Cloud Practitioner

Spis treści

Exam Guide Walkthrough

Here we will go over the Exam Guide Outline, I want to highlight the most important information for you so you have an idea of what we're trying to study for. We have four domains here.

We have: **Cloud Concepts** 28% | **Security** 24% | **Technology** 36% | **Billing and Pricing** 12%

The largest portion of the exam is Technology at 36% and Billing and Pricing is the lowest which is funny because I find it to be the most valuable information in the entire course. With **Cloud Concepts** we need to be able to define the AWS Cloud in its proposition, we need to be able to identify aspects of AWS Cloud Economics and list the different Cloud Architectural Principles.

For **Security** you will learn a variety of AWS Security Services and shared responsibility models. For **Technology** you will learn all core AWS Services and other AWS Services and Global Infrastructures.

Billing and Pricing is how we know how much things cost and how we can save money on AWS, how to compare and contrast various pricing models for AWS, how to recognize the various account structures in relation to ASW Billing and Pricing and how to Identify Resources for Billing Support. When you do take this exam it has 65 questions and you have both multiple choice and multiple response. For multiple choice you're going to choose one out of four, or multiple response where you choose two or more out of five or more options but generally it's two out of five or three out of six.

I just want to highlight one more thing, which is the white papers. Any time you study for an exam, AWS always has suggestion's to study these white papers first. At the CCP level it's not so important because we definitely cover the content here. When you study for harder exams however, especially the Professionals and Specialties, you have to read the white papers, but again at this level, it's not so important.

Reference: **AWS Certified Cloud Practitioner (CLF-C01) Exam Guide**

Cloud Computing

The "text-book" definition of **Cloud Computing**: **Cloud Computing** is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than on a local server or personal computer. Cloud computing allows companies or individuals to rent the resources they need for their companies or personal projects like storage space.

Companies no longer have to purchase physical hardware with expensive IT departments. This has helped a lot of smaller companies launch their projects or services quickly. Companies can adjust the types of services they need on demand instead of waiting weeks or longer for new servers or other equipment to scale their businesses. Individuals no longer need a computer with a huge hard drive for photos or files. They can now store these on services like Google Drive.

On-premise vs Cloud Providers

On-premise

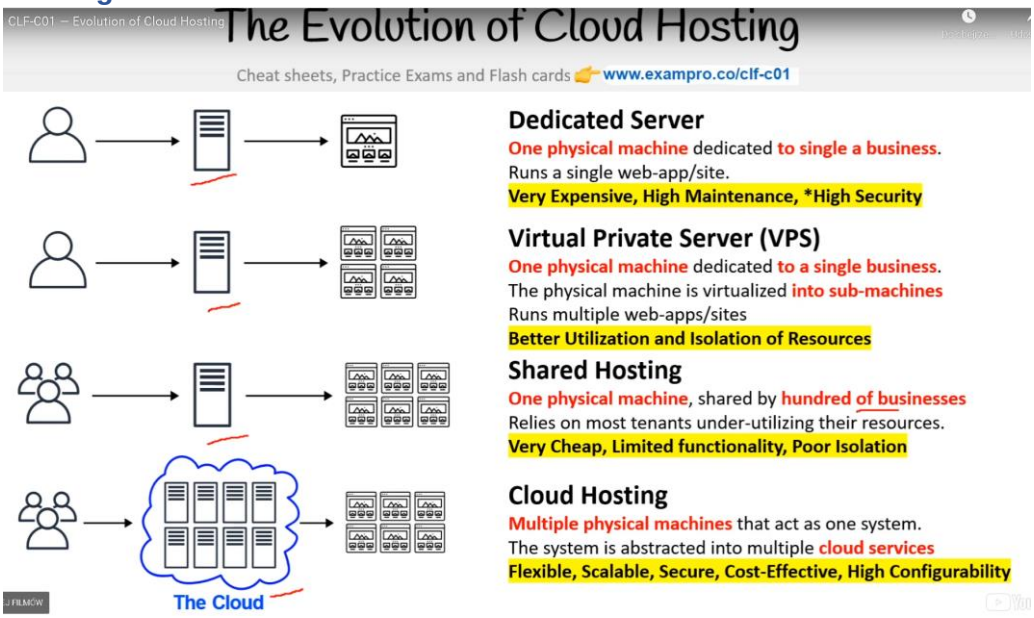
- You own the servers
- You hire the IT people

- You pay or rent the real-estate
- You take all the risk.

Cloud Providers

- Someone else owns the servers
- Someone else hires the IT people
- Someone else pays or rents the real-estate
- You are responsible for configuring your cloud services and code, someone else takes care of the rest

Cloud Hosting



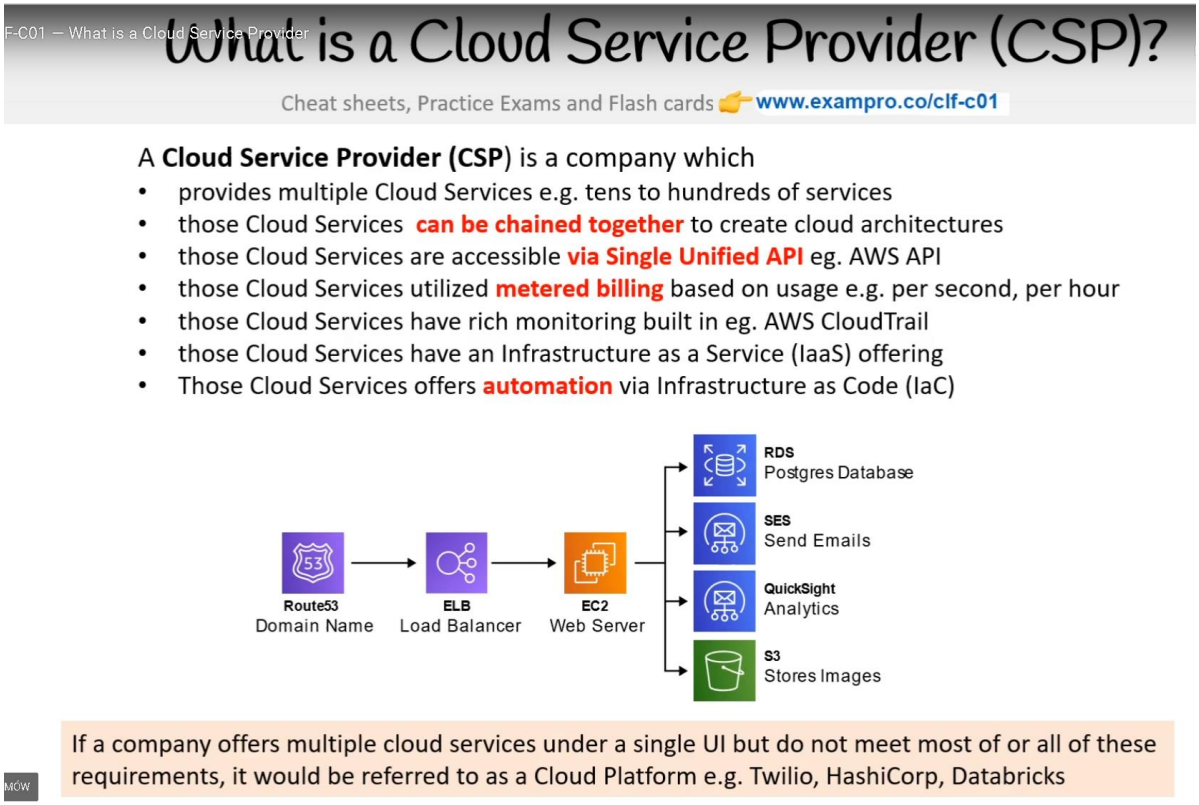
What is Amazon Web Services (AWS)?

Amazon is an American multinational computer technology corporation headquartered in Seattle, Washington. Amazon was founded in 1994 by Jeff Bezos and the company started as an online store for books and expanded to other products. Amazon many products include: - Amazon e-commerce - cloud computing - digital streaming - artificial intelligence.

Amazon calls their cloud provider service **Amazon Web Services** (Commonly referred to just AWS) AWS was launched in 2006 is the leading **Cloud Service Provider** in the world. **Simple Queue Service (SQS)** was the first AWS service launched for public use in 2004

Simple Storage Service (S3) was launched in March of 2006 **Elastic Compute Cloud (EC2)** was launched in August of 2006 **Note:** Cloud Service Providers can be initialized as CSPs.

What is a Cloud Service Provider?



A **Cloud Service Provider** - is a company which provides multiple **Cloud Services**, and those Cloud Services can be chained together to create cloud architectures Most commonly through internet-hosted computing, storage, and software services.

The Big Three Service Providers - There are three main cloud service providers that own the market share. These providers and their market share are:

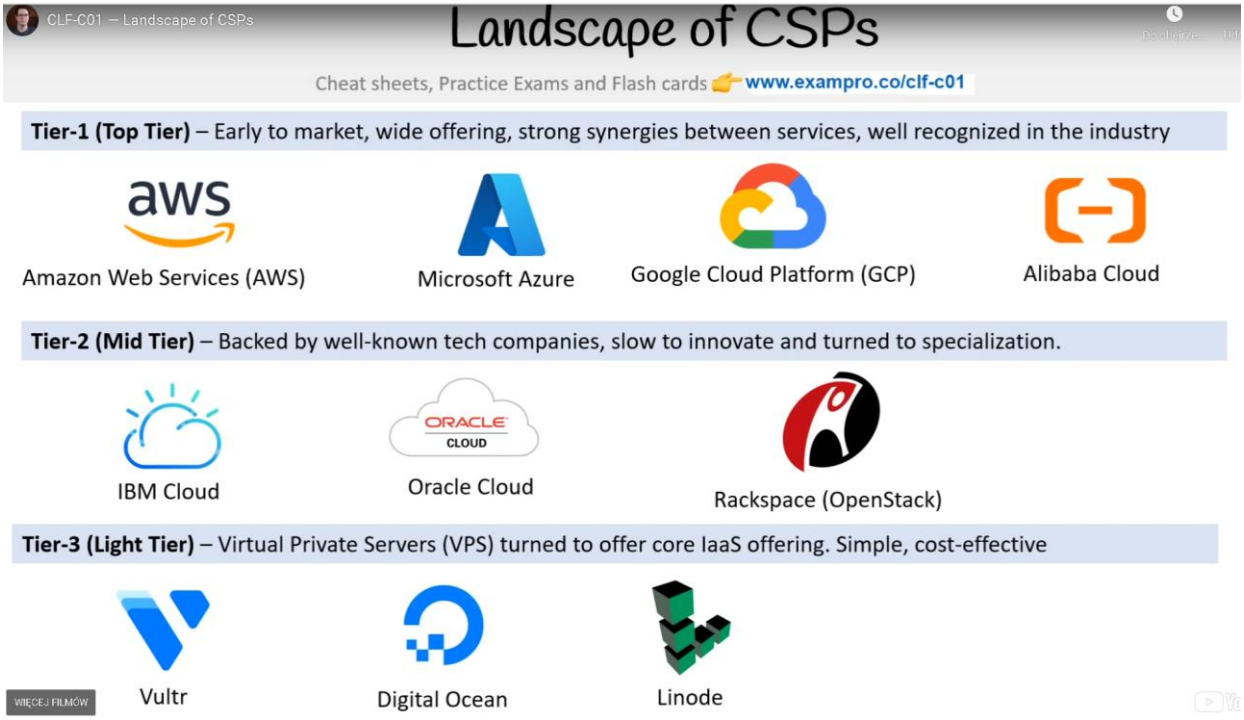
- Amazon Web Services (AWS) - 32.4% ($9.8B)
- Microsoft Azure - 7.6% ($5.3B)
- Google Cloud Platform - 6% ($1.8B)

Common Cloud Services

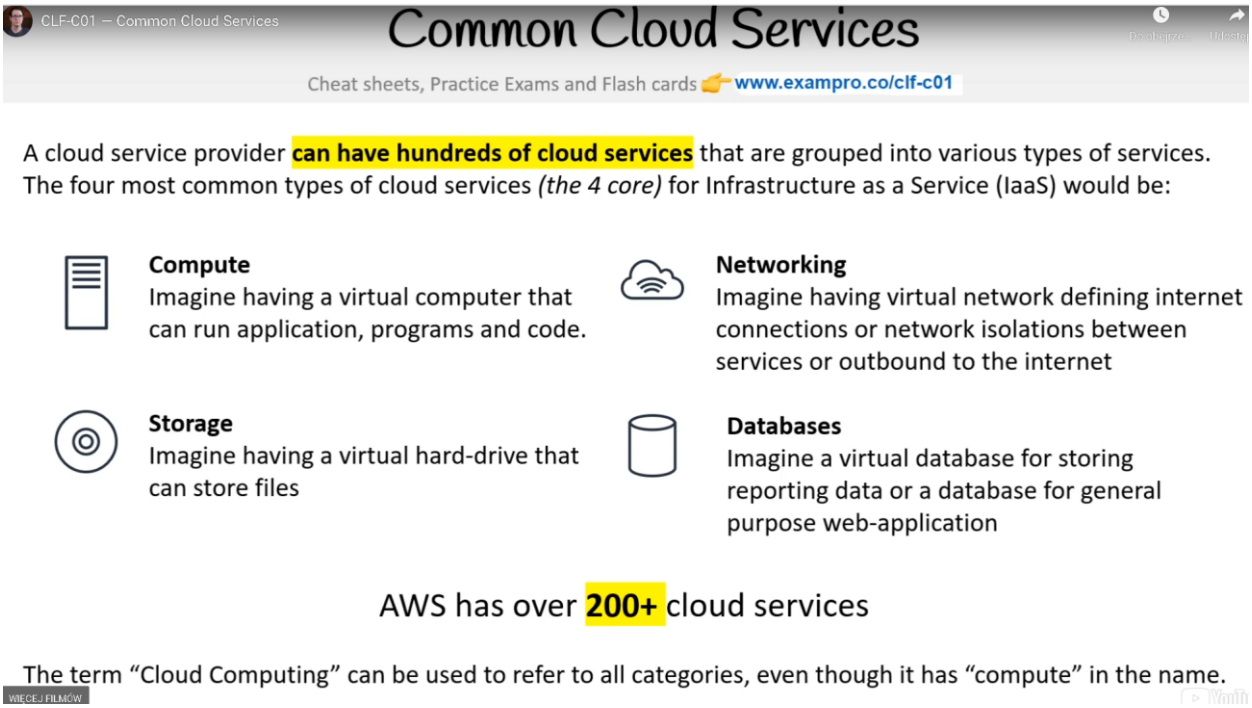
- **Compute** - Imagine having a virtual computer that can run applications, programs, and code.
- **Networking** - Imagine having a virtual network that allows you to define internet connections or network isolations
- **Storage**- Imagine having a virtual hard-drive that can store files
- **Databases** - Imagine a virtual database for storing and reporting data or a database for general-purpose web-application

Note: - 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.

Landscape of CSPs



Common Cloud Services



Technology Overview

Cloud Service Providers (CSPs) that are **Infrastructure as a Service (IaaS)** will always have **4 core cloud service** offerings:

Compute -EC2 Virtual Machines

Storage - EBS Virtual Hard drives

Database - RDS SQL databases

Networking and Content Delivery - VPC Private Cloud Network

The Evolution of Computing

Dedicated

- A physical server **wholly utilized by a single customer**.
- You have to guess your capacity
- You'll overpay for an underutilized server
- You can't vertical scale, you need a manual migration
- Replacing a server is very difficult
- You are limited by your Host Operating System
- Multiple apps can result in conflicts in resource sharing
- You have a **guarantee of security, privacy, and full utility of underlying resources**

VMs

- You can run **multiple Virtual Machines on one machine.**
- **Hypervisor** is the software layer that lets you run the VMs
- A physical server shared by multiple customers
- You are to pay for a fraction of the server
- You'll overpay for an underutilized Virtual Machine
- You are limited by your Guest Operating System
- Multiple apps on a single Virtual Machine can result in conflicts in resource sharing
- Easy to export or import images for migration
- Easy to Vertically or Horizontally scale

Containers

- Virtual Machine running multiple containers
- **Docker Deamon** is the name of the software layer that lets you run multiple containers.
- You can maximize the utilization of the available capacity which is more cost-effective
- Your containers share the same underlying OS so containers are more efficient than multiple VMs
- Multiple apps can run side by side without being limited to the same OS requirements and will not cause conflicts during resource sharing

Functions

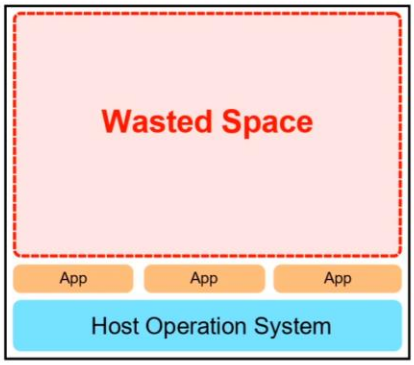
- Functions are managed VMs running managed containers.
- Known as **Serverless Compute**
- You upload a piece of code, choose the amount of memory and duration.
- Only responsible for code and data, nothing else
- Very cost-effective, only pay for the time code is running, VMs only run when there is code to be executed
- Cold Starts is a side-effect of this setup

CLF-C01 — Evolution of Computing

The Evolution of Computing

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

***Dedicated** 👉 VMs 👉 Containers 👉 Functions



physical server

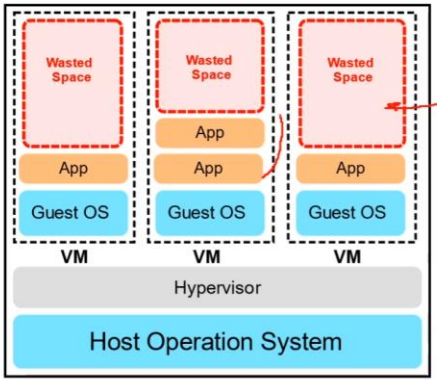
- A physical server **wholly utilized by a single customer**.
- You have to guess your capacity
- you'll overpay for an underutilized server
- You can't vertical scale, you need a manual migration
- Replacing a server is very difficult
- You are limited by your Host Operating System
- Multiple apps can result in conflicts in resource sharing
- You have a ***guarantee of security, privacy, and full utility of underlying resources**

CLF-C01 — Evolution of Computing

The Evolution of Computing

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

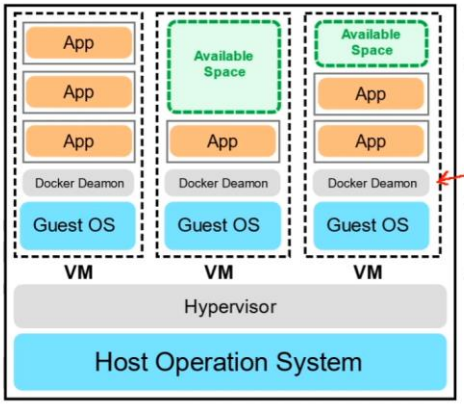
*Dedicated 👉 **VMs** 👉 Containers 👉 Functions



physical server

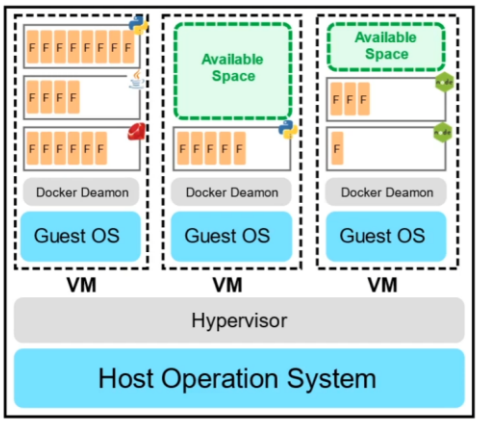
- You can run **multiple Virtual Machines on one machine**.
- **Hypervisor** is the software layer that lets you run the VMs
- A physical server shared by multiple customers
- You are to pay for a fraction of the server
- You'll overpay for an underutilized Virtual Machine
- You are limited by your Guest Operating System
- Multiple apps on a single Virtual Machine can result in conflicts in resource sharing
- Easy to export or import images for migration
- Easy to Vertical or Hortizonaalty scale

*Dedicated 👉 VMs 👉 **Containers** 👉 Functions



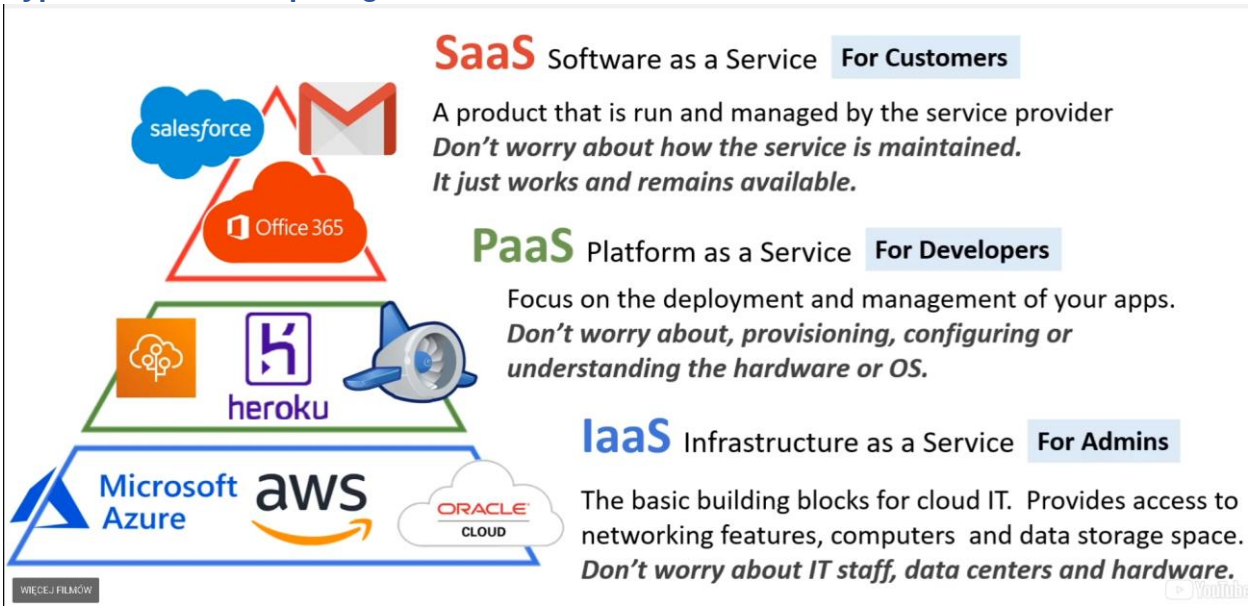
- Virtual Machine running multiple containers
- **Docker Deamon** is the name of the software layer that lets you run multiple containers.
- You can maximize the utilize of the available capacity which is more cost-effective
- Your containers share the same underlying OS so containers are more efficient than multiple VMs
- Multiple apps can run side by side without being limited to the same OS requirements and will not cause conflicts during resource sharing

