

FUNDAMENTALS OF AWS



What is Cloud?



Someone else's Computer?

A collection of Services that create a platform

Media Services

Databases

Security

Virtual Servers

Networking

Machine Learning

Data Storage

Analytics

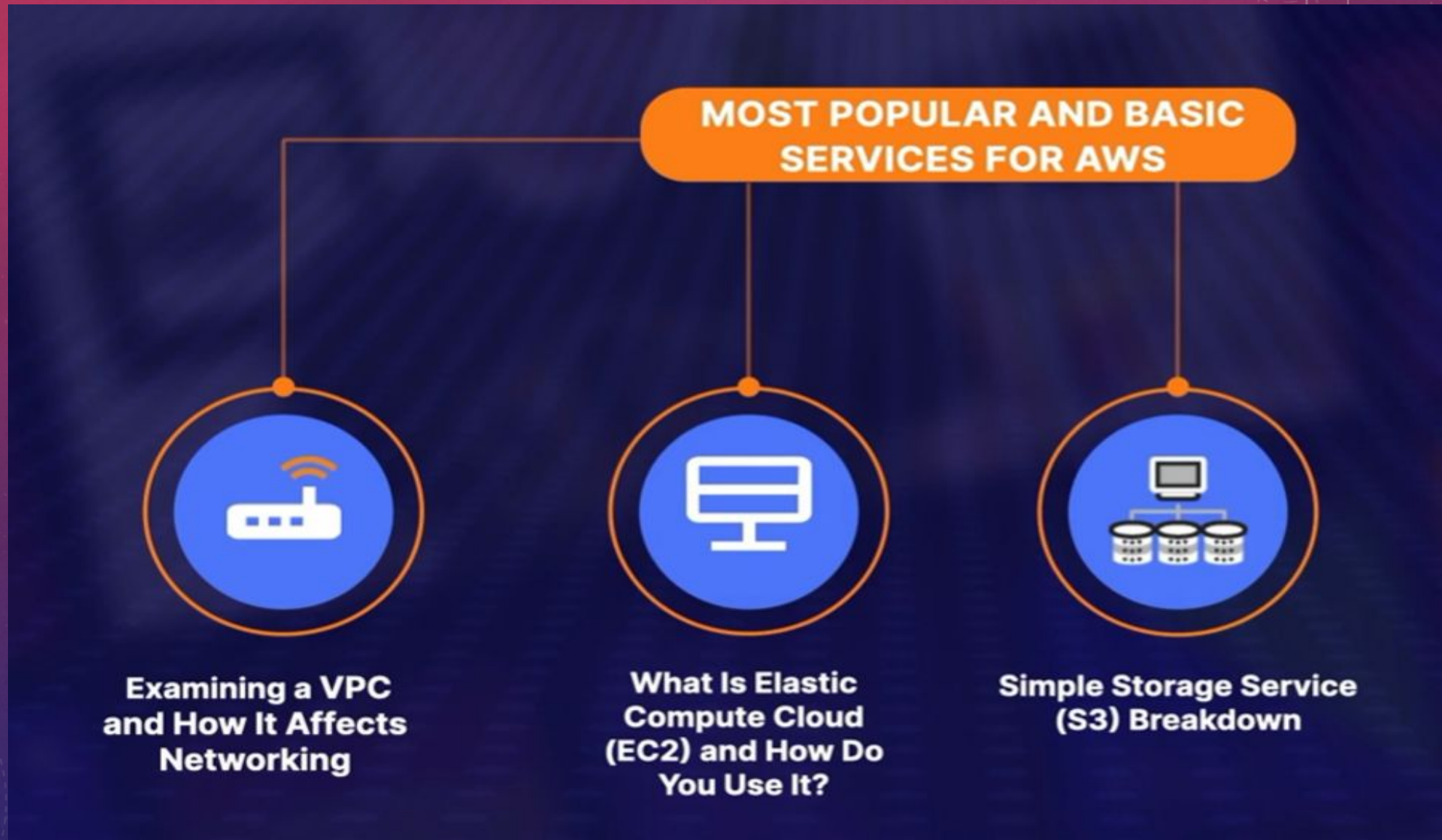
DEFINITION

"AWS is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers, including the fastest growing startups, largest enterprises and leading government agencies are using AWS to lower costs, become more agile and innovate faster."



