

AWS = Amazon Web Services

book list

Date / / No.

* Understanding Cloud Computing

* In the cloud : real place , Your data is stored somewhere.

* Cloud computing is the delivery of computing services over the internet

- ↳ Compute → EC2, Lambda
- ↳ Networking → VPC, Direct Connect
- ↳ Storage → S3, EBS
- ↳ Analytic → Athena, RedShift
- ↳ Development → Cloud9, CodeCommit
- ↳ Security → IAM, Macie
- ↳ Database → RDS, DynamoDB

* Virtualization lets you divide hardware resources on a single physical server into smaller units

↳ Virtualization is at the heart of cloud computing

(advantages of cloud computing)

1. go global in minutes
2. stop spending money running and maintaining data center
3. benefit from massive economies of scale
4. increase speed
5. stop guessing capacity
6. trade capital expense for variable expense

Capital Expenditures (CapEx)

are upfront purchases to ward fixed assets.

Operating Expenses (OpEx)

are funds used to run day to day operations.

benefits of cloud Computing ?

- ① **High Availability** → are designed to operate continuously without fail.
- ② **Elasticity** → You don't have to plan ahead of time how much capacity you need.
 - ↳ You can provision only what you need then grow, shrink based on demand.
- ③ **Agility** → increase agility. All services you have access to help you innovate faster, giving you speed to market.
- ④ **Durability** → is all about long-term data protection. Your data will remain intact without corruption.

IaaS

Infrastructure
as a Service

- * Building blocks
Web hosting

SaaS

Software
as a Service

- complete Application
Email Provider

PaaS

Platform
as a Service

- used by developer
Software website

Date / / No.

Cloud deployment Models

Private Cloud

"on-Premises"

Public Cloud

"AWS"

Hybrid Cloud

Private + Public cloud

* AWS logically groups its Regions into geographic locations.

* Region have several characteristics

+ Fully independent and isolated

+ Resource and service specific

Availability Zones

AZs

Consist of one or more physically separated data centers, each with redundant power, networking and connectivity, housed in separate facilities.

Characteristics of AZs

they are connected among themselves in a single region.

+ Physically Separated

+ Connected through low-latency links.

+ Fault tolerant

+ Allows for high availability.

Edge Locations

Used to cache content for speed delivery

+ Is like a mini data center, but it doesn't run your main infrastructure like EC2 instances.

AWS management console allows you to access your AWS accounts and manage applications running in your account from a web browser

- + broad usage:-
- 1. New to Cloud
 - 2. Non technical roles
 - 3. Technical roles
- + business analyst software engineer
+ project manager web developer
 solution architect

AWS command line interface CLI

allow you to access with your AWS account through a terminal or command window

Root user is automatically created when you open your account

Sections

EC2 = Elastic Compute Cloud

allows you to rent and manage Virtual servers in the cloud

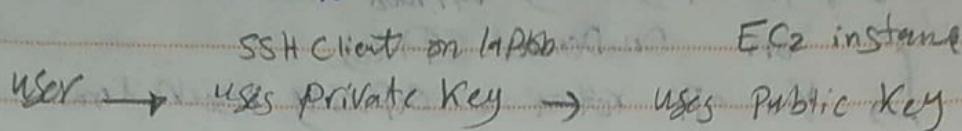
* Method to access an EC2 instance :-

- ① AWS management Console
- ② Secure Shell (SSH) : it allows you to establish a secure connection to your instance from your local laptop
- ③ EC2 Instance Connect (EIC) : it allows you to use IAM Policies to control SSH access to your instances, removing the need to manage SSH Keys.
- ④ AWS System Manager : allows you to manage your EC2 instances via a web browser or the AWS CLI

Date / / No.

the most common way to connect to Linux EC2 instances by (SSH) Secure Shell

- 1- Generates a Key Pair → which consists a Private Key and a Public Key. Proves your identity when connecting to an EC2 instance
- 2- Connect via SSH



EC2 Pricing Options

On-Demand → Fixed price → there is no contract, and you pay only for what you use

↳ used when → low cost

↳ Your applications have unpredictable workloads that can't be interrupted

↳ Your applications are under development

↳ Your workloads will not run longer than a year

* You can reserve capacity using it.

