AWS Cloud Practitioner

Category	
Files	
Created	@June 26, 2022 4:24 PM
Reminder	
Status	Open
URL	
Updated	@December 30, 2022 7:24 PM

▼ 1. Cloud Concepts

▼ 1. What is AWS

AWS stands for Amazon Web Services which is a collection of cloud services hosted under a single API to provide multiple no of workloads which was first launched in 2006.

▼ 2. Timelines of AWS Services

2004 - SQS (Simple Queue Service) which is still in use.

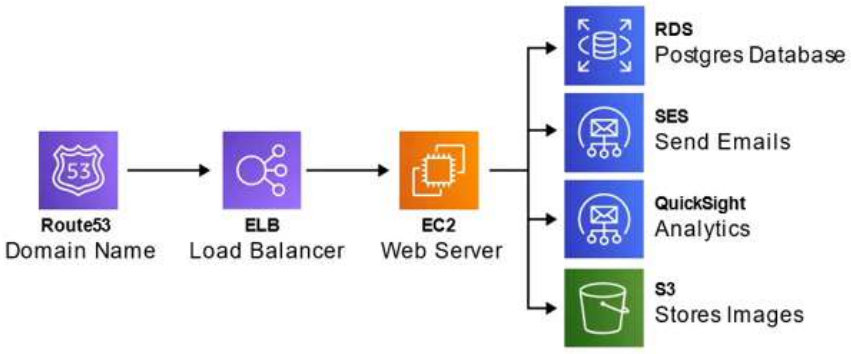
2006(March) - S3(Simple Storage Service) which is still in use.

2006(August) - EC2(Elastic Cloud Compete) which is the most used AWS Service now.

2010 - Amazon started using AWS

2013- Emerged as a Certification

▼ 3. Cloud Service Provider Architecture diagram.



▼ 4. 4 most Common Cloud Services

Common Cloud Services

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

A cloud service provider **can have hundreds of cloud services** that are grouped into various types of services.
The four most common types of cloud services *(the 4 core)* for Infrastructure as a Service (IaaS) would be:

Compute
Imagine having a virtual computer that can run application, programs and code.

Networking
Imagine having virtual network defining internet connections or network isolations between services or outbound to the internet

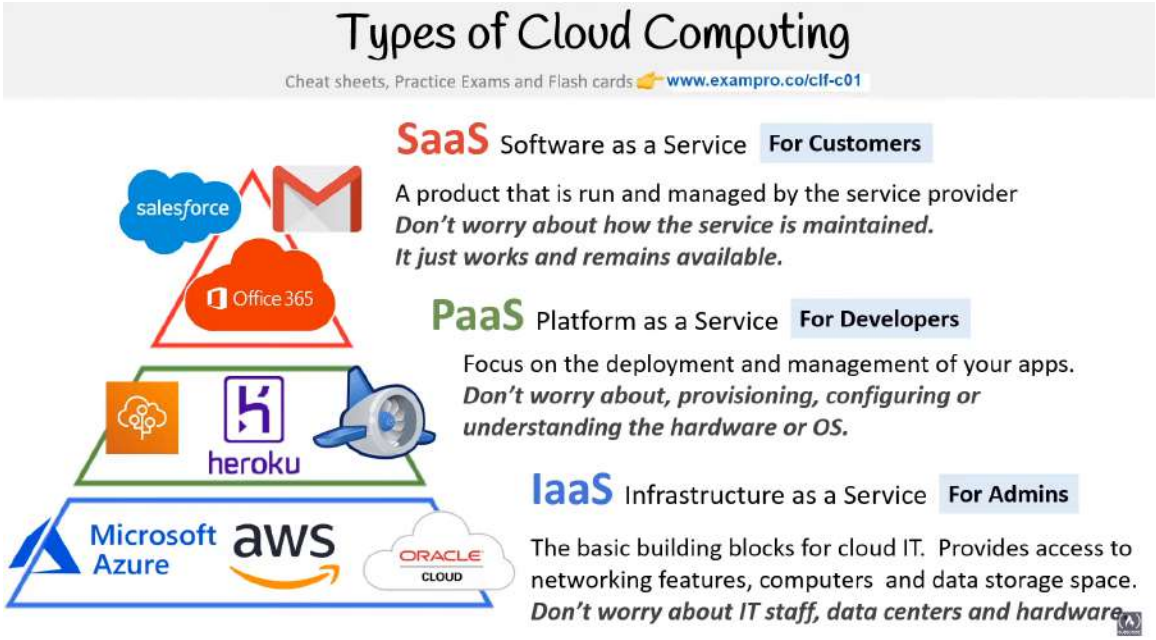
Storage
Imagine having a virtual hard-drive that can store files

Databases
Imagine a virtual database for storing reporting data or a database for general purpose web-application

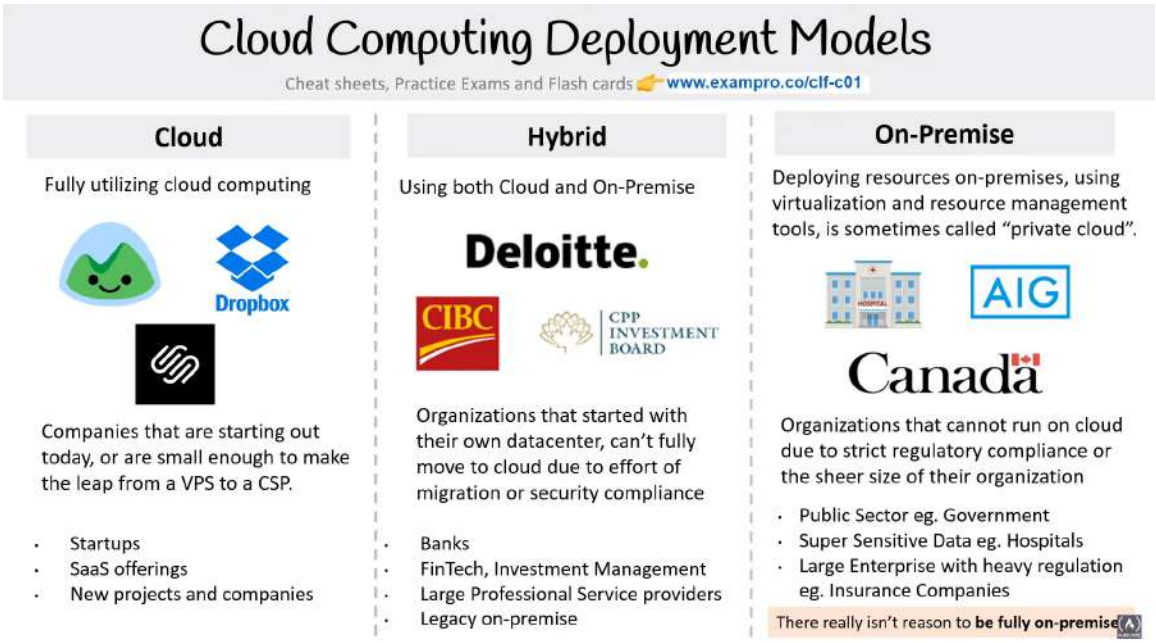
AWS has over **200+** cloud services

The term "Cloud Computing" can be used to refer to all categories, even though it has "compute" in the name.

▼ 5. Types of Cloud Computing



▼ 6. Cloud Computing Deployment Models



▼ 2. Digital Transformation

▼ 1. Evolution of Computing

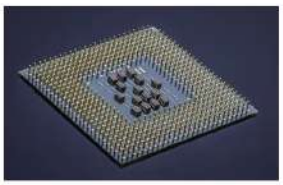
Evolution of Computing Power

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

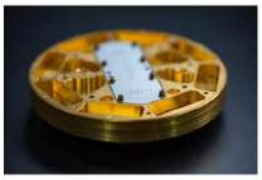
What is Computing Power?

The throughput measured at which a computer can complete a computational task.

General Computing
Xeon CPU Processor



GPU Computing
*50x faster than traditional CPUs



Quantum Computing
- D-Wave 2000Q
- Rigetti 16Q Aspen-4
- IonQ linear ion trap
- 100 Million times faster

AWS Service Offering

Elastic Compute Cloud EC2

AWS Inferentiare (Inf1)

AWS Bracket
Via CalTech

▼ 3. Benefits of Cloud

▼ 1. 7 Advantages of Cloud

Seven Advantages to Cloud

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Cost-effective	You **pay for what you consume**, **no up-front cost**. On-demand pricing or Pay-as-you-go (PAYG) with thousands of customers sharing the cost of the resources
Global	Launch workloads **anywhere in the world**, Just choose a region
Secure	Cloud provider takes care of physical security. **Cloud services can be secure by default** or you have the ability to configure access down to a granular level.
Reliable	Data backup, disaster recovery, data replication, and fault tolerance
Scalable	Increase or decrease resources and services based on demand
Elastic	**Automate** scaling during spikes and drop in demand
Current	The underlying hardware and managed software is patched, upgraded and replaced by the cloud provider without interruption to you.

▼ 4. AWS Global Infrastructure

▼ 1. What is AWS Global Infrastructure

AWS Global Infrastructure

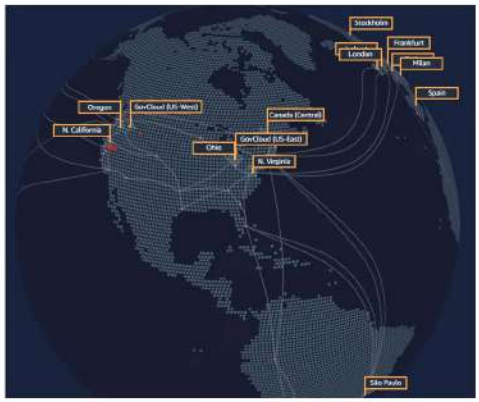
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

What is the AWS Global Infrastructure?

The AWS Global Infrastructure is **globally distributed hardware and datacenters** that **are physically networked together** to act as one large resource for the end customer.

The AWS Global Infrastructure is made up of the following resources:

- **25** Launched Regions
- **81** Availability Zones
- **108** Direct Connection Locations
- **275+** Points of Presence
- **11** Local Zone
- **17** Wavelength Zones



AWS has **millions** of active customers and **tens of thousands** of partners globally

▼ 2. Regions

Global Infrastructure - Regions

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Each region generally has three Availability Zones

- Some new users are limited to two eg. US-West

New services almost always become available first in **US-EAST**

Not all AWS Services are available in all regions

All your billing information appears in **US-EAST-1** (North Virginia)

The cost of AWS services vary per region

When you choose a region there are four factors you need to consider:

1. What Regulatory Compliance does this region meet?
2. What is the cost of AWS services in this region?
3. What AWS services are available in this region?
4. What is the distance or latency to my end-users?

▼ 3. Regions vs Global

Global Infrastructure – Regional vs Global Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Regional Services
AWS **scopes** their AWS Management Console on a selected Region.
This will determine where an AWS service will be launched and what will be seen within an AWS Service's console.
You generally don't explicitly set the Region for a service at the time of creation.

Global Services
Some AWS Services operate across multiple regions and the region will be fixed to "Global"
E.g. Amazon S3, CloudFront, Route53, IAM

For these global services at the time of creation:

- There is no concept of region. eg. IAM User
- A single region must be explicitly chosen eg. S3 Bucket
- A group of regions are chosen eg. CloudFront Distribution

▼ 4. Avalaibility Zones

Global Infrastructure – Availability Zones

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

An **Availability Zone** (AZ) is physical location made up of one or more datacenter.

A datacenter is a secured building that contains hundreds of thousands of computers.

A region will ***generally** contain **3 Availability Zones**

Datacenters within a region will be isolate from each other (different buildings). But they will be close enough to provide low-latency (< 10ms).

Its common practice to run workloads in at least 3 AZs to ensure services remain available in case one or two datacenters fail. (High Availability)

AZs are represented by a Region Code, followed by a letter identifier eg. **us-east-1a**

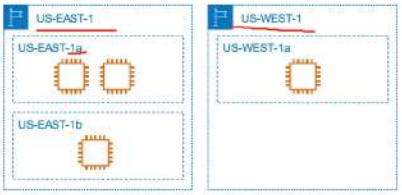
Global Infrastructure – Availability Zones

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

A Subnet is associated with an Availability Zone.

You never choose the AZ when launching resources.
You choose the Subnet which is associated to the AZ.

Example of an architectural diagram, representing two AZs, the Subnets associated with those AZs, and EC2 instances (Virtual Machines) launched in those subnets



The US-EAST-1 region has 6 AZs
(the most Availability Zones of any region)

Global Infrastructure – Availability Zones

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

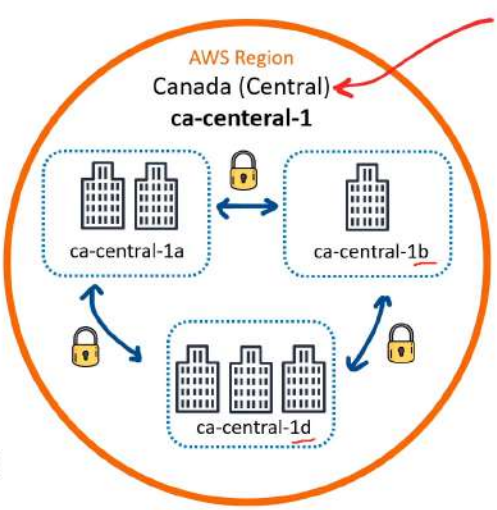
A region has multiple Availability Zones

An Availability Zone is made up of **one or more** datacenters

All AZs in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between

All traffic between AZs is encrypted

AZs are within 100 km (60 miles) of each other.



Montreal

@stevenwright Upsplash

▼ 5. Fault Tolerance

Global Infrastructure – Fault Tolerance

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Fault Domain

What is a fault domain?
A fault domain is a section of a network that is vulnerable to damage if a critical device or system fails. The purpose of a fault domain is that if a failure occurs **it will not cascade outside that domain**, limiting the damage possible.

You can have fault domains nested inside fault domains.

What is a fault level?
A fault level is a collection of fault domains.

The scope of a fault domain could be:
- specific servers in a rack
- an entire rack in a datacenter
- an entire room in a datacenter
- the entire data center building

Its up to the Cloud Service Provider (CSPs) to define the boundaries of a domain

An AWS Region would be a **Fault Level** → Fault Level: us-east-1 (Region)

A Availability Zone would be a **Fault Domain** → Fault Domain: us-east-1a (AZ), Fault Domain: us-east-1b (AZ)

Global Infrastructure – Fault Tolerance

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Each Amazon Region is designed to be completely **isolated** from the other Amazon Regions.
- This achieves the greatest possible fault tolerance and stability

Each Availability Zone is **isolated**, but the Availability Zones in a Region are connected through low-latency links
Each Availability Zone is designed as an **independent failure zone**
- *A "Failure Zone" is AWS describing a Fault Domain.*

Failure Zone
- Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains
- discrete uninterruptible power supply (UPS) and onsite backup generation facilities
- data centers located in different Availability Zones are designed to be supplied by independent substations to reduce the risk of an event on the power grid impacting more than one Availability Zone.
- Availability Zones are all redundantly connected to multiple tier-1 transit providers

Multi-AZ for High Availability
If an application is partitioned across AZs, companies are better isolated and protected from issues such as **power outages, lightning strikes, tornadoes, earthquakes**, and more.

▼ 6. Point of Presence(POPs)

Global Infrastructure – Point of Presence (PoP)

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

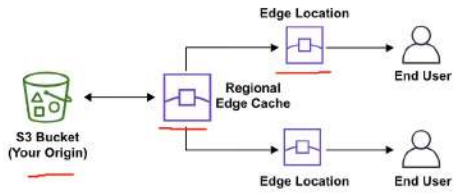
Points of Presence (PoP) is an intermediate location between an AWS Region and the end user, and this location could be a datacenter or collection of hardware.

For **AWS** a Point of Presence is a data center **owned by AWS or a trusted partner** that is utilized by AWS Services related **for content delivery or expediated upload.**

PoP resources are:
- **Edge Locations**
- **Regional Edge Caches**

Edge Locations are datacenters that hold cached (copy) on the most popular files (eg. web pages,images and videos) so that the delivery of distance to the end users are reduce

Regional Edge Locations are datacenters that hold much larger caches of less-popular files to reduce a full round trip and also to reduce the cost of transfer fees.



▼ 7. Services that use POPs

Global Infrastructure – Point of Presence (PoP)

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

The following AWS Services use PoPs **for content delivery or expediated upload.**

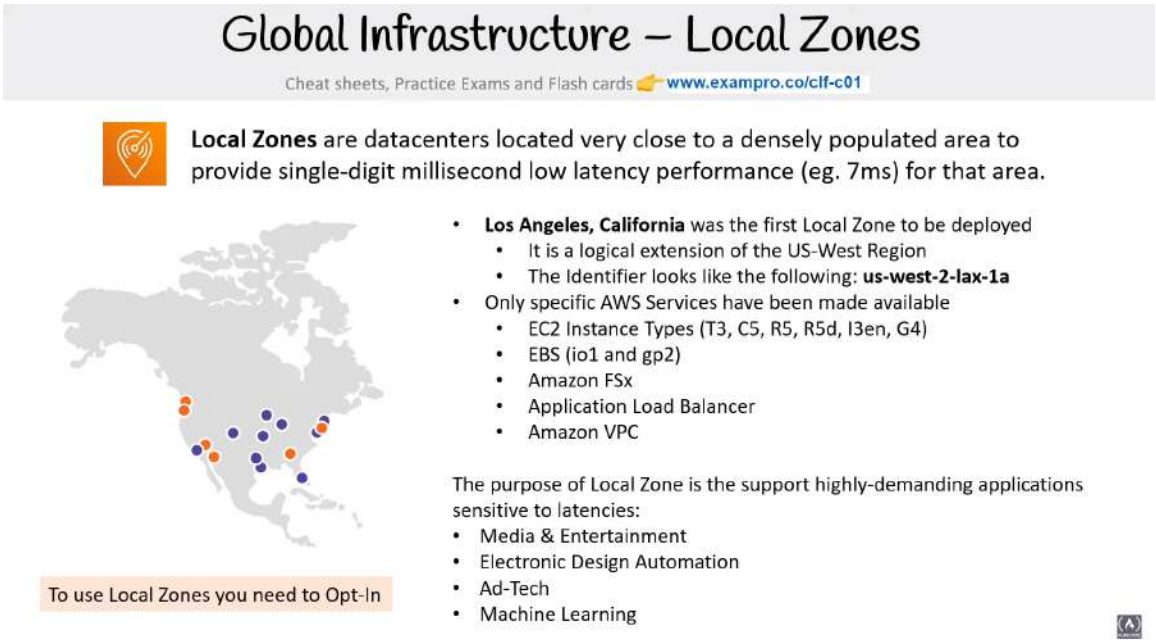
Amazon CloudFront is a **Content Delivery Network (CDN) service** that:
- You point your website to CloudFront so that it will route requests to nearest Edge Location cache
- allows you to choose an **origin** (such as a web-server or storage) that will be source of cached
- caches the contents of what origin would returned to various Edge Locations around the world

Amazon S3 Transfer Acceleration allows you to generate a special URL that can be used by end users to upload files to a nearby Edge Location. Once a file is uploaded to an Edge Location, it can move much faster within the AWS Network to reach S3.

AWS Global Accelerator can find the optimal path from the end user to your web-servers. Global Accelerator are deployed within Edge Locations so you send user traffic to an Edge Location instead of directly to your web-application.

▼ 8. AWS Direct Connect

▼ 9. Local Zones



▼ 10. Data Residency

Global Infrastructure – Data Residency

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

What is Data Residency?
The physical or geographic location of where an organization or cloud resources reside.

What is Compliance Boundaries?
A regulatory compliance (legal requirement) by a government or organization that describes where data and cloud resources are allowed to reside

What is Data Sovereignty?
Data Sovereignty is the jurisdictional control or legal authority that can be asserted over data because it's physical location is within jurisdictional boundaries

For workloads that need to meet compliance boundaries strictly defining the data residency of data and cloud resources in AWS you can use:

AWS Config is a Policy as Code service.
You can create rules to continuous check AWS resources configuration. If they deviate from your expectations you are alerted or AWS Config can in some cases auto-remediate.

IAM Policies can be written explicitly deny access to specific AWS Regions. A **Service Control Policy** (SCP) are permissions applied organization wide.

AWS Outposts is **physical rack of servers** that you can put in your data center. Your data will reside whenever the Outpost Physically resides

▼ 11. GovCloud

Global Infrastructure – GovCloud (US)

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

FedRAMP

Federal Risk and Authorization Management Program (FedRAMP)
a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

What is GovCloud?
A Cloud Service Provider (CSP) generally will offer an **isolated region** to run FedRAMP workloads.

AWS GovCloud Regions allow customers to host sensitive **Controlled Unclassified Information** and other types of regulated workloads.

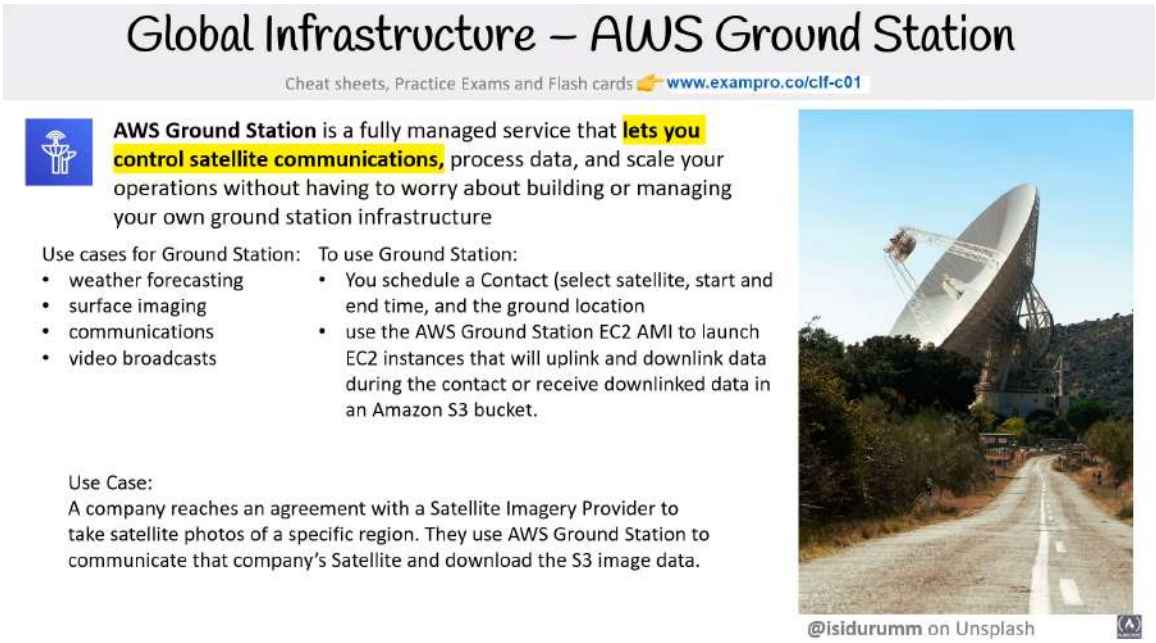
- GovCloud Regions are only operated by employees who are U.S. citizens, on U.S. soil.
- They are **only** accessible to U.S. entities and root account holders who pass a screening process

Customers can architect secure cloud solutions that comply with:

- FedRAMP High baseline
- DOJ's Criminal Justice Information Systems (CJIS) Security Policy
- U.S. International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)
- Department of Defense (DoD) Cloud Computing Security Requirements Guide

▼ 12. AWS China

▼ 13. AWS Ground Station



▼ 14. AWS Outposts

Global Infrastructure – AWS Outposts

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience.

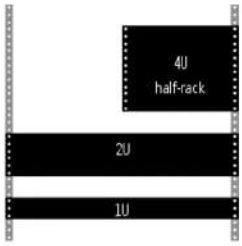
AWS Outposts is rack of servers running AWS Infrastructure on your physical location

42U Rack

What is a Server Rack?
A frame design to hold and organize IT equipment.

Rack Heights
U stands for "rack units" or "U spaces" with is equal to 1.75 inches.
The industry standard rack size is 48U (7 Foot Rack)

full-size rack cage is 42U high
- equipment is typically 1U, 2U, 3U, or 4U high



Global Infrastructure – AWS Outposts

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS Outposts comes in 3 form factors: 42U, 1U and 2U

This a full rack of servers provided by AWS

42U

AWS delivers it to your preferred physical site fully assembled and ready to be rolled into final position. It is installed by AWS and the rack needs to be simply plugged into power and network.

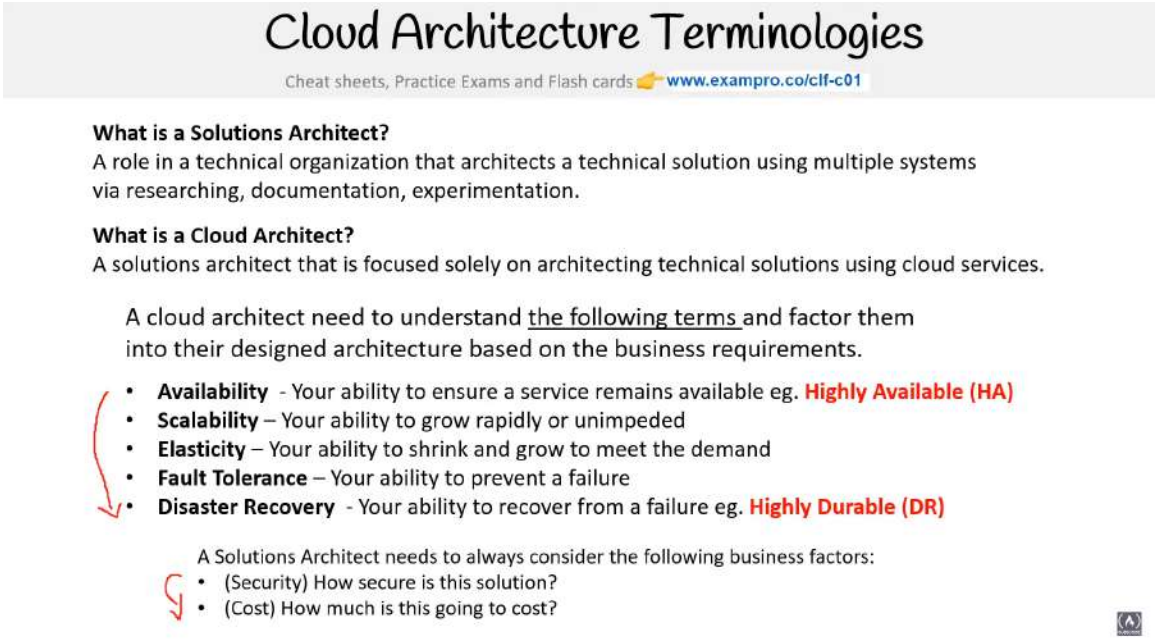
These are servers that you can place into your existing racks:

1U
suitable for 19-inch wide
24-inch deep cabinets
AWS Graviton2 (up to 64 vCPUs)
128 GiB memory
4 TB of local NVMe storage

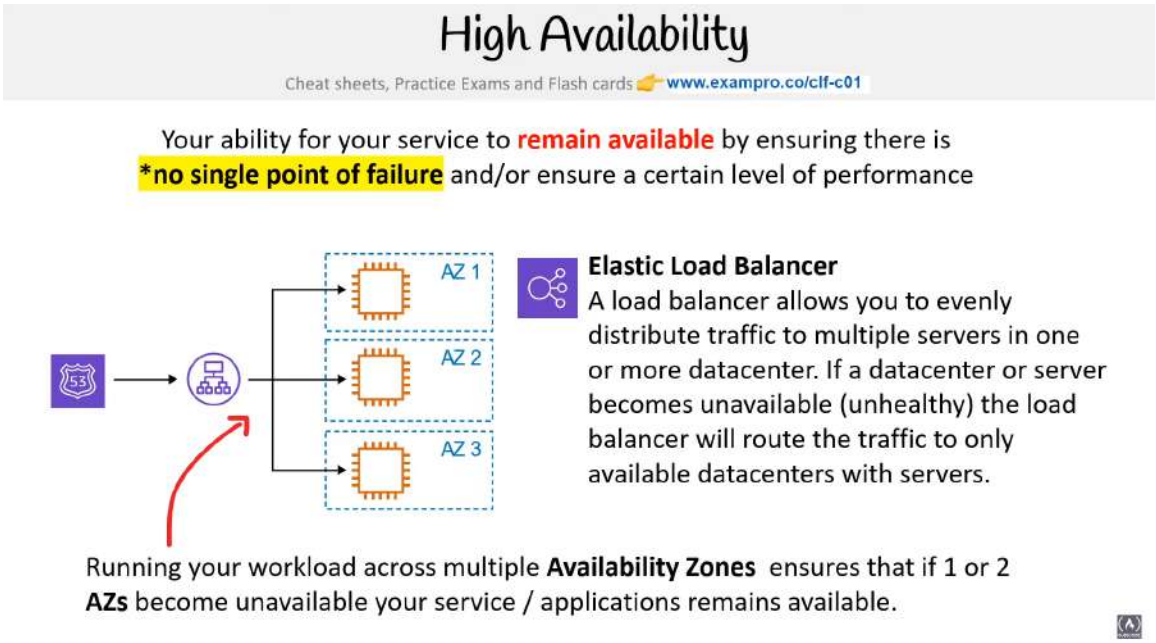
2U
suitable for 19-inch wide
36-inch deep cabinets,
Intel processor (up to 128 vCPUs)
256 GiB memory
8TB of local NVMe storage

▼ 5. Cloud Architecture

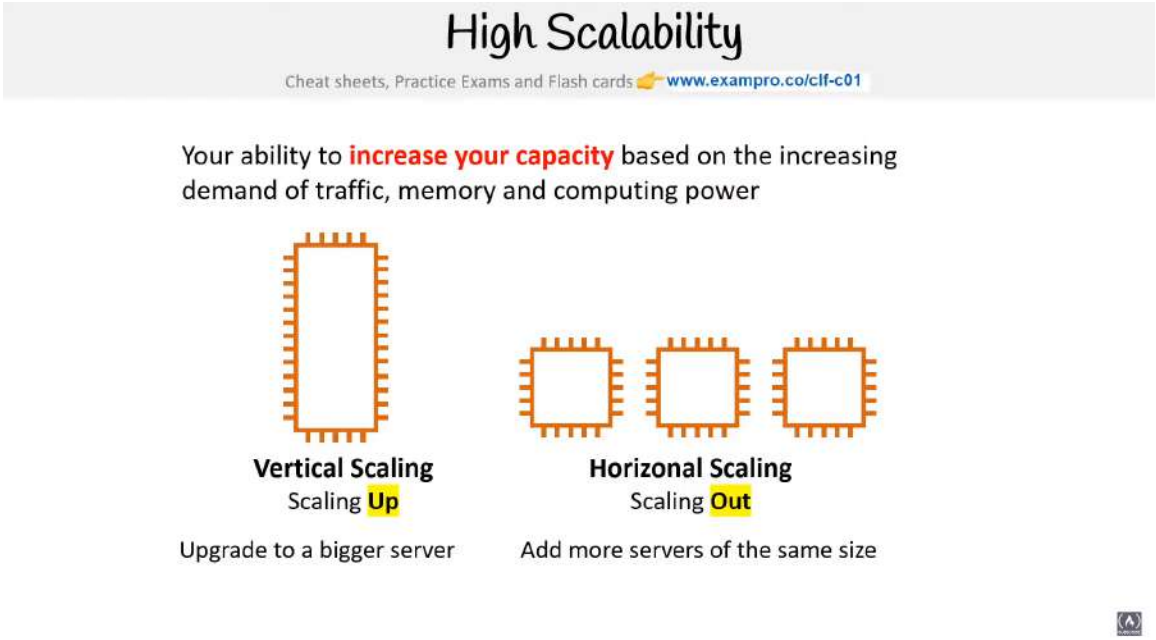
▼ 1. Cloud Architect and Solution Architect



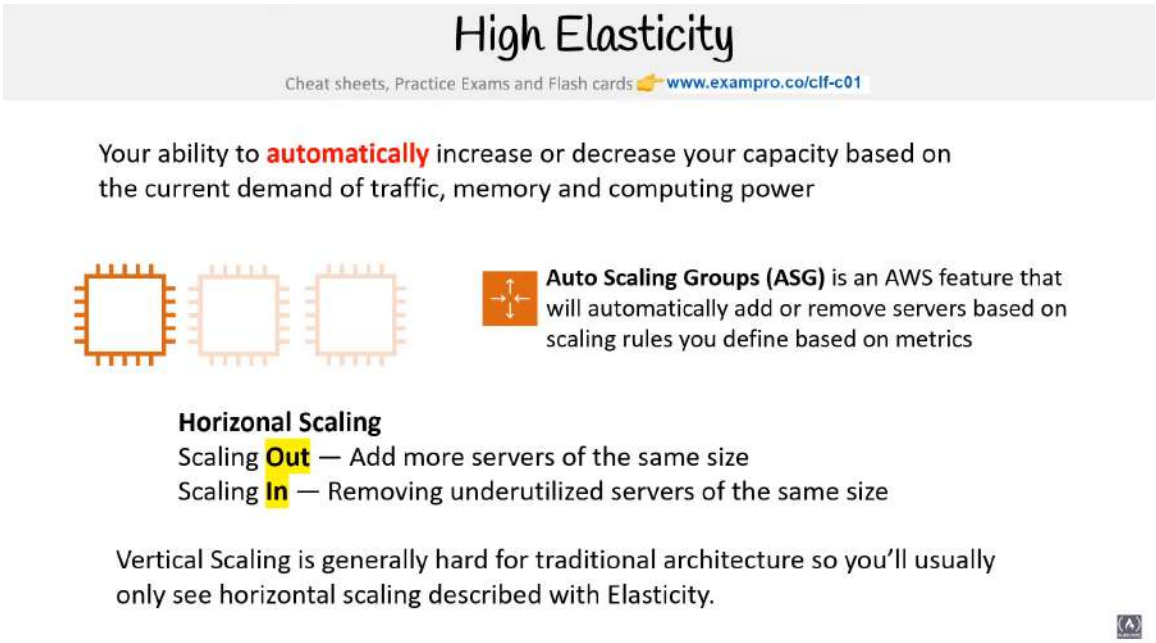
▼ 2. What is high availability



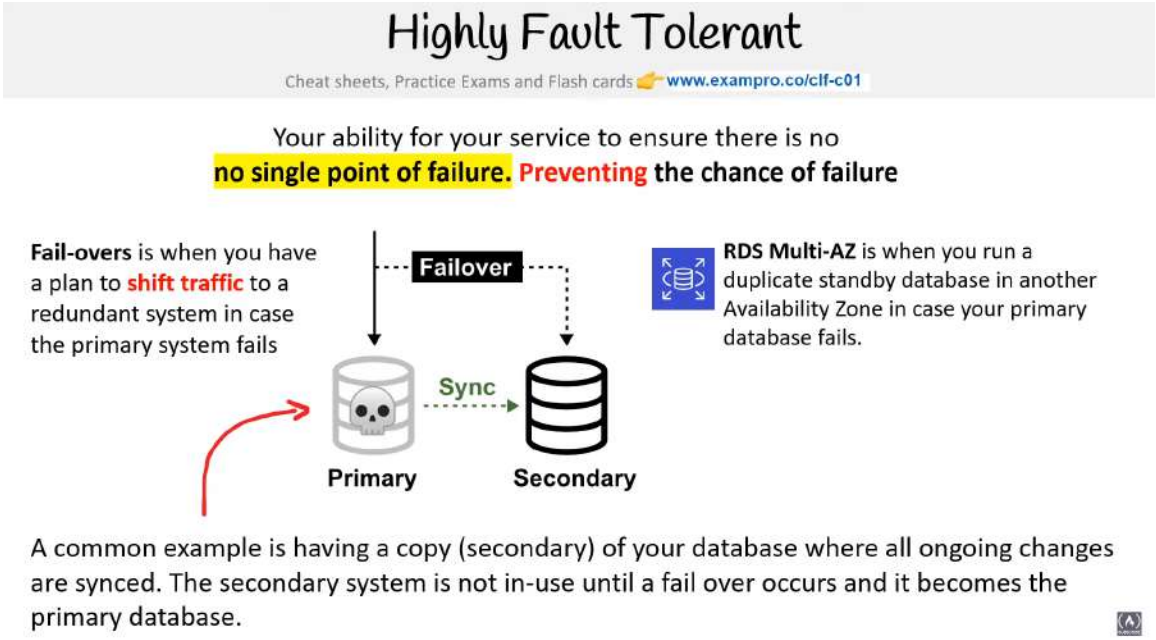
▼ 3. What is high scalability



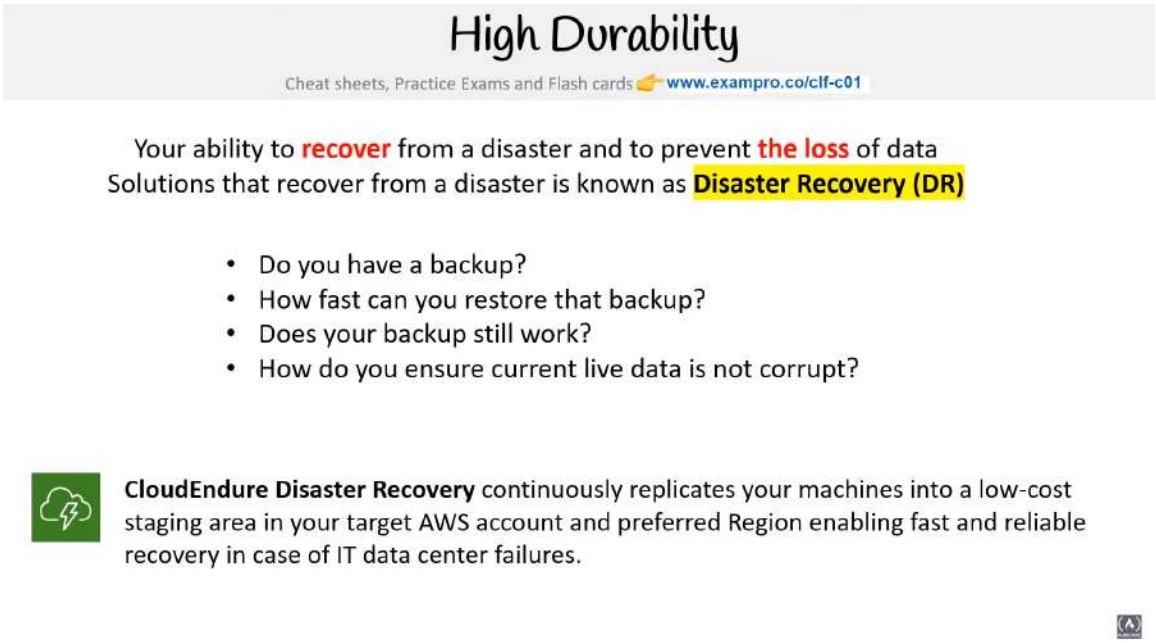
▼ 4. What is high elasticity



▼ 5. What is high fault tolerance



▼ 6. What is high durability

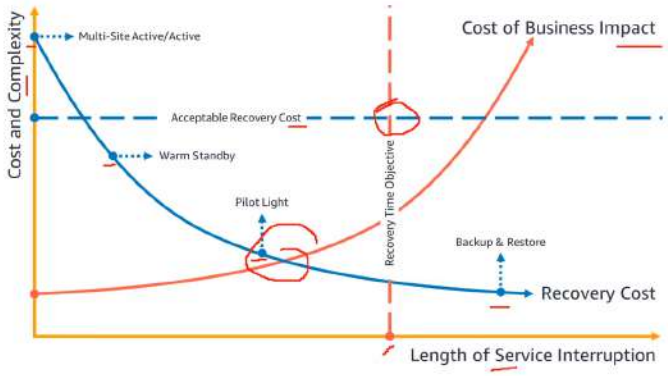


▼ 7. Recovery Time Objective (RTO)

RTO

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Recovery Time Objective (RTO) is the maximum acceptable delay between the interruption of service and restoration of service. This objective determines what is considered an acceptable time window when service is unavailable and is defined by the organization.