- Billed by second for using Services
- 60 seconds minimum
- Use 83 seconds, get charged for 83 seconds
- Lambda recently moved to per millisecond billing

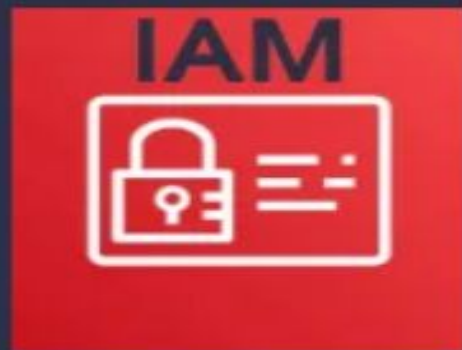
Most Popular and Basic Services for AWS





AWS Account Setup

in 2 Mins



Identity And Access
Management



HOW IDENTITY AND ACCESS MANAGEMENT WORKS?

AWS(Amazon Web Services) will allows you to maintain the fine-grained permissions to the AWS account and the services provided Amazon cloud. You can manage the permissions to the individual users or you can manage the permissions to certain users as group and roles will helps you to manage the permissions to the resources.



AWS Identity and Access Management

Apply fine-grained permissions to AWS services and resources

Who



Workforce users with AWS SSO and workloads with IAM roles

Can access



Permissions with IAM policies

What



Resources within your AWS organization

- Manage users and their level of access
- Used to set users, permissions and roles
- Grant access to the different parts of the aws platform

How Does AWS IAM Work?



- Create a directory of users called identities, and they can be users inside of your AWS account or users outside of your AWS account. Some of these users may need access to your website and services. Along with managing this directory, you manage what they can do once they log in.
- You can group identities to manage shared permissions and assign access permissions, using security policies and roles

Understand the difference between **authentication** and **authorization**.

