AGENDA

1)Architecture of AWS

2)Region and AZ

3)EC2 instance:- Types and pricing

4)Elastic block store(EBS)

5)Launching an EC2 instance

6)S3 storage:-Types, lifecycle policy and pricing

7)Creating and launching an S3 bucket

8) What is VPC

9) Detailed flow of traffic inside the AWS cloud

10)Routes/IGW's/Subnets/NACL's/Security Group's

What is Cloud Computing

Cloud computing, often referred to as simply “the cloud,” is the delivery of on-demand computing resources — everything from applications to data centers — over the internet on a pay-for-use basis.

Benefits of cloud computing

- Benefit from massive economies of scale
- Increase speed and agility
- Stop guessing capacity
- Stop spending money on running and maintaining data centers
- Go global in minutes

Types of Cloud

Types of cloud deployments: public, private, hybrid

Private cloud

A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

Public cloud

Public clouds are owned and operated by a third-party cloud service provider, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

Hybrid cloud

Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options.

Based on Services

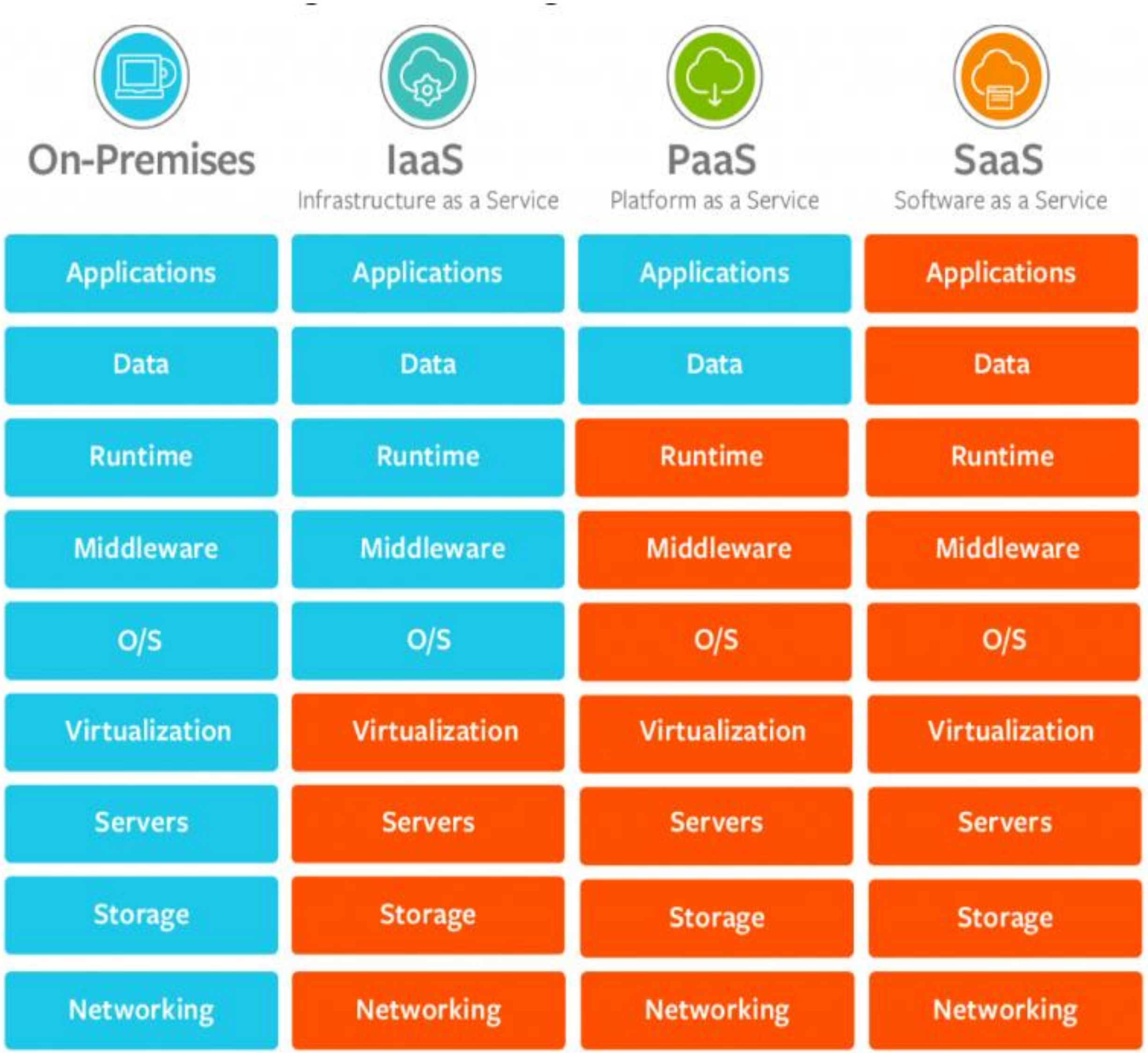
https://www.computerweekly.com/photostory/2240109268/The-Computer-Weekly-guide-to-Cloud-Computing/2/The-difference-between-Saas-Paas-and-Iaas

https://www.cmswire.com/information-management/iaas-vs-paas-vs-saas-cloud-computing-architectures-compared/

https://stackoverflow.com/questions/16820336/what-is-saas-paas-and-iaas-with-examples

Too many confusing definitions

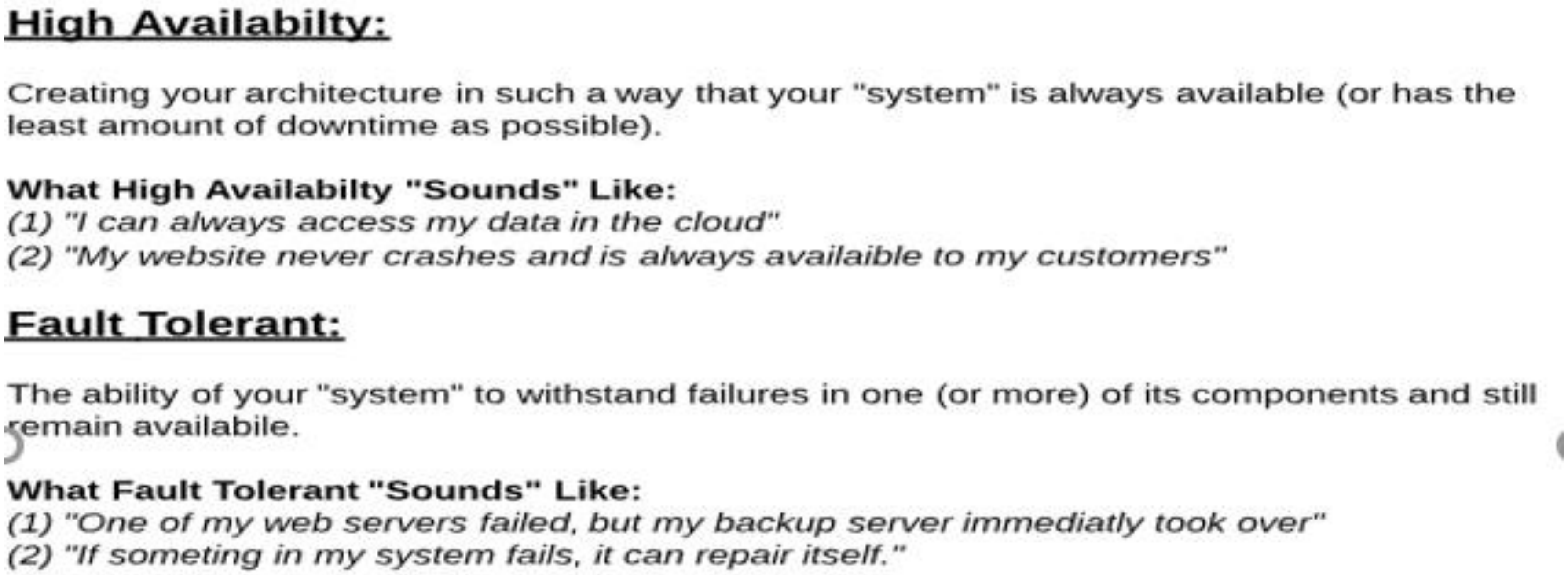
BOOM, now its easy



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	Online DB and servers e.g tomcat server, AWS elastic benstalk
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

HOW WILL BE THE CLOUD ARCHITECTURE



High Availabilty:

Creating your architecture in such a way that your "system" is always available (or has the least amount of downtime as possible).

What High Availabilty "Sounds" Like:
(1) "I can always access my data in the cloud"
(2) "My website never crashes and is always availaible to my customers"

Fault Tolerant:

The ability of your "system" to withstand failures in one (or more) of its components and still remain availabile.

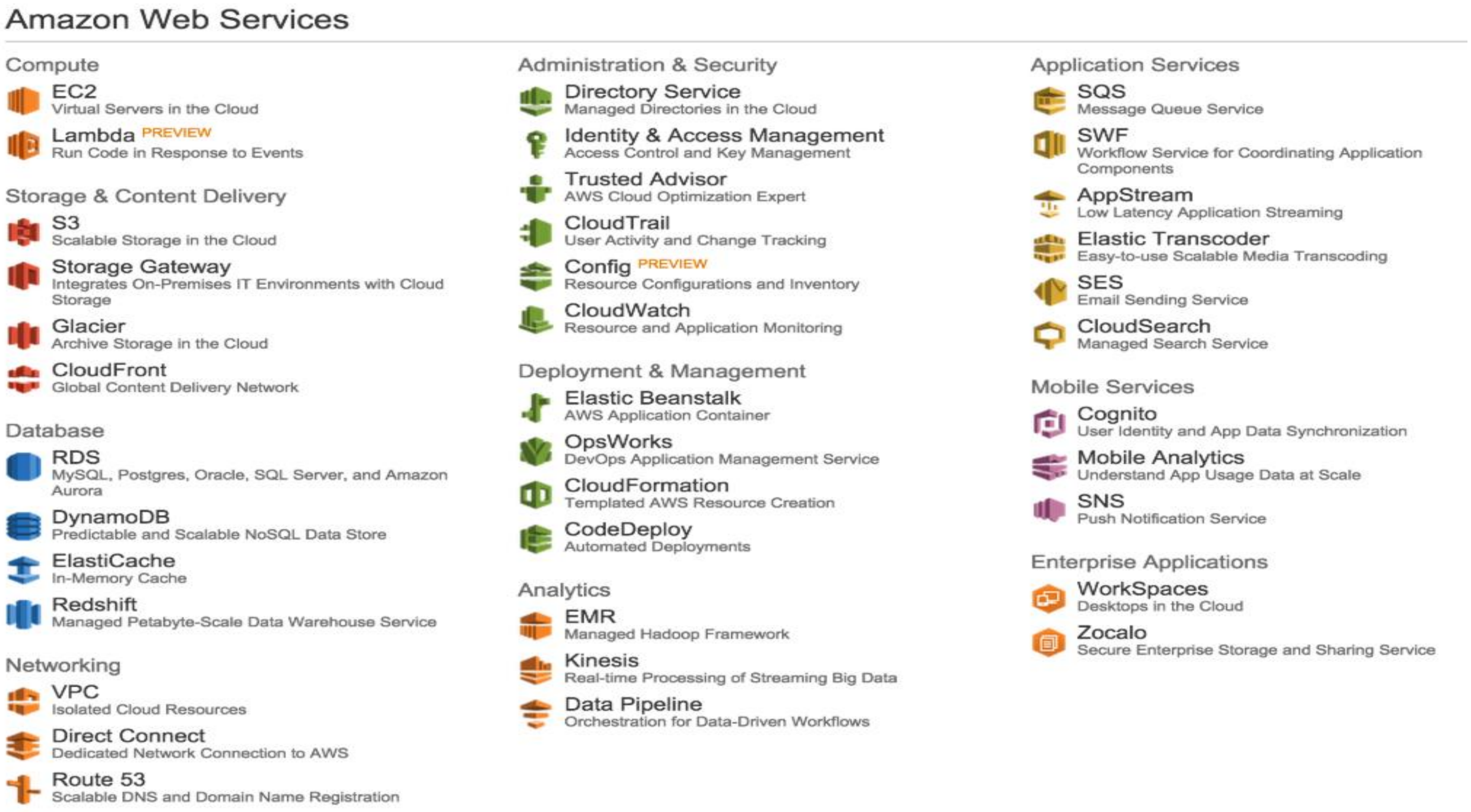
What Fault Tolerant "Sounds" Like:
(1) "One of my web servers failed, but my backup server immediatly took over"
(2) "If someting in my system fails, it can repair itself."

Scalability: "Increasing" the capacity to meet the "increasing" workload.
Elasticity: "Increasing or reducing" the capacity to meet the "increasing or reducing" workload.

