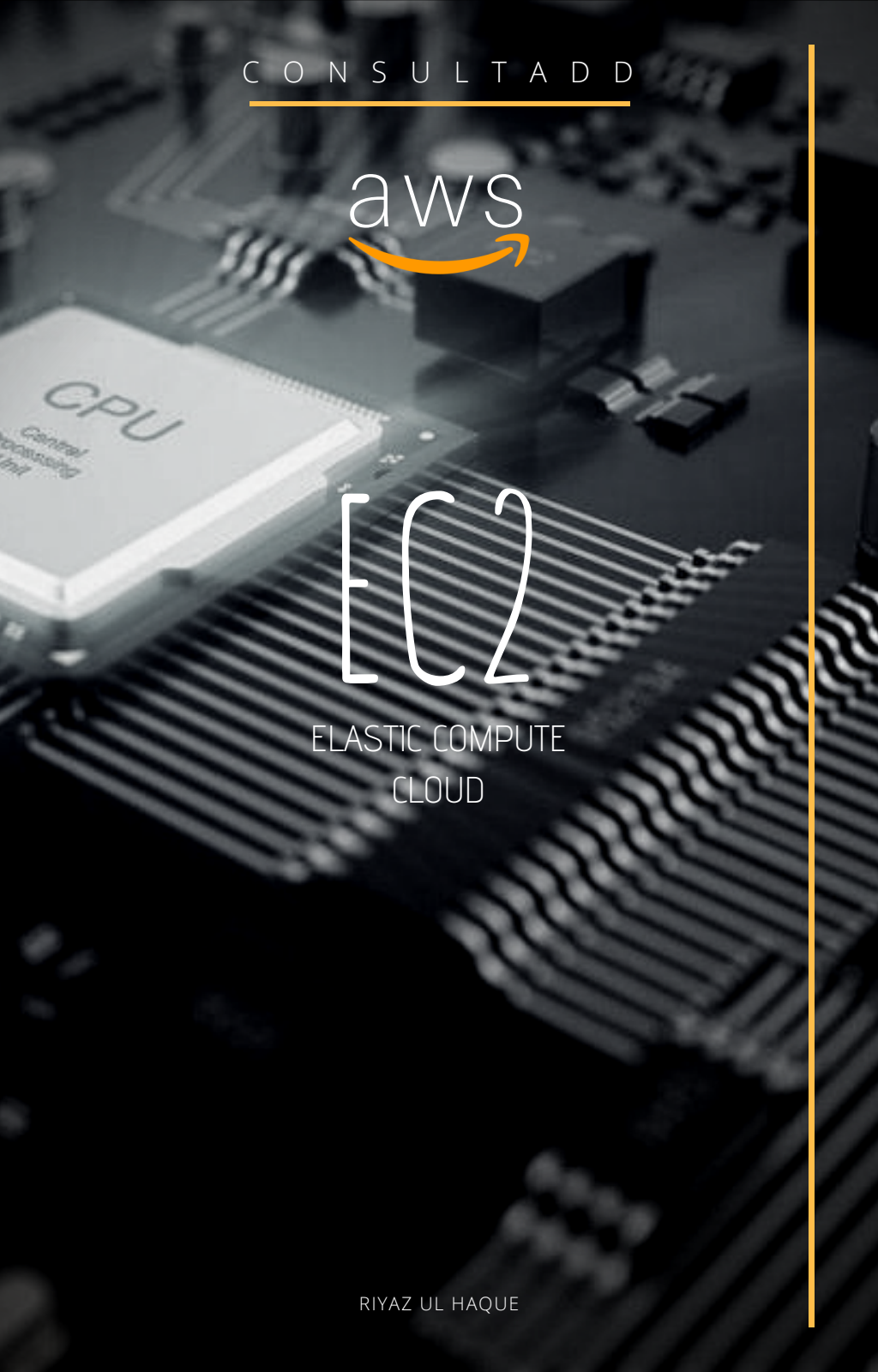

CONSULTADD
aws
EC2
ELASTIC COMPUTE
CLOUD
RIYAZ UL HAQUE

TABLE OF CONTENTS

INTRODUCTION TO AMAZON EC2

Amazon Elastic Compute Cloud is a web service that provides resizable compute capacity in the cloud. Moreover, It allows businesses to run application programs in the Amazon Web Services (AWS) public cloud. Amazon EC2 allows a developer to spin up virtual machines (VM), which provide compute capacity for IT projects and cloud workloads that run with global AWS data centers

With Amazon EC2:

- You can eliminates your need to invest in hardware up front.
- You can develop and deploy applications faster.
- You can launch as many or as few virtual servers as you need.
- You can configure security and networking.
- You can manage storage.