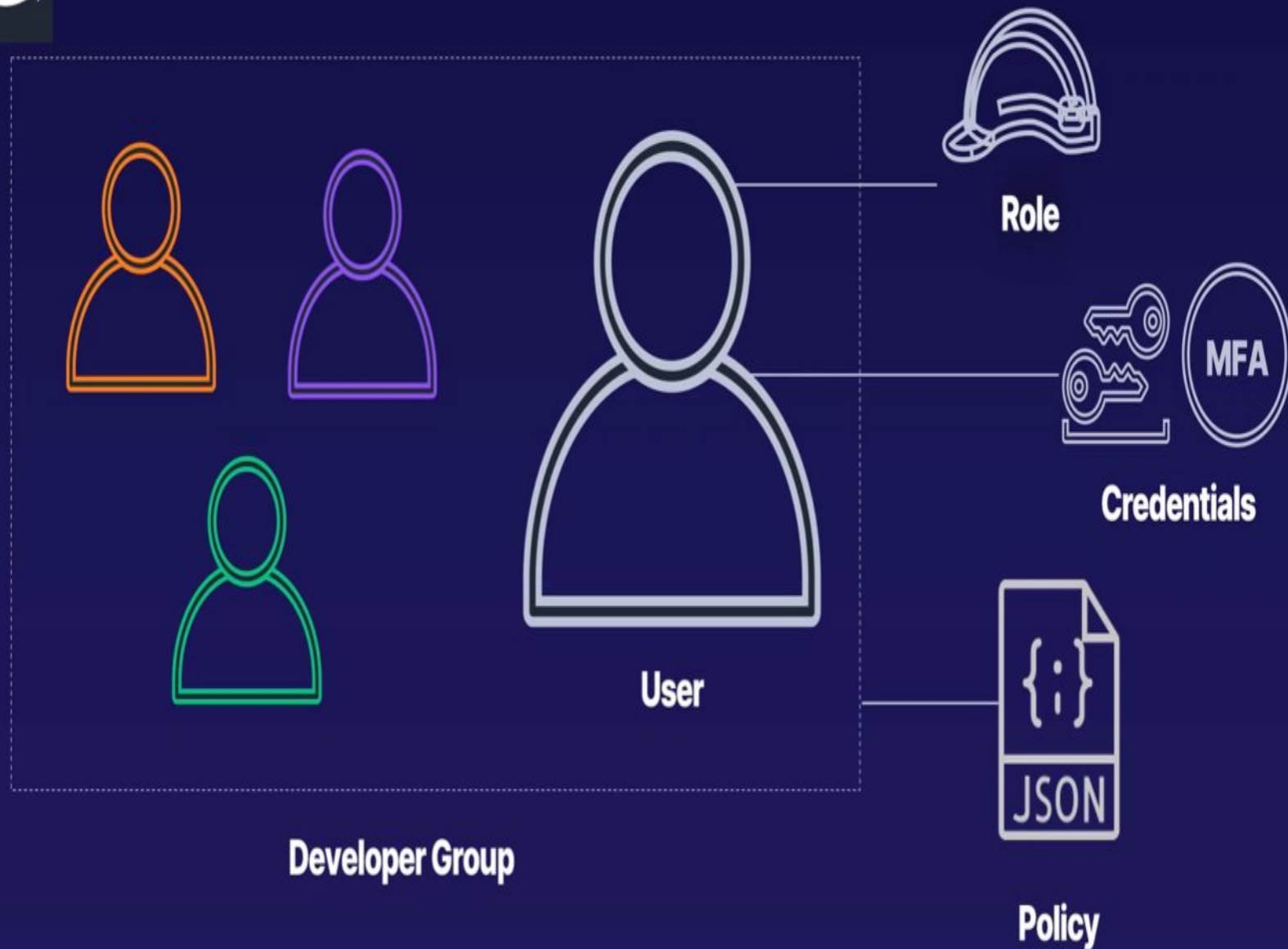
AUTHENTICATION

Authentication identifies **who** you are.

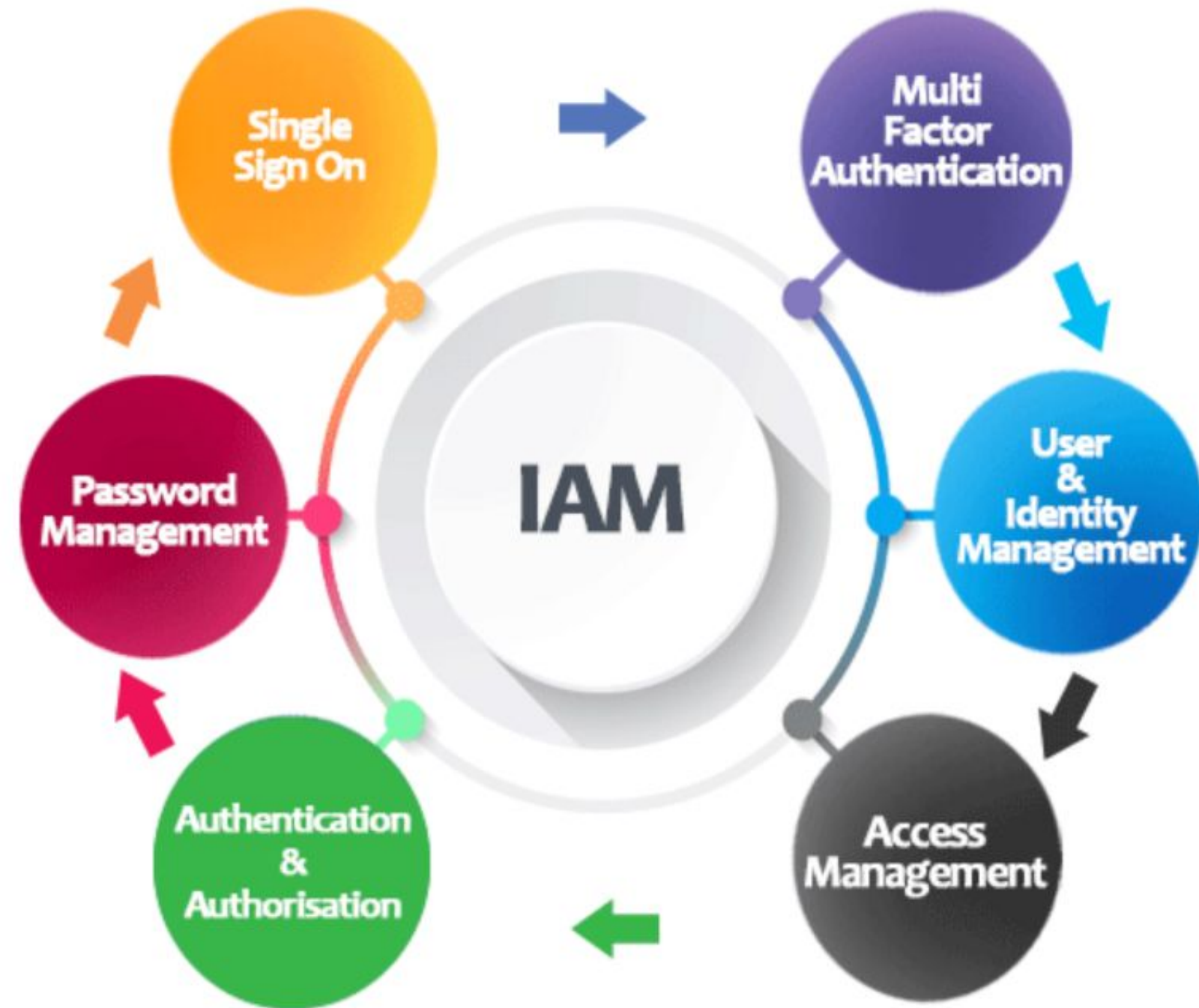
vs.