What is AWS?

American international multibillion dollar electronic commerce company with headquarters in Seattle, Washington, USA.
started in 1995 by Jeff Bezos as an online bookstore.
but soon diversified, selling DVDs, VHSs, CDs, video and MP3 downloads/streaming, software, video games, electronics, apparel, furniture, food, toys, and jewelry.
The company also produces consumer electronics: Kindle e-book reader and the Kindle Fire tablet computer.
In 2006, Amazon officially launched the Amazon Web Services (AWS) to became a major provider of cloud computing services.

Services Offered by AWS



Amazon Web Services

Compute

- **EC2**
  Virtual Servers in the Cloud
- **Lambda** PREVIEW
  Run Code in Response to Events

Storage & Content Delivery

- **S3**
  Scalable Storage in the Cloud
- **Storage Gateway**
  Integrates On-Premises IT Environments with Cloud Storage
- **Glacier**
  Archive Storage in the Cloud
- **CloudFront**
  Global Content Delivery Network

Database

- **RDS**
  MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora
- **DynamoDB**
  Predictable and Scalable NoSQL Data Store
- **ElastiCache**
  In-Memory Cache
- **Redshift**
  Managed Petabyte-Scale Data Warehouse Service

Networking

- **VPC**
  Isolated Cloud Resources
- **Direct Connect**
  Dedicated Network Connection to AWS
- **Route 53**
  Scalable DNS and Domain Name Registration

Administration & Security

- **Directory Service**
  Managed Directories in the Cloud
- **Identity & Access Management**
  Access Control and Key Management
- **Trusted Advisor**
  AWS Cloud Optimization Expert
- **CloudTrail**
  User Activity and Change Tracking
- **Config** PREVIEW
  Resource Configurations and Inventory
- **CloudWatch**
  Resource and Application Monitoring

Deployment & Management

- **Elastic Beanstalk**
  AWS Application Container
- **OpsWorks**
  DevOps Application Management Service
- **CloudFormation**
  Templated AWS Resource Creation
- **CodeDeploy**
  Automated Deployments

Analytics

- **EMR**
  Managed Hadoop Framework
- **Kinesis**
  Real-time Processing of Streaming Big Data
- **Data Pipeline**
  Orchestration for Data-Driven Workflows

Application Services

- **SQS**
  Message Queue Service
- **SWF**
  Workflow Service for Coordinating Application Components
- **AppStream**
  Low Latency Application Streaming
- **Elastic Transcoder**
  Easy-to-use Scalable Media Transcoding
- **SES**
  Email Sending Service
- **CloudSearch**
  Managed Search Service

Mobile Services

- **Cognito**
  User Identity and App Data Synchronization
- **Mobile Analytics**
  Understand App Usage Data at Scale
- **SNS**
  Push Notification Service

Enterprise Applications

- **WorkSpaces**
  Desktops in the Cloud
- **Zocalo**
  Secure Enterprise Storage and Sharing Service

Steps to create a free account

Amazon Web Services (AWS) is providing **12 months of Free Tier account** to new subscribers to get hands-on experience with all the AWS cloud services. In this AWS Free Tier account, Amazon is giving no. of deferent services use with some of the limitations to get hands-on practice and more knowledge on AWS Cloud services as well regular business use.

https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/

Free Tier

Services that are available in the AWS Free Usage Tier

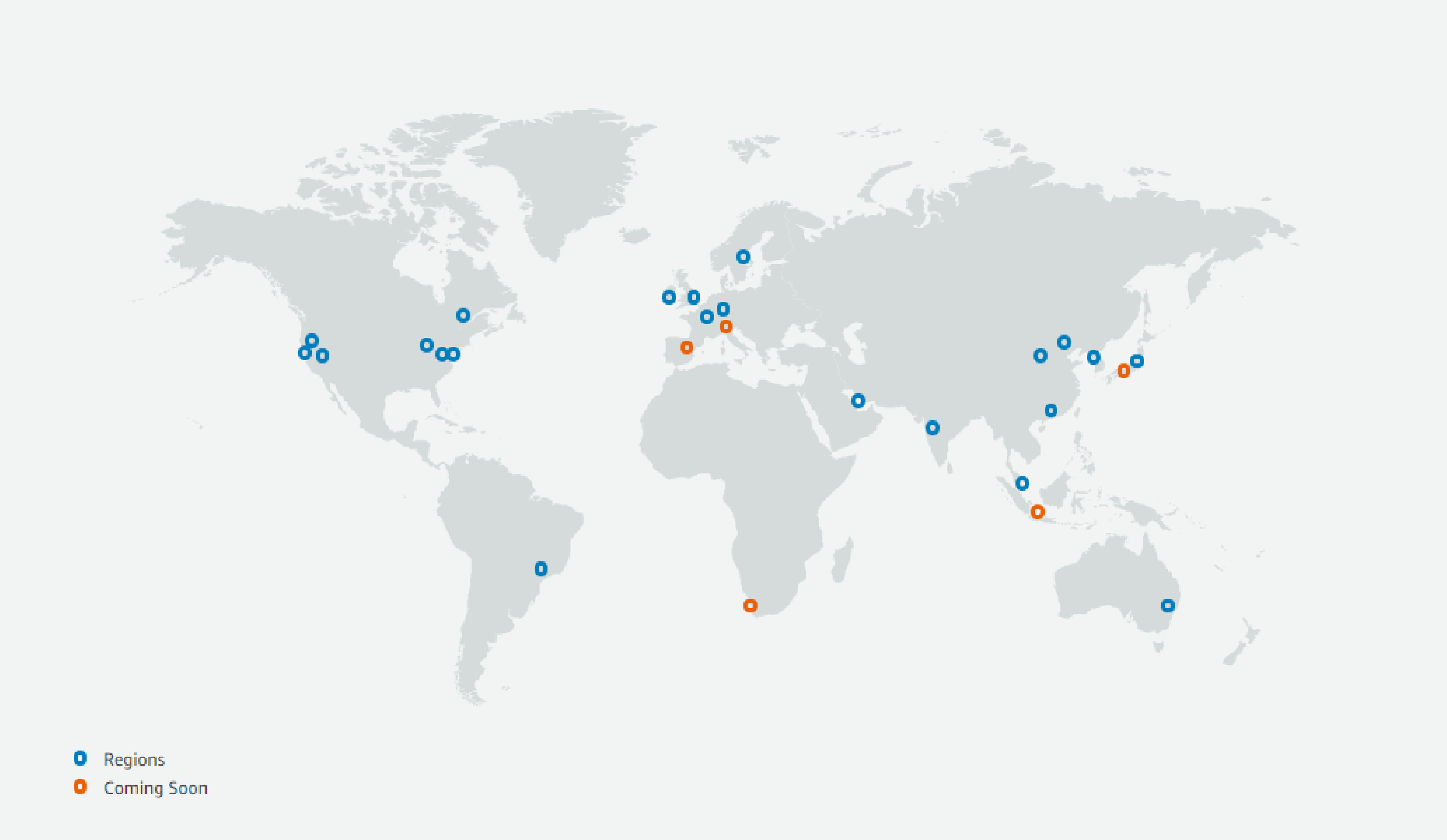
- 750 hours of Amazon EC2 Linux or RHEL or SLES t2.micro instance usage (1 GiB of memory and 32-bit and 64-bit platform support) – enough hours to run continuously each month
- 750 hours of an Elastic Load Balancer plus 15 GB data processing
- 750 hours of Amazon RDS Single-AZ Micro DB Instances, running MySQL, MariaDB, PostgreSQL, Oracle BYOL or SQL Server Express Edition – enough hours to run a DB Instance continuously each month. You also get 20 GB of database storage and 20 GB of backup storage
- 750 hours of Amazon ElastiCache Micro Cache Node usage – enough hours to run continuously each month.
- 30 GB of Amazon Elastic Block Storage in any combination of General Purpose (SSD) or Magnetic, plus 2 million I/Os (with EBS Magnetic) and 1 GB of snapshot storage
- 5 GB of Amazon S3 standard storage, 20,000 Get Requests, and 2,000 Put Requests
- 25 GB of Storage, 25 Units of Read Capacity and 25 Units of Write Capacity, enough to handle up to 200M requests per month with Amazon DynamoDB
- 25 Amazon SimpleDB Machine Hours and 1 GB of Storage
- 1,000 Amazon SWF workflow executions can be initiated for free. A total of 10,000 activity tasks, signals, timers and markers, and 30,000 workflow-days can also be used for free
- 100,000 Requests of Amazon Simple Queue Service
- 100,000 Requests, 100,000 HTTP notifications and 1,000 email notifications for Amazon Simple Notification Service
- 10 Amazon Cloudwatch metrics, 10 alarms, and 1,000,000 API requests
- 50 GB Data Transfer Out, 2,000,000 HTTP and HTTPS Requests for Amazon CloudFront
- 15 GB of bandwidth out aggregated across all AWS services

AWS Global (physical) Infrastructure:

AWS Regions:

- A grouping of ***AWS resources*** located in a specific geographical location.
- Designed to service AWS customers (or your users) that are located closest to a region.
- Regions are comprised of multiple ***Availability Zones***.

AWS now spans 69 Availability Zones within 22 geographic regions around the world, and has announced plans for sixteen more Availability Zones and five more AWS Regions in Indonesia, Italy, Japan, South Africa, and Spain.