Referenced : www.coggle.it

FEATURES OF EC2

Amazon EC2 provides the following features:

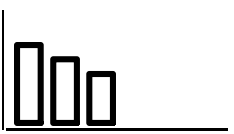
- Virtual computing environments, known as instances.
- Preconfigured templates for your instances, known as Amazon Machine Images (AMIs).
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as instance types.
- Secure login information for your instances using key pairs.
- Storage volumes for temporary data that are deleted when you stop or terminate your instance, known as instance store volumes.
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as Amazon EBS volumes.
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as regions and Availability Zones.
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups.
- Static IPv4 addresses for dynamic cloud computing, known as Elastic IP addresses.
- Metadata, known as tags, that you can create and assign to your Amazon EC2 resources.
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud and that you can optionally connect to your own network, known as virtual private clouds (VPCs).

BENEFITS OF EC2

- Elastic Web-Scale Computing
- Completely Controlled
- Flexible
- Integrated
- Easy to start
- Reliable
- Inexpensive
- Secure

EC2 OPTIONS

Amazon EC2 provides the following purchasing options to enable you to optimize your costs based on your needs:

ON-DEMAND	RESERVED	SPOT	DEDICATED
Pay, by the second for the instances that you launch.	Purchase, at a significant discount, instances that are always available, for a term from one to three years.	Request unused EC2 instances, which can lower your Amazon EC2 costs significantly	Pay, by the hour, for instances that run on single-tenant hardware.
For spiky workloads or to define needs	RIs provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. Pricing is calculated using three key variables - Instance attributes - Term commitment - Payment options	• Reduce costs • Pause & Resume • Familiar Interface • Scale your application • Integrated anywhere	Dedicated instances may share hardware with other instances from the same AWS account that are not Dedicated instances. You can also use Dedicated Hosts to launch Amazon EC2 instances on physical servers that are dedicated for your use.
			

GETTING STARTED WITH EC2

Getting started with Amazon EC2 is easy. Use the AWS Management Console, a point-and-click web-based interface.

Set up and log into your AWS account

Step 2

Launch an Amazon EC2 instance

Step 3

Configure your instance (Choose an Amazon Machine Image (AMI), Choose an instance type, Security group, Launch instance, and Create a key pair)

Step 4

Connect to your instance

Step 5

Terminate instances

NOTE: There are several ways to get started with Amazon EC2. Other than the AWS Management Console you can also use the AWS Command Line Tools (CLI), or AWS SDKs.

YOUR FIRST INSTANCE

To set-up your very first EC2 instance follow the following steps

STEP 01

Set up and log into your AWS account

- Log into the AWS Management Console and set up your root account.

Step 2

Launch an Amazon EC2 instance

- In the Amazon EC2 Dashboard, choose "Launch Instance" to create and configure your virtual machine.

Step 3

Configure your instance

- Choose an Amazon Machine Image (AMI): Choose the Amazon Linux AMI (free-tier eligible).
- Choose an instance type: Choose instance the t2.micro (free-tier eligible).
- Security group: Configure your virtual firewall.
- Launch an instance: Review your instance configuration and choose "Launch".
- Create a key pair: Select "Create a new key pair" and assign a name. The key pair file (.pem) will download automatically - save this in a safe place as we will later use this file to log in to the instance. Finally, choose "Launch Instances" to complete the setup.
- Note: It may take a few minutes to initialize your instance.

Step 4

Connect to your instance

- Select the EC2 instance you created and choose "Connect".
- Select "A Java SSH client directly from my browser". Ensure Java is installed and enabled.
- Enter the Private key path (example: C:\KeyPairs\my-key-pair.pem).
- Choose "Launch SSH Client".
- Note: You can also connect via SSH or PuTTY,

Step 5

Terminate instances

- Amazon EC2 is free to start but you should terminate your instances to prevent additional charges. The EC2 instance and the data associated will be deleted.
- Select the EC2 instance, choose "Actions", select "Instance State", and "Terminate".

EC2 RESOURCES AND TAGS

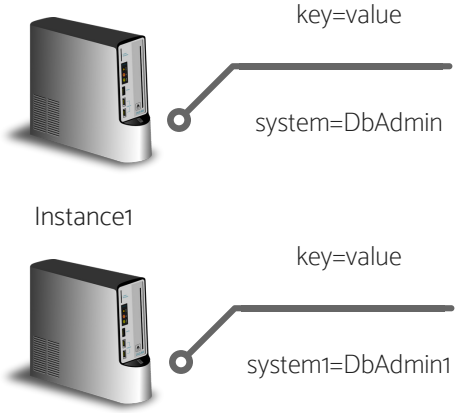
AWS allows you to manage your instances, images, and other Amazon EC2 resources, you can optionally assign your own metadata to each resource in the form of tags.

