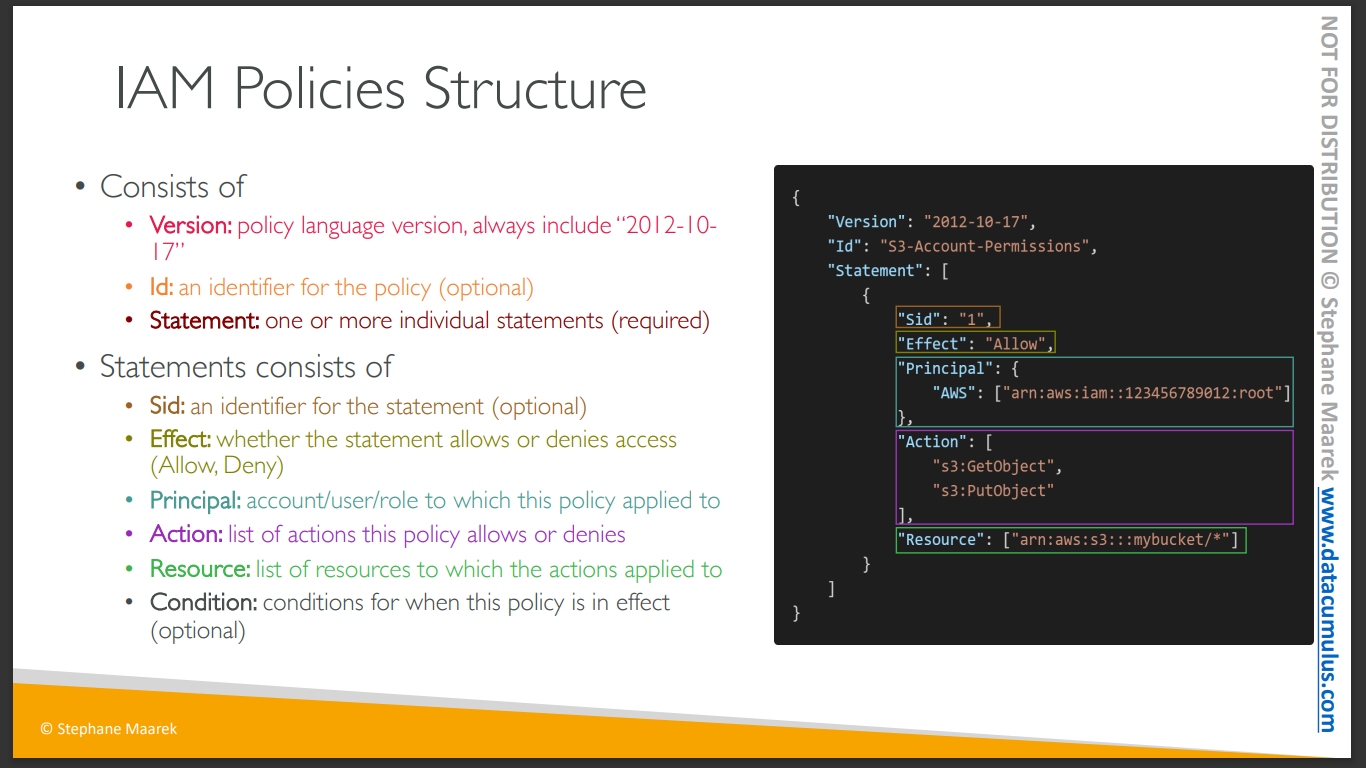
**IAM Section (global service)**

IAM: Users & Groups

* IAM = Identity and Access Management, Global service
* Root account created by default, shouldn’t be used or shared
* Users are people within your organization, and can be grouped
* Groups only contain users, not other groups
* Users don’t have to belong to a single group, and user can belong to multiple group

IAM: Permissions

* Users or Groups can be assigned JSON documents called policies
* These policies define the permissions of the users
* In AWS you apply the least privilege principle: don’t give more permissions than a user need



IAM – Password Policy •  
Strong passwords = higher security for your account

In AWS, you can setup a password policy:

• Set a minimum password length

• Require specific character types:

• including uppercase letters

• lowercase letters

• numbers

• non-alphanumeric characters

• Allow all IAM users to change their own passwords

• Require users to change their password after some time (password expiration)

• Prevent password re-use

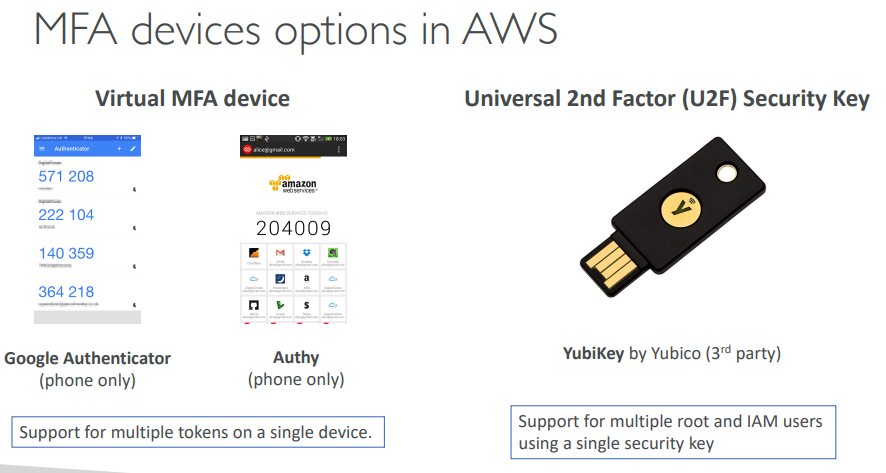
Multi Factor Authentication - MFA

• Users have access to your account and can possibly change configurations or delete resources in your AWS account

• You want to protect your Root Accounts and IAM users

• MFA = password you know + security device you own

• Main benefit of MFA: if a password is stolen or hacked, the account is not compromised



How can users access AWS ?