AUTHORIZATION

Authorization defines **what** you have access to.



- User is an identity.
- Users can be placed in groups. All users within a group share the same permissions.
- Perform a specific duty using a role.
- Policy with granular level permissions.



Key Components of IAM



How to create an IAM User



Simple Storage Service (Amazon S3)





Simple Storage Services (S3)

- Store infinite amount of data
- Highly scalable, reliable, fast, inexpensive data storage infrastructure
- Storage for:
 - Internet applications
 - Backup and recovery
 - Disaster recovery data archives
 - Data lakes for analytics
 - Hybrid cloud storage.

AWS S3 Overview



Object based Storage system - Files are stored as Objects inside Buckets

Key Concepts:

- Buckets
- Objects
- Consistency
- Storage Tiers
- S3 Lifecycle rules
- S3 Performance
- S3 Encryption
- S3 Security

Buckets

- Objects/Files are stored in Buckets (Directories)
- Bucket is an AWS S3 resource that you create
- Buckets are created in a particular region
- Buckets are named unique globally
- Naming convention for buckets:
 - ✓ Bucket names must be between 3 and 63 characters long.
 - ✓ Bucket names can consist only of lowercase letters, numbers, dots (.), and hyphens (-).
 - ✓ Bucket names must begin and end with a letter or number.
 - ✓ Bucket names must not be formatted as an IP address (for example, 192.168.5.4).



Objects (Files)

- **Objects or files have two key attributes:**
 1. **Key :** The name that you assign to an object. You use the object key to retrieve the object.
e.g., example-bucket/directory1/my_file.txt
 2. **Value:** The content that you are storing.
- Maximum size of an object is **5 TB**
- **Metadata** – A set of name-value pairs with which you can store information regarding the object.
- **Version ID** – Within a bucket, a key and version ID uniquely identify an object.
- **Access Control Information** – You can control access to the objects you store in Amazon S3.