*Dedicated 👉 VMs 👉 Containers 👉 **Functions**

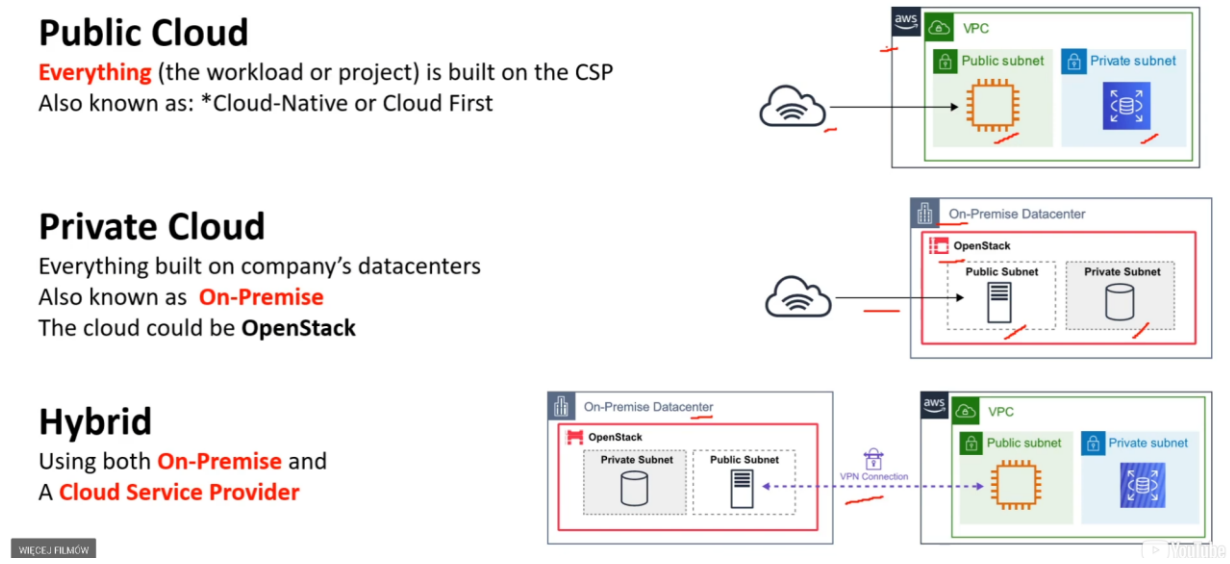


- Are managed VMs running managed containers.
- Known as **Serverless Compute**
- You upload a piece of code, choose the amount of memory and duration.
- Only responsible for code and data, nothing else
- Very cost-effective, only pay for the time code is running, VMs only run when there is code to be executed
- Cold Starts is a side-effect of this setup

Types of Cloud Computing



Cloud Computing Deployment Models



Cloud - When you think of **Cloud**, think of **small startups. -** Cloud Deployment

- 100% of IT infrastructure is on the cloud.
- All of a company's applications were migrated to or created on the cloud.
- Helps to remove roadblocks of costly and time consuming procurement processes for on-premises infrastructure (big servers and data centers!).
- Great for small businesses and start-ups.

Hybrid – When you think of **Hybrid**, think of **Fin Tech Companies -** Hybrid Deployment

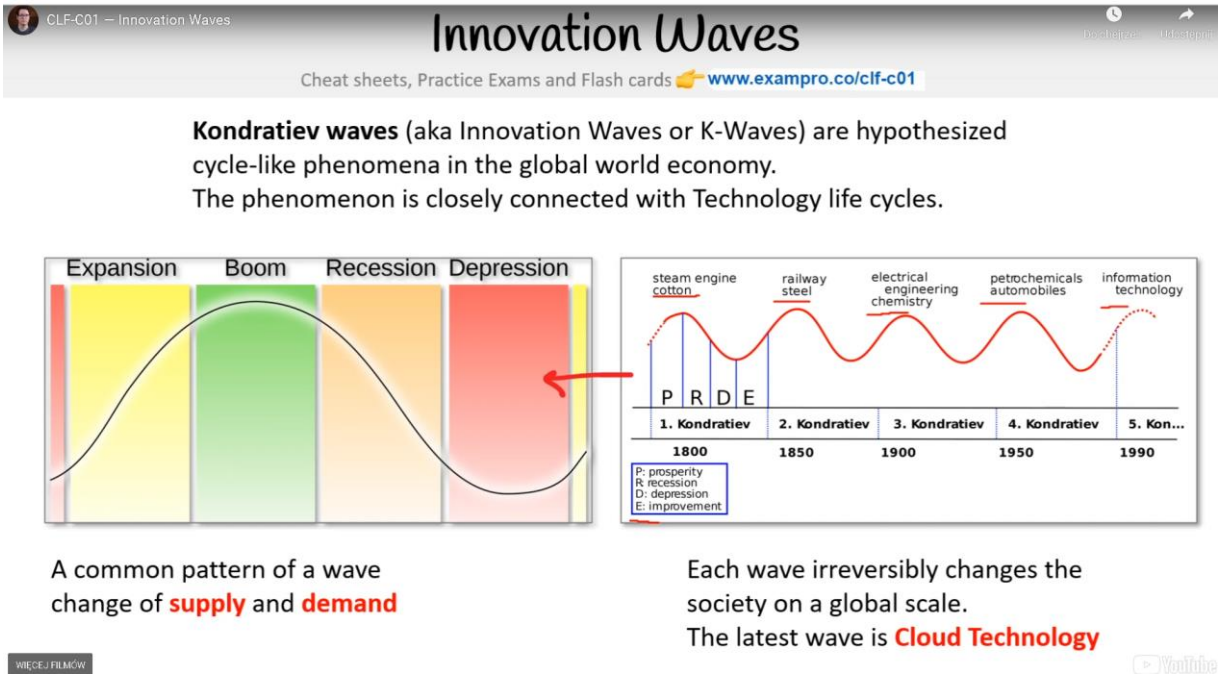
- Connects on-premises technology with cloud-based resources
- Great for established companies that had a dedicated data center but also wants to migrate processes over to the cloud
- Data is partially on the cloud, and partially in the on-premises
- Popular in the Fin Tech space

On-Premise - When you think of **On-premise**, think of **large old companies** or companies that are beholden to **Government Regulations**. - On-premises(Private cloud) Deployment

- Use virtualization to deploy resources in their on-premises data centers.
- Resembles traditional IT infrastructure with big servers, data centers, etc.
- Do not get the same benefits of cloud computing (ability to easily scale up and down on demand)
- Company has dedicated resources that are not shared with others(good for security)
- Resources cannot be accessed using the internet
- Typically older large companies or owned by Government organizations

Reference: What are public, private, and hybrid clouds?

Innovation Waves

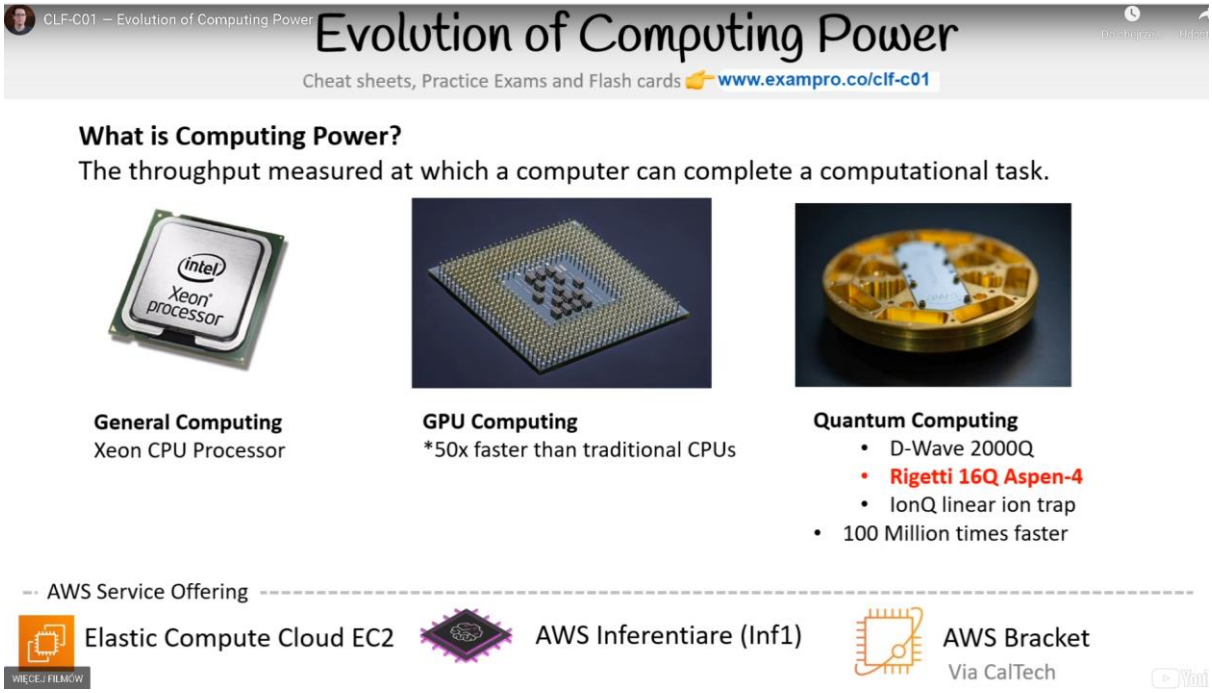


Kondratiev waves - (also known as Innovation Waves) are hypothesized cycle-like phenomena in the global world economy. The phenomenon is closely connected with Technology life cycles. A common pattern of a wave change of **supply** and **demand** Each wave irreversibly changes society on a global scale. The latest wave is **Cloud Technology**

Reference : Kondratiev wave

Burning platform - is a term used **when a company abandons old technology for new technology** with the **uncertainty of success and can be motivated by fear** that the organization future survival hinges on its **digital transformation**

Evolution of Computing Power



What is Computing Power? - The throughput is measured at which a computer can complete a computational task.

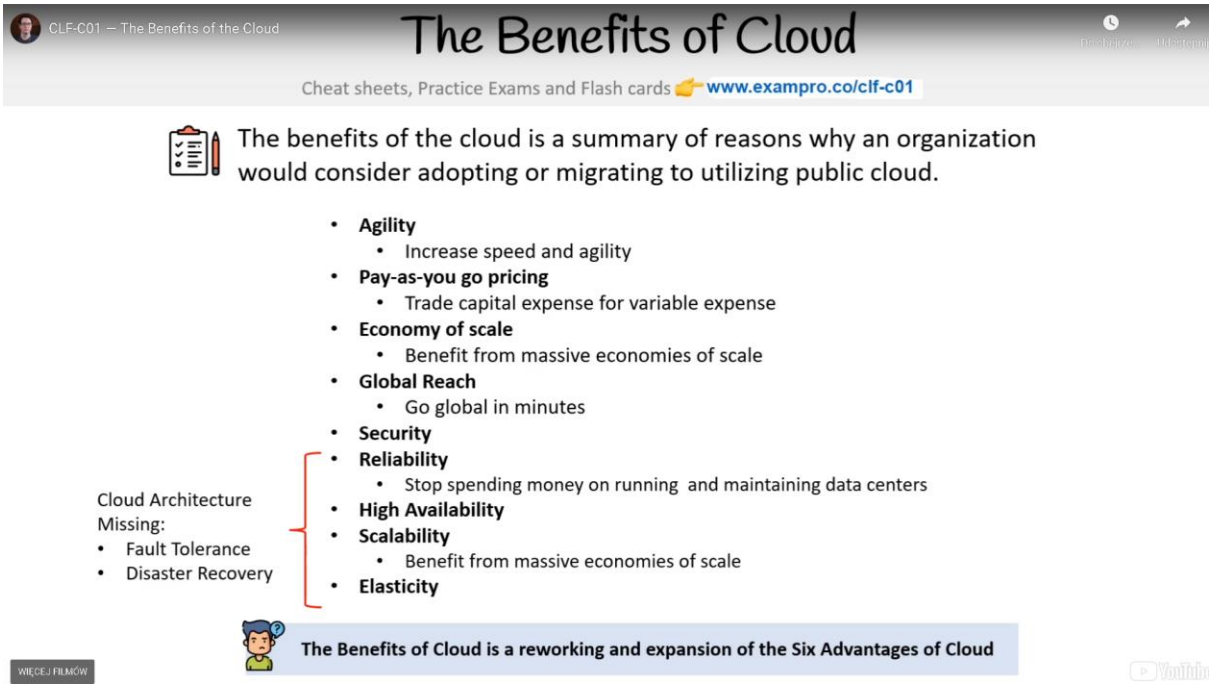
General Computing - Xeon CPU Processor

Tensor Computing -Tensor Processing Unit 3.0 (TPUs) 50x faster than traditional CPUs

Quantum Computing - 100 Million times faster

Google's Cloud Service Offering: Compute Engine Cloud TPU Google Quantum AI

The Benefits of Cloud



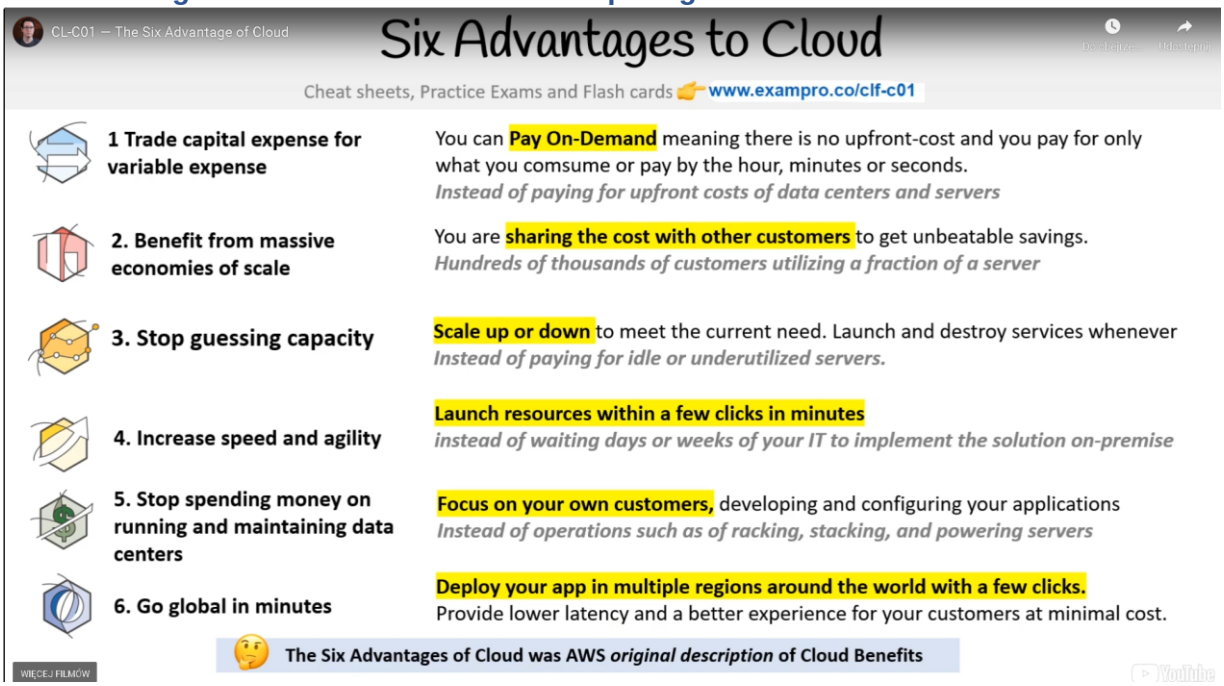
The benefits of the cloud are a summary of reasons why an organization would consider adopting or migrating to utilizing the public cloud.

- **Agility -** Increase speed and agility
- **Pay-as-you-go pricing -** Trade capital expense for variable expense
- **Economy of scale -** Benefit from massive economies of scale
- **Global Reach -** Go global in minutes
- **Security**
- **Reliability -** Stop spending money on running and maintaining data centers
- **High Availability**
- **Scalability -** Stop guessing capacity
- **Elasticity -** Cloud Architecture

Missing: Fault Tolerance, Disaster Recovery

The Benefits of Cloud is reworking and expansion of the Six Advantages of Cloud

Six Advantages and Benefits of Cloud Computing

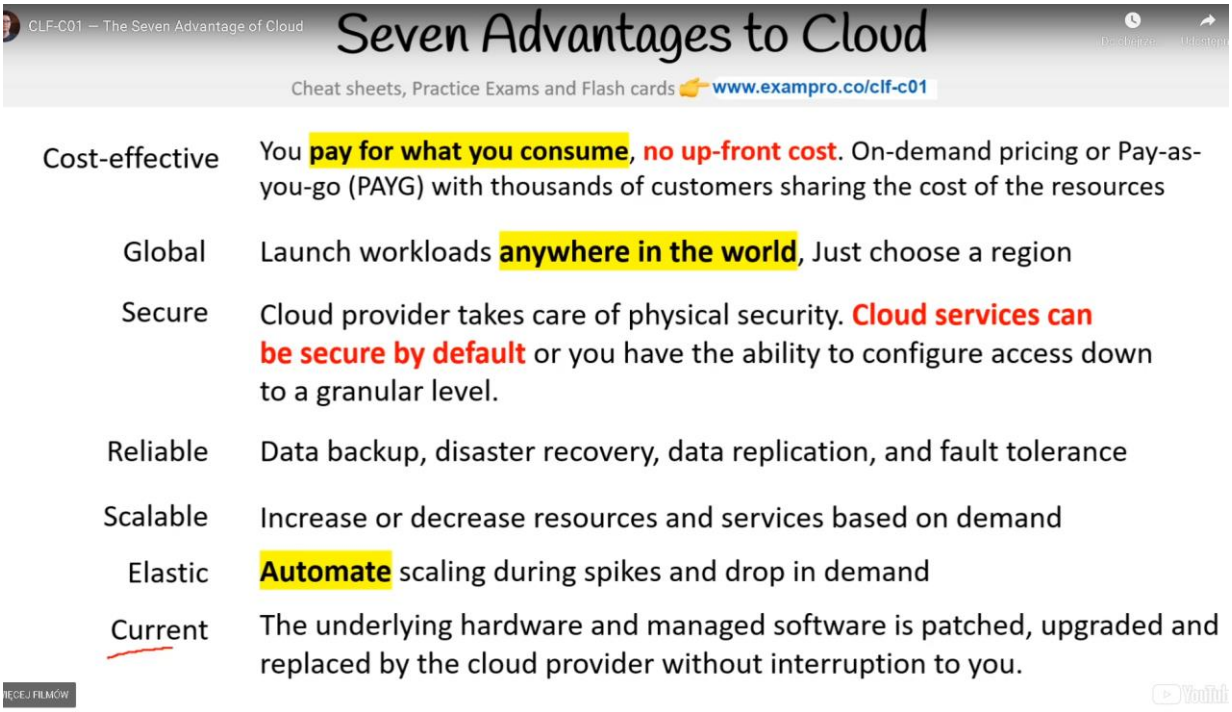


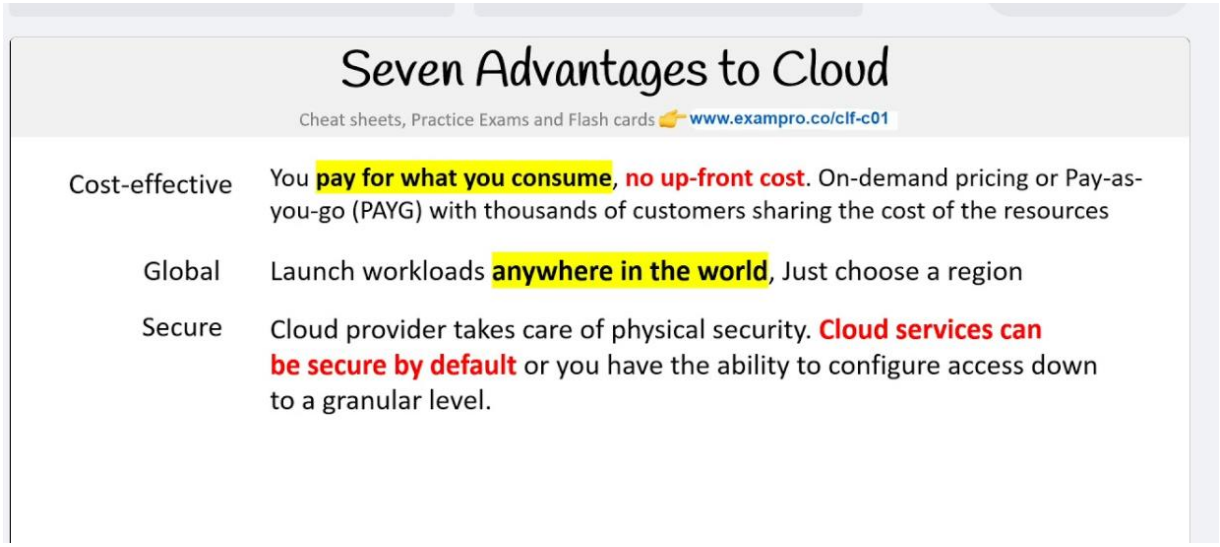
1. Trade capital expense for variable expense
2. Benefit from massive economies
3. Stop guessing capacity
4. Increase speed and agility
5. Stop spending money on running and maintaining data centers
6. Go global in minutes

You can Pay On-Demand meaning there is no upfront cost and you pay for only what you consume or pay by the hour, minutes, or seconds. Instead of paying for upfront costs of data centers and servers You are sharing the cost with other customers to get unbeatable savings. Hundreds of thousands of customers utilize a fraction of a server Scale up or down to meet the current need. Launch and destroy services whenever

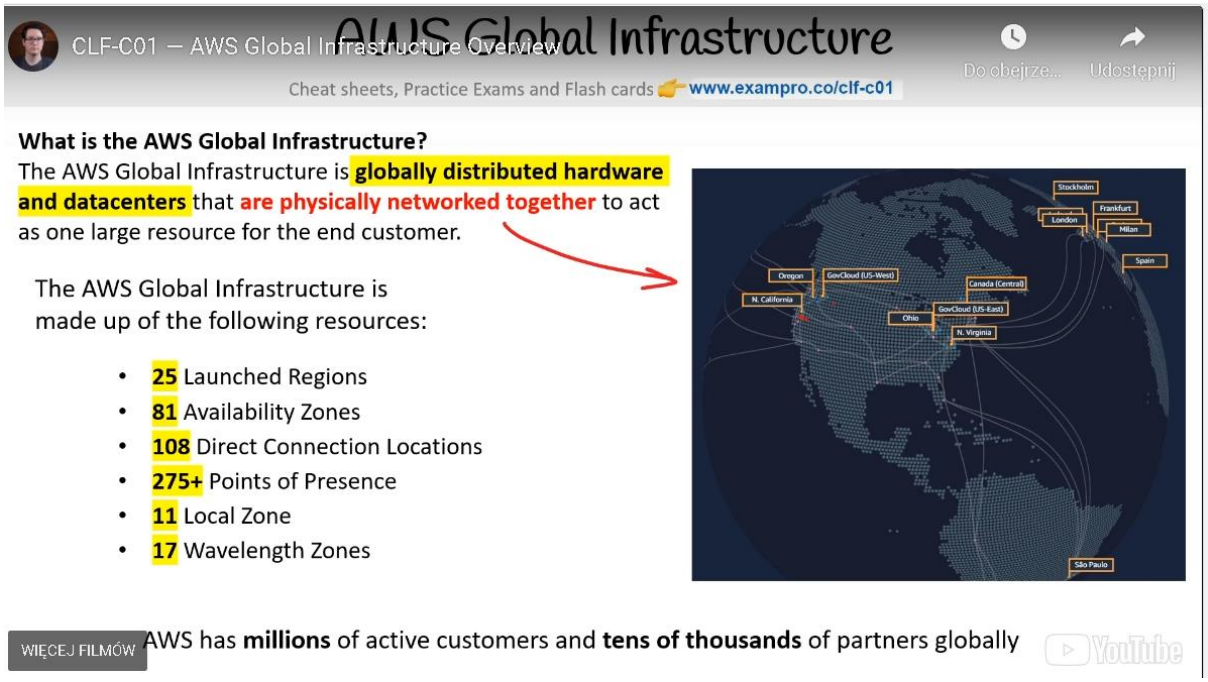
Instead of paying for idle or underutilized servers. Launch resources within a few clicks in minutes instead of waiting days or weeks of your IT to implement the solution on-premise Focus on your own customers, developing and configuring your applications Instead of operations such as racking, stacking, and powering servers Deploy your app in multiple regions around the world with a few clicks. Provide lower latency and a better experience for your customers at a minimal cost.

