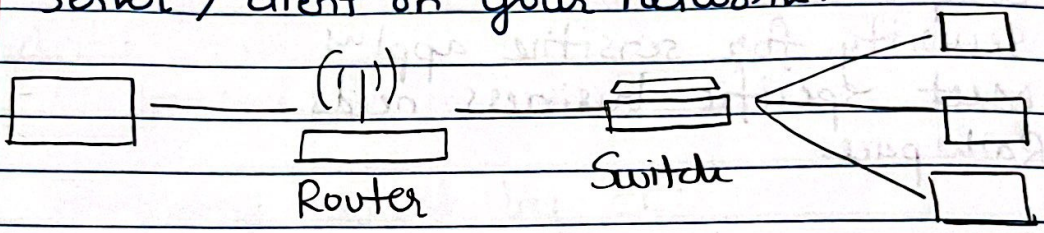
CLF-C01 Notes

Server:
1) Compute: CPU
2) Memory: RAM
3) Storage: Data
4) Database: Store Data in a structured way.
5) Network: Routers, switch, DNS server.

Network: Cables, Routers, Servers connected with each other.

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

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



What is cloud computing?

1) On-Demand delivery of compute power, database storage, appl^ns and other IT resources.
2) Pay-as-you-go pricing
3) Provision exactly the right type and size of computing resources.
4) Access as many resources as you need, almost instantly.
5) Simple way to access servers, storage, databases, set of application services.

Gmail:
E-mail cloud service
Pay for ONLY your emails stored.

Dropbox
Cloud storage service
Originally built on AWS

Netflix
Built on AWS
Video on demand.

The Deployment Models of the cloud.

Private cloud:
Single organization, not exposed to the public
Complete control
Security for sensitive apps
Meet specific business needs.
Rackspace

Public cloud:
Owned and operated by third party
Delivered over the Internet
Six advantages of CC.
AWS, Azure, GCP

Hybrid cloud:
Some servers on premise, some capabilities to the cloud.
Control private assets
Flexibility, cost-effectiveness of the public cloud.
Private cloud + AWS.

Five characteristics of cc:
On-demand self service:
Broad network access
Multi-tenancy & resource pooling
Rapid elasticity & ~~eq~~ scalability
Measured service

Six advantages of cc.

Trade Capital expense (CAPEX) for operational expense (OPEX):
Pay on-demand. Reduce Total cost of ownership (TCO) & Operational Expense (OPEX).
Benefit from massive economies of scale.
Stop guessing capacity
Increase speed & agility
Stop spending money running & maintaining data centers.
Go global in minutes.

Problems solved by cc:
Flexibility
Cost-effectiveness
Scalability
Elasticity
High availability & fault tolerance
Agility.

Types of cc:

Infrastructure as a Service (IaaS):
Building blocks for cloud IT.
Networking, computers, data storage space.
Highest level of flexibility
Easy parallel with traditional on-premises IT.
EC2, GCP, Azure, Rackspace, Digital Ocean, Linode.

2) Platform as a Service (PaaS):
- No underlying infrastructure needed
- Focus on deployment & management of apps.
eg: Elastic Beanstalk, Heroku, Google App Engine, Windows Azure

3) Software as a Service (SaaS):
Completed product that is run and managed by the service providers.
eg: Rekognition, Gmail, Dropbox, Zoom.

On-premise	Iaas	Paas	Saas
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
Managed by you,	Managed by others		

→ Pricing of the cloud.
3 pricing fundamentals + pay-as-you-go.
1) Compute
2) storage
3) Data transfer OUT of the cloud. (Data transfer IN is free)

→ AWS Global Infrastructure:
1) AWS Regions (cluster of data centers)
2) AWS Availability zones
3) AWS Data Centers
4) AWS Edge Locations / Points of Presence

Most AWS services are region scoped.

→ How to choose an AWS region ?.

1) Compliance
2) Proximity
3) Available services
4) Pricing.

→ AWS Availability zones.
Usually 3, min = 2, max = 6
One or more discrete data centers
Connected with high bandwidth, ultra-low latency networking.

→ AWS Points of Presence (Edge locations)
216 points of presence (205 EL & 11 Regional caches) in 84 cities across 42 countries.