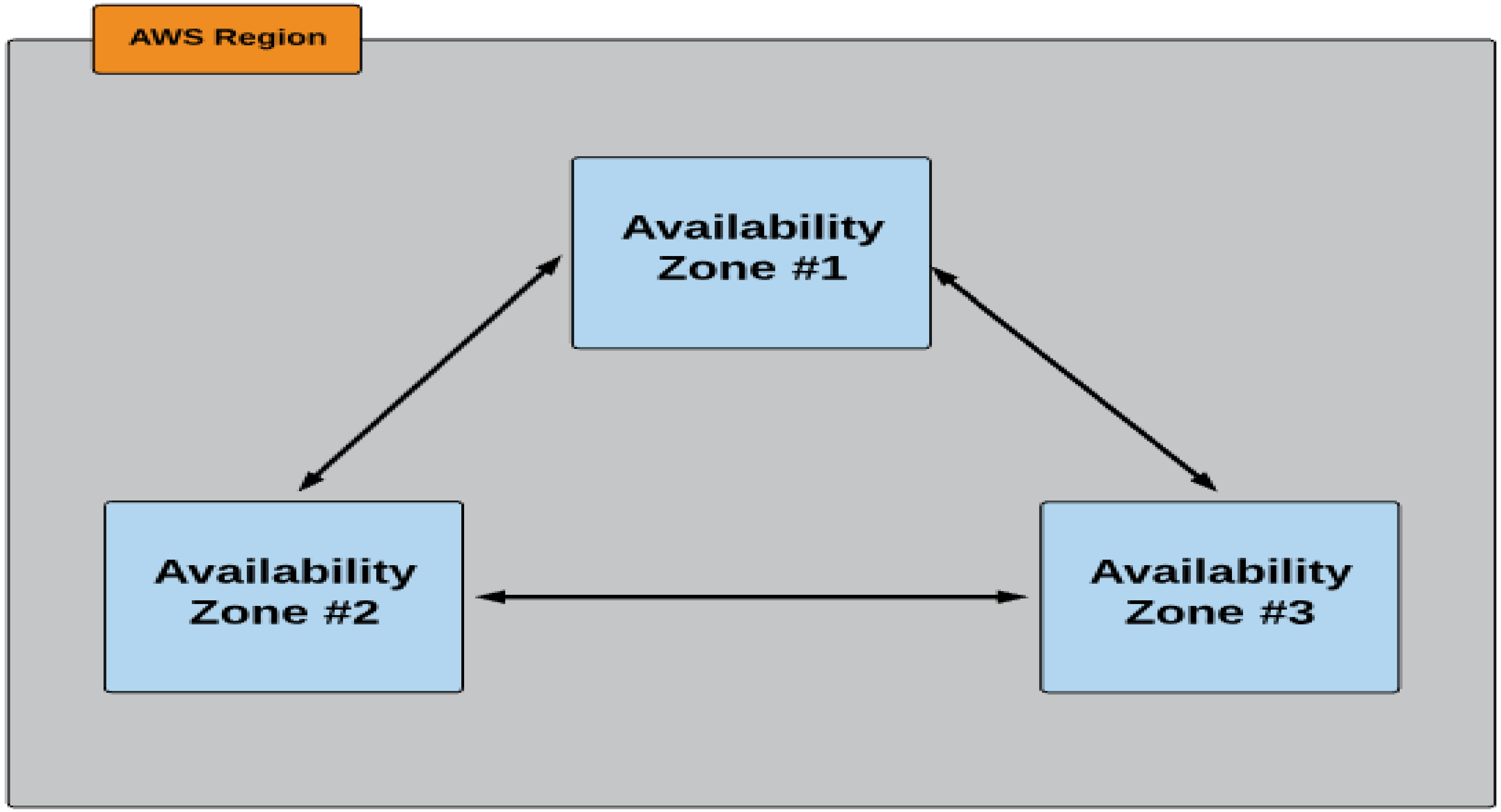


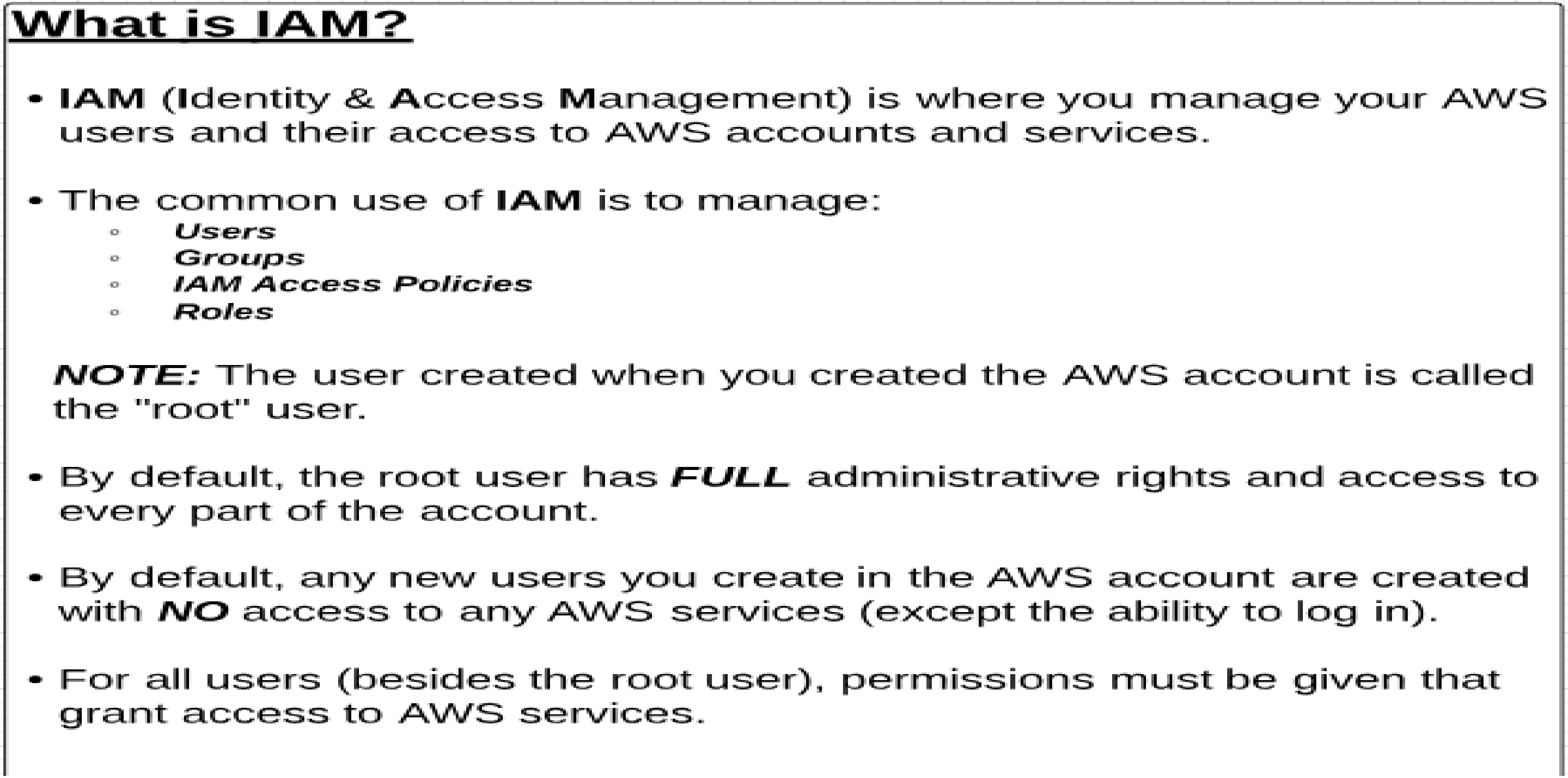
Code	Name
us-east-2	US East (Ohio)
us-east-1	US East (N. Virginia)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
ap-east-1	Asia Pacific (Hong Kong)
ap-south-1	Asia Pacific (Mumbai)
ap-northeast-3	Asia Pacific (Osaka-Local)
ap-northeast-2	Asia Pacific (Seoul)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)
ap-northeast-1	Asia Pacific (Tokyo)
ca-central-1	Canada (Central)
eu-central-1	Europe (Frankfurt)
eu-west-1	Europe (Ireland)
eu-west-2	Europe (London)
eu-west-3	Europe (Paris)
eu-north-1	Europe (Stockholm)
me-south-1	Middle East (Bahrain)
sa-east-1	South America (São Paulo)

AWS Global (physical) Infrastructure:

AWS Availability Zones:

- Geographically isolated zones within a region that house AWS resources
- Availability Zones (AZs) are where seperate, physical ***AWS data centers*** are located.
- Multiple AZs in each Region provide redundancy for AWS resources in that region.





What is IAM?

- **IAM** (**I**dentity & **A**ccess **M**anagement) is where you manage your AWS users and their access to AWS accounts and services.

- The common use of **IAM** is to manage:
  - ***Users***
  - ***Groups***
  - ***IAM Access Policies***
  - ***Roles***

NOTE: The user created when you created the AWS account is called the "root" user.

- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- By default, any new users you create in the AWS account are created with ***NO*** access to any AWS services (except the ability to log in).

- For all users (besides the root user), permissions must be given that grant access to AWS services.

EC2 = Elastic Compute Cloud

What is EC2?

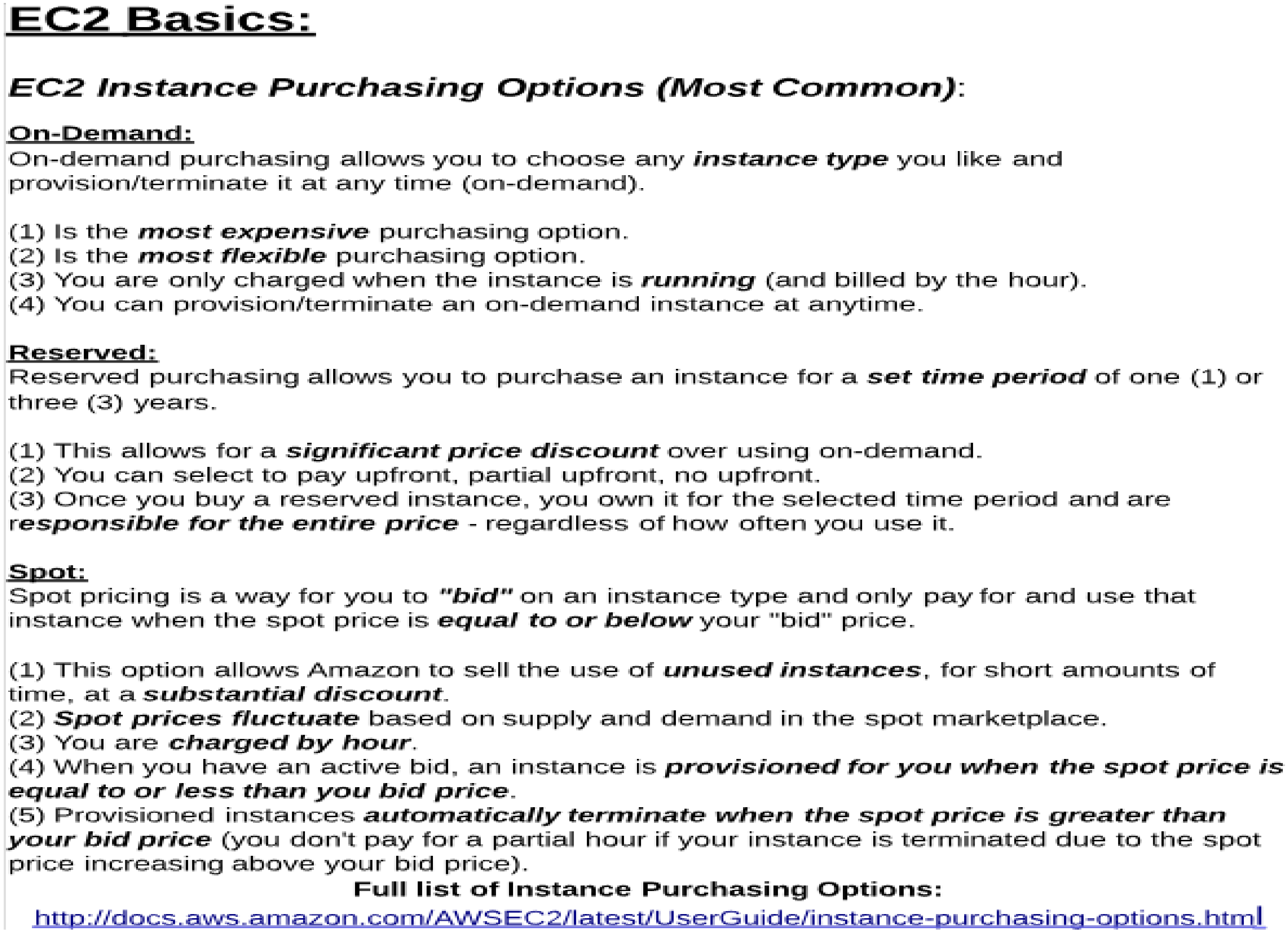
Simplified Definition:
Think of EC2 as your basic desktop computer.

AWS Definition:
"Amazon Elastic Compute Cloud (Amazon EC2) provides ***scalable computing capacity*** in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to ***launch as many or as few virtual servers as you need***, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic."

Amazon EC2 Instance Types

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more instance sizes, allowing you to scale your resources to the requirements of your target workload.

https://aws.amazon.com/ec2/instance-types/



EC2 Basics:

EC2 Instance Purchasing Options (Most Common):

On-Demand:
On-demand purchasing allows you to choose any ***instance type*** you like and provision/terminate it at any time (on-demand).

(1) Is the ***most expensive*** purchasing option.
(2) Is the ***most flexible*** purchasing option.
(3) You are only charged when the instance is ***running*** (and billed by the hour).
(4) You can provision/terminate an on-demand instance at anytime.

Reserved:
Reserved purchasing allows you to purchase an instance for a ***set time period*** of one (1) or three (3) years.

(1) This allows for a ***significant price discount*** over using on-demand.
(2) You can select to pay upfront, partial upfront, no upfront.
(3) Once you buy a reserved instance, you own it for the selected time period and are r***esponsible for the entire price*** - regardless of how often you use it.

Spot:
Spot pricing is a way for you to ***"bid"*** on an instance type and only pay for and use that instance when the spot price is ***equal to or below*** your "bid" price.

(1) This option allows Amazon to sell the use of ***unused instances***, for short amounts of time, at a ***substantial discount***.
(2) ***Spot prices fluctuate*** based on supply and demand in the spot marketplace.
(3) You are ***charged by hour***.
(4) When you have an active bid, an instance is ***provisioned for you when the spot price is equal to or less than you bid price***.
(5) Provisioned instances ***automatically terminate when the spot price is greater than your bid price*** (you don't pay for a partial hour if your instance is terminated due to the spot price increasing above your bid price).

Full list of Instance Purchasing Options:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html

EBS = **E**lastic **B**lock **S**tore

What is an EBS?

Simplified Definition:
EBS is a ***storage volume*** for an EC2 instance. (***Think of it as a hard drive.***)

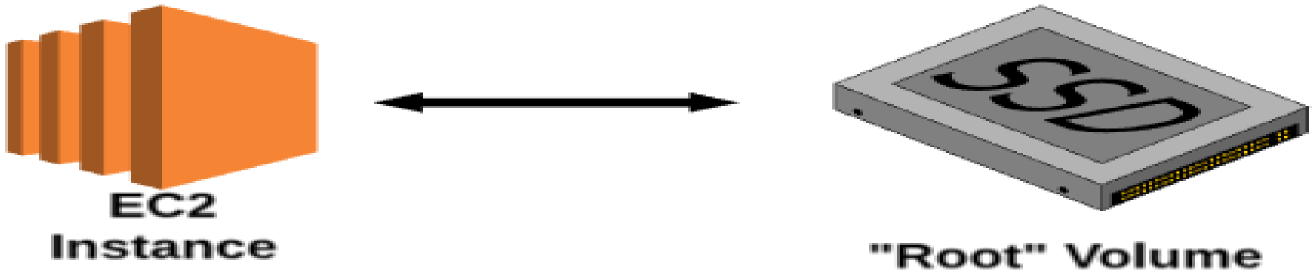
AWS Definition:
"Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes are ***highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone***. EBS volumes that are attached to an EC2 instance are exposed as ***storage volumes that persist independently from the life of the instance***."