Benefits of Cloud Computing



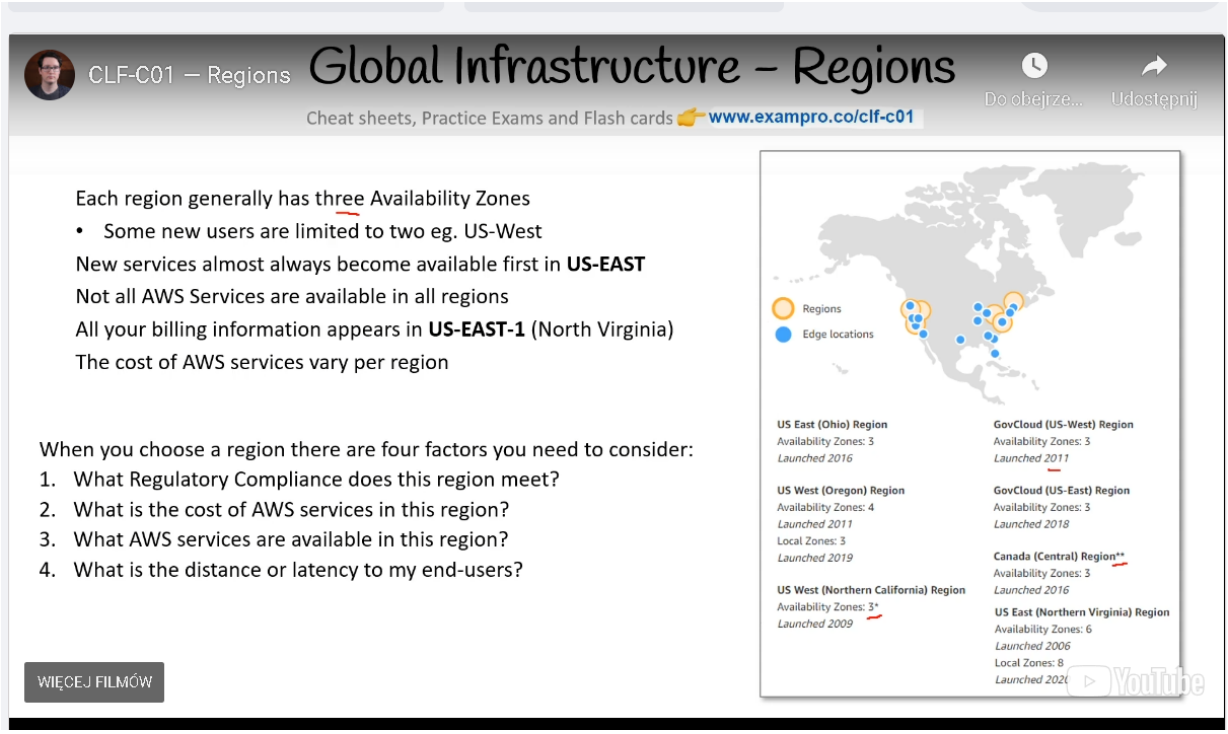


AWS Global Infrastructure



References: https://infrastructure.aws/ | Global Infrastructure

Regions



Region: a Geographically Distinct Location, which has multiple datacentres(AZs).

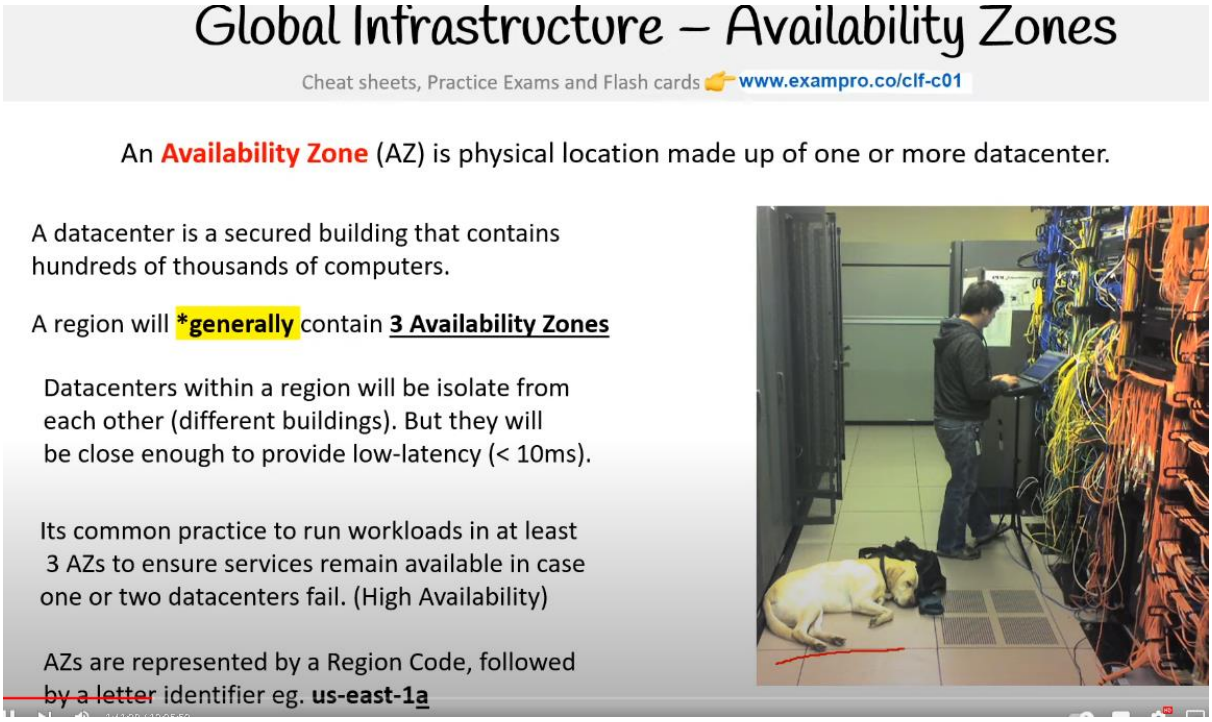
Every region is physically isolated from and independent of every other region in terms of location, power, water supply

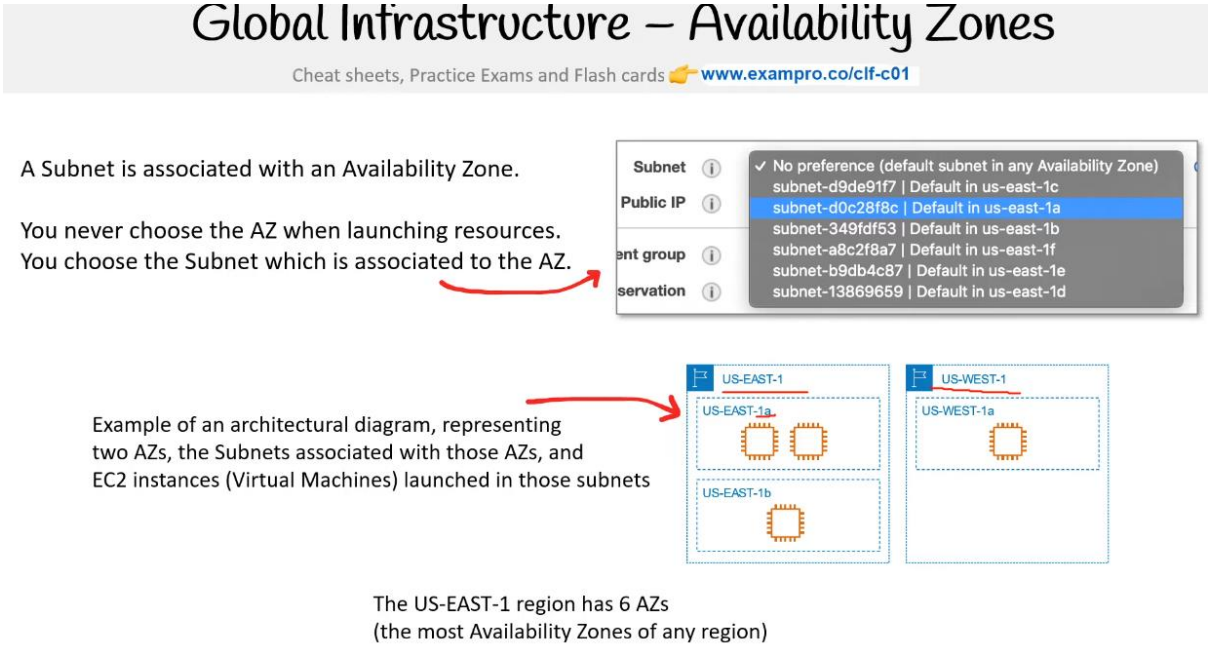
- Each region has at least two Availability Zones (AZs)
- AWS US-EAST-1 (North Virginia) is the largest region
- New services almost always become available first in US-EAST
- Not all AWS Services are available in all regions
- All your billing information appears in US-EAST-1 (North Virginia)
- AWS is always looking to expand their foot-print so new regions could be added in the upcoming years.

You can head over to AWS's Global Infrastructure page to learn more about Regions and see maps of their locations.

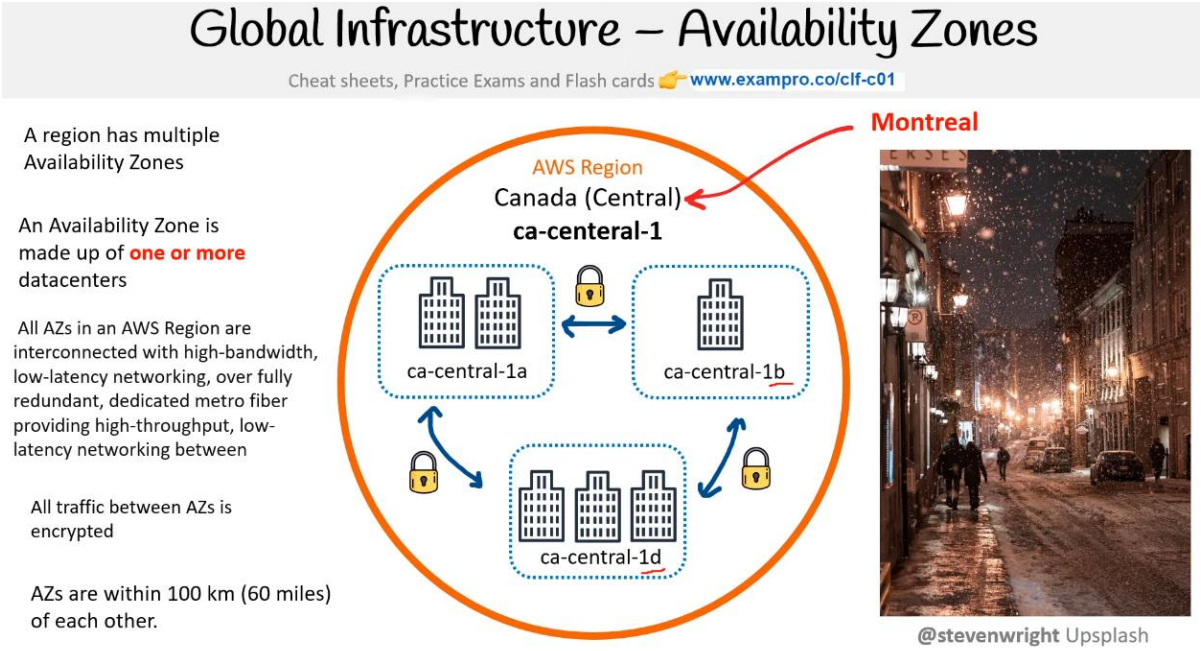
- In the AWS Console you can change AWS Regions. Whatever AWS resources you launch will be in that region.
- Some AWS Services such as CloudFront operate in multiple regions and you'll see the region change to Global

Availability Zones



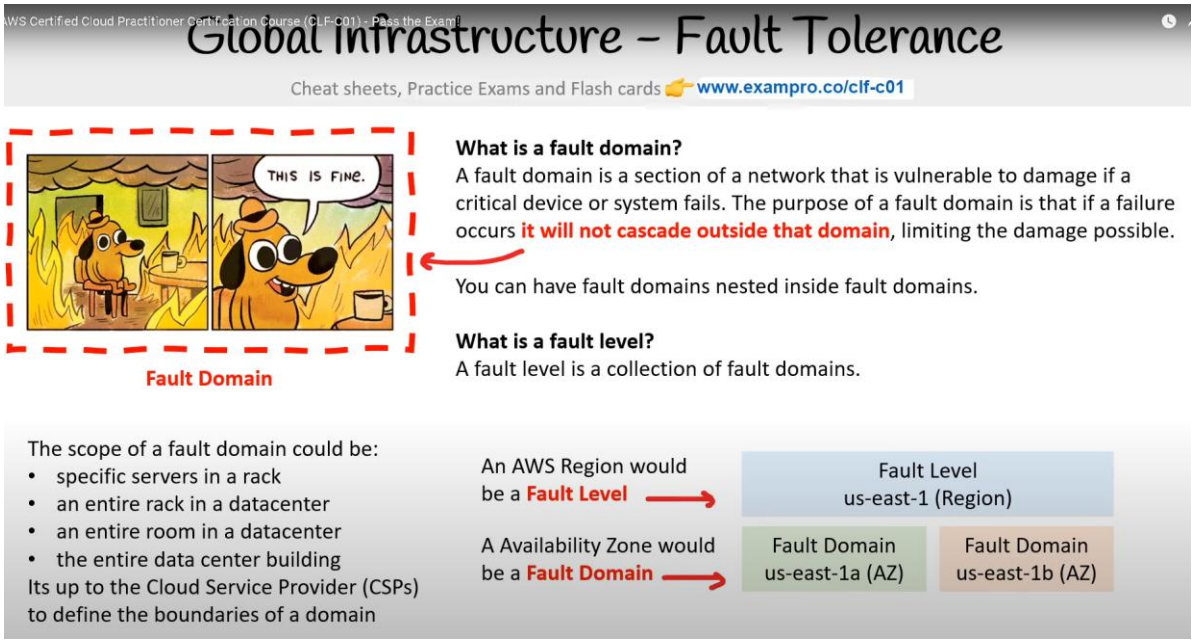


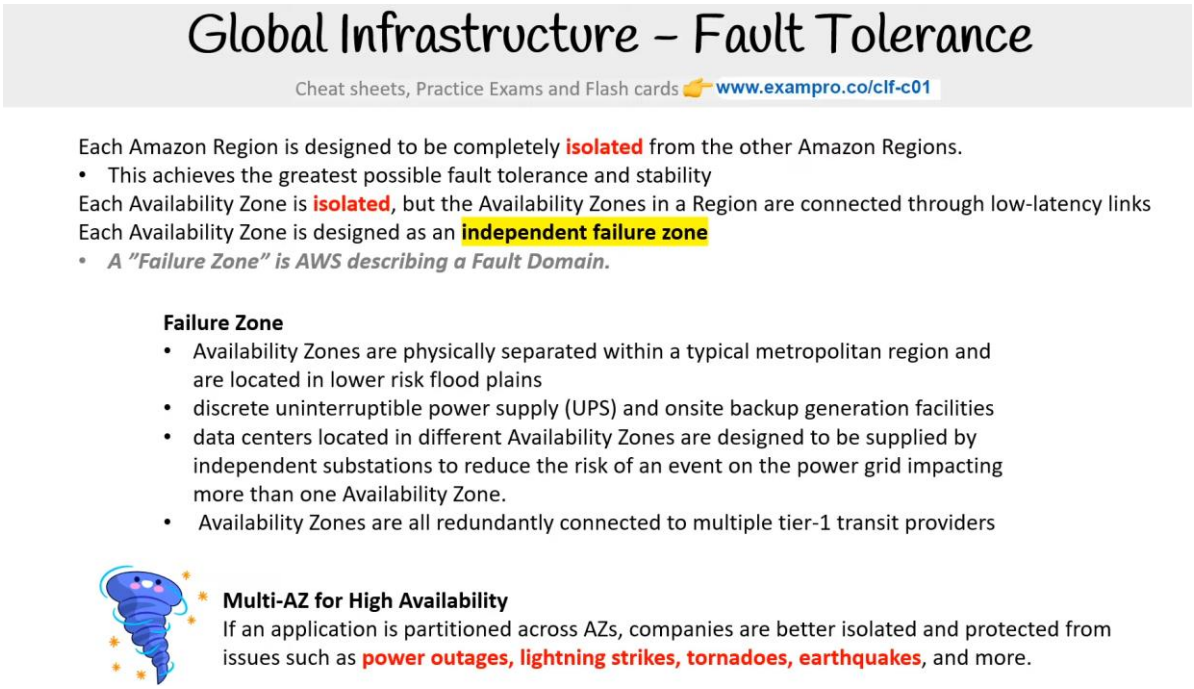
Global Infrastructure – Availability Zones



Reference: [Global Infrastructure]

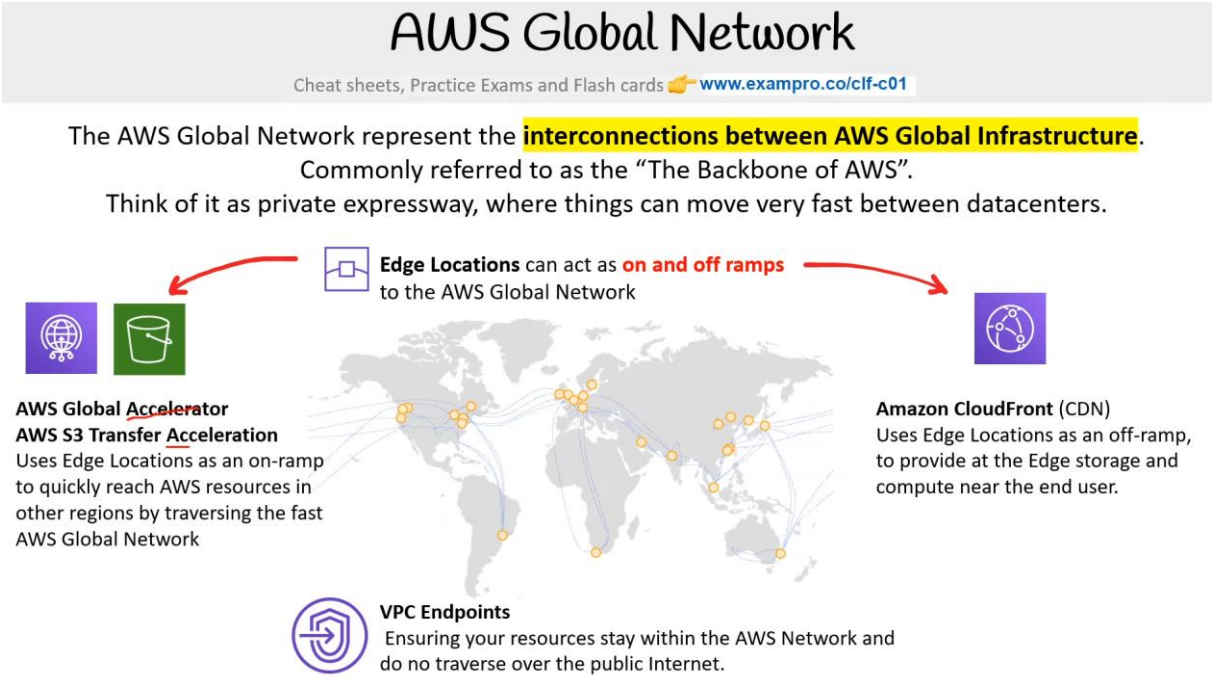
Global Infrastructure - Fault Tolerance





Reference - Global Infrastructure | Describing fault domains. | Fault Domain Awareness | Fault Domains and the Vegas Rule

AWS Global Network



The AWS Global Network represents the interconnections between AWS Global Infrastructure. Commonly referred to as the "The Backbone of AWS". Think of it as a private expressway, where things can move very fast between datacenters.