A tag can be treated as a label that you assign to an AWS resource. Each tag consists of a key and an optional value.

Using tags you to categorize your AWS resources in multiple:

- By purpose
- By Owner
- By environment

You can work with tags using the AWS Management Console, the AWS CLI, and the Amazon EC2 API.



In this example, you've assigned two tags to each of your instances–one tag with the key system and another with the key system1 Each tag also has an associated value.

KEY POINTS :

- Tags don't have any semantic meaning to Amazon EC2 and are interpreted strictly as a string of characters.
- Tags are not automatically assigned to your resource.
- You can edit tag keys and values, and you can remove tags from a resource at any time.
- If you add a tag that has the same key as an existing tag on that resource, the new value overwrites the old value. If you delete a resource, any tags for the resource are also deleted.

TAGS RESTRICTION

- Maximum number of tags per resource – 50
- For each resource, each tag key must be unique, and each tag key can have only one value.
- Maximum key length – 128 Unicode characters in UTF-8
- Maximum value length – 256 Unicode characters in UTF-8
- If your tagging schema is used across multiple services and resources, remember that other services may have restrictions on allowed characters.
- Generally allowed characters are: letters, numbers, and spaces representable in UTF-8, and the following characters: + - = . _ : / @.
- Tag keys and values are case-sensitive.
- Don't use the aws: prefix for either keys or values; it's reserved for AWS use. You can't edit or delete tag keys or values with this prefix. Tags with this prefix do not count against your tags per resource limit.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

TYPES OF INSTANCE

Specifying the instance type determines the hardware of the host computer used for your instance.
Each instance type offers different compute power, memory, and storage capabilities and accordingly they have categories into different families of instances.

Amazon EC2 provides the instance types listed in the following tables

Instance Family	Current Generation Instance Types
General purpose	t2.nano | t2.micro | t2.small | t2.medium | t2.large | t2.xlarge | t2.2xlarge | m4.large | m4.xlarge | m4.2xlarge | m4.4xlarge | m4.10xlarge | m4.16xlarge | m5.large | m5.xlarge | m5.2xlarge | m5.4xlarge | m5.12xlarge | m5.24xlarge | m5d.large | m5d.xlarge | m5d.2xlarge | m5d.4xlarge | m5d.12xlarge | m5d.24xlarge
Compute optimized	c4.large | c4.xlarge | c4.2xlarge | c4.4xlarge | c4.8xlarge | c5.large | c5.xlarge | c5.2xlarge | c5.4xlarge | c5.9xlarge | c5.18xlarge | c5d.xlarge | c5d.2xlarge | c5d.4xlarge | c5d.9xlarge | c5d.18xlarge
Memory optimized	r4.large | r4.xlarge | r4.2xlarge | r4.4xlarge | r4.8xlarge | r4.16xlarge | x1.16xlarge | x1.32xlarge | x1e.xlarge | x1e.2xlarge | x1e.4xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge
Storage optimized	d2.xlarge | d2.2xlarge | d2.4xlarge | d2.8xlarge | h1.2xlarge | h1.4xlarge | h1.8xlarge | h1.16xlarge | i3.large | i3.xlarge | i3.2xlarge | i3.4xlarge | i3.8xlarge | i3.16xlarge | i3.metal
Accelerated computing	f1.2xlarge | f1.16xlarge | g3.4xlarge | g3.8xlarge | g3.16xlarge | p2.xlarge | p2.8xlarge | p2.16xlarge | p3.2xlarge | p3.8xlarge | p3.16xlarge