AWS S3 Tutorial



Amazon
S3

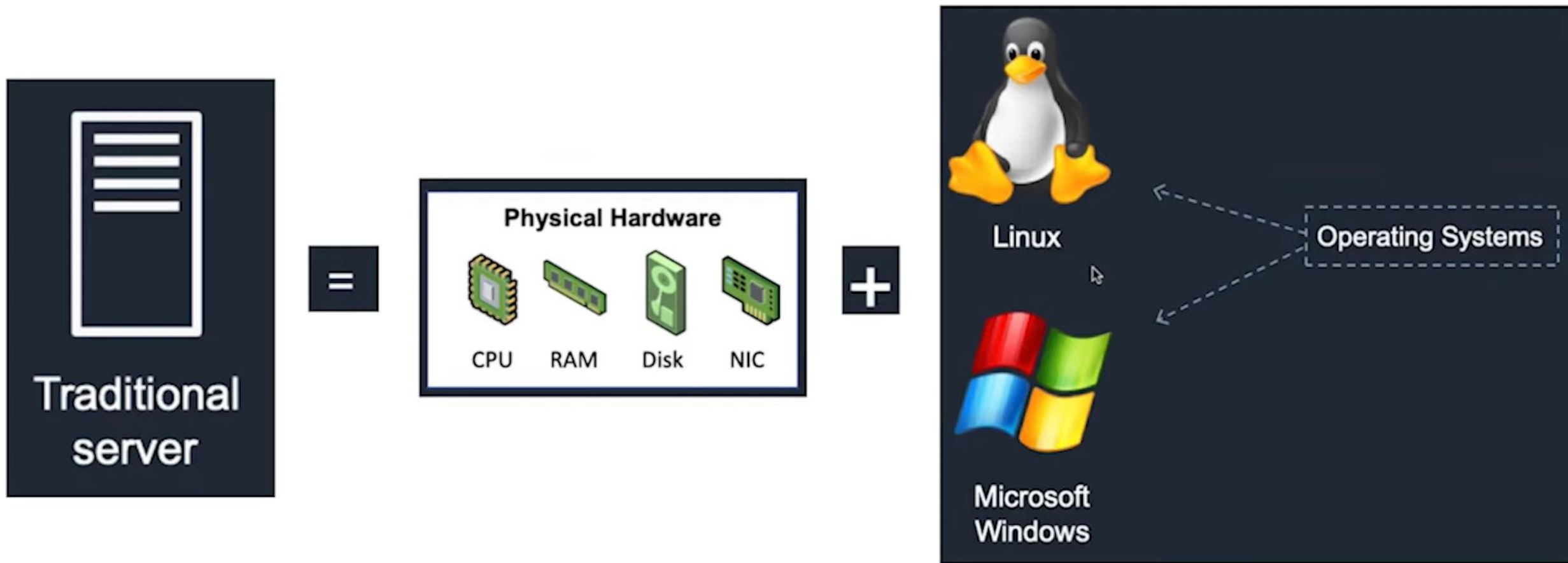
Introduction to AWS S3, How to create S3
Bucket, How to upload files to S3