Edge Locations - can act as on and off-ramps to the AWS Global Network

AWS Global Accelerator

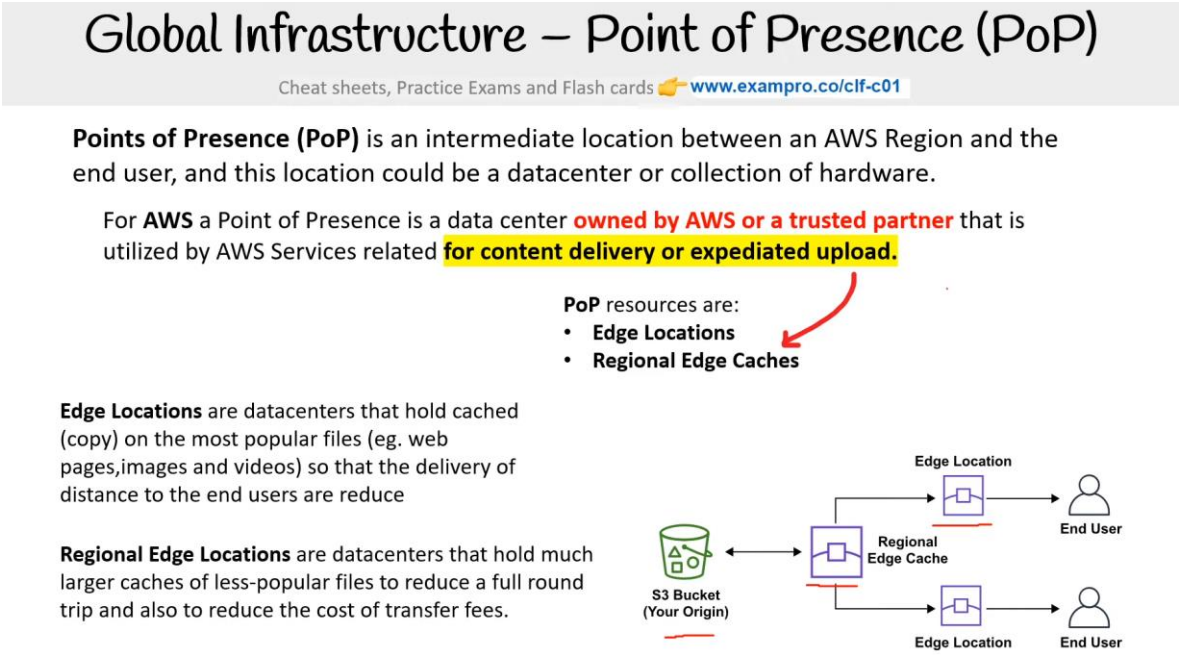
AWS S3 Transfer Acceleration - Uses Edge Locations as an on-ramp to quickly reach AWS resources in other regions by traversing the fast AWS Global Network

Amazon CloudFront (CDN) - Uses Edge Locations as an off-ramp, to provide at the Edge storage and compute near the end-user.

VPC Endpoints - Ensuring your resources stay within the AWS Network and do not traverse over the public Internet.

Reference - Global Network

Points of Presence



Points of Presence (PoP) are intermediate locations 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.

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 Cache - 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.

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

AWS CloudFront - is a Content Delivery Network (CDN) service that:

- You point your website to CloudFront so that it will route requests to the nearest Edge Location cache
- Allows you to choose an origin (such as a web-server or storage) that will be a source of cached
- Caches the contents of what origin would be returned to various Edge Locations around the world

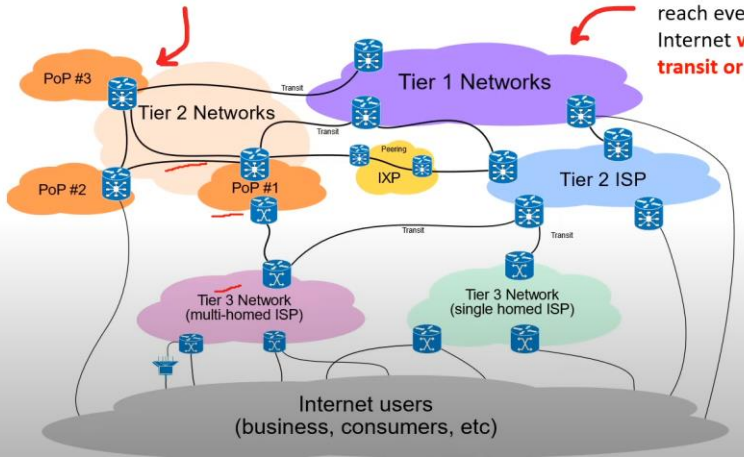
AWS S3 Transfer Acceleration - allows you to generate a special URL that can be used by end users to upload files to a nearby Edge Location. Once a file is uploaded to an Edge Location, it can move much faster within the AWS Network to reach S3.

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

Global Infrastructure – Point of Presence (PoP)

PoPs live at the edge/**intersection** of two networks

Tier 1 network is a network that can reach every other network on the Internet **without purchasing IP transit or paying for peering**.



AWS Availability Zones are all redundantly connected to multiple **tier-1 transit providers**

Global Infrastructure – Point of Presence (PoP)

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

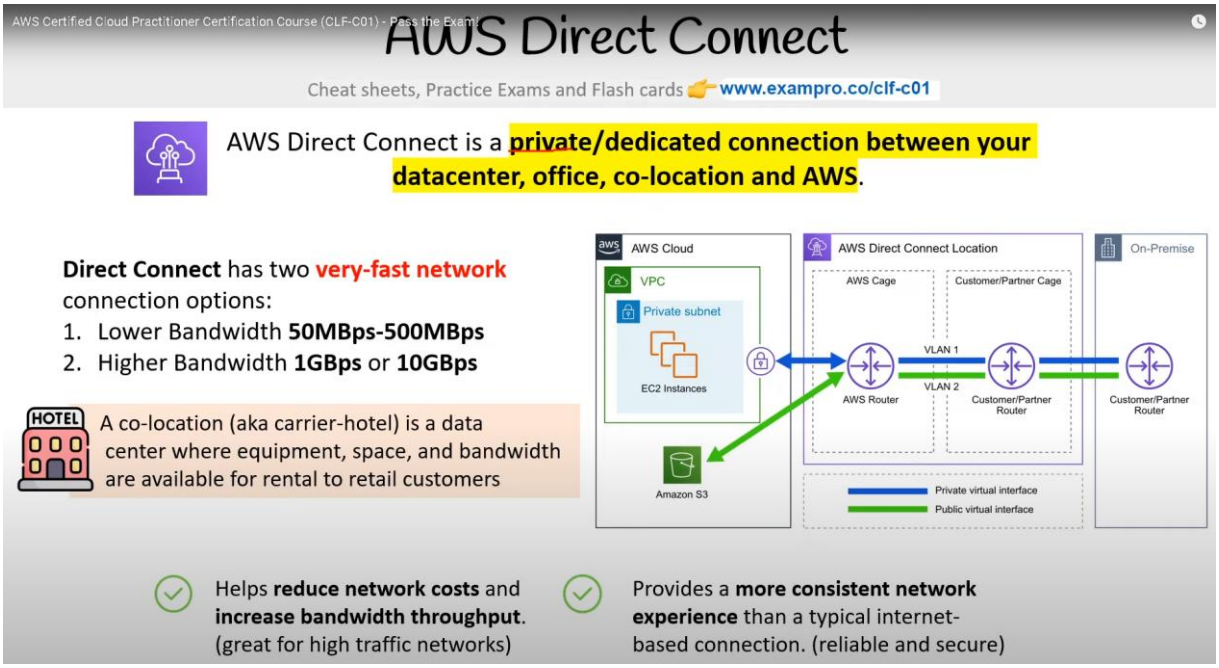
Amazon CloudFront is a **Content Delivery Network (CDN) service** that:

- 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.

AWS Direct Connect



AWS Direct Connect is a **private/dedicated connection between your data center, office, co-location, and AWS. Direct Connect** has two **very-fast network** connection options:

- Lower Bandwidth 50MBps-500MBps
- Higher Bandwidth 1GBps or 10GBps

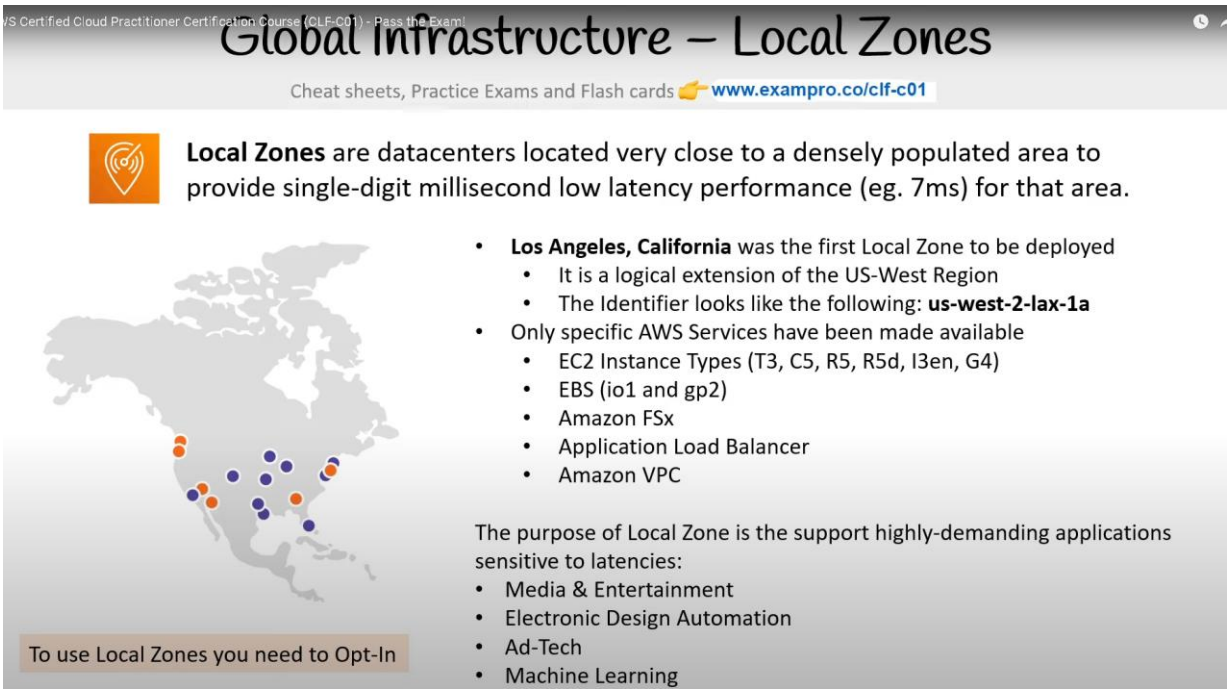
A co-location (aka carrier-hotel) is a data center where equipment, space, and bandwidth are available for rental to retail customers. Helps **reduce network costs and increase bandwidth throughput**. (great for high traffic networks). Provides a **more consistent network experience** than a typical internet-based connection. (reliable and secure)

Reference - AWS Direct Connect

Direct Connect Locations - are trusted third-party datacenters that you can establish a dedicated high speed, low-latency connection from your on-premise to the AWS network.

- DirectConnect connections are always established through a third-party provider. These APN (Amazon Partner Network) Partners can help you establish network circuits between an AWS Direct Connect location and your datacenter, office, or colocation environment, or assist you in constructing a hybrid environment.

Local Zones - are datacenters located very close to a density populated area to provide *single-digit millisecond low latency performance* (eg. 7ms) for that area.



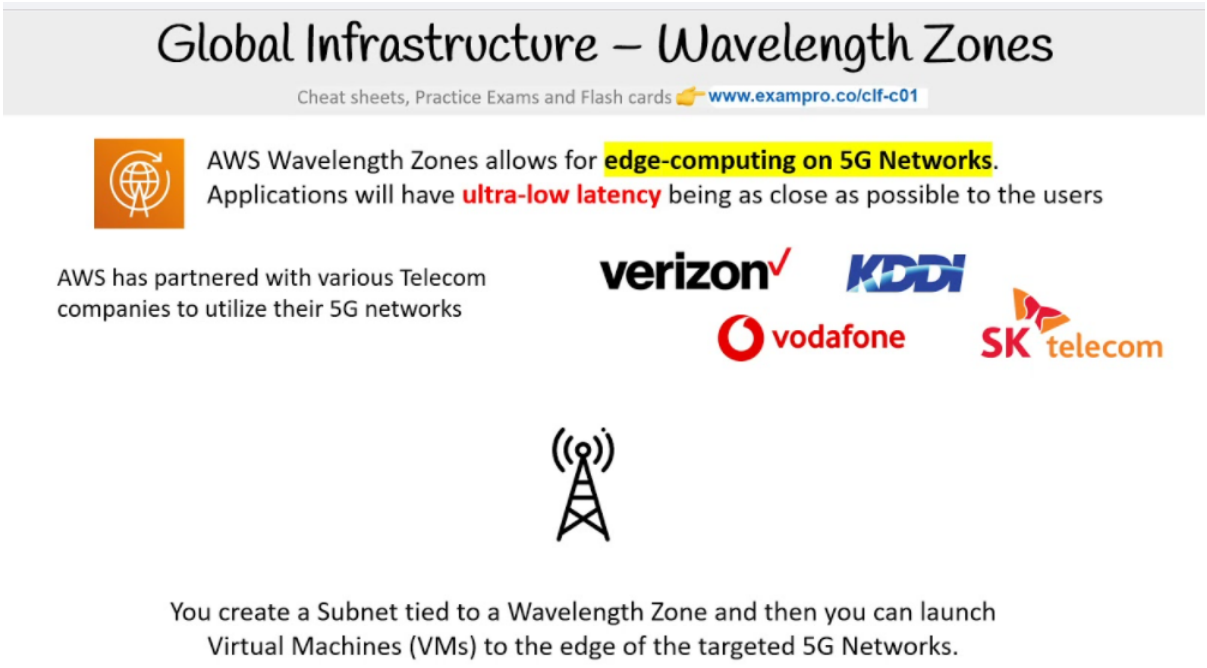
Los Angeles, California was the first Local Zone to be deployed

- It is a logical extension of the US-West Region
- The Identifier looks like the following: us-west-2-lax-1a
- Only specific AWS Services have been made available
    - EC2 Instance Types (T3, C5, R5, R5d, I3en, G4)
    - EBS (io1 and gp2)
    - Amazon FSx
    - Application Load Balancer
    - Amazon VPC

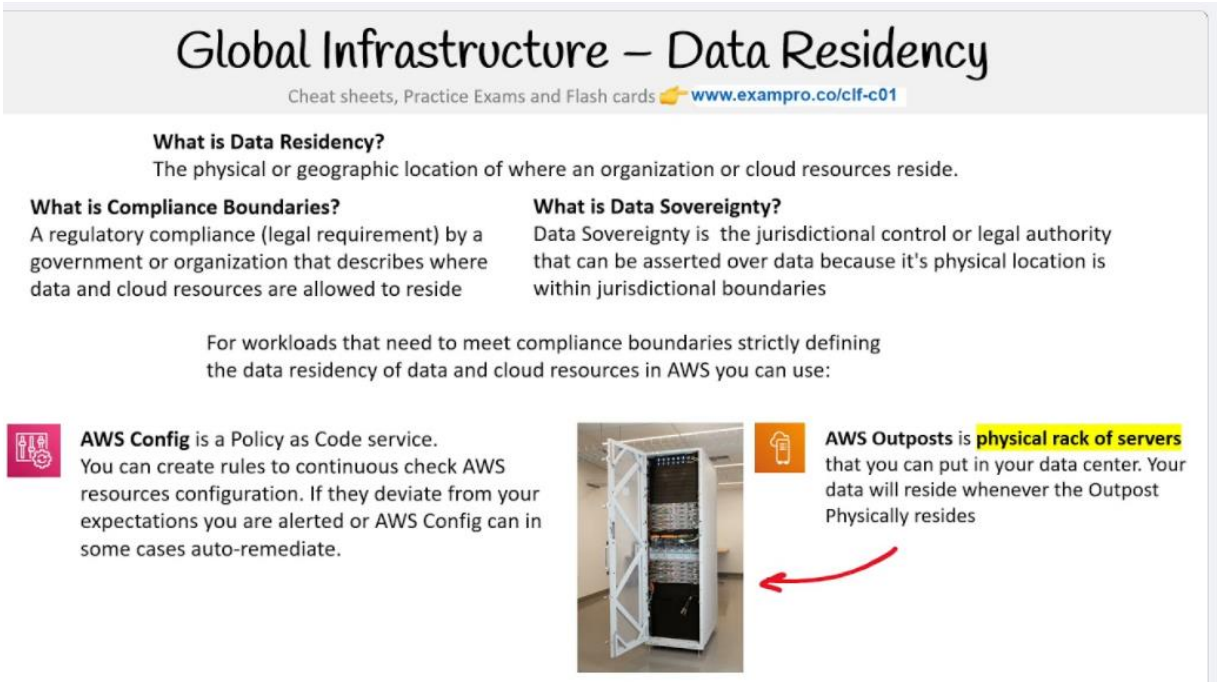
The purpose of Local Zone is to support highly-demanding applications sensitive to latency:

- Media & Entertainment
- Electronic Design Automation
- Ad-Tech
- Machine Learning

Global Infrastructure - Wavelength Zones



Global Infrastructure – Data Residency



Reference: [Addressing Data Residency with AWS]

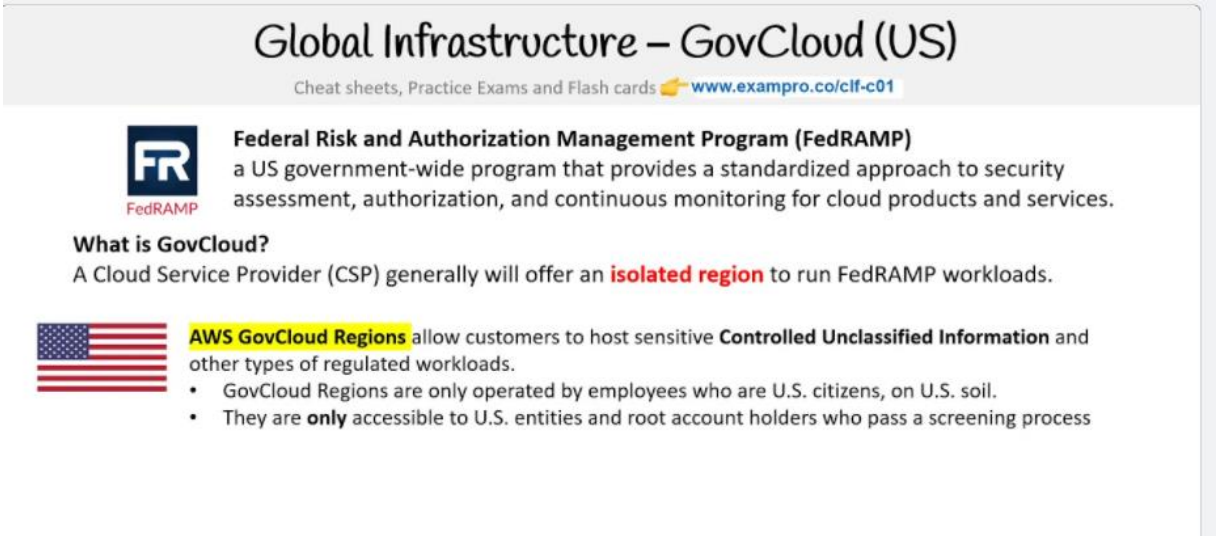
Global Infrastructure - AWS for Government

What is Public Sector? - Public sectors include public goods and governmental services such as:

- Military | law enforcement | infrastructure | public transit | public education | health care | the government itself

AWS can be utilized by the public sector or organizations developing cloud workloads for public sector. AWS achieve this by meeting **regulatory compliance programs** along with specific governance and security controls. AWS has special regions for US regulation called **GovCloud**

GovCloud



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

- GovCloud Regions are only operate by employees who are U.S. citizens on U.S. soil.
- Only accessible to U.S. entities and account state holders who pass a screening process.
- Customers can architect secure cloud solutions that comply with:
    - Fed**RAMP** High baseline
    - DOJ's Criminal Justice Information Systems (CJIS) Security Policy
    - U.S. International Traffic in Arms Regulations (TAR)
    - Export Administration Regulations (EAR)
    - Department of Defense (DoD) Cloud Computing Security Requirements Guide

GovCloud Regions are currently only in the US.

- You can view their regions on AWS Map of Regions and Edge Networks.
- You can view more about GovCloud on the official AWS GovCloud page.

Global Infrastructure – AWS in China

Global Infrastructure – AWS in China

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

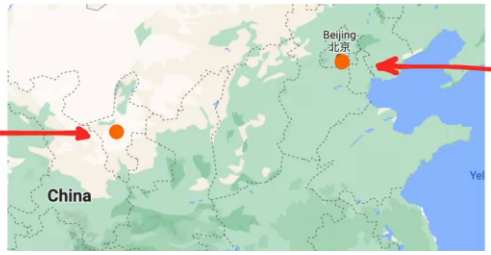
AWS China is the AWS cloud offerings in Mainland China.

AWS China is completely isolate *intentionally* from AWS Global to meet regulatory compliance for Mainland China.
AWS China is on its own domain at: **amazonaws.cn**

In order to operate in a AWS China Region you need have a Chinese Business License (ICP license)
Not all services are available in china eg. Route53
Running in Mainland China (instead of Singapore) means you would not need to traverse the The Great Firewall.

AWS has two Regions in Mainland China:

Ningxia CN-NorthWest-1
Operated by NSWCF



Beijing CN-North-1
operated by SINNET

Reference | [My experience with AWS China | AWS China]

Global Infrastructure – Sustainability

Global Infrastructure – Sustainability

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

Amazon co-founded the Climate Pledge to achieve Net-Zero Carbon Emissions by 2040 across all of Amazon's business (this includes AWS)
sustainability.aboutamazon.com

AWS Cloud's Sustainability goals are composed of three parts:

1. Renewable Energy
AWS is working towards having their AWS Global Infrastructure powered by 100% renewable energy by 2025.