→ Tours of the AWS console.

1) AWS has Global services.
Identity & Access Management (IAM)
Route 53 (DNS service)
CloudFront (Content Delivery Network)
WAF (Web Application Firewall)

2) Most AWS services are Region-Scoped:
EC2 (IaaS)
Elastic Beanstalk (Paas)
Lambda (FaaS)
Rekognition (Saas).

→ Shared Responsibility Model.

1) Customer = Responsible for the security IN the cloud.
- Customer Data
- Platform, applications, Identity & Access Management
- OS, Network, Firewall config.
- Client side data encryption & data integrity authentication,

Server side encryption (file system and/or data), Networking traffic protection (encryption, integrity, identity).)

AWS = Responsible for security OF the cloud
Software
Compute
Storage
Database
Networking
Hardware / AWS Global Infrastructure
Regions
Availability zones
Edge locations.

IAM
IAM: Users & Groups
IAM: Identity & Access Management
Root account created by default.
Groups only contain users and not groups.
User's don't have to belong to a group, and user can belong to multiple groups.
IAM: Permissions
Users or Groups assigned JSON docs called policies
Policies define permission to users
Least privilege principle.
IAM Policies structure:
Consists of:
Version
Id
Statement
Statement consists of:
Sid
Effect (Allow / Deny)
Principal (account/user/role)
Action: list of actions this policy allows or denies

Resources: list of resources to which the actions applied to.
Condition:

MFA = Multi Factor Authentication

MFA devices options in AWS:
Virtual MFA device
Google Authenticator (phone only) } Support for multiple tokens on a single device
Authy (multi-device)

Universal 2nd factor (U2F) Security key:
Yubikey by Yubico (3rd party)
Support for multiple root and IAM users using a single security key.

Hardware Key Fob MFA device
Provided by Gemalto (3rd party)

Hardware Key Fob MFA device for AWS GovCloud (US)
Provided by SurePassID (3rd party).

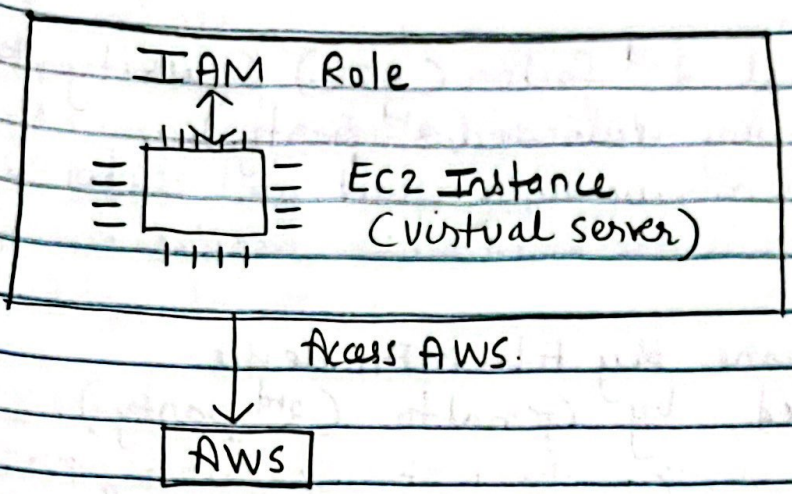
How can Users access AWS?
AWS Management Console
Protected by password + MFA
AWS Command Line Interface (CLI)
Protected by access keys.
AWS Software Developer Kit (SDK):
For code, protected by access keys.
Access keys are generated by AWS console.

AWS SDK - Language specific APIs (set of libraries)
Embedded within your application.
Supports:
SDKs (Javascript, Python, PHP, .NET, Ruby, Java, Go, Node.js, C++)
Mobile SDKs (Android, iOS).
IoT Devices SDKs (Embedded C, Arduino)
AWS CLI is built on AWS SDK for python

IAM Roles for Services:

Assign permissions to AWS services with IAM roles.

Common roles:
EC2 Instance Roles
Lambda Function Roles
Roles for CloudFormation.



IAM Security Tools:

1) IAM Credential Report (Account-level)
A report that lists all your account's users and the status of their various credentials.

2) IAM Access Advisor (User-level)
Shows the service permissions granted to a user and when those services were last accessed. Use this information to revise your policies.