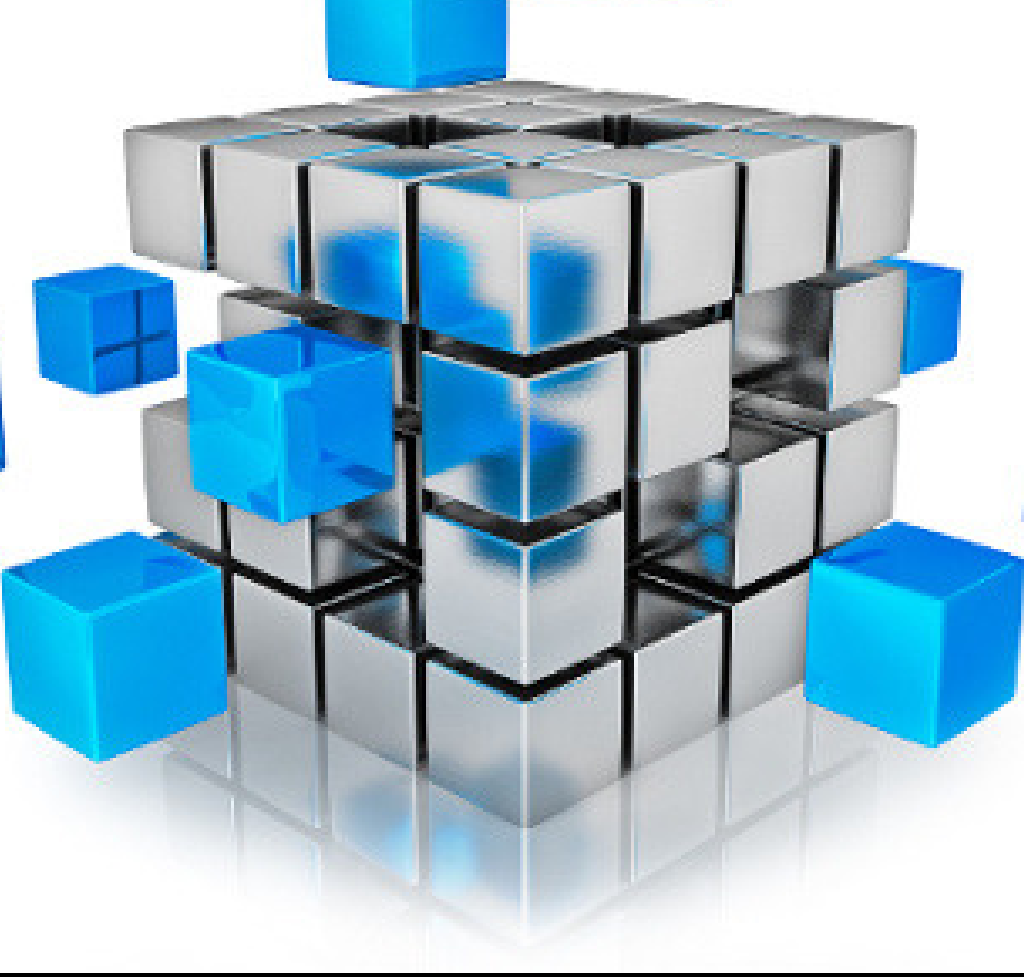
Current Generation Instances

Amazon EC2 provides each instance with a consistent and predictable amount of CPU capacity, regardless of its underlying hardware.

There is a limit on the total number of instances that you can launch in a region, and there are additional limits on some instance types.

- The total 20 On-Demand instances across the instance family.
- Purchasing 20 Reserved Instances
- Requesting Spot Instances per your dynamic Spot limit per region.

To check Certain instance types with their further limits per region- https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2



E LASTIC
B LOCK
S TORAGE

aws

WHAT IS EBS?

Amazon Elastic Block Store also known as EBS provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.

- It is tightly integrated with Amazon EC2 instances.
- It provides high performance and low latency.
- It also provides five nines of availability.

With Amazon EBS, you can scale your usage up or down within minutes – all while paying a low price for only what you provision.

The current generation of Amazon EBS volumes offers four different types of volumes, each with a unique pair of characteristics to meet different needs of your workloads.

Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability.

The following table describes the use cases and performance characteristics for each volume type

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads

Use Cases	• Recommended for most workloads
	• System boot volumes
	• Virtual desktops
	• Low-latency interactive apps
	• Development and test environments
		• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume
		• Large database workloads, such as:
		  ◦ MongoDB
		  ◦ Cassandra
		  ◦ Microsoft SQL Server
		  ◦ MySQL
		  ◦ PostgreSQL
		  ◦ Oracle
			• Streaming workloads requiring consistent, fast throughput at a low price
			• Big data
			• Data warehouses
			• Log processing
			• Cannot be a boot volume
				• Throughput-oriented storage for large volumes of data that is infrequently accessed
				• Scenarios where the lowest storage cost is important
				• Cannot be a boot volume

API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	10,000	32,000***	500	250
Max. Throughput/Volume	160 MiB/s	500 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instance	80,000	80,000	80,000	80,000
Max. Throughput/Instance††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

FEATURES

As being the persistent block storage for Amazon EC2, It provides delivering capabilities and performance for the most demanding applications which includes the following:

High Performance Volumes

Choose between SSD-backed or HDD-backed volumes that can deliver the performance you need for your most demanding applications.