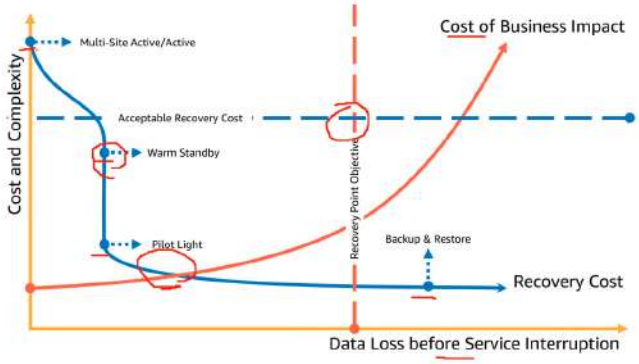


▼ 8. Recovery Point Objective (RPO)

RPO

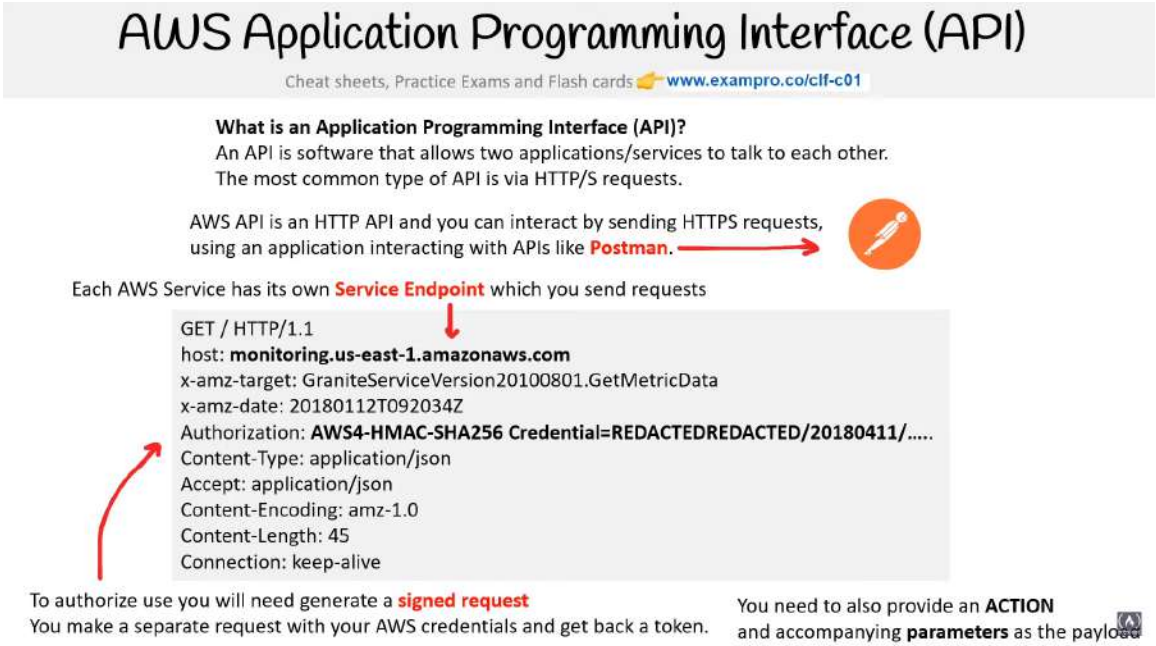
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Recovery Point Objective (RPO) is the maximum acceptable amount of time since the last data recovery point. This objective determines what is considered an acceptable loss of data between the last recovery point and the interruption of service and is defined by the organization.

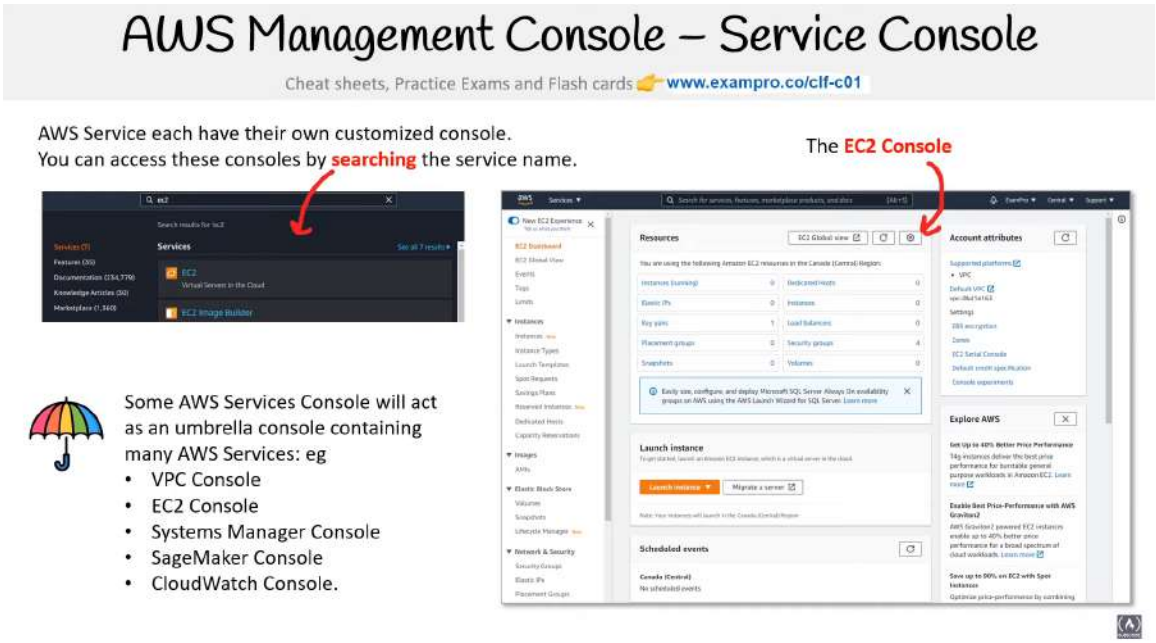


▼ 6. Management and AWS Tools

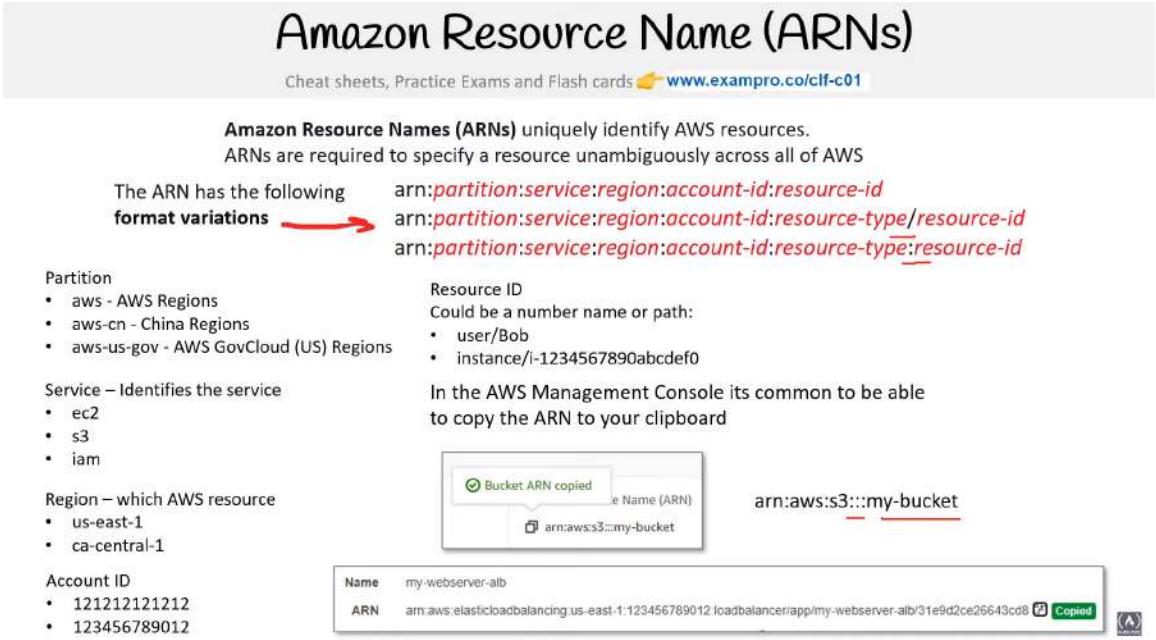
▼ 1. AWS API



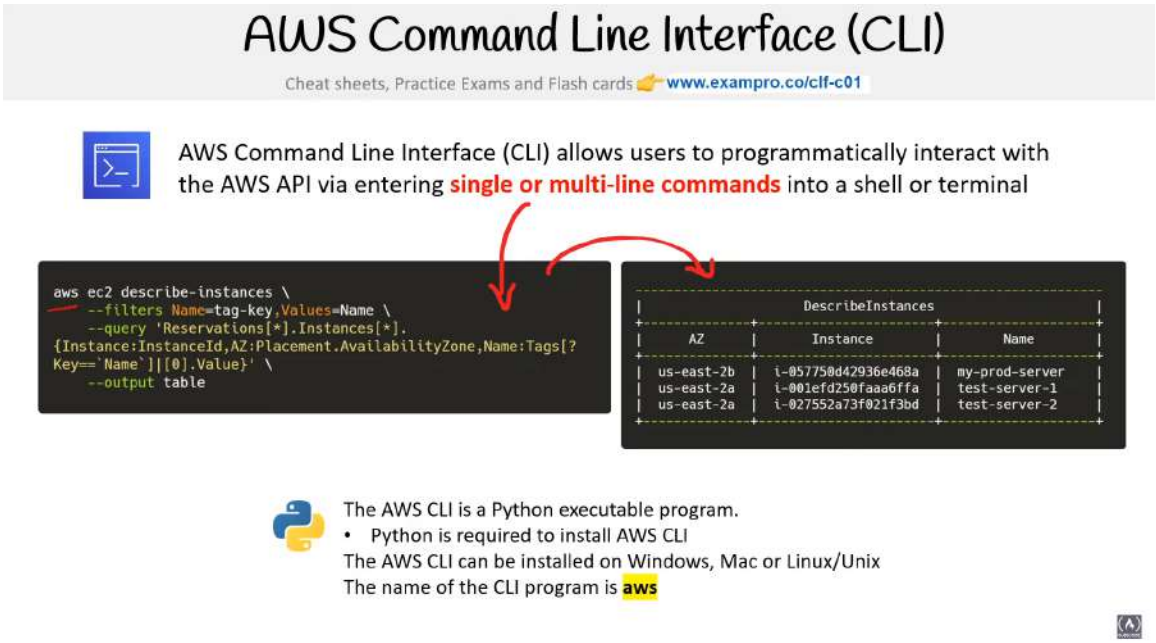
▼ 2. Service Console



▼ 3. Amazon Resource Name

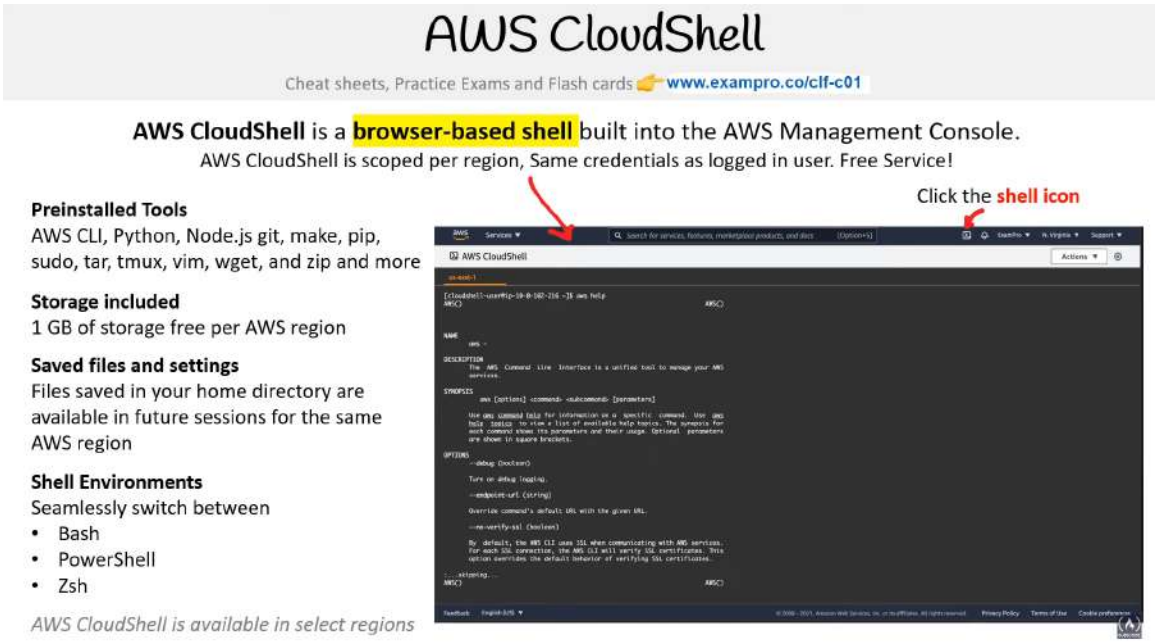


▼ 4. AWS Command Line Interface (CLI)

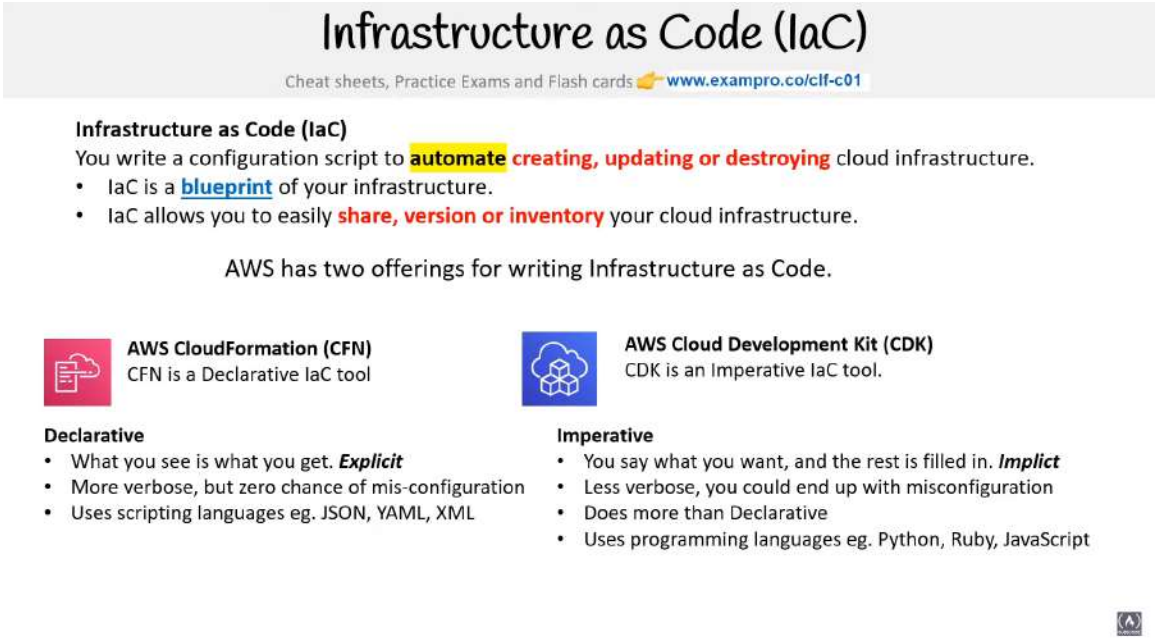


▼ 5. AWS SDK

▼ 6. AWS Cloud Shell

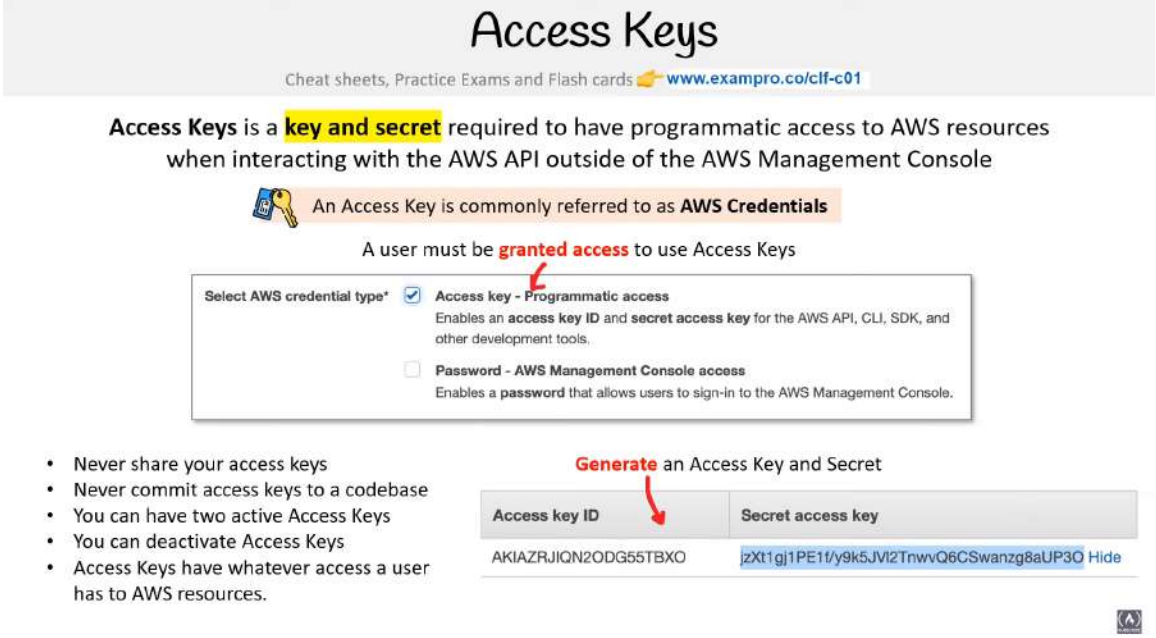


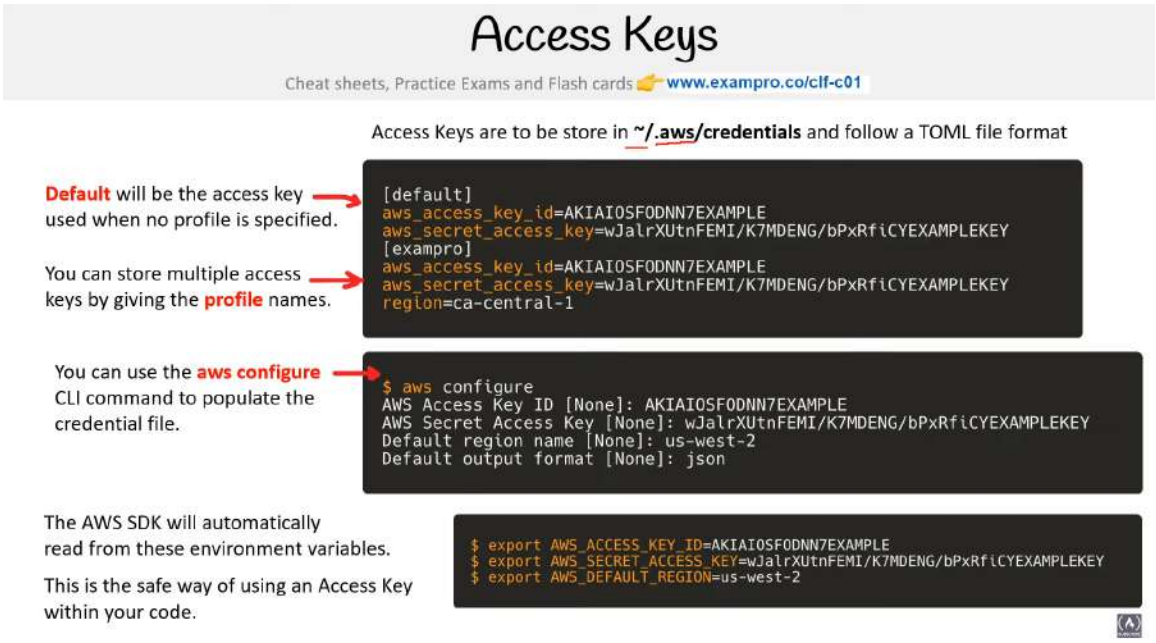
▼ 7. Infrastructure as Code (IaC)



▼ 8. Cloud Development Kit (CDK)

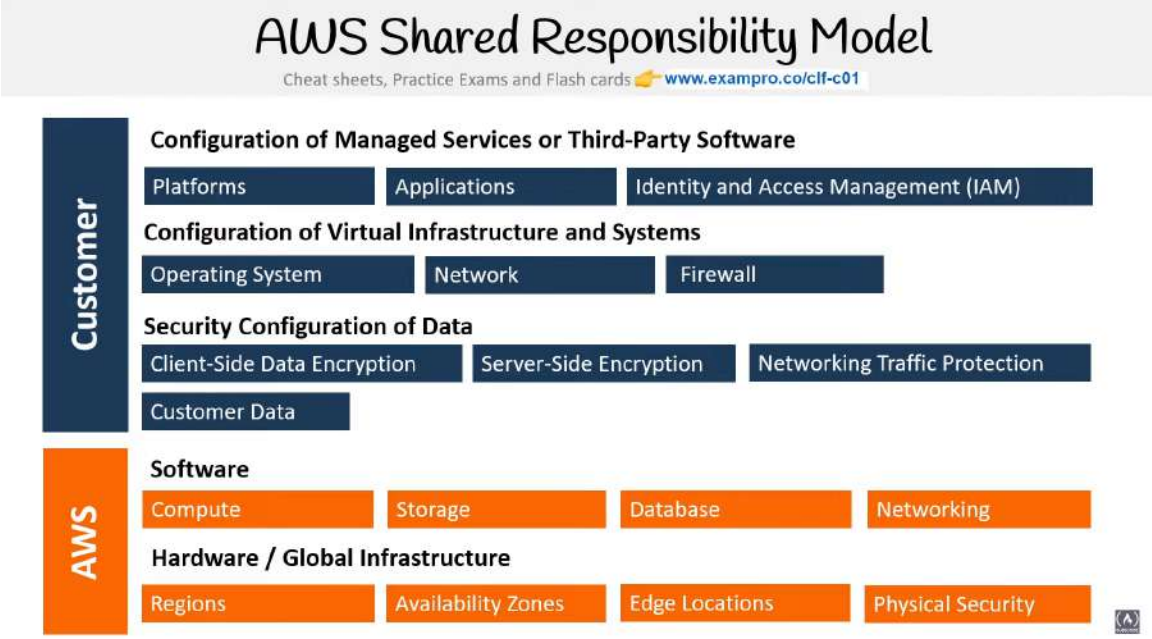
▼ 9. Access Keys

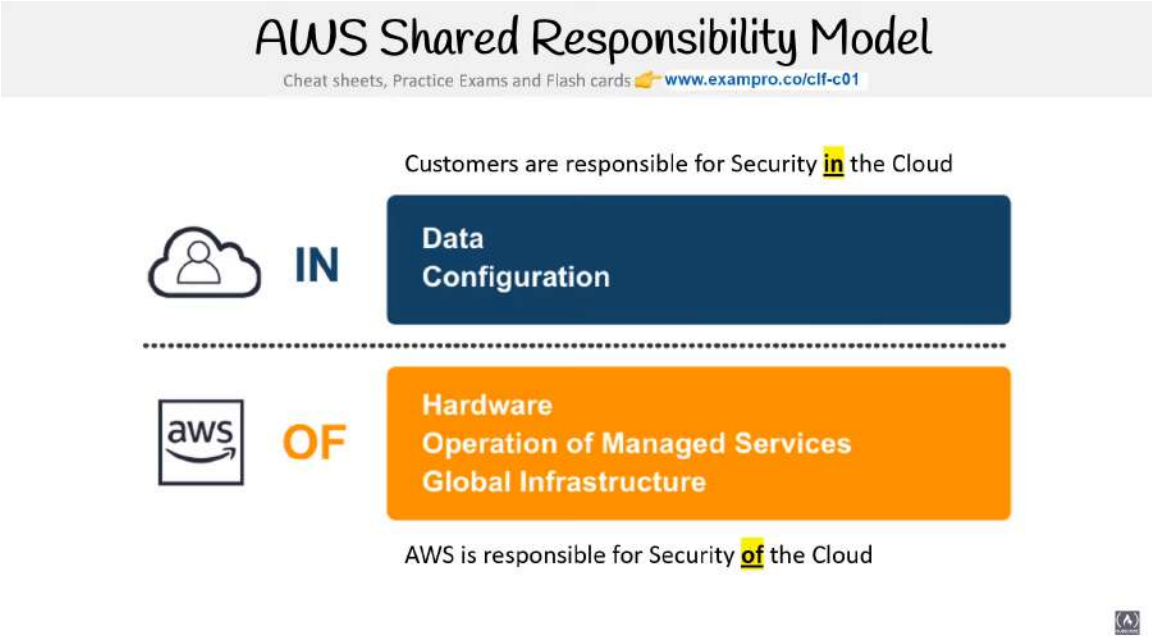




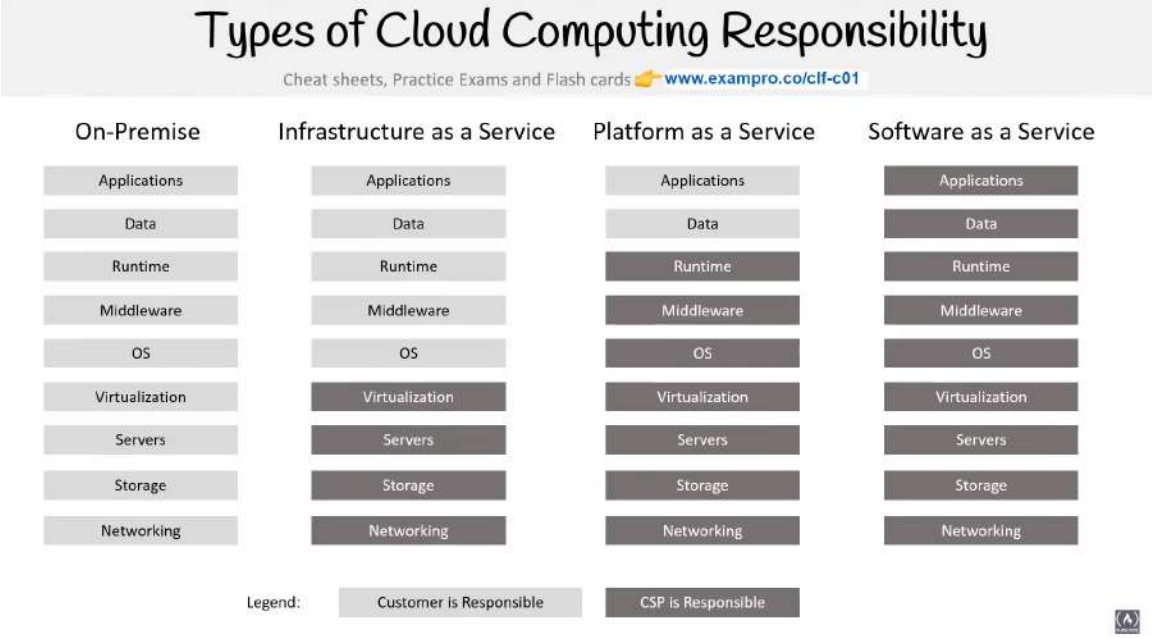
▼ 7. Shared Responsibility Model

▼ 1. What is Shared Responsibility Model

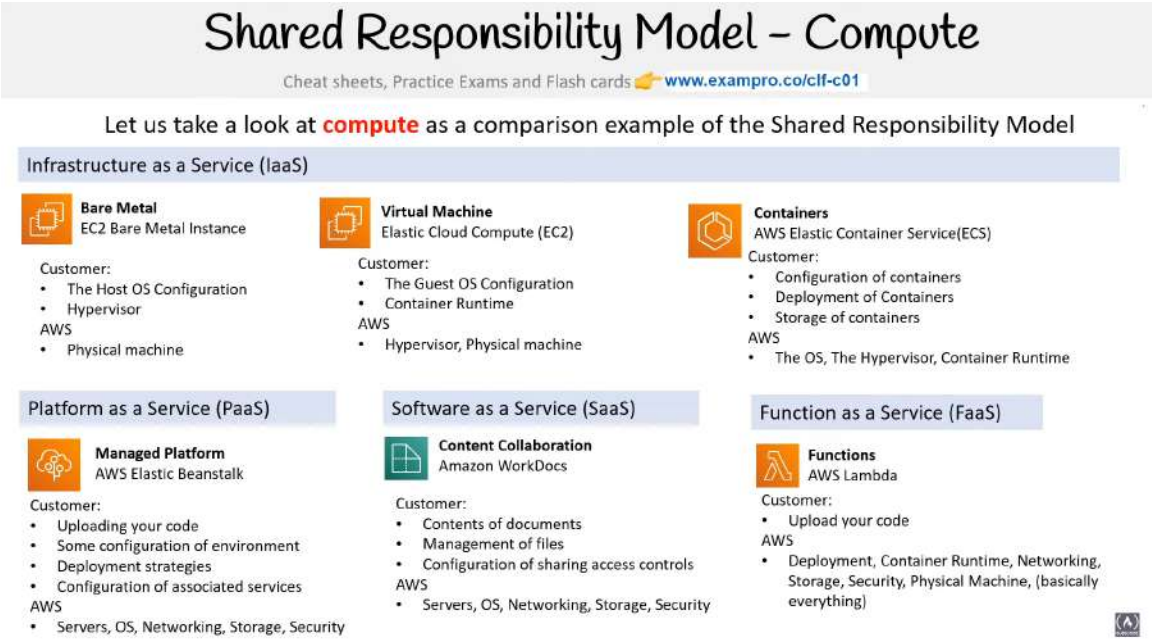




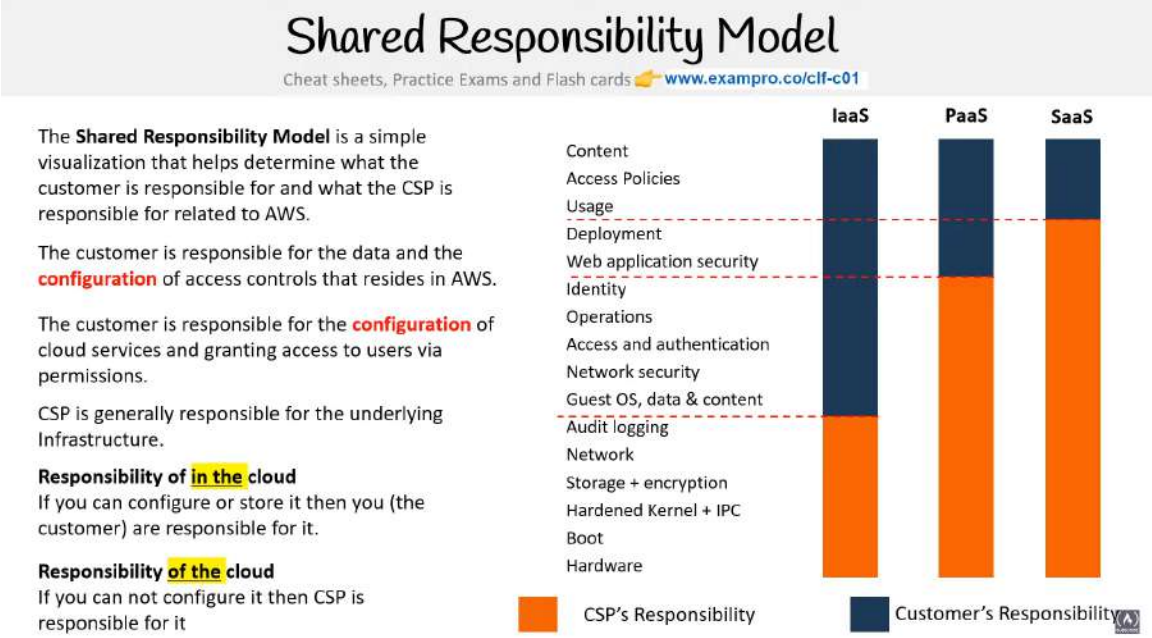
▼ 2. Types of Cloud Computing Responsibility



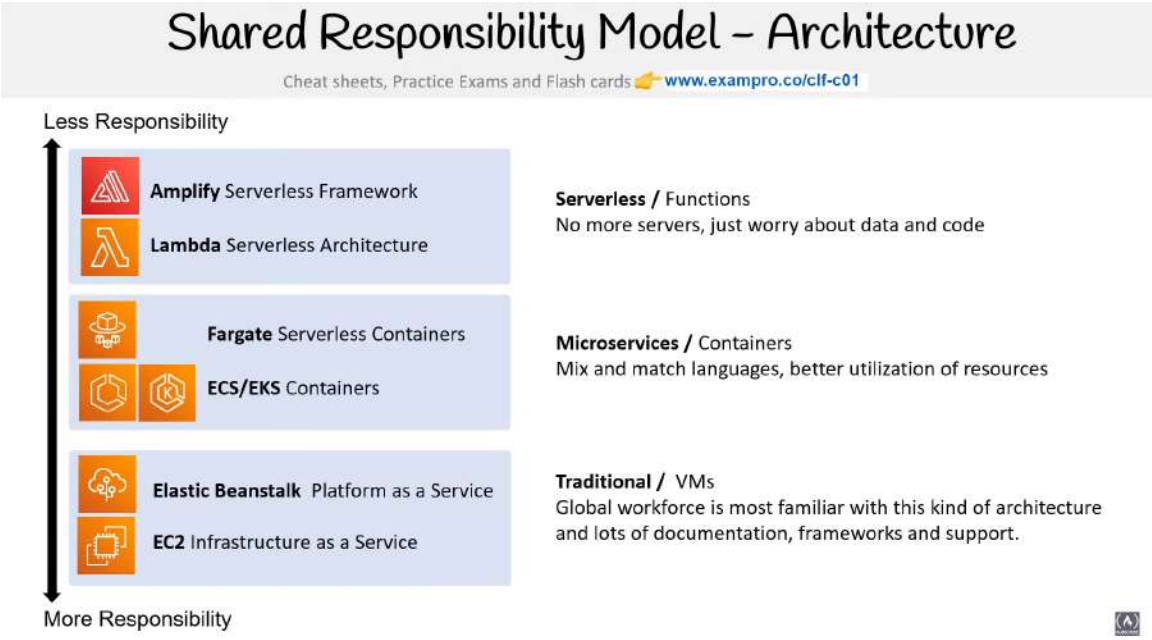
▼ 3. Shared Responsibility Model Compute



▼ 4. Shared Responsibility Model for IaaS, Paas and Saas

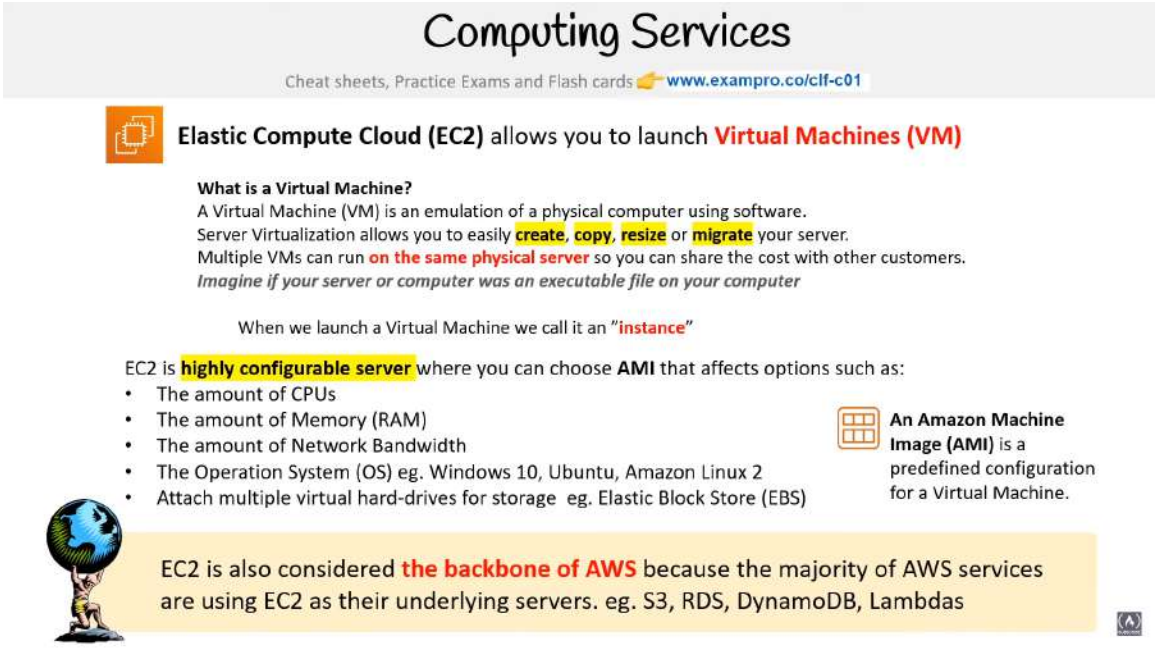


▼ 5. User responsibility level on AWS Server/ function.

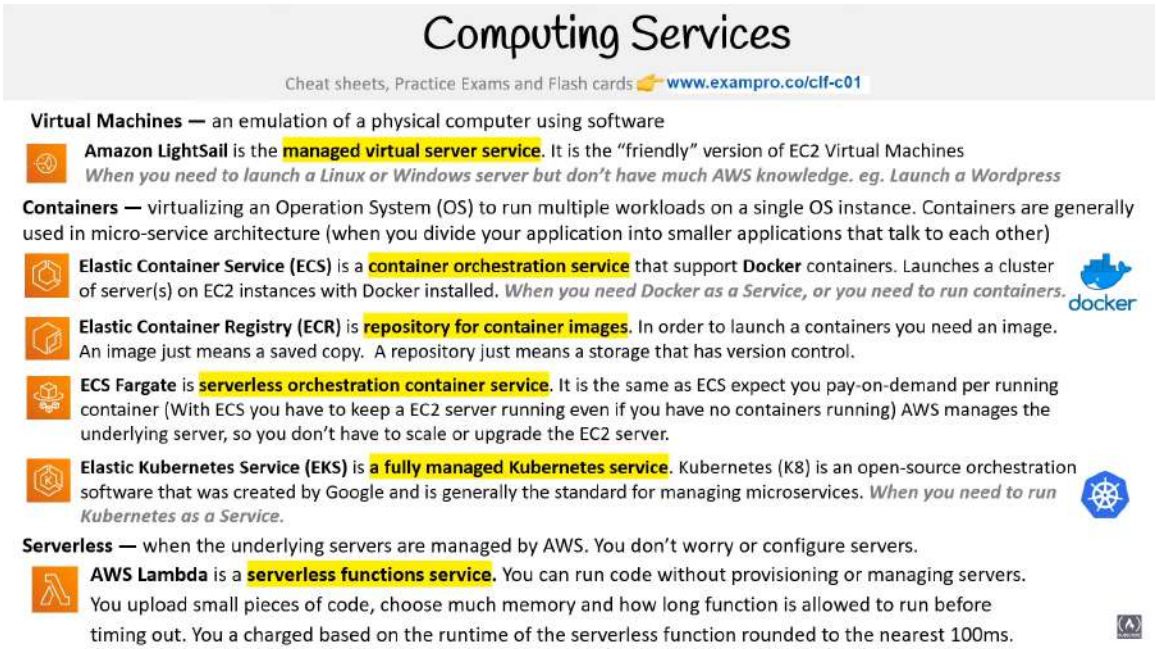


▼ 8. Compute

▼ 1. EC2 Overview



▼ 2. Computing Services



▼ 3. High Computing Services

Higher Performance Computing Services

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

The Nitro System A combination of **dedicated hardware and lightweight hypervisor** enabling faster innovation and enhanced security. All new EC2 instance types use the Nitro System.

- Nitro Cards — specialized cards for VPC, EBS and Instance Storage and controller card
- Nitro Security Chips — Integrated into motherboard. Protects hardware resources.
- Nitro Hypervisor — lightweight hypervisor Memory and CPU allocation Bare Metal-like performance

Bare Metal Instance You can launch EC2 instance that have no hypervisor so you can run workloads directly on the hardware for maximum performance and control. The **M5 and R5** EC2 instances run are bare metal.

Bottlerocket is a Linux-based open-source operation system that is purpose-built by AWS for running containers on Virtual Machines or bare metal hosts

What is High Performance Computing (HPC)?
A cluster of hundreds of thousands of servers with fast connections between each of them with the purpose of boosting computing capacity.
When you need a supercomputer to perform computational problems too large to run on a standard computers or would take to long.

AWS ParallelCluster is an **AWS-supported open source cluster management tool** that makes it easy for you to deploy and manage High Performance Computing (HPC) clusters on AWS.

▼ 4. Edge and Hybrid Computing Services

Edge and Hybrid Computing Services

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is Edge Computing?
When you push your computing workloads outside of your networks to run close to the destination location.
eg. Pushing computing to run on phones, IoT Devices, or external servers not within your cloud network.

What is Hybrid Computing?
When you're able to run workloads on both your on-premise datacenter and AWS Virtual Private Cloud (VPC)

AWS Outposts is **physical rack of servers** that you can put in your data center. AWS Outposts allows you to use AWS API and Services such as EC2 right in your datacenter.

verizon vodafone business

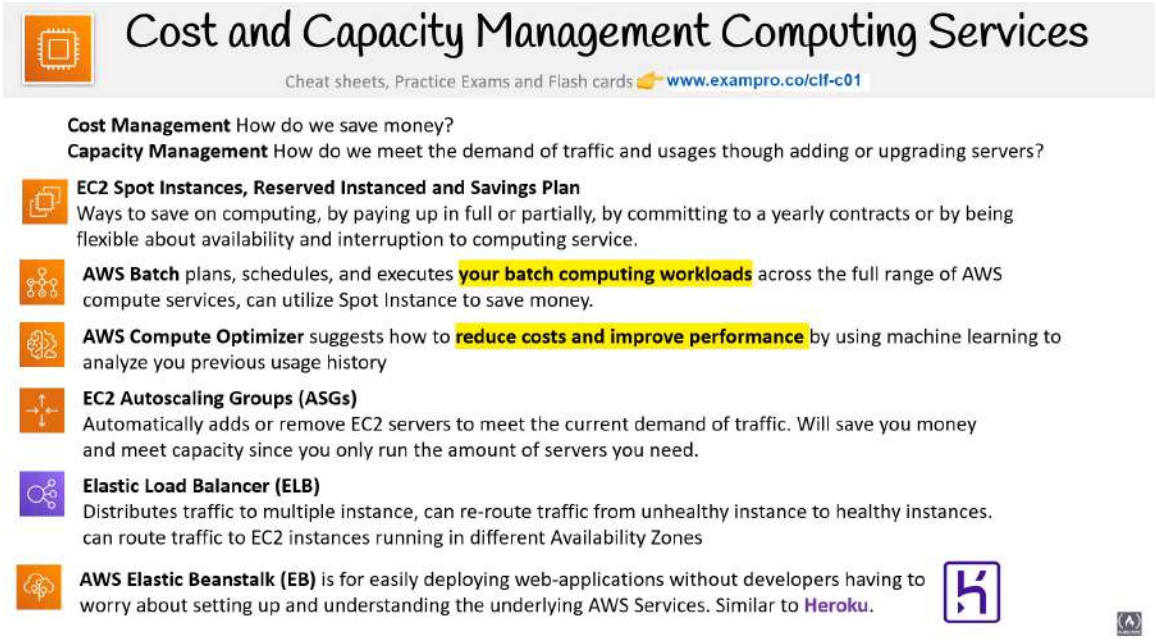
AWS Wavelength allows you **to build and launch your applications in a telecom datacenter**. By doing this your applications with have ultra-low latency since they will be pushed over a the **5G network** and be closest as possible to the end user.