Play from 7:00

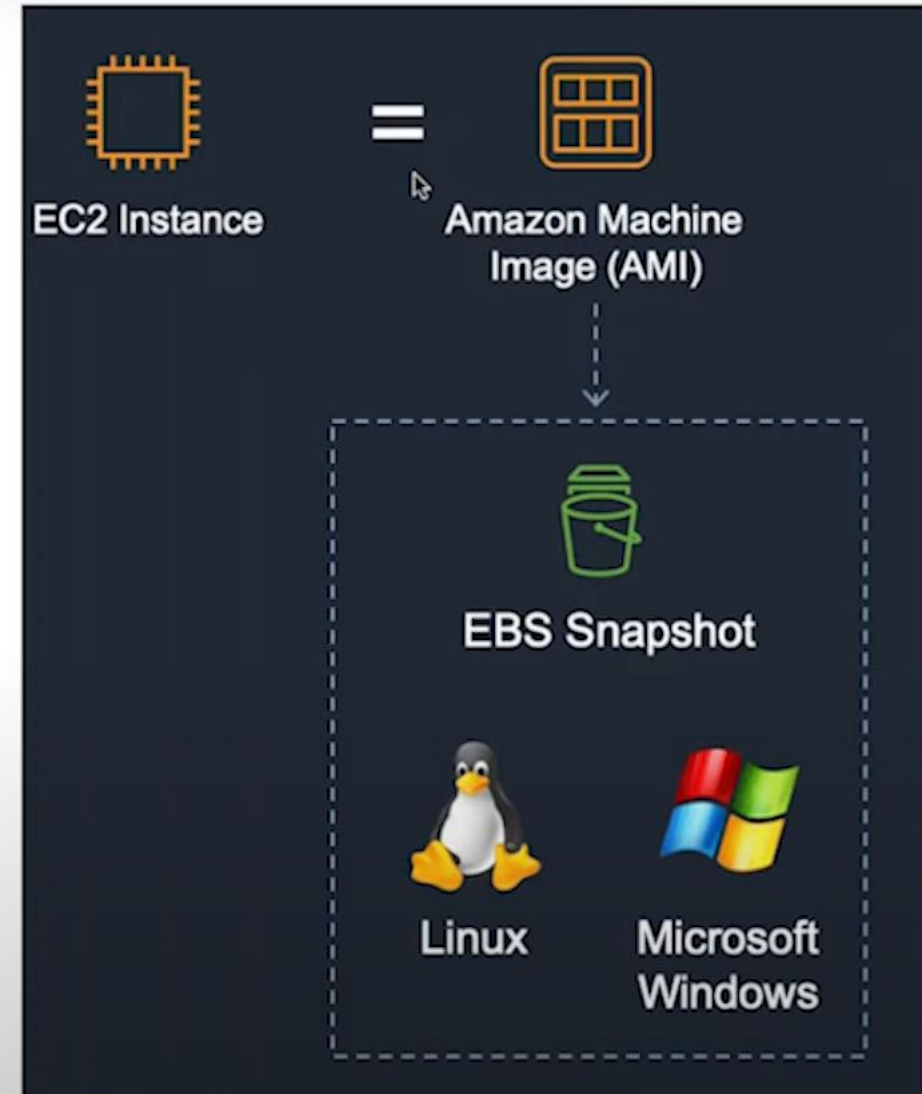


Amazon EC2

Elastic Compute Cloud EC2



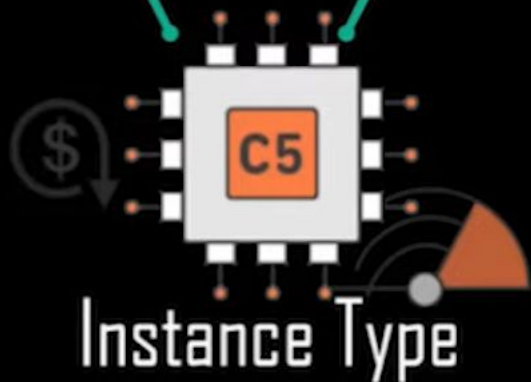
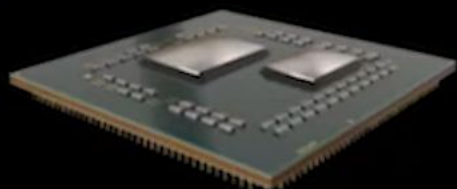
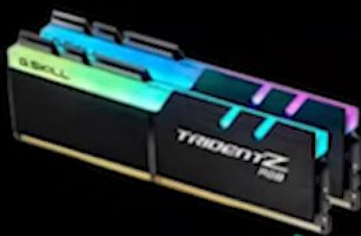
Elastic Compute Cloud EC2