2. Cloud Efficiency
AWS's infrastructure is 3.6 times more energy efficient than the median of U.S. enterprise data centers surveyed.

3. Water Stewardship
Direct evaporative technology to cool our data center
Use of non-potable water for cooling purposes (recycled water)
On-site water treatment allows us to remove scale-forming minerals and reuse water for more cycles
Water efficiency metrics to determine and monitor optimal water use for each AWS Region

AWS purchases and retires environmental attributes to cover the non-renewable energy for AWS Global Infrastructure:

- Renewable Energy Credits (RECs)
- Guarantees of Origin (GOs)

Global Infrastructure – AWS Ground Station

Global Infrastructure – AWS Ground Station

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

AWS Ground Station is a fully managed service that **lets you control satellite communications,** process data, and scale your operations without having to worry about building or managing your own ground station infrastructure

Use cases for Ground Station:
- weather forecasting
- surface imaging
- communications
- video broadcasts

To use Ground Station:
- You schedule a Contact (select satellite, start and end time, and the ground location
- use the AWS Ground Station EC2 AMI to launch EC2 instances that will uplink and downlink data during the contact or receive downlinked data in an Amazon S3 bucket.

Use Case:
A company reaches an agreement with a Satellite Imagery Provider to take satellite photos of a specific region. They use AWS Ground Station to communicate that company's Satellite and download the S3 image data.

@isidurumm on Unsplash

Reference AWS Ground Station

Global Infrastructure – 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.

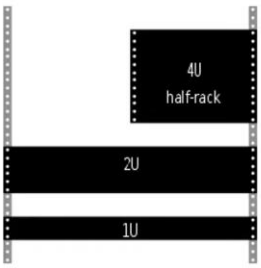
AWS Outposts is rack of servers running AWS Infrastructure on your physical location

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 inch
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

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

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 a rack of servers running AWS Infrastructure on your physical location

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

Reference - AWS Outposts

Cloud Architecture Terminologies

What is a Solutions Architect? - A role in a technical organization that architects a technical solution using multiple systems via researching, documentation, experimentation.

What is a Cloud Architect? -A solutions architect that is focused solely on architecting technical solutions using cloud services. A cloud architect needs to understand the following terms and factor them into their design architecture based on the business requirements.

- **Availability** - Your ability to ensure service remains available e.g. **Highly Available (HA)**
- **Scalability** - Your ability to grow rapidly or unimpeded
- **Elasticity** - Your ability to shrink and grow to meet the demand
- **Fault Tolerance** - Your ability to prevent a failure
- **Disaster Recovery** - Your ability to recover from a failure e.g. **High Durable (DR)**

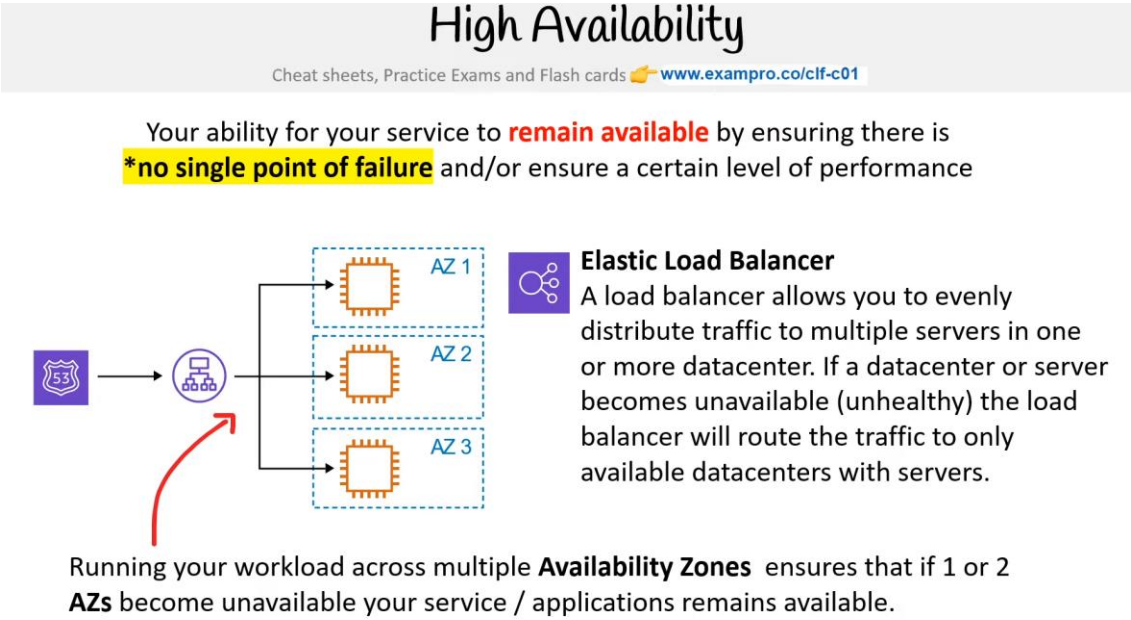
A Solutions Architect needs to always consider the following business factors:

- (Security) How secure is this solution?

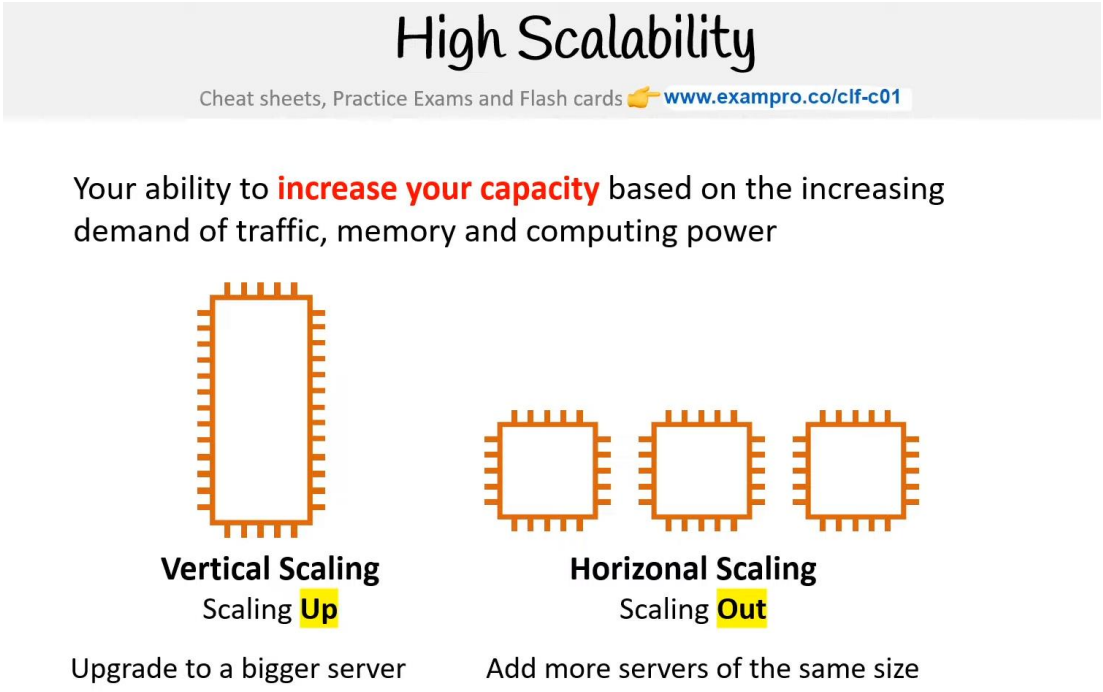
- (Cost) How much is this going to cost?

High Availability

What is High Availability (HA)?



High Scalability



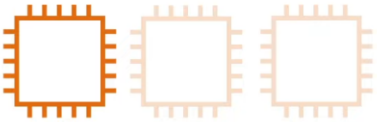
What is High Scalability? - Your ability to increase your capacity based on the increasing demand of traffic, memory and computing power

How is High Scalability defined?

- Vertical Scaling is known as **Scaling Up** (When Upgrade to a bigger server)
- Horizontal Scaling is known as **Scaling Out** (When Add more servers of the same size)

High Elasticity

Your ability to **automatically** increase or decrease your capacity based on the current demand of traffic, memory and computing power



Auto Scaling Groups (ASG) is an AWS feature that will automatically add or remove servers based on scaling rules you define based on metrics

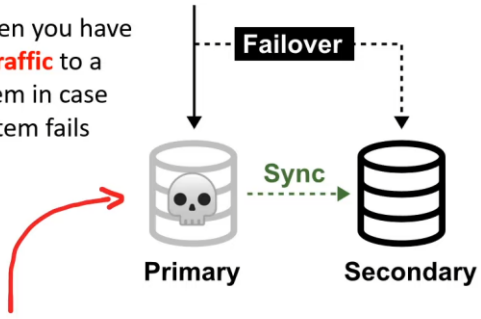
Horizonal Scaling
Scaling **Out** — Add more servers of the same size
Scaling **In** — Removing underutilized servers of the same size

Vertical Scaling is generally hard for traditional architecture so you'll usually only see horizontal scaling described with Elasticity.

Fault Tolerance

Your ability for your service to ensure there is no **no single point of failure. Preventing the chance of failure**

Fail-overs is when you have a plan to **shift traffic** to a redundant system in case the primary system fails



A common example is having a copy (secondary) of your database where all ongoing changes are synced. The secondary system is not in-use until a fail over occurs and it becomes the primary database.

What is Highly Fault Tolerant? - The ability for your service to ensure there is no single point of failure. Preventing the chance of failure

What is a Fail-over? - Fail-overs are when you have a plan to shift traffic to a redundant system in case the primary system fails

How can Fault Tolerance be achieved? A common example is having a copy (secondary) of your database where all ongoing changes are synced. The Secondary is not in-use until a failover occurs and it becomes the primary database.

How can Fault Tolerance be implemented using AWS? - **RDS Multi-AZ** - is when you run a duplicate standby database in another Availability Zone in case your primary database fails.

High Durability

Your ability to **recover** from a disaster and to prevent **the loss** of data
Solutions that recover from a disaster is known as **Disaster Recovery (DR)**

- Do you have a backup?
- How fast can you restore that backup?
- Does your backup still work?
- How do you ensure current live data is not corrupt?

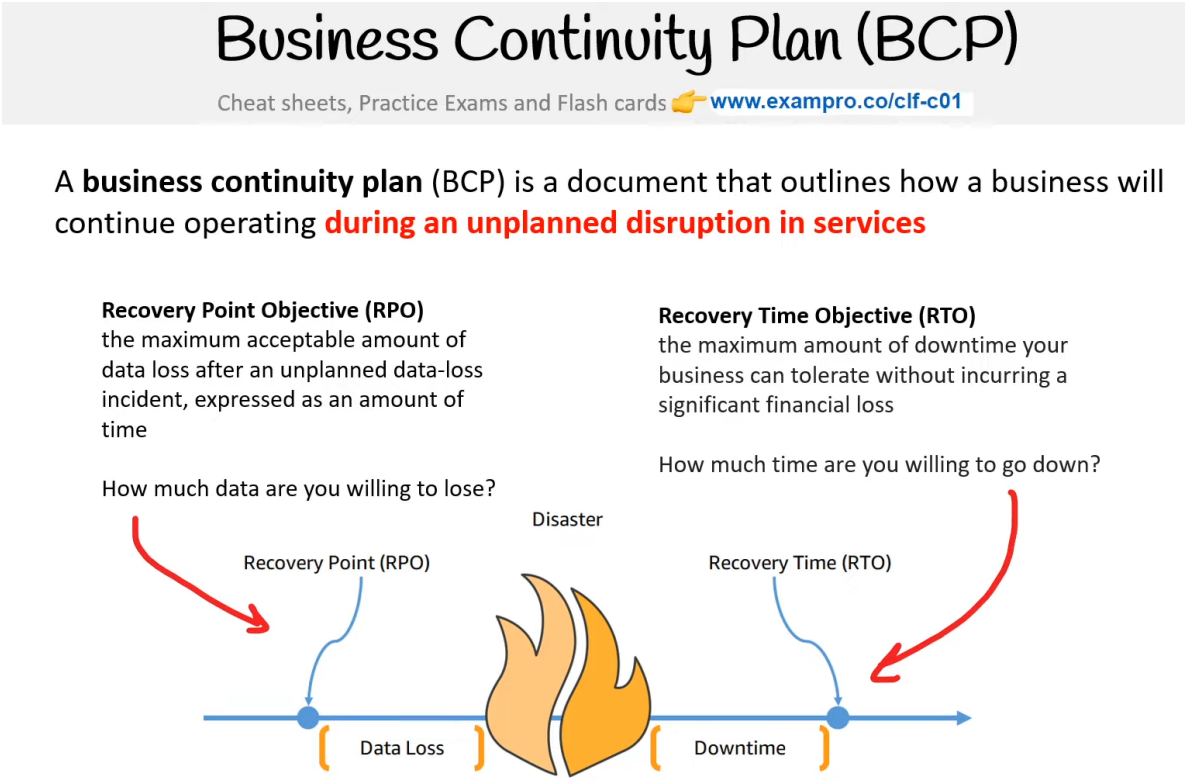
CloudEndure Disaster Recovery continuously replicates your machines into a low-cost staging area in your target AWS account and preferred Region enabling fast and reliable recovery in case of IT data center failures.

Your ability to recover from a disaster and to prevent the loss of data solutions that recover from a disaster is known as **Disaster Recovery** (DR). **Questions you should be asking about your Disaster Recovery procedures:**

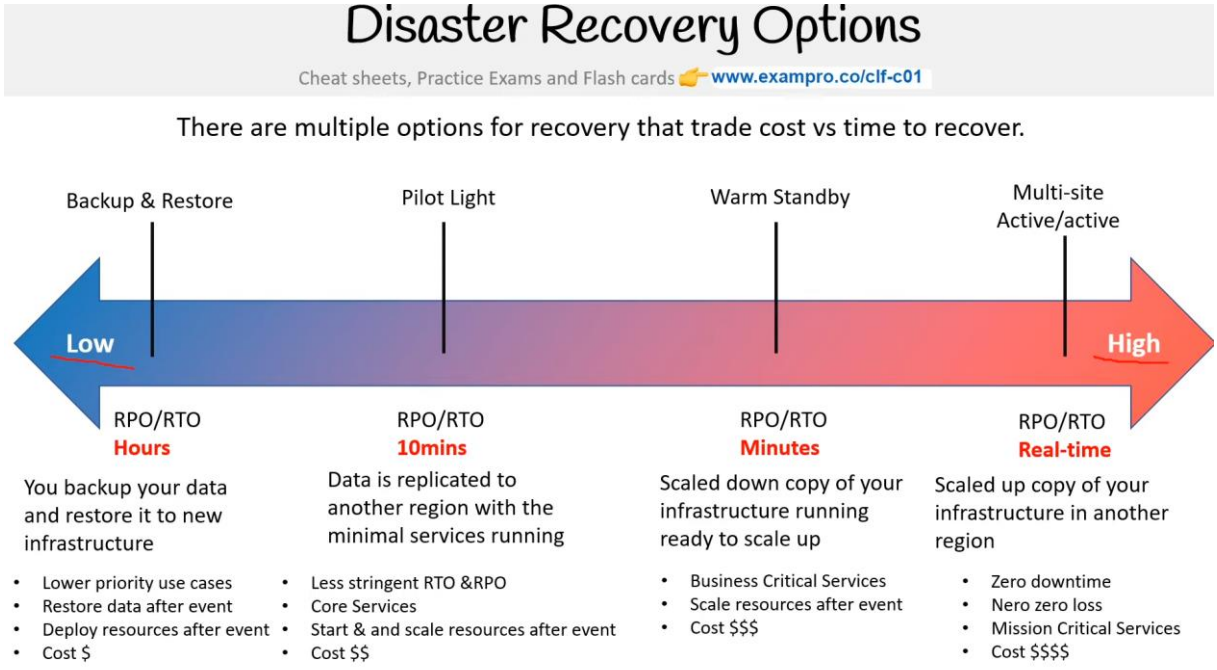
- Do you have a backup?
- How fast can you restore that backup?
- Does your backup still work?
- How do you ensure current live data is not corrupt?

CloudEndure Disaster Recovery continuously replicates your machines into a low-cost staging area in your target AWS account and preferred Region enabling fast and reliable recovery in case of IT data center failures.

Business Continuity Plan



Disaster Recovery Options



There are multiple options for recovery that trade cost vs time to recover.

Backup & Restore - RPO/RTO (Hours). You back up your data and restore it to new infrastructure

- Lower priority use cases
- Restore data after the event
- Deploy resources after the event
- Cost $

Pilot Light RPO/RTO (10 mins). Data is replicated to another region with minimal services running

- Less stringent RTO & RPO
- Core Services
- Start & scale resources after the event
- Cost $$

Warm Standby - RPO/RTO (Minutes) - Scaled-down copy of your infrastructure running ready to scale up

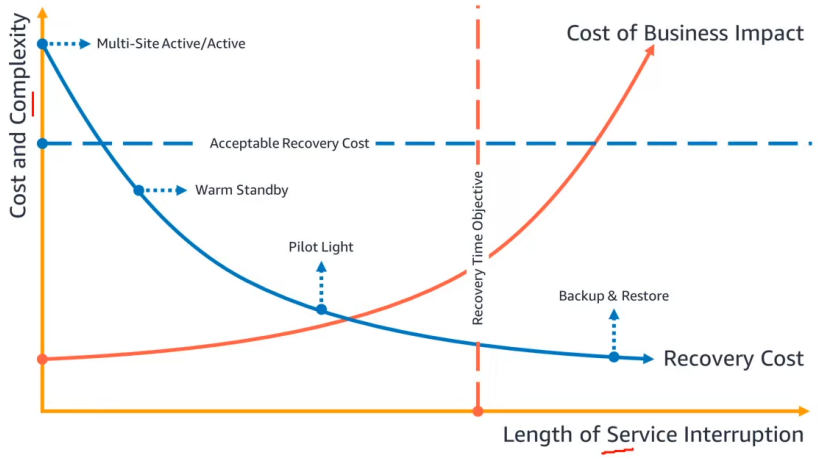
- Business Critical Services
- Scale resources after the event
- Cost $$$

Multi-site Active/active - RPO/RTO (Real-time) - Scaled up copy of your infrastructure in another region

- Zero downtime
- Near-zero loss
- Cost $$$$

RTO

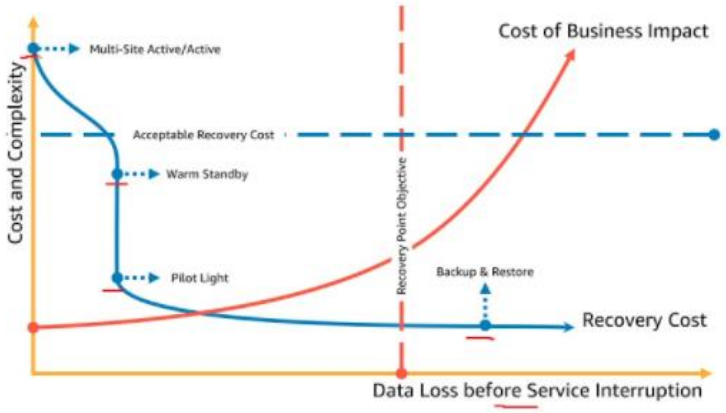
Recovery Time Objective (RTO) is the maximum acceptable delay between the interruption of service and restoration of service. This objective determines what is considered an acceptable time window when service is unavailable and is defined by the organization.



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.

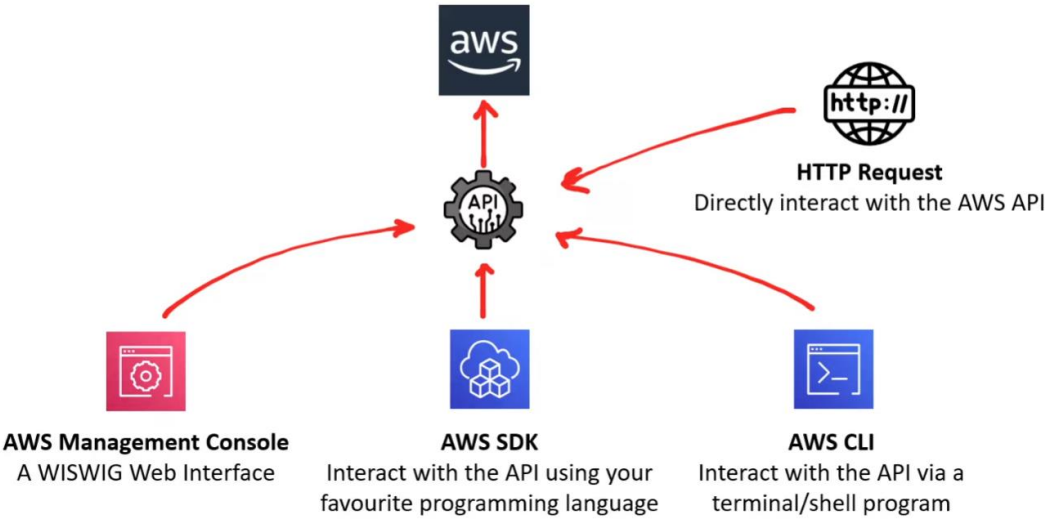


AWS API

AWS Application Programming Interface (API)

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

Rarely do users directly send HTTP requests directly to the AWS API.
Its much easier to interact with the API via a variety of Developer Tools



What is an Application Programming Interface (API)? - An API is software that allows two applications/services to talk to each other. The most common type of API is via HTTP/S requests.