VMWare Cloud on AWS allows you to **manage on-premise virtual machines using VMWare** as EC2 instances. The data-center must being using VMWare for Virtualization.

vmware vSphere

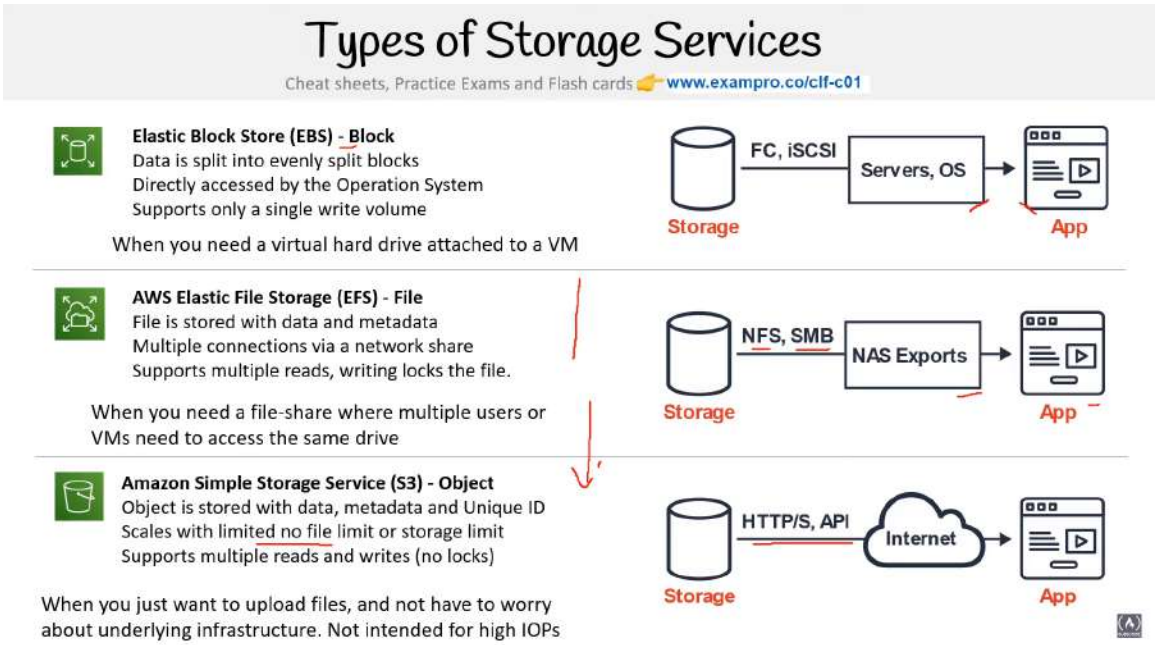
AWS Local Zones are **edge datacenters located outside of an AWS region** so you can use AWS closer to end destination.
When you need faster computing, storage and databases in populated areas that are outside of an AWS Region

▼ 5. Cost and Capacity Management

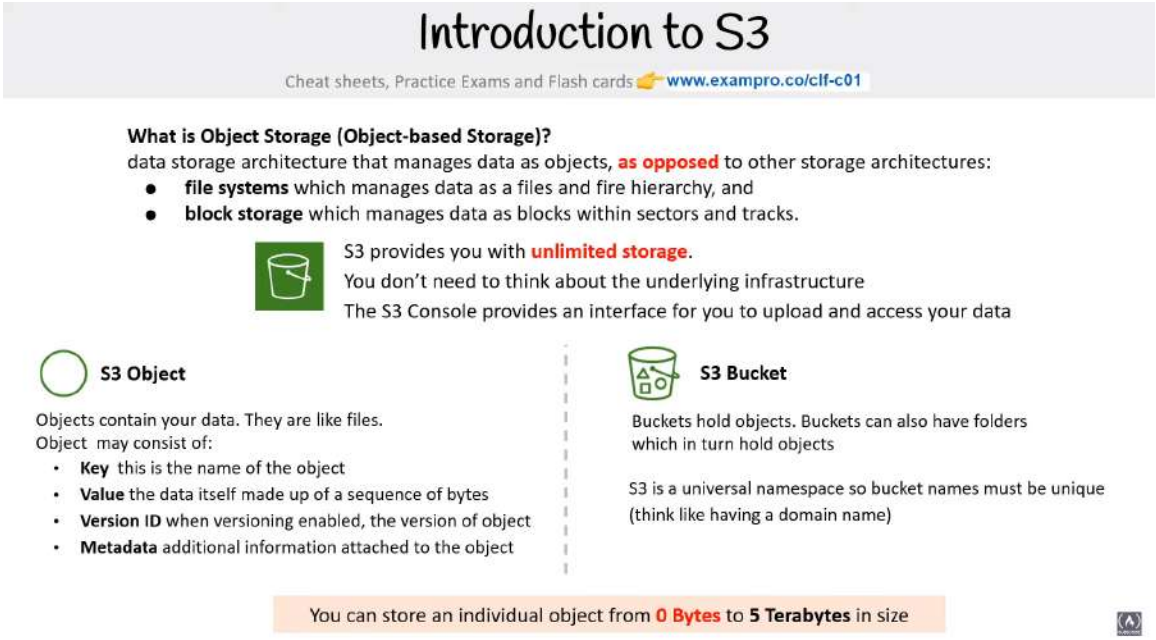


▼ 9. Storage

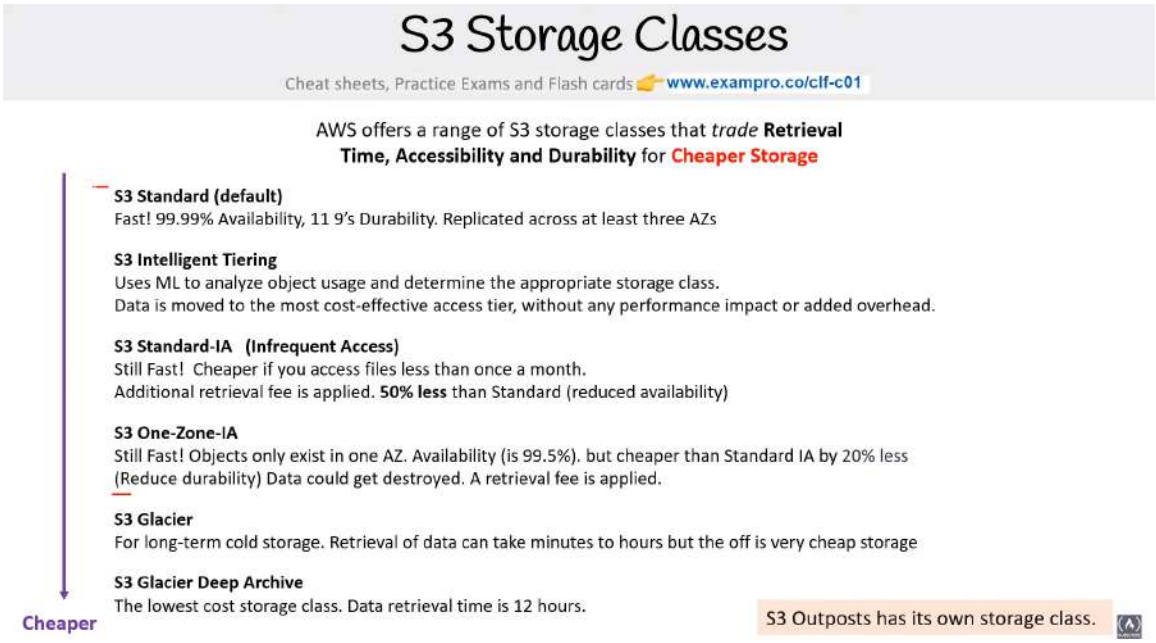
▼ 1. Types of Storage Services



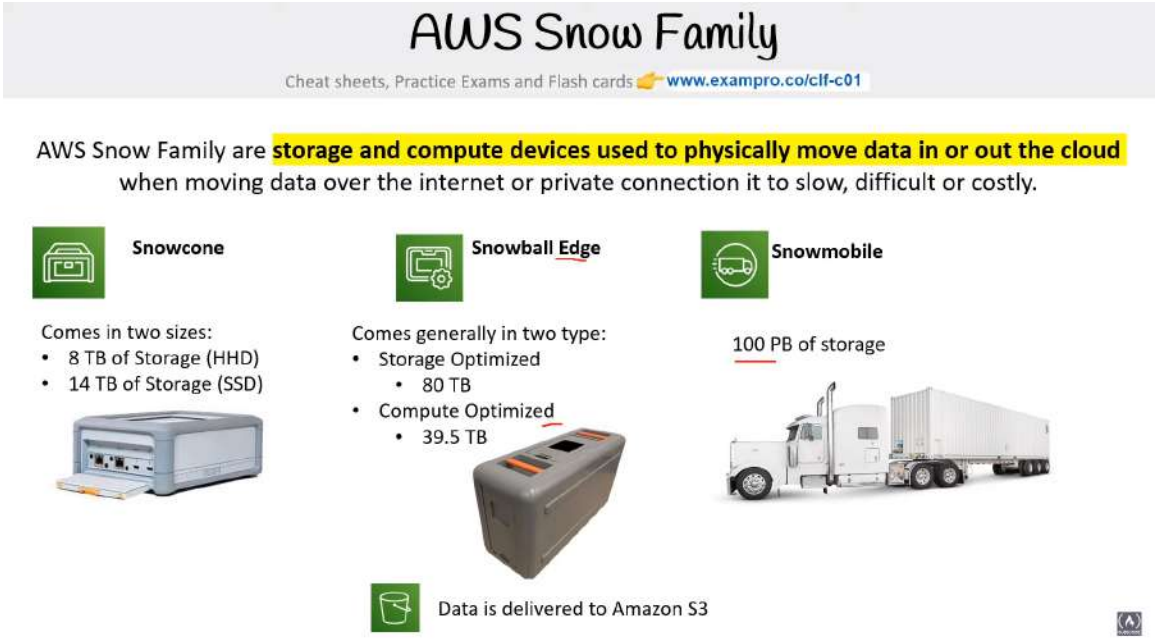
▼ 2. What is S3



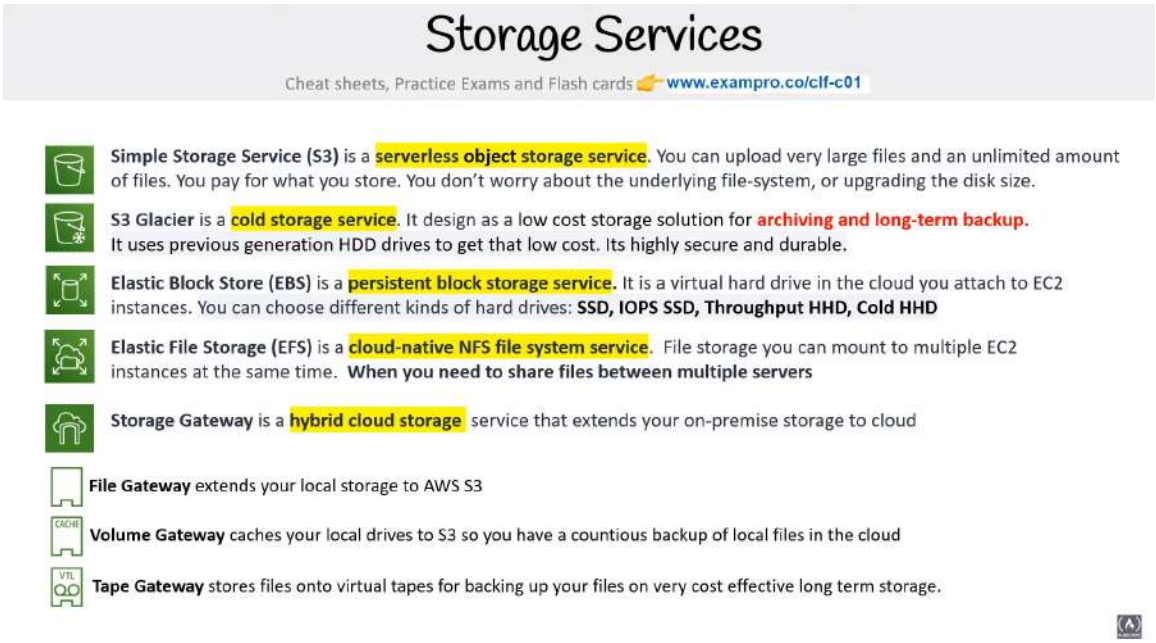
▼ 3. S3 Storage Classes



▼ 4. AWS Snow Family



▼ 5. Storage Services



▼ 10. Database

▼ 1. Data Warehouse

What is Data Warehouse?

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

A relational datastore designed for **analytic workloads**, which is generally **column-oriented data-store**

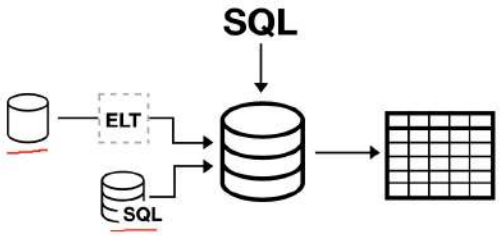
Companies will have **terabytes and millions of rows of data**, and they need a fast way to be able to produce analytics reports

Data warehouses generally perform **aggregation**

- aggregation is grouping data eg. find a total or average
- Data warehouses are optimized around columns since they need to quickly aggerate column data

Data warehouses are generally designed be HOT

- Hot means they can return queries very fast even though they have vast amounts of data



Data warehouses are infrequently accessed meaning they aren't intended for real-time reporting but maybe once or twice a a day or once a week to generate business and user reports.

A data warehouse needs to consume data from a relational databases on a regular basis.

▼ 2. Key/Value Store

What is a Key / Value store?

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

A **key-value database** is a type of non-relational database (NoSQL) that uses a simple key-value method to store data.

A key/value stores a **unique key** alongside a value

Key	Value
Data	10101010001010110010100101010 01
Worf	01101011000101010101011100010
Ro Laren	00101010010101100101010101010

Key values stores are **dumb and fast**. They generally lack features like:

- Relationships
- Indexes
- Aggregation

Key	Value
Data	{species: android, rank: 'lt commander' }
Worf	{species: klingon, rank: 'lt commander' }
Ro Laren	{species: bajoran, affiliation: 'maquis'}

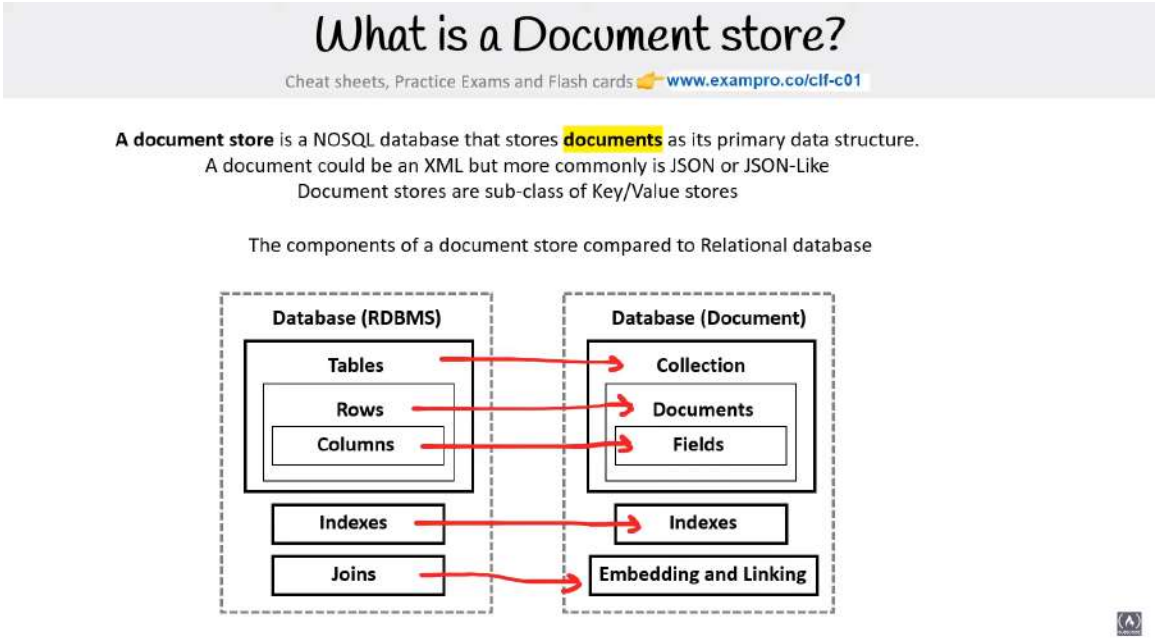
A simple key/value store will interpret this data resembling a dictionary (aka Associative arrays or hash)

A key/value store can resemble tabular data, it does not have to have the consistent columns per row (hence its schemaless)

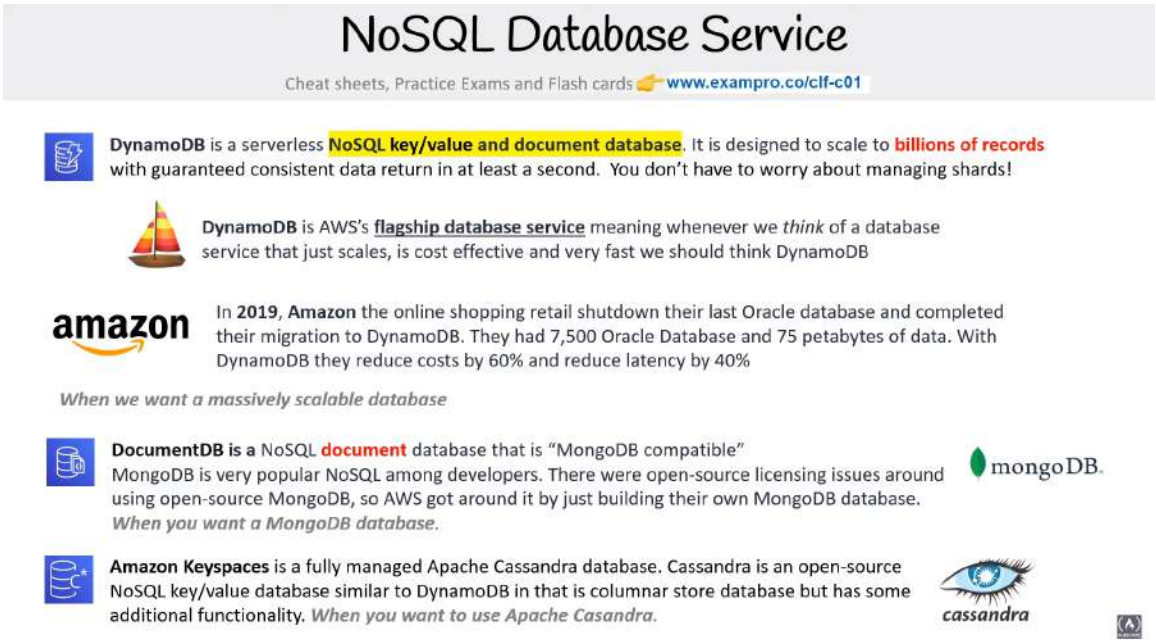
Key (Name)	Species	Rank	Affiliation
Data	andriod	Lt commander	
Worf	klingon	Lt commander	
Ro Laren	bajoran		maquis