IAM Guidelines & Best Practices

1) Assign users to groups & assign permissions to groups.
2) MFA
3) Create and use Roles for giving permissions to AWS services.
4) Use Access keys for Programmatic Access (CLI/SDK)
5) Never share IAM users & Access keys.

Shared Responsibility Model for IAM

AWS:
Infrastructure (global network security)
Configuration and vulnerability analysis
Compliance validation.

You
Users, groups, Roles, Policies management and monitoring
Enable MFA on all accounts
Rotate all your keys often
Use IAM tools to apply appropiate permissions
Analyze access patterns & review permissions.

IAM Section Summary *

Users: Mapped to a physical user, has a password for AWS console.
Groups: Contains users only
Policies: JSON documents that outlines permissions for users or groups
Roles: for EC2 instances or AWS services
Security: MFA + Password Policy
AWS CLI: Manage your AWS resources using the command line.
AWS SDK: Manage your AWS service using a programming language.
Access Keys: Access AWS using CLI or SDK
Audit: IAM Credentials Report & IAM Access Advisor.

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.

Bootstraping means launching commands when a machine starts.

→ EC2 Instance types: Overview

eg: 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.

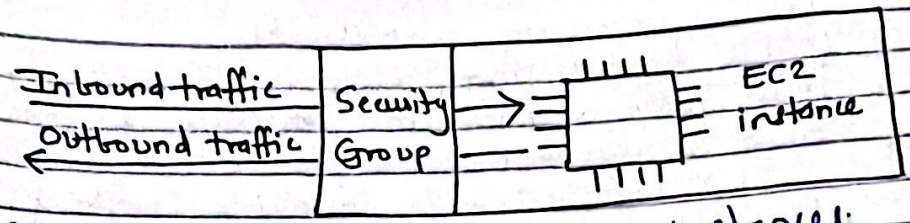
Memory optimized:
Fast performance for workloads that process large data sets in memory.
Use cases:
High performance, relational / non-relational DB.
Distributed web scale cache stores
In-memory databases optimized for BI
Applns performing real-time processing for big unstructured data

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 (eg: Redis)
Data warehousing applns.
Distributed file systems.

Introduction to Security Group.

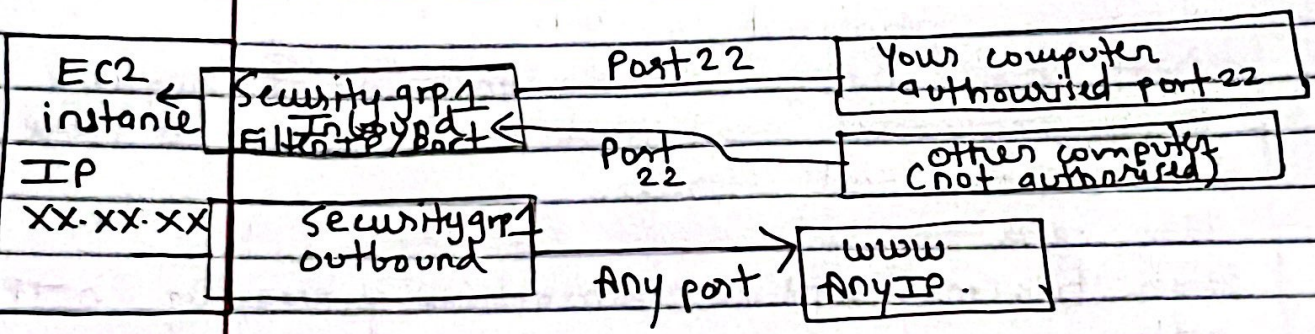
They control how traffic is allowed into or out of our EC2 instances.