AWS API is an HTTP API and you can interact by sending HTTPS requests, using an application interacting with APIs like Postman. Each AWS Service has its own Service Endpoint which you send requests

```
GET / HTTP/1.1
host: monitoring.us-east-1.amazonaws.com
x-amz-target: GraniteServiceVersion20100801.GetMetricData
x-amz-date: 20180112T092034Z
Authorization: AWS4-HMAC-SHA256 Credential=REDACTEDREDACTED/20180411/…..
Content-Type: application/json
Accept: application/json
Content-Encoding: amz-1.0
Content-Length: 45
Connection: keep-alive
```

To authorize use you will need generate a signed request You make a separate request with your AWS credentials and get back a token. You need to also provide an ACTION and accompanying parameters as the payload Rarely do users directly send HTTP requests directly to the AWS API. Its much easier to interact with the API via a variety of Developer Tools

HTTP Request - Directly interact with the AWS API

AWS Management Console - A WISWIG Web Interface

AWS SDK Interact with the API using your favourite programming language

AWS CLI Interact with the API via a terminal/shell program

Reference - https://en.wikipedia.org/wiki/API

https://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/making-api-requests.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/programming.html

https://docs.aws.amazon.com/general/latest/gr/aws-apis.html

AWS Management Console

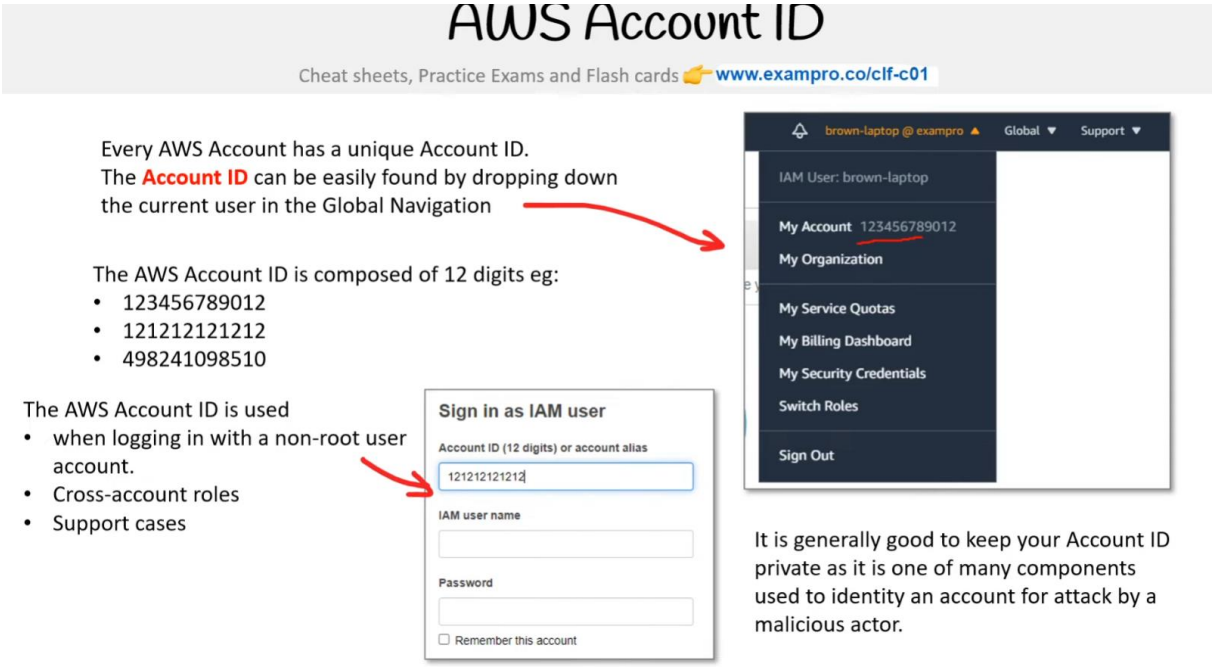
The AWS Management Console is a **web-based** unified console. **Build, manage, and monitor everything** from simple web apps to complex cloud deployments. Point and Click to manually launch and configure AWS resources with limited programming knowledge. This is known as “ClickOps” since you can perform all your system operations via clicks. The AWS Management Console is located at: console.aws.amazon.com

AWS Management Console - Service Console

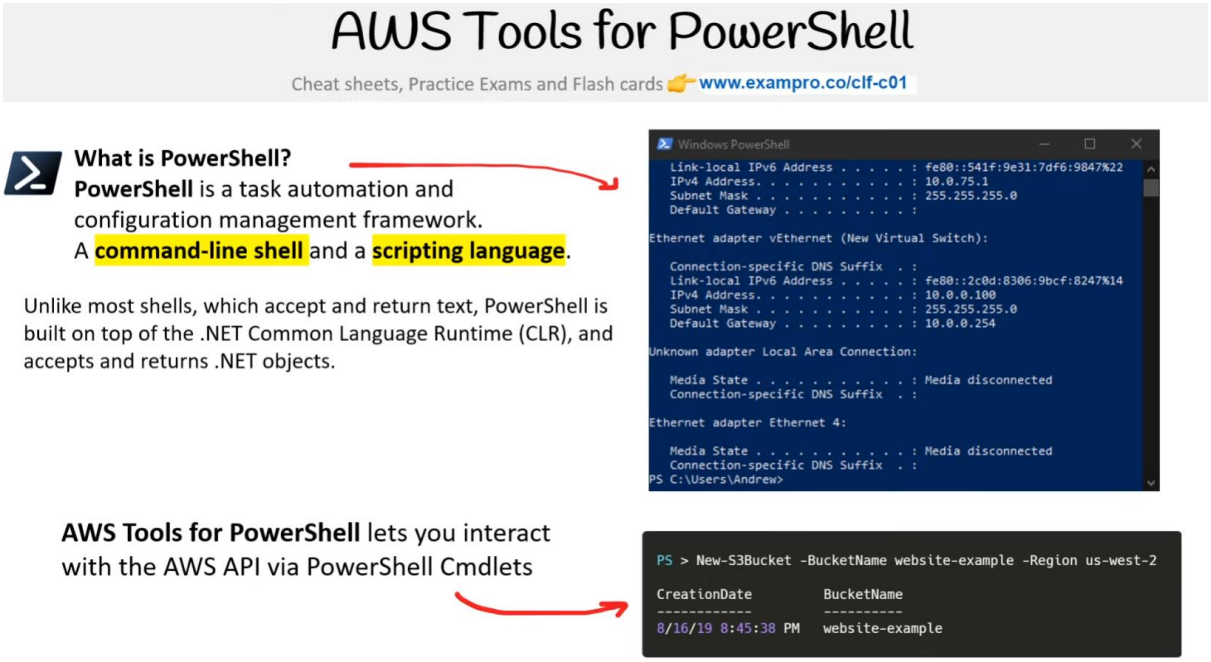
AWS Service each have their own customized console. You can access these consoles by **searching** the service name Some AWS Services Console will act as an umbrella console containing many AWS Services: e.g.

- VPC Console
- EC2 Console
- Systems Manager Console
- SageMaker Console
- CloudWatch Console

AWS Account ID



AWS Tools for PowerShell



What is PowerShell? - **PowerShell** is a task automation and configuration management framework.

A **command-line shell** and a **scripting language** - Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. **AWS Tools for PowerShell** lets you interact with the AWS API via PowerShell Cmdlets. Cmdlet is a special type of command in PowerShell in the form of capitalized verb-and-noun e.g. New-S3Bucket

Amazon Resource Name (ARNs)

Amazon Resource Names (ARNs) uniquely identify AWS resources. ARNs are required to specify a resource unambiguously across all of AWS The ARN has the following **format variations**

arn:**partition:service:region:account-id:resource-id**
arn:**partition:service:region:account-id:resource-type/resource-id**
arn:**partition:service:region:account-id:resource-type:resource-id**

Partition

- aws - AWS Regions
- aws-cn - China Regions
- aws-us-gov - AWS GovCloud (US) Regions

Service – Identifies the service

- ec2
- s3
- iam

Region – which AWS resource

- us-east-1
- ca-central-1

Account ID

- 121212121212
- 123456789012

Resource ID **-** Could be a number name or path:

- user/Bob
- instance/i-1234567890abcdef0

In the AWS Management Console its common to be able to copy the ARN to your clipboard

arn:aws:s3:::my-bucket

Paths in ARNs - Resource ARNs can include a path Paths can include a wildcard character, namely an asterisk (*)

IAM Policy ARN Path - arn:aws:iam::123456789012:user/Development/product_1234/*

S3 ARN Path - arn:aws:s3:::my*corporate*bucket/Development/*

Reference - Amazon Resource Names (ARNs)

AWS Command Line Interface (CLI)

What is a CLI? - A Command Line Interface (CLI) **processes commands to a computer program in the form of lines of text**. Operating systems implement a command-line interface in a shell.

What is a Terminal? - A terminal is a text only interface (input/output environment)

What is a Console? - A console is a physical computer to physically input information into a terminal

What is a Shell? - A shell is the command line program that users interact with to input commands. Popular shell programs:

- **Bash**
- Zsh
- PowerShell

People commonly (erroneously) use Terminal, Shell or Console to generally describe interacting with a Shell. AWS Command Line Interface (CLI) allows users to programmatically interact with the AWS API via entering **single or multi-line commands** into a shell or terminal

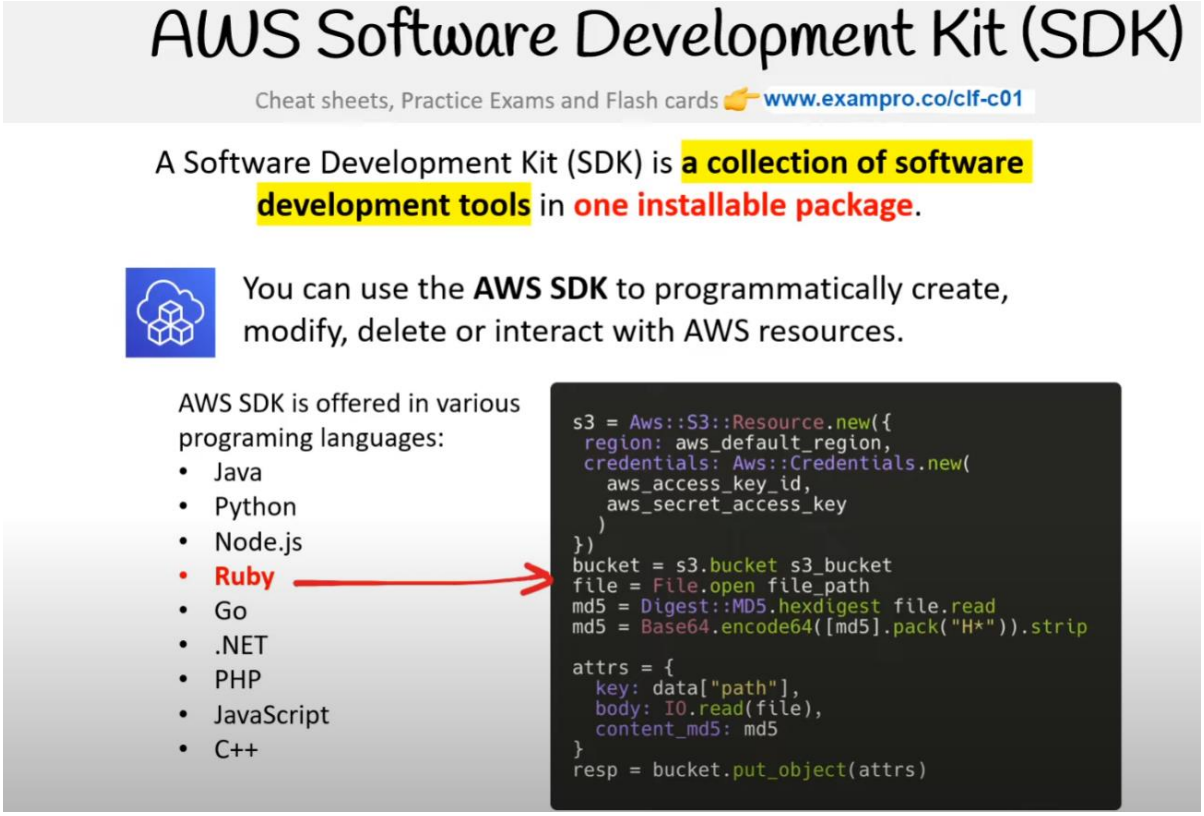
The AWS CLI is a Python executable program.

- Python is required to install AWS CLI

The AWS CLI can be installed on Windows, Mac or Linux/Unix. The name of the CLI program is **aws**

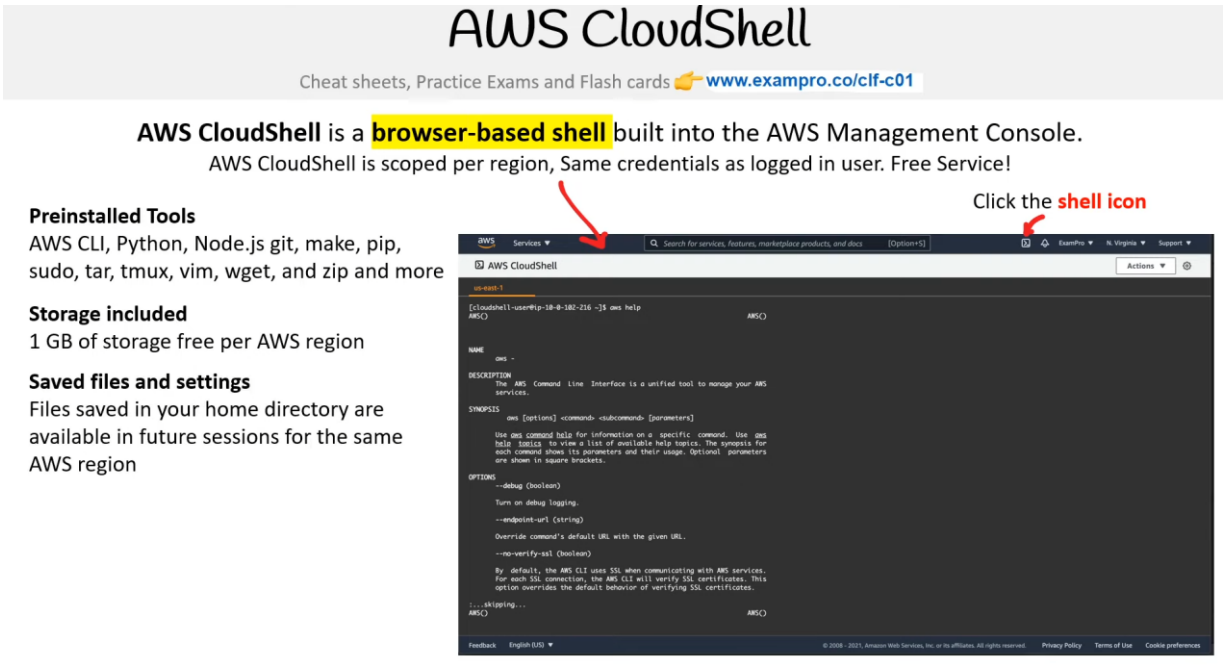
Reference - What is the difference between Terminal, Console, Shell, and Command Line?

AWS Software Development Kit (SDK)



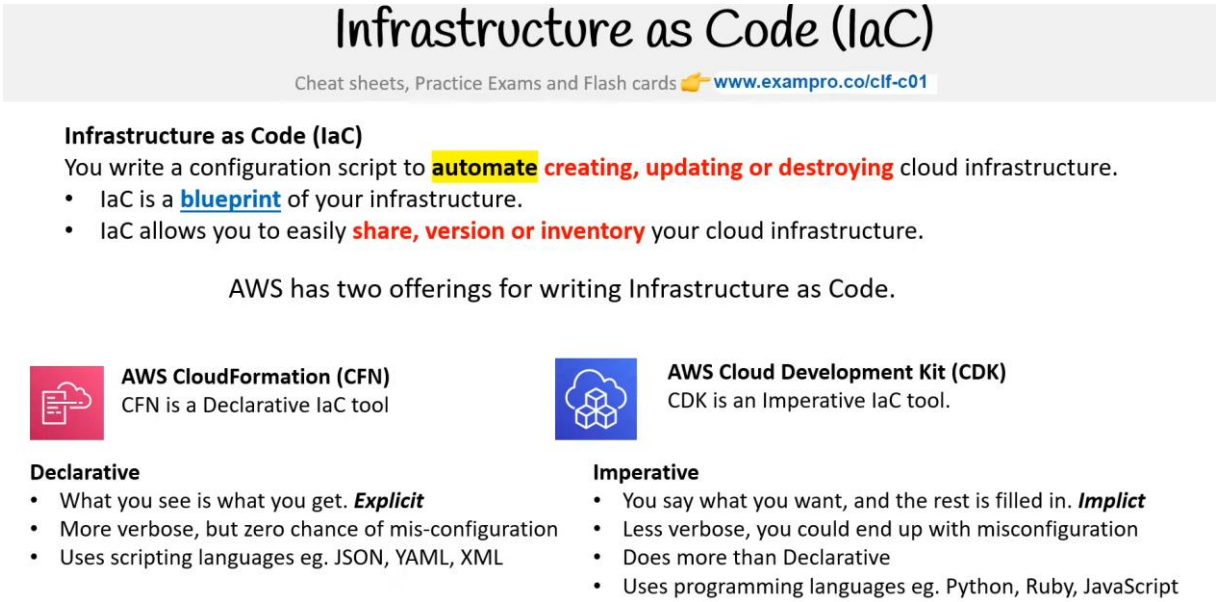
Reference - [Software Development Kit (SDK)]

AWS CloudShell



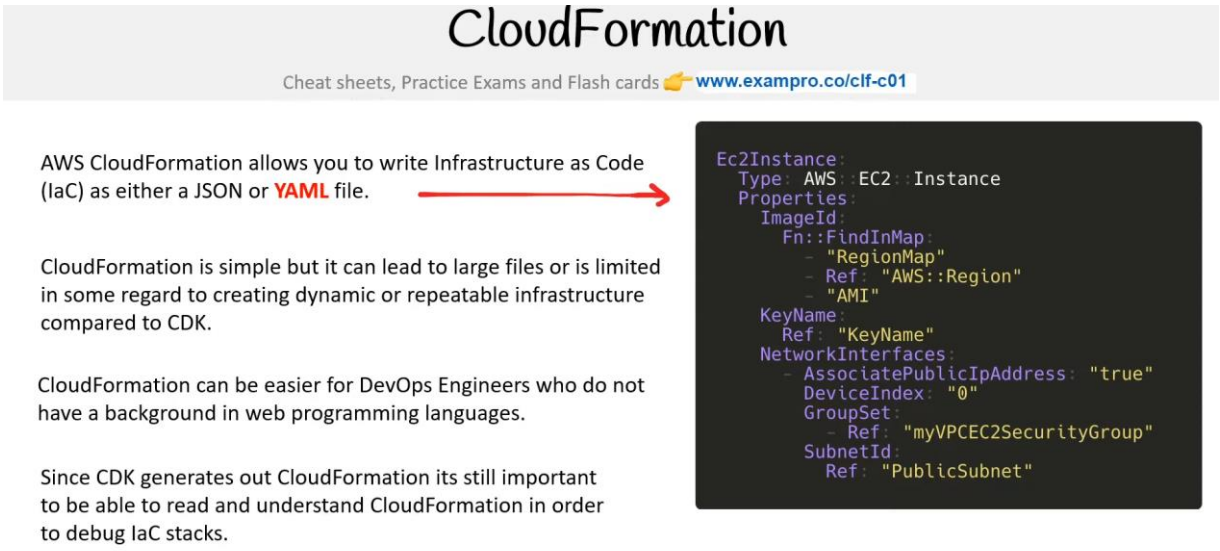
Reference - [What is AWS CloudShell?]

Infrastructure as Code (IaC)

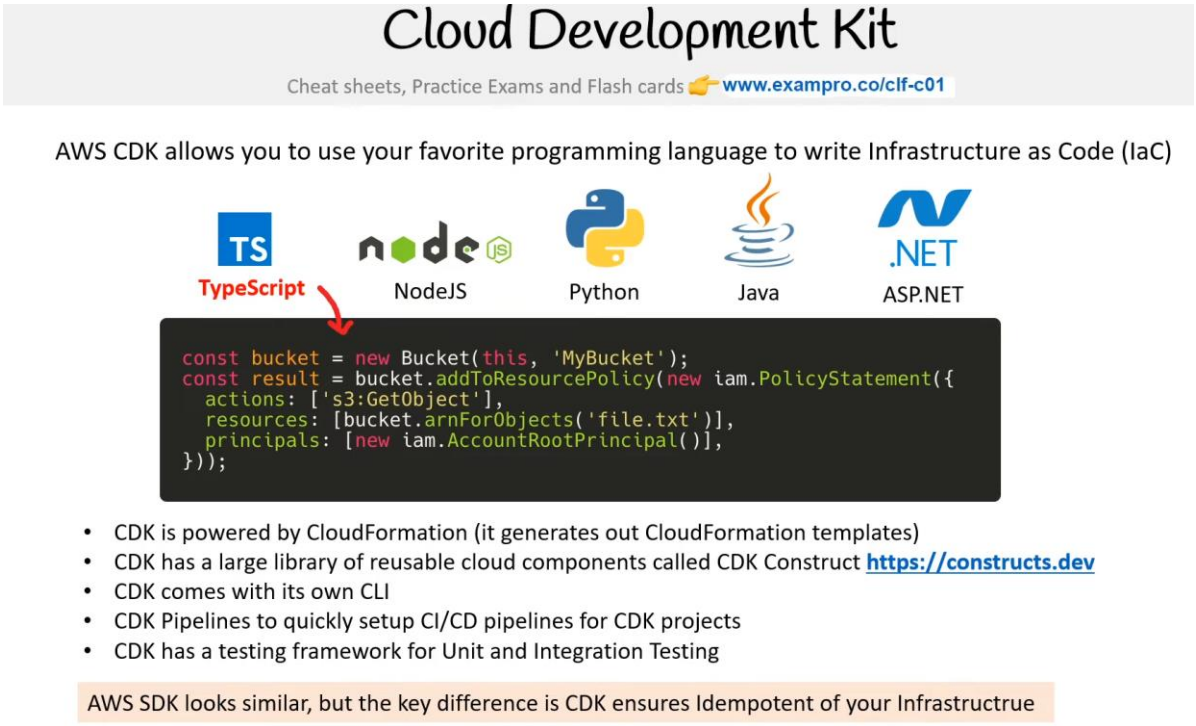


Reference - Infrastructure as code | Declarative programming | Imperative programming

CloudFormation



Cloud Development Kit



Reference - Construct Hub | CDK Pipelines: Continuous delivery for AWS CDK applications

AWS Toolkit for VSCode

AWS Toolkit is an open-source plugin for VSCode to create, debug, deploy AWS resources

1. AWS Explorer - Explore a wide range of AWS resources to your linked AWS Account

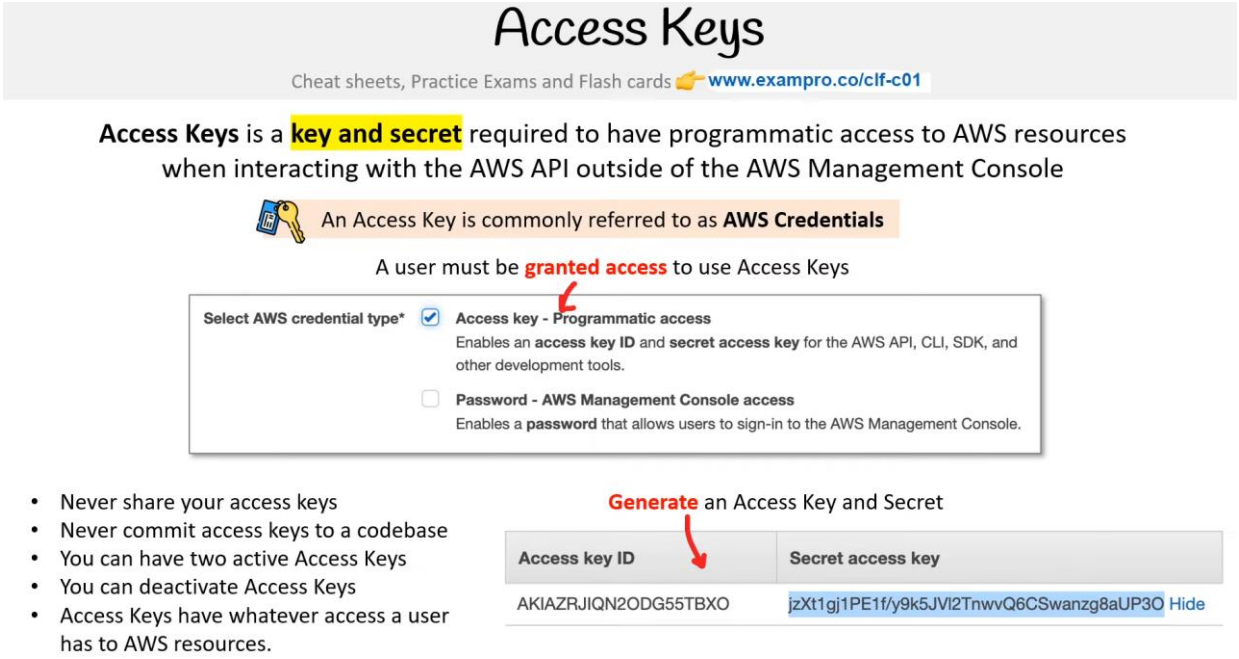
2. AWS CDK Explorer - Allows you to explore your stacks defined by CDK.