Due to their simple design they can scale well beyond a relational database

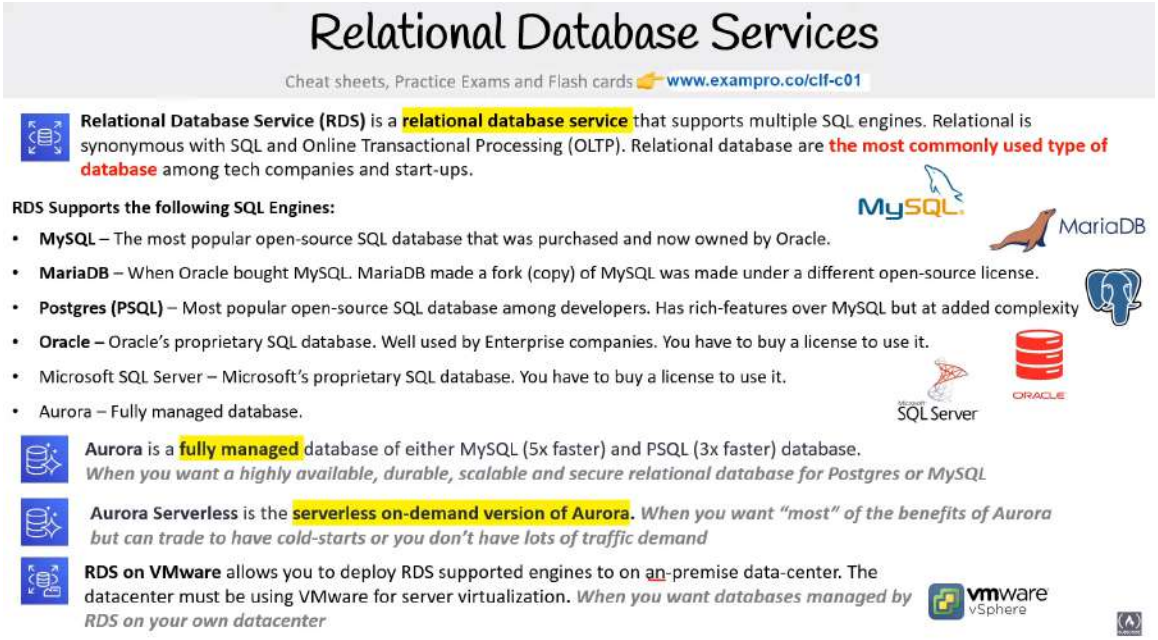
▼ 3. Document Store



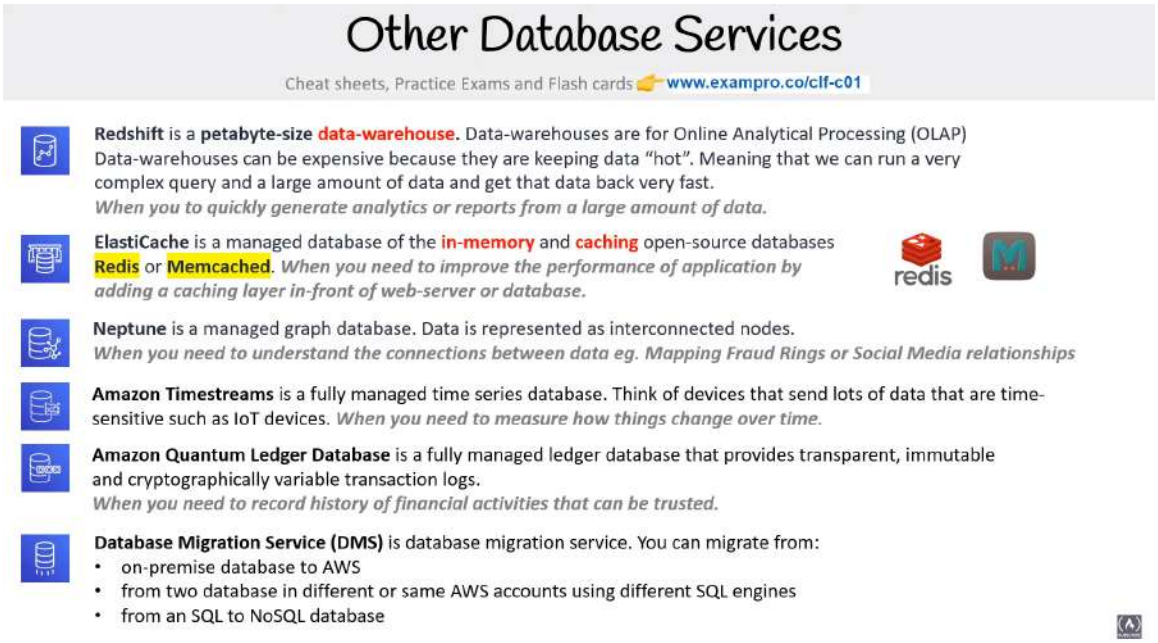
▼ 4. No SQL Database Service



▼ 5. Relational Database Services

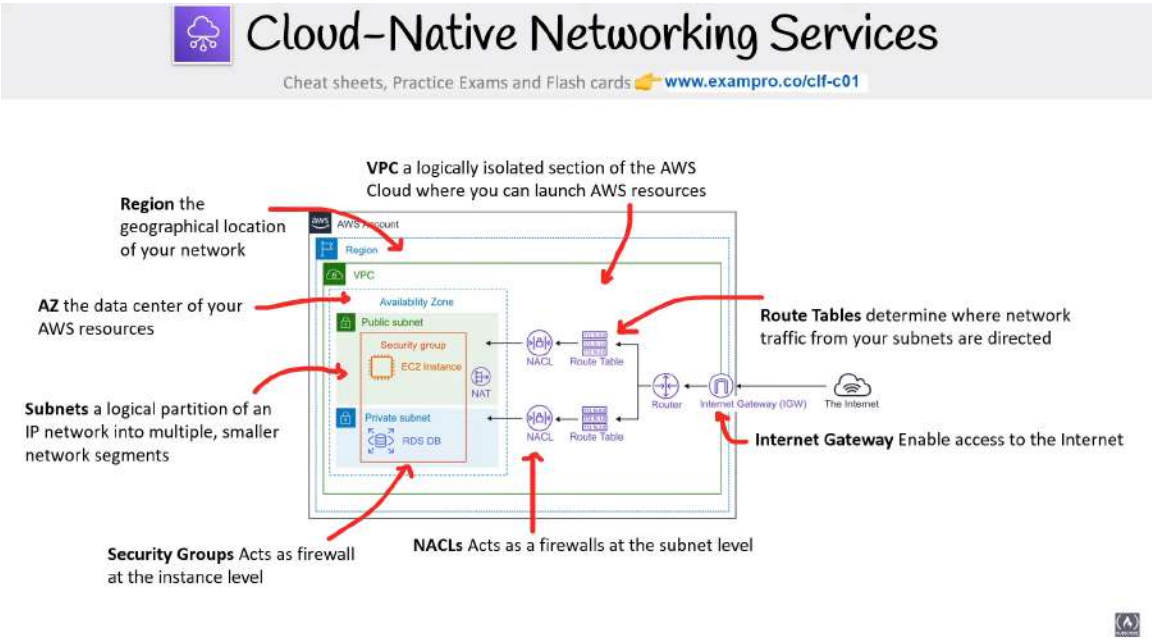


▼ 6. Other Database Services

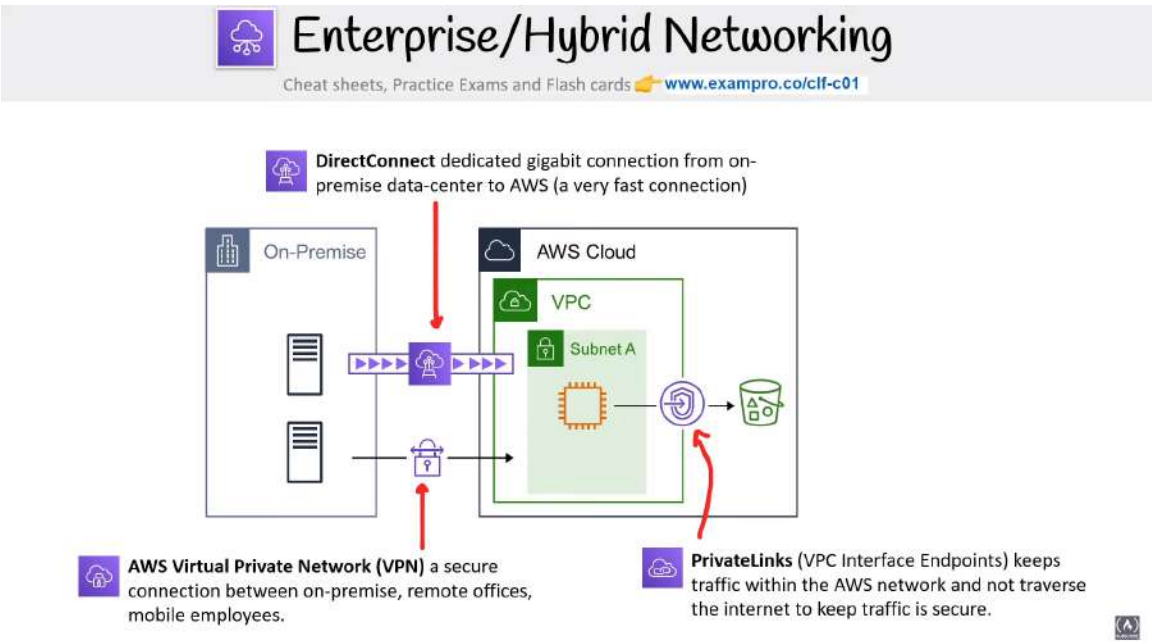


▼ 11. Networking

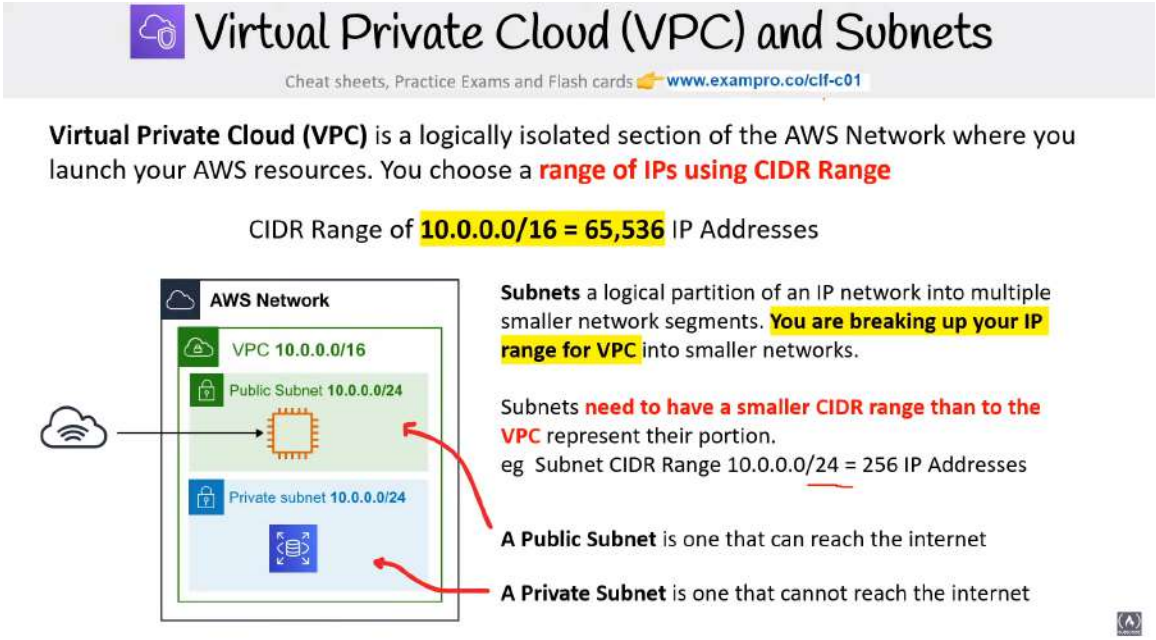
▼ 1. Cloud Native Networking Services



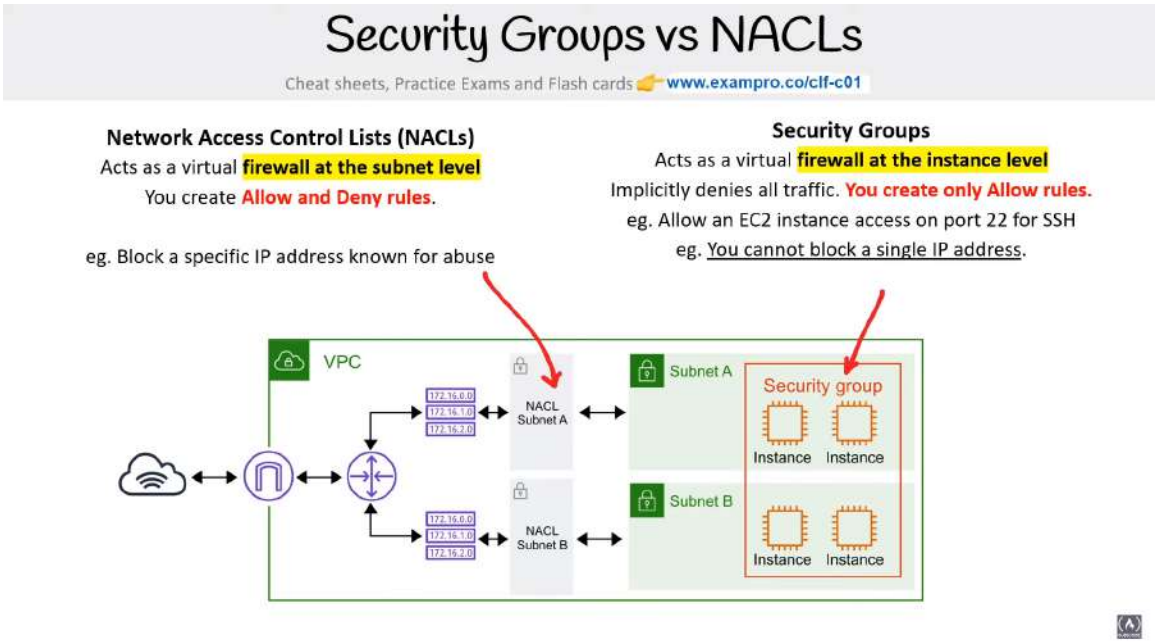
▼ 2. Enterprise/Hybrid Networking



▼ 3. VPC and Subnets

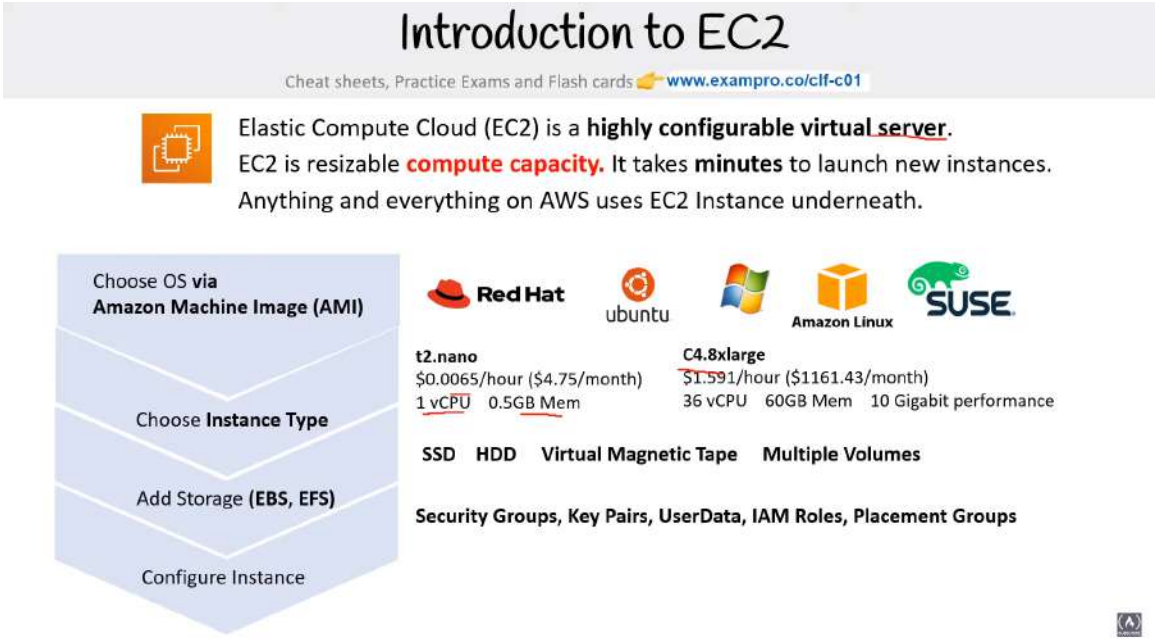


▼ 4. Security Group vs NACL

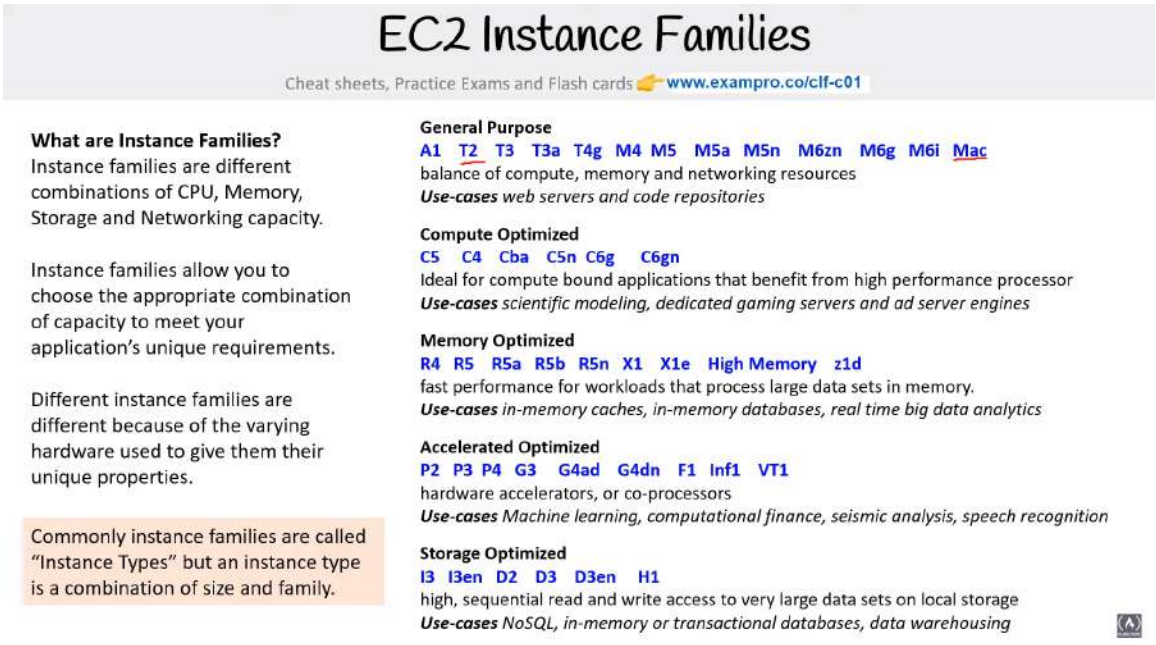


▼ 12. EC2

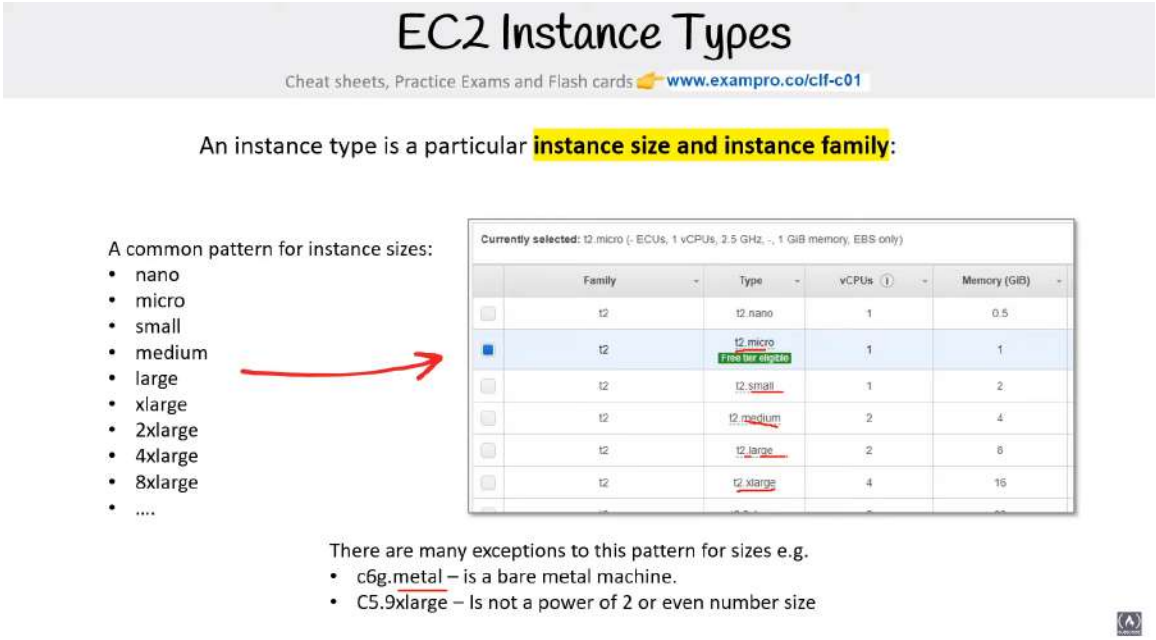
▼ 1. Introduction to EC2



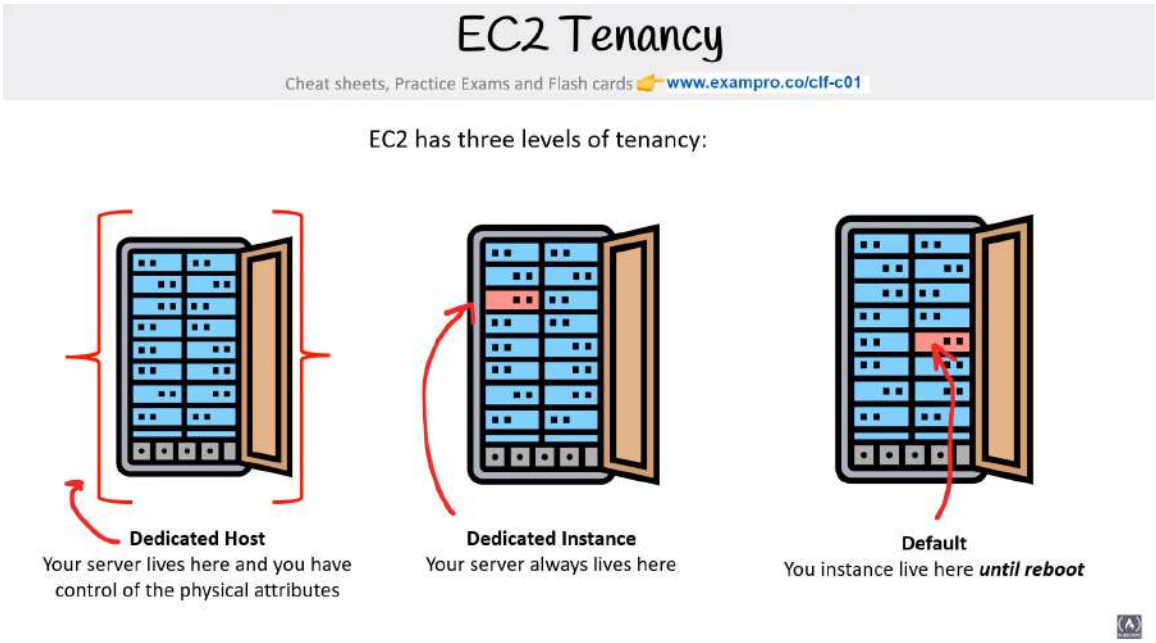
▼ 2. EC2 Instance Families



▼ 3. EC2 Instance Types

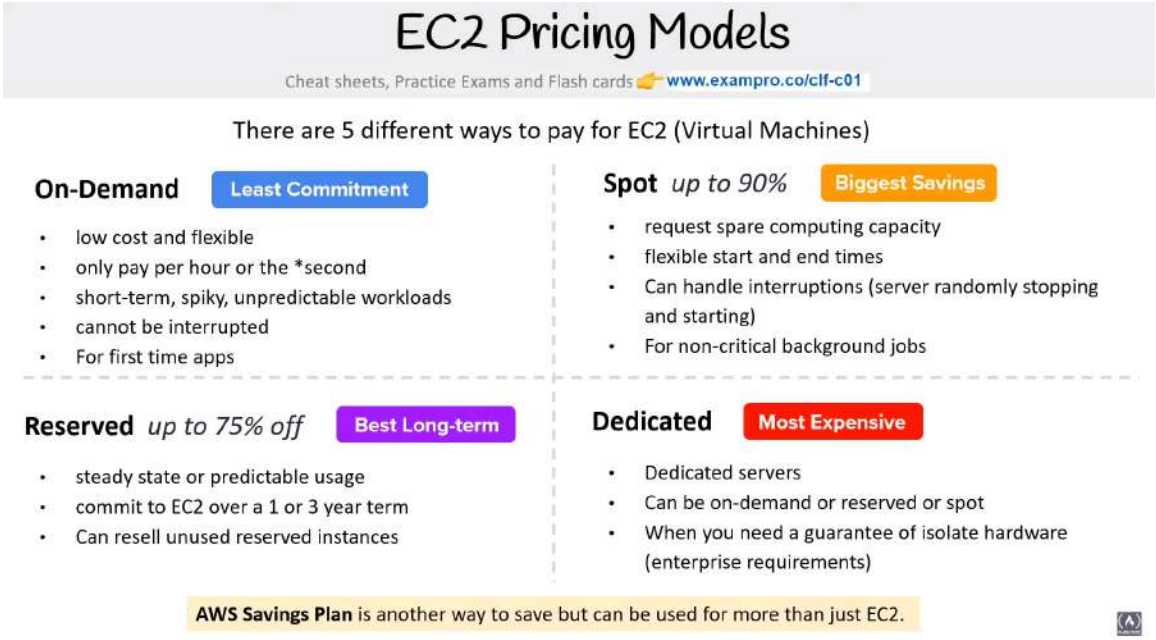


▼ 4. EC2 Tenancy

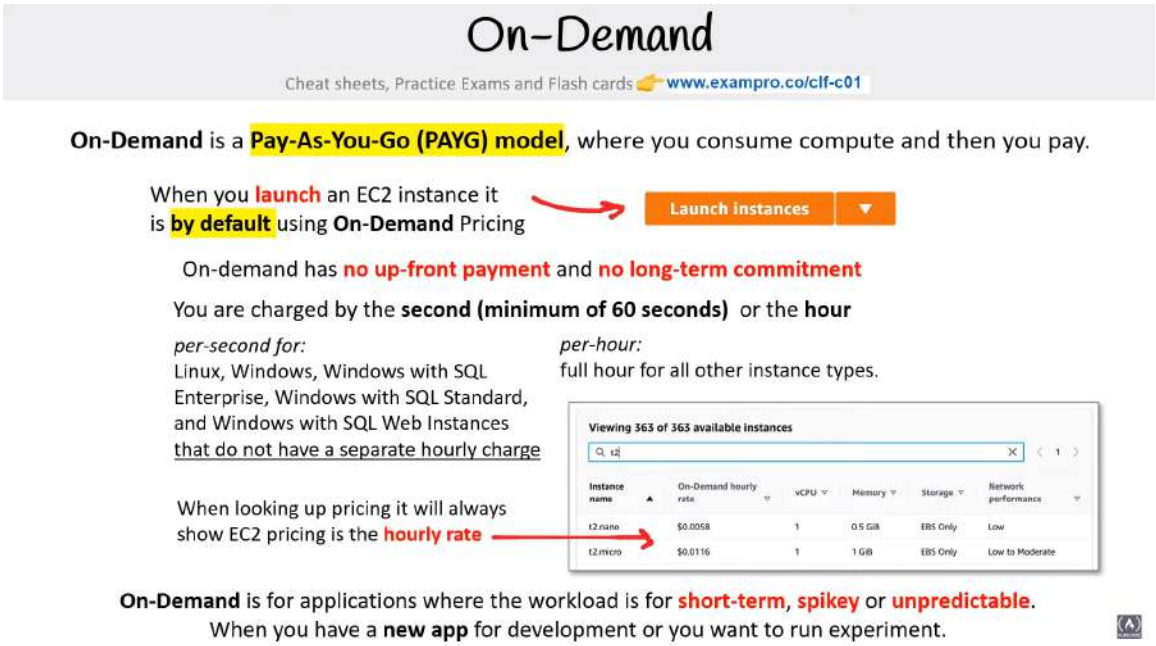


▼ 13. EC2 Pricing Model

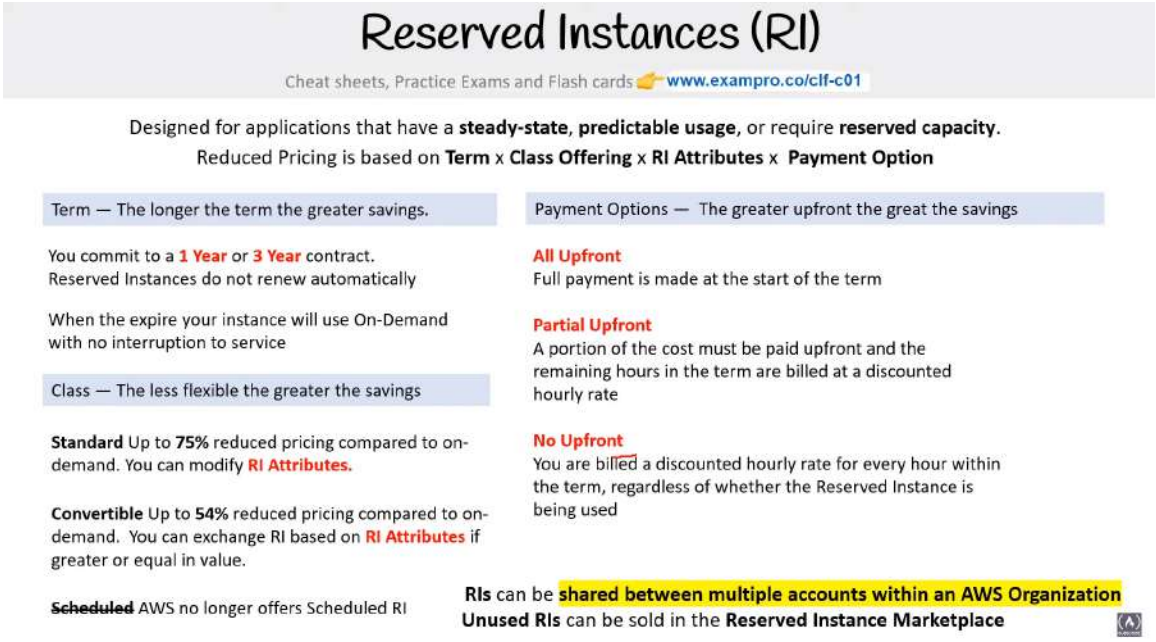
▼ 1. EC2 Pricing Model



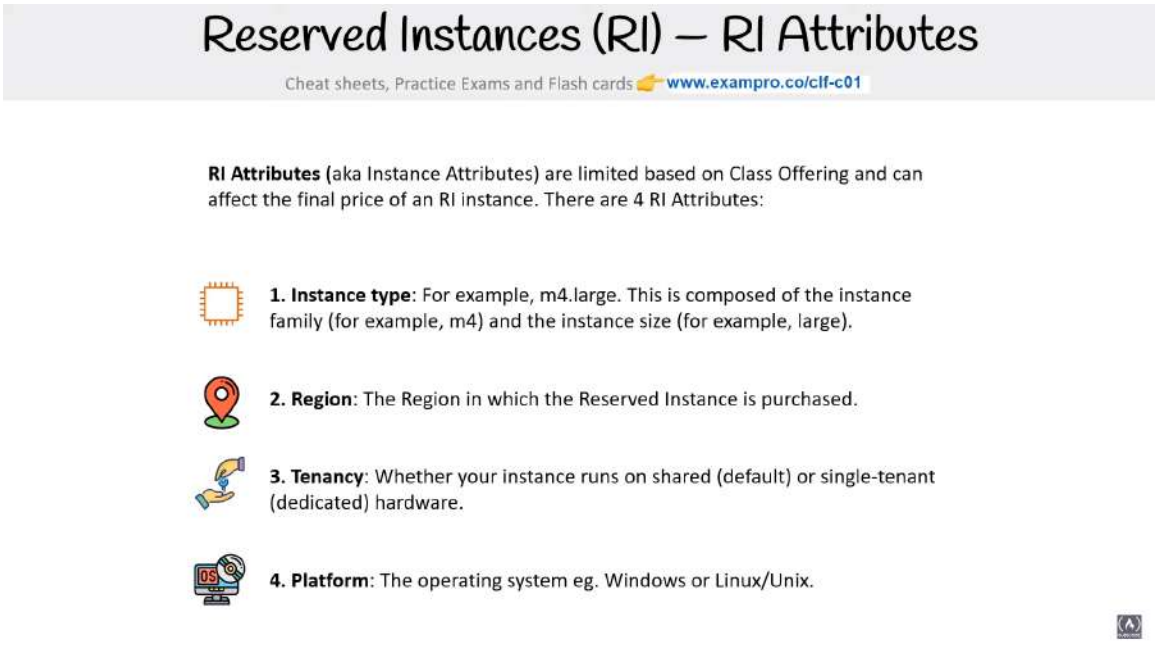
▼ 2. On Demand



▼ 3. Reserved Instance



▼ 4. Reserved Instance Attributes



▼ 5. RI Limits

RI Limits

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

There is a limit to the number of Reserved Instances that you can purchase per month.

Per month you can purchase
- **20** Regional Reserved Instances *per Region*
- **20** Zonal Reserved Instances *per AZ*

Regional Limits
You cannot exceed your running On-Demand Instance limit by purchasing regional Reserved Instances.
The default On-Demand Instance limit is 20.

Before purchasing RI ensure your On-Demand limit is equal to or greater than your RI you intend to purchase

Zonal Limits
You can exceed your running On-Demand Instance limit by purchasing zonal Reserved Instances

If you already have 20 running On-Demand Instances, and you purchase 20 zonal Reserved Instances, you can launch a further 20 On-Demand Instances that match the specifications of your zonal Reserved Instances

▼ 6. Standard vs Convertible RI

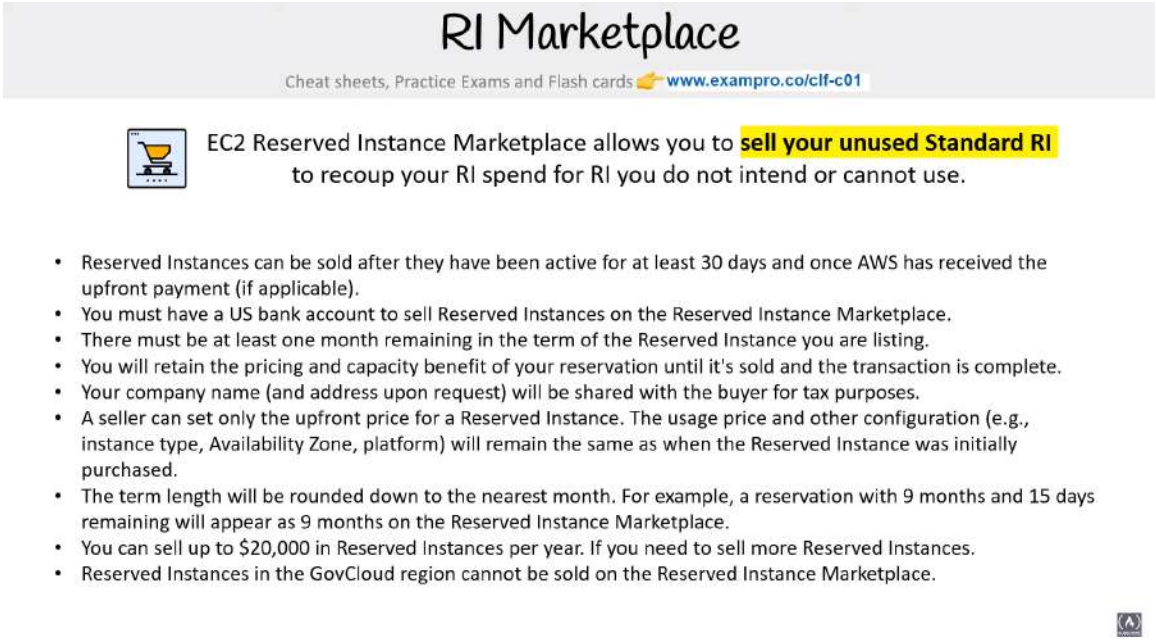
Standard vs Convertible RI

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

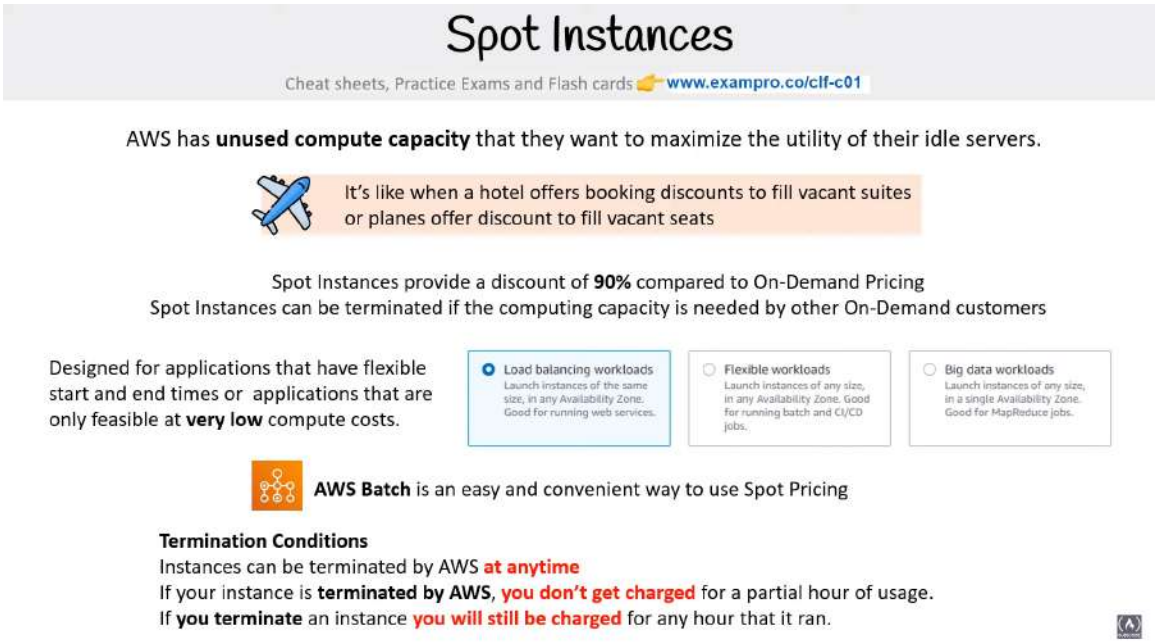
There are some key difference between Standard and Convertible

Standard RI	Convertible RI
RI attributes can be modified • Change the AZ within same Region • Change the scope of the Zonal RI to Regional RI or visa versa • Change the instance size (Linux/Unix only, default tenancy) • Change network from Ec2-Classic to VPC and visa-versa	RI attributes can't be modified (you perform an exchange)
Can't be exchanged	Can be exchanged during the term for another Convertible RI with new RI attributes, including: • instance family • instance type • platform • scope • tenancy
Can be bought or sold in the RI Marketplace	Can't be bought or sold in the RI Marketplace

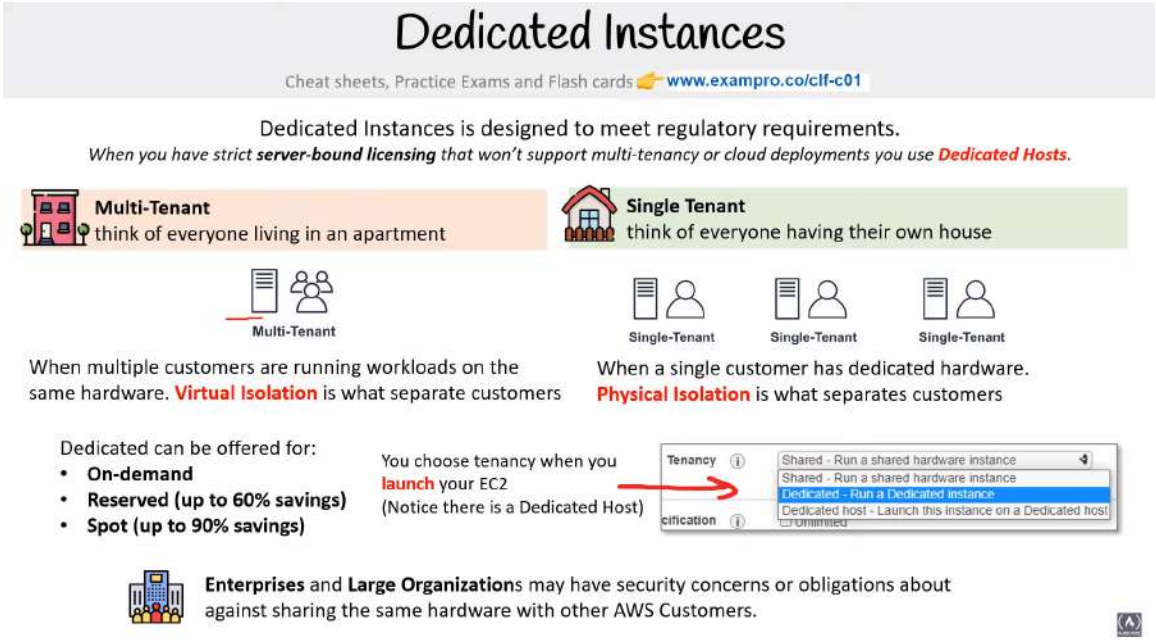
▼ 7. RI MarketPlace



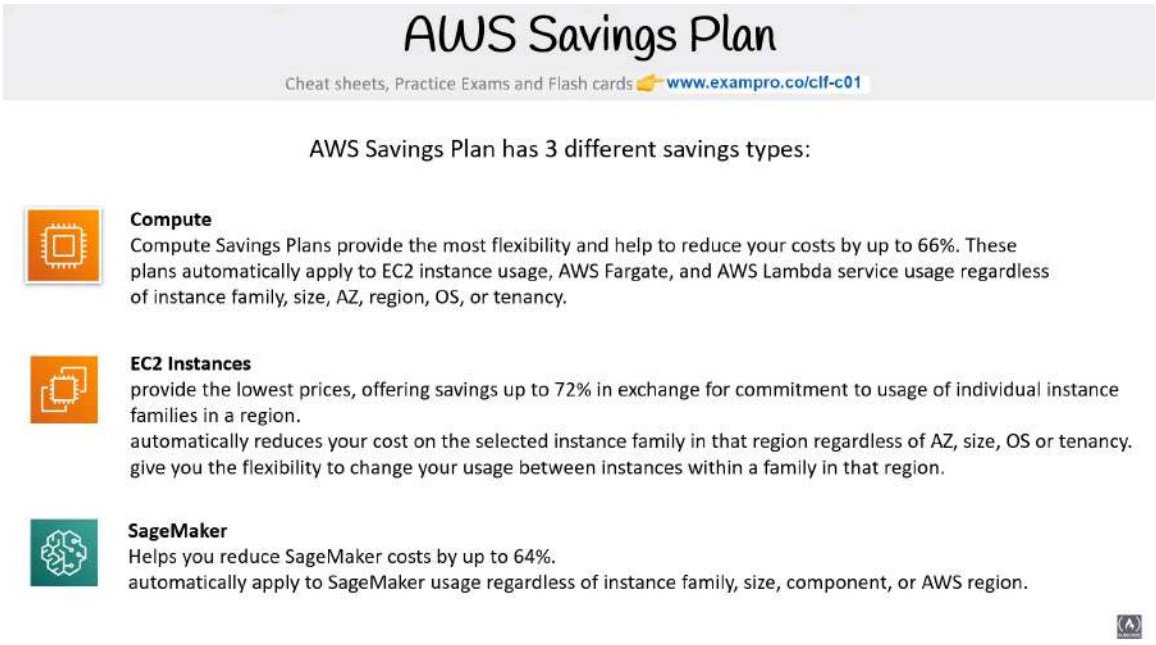
▼ 8. Spot Instances



▼ 9. Dedicated Instances

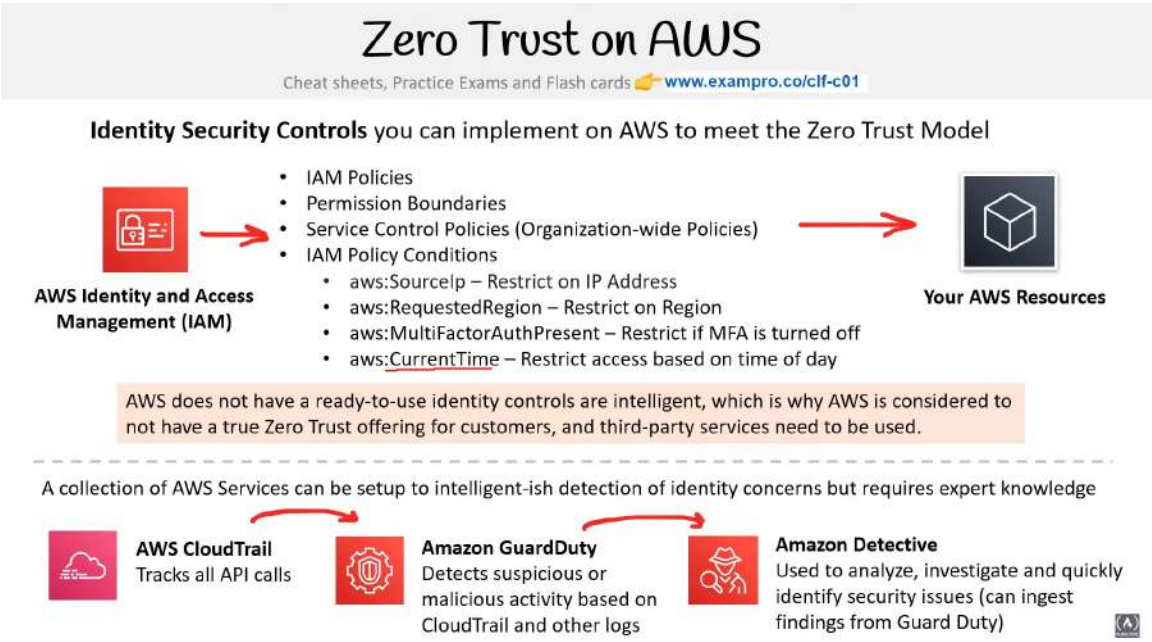


▼ 10. AWS Savings Plan

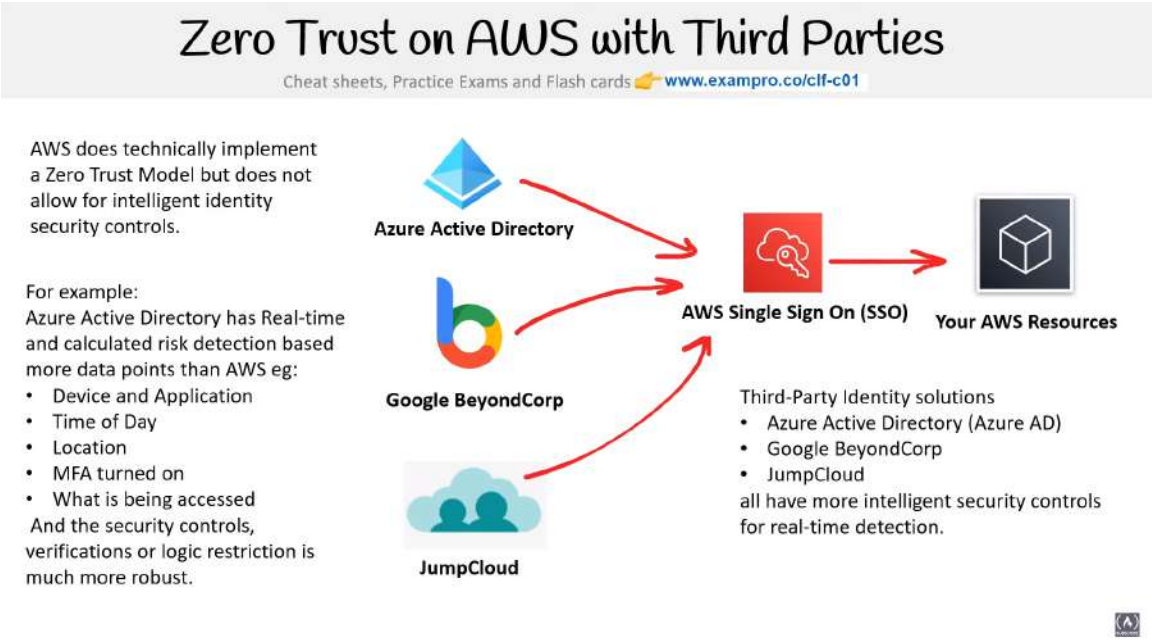


▼ 14. Identity

▼ 1. Zero Trust Model



▼ 2. Zero Trust Model on Third Parties



▼ 3. Directory Service

Directory Service

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

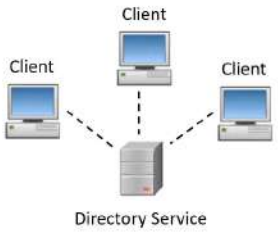
What is a directory service?
A directory service maps the **names of network resources to their network addresses.**

A directory service is shared information infrastructure for **locating, managing, administering and organizing** resources:

- Volumes
- Folders
- Files
- Printers
- Users
- Groups
- Devices
- Telephone numbers
- other objects

A directory service is a critical component of a network operating system
A directory server (name server) is a server which provides a directory service

Each resource on the network is considered an object by the directory server. Information about a particular resource is stored as a collection of attributes associated with that resource or object



Well known directory services:

- Domain Name Service (DNS)
  - the directory service for **the internet**
- **Microsoft Active Directory**
  - Azure Active Directory
- Apache Directory Server
- Oracle Internet Directory (OID)
- OpenLDAP
- Cloud Identity
- JumpCloud

▼ 4. Internet Providers

Identity Providers (IdPs)

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Identity Provider (IdP) a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to applications within a **federation** or distributed network.
A trusted provider of your user identity that lets you use authenticate to access other services.
Identity Providers could be: **Facebook, Amazon, Google, Twitter, Github, LinkedIn**

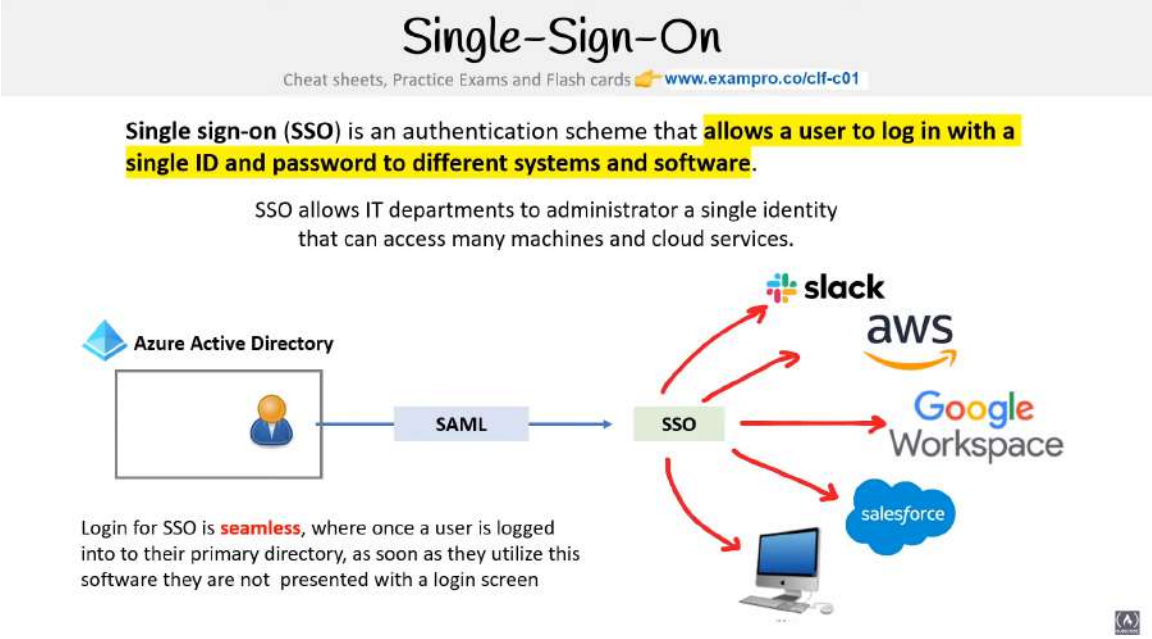
Federated identity is a method of linking a user's identity across multiple separate identity management systems

OpenID
open standard and decentralized authentication protocol. Eg be able to login into a different social media platform using a Google or Facebook account
OpenID is about providing who are you

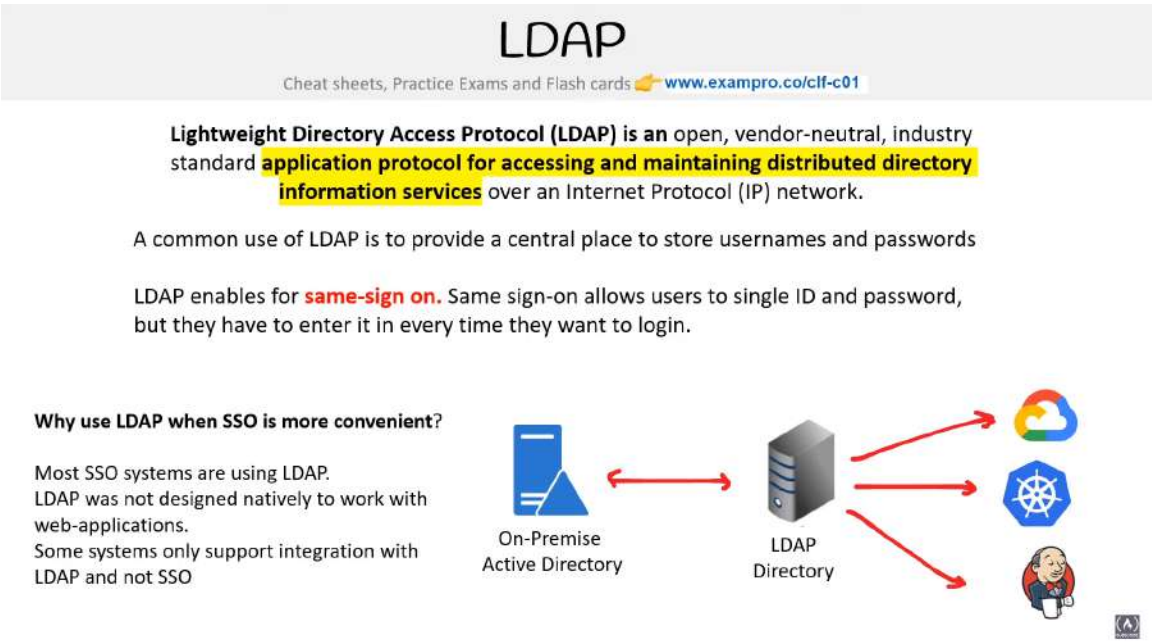
OAuth2.0
industry-standard protocol for authorization OAuth doesn't share password data but instead uses authorization tokens to prove an identity between consumers and service providers.
Oauth is about granting access to functionality

SAML
Security Assertion Markup Language is an open standard for exchanging authentication and authorization between an identity provider and a service provider.
An important use case for SAML is **Single-Sign-On via web browser**.

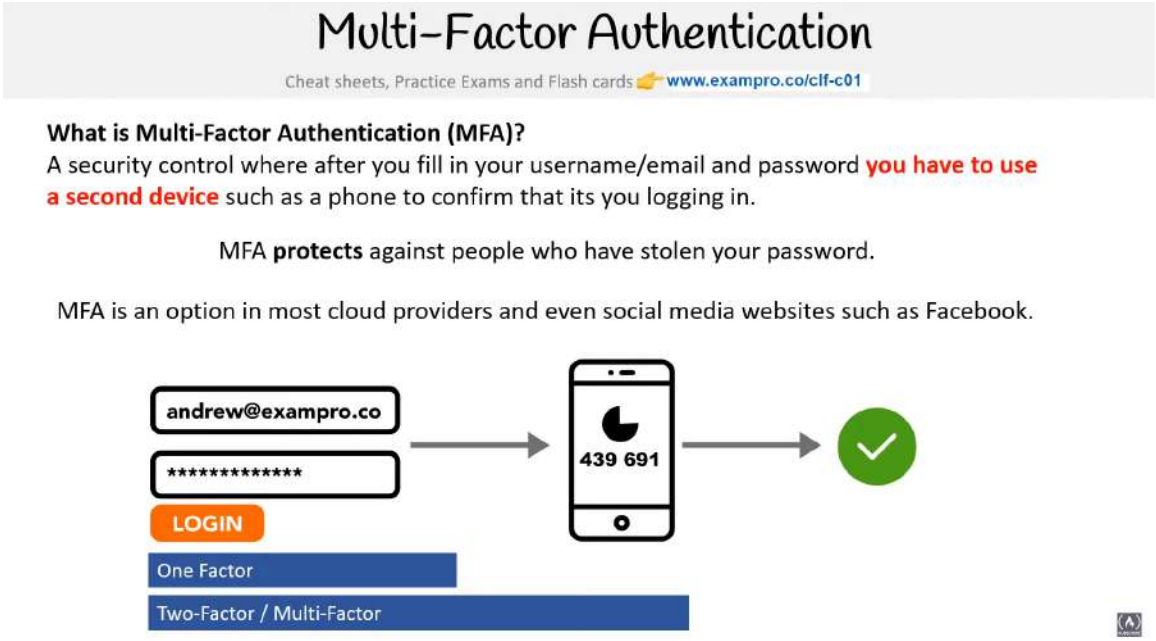
▼ 5. Single Sign On (SSO)



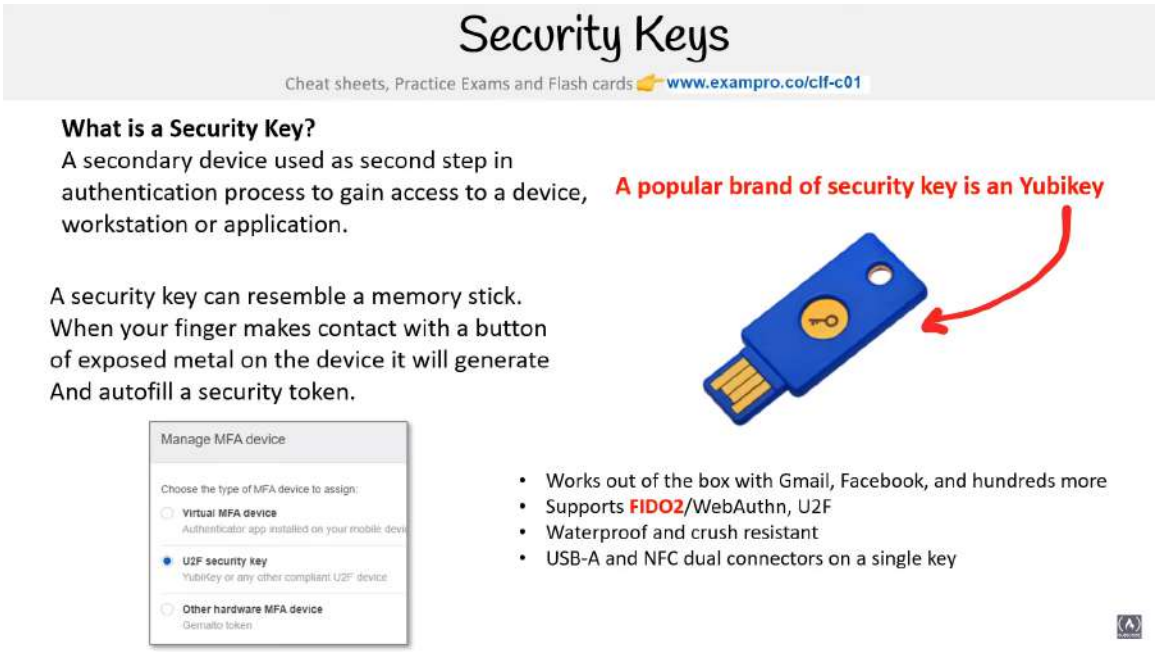
▼ 6. Lightweight Directory Access Protocol (LDAP)



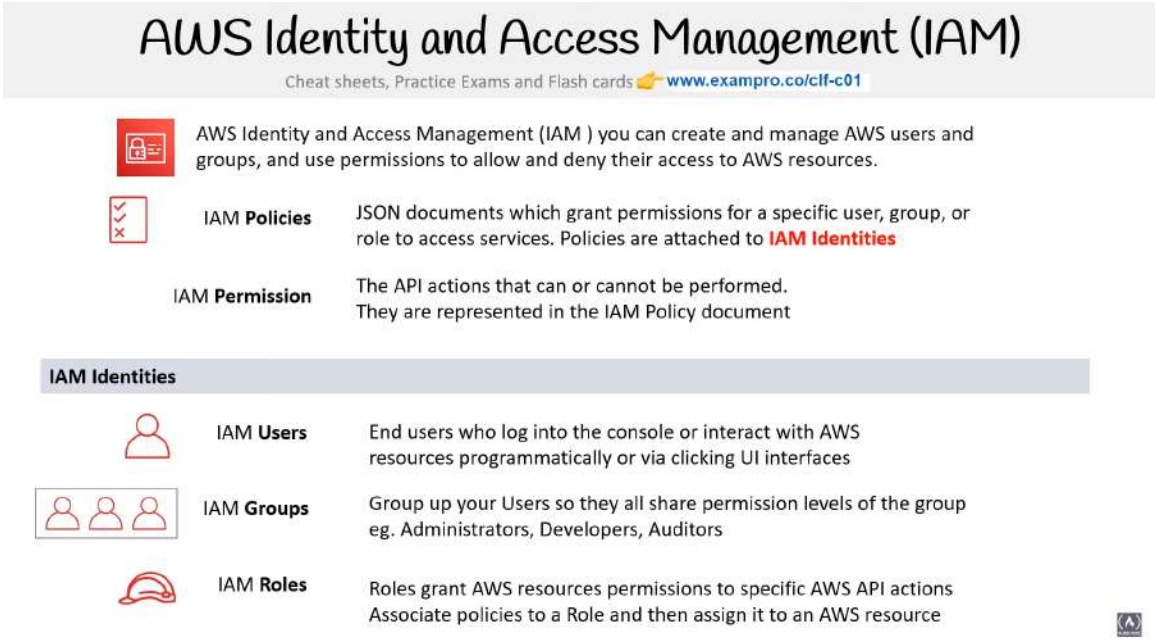
▼ 7. Multi Factor Authentication (MFA)



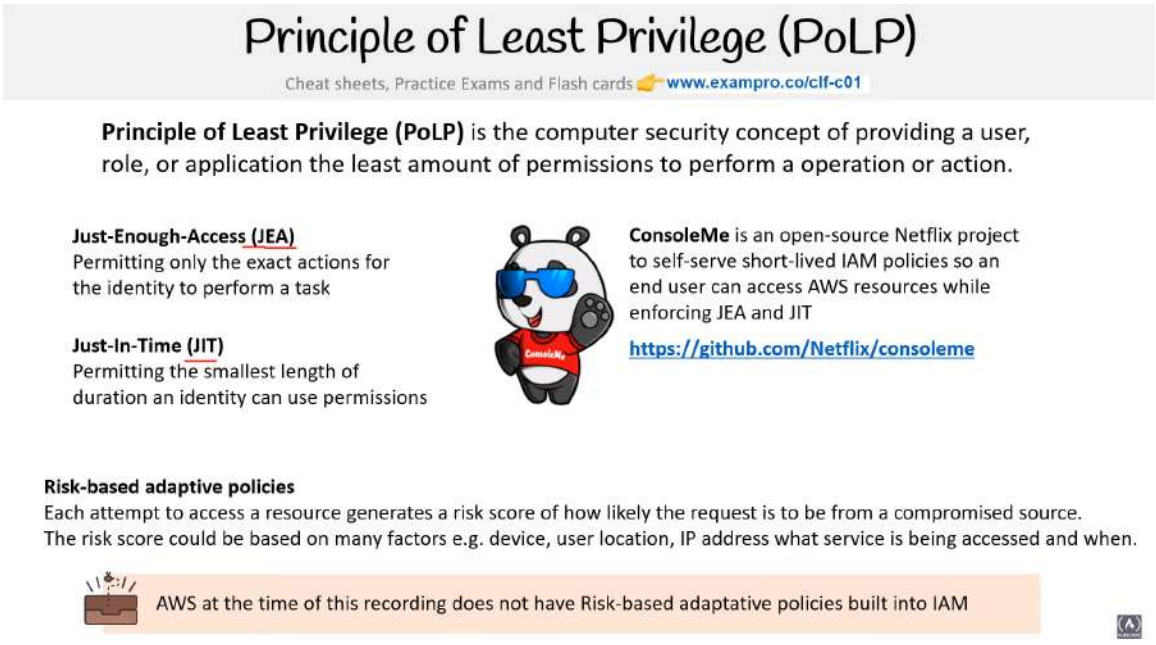
▼ 8. Security Keys



▼ 9. AWS Identity Access Management (IAM)



▼ 10. Principal of Least Privilege (POLP)



▼ 11. AWS Account Root User

AWS Account Root User

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Administrative Tasks **that only the Root User can perform**:

- **Change your account settings**.
  - includes the account name, email address, root user password, and root user access keys.
  - Other account settings, such as contact information, payment currency preference, and Regions, do not require root user credentials.
- Restore IAM user permissions.
  - If the only IAM administrator accidentally revokes their own permissions, you can sign in as the root user to edit policies and restore those permissions.
- Activate IAM access to the Billing and Cost Management console.
- View certain tax invoices
- **Close your AWS account**.
- **Change or Cancel AWS Support plan**
- Register as a seller in the Reserved Instance Marketplace.
- Enable MFA Delete on an S3 Bucket.
- Edit or delete an Amazon S3 bucket policy that includes an invalid VPC ID or VPC endpoint ID.
- Sign up for GovCloud.