Spot → let you take advantage of unused EC2 capacity. Your request is fulfilled only if capacity is available.

↳ ask it when → You are not concerned about the start or stop time of your app

↳ Your workloads can be interrupted.

↳ Your application is only feasible at very low compute prices

* You can save up to 90% off on-Demand prices

Date / / No.

Reserved Instances RIS

allows you to commit a specific instance type in a particular Region for 1 or 3 years.

- When you use → Your app has steady state usage, you commit to 1 or 3 years
 - ↳ You can pay money upfront in order to receive a discount on On-Demand Prices
 - ↳ Your app retains a capacity reservation.

→ Set up 75% of on-demand prices

→ Required to sign a contract

→ You can reserve capacity in an Availability Zone for any duration

Dedicated Hosts

allow you to pay for physical server that is fully dedicated to running your instances.

↳ Use it when → You want to bring your own server-based software license from vendors like Microsoft or Oracle.

↳ You have regulatory or corporate compliance requirements around tenancy model

→ Set up to 70% of on-demand
the server is not shared with other customers

Saving Plans

allow → to commit to compute usage (measured per hour) for 1 or 3 years.

use when → You want to lower your bill across multiple compute services

↳ You want to the flexibility to change compute services, instance types, operating system or regions.

→ This doesn't provide a capacity reservation.

Date / No

automatically distributes your incoming application traffic across EC2

(Features)

EC2 instances offer (load balancing) And (Auto Scaling)

- EC2 Auto Scaling adds or replaces EC2 instances automatically across AZs, based on need and changing demand.
- Reduces the impact of system failures and improves the availability of your applications.

AWS Lambda

Lambda is a serverless compute service that lets you run code without managing servers

- scales automatically
- Serverless means you don't worry about managing servers like with EC2.

- * it allows developers to focus on core business logic for the apps, they are developing instead of worrying about managing servers
- * it is a building block for many serverless applications.

Pricing Model of Lambda

- You are charged on the duration and number of requests
- 1. Compute time
 - 2. Request count
 - 3. Always free

AWS Fargate

is a Serverless Compute engine for containers,

- * Serverless . * Scales automatically
- * allows you to manage containers like Docker

Amazon Lightsail

* to quickly launch all the resources you need for small projects

- * deploy preconfigured apps like WordPress at the click of a button
- * simple screens for people with no cloud experience
- * includes a virtual machine, SSD-based storage, data transfer, DNS management, and a static IP
- * low, predictable monthly fee

AWS Outposts

* to run cloud services in your internal data center

- * support workloads → reason on-premises due to latency
- * used for hybrid experience
- * access to cloud services and API

AWS Batch

to process large workloads in smaller chunks

- * run hundreds and thousands of smaller batch processing jobs
- * dynamically provisions instances based on volume

Amazon Simple Storage Service**S3**

- * is an object storage service for the cloud that is highly available
- * objects are stored in buckets (or directories)
- * can be public or private
- * you can upload objects via the console
- * essentially unlimited storage that can hold millions of objects per bucket

Data Accessibility

Durability: is important so your objects are never lost or compromised
Availability: You can access your data quickly when you need.

S3 Storage Classes → in your uses and your budget

S3 Standard

S3 Intelligent-Tiering

S3 Standard Infrequent Access (IA)

S3 One Zone Infrequent

S3 Glacier

S3 Glacier Deep Archive

S3 Cold Posts

S3 in the real World

① Static website ③ Analytic systems

② Data archive ④ Mobile applications

EC2 Storage

EC2 supports several storage options for your instances

Amazon Elastic Block Store [EBS] is storage device (called a volume) that can be attached to (or removed from) your instance

EC2 Instance Store is local storage that is physically attached

to the host computer and cannot be removed

* Storage on disks Physically attached to an instance

* Faster with higher I/O speed

* Storage is temporary since data loss occurs when EC2 stops

recommended for → temporary storage needs, Data replicated across instances

Amazon Elastic File System (EFS)

is a serverless network file system for shared files

* only for Linux

* more expensive than EBS

* Accessible across different Availability Zones in the same region

for main directories for business-critical apps

↳ lift and shift existing enterprise apps

Storage Gateway is a hybrid storage service.