Availability

Each Amazon EBS volume is designed for 99.999% availability and automatically replicates within its Availability Zone to protect your applications from component failure.

Encryption

Amazon EBS encryption provides seamless support for data-at-rest and data-in-transit between EC2 instances and EBS volumes.

Access Management

Amazon's flexible access control policies allow you to specify who can access which EBS volumes ensuring secure access to your data.

Snapshots

Protect your data by creating point-in-time snapshots of EBS volumes, which are backed up to Amazon S3 for long-term durability.

Elastic Volumes

Dynamically increase capacity, tune performance, and change the type of live EBS volumes.

BENEFITS

Instead of just being highly available, excellent at performance, persistent block storage for Amazon EC2 , Amazon EBS provides following benefits as well

Consistent, Low-latency Performance

Each Amazon EBS volume provides redundancies within its Availability Zone to protect against failures. Encryption and access control policies deliver a strong defense-in-depth security strategy for your data.

Reliable, Secure Storage

Amazon EBS General Purpose (SSD) volumes and Amazon EBS Provisioned IOPS (SSD) volumes deliver low-latency through SSD technology and consistent I/O performance scaled to the needs of your application.

Backup, Restore, Innovate

Protect your data by taking point-in-time snapshots of your Amazon EBS volumes providing long-term durability for your data. Boost the agility of your business by using Amazon EBS snapshots to create new EC2 instances.

Quickly Scale Up, Easily Scale Down

Amazon EBS allows you to optimize your volumes for capacity, performance, or cost giving you the ability to dynamically adapt to the changing needs of your business.

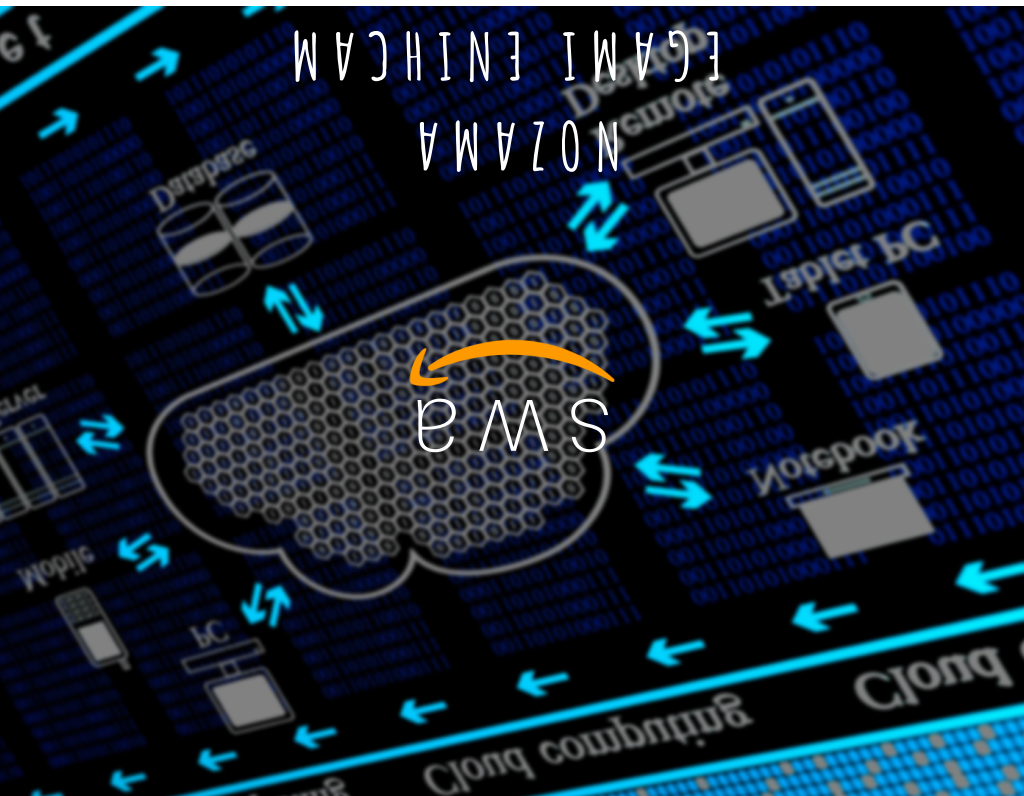
Geographic Flexibility

Amazon EBS provides the ability to copy snapshots across AWS regions, enabling geographical expansion, data center migration, and disaster recovery providing flexibility and protecting for your business.