▼ 15. Application Integration

▼ 1. What is Application Integration.

Application Integration

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is Application Integration?
Application Integration is the process of letting two independent applications to communicate and work with each other, commonly facilitated by an intermediate system.

Cloud workloads encourage systems and services to be loosely coupled and so AWS has many service for the specific purpose of application integration.

The common systems or design patterns utilized for Application Integration generally are:

- Queueing
- Streaming
- Pub/Sub
- API Gateways
- State Machine
- Event Bus

▼ 2. Queuing

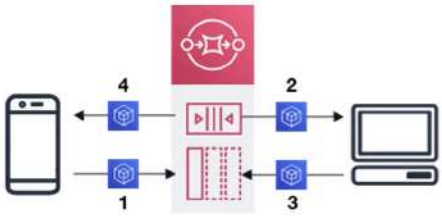
Queveing

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is a Messaging System?
Used to provide asynchronous communication and decouple processes via messages / events
From a sender and receiver (producer and consumer)

What is a Queueing System?
A Queueing system is a messaging system that generally will delete messages once they are consumed.
Simple communication. **Not Real-time.** Have to pull. Not reactive.

Simple Queueing Service (SQS)
Fully managed **queuing service** that enables you to decouple and scale microservices, distributed systems, and serverless applications



Use Case: You need to queue up transaction emails to be sent e.g. Signup, Reset Password.

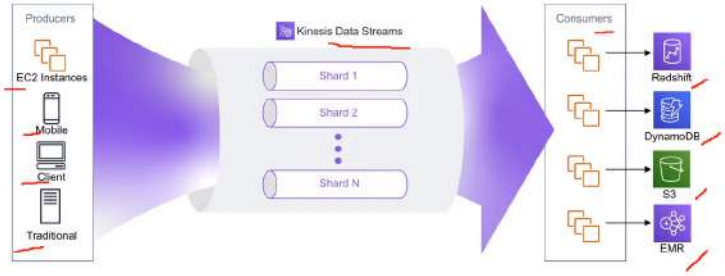
▼ 3. Streaming

Streaming

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is streaming?
Multiple consumers can **react** to events (messages)
Events live in the stream for long periods of time, so complex operations can be applied. **Real-time**

Amazon Kinesis
Amazon Kinesis is the AWS fully managed solution for collecting, processing, and analyzing streaming data in the cloud.



▼ 4. Pub/Sub (Publisher/Subscriber)

Pub/Sub

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

What is Pub/Sub?

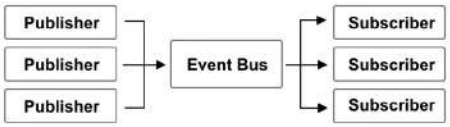
Publish–subscribe pattern commonly implemented in **messaging systems**.

In a pub/sub system the sender of messages (**publishers**) do not send their messages directly to receivers.

They instead send their messages to an **event bus**. The event bus categorizes their messages into groups.

Then receivers of messages (**subscribers**) subscribe to these groups.

Whenever new messages appear within their subscription the messages are immediately delivered to them.



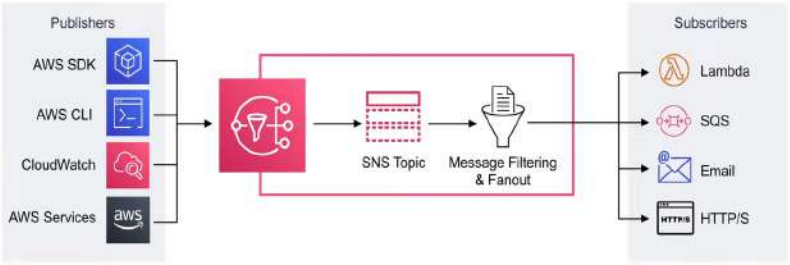
Use Case: a real-time chat system. A web-hook system

- Publisher have no knowledge of who their subscribers are.
- Subscribers do **not pull** for messages.
- Messages are instead automatically and immediately **pushed** to subscribers.
- Messages and events are interchangeable terms in pub/sub

Pub/Sub

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Simple Notification Service (SNS) is a highly available, durable, secure, fully managed **pub/sub messaging** service that enables you to **decouple** microservices, distributed systems, and serverless applications.



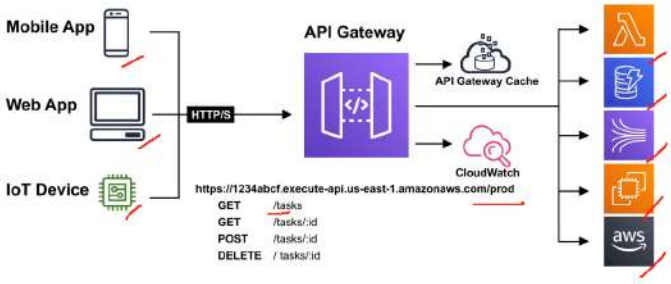
▼ 5. API Gateway

API Gateway

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

What is an API Gateway?
An API Gateway is a program that sits between a single-entry point and multiple backends.
API Gateway allows for throttling, logging, routing logic or formatting of the request and response

Amazon API Gateway is a solution for **creating secure APIs** in your cloud environment at **any scale.**
Create APIs that act as a front door for applications to access data, business logic, or functionality from back-end services.



▼ 6. State Machines

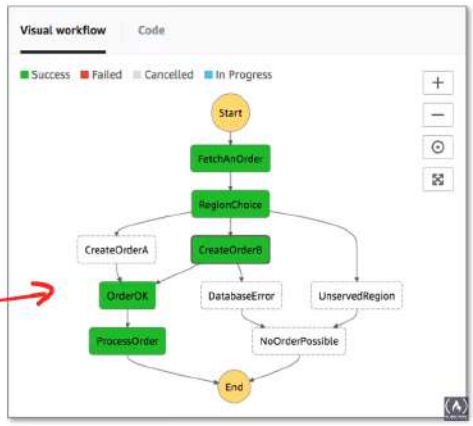
State Machines

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

What is a state machine?
A state machine is an abstract model which decides how one state moves to another based on a series of conditions. **Think of a state machine like a flow chart.**

What is AWS Step Functions?
- Coordinate multiple AWS Services into a serverless workflow
- A graphical console to visualize the components of your application as a series of steps.
- Automatically triggers and tracks each step, and retries when there are errors, so your application executes in order and as expected, every time
- logs the state of each step, so when things go wrong, you can diagnose and debug problems quickly

Any one of these steps could be using an AWS Service



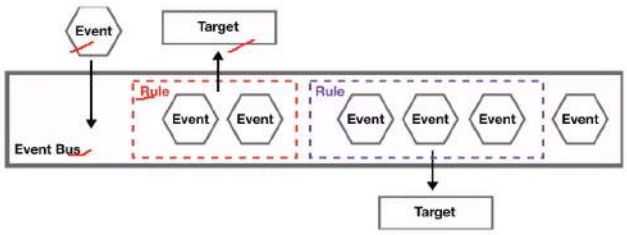
▼ 7. Event Bus and Amazon Event Bridge

Event Bus

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is an Event Bus?

An event bus **receives events** from a **source** and **routes events** to a **target** based on **rules**



EventBridge is a **serverless** event bus service that is used for application integration by **streaming real-time** data to your applications

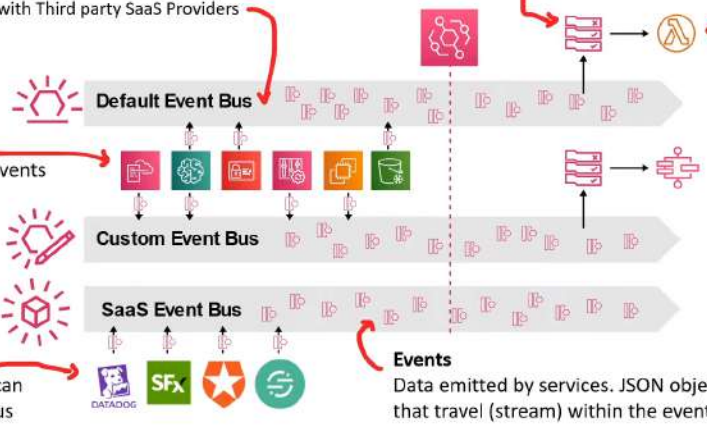
EventBridge was *formerly* called **Amazon CloudWatch** Events.

Amazon Event Bridge

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Event Bus
Holds event data, define rules on an event bus to react to events.
Default Event Bus — An AWS account has a default event bus
Custom Event Bus — Scoped to multiple accounts or other AWS accounts
SaaS Event Bus — Scoped to with Third party SaaS Providers

Rules
Determines what events to capture and pass to targets. (100 Rules per bus)



Producers
AWS Services that emit events

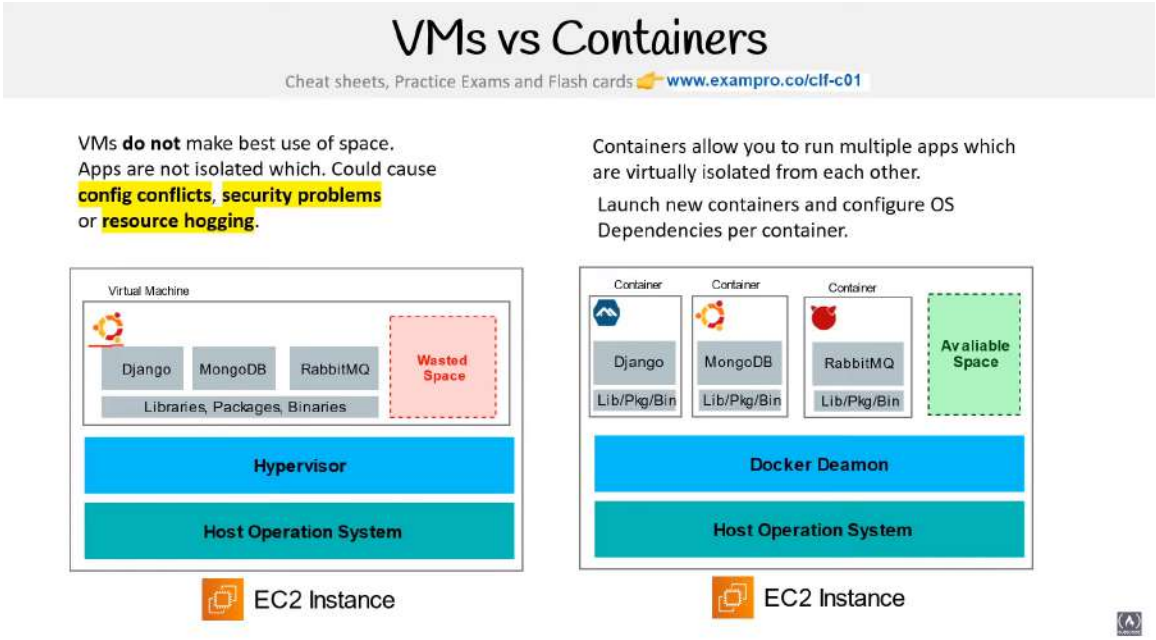
Targets
AWS Services that consume events
(5 targets per rule)

Partner Sources
Are third-party apps that can emit events to an event bus

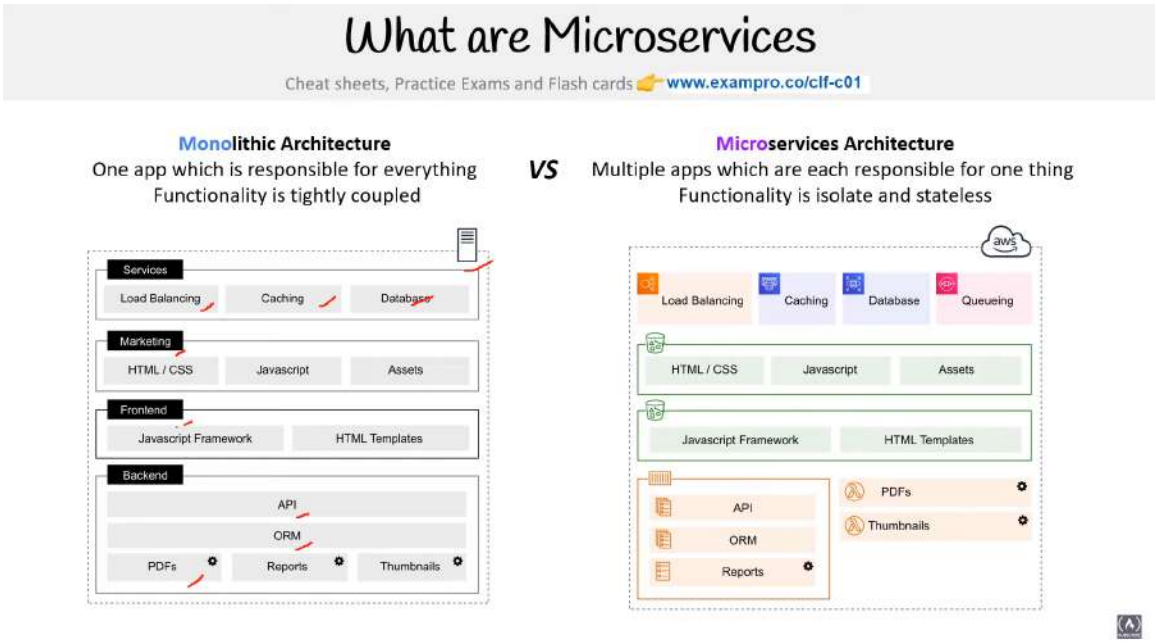
Events
Data emitted by services. JSON objects that travel (stream) within the event bus.

▼ 16. Containers

▼ 1. VMs vs Containers



▼ 2. What are Microservices



▼ 3. Kubernetes

Kubernetes

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Kubernetes is an **open-source container orchestration system** for automating **deployment, scaling and management** of containers.

Originally created by Google and now maintained by the **Cloud Native Computing Foundation (CNCF)**

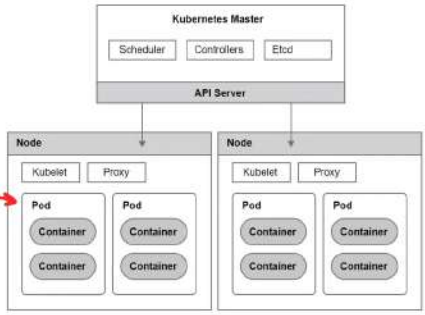
Kubernetes is commonly called **K8**

- The 8 represent the remaining letters "ubernete"

The advantage of Kubernetes over Docker is the ability to run containers distributed across multiple VMs

A unique component of Kubernetes are **Pods.**
A pod is a group of one more containers with shared storage, network resources and other shared settings.

Kubernetes is ideally for micro-service architectures where a company has tens to hundreds of services they need to manage



▼ 4. Docker

Docker

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Docker is a set of Platform as a Service (PaaS) products that use OS-level virtualization to deliver software in packages called containers.

Docker was the earliest popularized open-source container platform.
When people think of containers, they think of Docker.

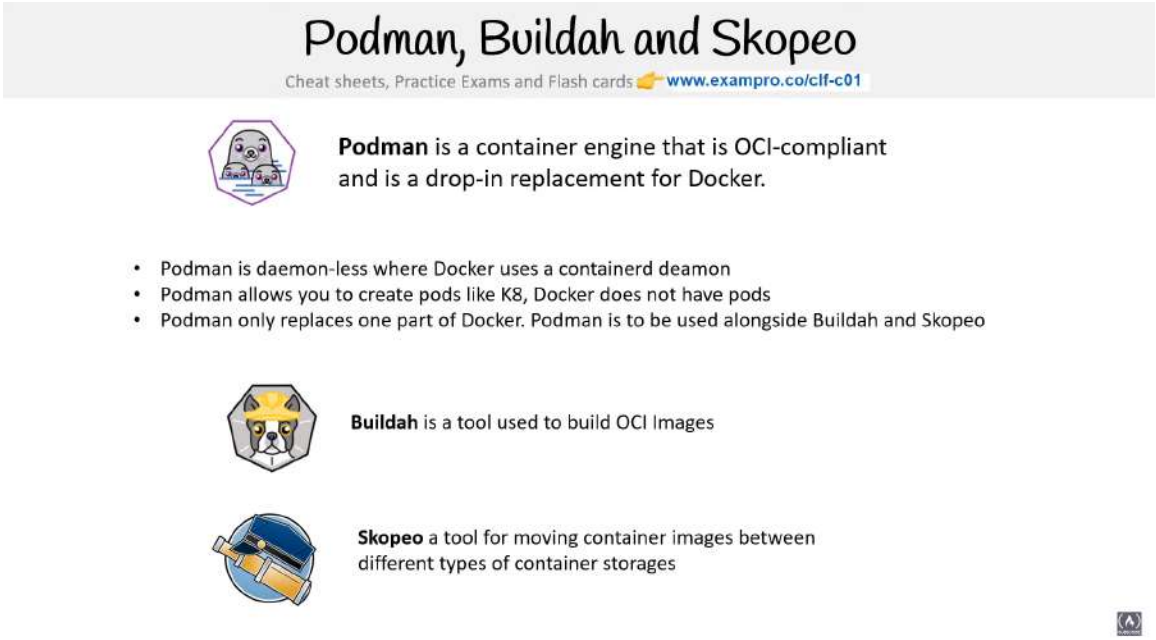
```
FROM python:3.8-alpine3.12
COPY . /app
WORKDIR /app
RUN pip install -r requirements.txt
CMD ["python3", "app.py"]
```

Docker CLI – CLI commands to download, upload, build run and debug containers
Dockerfile – a configuration file on how to provision a container
Docker Compose – is a tool and configuration file when working with multiple containers
Docker Swarm – An orchestration tool for managing deployed multi-containers architectures
Dockerhub – a public online repository for containers published by the community for download

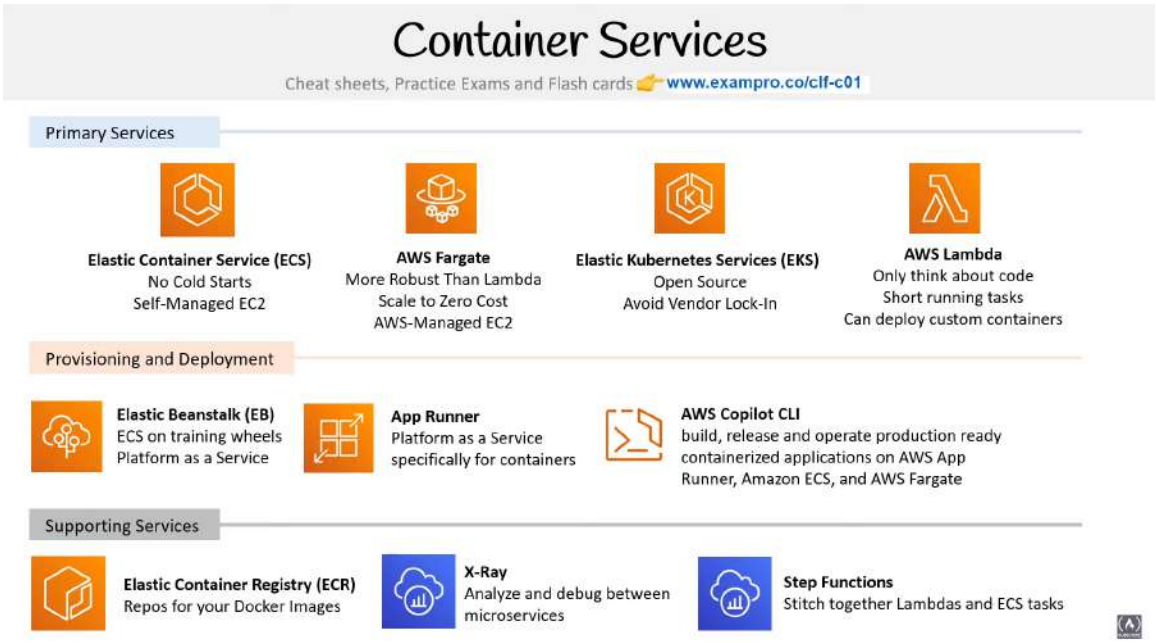
The Open Container Initiative (OCI) is an open governance structure for creating open industry standards around container formats and runtime.
Docker established the OCI and it is now maintained by the Linux Foundation.

Docker has been losing favor with developers due to their handling of introducing a paid open-source model and alternative like Podman are growing.

▼ 5. PodMan

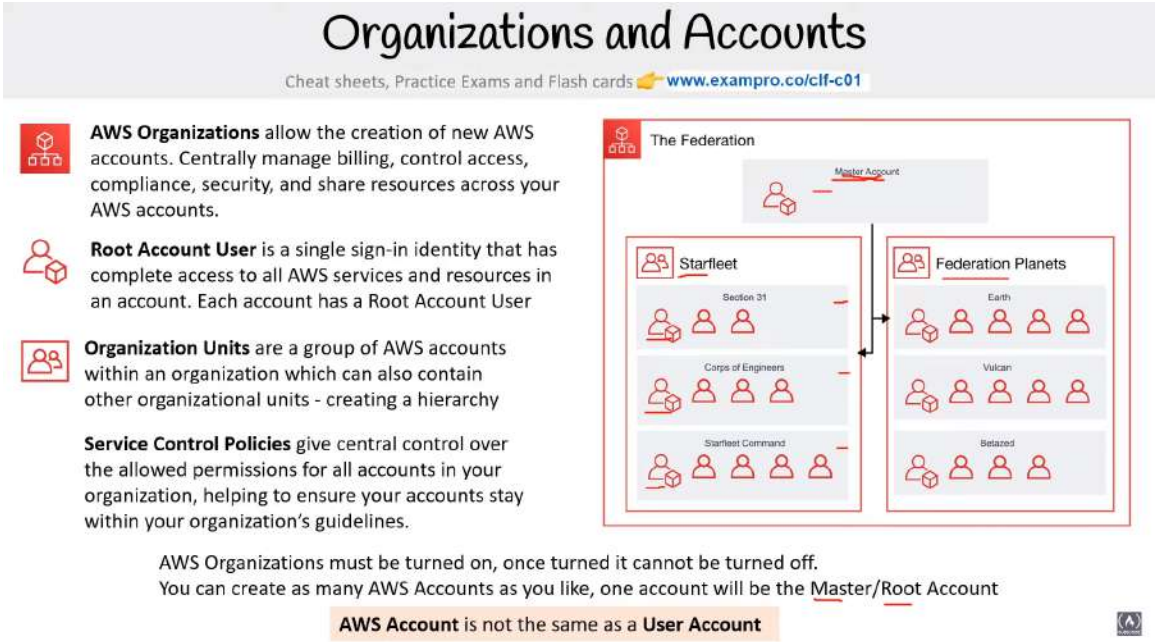


▼ 6. Container Services

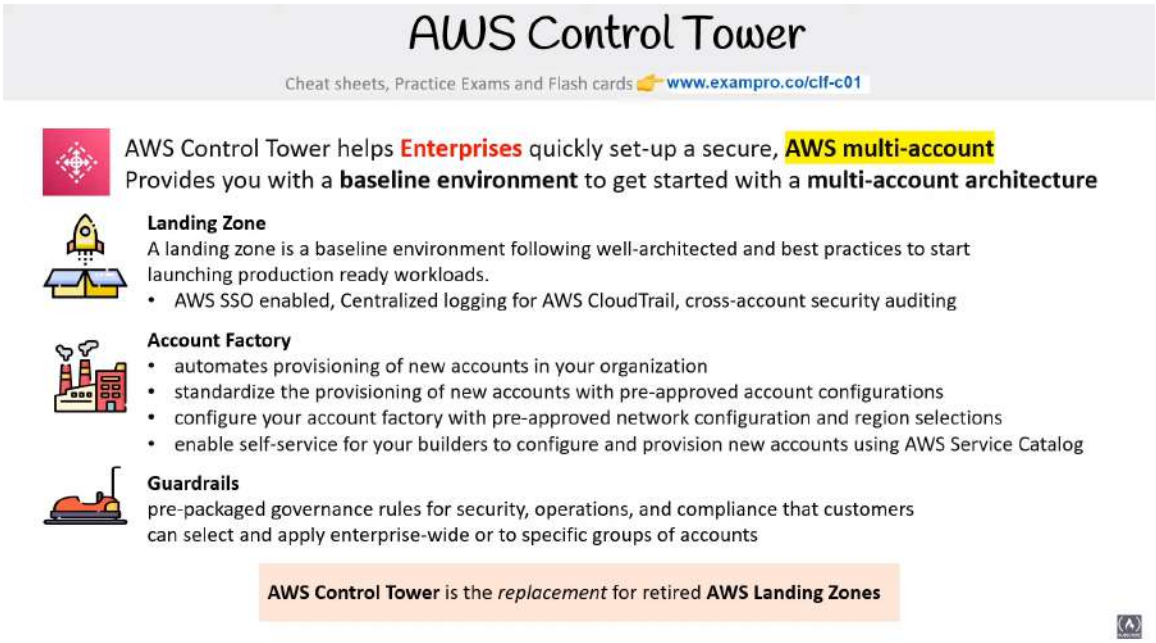


▼ 17. Governance

▼ 1. AWS Organizations and Accounts



▼ 2. AWS Control Tower



▼ 3. AWS Config

AWS Config

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is Change management?
Change management in the context of Cloud Infrastructure is when we have **formal process** to:

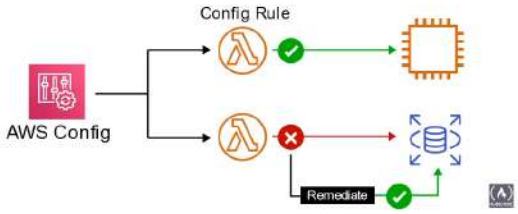
- monitor changes
- enforce changes
- Remediate changes

What is Compliance-as-code (CaC)?
Compliance as code is when we utilize programming to automate the monitoring, enforcing and remediating changes to stay compliant with a compliance programs or expected configuration.

What is AWS Config?
AWS Config as is **Compliance-as-Code framework** that allows us to **manage change** in your AWS accounts on a **per region basis**.

When should you use AWS Config?

- I want this **resource** to stay **configured** a **specific way** for **compliance**.
- I want to **keep track** of configuration **changes** to resources.
- I want **a list of all resources** within a region.
- I want to use **analyze potential security** weaknesses, you need detailed historical information.



▼ 4. AWS Quick Starts

AWS Quick Starts

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

AWS Quick Starts are **Prebuilt templates** by AWS and AWS Partners to **help deploy wide range of stacks**

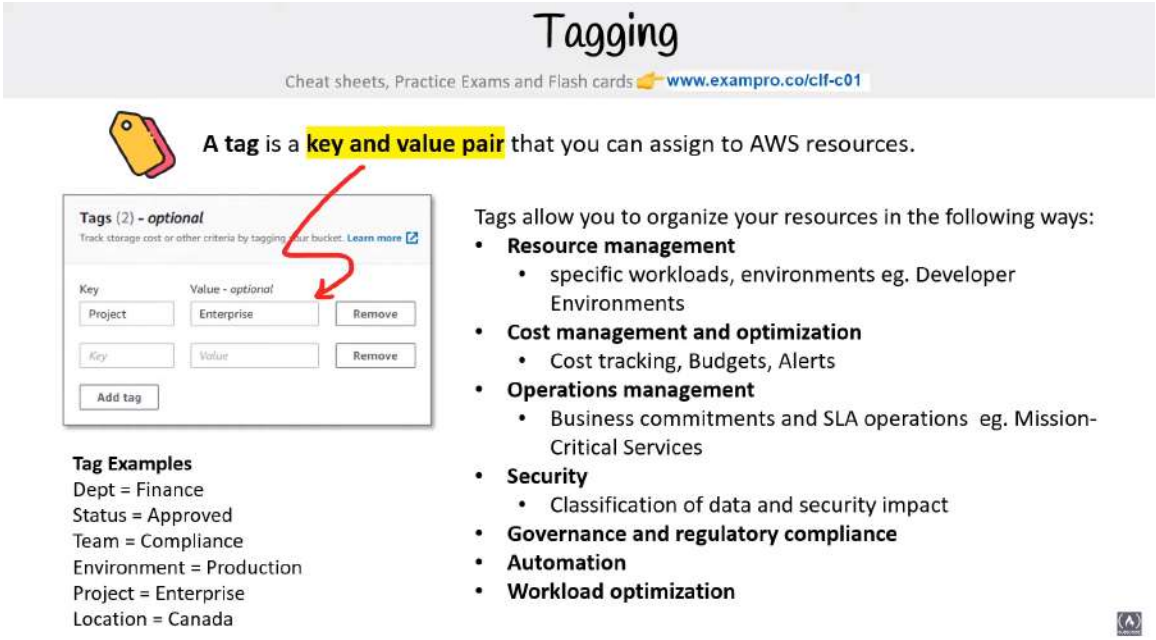
Reduce hundreds of manual procedures into just a few steps

A Quick Start is composed of **3** parts

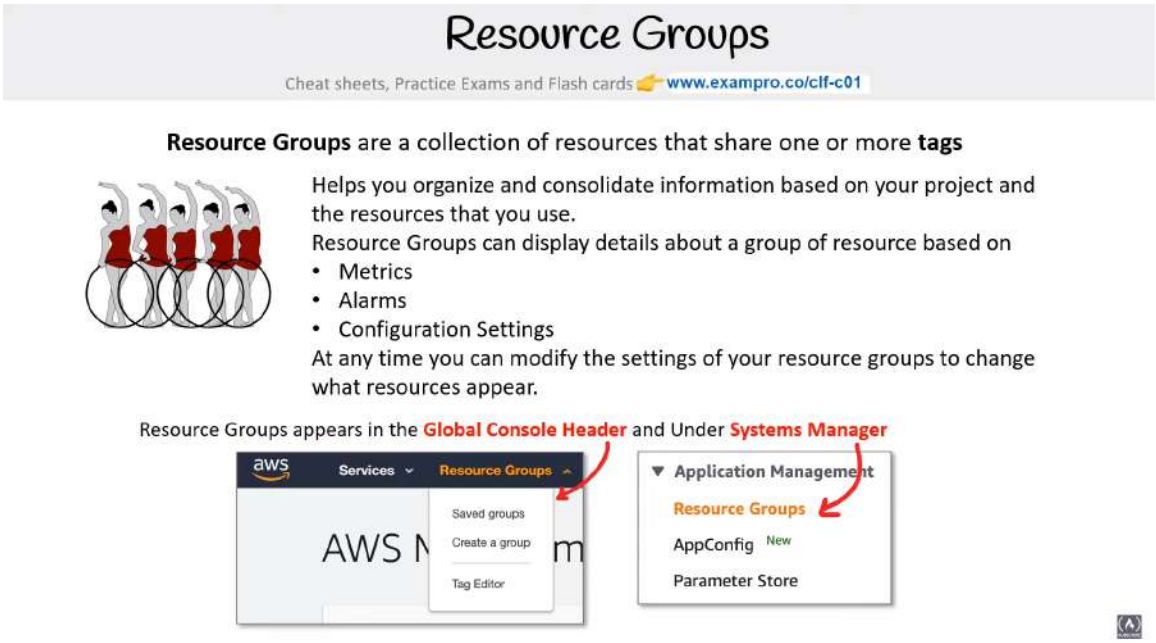
1. A reference architecture for the deployment
2. AWS CloudFormation templates that automate and configure the deployment
3. A deployment guide explaining the architecture and implementation in detail

Most Quick Start reference deployments enable you to spin up a fully functional architecture in less than an hour!