Connect on-premises and cloud data

for → moving backups to the cloud

↳ reducing costs for hybrid cloud storage

↳ low latency access to data

AWS Backup

helps you manage data backups across multiple AWS services.

* create a backup plan that includes frequency and retention

AWS

world is built



Date / / No.

Content delivery network [CDN]

is a mechanism to deliver content quickly and efficiently based on geographic location

Amazon CloudFront

is CDN that delivers data applications globally with low latency.

- * makes content available globally or restricts it based on location
- * Speed up delivery of static and dynamic web content
- * uses edge locations to cache content

In Real World

① S3 static websites

② prevent attacks

③ IP address blocking

Amazon Global Accelerator

sends your users through the AWS global network

* improves latency and availability

* sends traffic through the AWS global network infrastructure

Amazon S3 Transfer Acceleration

improves content uploads and downloads to from S3 buckets

* fast transfer of files

* uses CloudFront's globally distributed edge locations

Amazon Virtual Private Cloud

VPC

is a networking service that allows you to create a secure private network in the AWS cloud where you launch your resources

* private virtual network

* launch resources like EC2 instances inside the VPC

* isolate and protect resources

* VPC spans Availability Zones in a Region





DNS : Domain Name System

direct internet traffic by connecting domain names with web servers.

AWS CloudFront is a DNS service that routes users to applications.

- * Supports hybrid cloud architectures
- * Performs health checks on AWS resources

AWS Direct Connect

is a dedicated physical network connection from your on-premises data center to AWS.

in real world → 1- Large datasets

2- Business critical data

3- Hybrid model

AWS VPN

Site-to-Site VPN creates a secure connection between your internal networks and your AWS VPCs.

* Similar to Direct Connect, but data travels over the public

* Data is automatically encrypted

Supports hybrid

API Gateway → allows you to build and manage API
of Share data between system

Date / / No.



Data base DB

RDS

Relational Database Service

Support Popular database Engine

MySQL, Oracle, ...

* offer high availability

Amazon DynamoDB

Managed NoSQL key-value and document db

Amazon Neptune

Managed graph db that supports highly connected datasets

Amazon Aurora

Aurora is a relational db compatible with MySQL and PostgreSQL that created by Amazon

Amazon Document DB

managed document db that supports MongoDB

Amazon ElastiCache

managed in memory data store

Compatible with Redis or Memcached

Database Migration Service [DMS] helps you migrate db to or with AWS

external world → ① Oracle to Aurora MySQL

② Oracle to Oracle

③ RDS Oracle to Aurora MySQL

Server Migration Services [SMS] allows you to migrate on premises servers to AWS

* Server saved as a new Amazon machine image (AMI)

* use AMI to launch servers as EC2 instances





data warehouse is a data storage solution that aggregates massive amounts of historical data from disparate source
↳ benefits → support query, reporting analytics, business intelligence

Amazon Redshift is a scalable data warehouse solution
↳ for Data consolidation
↳ Relational databases

Analytics: is the act of querying or processing your data

Athena is a query service for S3, analyse S3 data using SQL

Glue Prepare your data for analytics

Kinesis allows you to analyse data and video streams in real time

EMR Elastic MapReduce → helps you process large amounts of data

Data-Pipeline helps you move data between compute and storage services
Running either on AWS or on-premises

QuickSight helps you visualize your data

AI, Machine learning

Rekognition: allows you to automate your image and video analysis

Comprehend is a natural-language processing (NLP) service that finds relationships in text

Polly: turns text into speech

SageMaker: helps you build, train and deploy machine learning models quickly



Date / / No.



translate : Provides language translation
lex : helps you build conversational interfaces like chatbots

AWS tools Software developer use tools to accelerate the software development and release cycle

Cloud9 allows you to write code within an integrated development environment (IDE) from within your web browser

Code Commit is a source control system for private git repositories

Code build allows you to build and test your app source code

Code Deploy manages the deployment of code to compute services in the cloud or on-premises

Code Pipeline automates the software release process

X-ray helps you debug production apps

Code Star helps developer collaboratively work on development projects





Benefit of deployment and IT infrastructure management

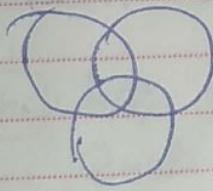
* these services help you quickly stand up new applications, automate the management of infrastructure and provide real-time visibility into system health.