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



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	122.149.196.85/32	
Custom TCP Rule	TCP	4567	0.0.0.0/0	java app



* Security Group Imp Points *

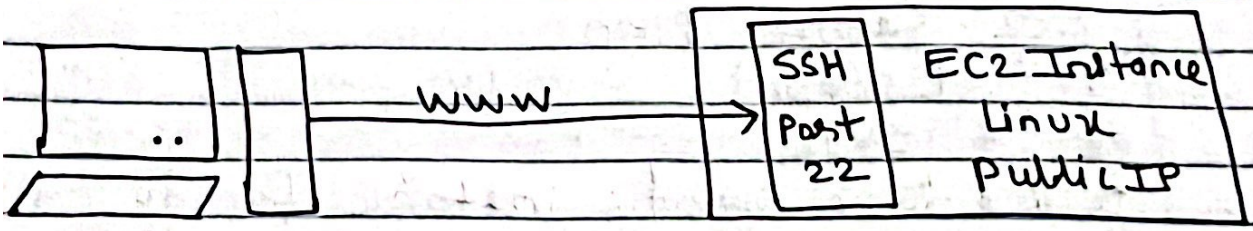
1) Can be attached to multiple instances
2) Locked down to a region / VPC combination
3) Live "outside" EC2.
4) Good to maintain one seperate SG for SSH access.
5) Appl^{n} not accessible (time out) - SG issue.
6) Appl^{n} gives "connection refused" - Appl^{n} error.
7) All inbound traffic blocked by 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 website.
3389 = RDP (Remote Desktop Protocol) - log into a Windows instance.

SSH.

SSH ✓ Putty ✓ EC2 Instance connect ✓



EC2 Instance Purchasing options:

On demand = Short workload, predictable pricing, pay by second.
Reserved - 1 & 3 yrs, long workloads
Savings Plans: (1 & 3 yrs) Commitment to an amou of usage, long workload.
Spot Instances: Short workloads, cheap, can lo instances.
Dedicated Hosts: book an entire physical server.
Dedicated Instances: No other customer will share
Capacity Reservations: Reserve capacity in specific for any duration.

1) EC2 On Demand:
- Pay for what you use
- Linux / Windows: Billing per second, after first min
- All other OS: Billing per hour
- 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-stage usage applns
- 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.

Dedicated Hosts:
Physical server with EC2 instance capacity fully dedicated to your use.
Compliance requirements, use 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, Access Management
Data security on your instance.

1) EC2 Section Summary ✱

2) EC2 instance: AMI (OS) + Instance size (CPU + RAM) + storage + SG + EC2 User data

3) SG: Fire wall attached to EC2 instance

4) EC2 User data: Script launched at the first start of an instance.

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

6) EC2 instance role: link to IAM roles

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

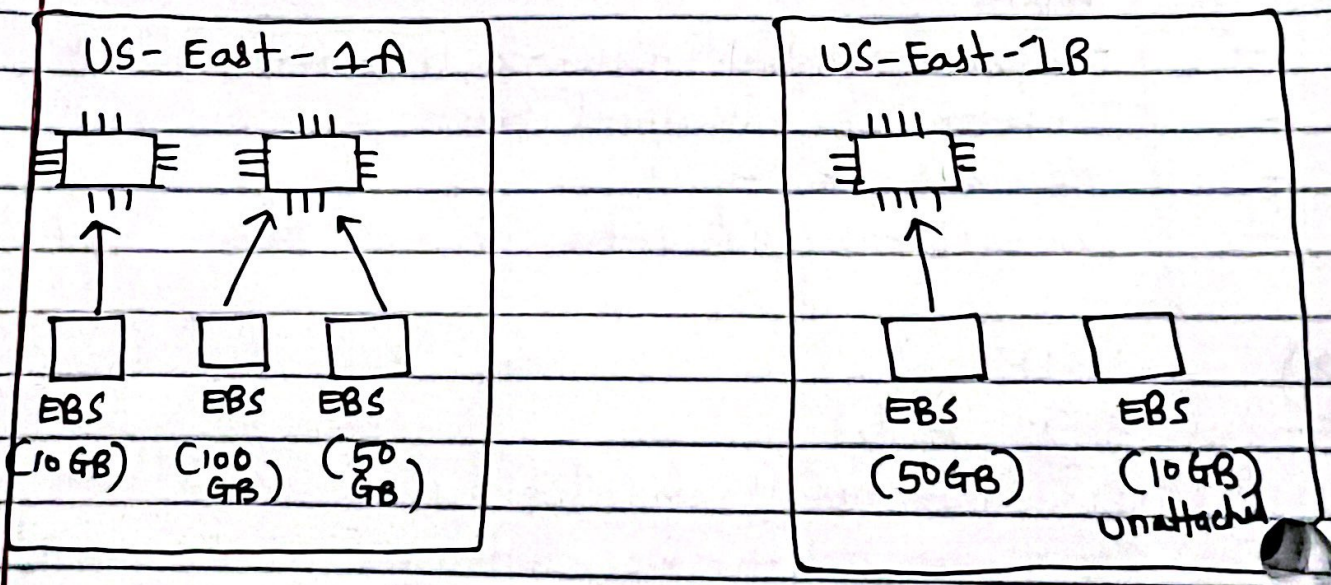
– Only one instance at a time

– Bound to a specific AZ.