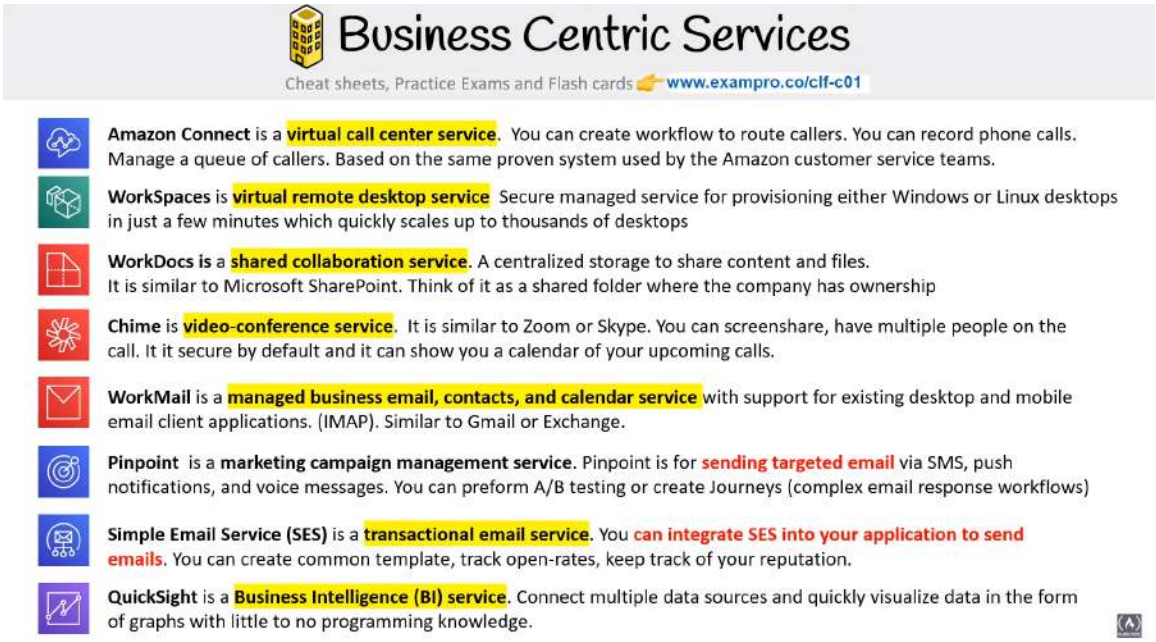
▼ 5. Tagging



▼ 6. Resource Groups

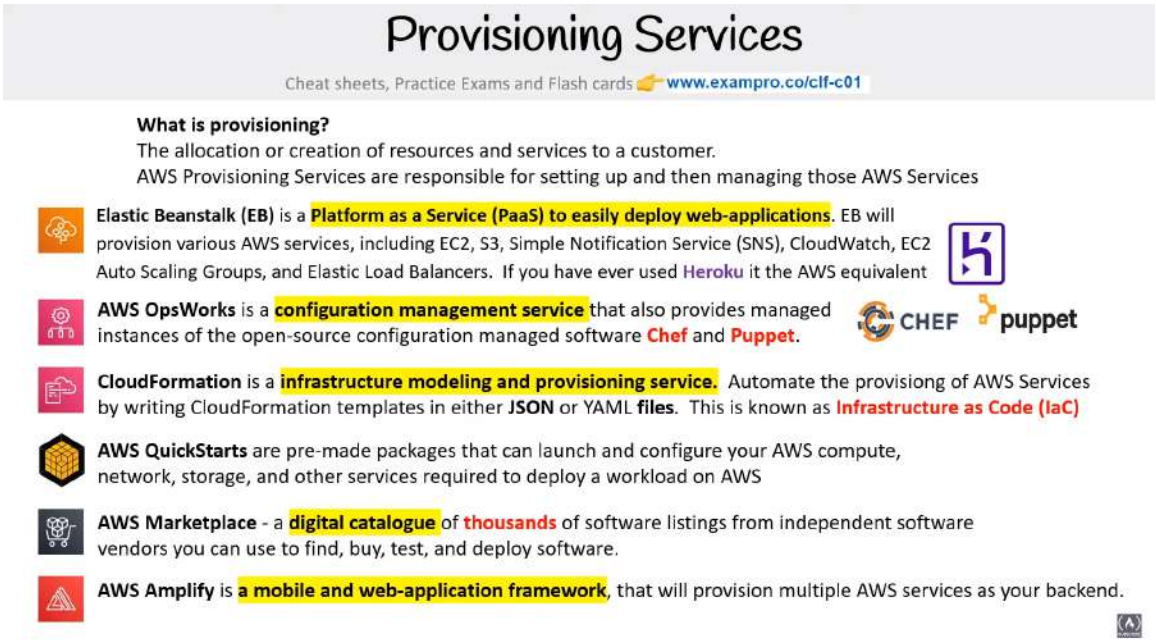


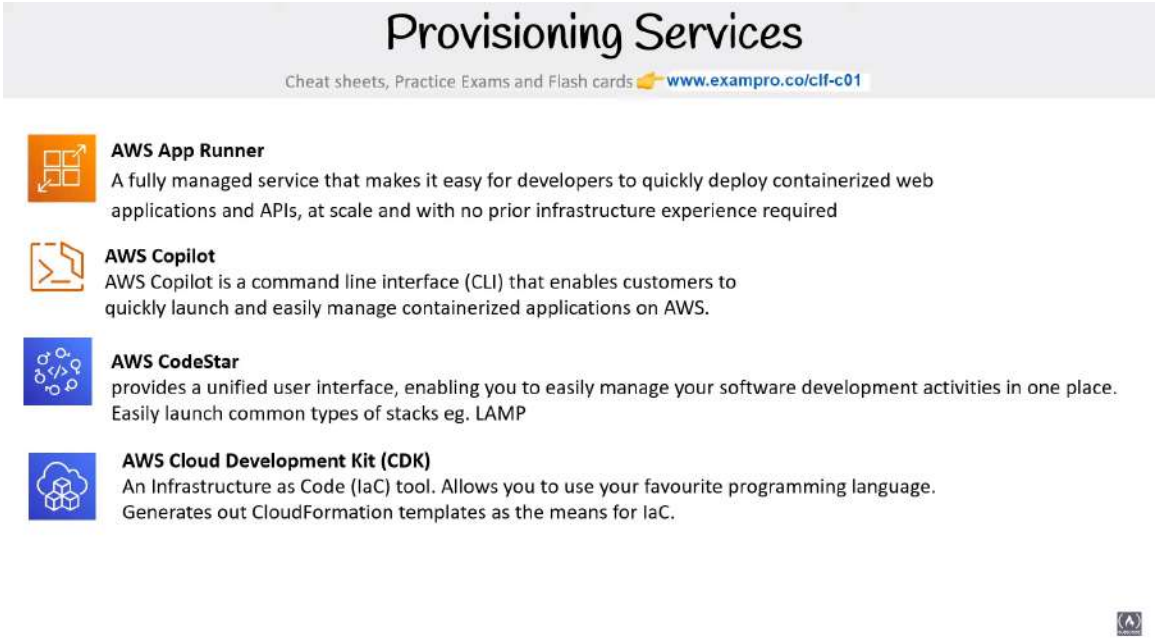
▼ 7. Business Centric Services



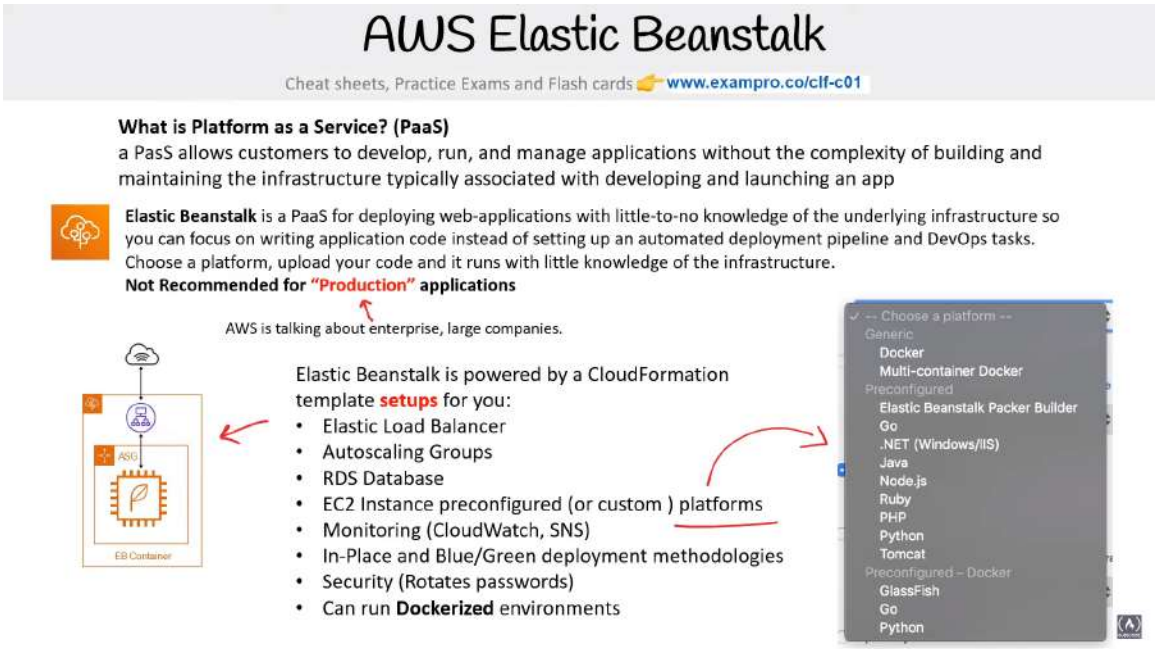
▼ 18. Provisioning

▼ 1. Provisioning Services



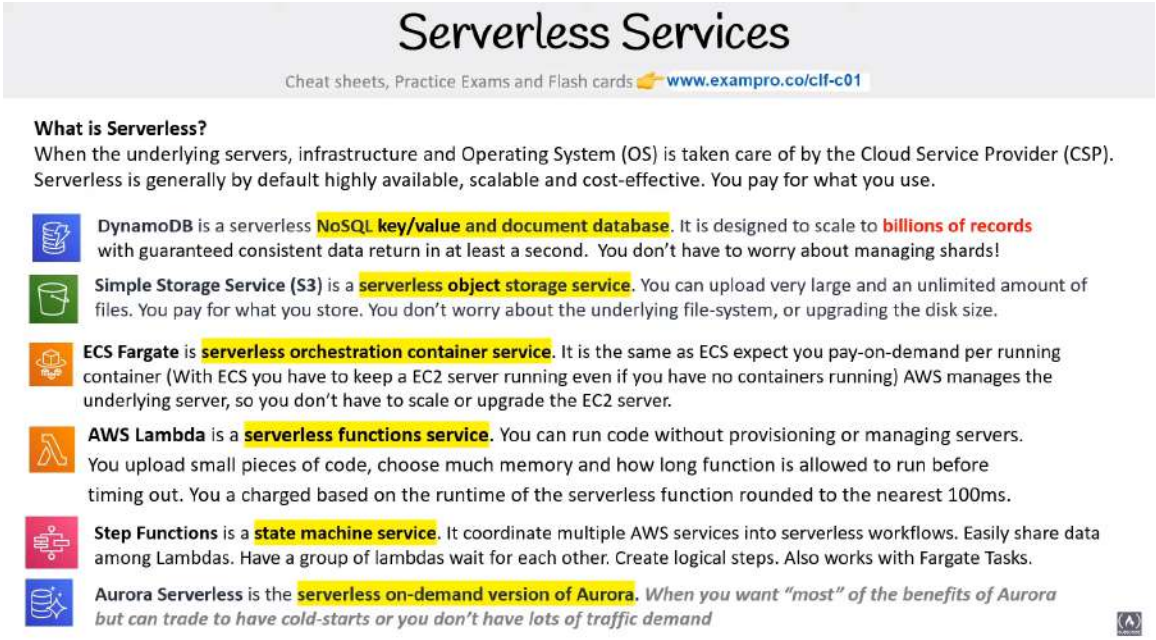


▼ 2. AWS Elastic Beanstalk

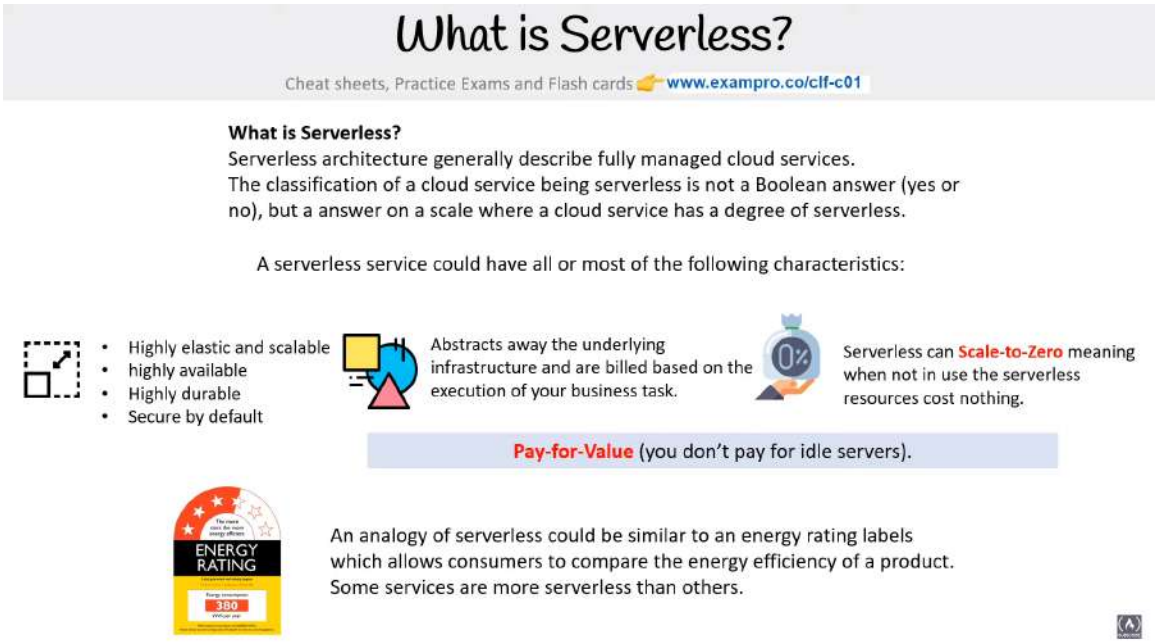


▼ 19. Serverless

▼ 1. Serverless Services

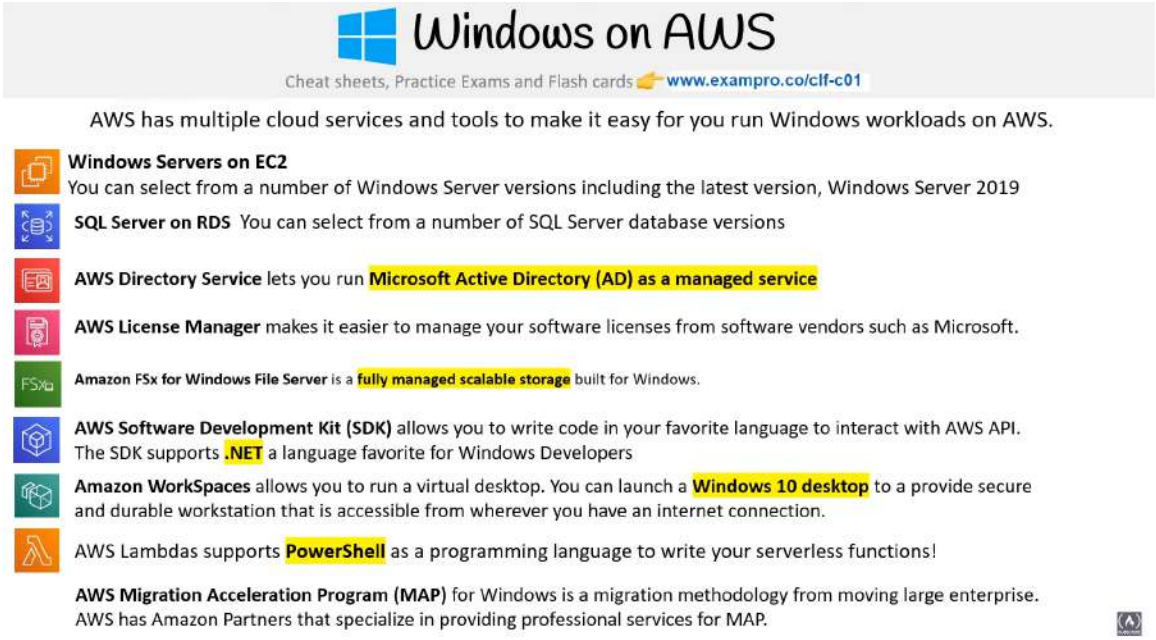


▼ 2. What is Serverless

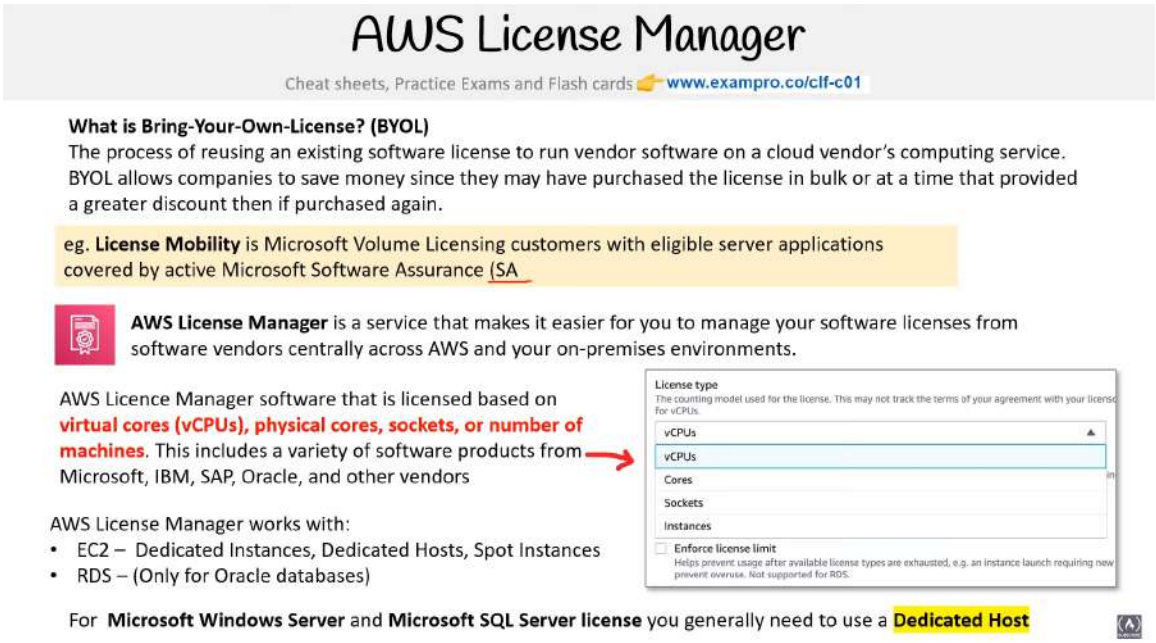


▼ 20. Windows on AWS

▼ 1. Windows on AWS

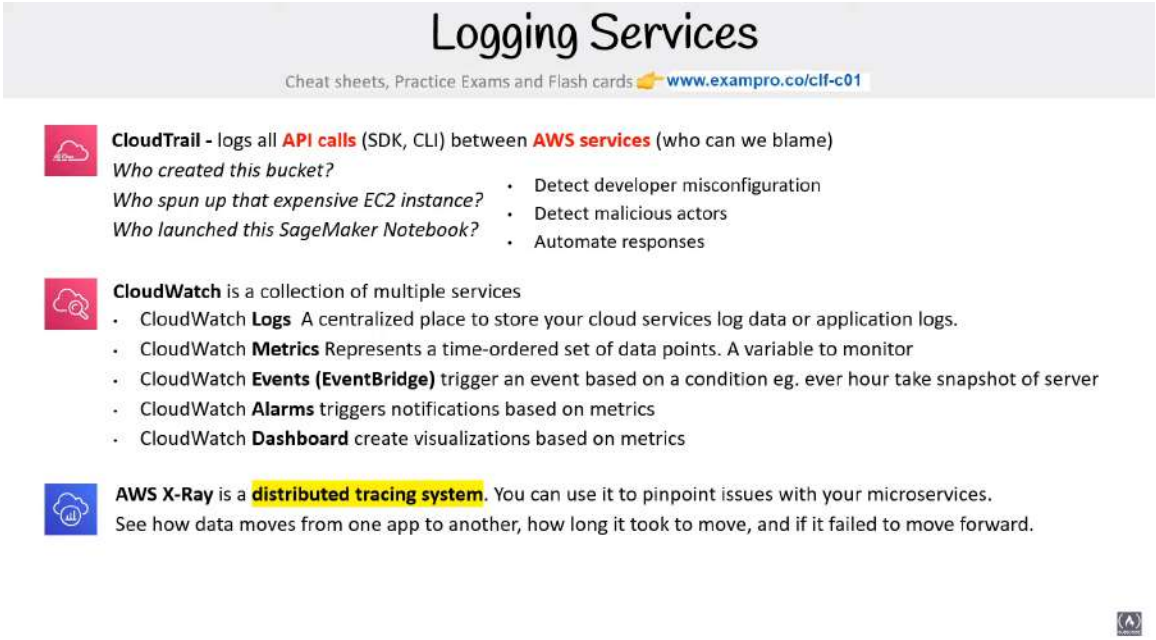


▼ 2. AWS License Manager

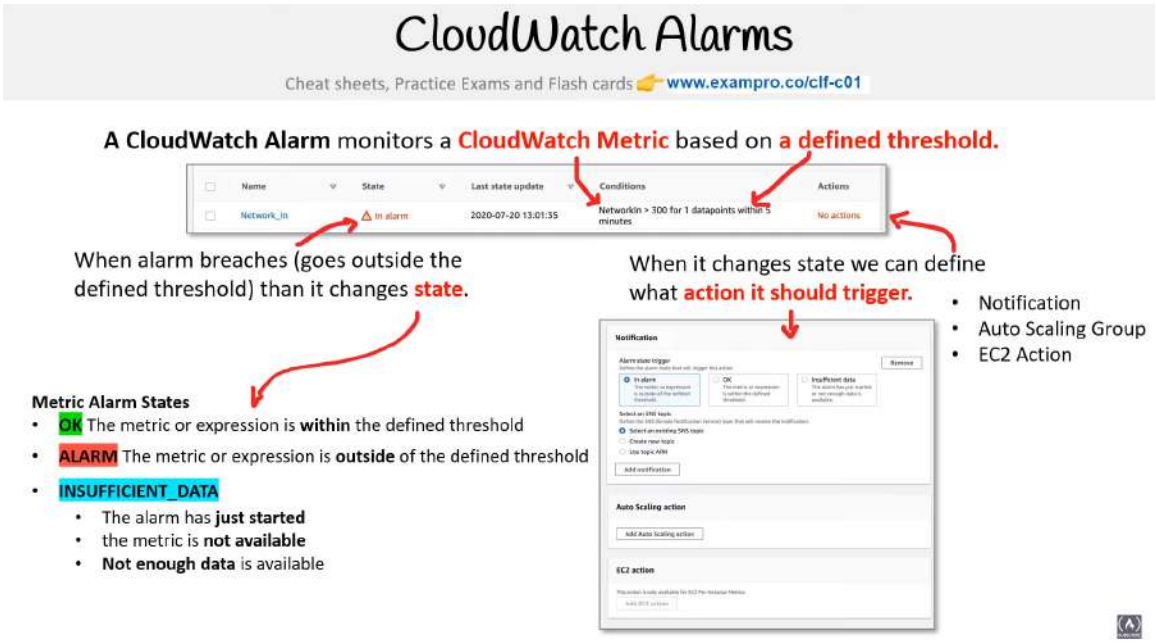


▼ 21. Logging

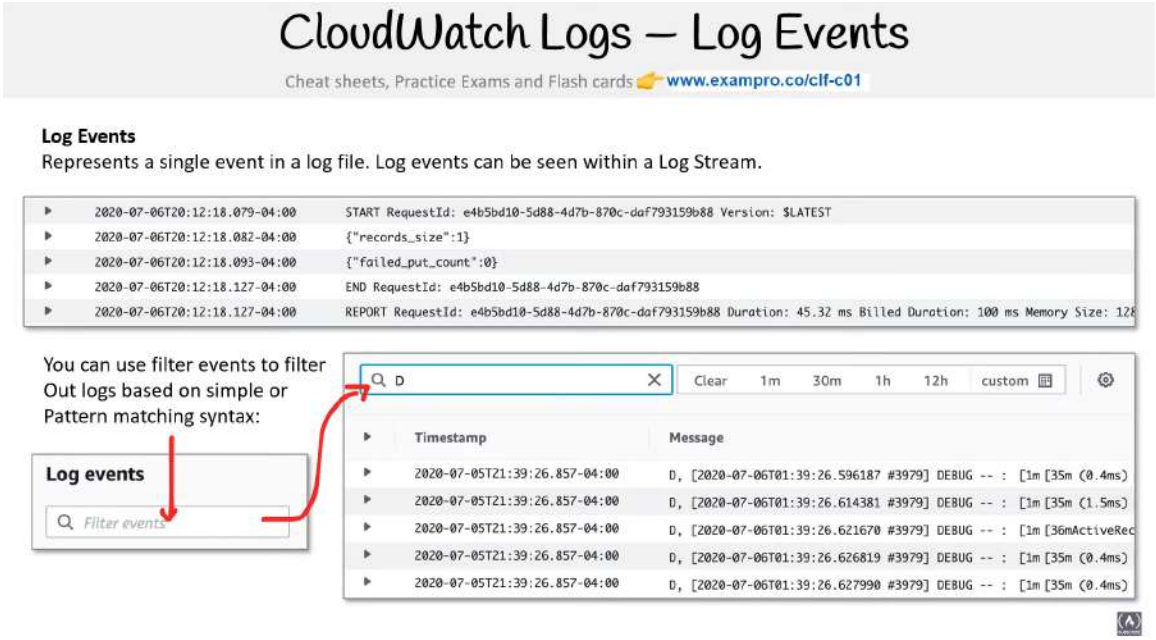
▼ 1. Logging Services



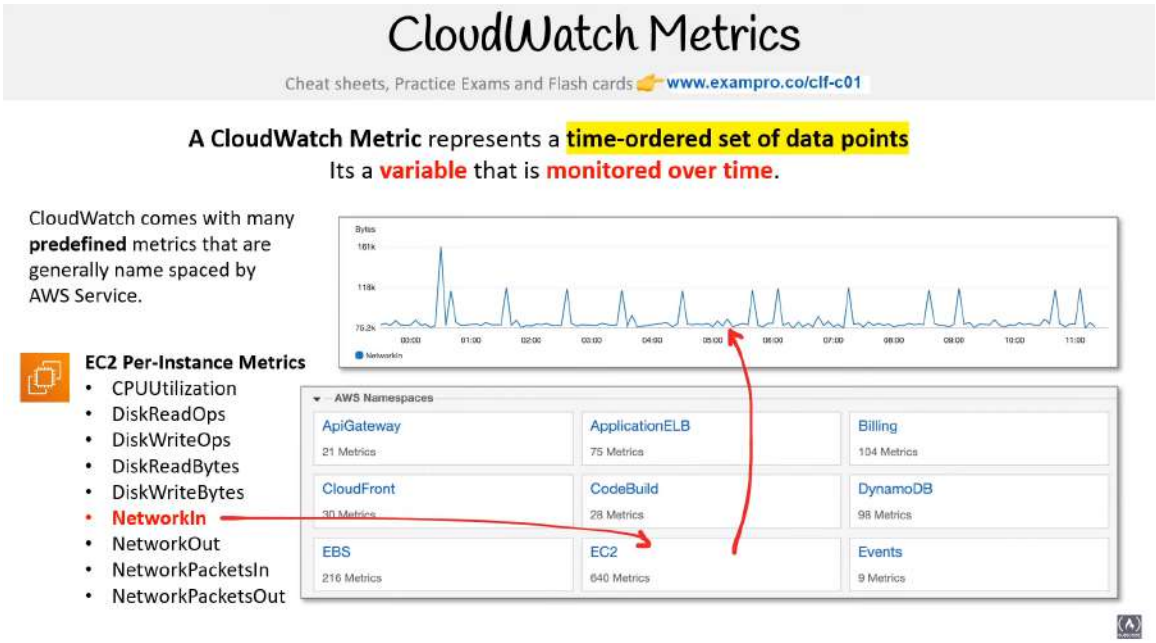
▼ 2. Cloud Watch Alarms



▼ 3. LOG Events



▼ 4. Cloud Watch Metrics

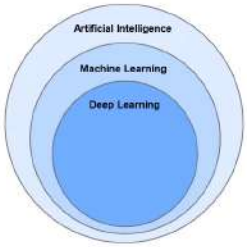


▼ 22. ML, AI and Big Data

▼ 1. Machine Learning and AI Services

Machine Learning and AI Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01



What is Artificial Intelligence (AI)?
Machines that perform jobs that mimic human behavior

What is Machine Learning (ML)?
Machines that get better at a task without explicit programming

What is Deep Learning (DL)?
Machines that have an artificial neural network inspired by the human brain to solve complex problems.

Amazon SageMaker is a fully managed service to **build, train, and deploy machine learning models** at scale

- **Apache MXNet on AWS**, open-source deep learning framework
- **TensorFlow on AWS** open-source machine intelligence library
- **PyTorch on AWS** open-source machine learning framework

Amazon SageMaker Ground Truth is **data-labeling service**. Have humans label a dataset that will be used to train machine learning models

Amazon Augmented AI human-intervention review service. When SageMaker's uses machine Learning to make a prediction is not confident it has the right answer queue up the predication for human review.

Machine Learning and AI Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Amazon CodeGuru is **machine-learning code analysis service**. CodeGuru performs code-reviews and will suggest changes to improve the quality of code. It can show visual code profiles (show the internals of your code) to pinpoint performance.

Amazon Lex is a **conversion interface service.** With Lex you can build **voice and text chatbots**

Amazon Personalize is a **real-time recommendations** service. Same technology used to make product recommendations to customers shopping on the Amazon platform

Amazon Polly is a **text-to-speech** service. Upload your text and an audio file spoken by synthesized voice is generated.

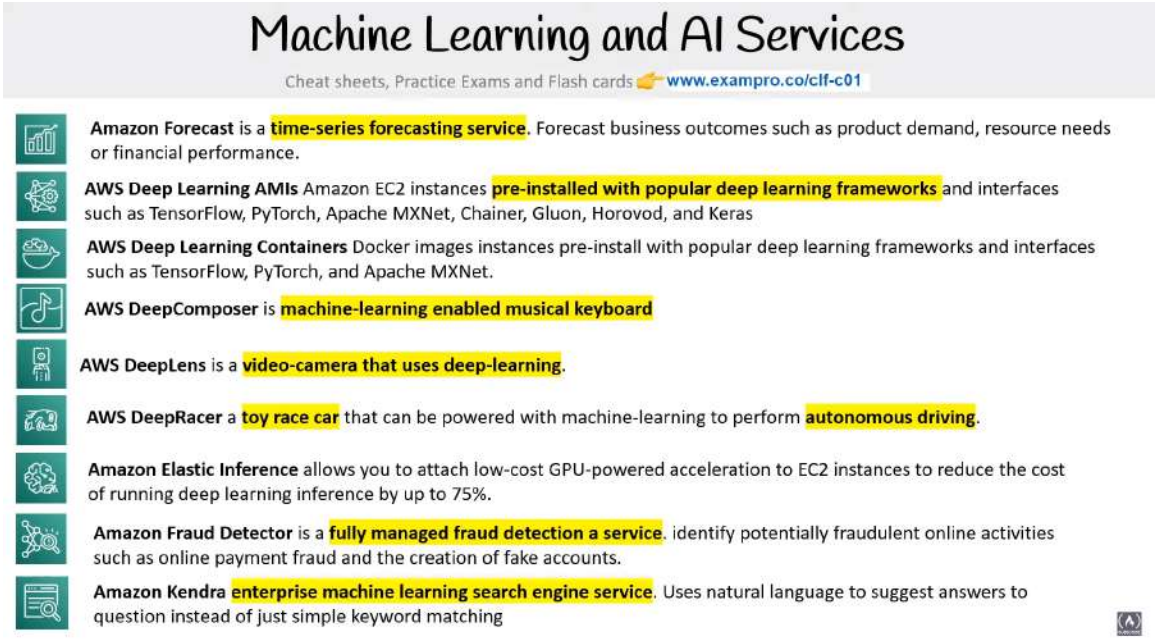
Amazon Rekognition is **image and video recognition service**. Analyze images and videos to detect and label objects, people, celebrities.

Amazon Transcribe is a **speech-to-text service**. Upload your audio file and it is converted

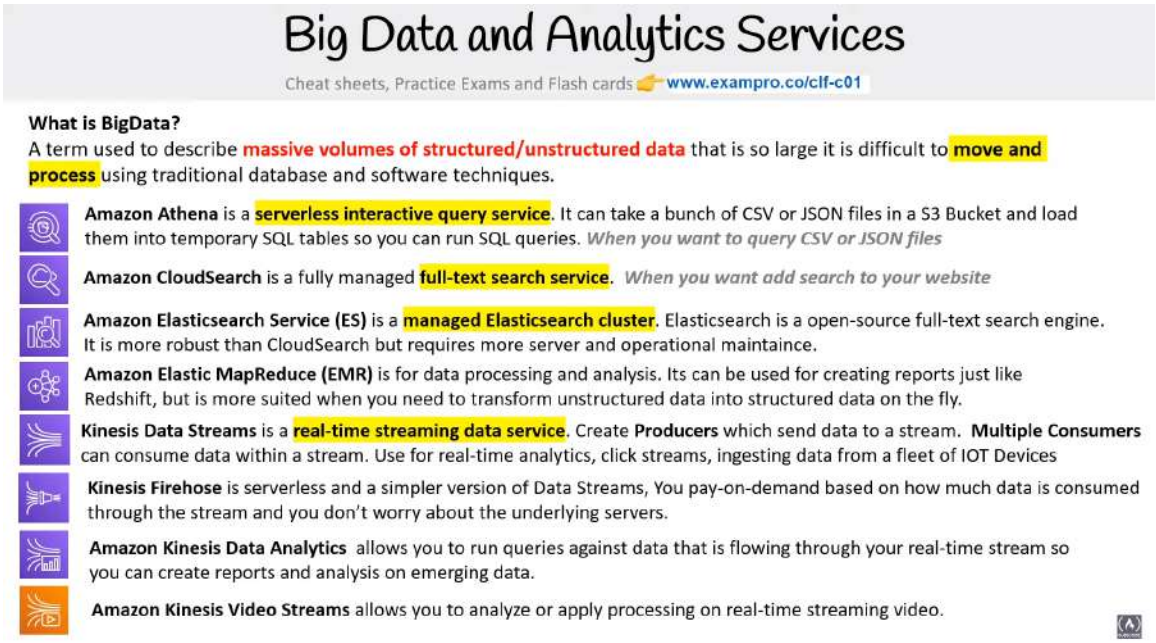
Amazon Textract and **OCR (extract text from scanned documents) service**. When you have paper forms and you want to digitally extract the data.

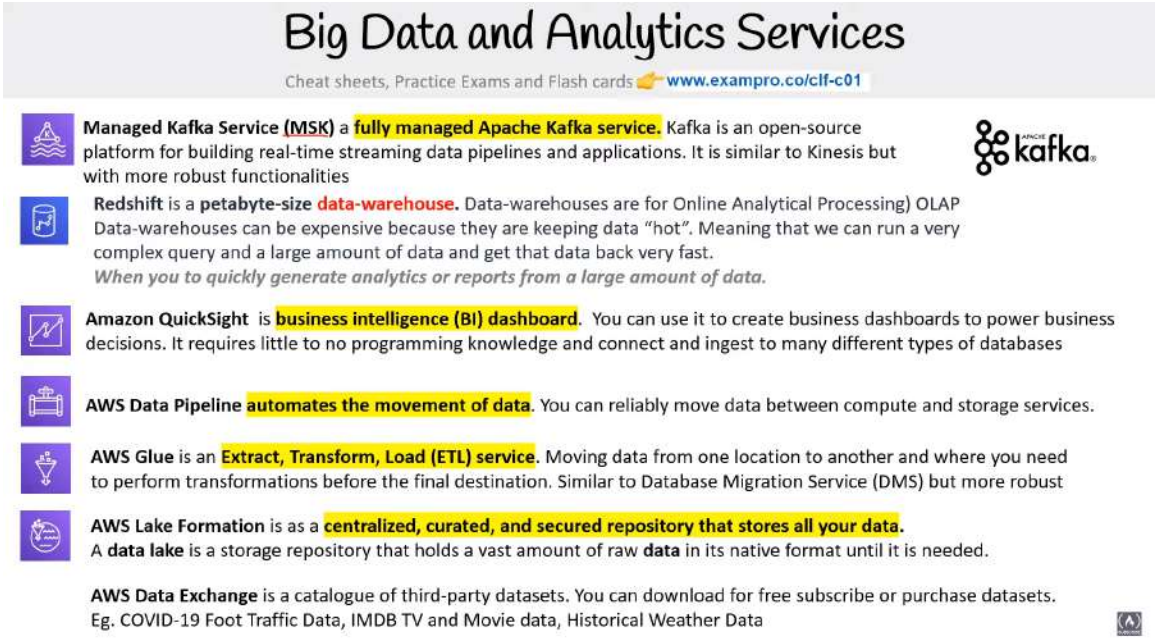
Amazon Translate **neural machine learning translation service**. Uses deep learning models to deliver more accurate and natural sounding translations.

Amazon Comprehend is a **Natural Language Processor (NLP) service**. Find relationships between text to produce insights. Looks at data such as Customer emails, support tickets, social media and makes predictions.

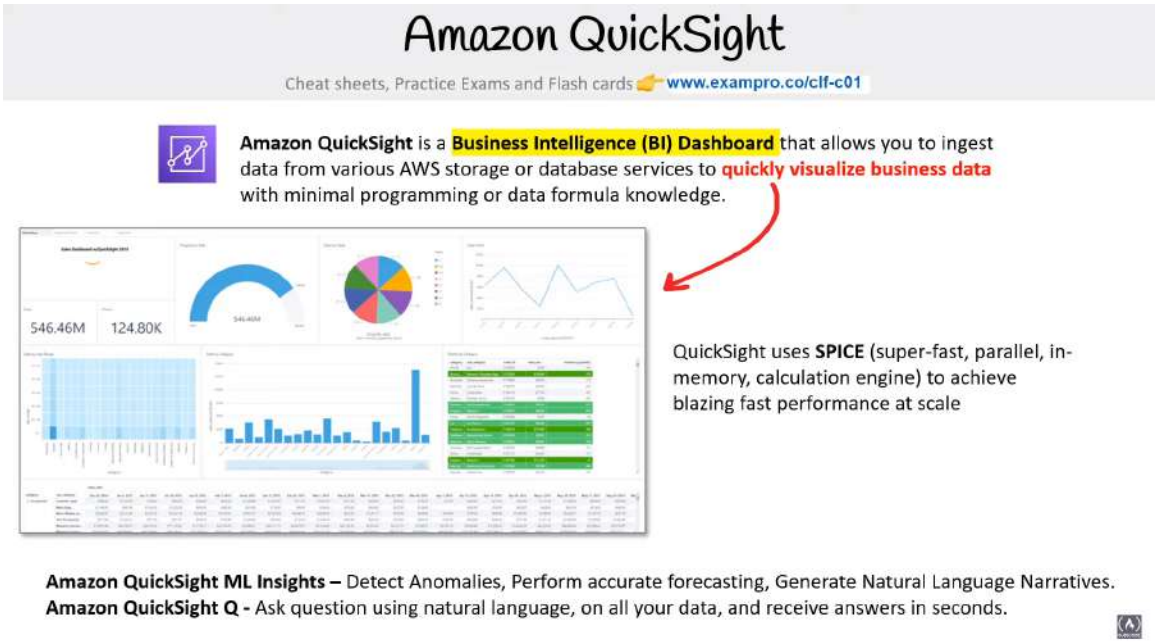


▼ 2. Big Data and Analysis Service



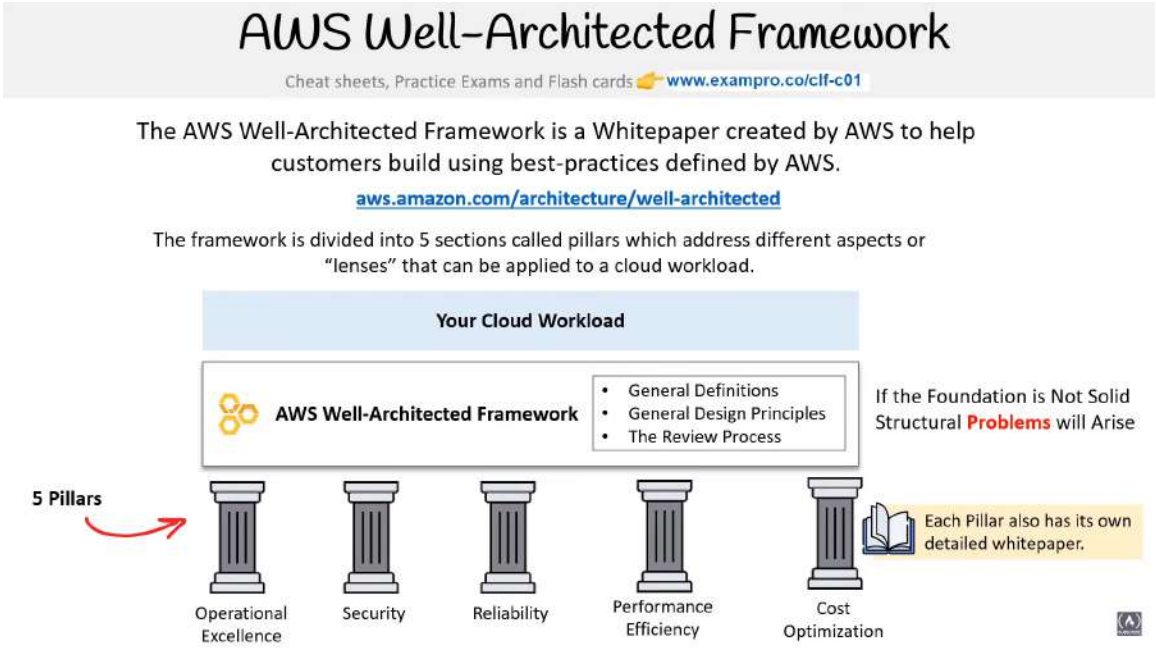


▼ 3. Amazon Quick Sight

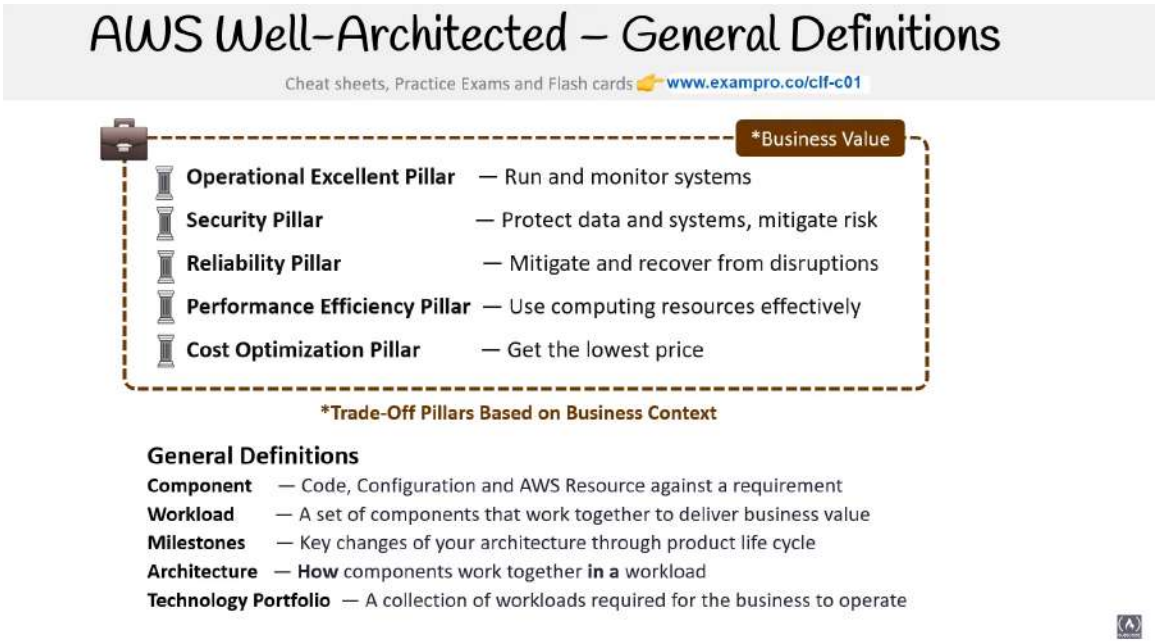


▼ 23. AWS Well-Architected Framework

▼ 1. The 5 Pillars



▼ 2. General Definitions



▼ 3. Operational Excellence Design Principles

▼ 4. Security Design Principles

▼ 5. Reliability Design Principles

▼ 6. Performance Efficiency Design Principles

▼ 7. Cost Optimization

AWS Well-Architected – Design Principles

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Cost Optimization Design Principles

Implement Cloud Financial Management:
Dedicate time and resources to build capability Cloud Financial Management and Cost Optimization tooling.

Adopt a consumption model
Pay only for the computing resources that you require and increase or decrease usage depending on business requirements

Measure overall efficiency
Measure the business output of the workload and the costs associated with delivering it.
Use this measure to know the gains you make from increasing output and reducing costs.

Stop spending money on undifferentiated heavy lifting
AWS does the heavy lifting of data center operations like racking, stacking, and powering servers.
It also removes the operational burden of managing operating systems and applications with managed services.
This allows you to focus on your customers and business projects rather than on IT infrastructure.

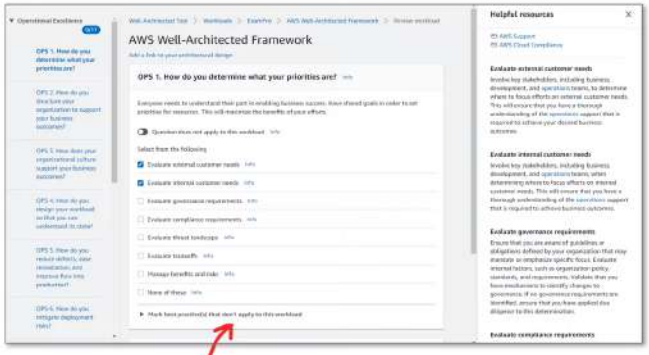
Analyze and attribute expenditure
The cloud makes it easier to accurately identify the usage and cost of systems, which then allows transparent attribution of IT costs to individual workload owners. This helps measure return on investment (ROI) and gives workload owners an opportunity to optimize their resources and reduce costs.

