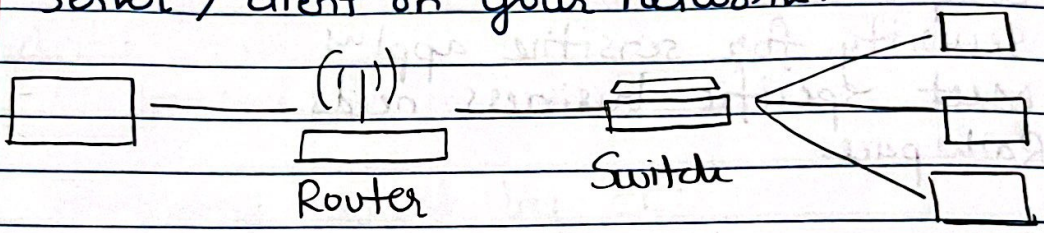
CLF-C01 Notes

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).

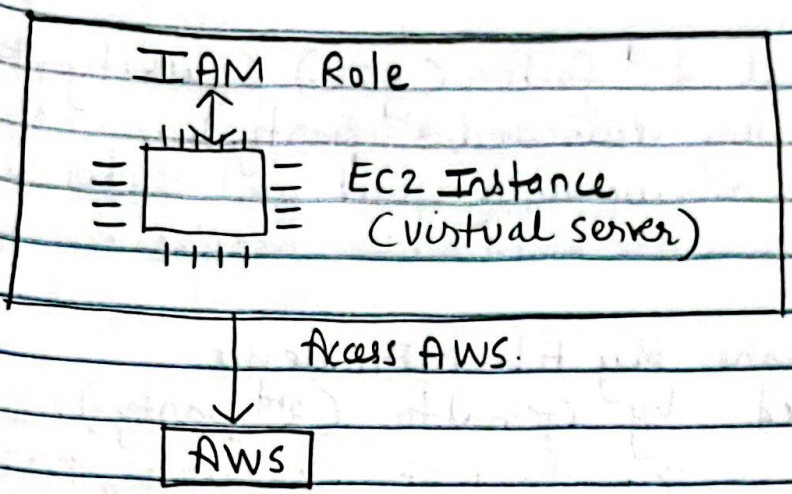
How can Users access AWS?
AWS Management Console
Protected by password + MFA
AWS Command Line Interface (CLI)
Protected by access keys.
AWS Software Developer Kit (SDK):
For code, protected by access keys.
Access keys are generated by AWS console.

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.