EBS:

"Root" vs. Additional EBS Volumes:

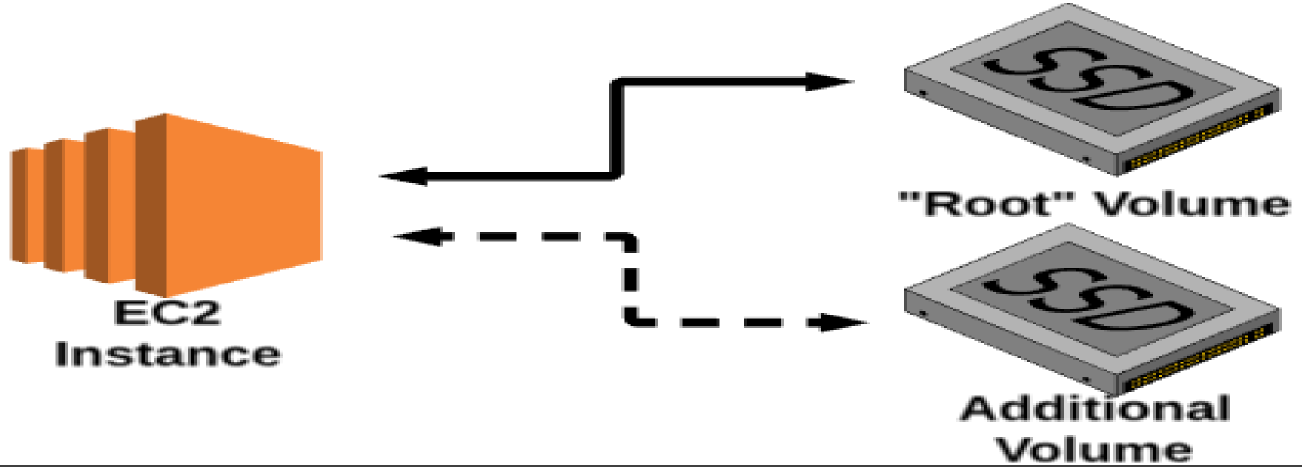
(1) Every EC2 instance MUST have a "root" volume, which may or may not be EBS.

(2) By default, EBS "root" volumes are set to be deleted when the instance is terminated. However, you can choose to have EBS volumes persist after termination.

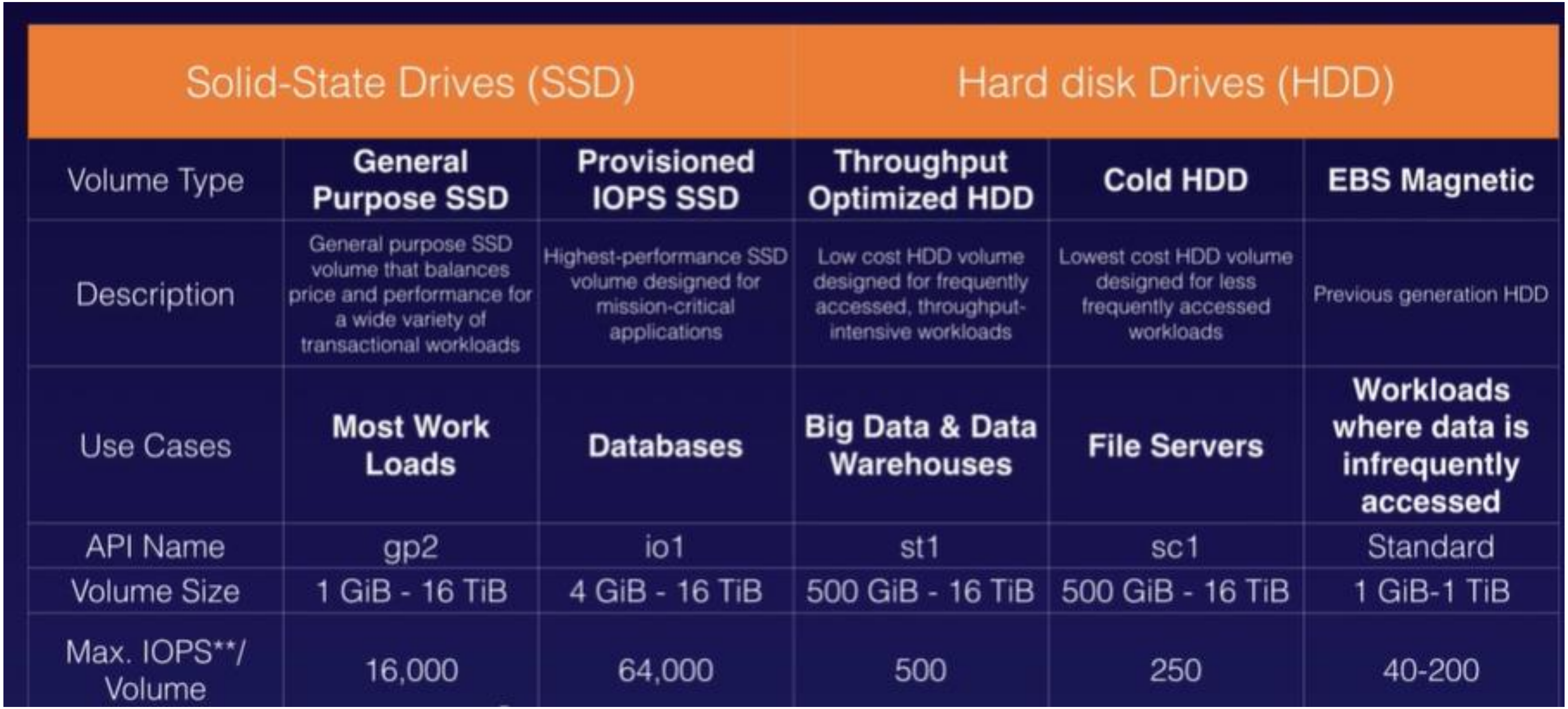


(3) During the creation of an EC2 instance (or anytime afterwards) you can add additional EBS Volumes to the instance.

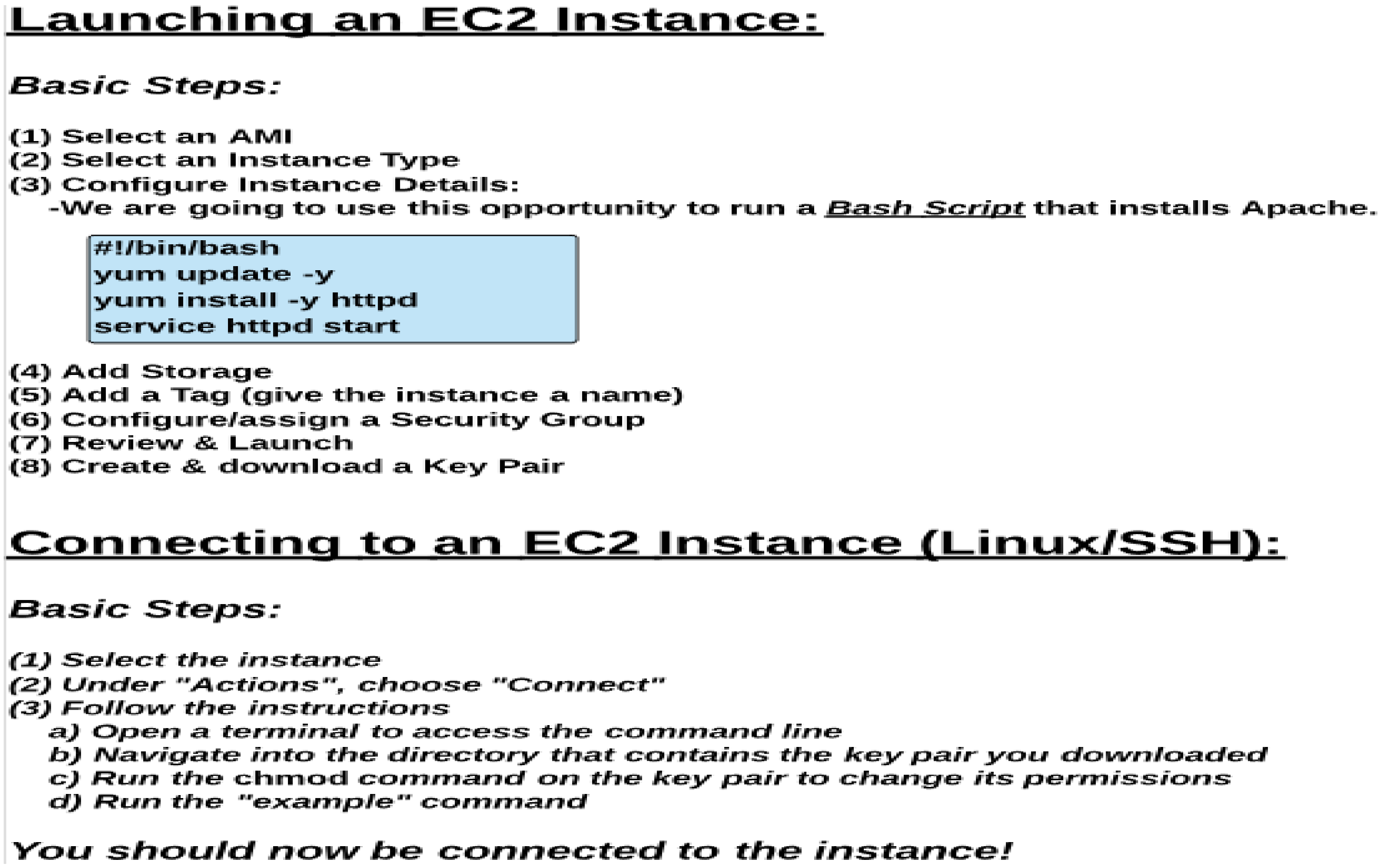
(4) Any additional volume can be attached or detach from the instance at any time, and is NOT deleted (be default) when the instance is terminated.



EBS types



	Solid-State Drives (SSD)		Hard disk Drives (HDD)		
Volume Type	**General Purpose SSD**	**Provisioned IOPS SSD**	**Throughput Optimized HDD**	**Cold HDD**	**EBS Magnetic**
Description	General purpose SSD volume that balances price and performance for a wide variety of transactional workloads	Highest-performance SSD volume designed for mission-critical applications	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads	Previous generation HDD
Use Cases	**Most Work Loads**	**Databases**	**Big Data & Data Warehouses**	**File Servers**	**Workloads where data is infrequently accessed**
API Name	gp2	io1	st1	sc1	Standard
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB	1 GiB-1 TiB
Max. IOPS**/ Volume	16,000	64,000	500	250	40-200



Launching an EC2 Instance:

Basic Steps:

(1) Select an AMI
(2) Select an Instance Type
(3) Configure Instance Details:
-We are going to use this opportunity to run a *Bash Script* that installs Apache.

```
#!/bin/bash
yum update -y
yum install -y httpd
service httpd start
```

(4) Add Storage
(5) Add a Tag (give the instance a name)
(6) Configure/assign a Security Group
(7) Review & Launch
(8) Create & download a Key Pair

Connecting to an EC2 Instance (Linux/SSH):

Basic Steps:

(1) Select the instance
(2) Under "Actions", choose "Connect"
(3) Follow the instructions
a) Open a terminal to access the command line
b) Navigate into the directory that contains the key pair you downloaded
c) Run the chmod command on the key pair to change its permissions
d) Run the "example" command

You should now be connected to the instance!

EFS

Amazon EFS (Elastic File System) is a cloud-based file storage service for applications and workloads that run in the Amazon Web Services (AWS) public cloud.

AWS automatically deploys and manages the infrastructure for EFS, which is distributed across an unconstrained number of servers to avoid performance bottlenecks. Amazon EFS provides elastic storage capacity that scales to accommodate workloads that run on Elastic Compute Cloud (EC2) instances and access files through application programming interface (API) requests. An administrator interacts with EFS through its file system interface.

Amazon EFS is designed to be highly available and durable for thousands of EC2 instances that are connected to the service. Amazon EFS stores each file system object in multiple availability zones (AZs); an IT pro can access each file system from different AZs in the region it is located. The service also supports periodic backups from on-premises storage services to EFS for disaster recovery.