– Provisioned capacity (Billed for all)

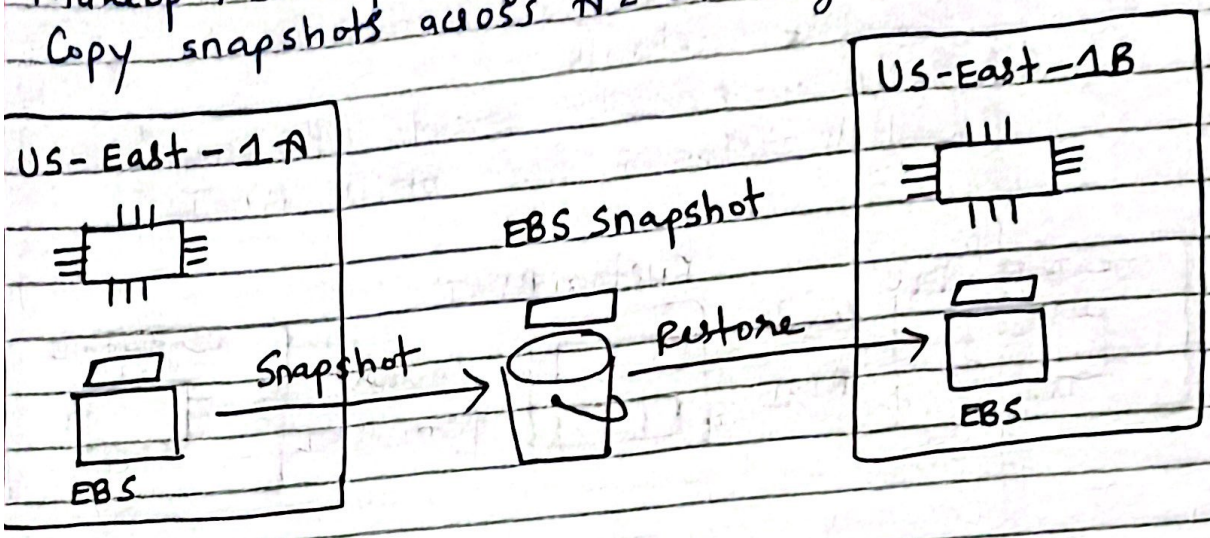
– To move volume across, first snapshot it.

eg:

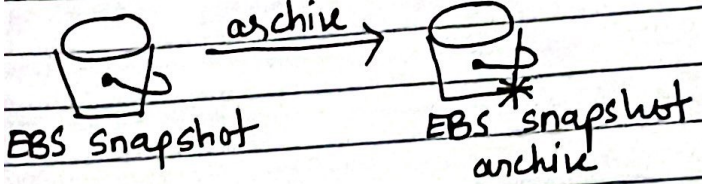


EBS - Delete on Termination attribute
By default, root EBS is deleted
Any other attached EBS vol is not deleted

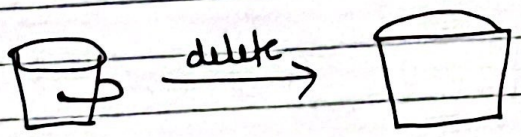
EBS Snapshots:
Makeup / Backup of your EBS volume
Copy snapshots across AZ or region ✓



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 s/w, OS.
Built for specific region (can be copied across regions)

Launch EC2 instances from:
1) Public AMI: AWS provided
2) own AMI:
3) AWS Marketplace AMI

AMI Process:
1) Start an EC2; customize it
2) Stop the instance
3) Build an AMI - create EBS snapshots
4) Launch instances from other AMIs