Optimized Performance

An Amazon EBS–optimized instance provides dedicated network capacity for Amazon EBS volumes. This provides the best performance for your EBS volumes by minimizing network contention between EBS and your instance.


Cloud computing
PC
Mobile
Notebook
aws
Tablet PC
Database
Desktop
AMAZON MACHINE
IMAGE


AMAZON
IMAGE MACHINE
aws

WHAT IS AN AMI ?

Pre-configured packages required to launch an EC2 instance, including operating system, software packages, and other required settings.

An Amazon Machine Image (AMI) is a master image for the creation of virtual servers (known as EC2 instances) in the Amazon Web Services (AWS) environment.

AWS | An Amazon Machine Image (AMI) provides the information to launch an instance, which is a virtual server in the cloud. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need.
All you need is the EC2 things to be getting developed.

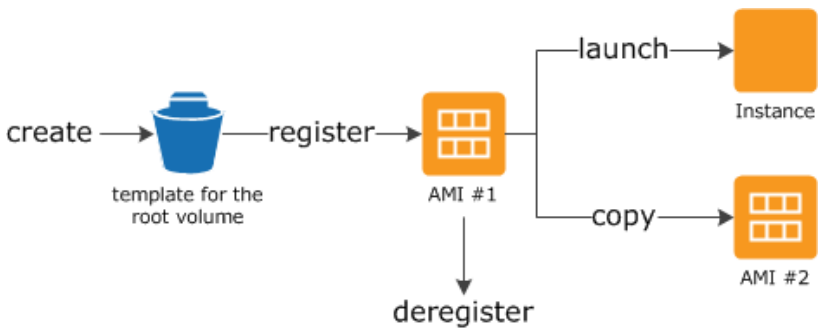
Conceptually AMI includes:

- A template for the root volume for the instance.
- Launch permissions.
- Block device mapping.

HOW TO USE AN AMI ?

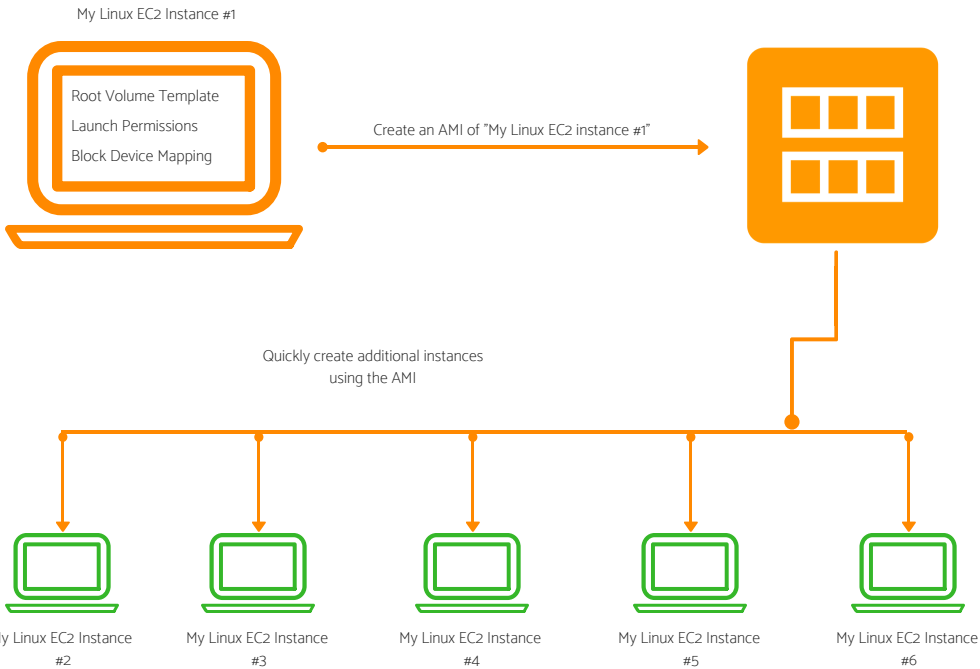
Using an AMI involves:

- Create
- Register
- Launch



CREATE YOUR OWN AMI

When you create an AMI, you are essentially creating a template that you can use to launch another EC2 instance that has the exact same components as the original instance.



When you launch an EC2 instance, the first thing you do is select an AMI

Selecting an AMI:

AMIs comes in three main categories:

1- Community AMIs:

Free to use.

Generally, with these AMIs you are just selecting the OS you want.

2- AWS Marketplace AMIs:

Pay to use.

Generally comes packaged with additional, licensed software.

