

One of EC2

Most popular AWS offering.

EC2 = Elastic Compute Cloud = IaaS.

- 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)

→ EC2 sizing & configuration options:

Operating systems: Linux / windows / MacOS

CPU - Compute power

RAM - Memory

Storage space

Network attached (EBS & EFS)

Hardware (EC2 instance group)

Network card: Speed of the card, public IP address

Firewall rules: Security group

Bootstrap config: script: EC2 user data.

Bootstrapping means launching commands when a machine starts.

→ EC2 Instance types: Overview

cg:

m5.2xlarge

m = Instance class

5 = Generation

2xlarge = size within the instance class.

1)

General Purpose:

Great for a diversity of workloads - web servers or code repos.

-

Balance between: Compute, Memory, Networking

-

t2.micro → General purpose EC2.

Compute optimized:
Great for compute-intensive tasks that require high performance processors:
Batch processing workloads
Media transcoding
High performance web servers
High performance computing
Scientific modeling & machine learning
Dedicated game servers.

Memory optimized:
Fast performance for workloads that process large data sets in memory.

Use cases:

High performance, relational / non-relational DB.
Distributed web scale cache stores
In-memory databases optimized for BI
Applying performing real-time processing for big unstructured data

Storage optimized:

Great for storage intensive tasks that require high, sequential read and write access to large data sets on local storage.

Use cases:

High frequency online transaction processing (OLTP) systems.

Relational & NoSQL DB

Cache for in-memory DB (e.g.: Redis)

Data warehousing applns.

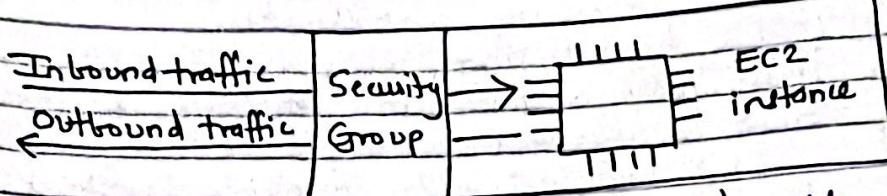
Distributed file systems.

Introduction to Security Group.

They control how traffic is allowed into or out of our EC2 instances.

Contain allow rules
SG rules can reference by IP or by SG

www



Acting as "firewall" on EC2 instances.

They regulate:

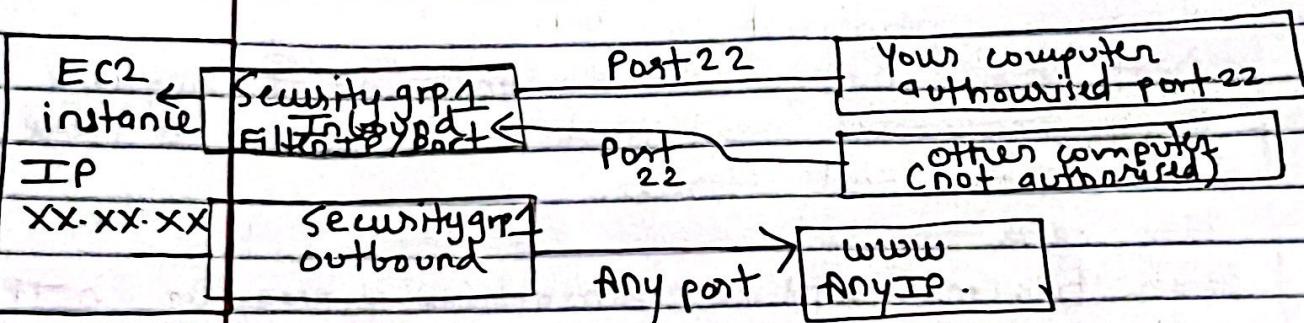
Access to ports

Authorized IP ranges - IPv4 and IPv6

Control of inbound network

Control of outbound network

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	test http page
SSH	TCP	22	122.149.196.25/32	
Custom TCP Rule	TCP	4567	0.0.0.0/0	java app



* Security Group Imp Points *

Can be attached to multiple instances

Locked down to a region / VPC combination

Live "outside" EC2.

Good to maintain one separate SG for SSH access.

5) App^{lu} not accessible (time out) - SG issue.

App^{lu} gives "connection refused" - App^{lu} error.

7) All inbound traffic blocked by default

8) All outbound traffic authorized by default.

Classic Ports:

22 = SSH (Secure Shell) - Log into a Linux instance

21 = FTP (File Transfer Protocol) - Upload files into a file share

22 = SFTP (Secure File Transfer Protocol) - Upload files using SSH.

80 = HTTP - Access unsecured websites

443 = HTTPS - Access secured websites

3389 = RDP (Remote Desktop Protocol) - Log into a Windows instance.