Elastic Compute Cloud EC2

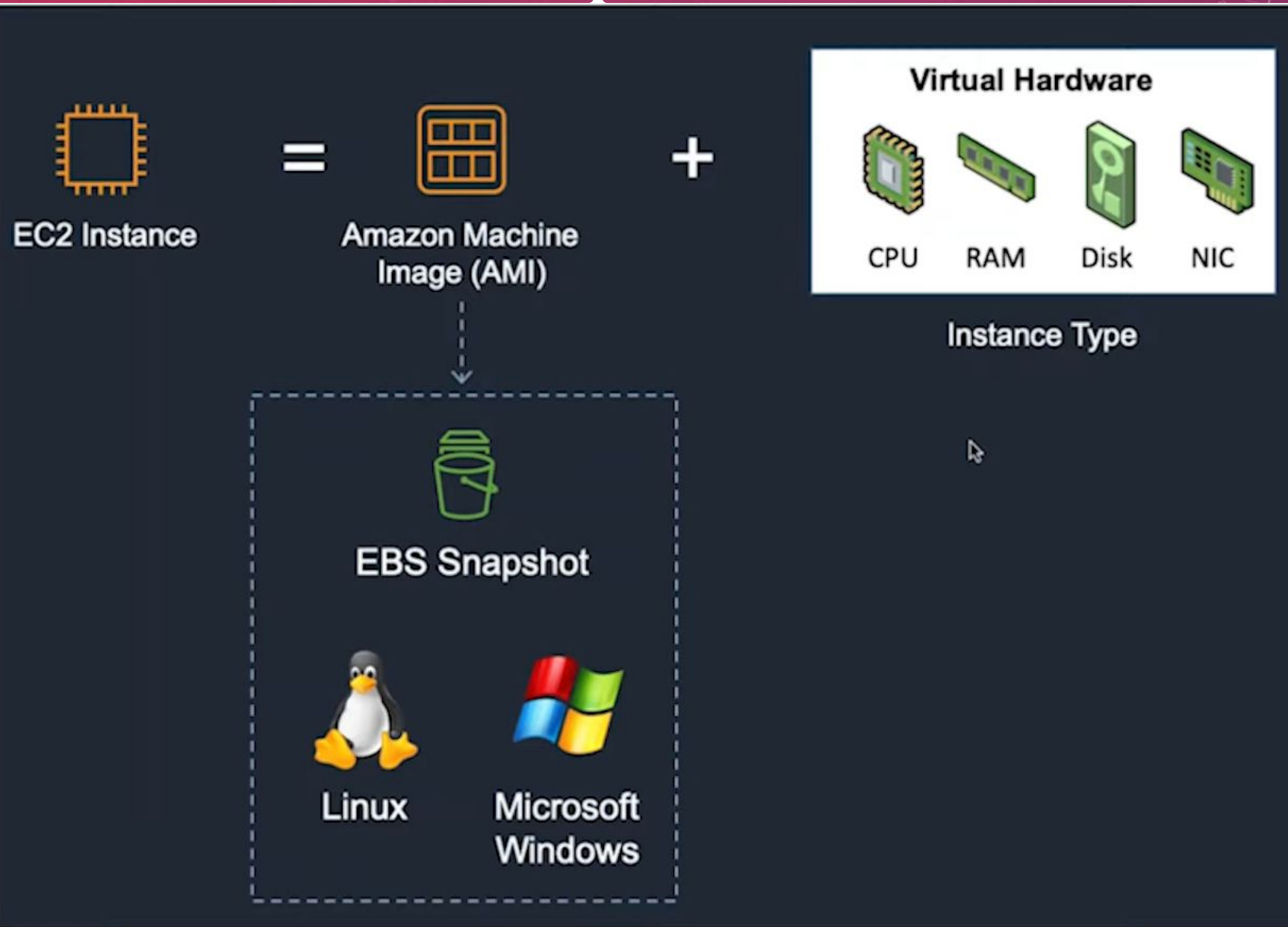


is a virtual computer and scalable



Amazon Machine Images

Elastic Compute Cloud EC2



Elastic Compute Cloud EC2

- EC2 Instances – Virtual servers in AWS(billed by Second)
- EC2 service – Provision EC2 instances or virtual servers
- You can create new instances based on AMIs.
- AMIs are preconfigured templates that include base operating systems and any additional software in a single package.
- It provides various combinations of CPU, memory, storage, and networking capacity for provisioning instances. These combinations are called instance types.

Elastic Compute Cloud EC2

Create an Amazon **EC2** instance

Step by Step Tutorial



Amazon EC2



Amazon VPC

WHAT IS VIRTUAL PRIVATE CLOUD?



A Virtual Private Cloud (VPC) is a special implementation of public cloud that uses a corporate firewall with virtual data isolation and is managed by a cloud provider.

In a VPC, the cloud provider allocates and provisions a portion of its public cloud infrastructure for a single user of VPC, thus keeping the data of a VPC user isolated from other public cloud users.



FEATURES OF A VIRTUAL PRIVATE CLOUD

- User data is stored on a public cloud but isolated from other users using virtualization.
- Offers very high data security with encryption chip security, tunneling, and private IP addressing.
- User gets dedicated cloud server and virtual networks in a VPC.
- It's fully managed by the [cloud provider](#).