Cloud Formation allows you to provision AWS resources using infrastructure as code (IaC)

Elastic Beanstalk, allows you to deploy your web apps and services to AWS

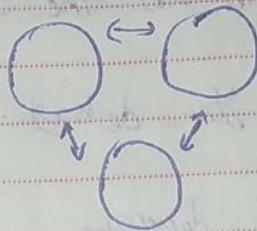
Ops Works allows you to use Chef or Puppet to automate the configuration of your servers and deploy code

Monolithic app



tight coupling

Micro Services



loose coupling

Components are highly dependent on each other

Components are connected but Not dependent on each other

(messing and Integrations)

SQS [Simple Queue Service] is a message queuing service that allows you to build loosely coupled systems.



Date

/ / No

(SNS)

Simple Notification Service
allow you to send emails and text message from your apps

(SES)

Simple Email Service
is an Email Service that allows you to send richly formatted
HTML emails from your applications.

AWS
alerting, monitoring and logging → give you insight into how
well your systems are performing and help you proactively
find and resolve errors

CloudWatch

is a collection of services that help you monitor
and observe your cloud resources

CloudWatch [Alarms, logs, Metrics, Events]

Cloud Trail tracks user activity and API calls within your account

Amazon WorkSpaces allows you to host virtual desktops in the
cloud.

Amazon Connect is a cloud contact center service

Shared Responsibility Model

AWS' responsibility
Security of the cloud

* AWS is responsible for protecting and securing
their infrastructure

Your responsibility
Security in the cloud

You are responsible for how
services are implemented and
managing your app data

Well-Architected Framework :-

Code Commit → Operational Excellence → Create app support production workloads
 CloudTrail → Security → Put mechanisms in place that protect your data
 RDS → Reliability → Design systems that work consistently and recover quickly
 Lambda → Performance Efficiency → Effective use of computing resources
 S3 → Cost Optimization → Delivering optimum and resilient solution
 Auto Scaling → Sustainability → environmental impacts especially energy consumption and efficiency

IAM = Identity and Access Management

allows you to control access to your AWS services and resources

Authentication

is where you present your username and verification of password

Authorization

determine which services and resources the authenticated identity has access to

(Who)

→ what

(What)

* the principle of least privilege involves giving a user the minimum access required to do the job done.

(Role)

define access permissions and are temporarily assumed by an IAM user or service

(Policies)

You manage permissions for IAM users, groups, and roles by creating a policy document in JSON format

IAM Credential Report → lists all users in your account and the status of their various credentials

Application Security Services →

Date

/ / No

Firewall

Help You to monitor and Protect your resources

Prevent unauthorized access to your network by inspecting incoming and outgoing traffic against security rules

WAF

Web Application Firewall

↳ helps protect your web apps against common web attacks

DDoS

Distributed Denial of Services

Causes a traffic jam on website or app in an attempt to cause it to crash

Shield

is a managed Distributed Denial of Protection Service.

Macie

helps You discover and protect sensitive data

Config → allows You to assess, audit and evaluate the configuration

GuardDuty → is an intelligent threat detection system that uncovers unauthorized behavior

Inspector → works with EC2 instances to uncover and report vulnerabilities

Artifact → offers on demand access to AWS security and compliance reports

Cognito → helps You to control access to mobile, web apps

KMS : Key Management Services

allows You to generate and store encryption keys

Cloud HSM : to generate encryption key.

Secrets Manager to manage and retrieve secrets [key, passwords]



Billing Services

Date _____ No. _____

Budgets → allows you to set custom budgets that alert you when your cost or usage exceed your budgeted

Cost and usage Report → contain most comprehensive set of cost and usage data

Organizations → allows you to centrally manage multiple AWS accounts under one umbrella

Control Tower → to ensure your accounts conform to company-wide policies

System Manager → gives you visibility and control over your AWS resources

Managed Services → provide you AWS infrastructure

Professional Services → enterprise customers move to a cloud based operating model

AWS Partner Network (APN) → approved partners that offer software solutions and consulting services for AWS