3- My AMIs:

AMIs that you create yourself

AMI WITH ENCRYPTED SNAPSHOTS

AMIs that are backed by Amazon EBS snapshots can take advantage of Amazon EBS encryption. Snapshots of both data and root volumes can be encrypted and attached to an AMI.

Note that EC2 instances with encrypted volumes are launched from AMIs in the same way as other instances.

Snapshots can be encrypted with either your default AWS Key Management Service customer master key(CMK), or with a custom key that you specify.

- Must have permission to use the selected key.
- CopyImage action accepts only one key at a time and encrypts all of an image's snapshots(whether root or data) to that key.
- It is possible to manually build an AMI with snapshots encrypted to multiple keys.

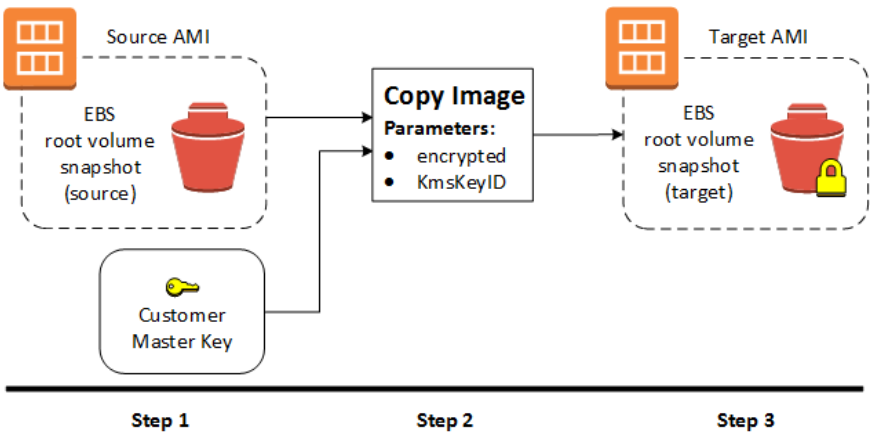
The CopyImage action can be used to create an AMI with encrypted snapshots from an AMI with unencrypted snapshots. By default, CopyImage preserves the encryption status of source snapshots when creating destination copies. However, you can configure the parameters of the copy process to also encrypt the destination snapshots.

AMI SCENARIOS INVOLVING ENCRYPTED EBS SNAPSHOTS

- AMI Scenarios Involving Encrypted EBS Snapshots.
- Copying an AMI Backed by An Encrypted Root Snapshot.
- Creating an AMI with Encrypted Root Snapshot from an Unencrypted AMI.
- Creating an AMI with an Encrypted Root Snapshot from a Running Instance.
- Creating an AMI with Unique CMKs for Each Encrypted Snapshot.