3. Amazon Elastic Container Service - Provides IntelliSense for ECS task-definitions files

4. Serverless Applications - Create, debug and deploy serverless applications via SAM and CFN

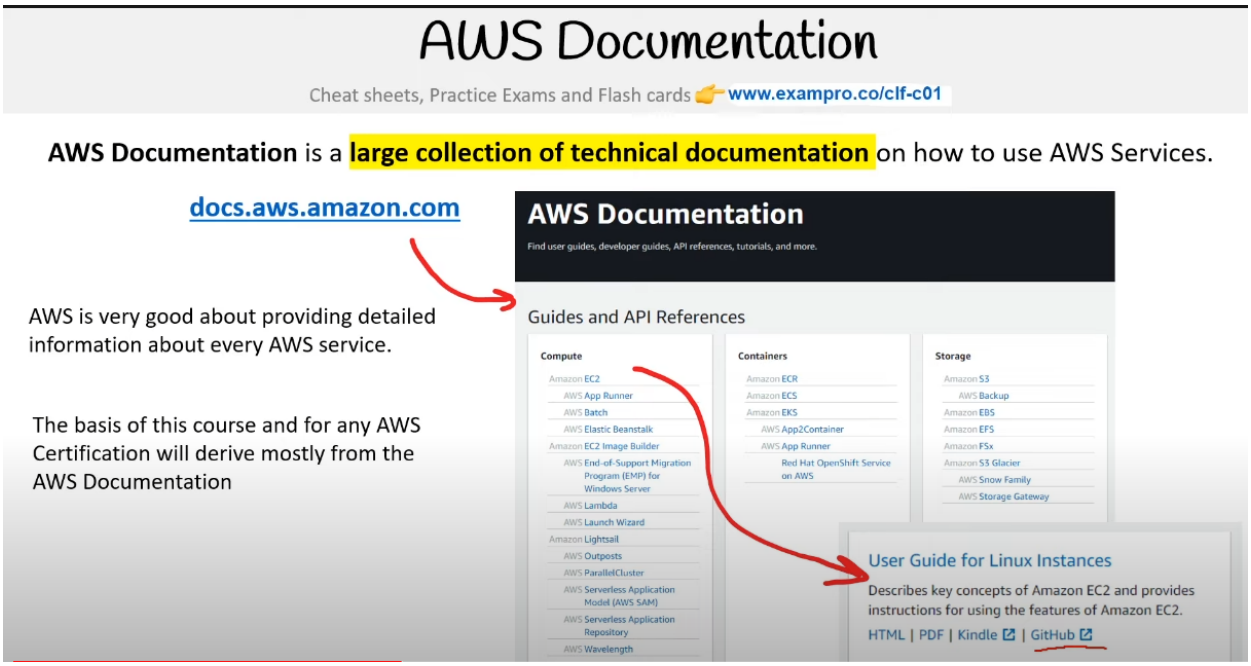
Reference - Working with AWS Services

Access Keys

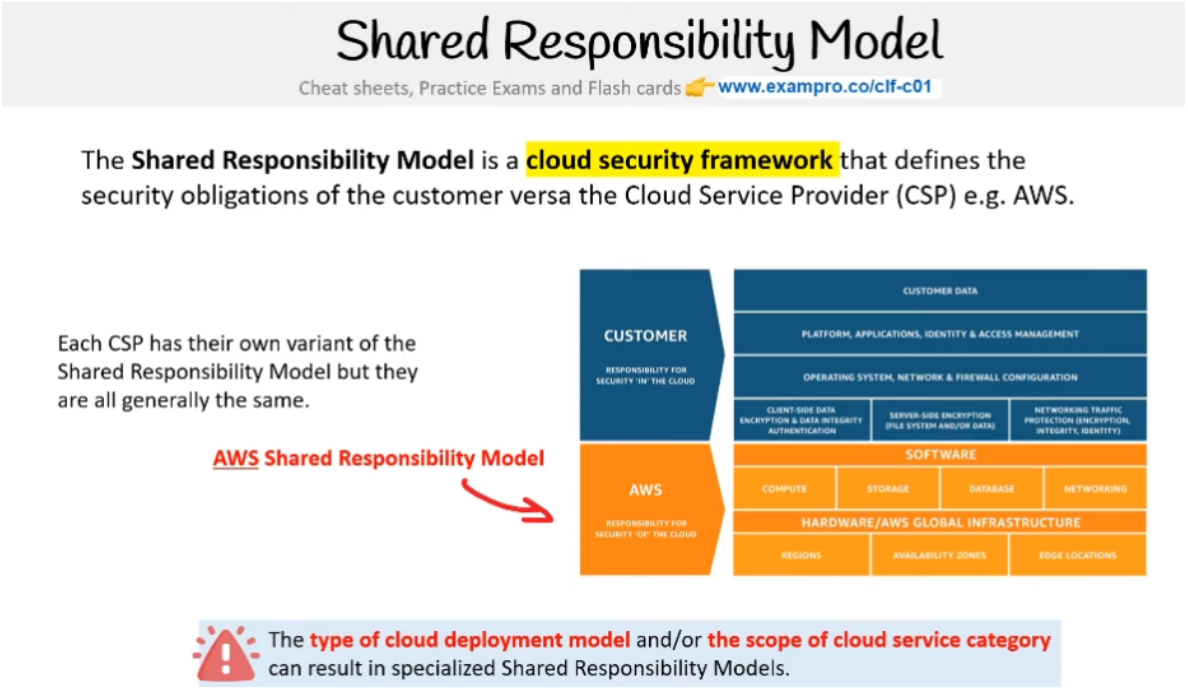


Reference - [Configuration and credential file settings | Environment variables to configure the AWS CLI]

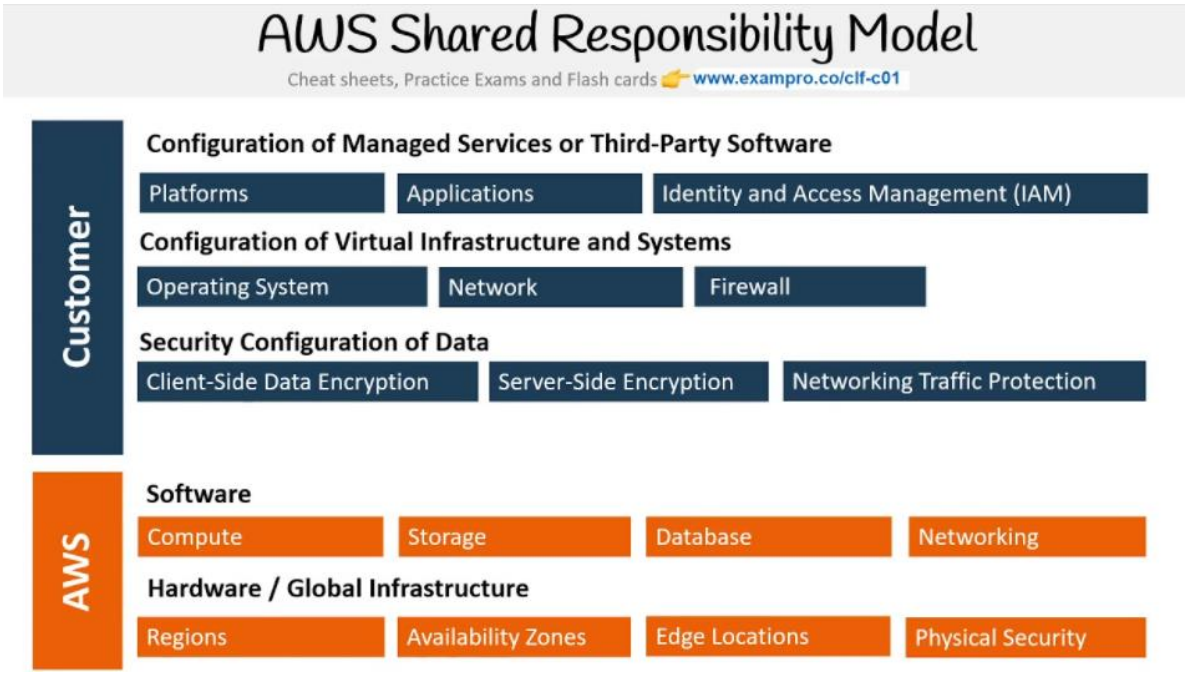
AWS Documentation



Shared Responsibility Model

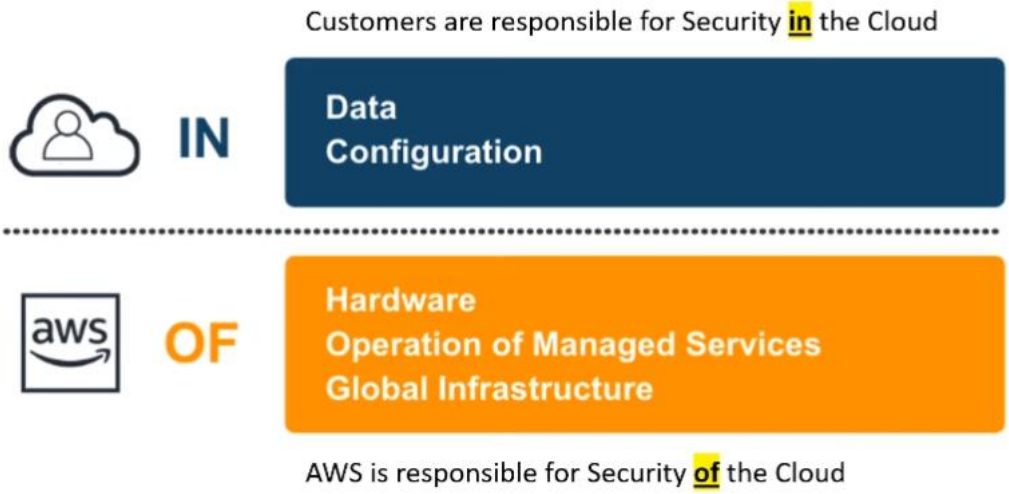


Reference - [Shared Responsibility Model]



AWS Shared Responsibility Model

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



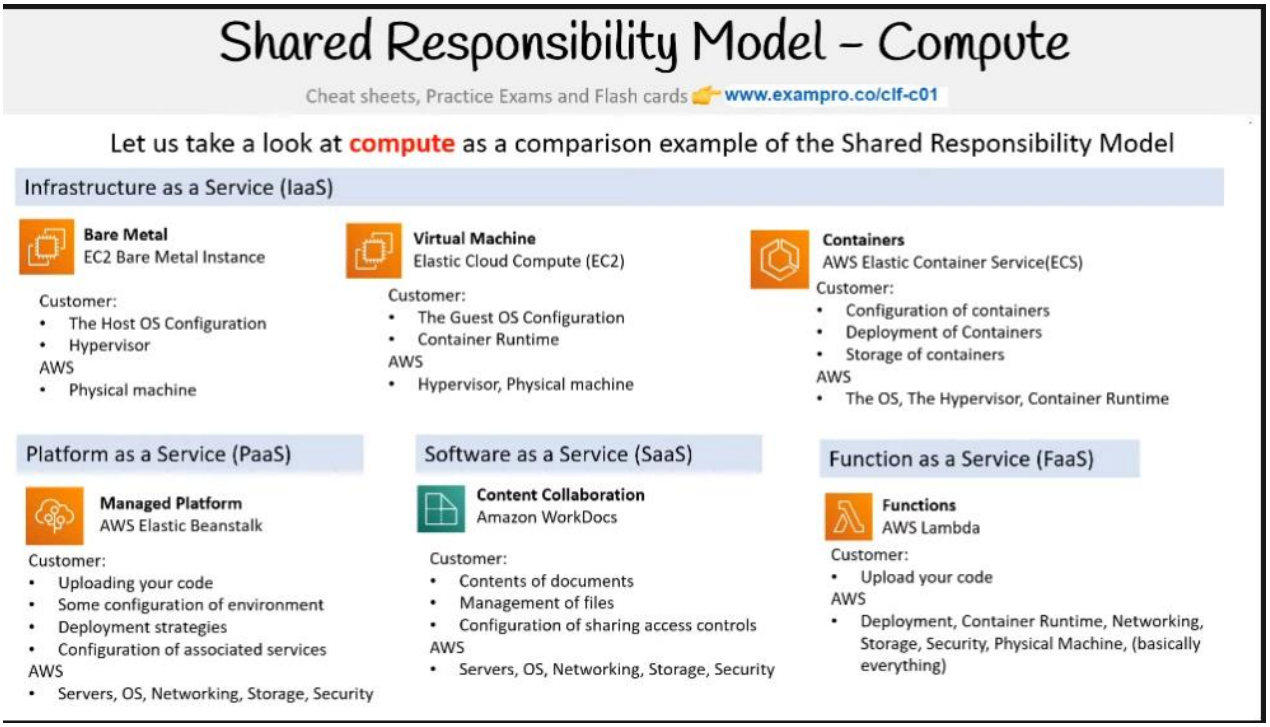
Types of Cloud Computing Responsibility

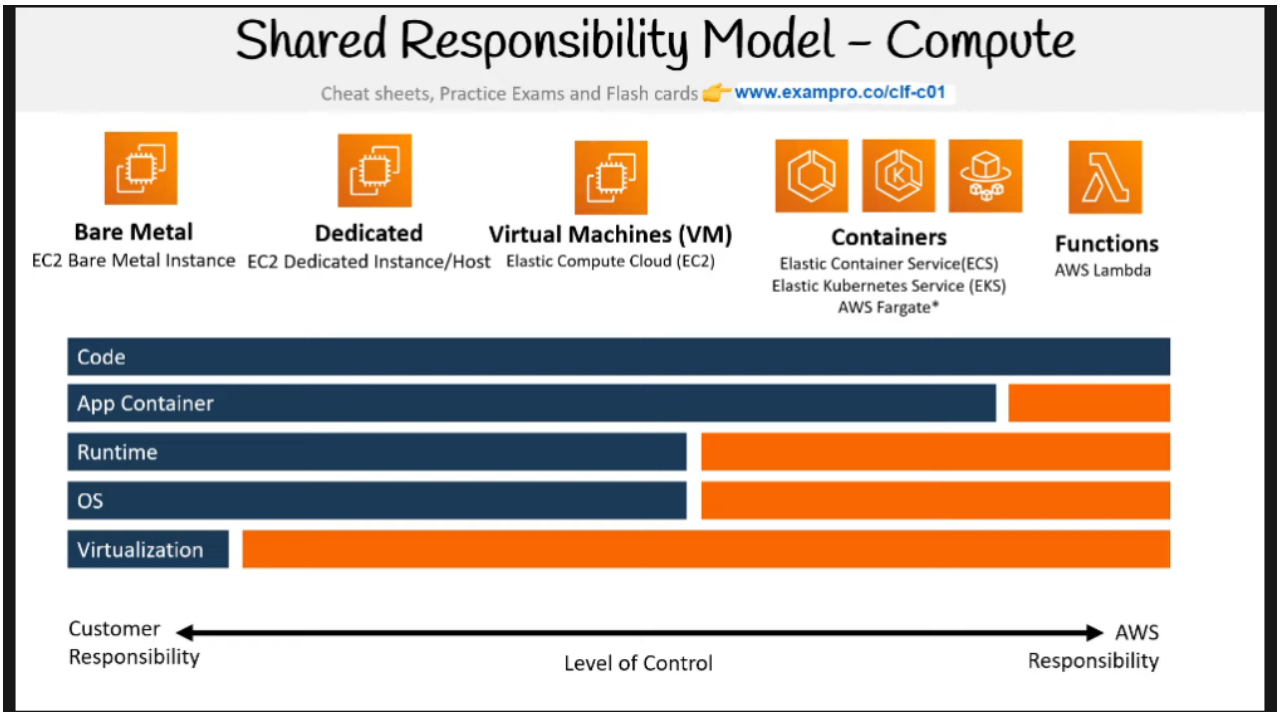
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

On-Premise	Infrastructure as a Service	Platform as a Service	Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Legend: Customer is Responsible | CSP is Responsible

Shared Responsibility Model - Compute





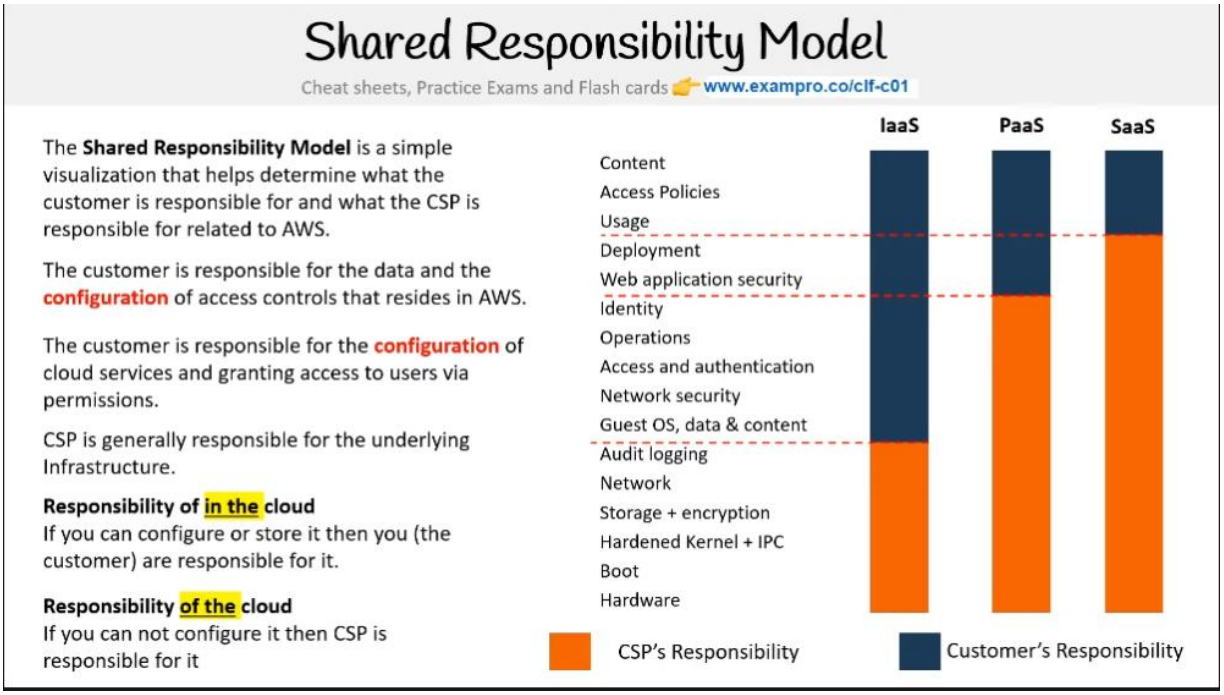
Reference

[Shared Responsibility: What This Means for You as a CISO (Cloud Next '19)]