In lay man terms think of it as a Shared drive that can attach to multiple systems

ISSUE FACED

AWS EBS provides persistent block-level data storage. Block storage stores files in multiple volumes called blocks, which act as separate hard drives; block storage devices are more flexible and offer higher performance than regular file storage. You need to mount EBS onto an Amazon EC2 instance. Use cases include business continuity, software testing, and database management.

AWS EFS is a shared, elastic file storage system that grows and shrinks as you add and remove files. It offers a traditional file storage paradigm, with data organized into directories and subdirectories. EFS is useful for SaaS applications and content management systems. You can mount EFS onto several EC2 instances at the same time.

S3 = Simple Storage Service

What is S3

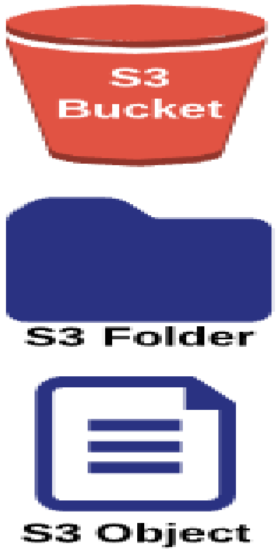
Simplified Definition:
An online, bulk storage service that you can access from almost any device.

AWS Definition:
"Amazon S3 has a simple web services interface that you can use to ***store and retrieve any amount of data, at any time, from anywhere on the web***. It gives any user access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits on to users."

AWS S3

S3 Basics:

Components and Structure:



Basics:
(1) S3 = Simple Storage Service
(2) It is AWS's primary storage service.
(3) You can store any type of file in S3.

Buckets:
(1) Root level "Folders" you create in S3 are referred to as ***buckets***.
(2) Any "subfolder" you create in a bucket is referred to as a ***folder***.

Objects:
(1) Files stored in a bucket are referred to as ***objects***.

Regions:
(1) When you create a bucket, you must select a specific region for it to exist. This means that ***any data you upload to the S3 bucket will be physically located in a data center in that region***.

(2) ***Best practice*** is to select the region that is physically ***closest to you***, to ***reduce transfer latency***.

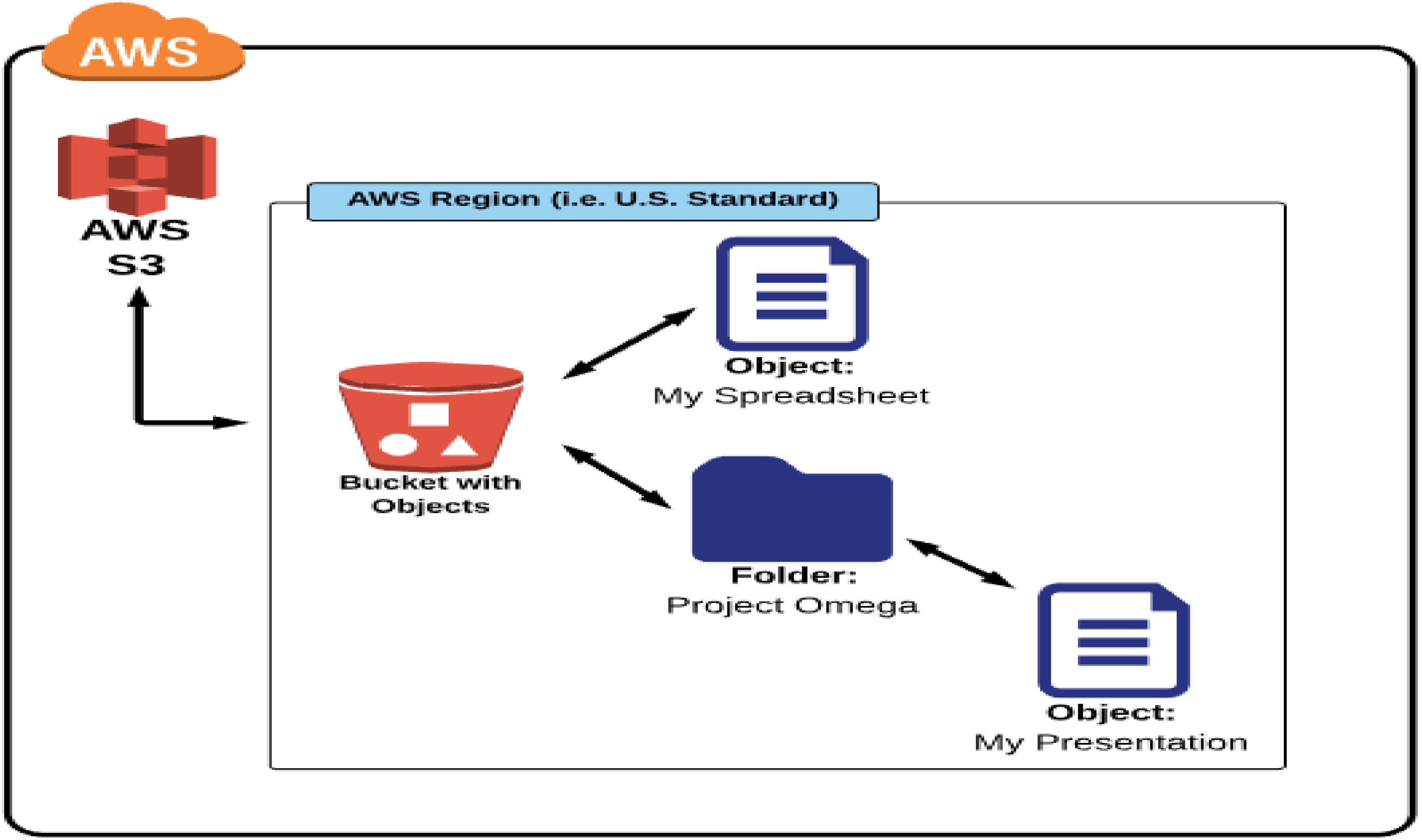
OR

(3) If you are serving files to a ***customer*** based in a certain area of the world, ***create the bucket in a region closest to your customers*** (to reduce latency for your customers).

NOTE: Some AWS services only work with/communicate with each other if they are in the same AWS region.

S3 Basics:

Components & Structure:



Buckets and Folders:

Creating an S3 Bucket:

(1) Choose a bucket name:

Bucket names must follow a set of rules:
-Bucket names must be unique across ALL of AWS.
-Bucket names must be 3 to 63 characters in length.
-Bucket names can only contain lowercase letters, numbers and hyphens.
-Bucket names must not be formatted as an IP address (e.g., 192.168.5.4).

(2) Select a region

NOTE: There are more "advanced" rules that allow for some varying formats, which can be found here: http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html

Uploading (Import) an Object to a Bucket:

(1) Navigate into a bucket
(2) Under "Actions" select "upload"
(3) Select a file to upload
(4) Click "Start Upload"

Creating a Folder in a Bucket:

(1) Navigate into a bucket
(2) Click on "Create Folder"
(3) Give the folder a name

NOTE: Uploading an object directly into folder is the same process, just navigate into the folder first.

Types of S3 Buckets

Amazon S3 Standard

- This storage class is suitable for frequently accessed data.

•It is a default storage class.

•Can be used for cloud applications, dynamic websites, content distribution, gaming applications, and Big data analytics

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access

Amazon S3 Standard –Infrequent Access

- **T**his storage class is suitable for infrequently accessed data.

•It demands rapid access.

•It is suitable for backups, disaster recovery and lifelong storage of data.

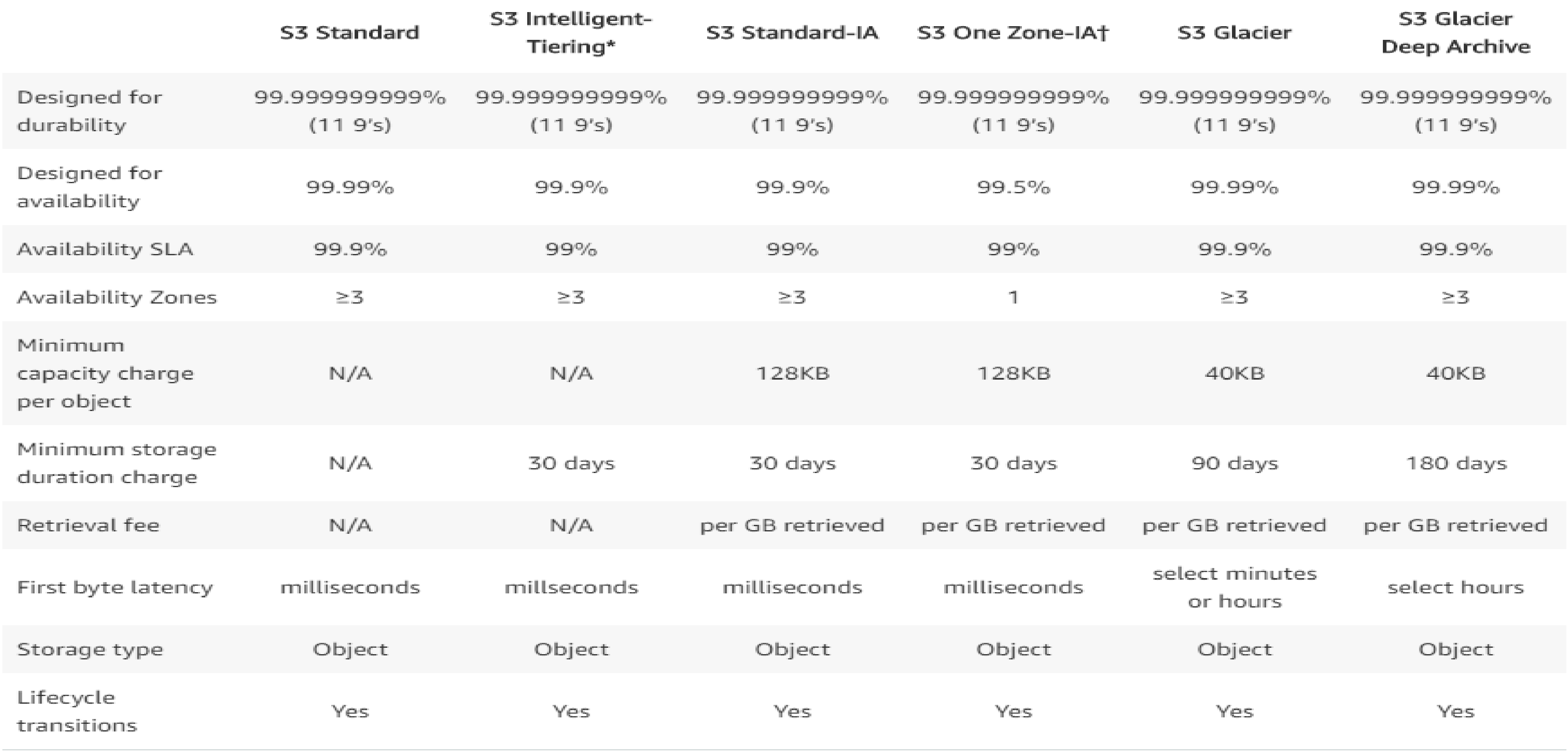
Amazon Glacier

•This storage class is suitable for archiving data where data access is infrequent.

•It has a vault-lock feature which provides a long term data storage.