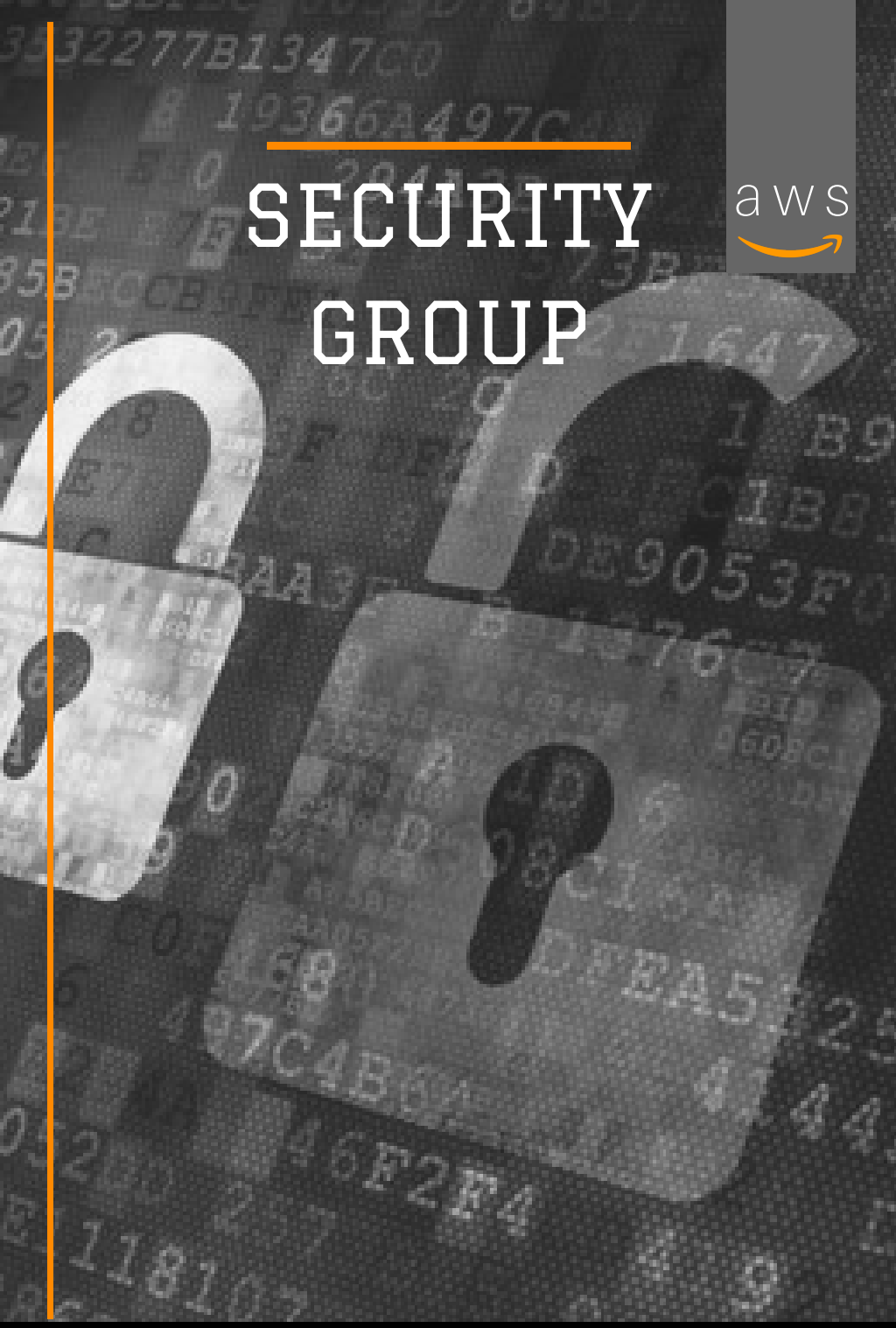
CREATING AN AMI WITH ENCRYPTED ROOT SNAPSHOT FROM AN UNENCRYPTED AMI

In this scenario, an Amazon EBS-backed AMI has an unencrypted root snapshot, shown in step 1, and an AMI is created with an encrypted root snapshot, shown in step 3.



The CopyImage action in step 2 is invoked with two encryption parameters, including the choice of a CMK. As a result, the encryption status of the root snapshot changes, so that the target AMI is backed by a root snapshot containing the same data as the source snapshot, but encrypted using the specified key. You will incur storage costs for the snapshots in both AMIs, as well as charges for any instances you launch from either AMI.

SECURITY GROUP



BASICS OF SECURITY GROUPS

In order to control the traffic for one or more instances we use security groups which acts as a firewall

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 after a short period.

AWS provides several security capabilities and services to increase privacy and control network access.

SECURITY GROUPS RULES

The actual rule set that filters traffic is made up of two tables:

- Inbound
- Outbound

AWS Security groups are stateful, meaning you do not need the same rules for both outbound traffic and inbound. Therefore any rule that allows traffic into an EC2 instance, will allow responses to pass back out without an explicit rule in the Outbound rule set.

Each security rule is comprised of four fields:

- Type
- Protocol
- Port Range
- Source

Type.: The drop-down list allows you to select common protocols like SSH, RDP, or HTTP. You can also choose custom protocols.
Protocol: This is typically greyed out, as it's covered by most 'Type' choices. However, if you create a custom rule, you can specify your protocol (TCP/UDP etc.) here.
Port Range: This value will also usually be pre-filled, reflecting the default port or port range for your chosen protocol. However, there might be times when you prefer to use custom ports.
Source: This can be a Network Subnet range, a specific IP address, or another AWS security group. You can also leave access open to the entire Internet using the 'Anywhere (0.0.0.0/0)' value.

DEFAULT & CUSTOM SECURITY GROUP

Your VPC automatically comes with a default security group. Each EC2 instance that you launch in your VPC is automatically associated with the default security group if you don't specify a different security group when you launch the instance.

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

- You can change the rules for the default security group.
- You can't delete a default security group. If you try to delete the default security group, you'll get the following error: Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user.

Although you can use the default security group for your instances, you might want to create your own groups to reflect the different roles that instances play in your system.

- Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
- In the navigation pane, choose Security Groups
- Choose to Create Security Group.
- Enter a name of the security group (for example, my-security-group) and provide a description. Select the ID of your VPC from the VPC menu and choose Yes, Create.


THANK YOU
RIYAZ UL HAQUE
CONSULTADD