To access AWS, you have three options:

• AWS Management Console (protected by password + MFA)

• AWS Command Line Interface (CLI): protected by access keys

• AWS Software Developer Kit (SDK) - for code: protected by access keys

• Access Keys are generated through the AWS Console

• Users manage their own access keys

• Access Keys are secret, just like a password. Don’t share them

• Access Key ID ~= username • Secret Access Key ~= password

**What’s the AWS CLI?**

• A tool that enables you to interact with AWS services using commands in your command-line shell

• Direct access to the public APIs of AWS services • You can develop scripts to manage your resources

• It’s open-source <https://github.com/aws/aws-cli>

• Alternative to using AWS Management Console © Stephane Maarek NOT FOR DISTRIBUTION © Stephane Maarek [www.datacumulus.com](http://www.datacumulus.com)

**What’s the AWS SDK?**

• AWS Software Development Kit (AWS SDK)

• Language-specific APIs (set of libraries)

• Enables you to access and manage AWS services programmatically • Embedded within your application

• Supports

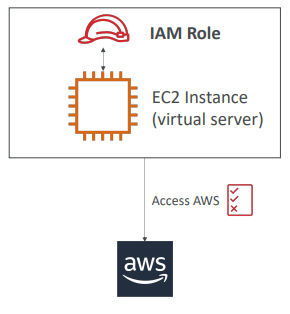
• SDKs (JavaScript, Python, PHP, .NET, Ruby, Java, Go, Node.js, C++)

• Mobile SDKs (Android, iOS, …)

• IoT Device SDKs (Embedded C, Arduino, …)

• Example: AWS CLI is built on AWS SDK for Python

**IAM Roles for Services**



• Some AWS service will need to perform actions on your behalf

• To do so, we will assign permissions to AWS services with IAM Roles

• Common roles:

• EC2 Instance Roles

• Lambda Function Roles

• Roles for CloudFormation

**IAM Security Tools**

• IAM Credentials Report (account-level)

• a report that lists all your account's users and the status of their various credentials

• IAM Access Advisor (user-level)

• Access advisor shows the service permissions granted to a user and when those services were last accessed.

• You can use this information to revise your policies.

**IAM Guidelines & Best Practices**

• Don’t use the root account except for AWS account setup

• One physical user = One AWS user

• Assign users to groups and assign permissions to groups

• Create a strong password policy

• Use and enforce the use of Multi Factor Authentication (MFA)

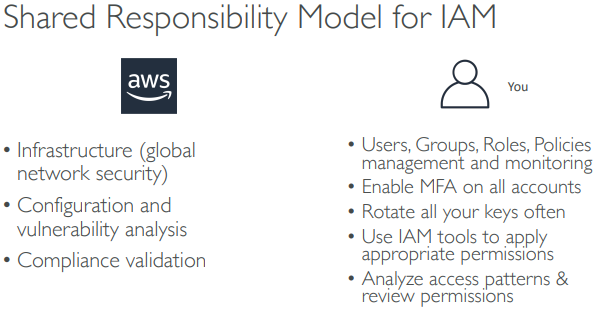
• Create and use Roles for giving permissions to AWS services

• Use Access Keys for Programmatic Access (CLI / SDK)

• Audit permissions of your account using IAM Credentials Report & IAM

Access Advisor

• Never share IAM users & Access Keys



**IAM Section – Summary**

• Users: mapped to a physical user, has a password for AWS Console

• Groups: contains users only

• Policies: JSON document that outlines permissions for users or groups

• Roles: for EC2 instances or AWS services

• Security: MFA + Password Policy

• AWS CLI: manage your AWS services using the command-line

• AWS SDK: manage your AWS services using a programming language

• Access Keys: access AWS using the CLI or SDK

• Audit: IAM Credential Reports & IAM Access Advisor

Amazon EC2

• EC2 is one of the most popular of AWS’ offering

• EC2 = Elastic Compute Cloud = Infrastructure as a Service

• It mainly consists in the capability of :

• Renting virtual machines (EC2)

• Storing data on virtual drives (EBS)

• Distributing load across machines (ELB)

• Scaling the services using an auto-scaling group (ASG)

• Knowing EC2 is fundamental to understand how the Cloud works

EC2 sizing & configuration options

• Operating System (OS): Linux, Windows or Mac OS

• How much compute power & cores (CPU)

• How much random-access memory (RAM)

• How much storage space:

• Network-attached (EBS & EFS)

• hardware (EC2 Instance Store)

• Network card: speed of the card, Public IP address

• Firewall rules: security group

• Bootstrap script (configure at first launch): EC2 User Data

EC2 User Data

• It is possible to bootstrap our instances using an EC2 User data script.

• bootstrapping means launching commands when a machine starts

• That script is only run once at the instance first start

• EC2 user data is used to automate boot tasks such as:

• Installing updates

• Installing software

• Downloading common files from the internet

• Anything you can think of

• The EC2 User Data Script runs with the root user