▼ 8. AWS Well Architected Tool

AWS Well-Architected Tool

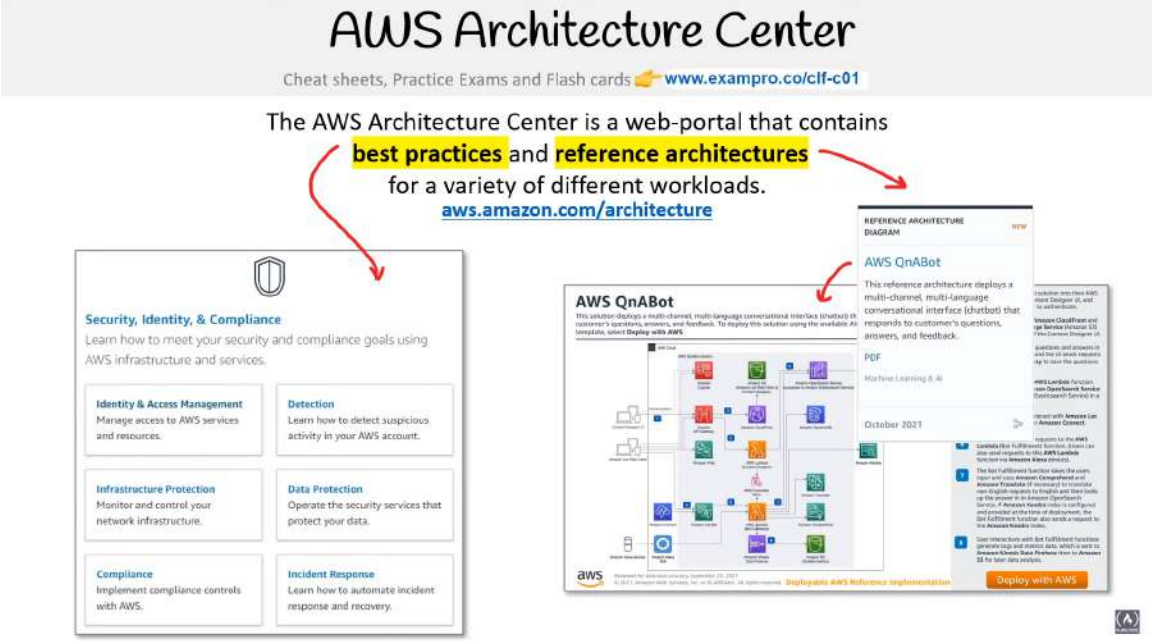
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

The Well-Architected Tool is **an auditing tool** to be used to asset your cloud workloads for alignment with the AWS Well Architected Framework.



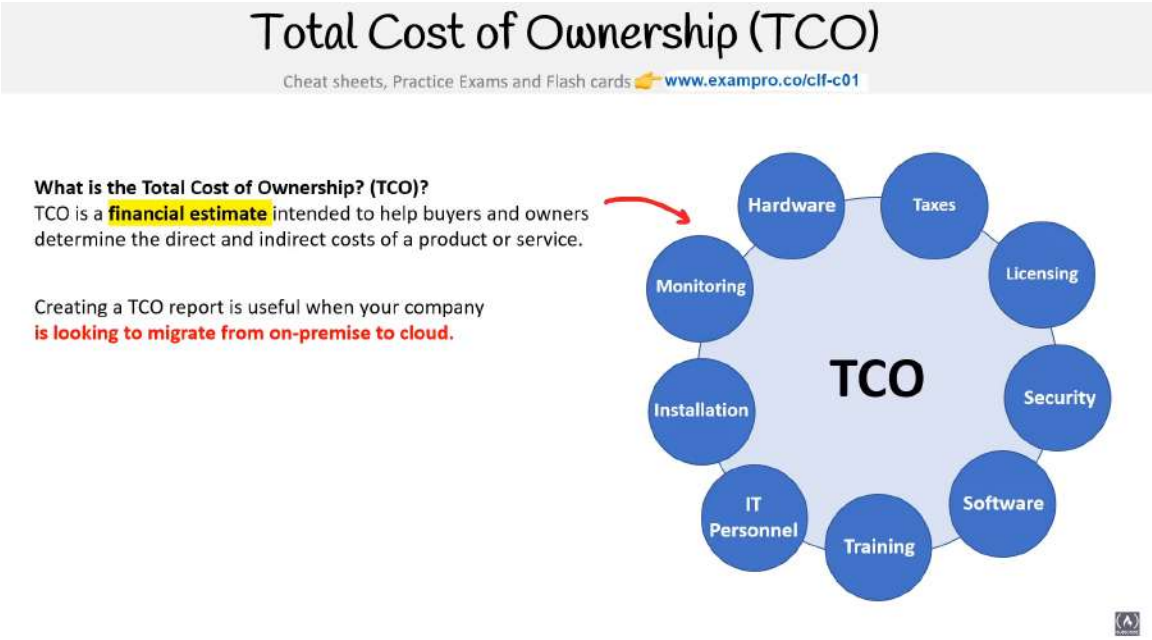
Its essentially **a checklist**, with nearby references to help you assemble a report to share with executives and key stake-holders

▼ 9. AWS Architecture Centre

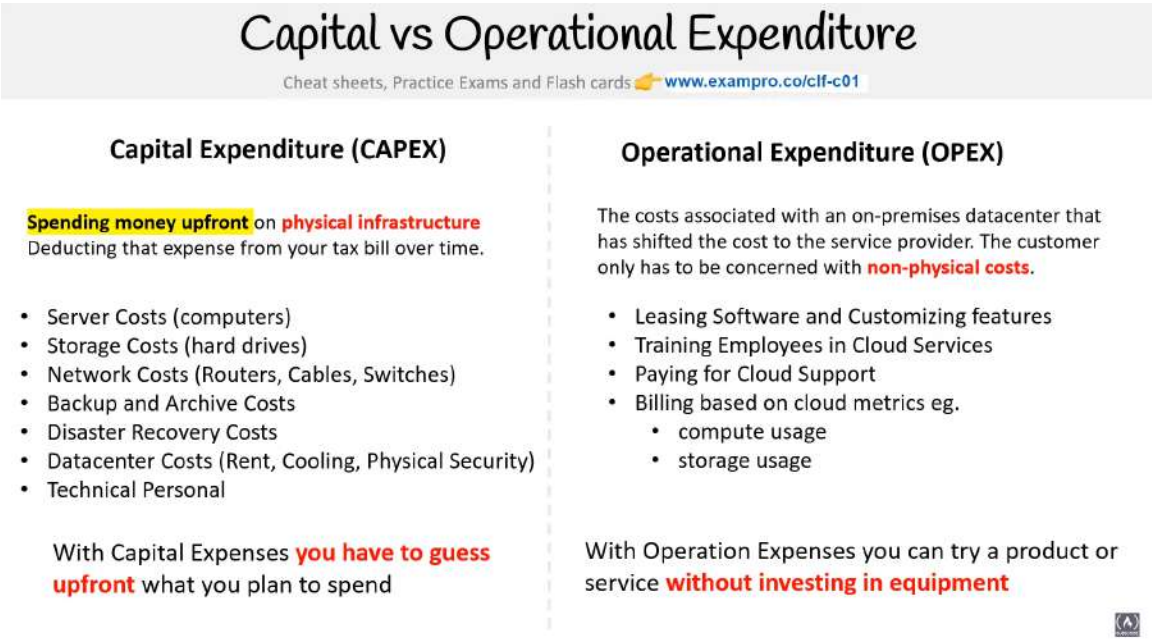


▼ 24. TCO and Migration

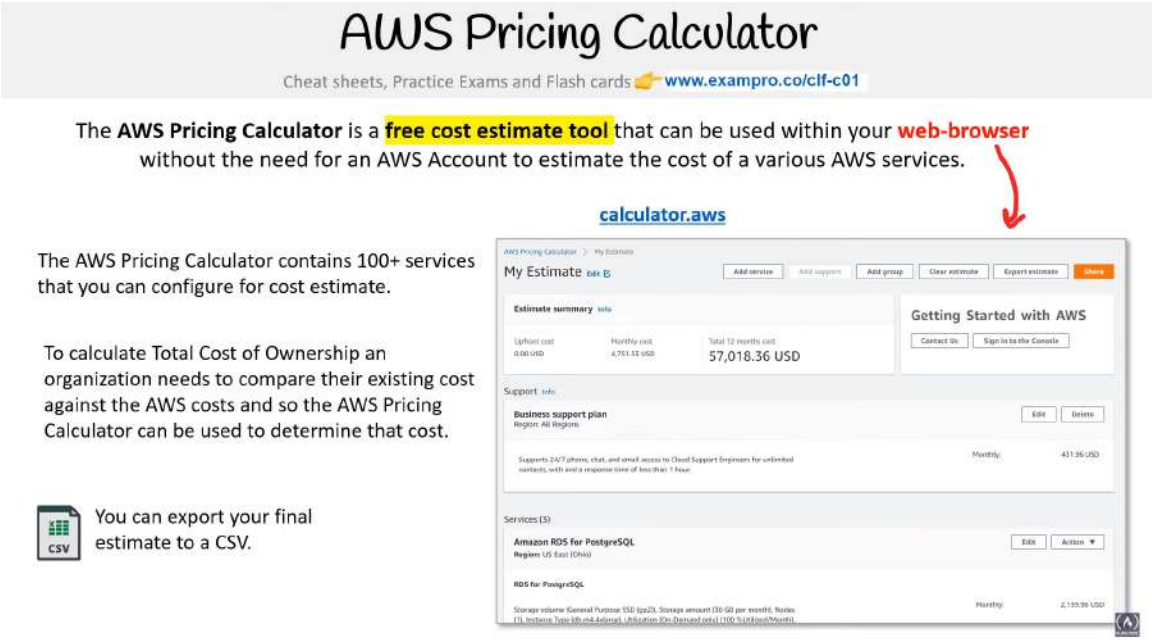
▼ 1. Total Cost of Ownership (TCO)



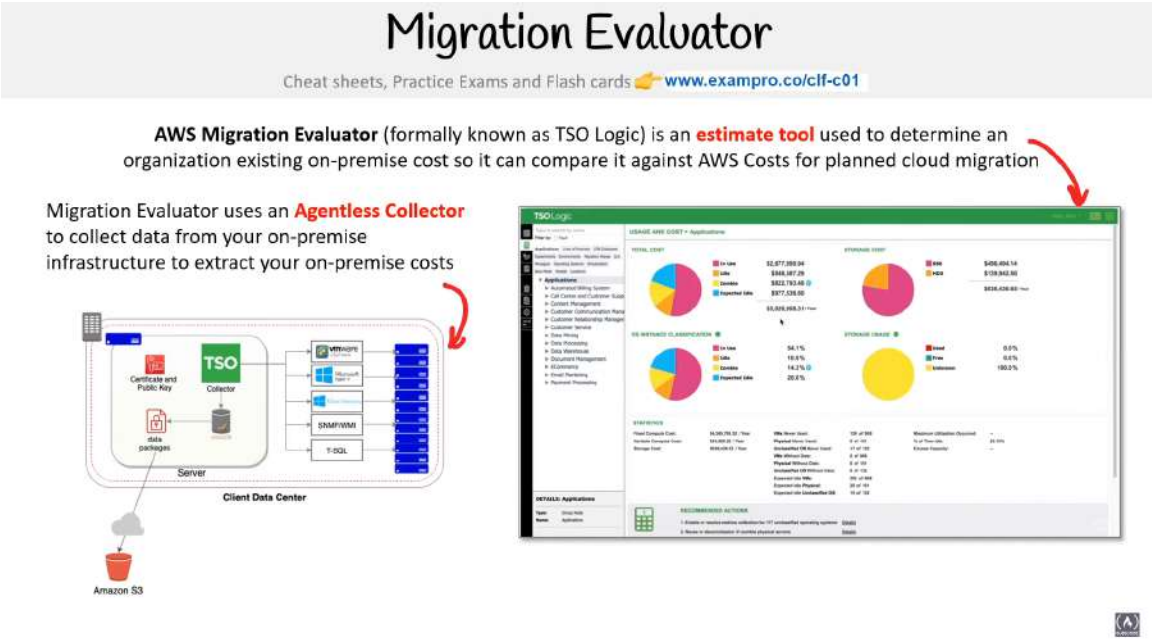
▼ 2. Capital Expenditure (CAPEX) vs Operational Expenditure (OPEX)



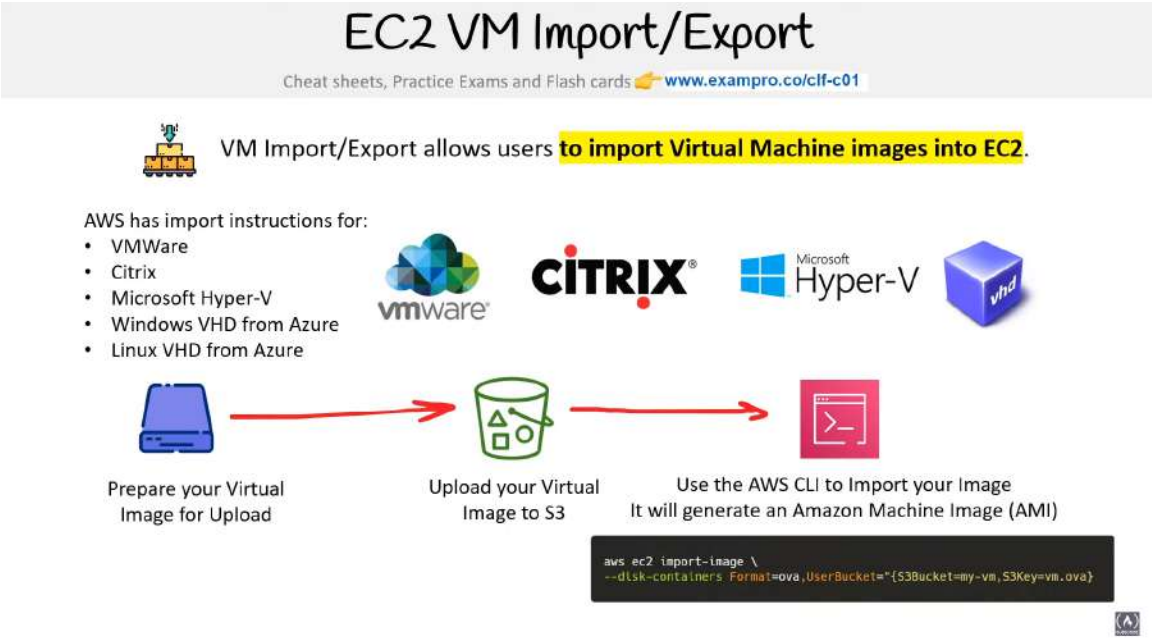
▼ 3. AWS Pricing Calculator



▼ 4. AWS Migration Evaluator



▼ 5. VM Import / Export



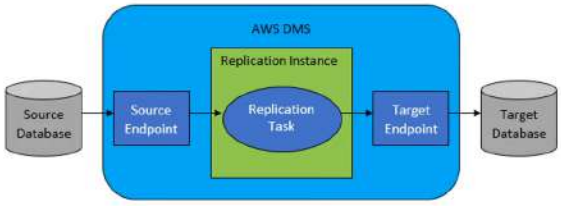
▼ 6. Database Migration Service (DMS)

Database Migration Service (DMS)

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

AWS Database Migration Service (DMS) allows you to quickly and securely migrate one database to another. DMS can be used to migrate your on-premise database to AWS.

Possible Sources:
- Oracle Database
- Microsoft SQL
- MySQL
- MariaDB
- PostgreSQL
- MongoDB
- SAP ASE
- IMDB Db2
- Azure SQL Database
- Amazon RDS
- Amazon S3 (database dumps)
- Amazon Aurora
- Amazon DocumentDB



AWS Schema Conversion Tool is used in many cases to automatically convert a source database schema to a target database schema.

Each migration path requires a bit of research since not all combination of sources and targets are possible.

Possible Targets:
- Oracle Database
- Microsoft SQL
- MySQL
- MariaDB
- PostgreSQL
- Redis
- SAP ASE
- Amazon Redshift
- Amazon RDS
- Amazon DynamoDB
- Amazon S3
- Amazon Aurora
- Amazon OpenSearch Service
- Amazon ElastiCache for Redis
- Amazon DocumentDB
- Amazon Neptune
- Apache Kafka

▼ 7. AWS Cloud Adoption Framework

AWS Cloud Adoption Framework (CAF)

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

The AWS Cloud Adoption Framework is a whitepaper to help you plan your migration from on-premise to AWS.

At the highest level, the AWS CAF organizes guidance into **six focus areas**.

1 Business Perspective e.g. Business Managers, Finance Managers, Budget Owners, and Strategy Stakeholders.

How to update the staff skills and organizational processes to optimize business value as they move ops to the cloud

2 People Perspective e.g. Human Resources, Staffing, People Managers.

how to update the staff skills and organizational processes to optimize and maintain their workforce, and ensure competencies are in place at the appropriate time.

3 Governance Perspective e.g. CIO, Program Managers, Project Managers, Enterprise Architects, Business Analysts

how to update the staff skills and organizational processes that are necessary to ensure business governance in the cloud, and manage and measure cloud investments to evaluate their business outcomes.

4 Platform Perspective e.g. CTO, IT Managers, Solution Architects.

how to update the staff skills and organizational processes that are necessary to deliver and optimize cloud solutions and services.

5 Security Perspective e.g. CISO, IT Security Managers, IT Security Analysts.

how to update the staff skills and organizational processes that are necessary to ensure that the architecture deployed in the cloud aligns to the organization's security control requirements, resiliency, and compliance requirements.

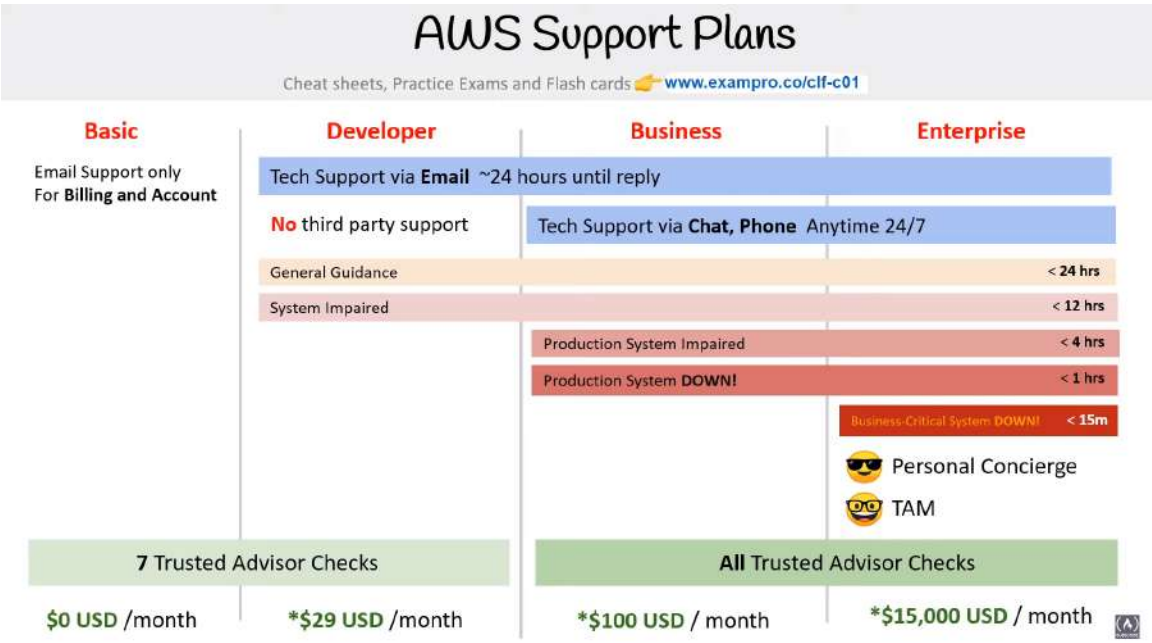
6 Operations Perspective e.g. IT Operations Managers, IT Support Managers.

how to update the staff skills and organizational processes that are necessary to ensure system health and reliability during the move of operations to the cloud and then to operate using agile, ongoing, cloud computing best practices.

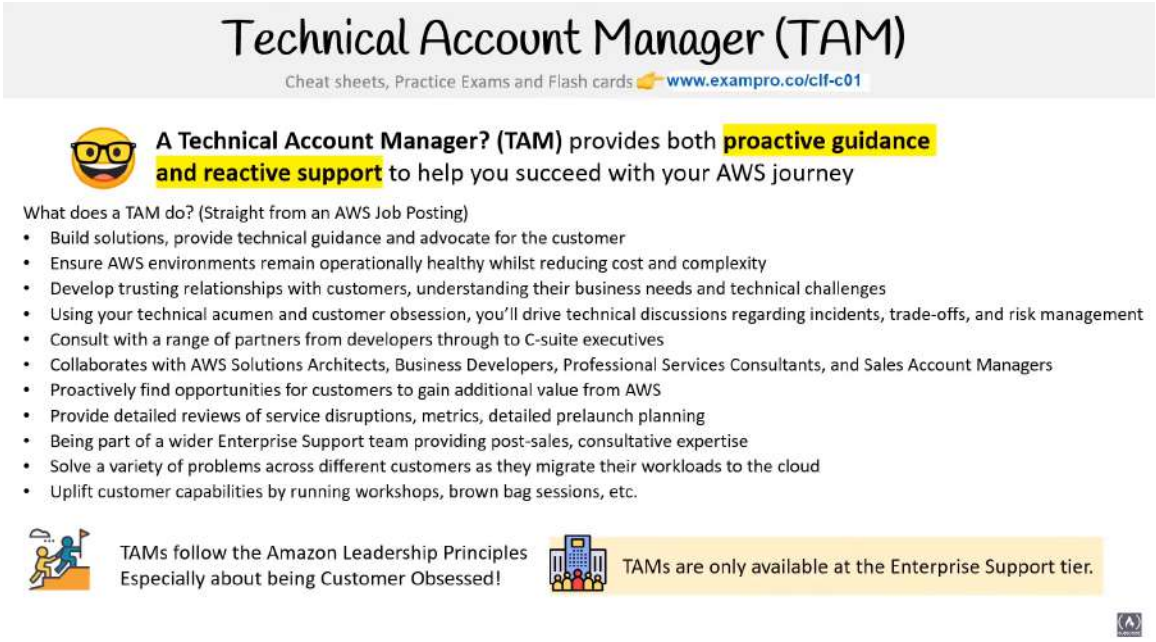
▼ 25. AWS Billing and Pricing

▼ 1. AWS Free Services

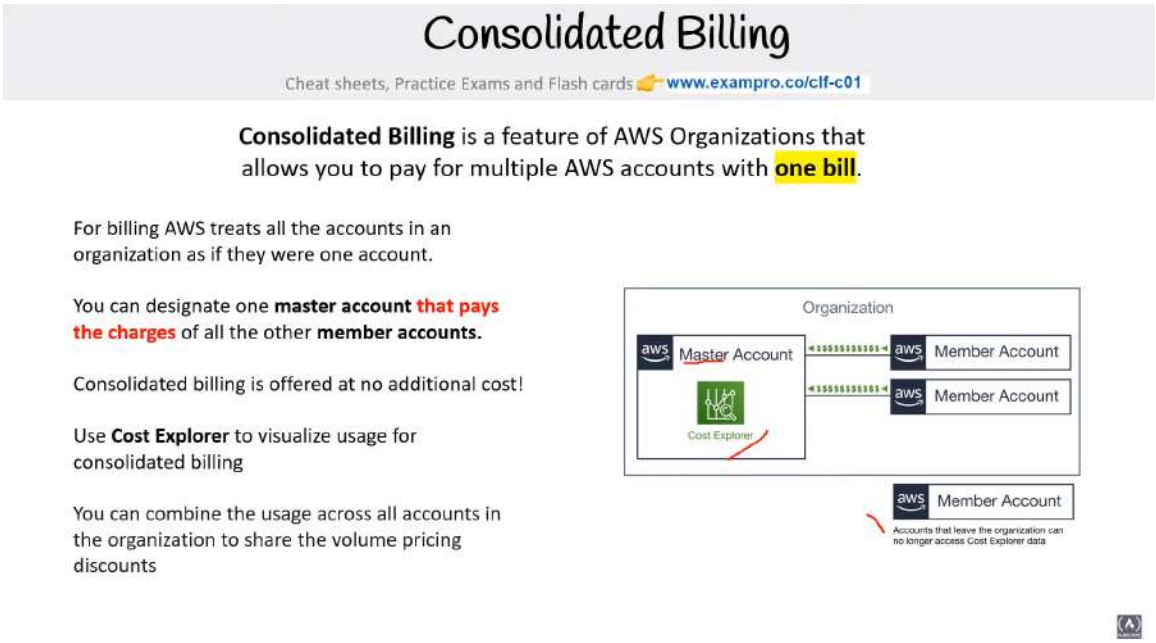
▼ 2. Support Plans



▼ 3. Technical Account Manager



▼ 4. Consolidated Billing

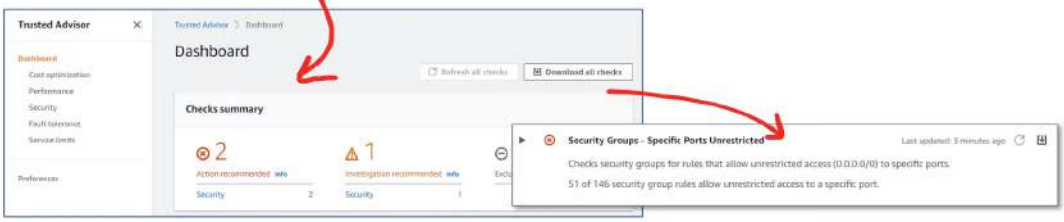


▼ 5. AWS Trusted Advisor

AWS Trusted Advisor

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS Trusted Advisor is a **recommendation tool** which automatically and actively monitors your AWS account to provide **actional recommendations** across a series of categories.



Think of AWS Trusted Advisor like an automated checklist of best practices on AWS

The 5 categories of AWS Trusted Advisor

- Cost Optimization – How can we save money?
- Performance – How can improve performance?
- Security – How we can improve security?
- Fault Tolerance – How can we prevent a disaster or data loss?
- Service Limits – Are we are going to hit the maximum limit for a service?

AWS Trusted Advisor

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

Cost Optimization

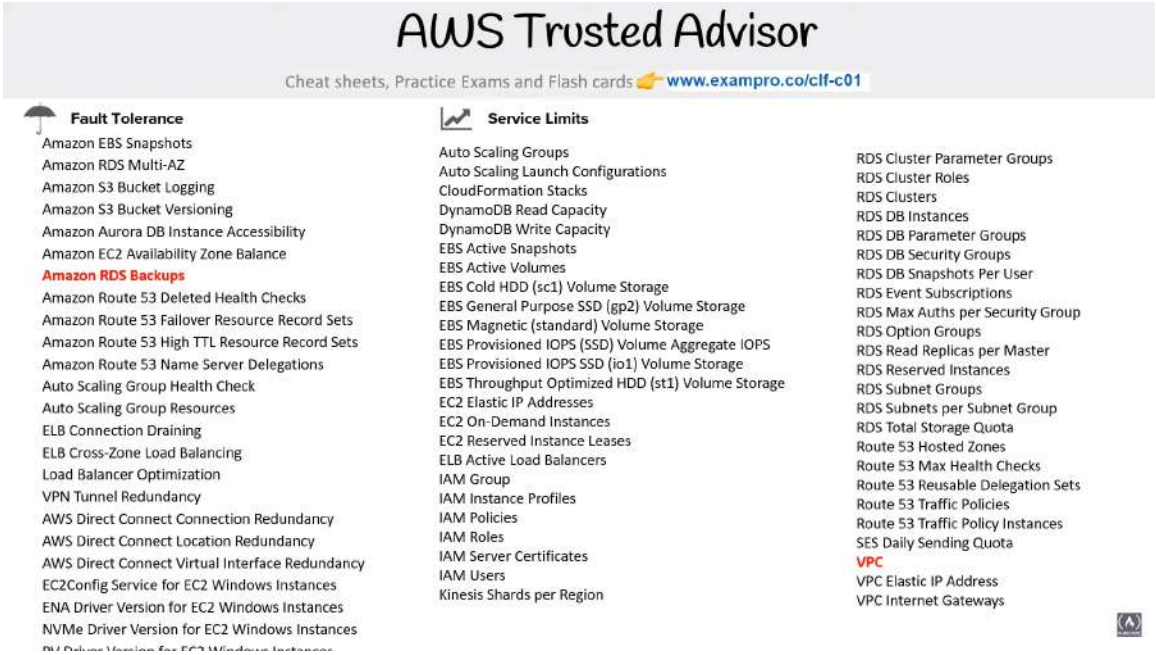
Amazon EC2 Reserved Instances Optimization
Low Utilization Amazon EC2 Instances
Underutilized Amazon EBS Volumes
Amazon EC2 Reserved Instance Lease Expiration
Amazon RDS Idle DB Instances
Amazon Route 53 Latency Resource Record Sets
Idle Load Balancers
Unassociated Elastic IP Addresses
Underutilized Amazon Redshift Clusters

Performance

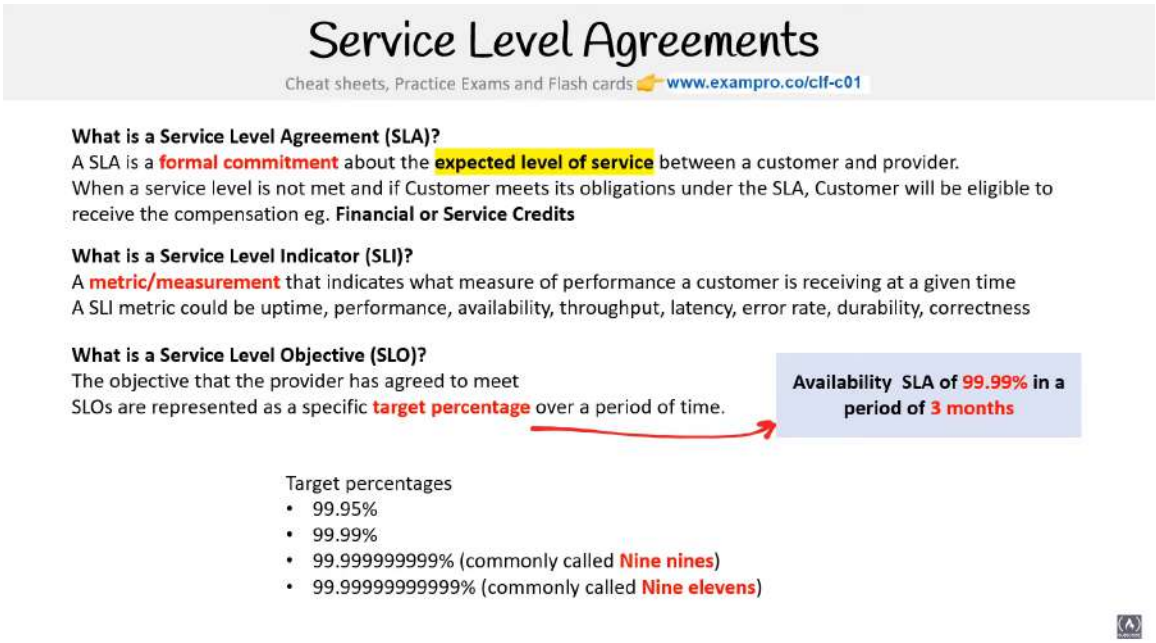
CloudFront Alternate Domain Names
Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration
Amazon EC2 to EBS Throughput Optimization
Amazon Route 53 Alias Resource Record Sets
CloudFront Content Delivery Optimization
CloudFront Header Forwarding and Cache Hit Ratio
High Utilization Amazon EC2 Instances
Large Number of EC2 Security Group Rules Applied to an Instance
Large Number of Rules in an EC2 Security Group
Overutilized Amazon EBS Magnetic Volumes

Security

AWS CloudTrail Logging
IAM Password Policy
MFA on Root Account
Security Groups - Specific Ports Unrestricted
Security Groups - Unrestricted Access
Amazon S3 Bucket Permissions
IAM Access Key Rotation
Amazon EBS Public Snapshots
Amazon RDS Public Snapshots
Amazon RDS Security Group Access Risk
Amazon Route 53 MX Resource Record Sets and Sender Policy Framework
CloudFront Custom SSL Certificates in the IAM Certificate Store
CloudFront SSL Certificate on the Origin Server
ELB Listener Security
ELB Security Groups
Exposed Access Keys
IAM Use



▼ 6. Service Level Agreement (SLA)

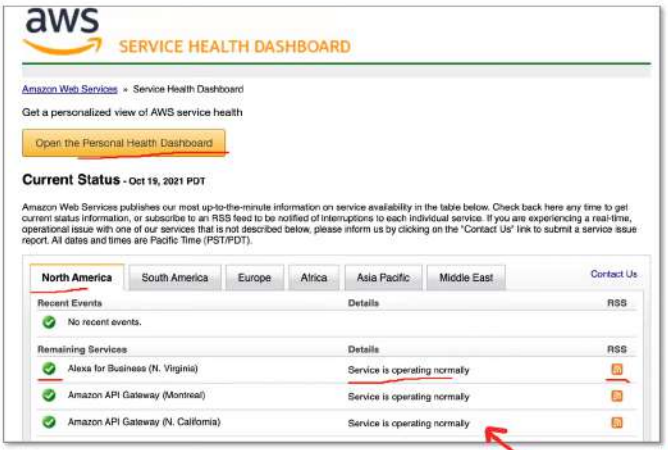


▼ 7. Service Health Dashboard

Service Heath Dashboard

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

The **Service Health Dashboard** shows the general status of AWS services,



An **icon** and **details** will indicate the status of each AWS Service

▼ 8. Personal Health Dashboard

AWS Personal Heath Dashboard

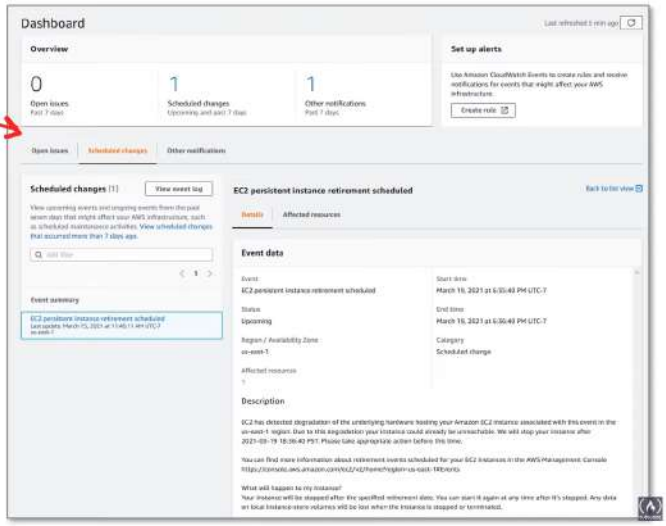
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS Personal Health Dashboard provides **alerts and guidance** for AWS events that might affect your environment.

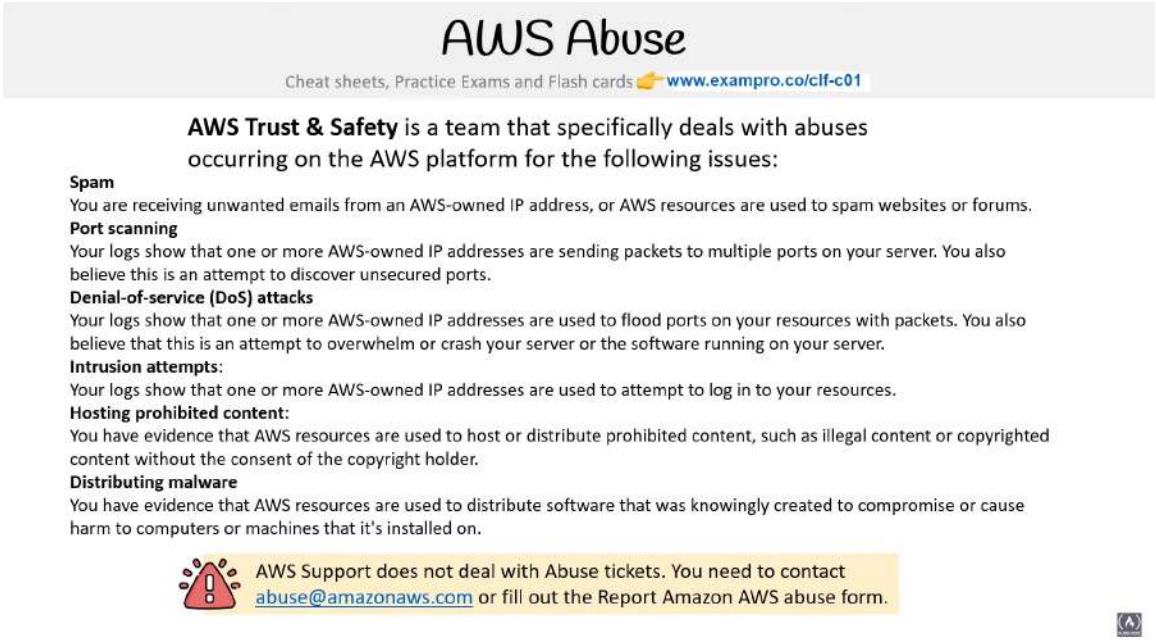
All AWS customers can access the Personal Health Dashboard.

The Personal Health Dashboard shows recent events to help you manage active events, and shows proactive notifications so that you can plan for scheduled activities

Use these alerts to get notified about changes that can affect your AWS resources, and then follow the guidance to diagnose and resolve issues.