SSH:

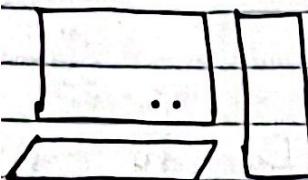
SSH



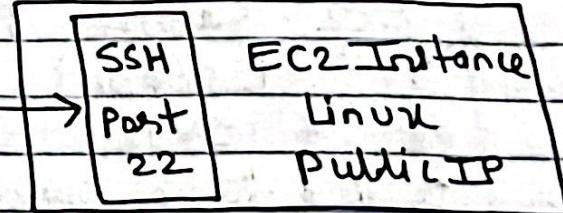
Putty



EC2 Instance connect



www



EC2 Instance Purchasing Options:

On demand - Short workload, predictable pricing, pay by second.

Reserved - 1 & 3 yrs, long workloads

Spots Plan: (1 & 3 yrs) Commitment to an amount of usage, long workload.

Spot Instances: Short workloads, cheap, can lose instances.

Dedicated Hosts: Book an entire physical server.

Dedicated Instances: No other customer will share capacity.

Capacity Reservations: Reserve capacity in specific for any duration.

1) EC2

- Pay on Demand:
Linux for what you use
- All other OS / Windows: Billing per second, after first min
- Highest cost, no upfront payment
- No long-term commitment
- Short-term, un-interrupted workload

2)

EC2 Reserved Instances:

- 72% discount compared to on-demand.
- Reserve: Instance Type, Region, OS, Tenancy
- Period: 1 or 3 yrs
- Payment Options: No / Partial / full Upfront
- Regional or Zonal Reserved instance scope
- Steady-state usage applies
- Buy & sell

Convertible Reserved Instance (66% discount)

3)

EC2 Savings Plan

- 72% discount
- eg: \$10/hr for 1 or 3 yrs
- Locked to a specific instance family & AWS region
- Flexible across: size, OS, Tenancy.

4)

EC2 Spot Instances

- 90% discount compared to on-demand

Max price < Current spot price - Lose

MOST cost efficient

Workloads resilient to failure:

- Batch job
- Data analysis
- Image Processing
- Any distributed workloads
- Workloads with flexible start & end date

Not suitable for critical jobs or databases.

~~Physical Hosts:~~
dedicated server with EC2 instance capacity fully dedicated to your use.

~~Compliance requirements, we your existing server bound software licenses.~~

On-Demand : Pay per sec

Reserved: 1/3 yrs

MOST expensive option

Software that have complicated licensing model

For companies: Strong regulatory / compliance needs.

EC2 Dedicated Instances:

Share h/w with other instances in same account

No control over instance placement

EC2 Capacity Reservations:

On-demand instances, specific AZ

No time commitment

No billing discounts

Short-term, uninterrupted workloads.

Shared Responsibility Model for EC2:

AWS

Infra (Global network security)

Isolation on physical hosts

Replace faulty h/w

Compliance validation.

YOU

SG rules

OS patches & updates

Software & utilities installed on EC2 instance

IAM roles: EC2, User, ^{Object}Management

Data security on your instance.

1)

EC2 Section Summary *

EC2 instance: AMI (os) + Instance size (CPU + RAM) + storage + SG + EC2 user data

2)

SG: Firewall attached to EC2 instance

3)

EC2 user data: Script launched at the first start of an instance.

4)

SSH: Start a terminal into our EC2 instance (port 22)

5)

EC2 instance role: link to IAM roles

6)

Purchasing options: On-demand, Spot, Reserved (Std + Convertible + Scheduled), Dedicated (Host + Instance).

EC2 Instance Storage Section:

EBS Volume

Elastic Block Store: Network drive, attach to instances while they run.