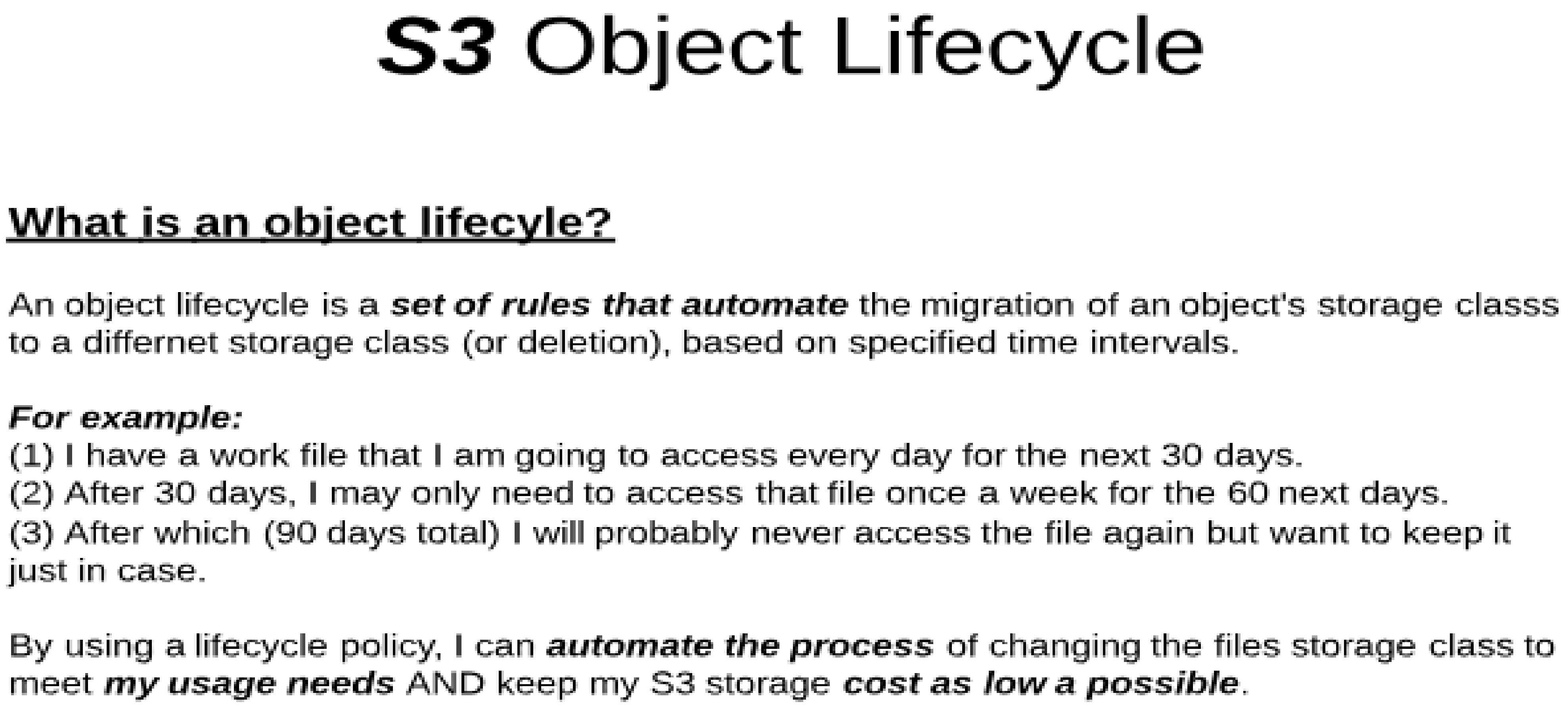
•It provides the lowest cost availability.

Pricing and All



	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128KB	128KB	40KB	40KB
Minimum storage duration charge	N/A	30 days	30 days	30 days	90 days	180 days
Retrieval fee	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	millseconds	milliseconds	milliseconds	select minutes or hours	select hours
Storage type	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes

https://aws.amazon.com/s3/pricing/



S3 Object Lifecycle

What is an object lifecyle?

An object lifecycle is a ***set of rules that automate*** the migration of an object's storage classs to a differnet storage class (or deletion), based on specified time intervals.

For example:
(1) I have a work file that I am going to access every day for the next 30 days.
(2) After 30 days, I may only need to access that file once a week for the 60 next days.
(3) After which (90 days total) I will probably never access the file again but want to keep it just in case.

By using a lifecycle policy, I can ***automate the process*** of changing the files storage class to meet ***my usage needs*** AND keep my S3 storage ***cost as low a possible***.

VPC = Virtual Private Cloud

What is a VPC?

Simplified Definition:
A private sub-section of AWS that you control, in which you can place AWS resources (such as EC2 instances and databases). You have FULL control over who has access to the AWS resources that you place inside your VPC.

AWS Definition:
"Amazon Virtual Private Cloud (Amazon VPC) lets you provision a ***logically isolated*** section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a ***virtual network*** that you define. ***You have complete control over your virtual networking environment***, including selection of your own IP address range, creation of ***subnets*** and configuration of ***route tables*** and ***network gateways***."

NOTE: When you create an AWS account, a "default" VPC is created for you. Including the standard components that are needed make it functional.
(1) Internet Gateway (IGW)
(2) A route table (with predefied routes to the default subnets)
(3) A Network Access Control List (with predefired rules for access)
(4) Subnets to provision AWS resources in (such as EC2 Instances)

Availabili

Availability Zones and VPCs:

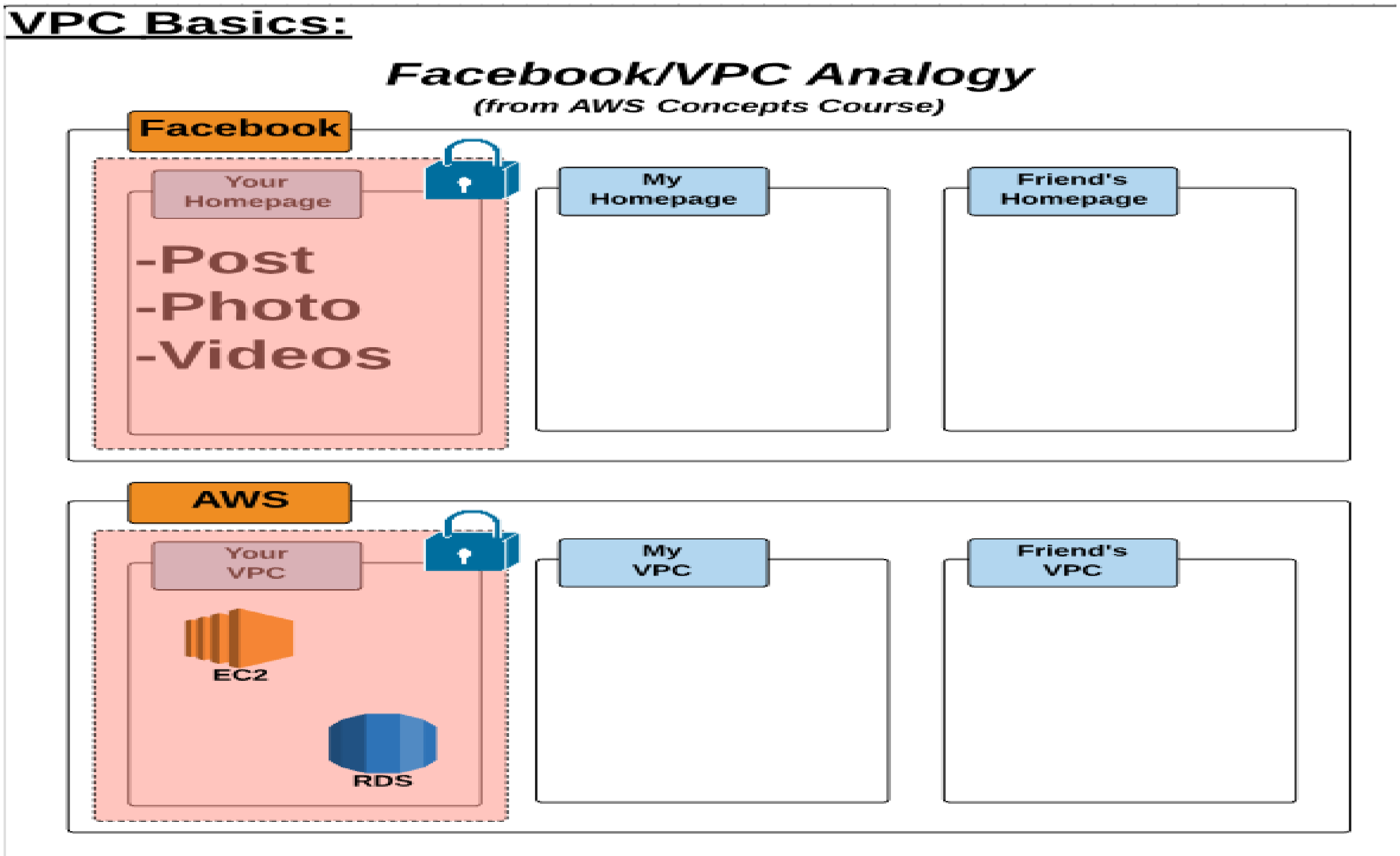
Simplified Definition/Explanation:
Any AWS resource that you launch (like EC2/R
given subnet must be located in an Availbility Z
Availabilty Zones to create redundacy in your a
Availabilty and ***Fault Toleratent*** systems.

AWS Definition/Explanation:
"When you create a ***VPC, it spans all of the A***
a VPC, you can add ***one or more subnets in e***
reside entirely within one Availability Zone and

Availability Zones are distinct locations that
in other Availability Zones. By launching ins
can protect your applications from the failur

NOTE: Your "default" VPC already has a subn

Availabil

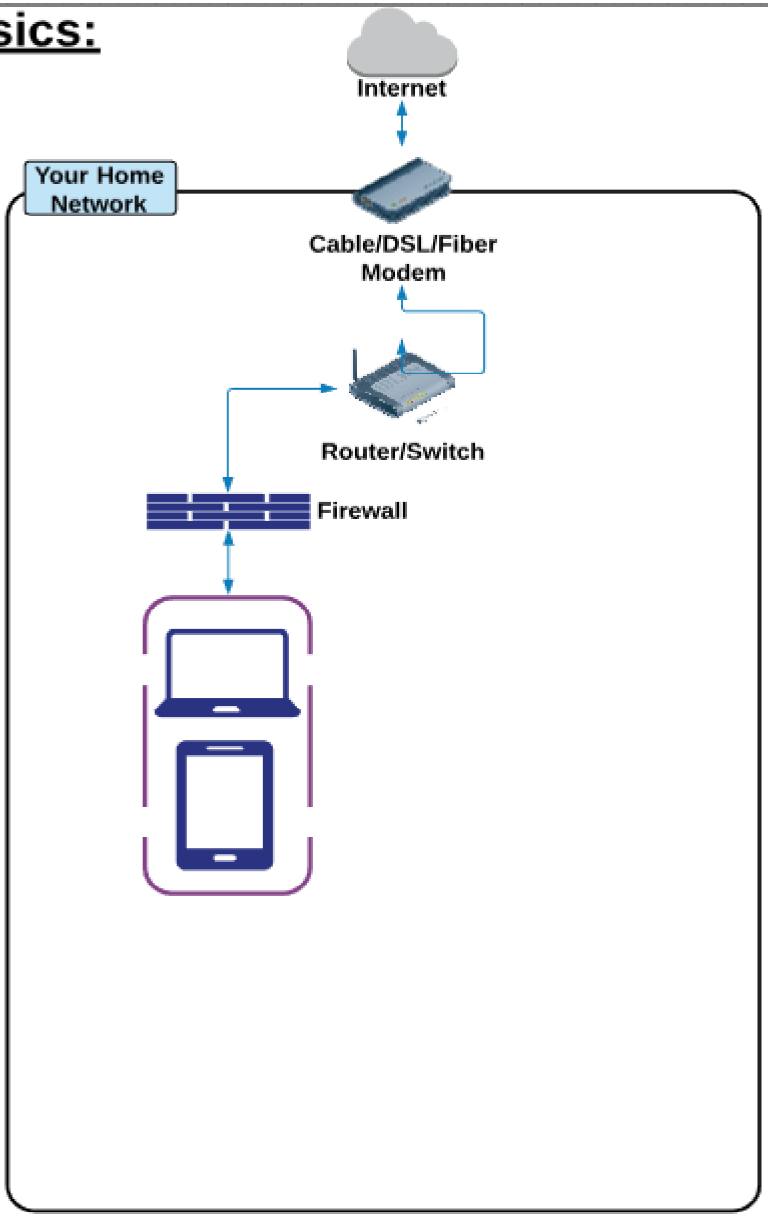


VPC Basics:

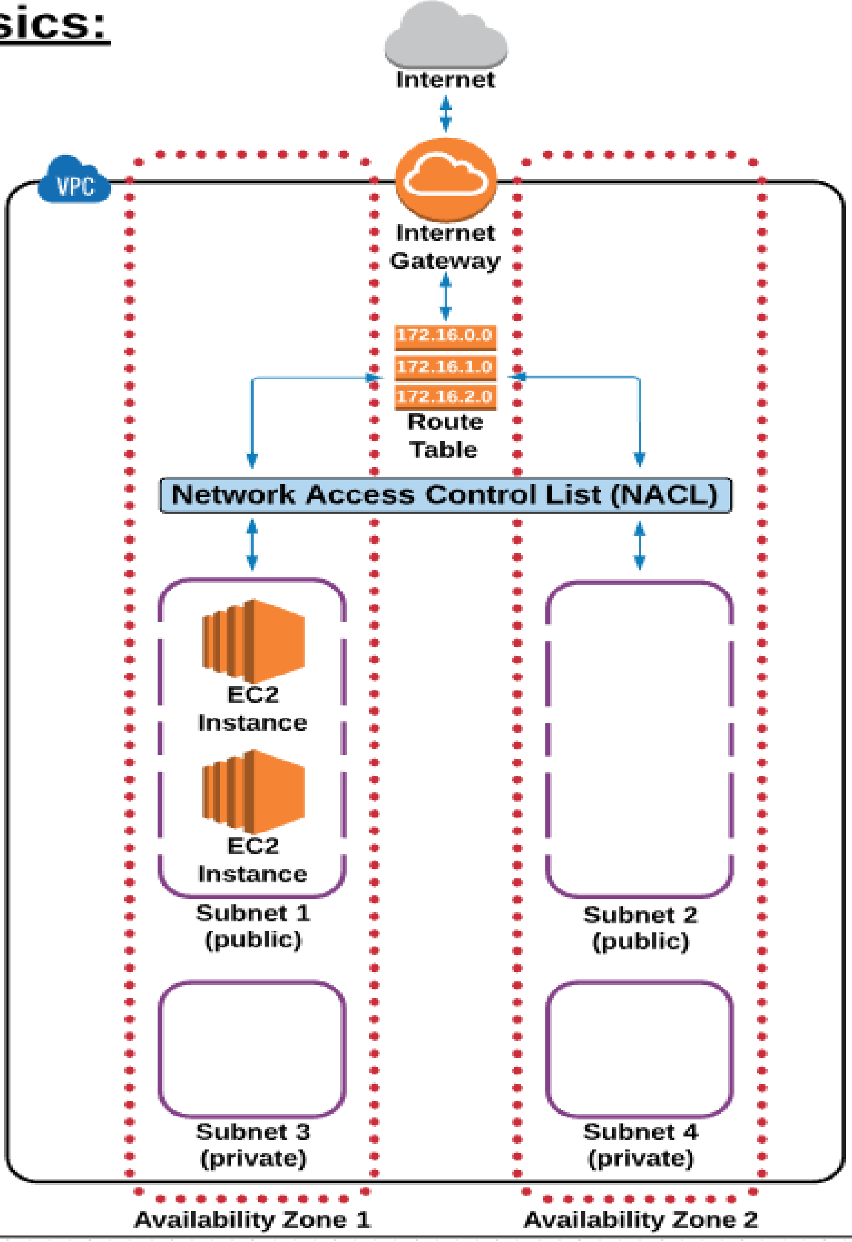
Facebook/VPC Analogy

(from AWS Concepts Course)

VPC Basics:



VPC Basics:



IGW = Internet Gateways

What is an IGW?

Simplified Definition:
A combination of hardware and software that provides your private network with a ***route*** to the world outside (meaning the Internet) of the VPC.

AWS Definition:
An Internet gateway is a horizontally scaled, ***redundant and highly available*** VPC component that ***allows communication between instances in your VPC and the Internet***. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

NOTE: Your "default" VPC already has an IGW ***attached***.

RTs = Route Tables

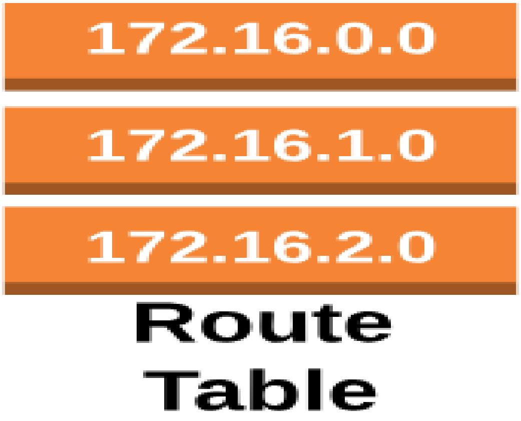
What is a Route Table?

Simplified Definition:
The AWS definition is simple enough, so let's jump right down to it!

AWS Definition:
"A route table contains a ***set of rules***, called ***routes***, that are used to ***determine where network traffic is directed***."

NOTE: Your "default" VPC already has a ***"main"*** route table.

Route table rules and details you need to know:
(1) Unlike an IGW, you can have multiple "active" route tables in a VPC
(2) You cannot delete a route table if it has ***"dependancies"*** (associated subnets)



172.16.0.0

172.16.1.0

172.16.2.0

Route Table

NACLs = Network Access Control Lists

What is a NACL?

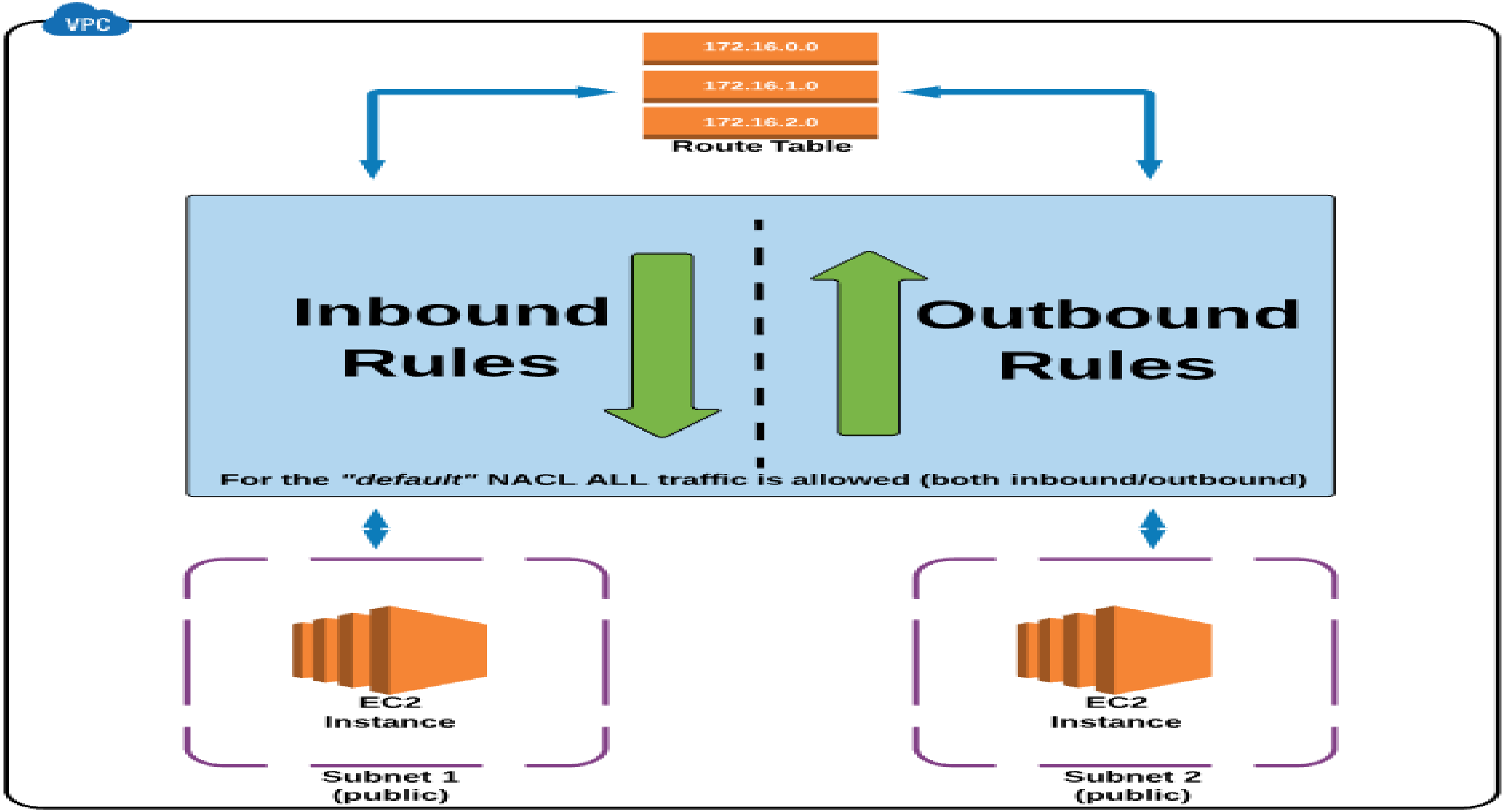
Simplified Definition:
The AWS definition is simple enough, so let's jump right down to it!

AWS Definition:
A network access control list (NACL) is an ***optional layer of security*** for your VPC that acts as a ***firewall*** for controlling traffic in and out of one or more ***subnets***.

NOTE: Your "default" VPC already has a NACL in place and associated with the default subnets.

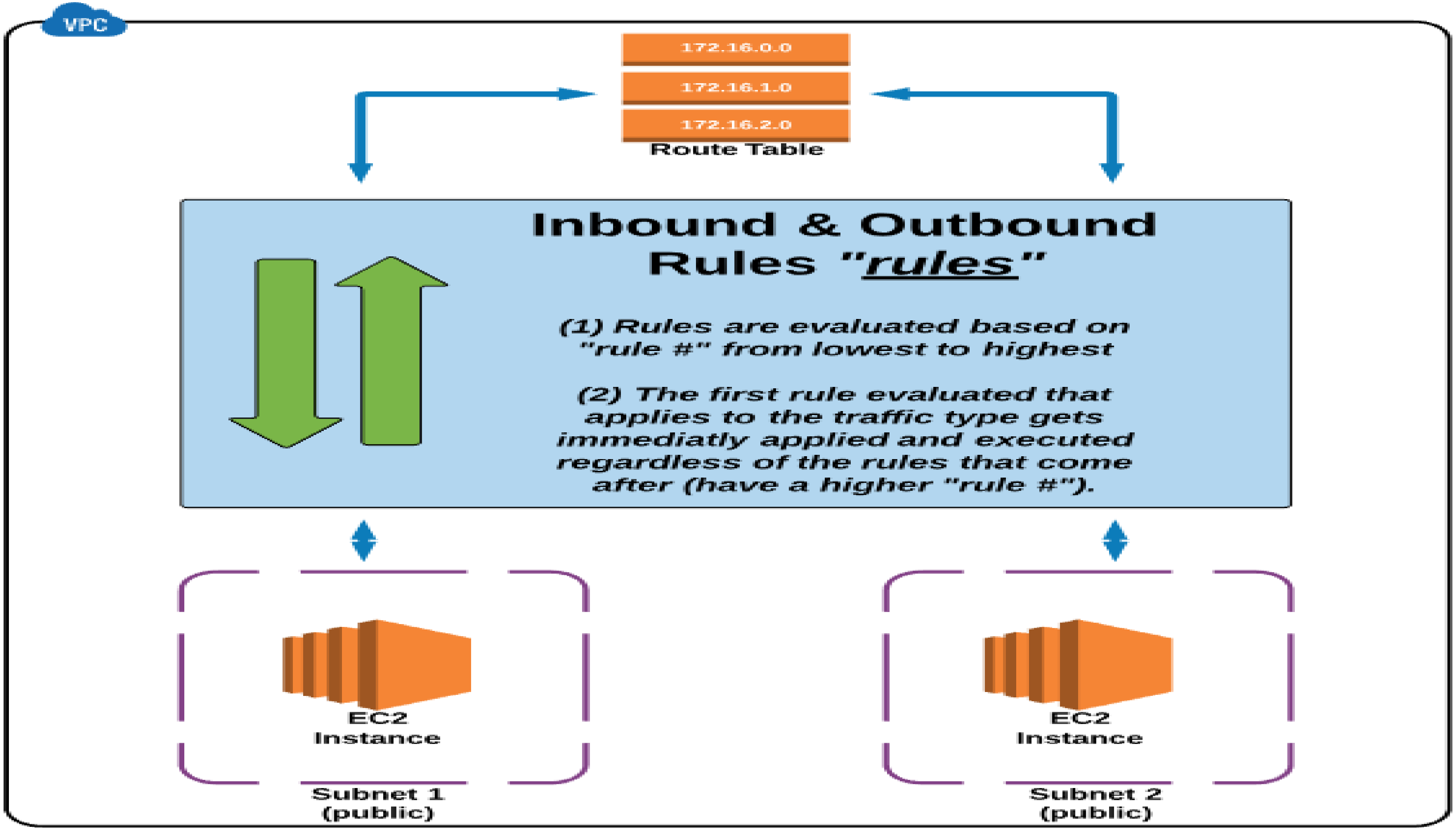
Network Access Control List (NACL)

NACLs:



VPC
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Inbound Rules
Outbound Rules
For the *"default"* NACL ALL traffic is allowed (both inbound/outbound)
EC2 Instance
Subnet 1 (public)
EC2 Instance
Subnet 2 (public)