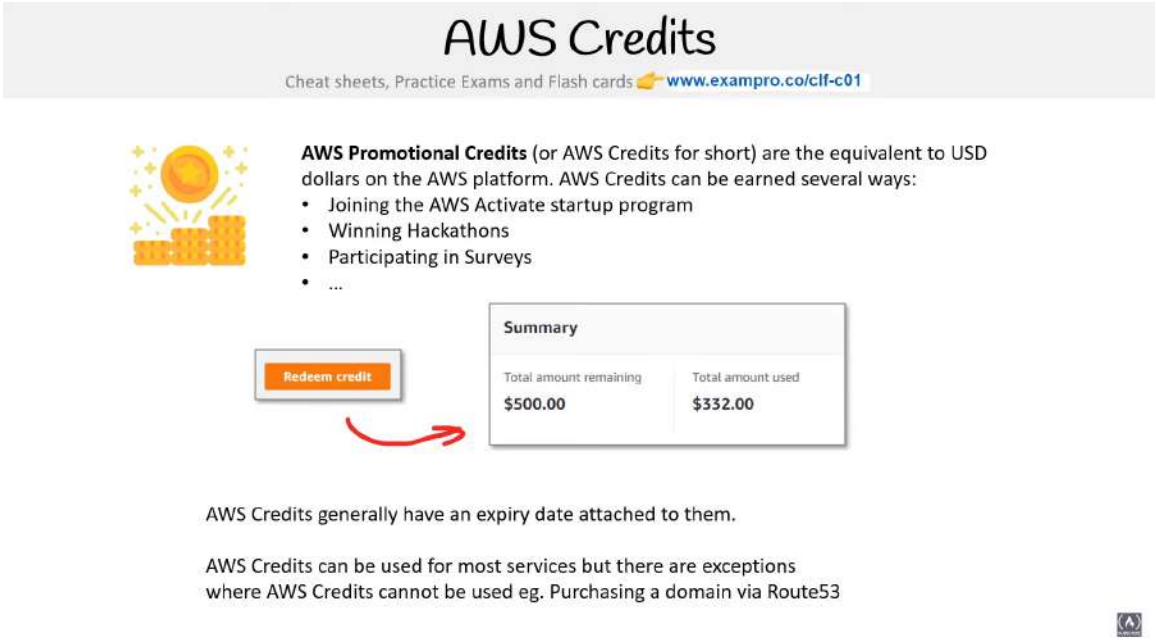


▼ 9. AWS Abuse

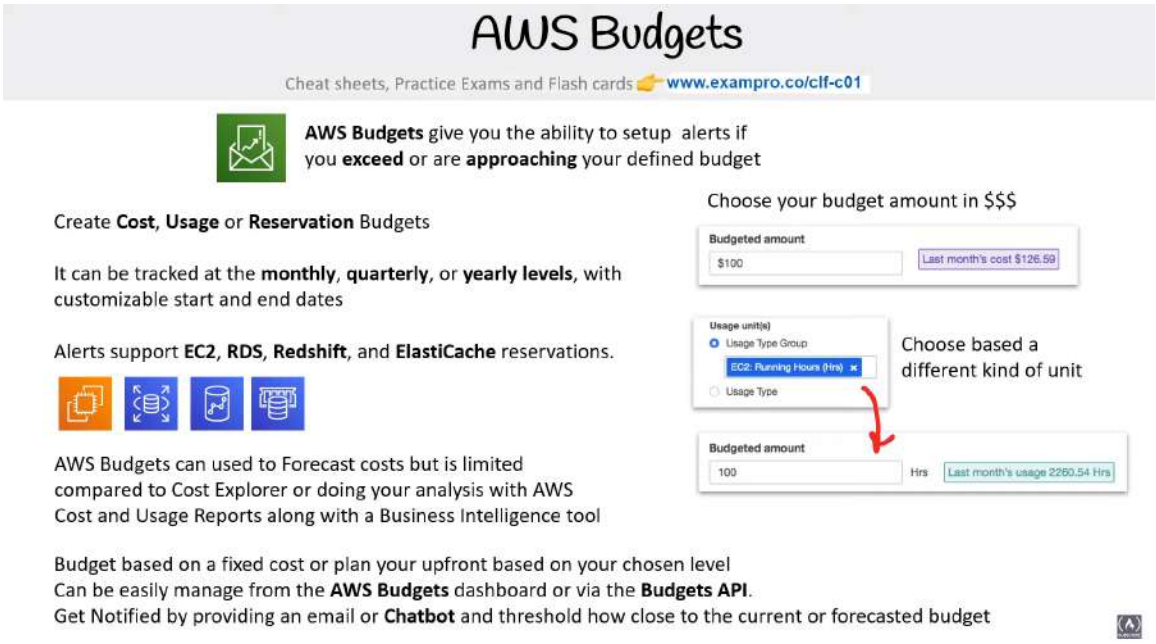


▼ 10. AWS Free-Tier

▼ 11. AWS Credits

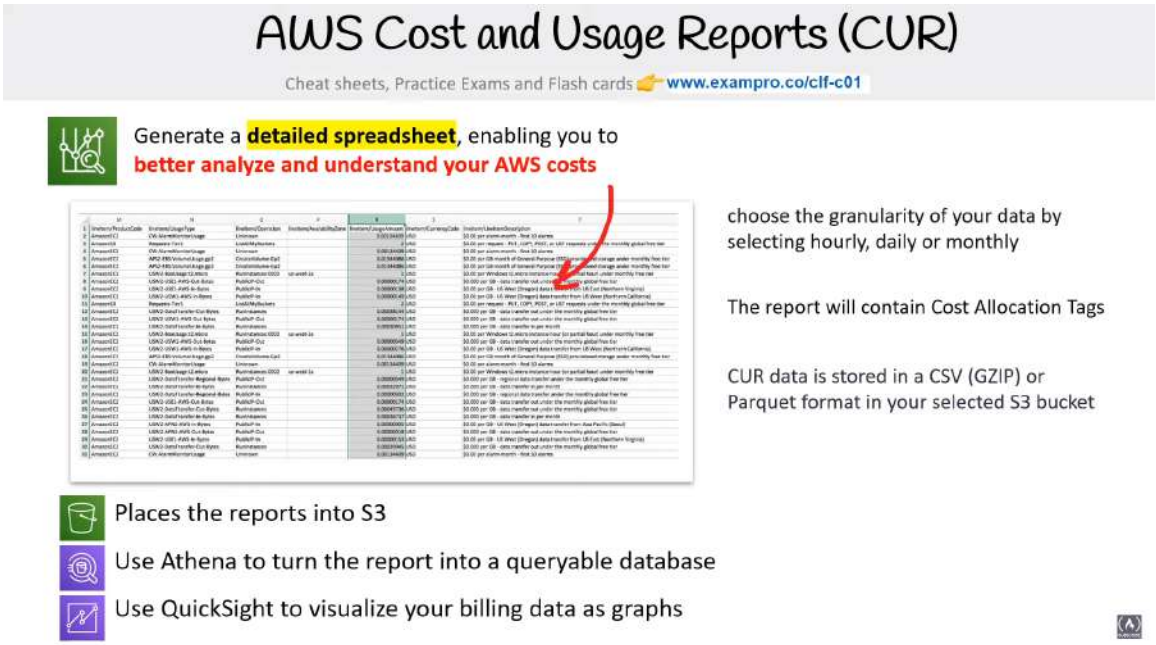


▼ 12. AWS Budgets

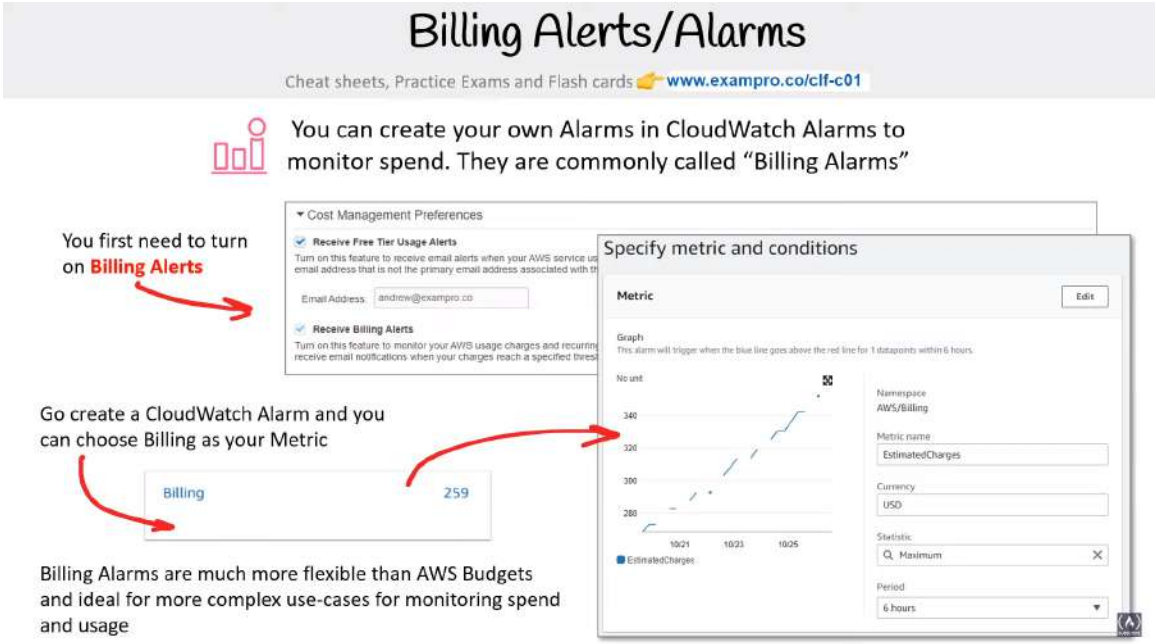


▼ 13. AWS Budget Reports

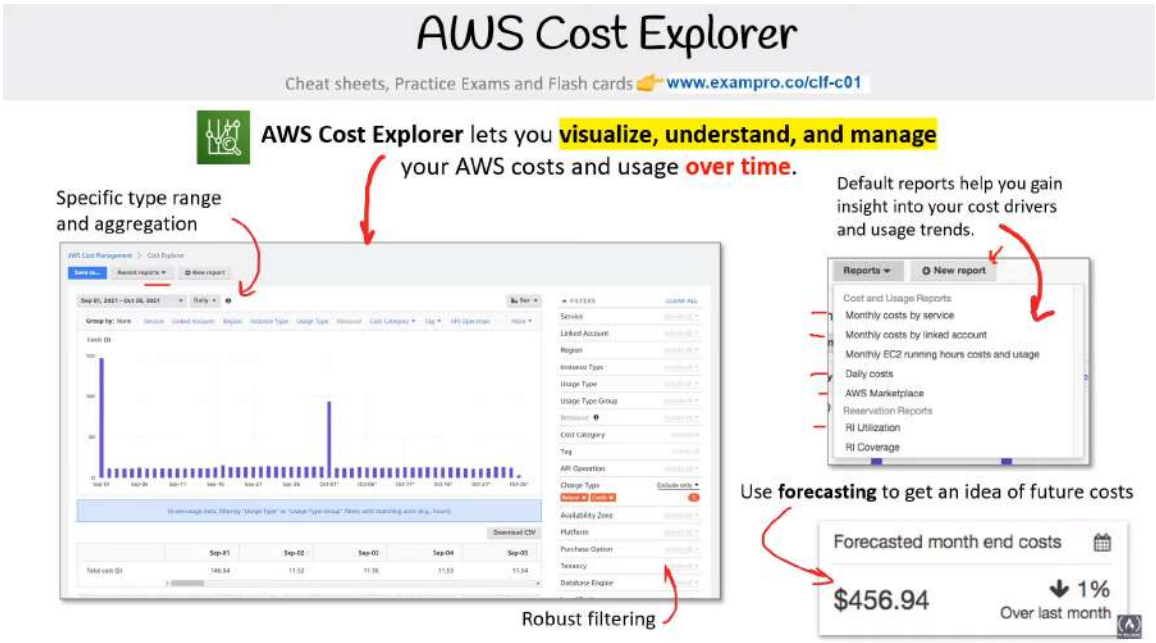
▼ 14. AWS Cost and Usage Reports



▼ 15. Billing Alerts / Alarms



▼ 16. AWS Cost Explorer



▼ 17. AWS Pricing API

AWS Pricing API

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

With AWS you can programmatically access pricing information to get the latest price offering for services.

There are two versions of this API:

- Query API – The Pricing Service API via **JSON**
  - https://api.pricing.us-east-1.amazonaws.com
- Batch API – The Price List API via **HTML**
  - https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/index.json

You can also subscribe to Amazon Simple Notification Service (Amazon SNS) notifications to get alerts when prices for the services change.

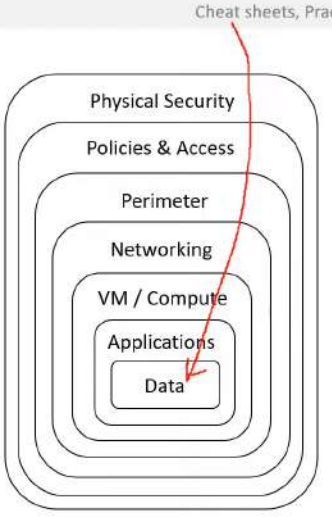
AWS prices change periodically, such as when AWS cuts prices, when new instance types are launched, or when new services are introduced

▼ 26. Security

▼ 1. 7 Layers of Security

Defense in Depth

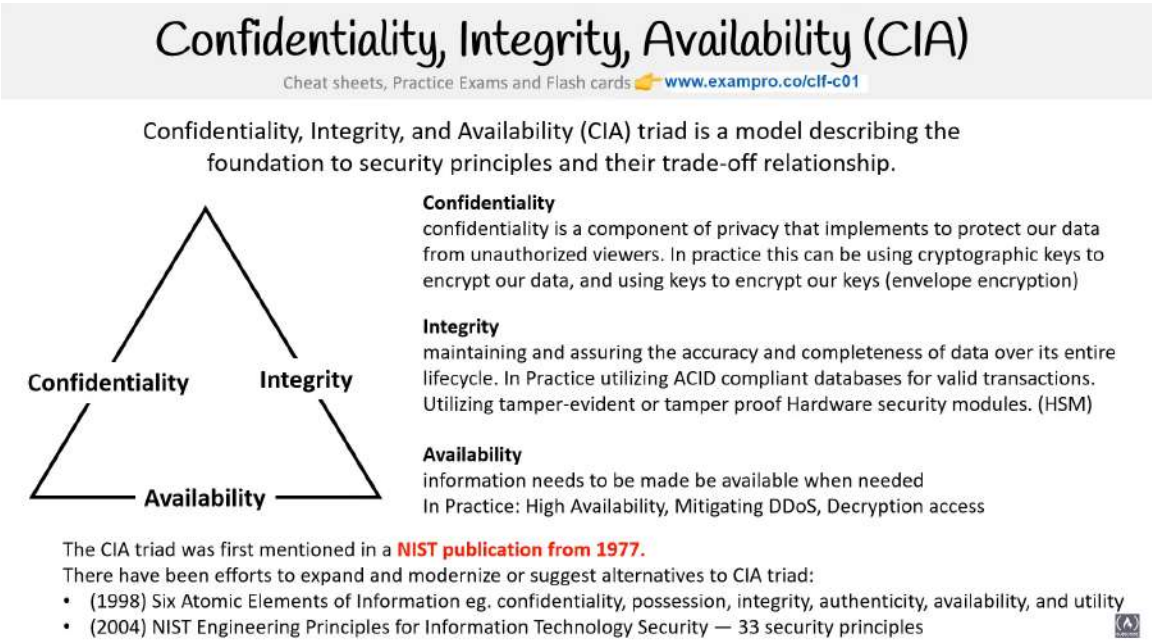
Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01



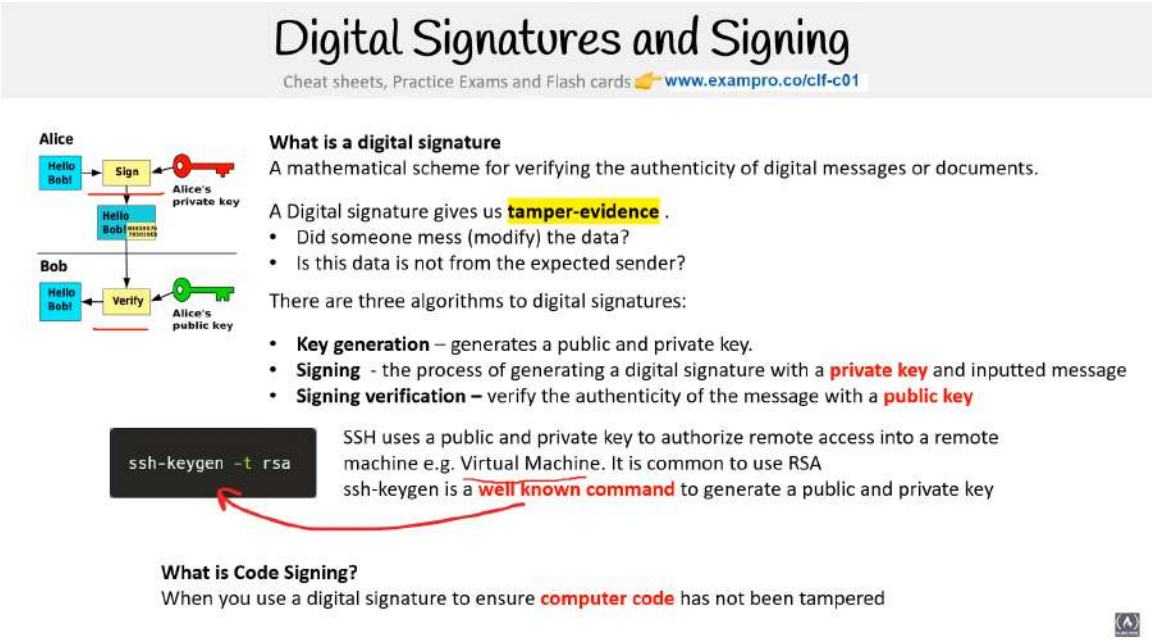
The 7 Layers of Security

1. Data
access to business and customer data, and encryption to protect data.
2. Application
applications are secure and free of security vulnerabilities.
3. Compute
Access to virtual machines (ports, on-premise, cloud)
4. Network
limit communication between resources using segmentation and access controls.
5. Perimeter
distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
6. Identity and access
controlling access to infrastructure and change control.
7. Physical
limiting access to a datacenter to only authorized personnel.

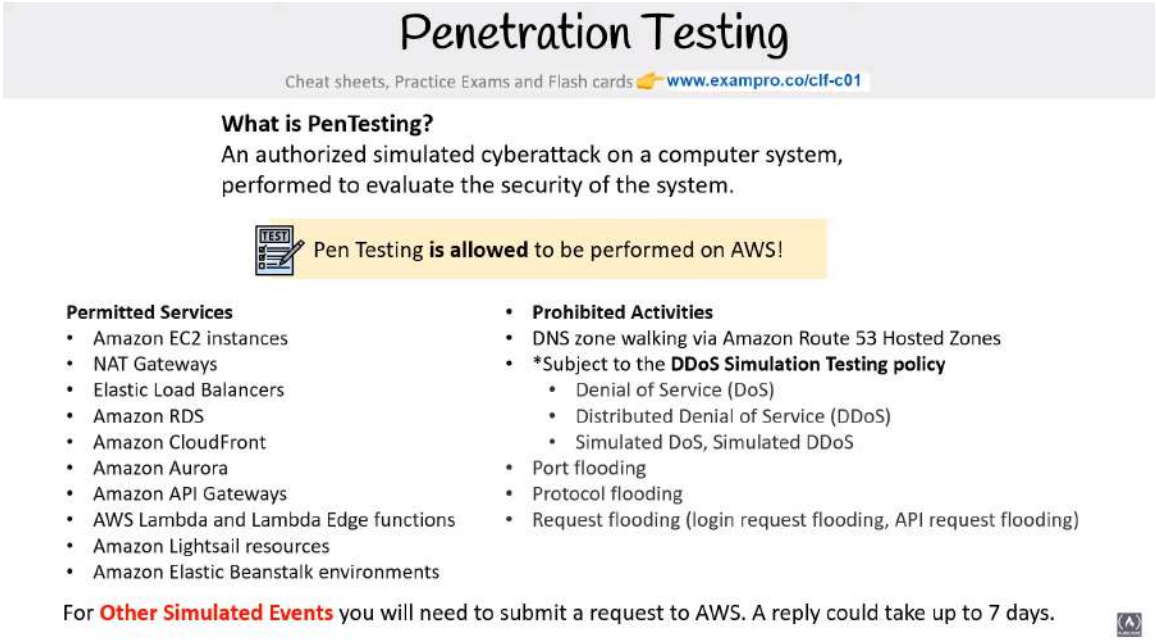
▼ 2. CIA Triad



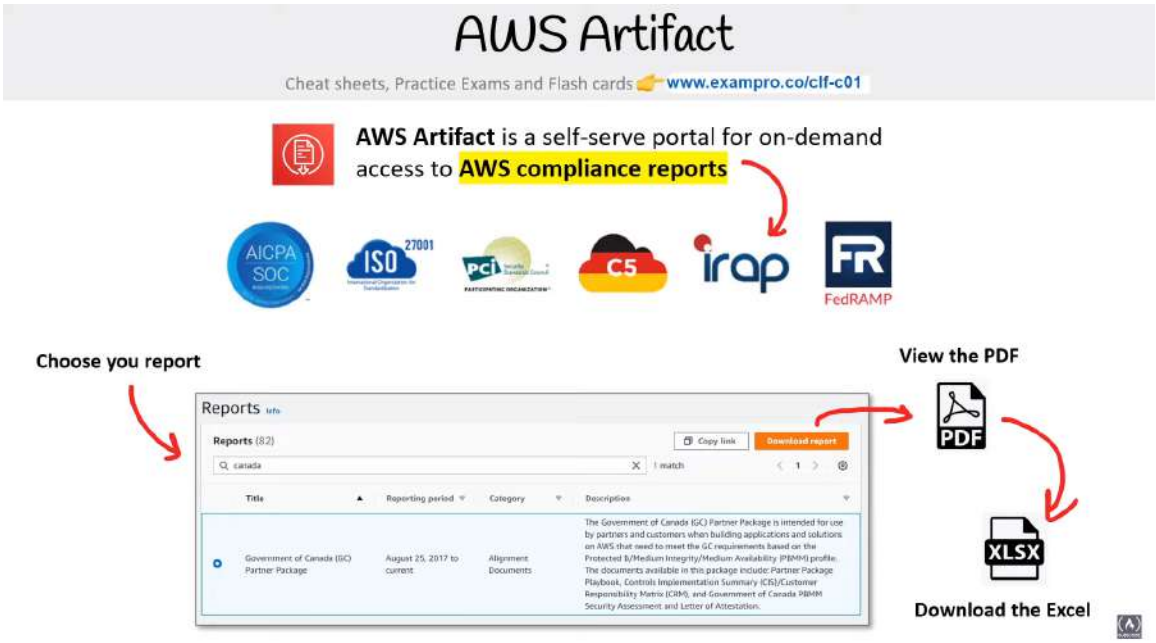
▼ 3. Digital Signature and Signing



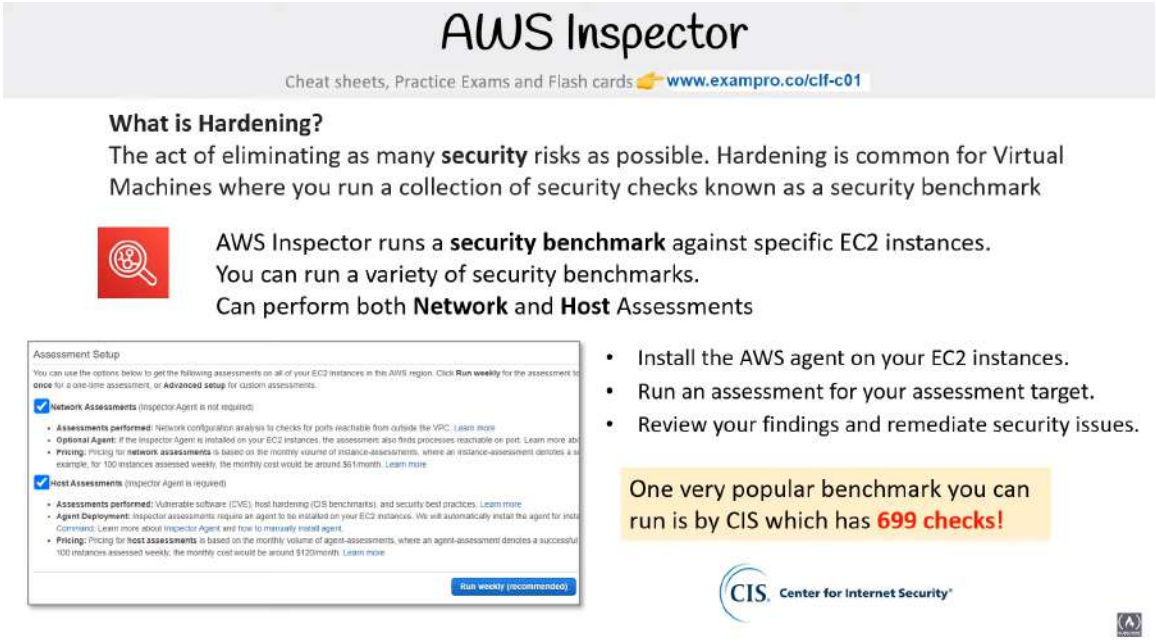
▼ 4. Penetration Testing



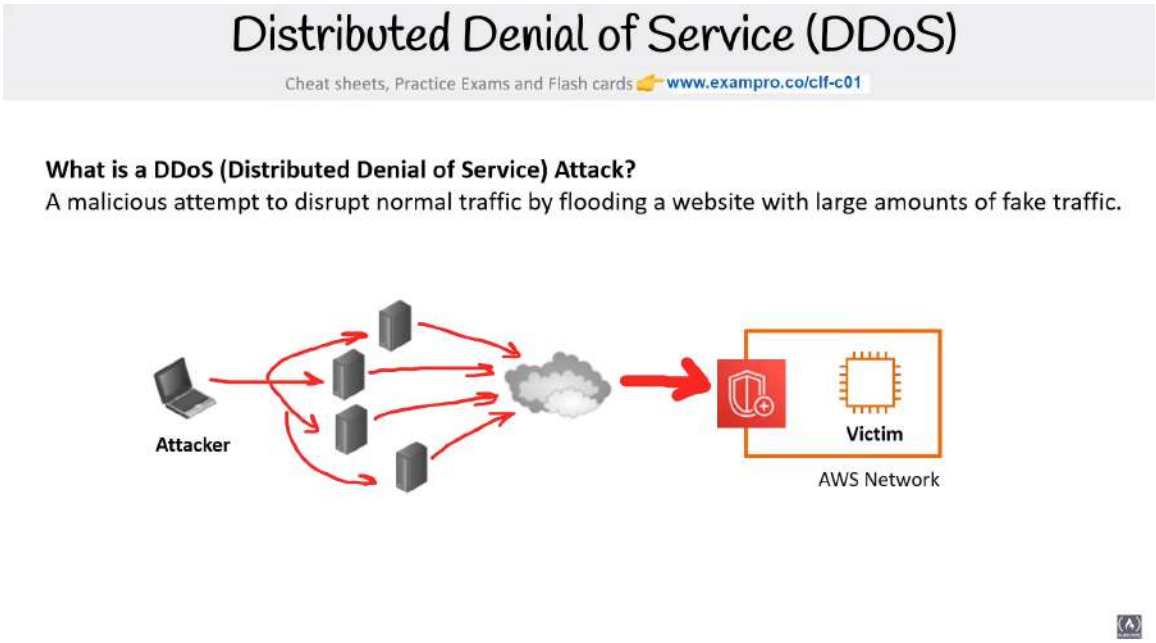
▼ 5. AWS Artifact



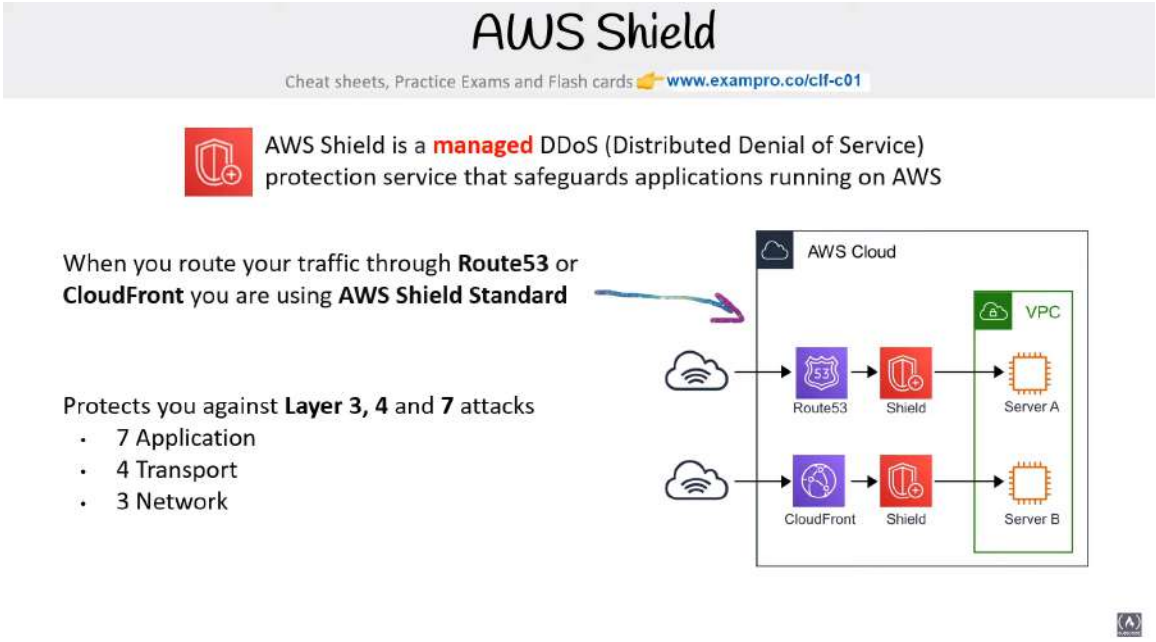
▼ 6. AWS Inspector



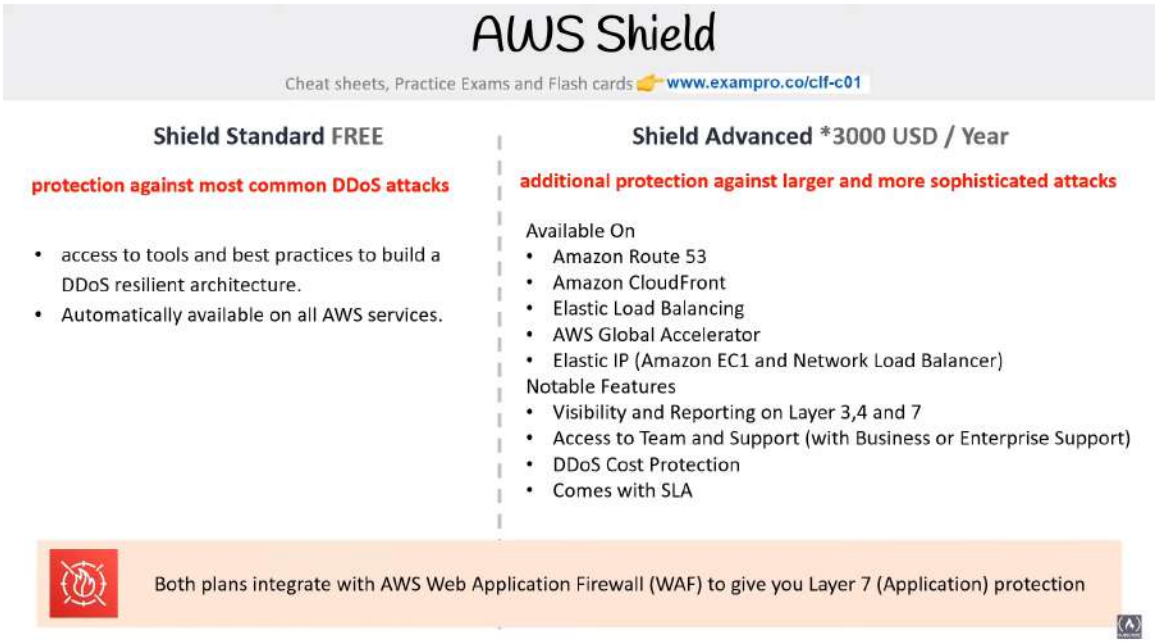
▼ 7. DDoS Attack



▼ 8. AWS Shield



▼ 9. Shield Standard vs Shield Advanced



▼ 10. Guard Duty

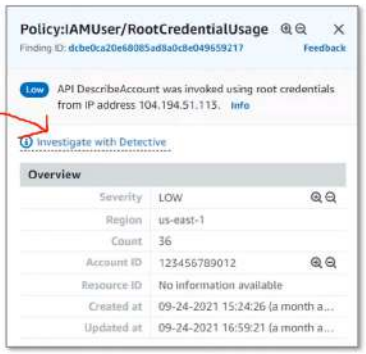
Amazon Guard Duty

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

What is IDS/IPS?
Intrusion Detection System and Intrusion Protection System.
A device or software application that monitors a network or systems for malicious activity or policy violations.

Guard Duty is a **threat detection service** that continuously monitors for malicious, suspicious activity and unauthorized behavior. It uses Machine Learning to analyze the following AWS logs:

- CloudTrail Logs
- VPC Flow Logs
- DNS logs



It will alert you of **Findings** which you can automate a incident response via CloudWatch Events or with 3rd Party Services

▼ 11. Amazon Macie

Amazon Macie

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Macie is a fully managed service that continuously monitors **S3 data access** activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks.

Macie works by uses Machine Learning to Analyze your CloudTrail logs

Macie has a variety of alerts

- Anonymized Access
- Config Compliance
- Credential Loss
- Data Compliance
- File Hosting
- Identity Enumeration
- Information Loss
- Location Anomaly
- Open Permissions
- Privilege Escalation
- Ransomware
- Service Disruption
- Suspicious Access

Macie's will identify your most at-risk users which could lead to a compromise

▼ 12. VPN

AWS Virtual Private Network (VPN)

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS VPN lets you establish a **secure** and **private tunnel** from your network or device to the AWS global network

AWS Site-to-Site VPN
securely connect on-premises network or branch office site to VPC

AWS Client VPN
securely connect users to AWS or on-premises networks

What is IPSec?
Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs)

▼ 13. WAF

AWS WAF

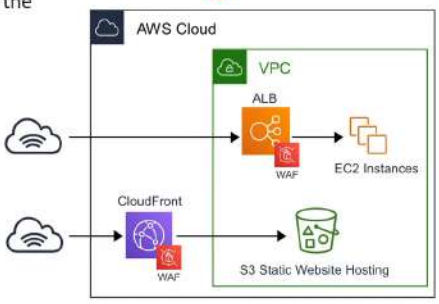
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS **Web Application Firewall (WAF)** protect your web applications from common web exploits

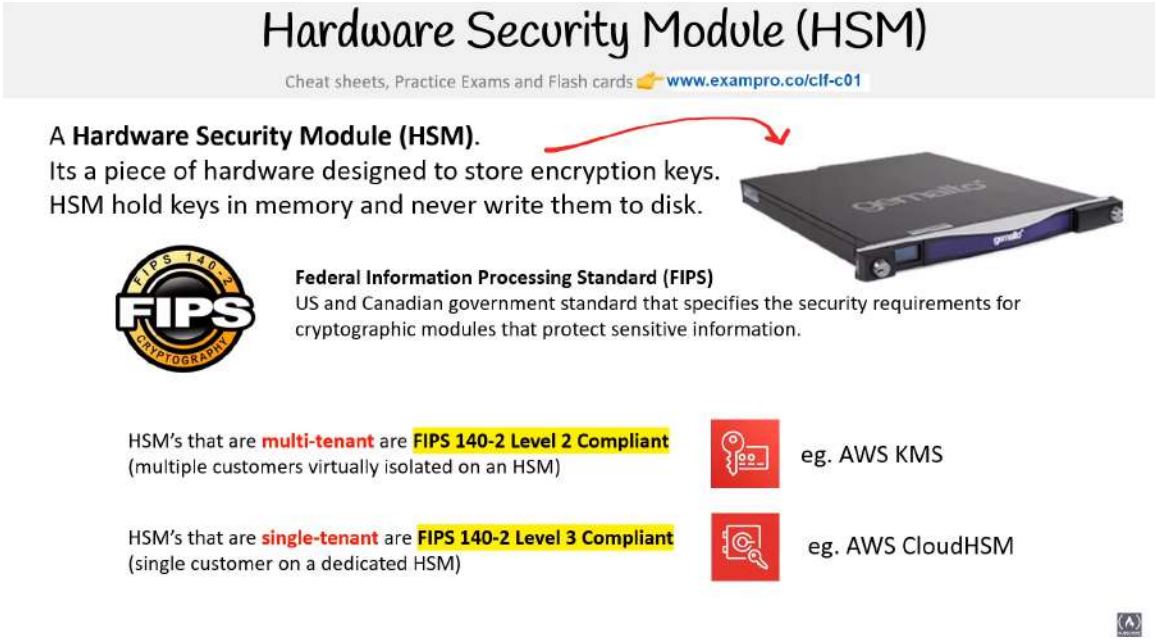
Write your own **rules** to ALLOW or DENY traffic based on the contents of an HTTP requests
Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Rules Marketplace
WAF can be attached to either **CloudFront** or an **Application Load Balancer**

Protect web applications from attacks covered in the **OWASP Top 10** most dangerous attacks:

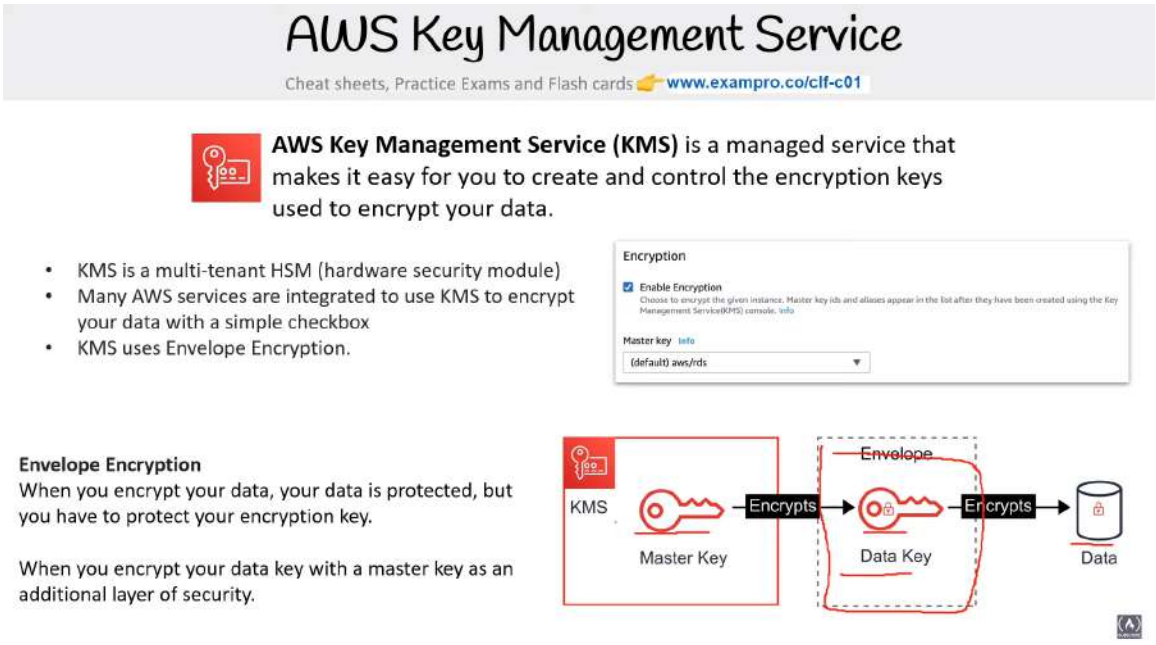
1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilitie
10. Insufficient logging and monitoring



▼ 14. Hardware Security Module



▼ 15. AWS KSM



▼ 16. AWS Cloud HSM

CloudHSM

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

CloudHSM is a single-tenant HSM as a service that automates hardware provisioning, software patching, high availability and backups.

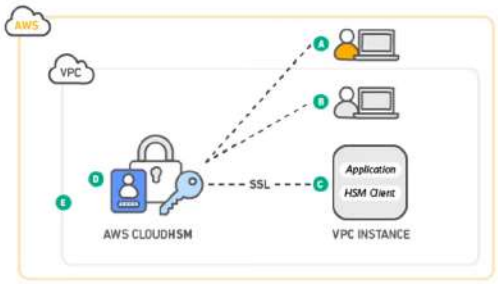
AWS CloudHSM enables you to generate and use your encryption keys on a FIPS 140-2 Level 3 validated hardware.

Built on Open HSM industry standards to integrate with:

- PKCS#11
- Java Cryptogrpahy Extensions (JCE)
- Microsoft CryptoNG (CNG) libraries

You can also transfer your keys to other commercial HSM solutions to make it easy for you to migrate keys on or off of AWS.

Configure AWS KMS to use AWS CloudHSM cluster as a custom key store rather than the default KMS key store.



▼ 27. Variation Study

▼ 1. AWS Config vs AWS AppConfig

AWS Config vs AWS AppConfig

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

AWS Config

AWS Config is a governance tool for Compliance as Code (CoC).

You can create rules that will check to see if resources are configured the way you expect them to be.

If a resource drifts from the expected configuration you are notified or AWS Config can auto-remediate (correct) the configuration back to the expected state

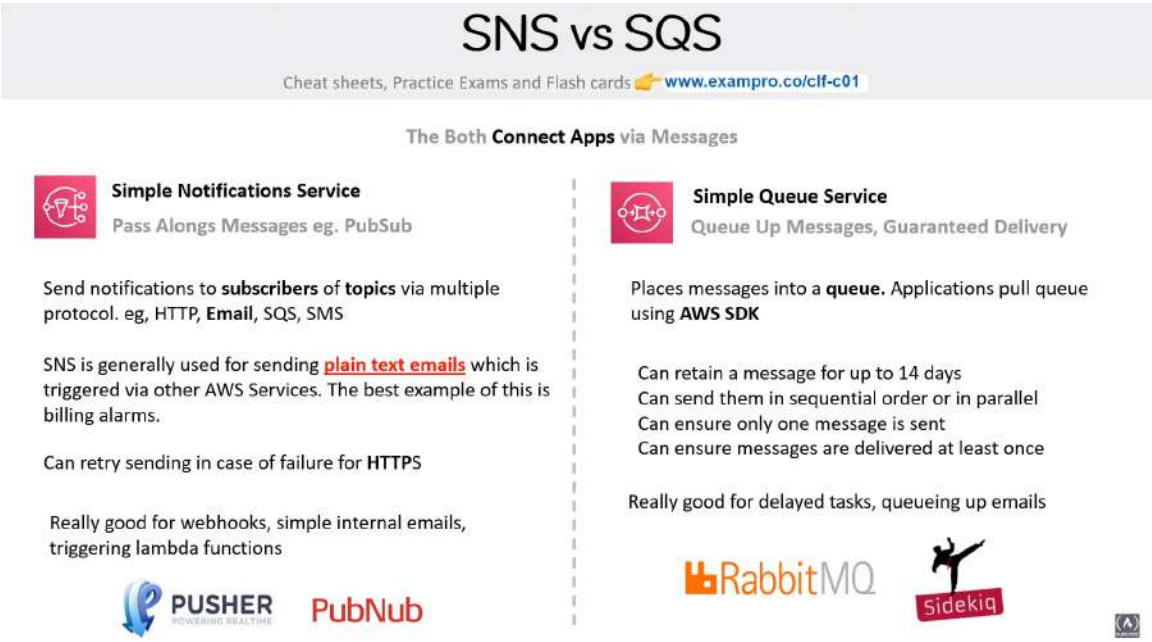
AWS AppConfig

AWS App Config is used to automat the process of deploying application configuration variable changes to your web-application(s).

You can write a validator to ensure the changed variable will not break your web-app

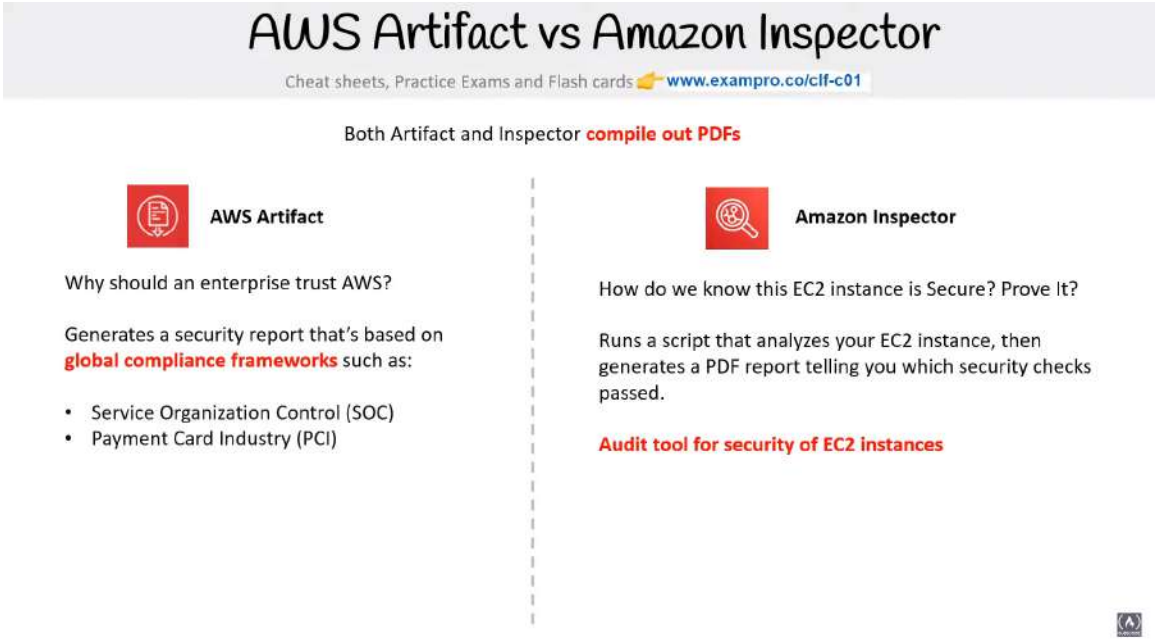
You can monitor deployments and automate integrations to catch errors or rollback.

▼ 2. SNS vs SQS



▼ 3. AWS Inspector vs AWS Trusted Advisor

▼ 4. AWS Artifact vs AWS Inspector



▼ 5. Types of Load Balancers