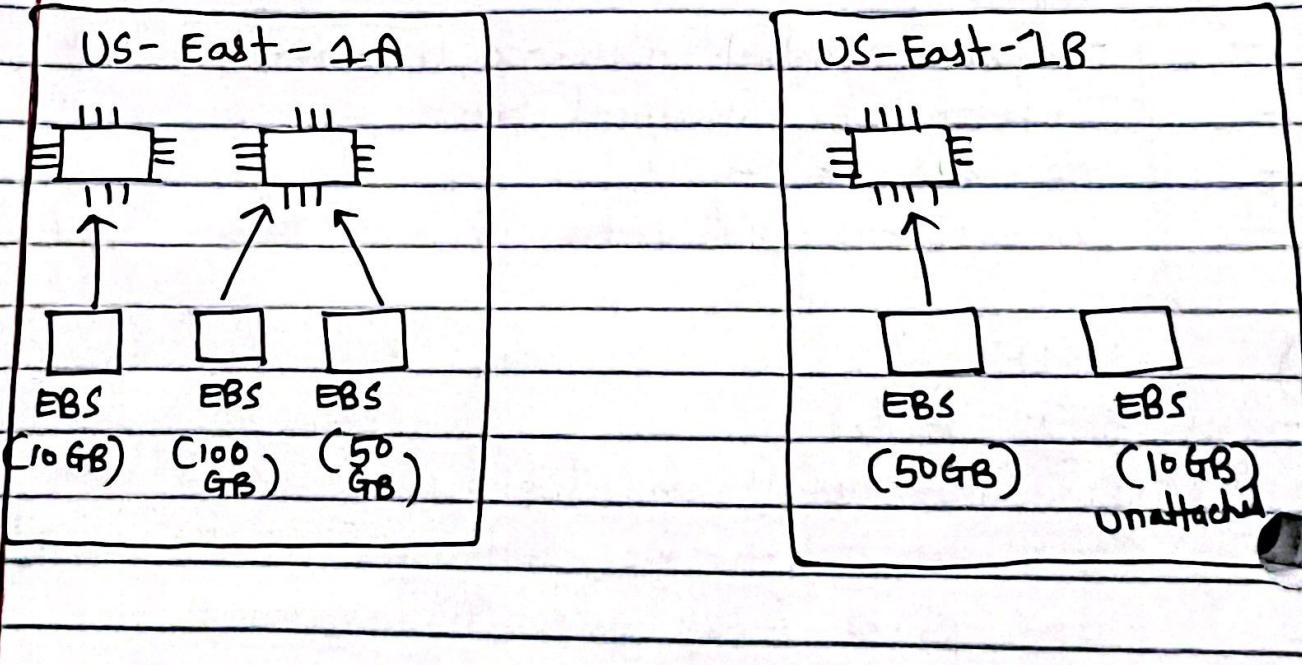
Persist data, even after termination

Only one instance at a time

Bound to a specific AZ.

Provisioned capacity (Billed for all)

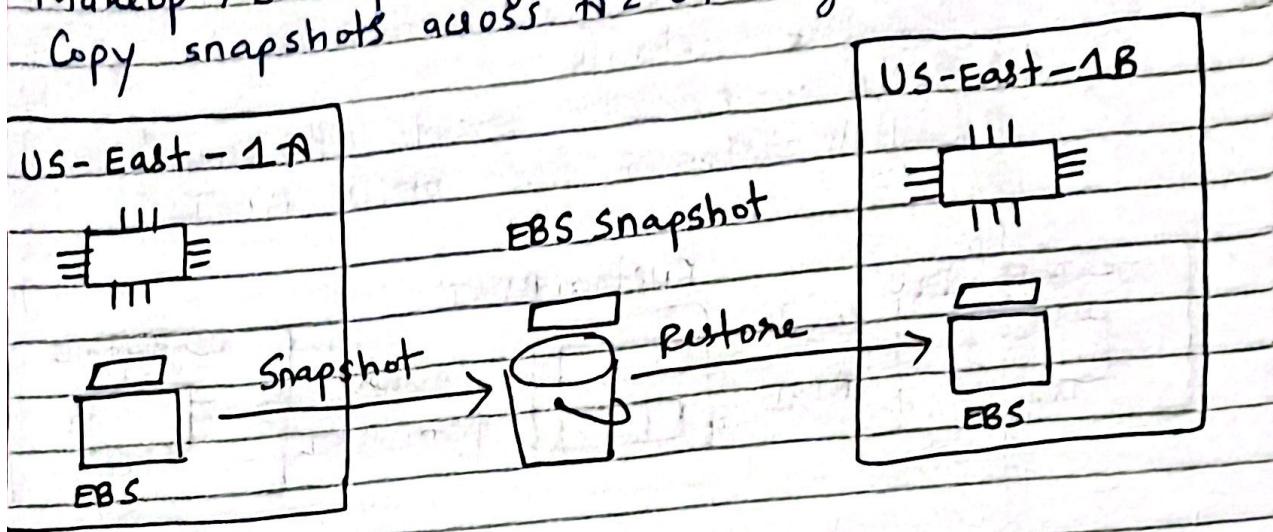
To move volume across, first snapshot it.



EBS - Delete on Termination attribute
By default, root EBS is deleted
Any other attached EBS vol is not deleted

EBS Snapshots.

Backup of your EBS volume
Copy snapshots across AZ or region ✓

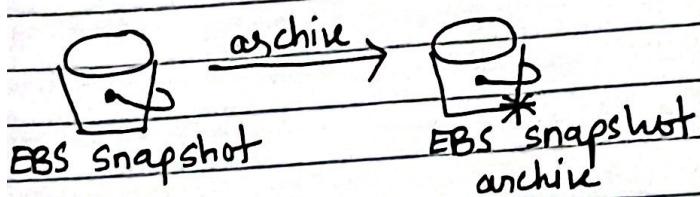


Features:

EBS Snapshot archive:

Archive tier: 75% cheaper

24 to 72 hrs for restoring the archive.



Recycle Bin for EBS snapshots:

Specify Retention (1 day to 1 year)



AMI

AMI = Amazon Machine Image

They are customization of an EC2 instance

Add own SW, OS

Built for specific region (can be copied across regions)

1) Launch EC2 instances from:
Public AMI: AWS provided
Own AMI:
AWS Marketplace AMI

AMI Process

Start an EC2; customize it

Stop the instance

Build an AMI - create EBS snapshots

Launch instances from other AMIs