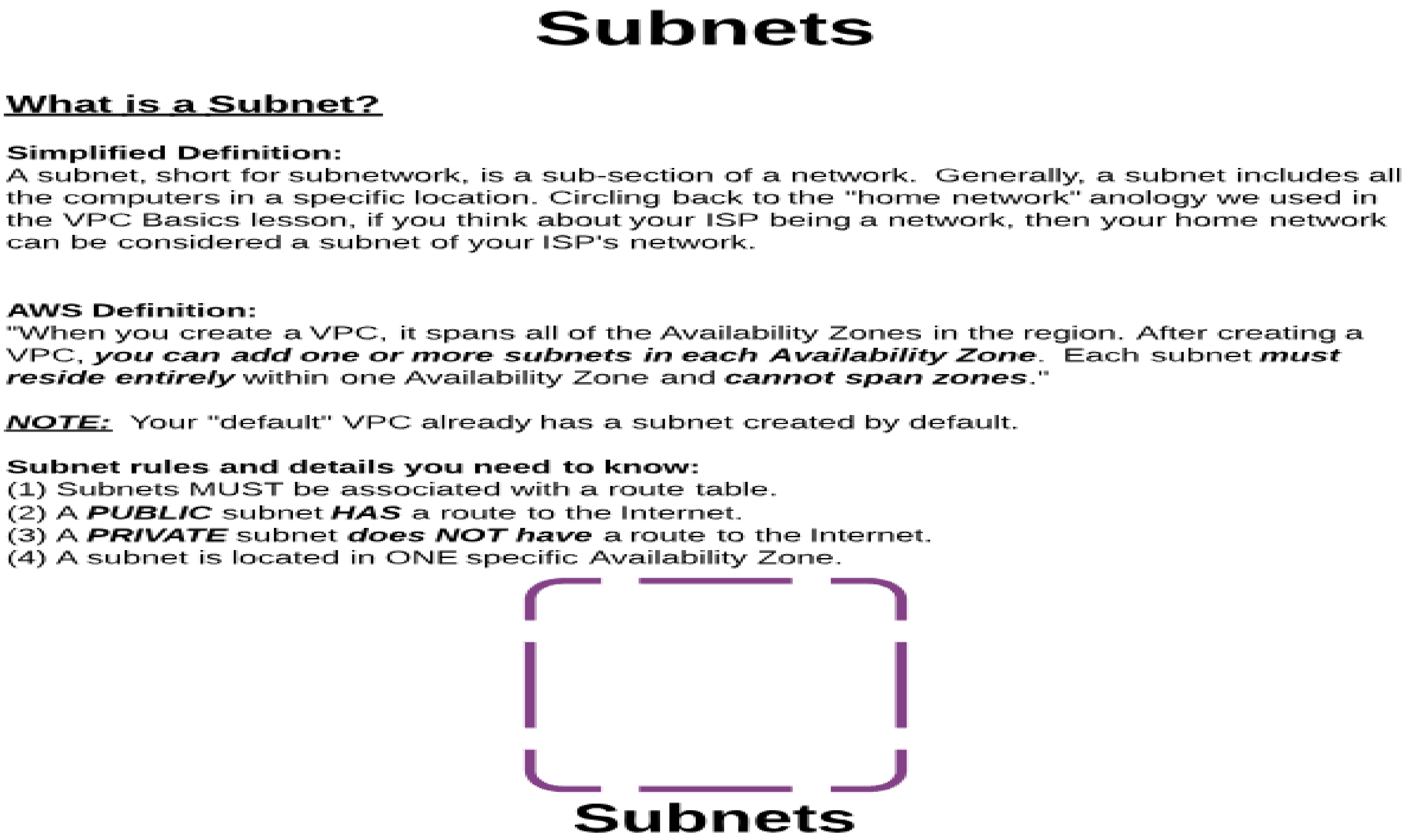
NACLs:



Inbound & Outbound Rules "*rules*"

(1) Rules are evaluated based on "rule #" from lowest to highest

(2) The first rule evaluated that applies to the traffic type gets immediatly applied and executed regardless of the rules that come after (have a higher "rule #").



Subnets

What is a Subnet?

Simplified Definition:
A subnet, short for subnetwork, is a sub-section of a network. Generally, a subnet includes all the computers in a specific location. Circling back to the "home network" anology we used in the VPC Basics lesson, if you think about your ISP being a network, then your home network can be considered a subnet of your ISP's network.

AWS Definition:
"When you create a VPC, it spans all of the Availability Zones in the region. After creating a VPC, ***you can add one or more subnets in each Availability Zone***. Each subnet ***must reside entirely*** within one Availability Zone and ***cannot span zones***."

NOTE: Your "default" VPC already has a subnet created by default.

Subnet rules and details you need to know:
(1) Subnets MUST be associated with a route table.
(2) A ***PUBLIC*** subnet ***HAS*** a route to the Internet.
(3) A ***PRIVATE*** subnet ***does NOT have*** a route to the Internet.
(4) A subnet is located in ONE specific Availability Zone.

Subnets

Security Groups

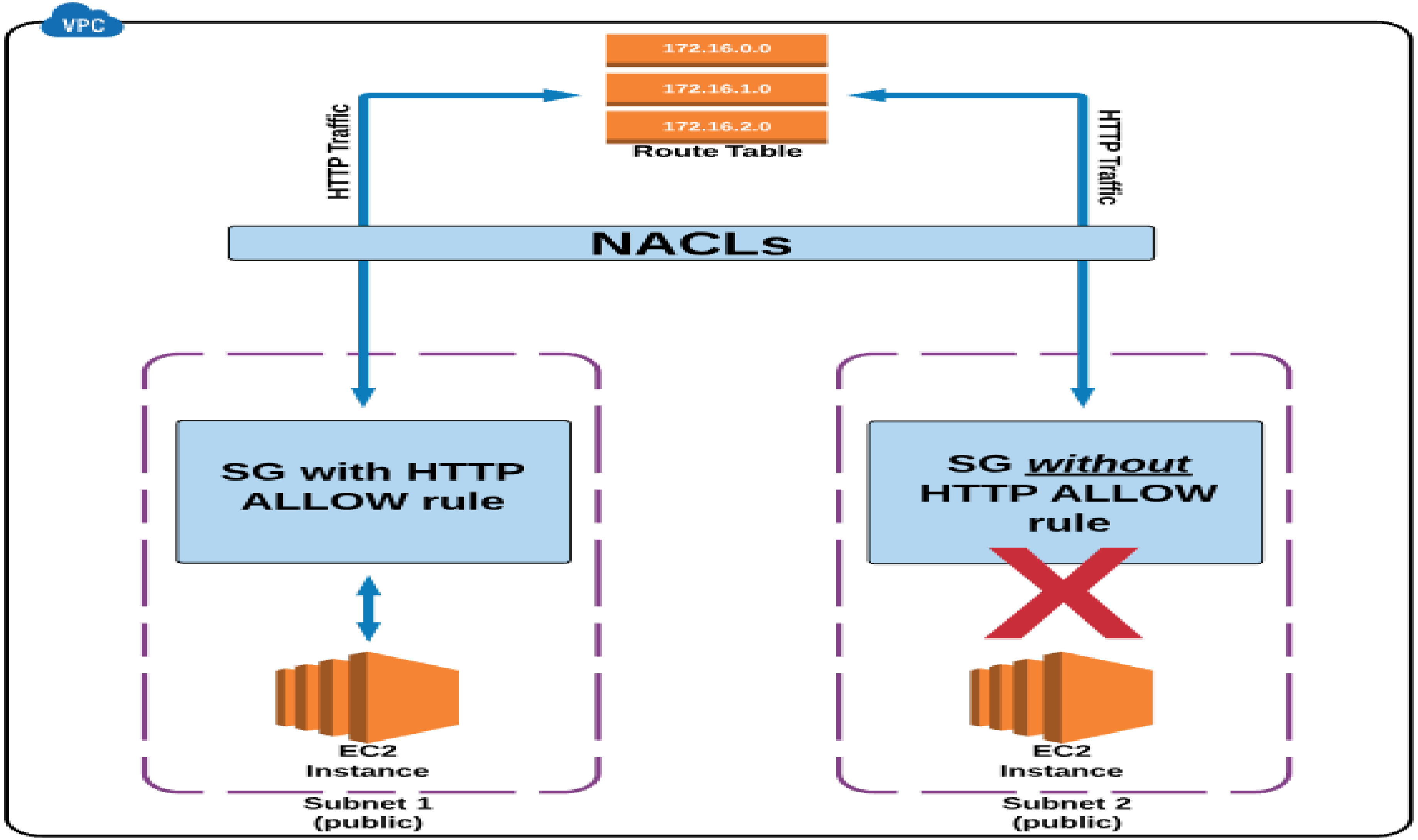
What are Security Groups?

Simplified Definition:
Security groups are very similar to NACLs in that they ***allow/deny traffic***. However, security groups are found on the ***instance level*** (as opposed to the subnet Level). In addition, the way ***allow/deny "rules" are work are differnt from NACL***.

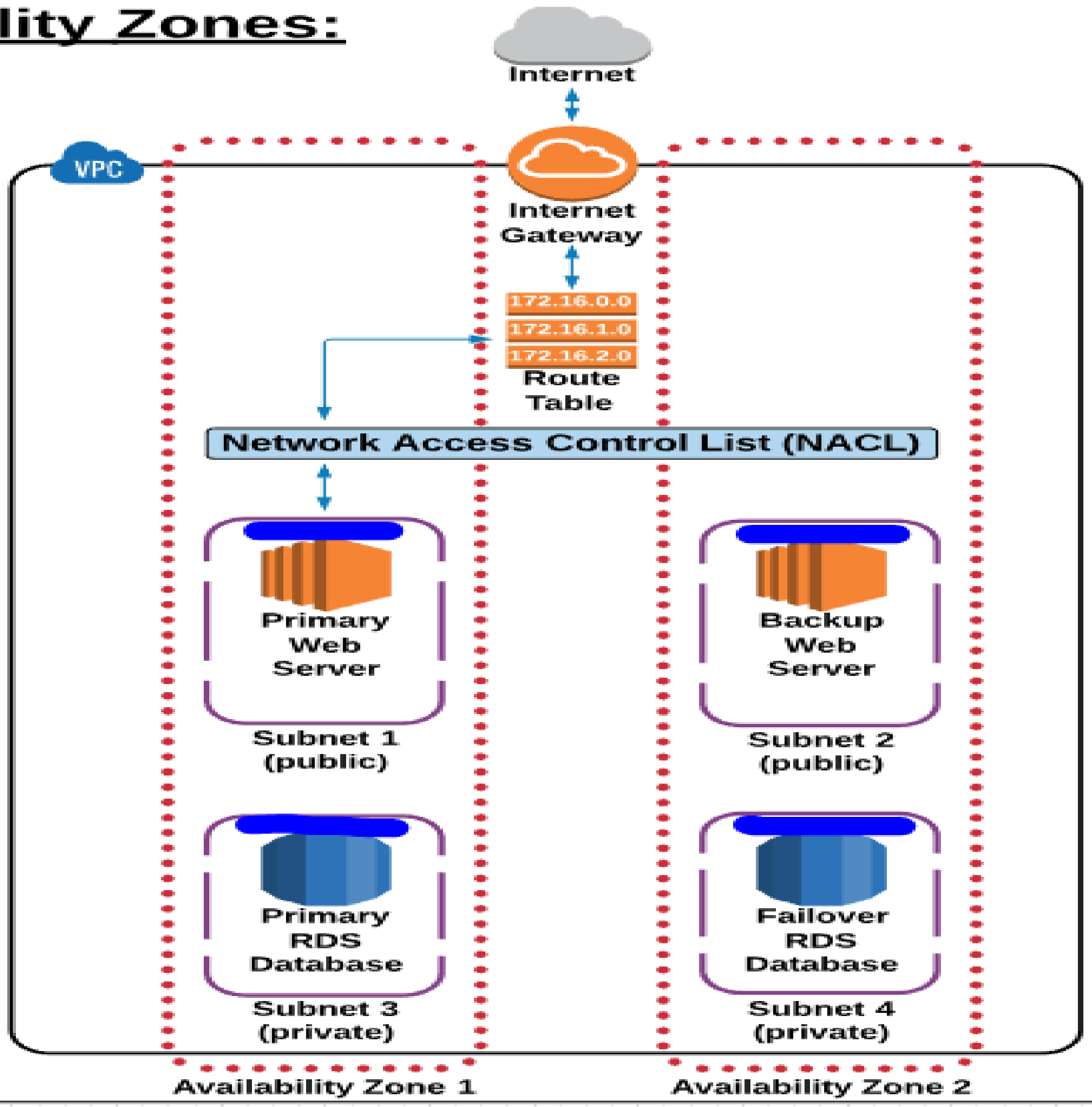
AWS Definition:
"A *security group* acts as a ***virtual firewall that controls the traffic for one or more instances***. When you ***launch an instance, you associate one or more security groups with the instance***. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance."

NOTE: Best practice is to allow ONLY traffic that is required.

Security Groups:



Availability Zones:



▬

Blue line represent Security Group