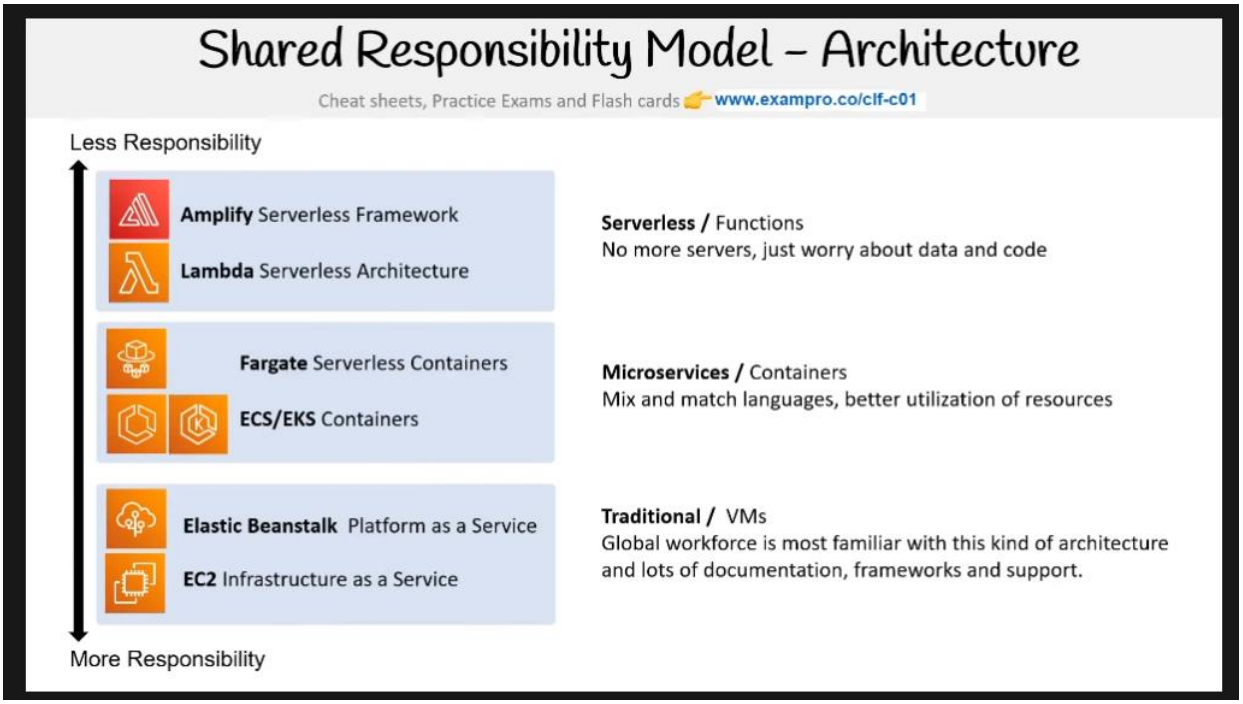
[Exploring container security: the shared responsibility model in GKE]

[Google Cloud Platform: Shared Responsibility Matrix]

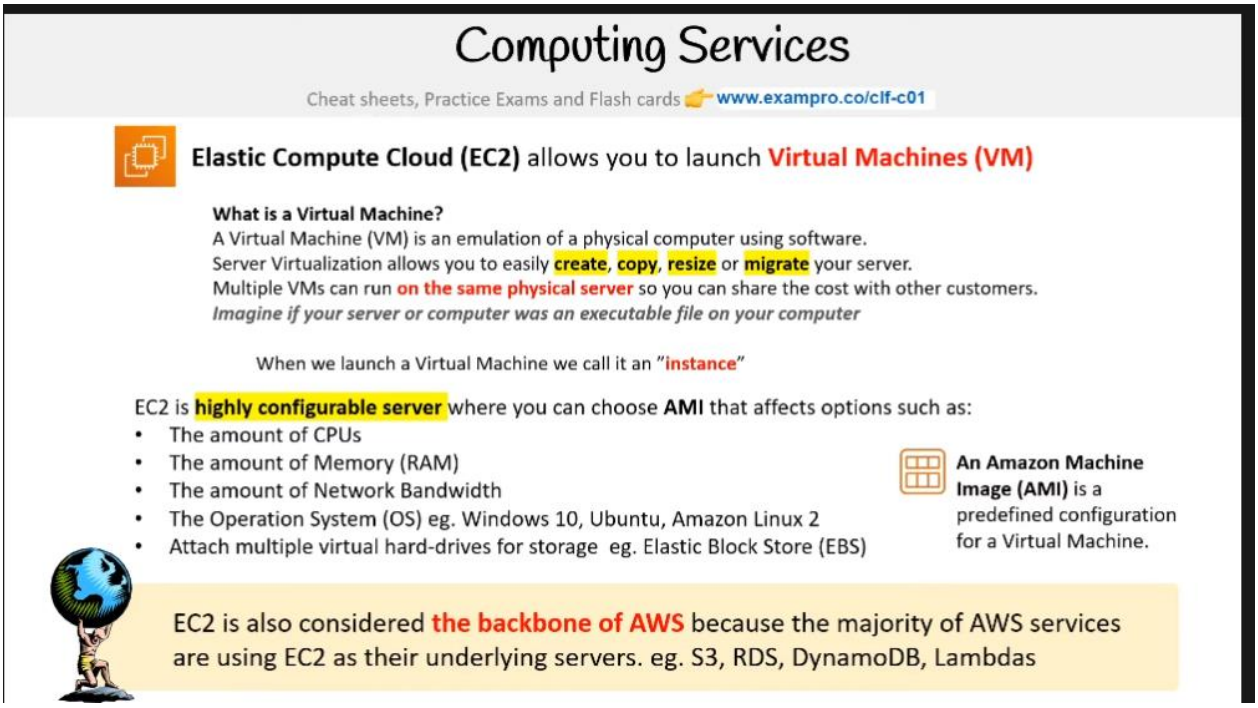
Shared Responsibility Model



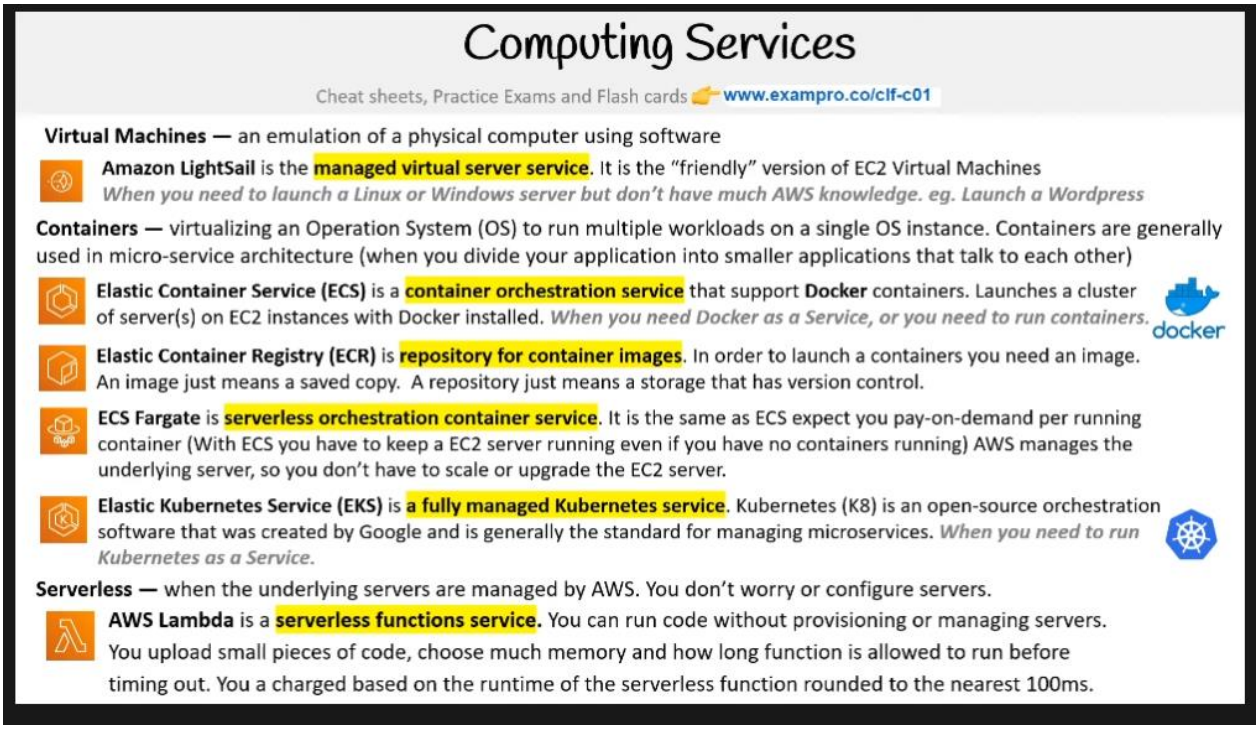
Shared Responsibility Model - Architecture



Computing Services



Containers



- virtualizing an Operation System (OS) to run multiple workloads on a single OS instance. Containers are generally used in micro-service architecture (when you divide your application into smaller applications that talk to each other)

Elastic Container Service (ECS) - is a container orchestration service that support Docker containers. Launches a cluster of server(s) on EC2 instances with Docker installed. When you need Docker as a Service, or you need to run containers.

Elastic Container Registry (ECR) - is repository for container images. In order to launch a containers you need an image. An image just means a saved copy. A repository just means a storage that has version control.

ECS Fargate - is a serverless orchestration container service. It is the same as ECS expect you pay-on-demand per running container (With ECS you have to keep a EC2 server running even if you have no containers running) AWS manages the underlying server, so you don't have to scale or upgrade the EC2 server.

Elastic Kubernetes Service (EKS) - is a fully managed Kubernetes service. Kubernetes (K8) is an open-source orchestration software that was created by Google and is generally the standard for managing microservices. When you need to run Kubernetes as a Service.

Serverless

- when the underlying servers are managed by AWS. You don't worry or configure servers.

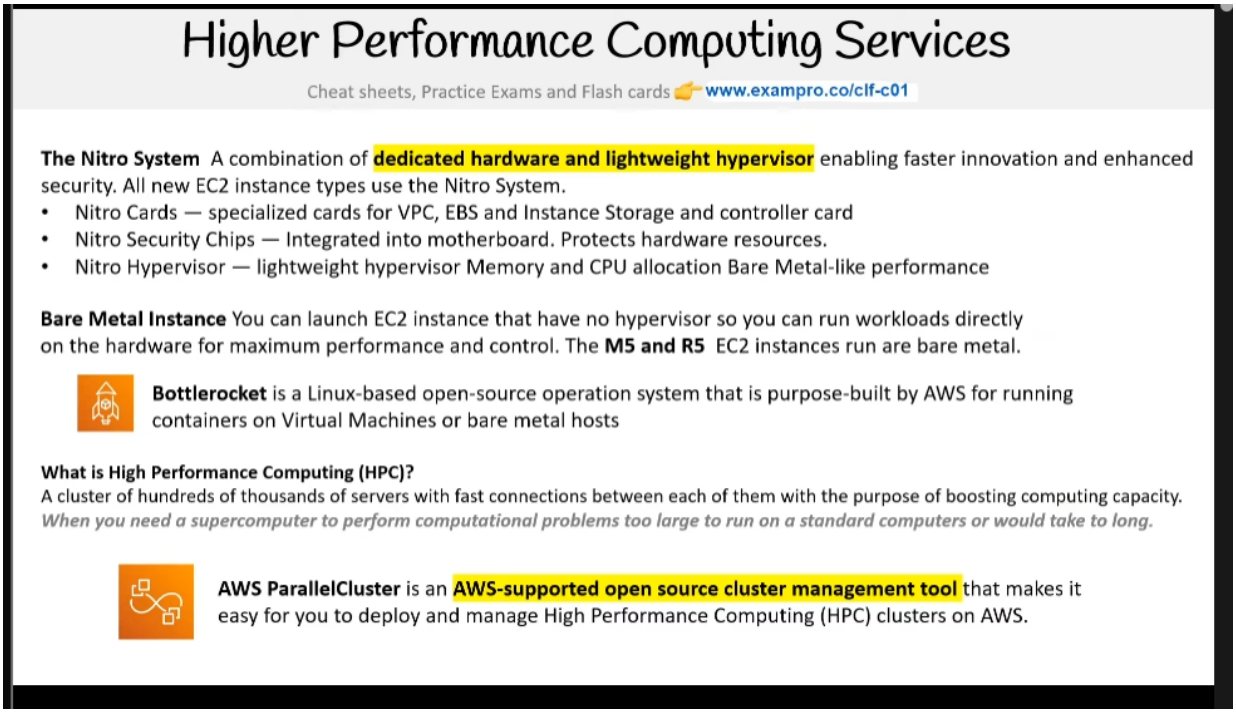
AWS Lambdais a serverless functions service. You can run code without provisioning or managing servers. You upload small pieces of code, choose much memory and how long function is allowed to run before timing out. You a charged based on the runtime of the serverless function rounded to the nearest 100ms.

Virtual Machines

- an emulation of a physical computer using software

Amazon LightSail - is the managed virtual server service. It is the "friendly" version of EC2 Virtual Machines

Higher Performance Computing



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

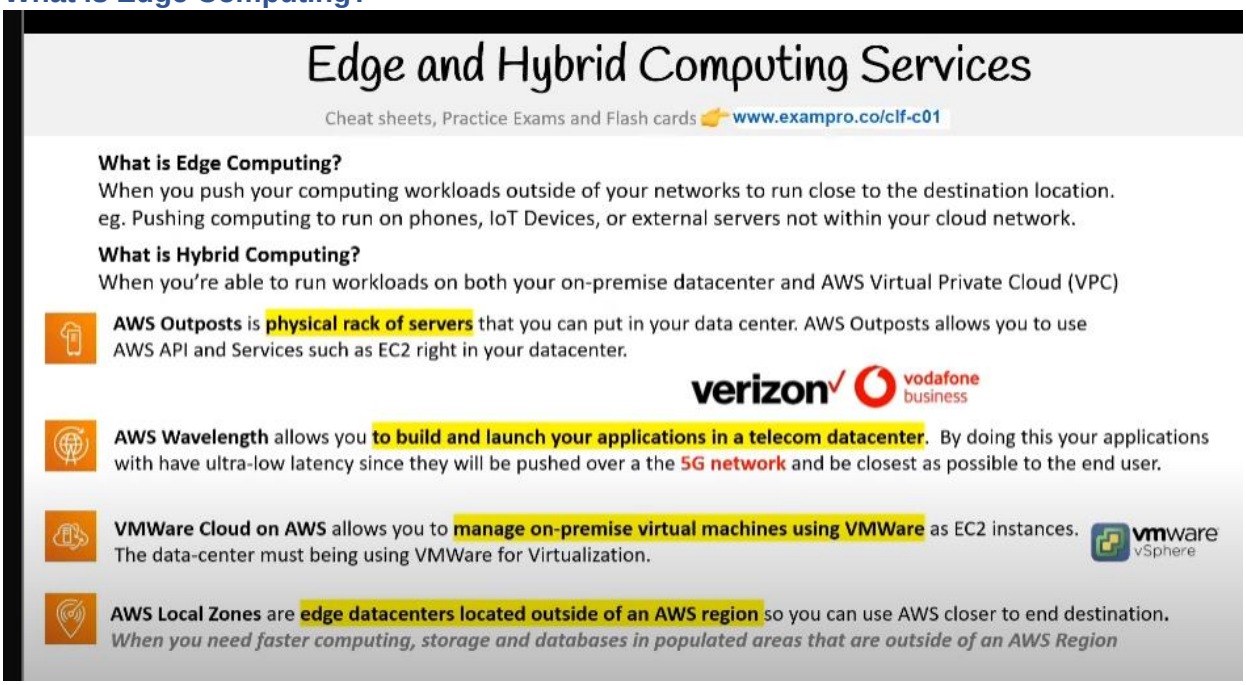
Bare Metal Instance - You can launch EC2 instance that have no hypervisor so you can run workloads directly on the hardware for maximum performance and control. The M5 and R5 EC2 instances run are bare metal.

- **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 to large to fix 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.

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)

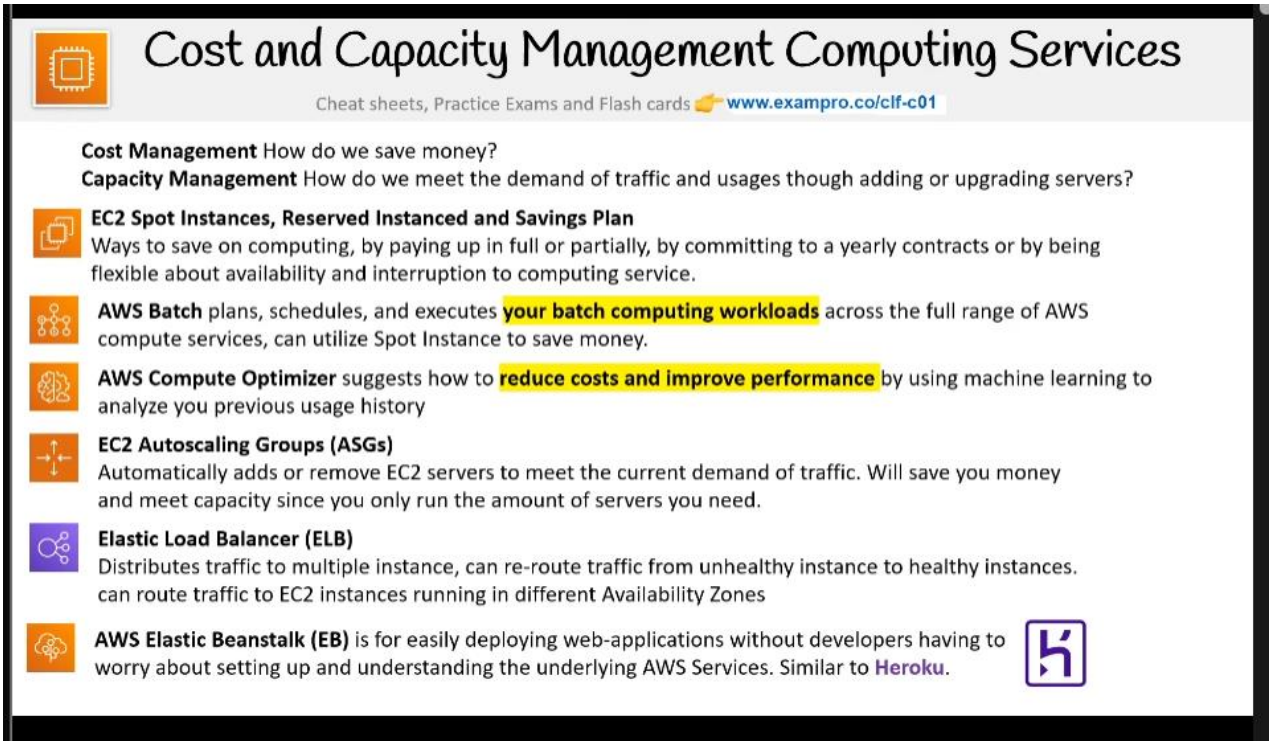
AWS Outposts - is physical rack of servers that you can put in your data center. AWS Outposts allows you to use AWS API and Services such as EC2 right in your datacenter.

AWS Wavelength - 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.

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

Cost managemant



Cost Management - How do we save money? **Capacity Management** - How do we meet the demand of traffic and usages though adding or upgrading servers?

EC2 Spot Instances, Reserved Instanced and Savings Plan - Ways to save on computing, by paying up in full or partially, by committing to a yearly contracts or by being flexible about availability and interruption to computing service.

AWS Batch - plans, schedules, and executes your batch computing workloads across the full range of AWS compute services, can utilize Spot Instance to save money.

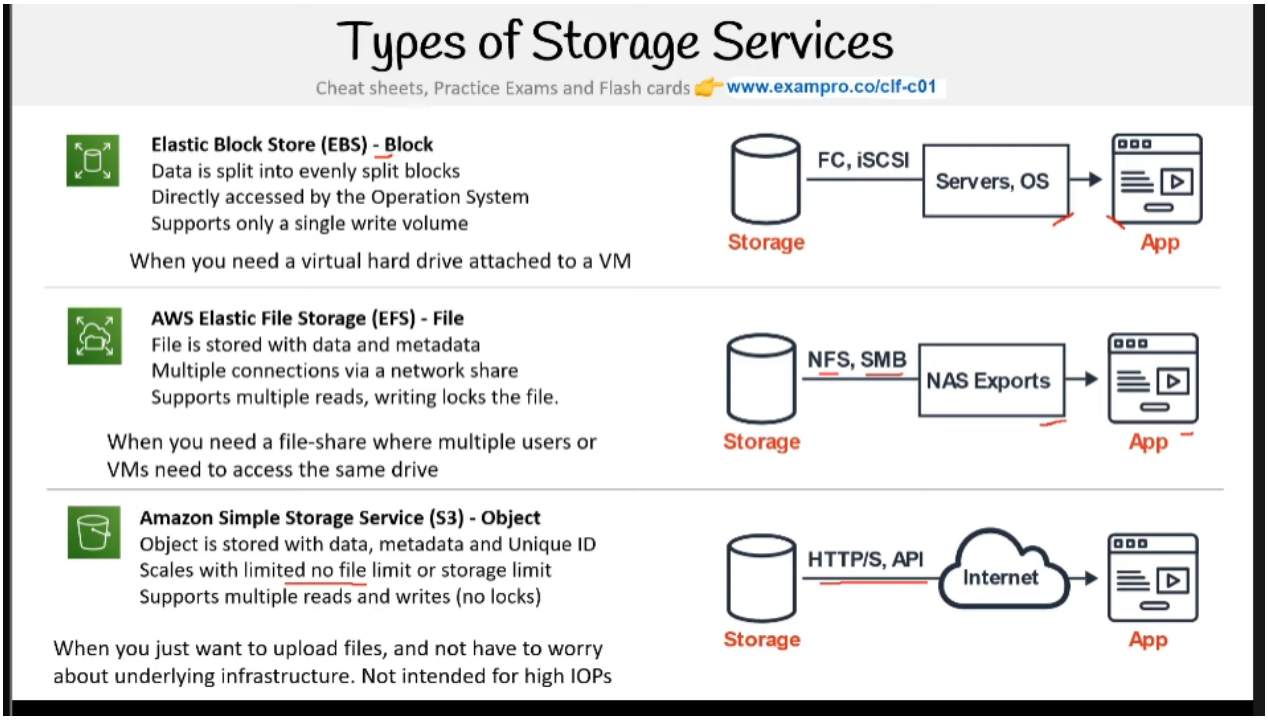
AWS Compute Optimizer - Suggests how to reduce costs and improve performance by using machine learning to analyze you previous usage history

EC2 Autoscaling Groups (ASGs) - Automatically adds or remove EC2 servers to meet the current demand of traffic. Will save you money and meet capacity since you only run the amount of servers you need.

Elastic Load Balancer (ELB) - Distributes traffic to multiple instance, can re-route traffic from unhealthy instance to healthy instances. Can route traffic to EC2 instances running in different Availability Zones

Elastic Beanstalk (EB) - is for easily deploying web-applications without developers having to worry about setting up and understanding the underlying AWS Services. Similar to Heroku.

Types of Storage Services

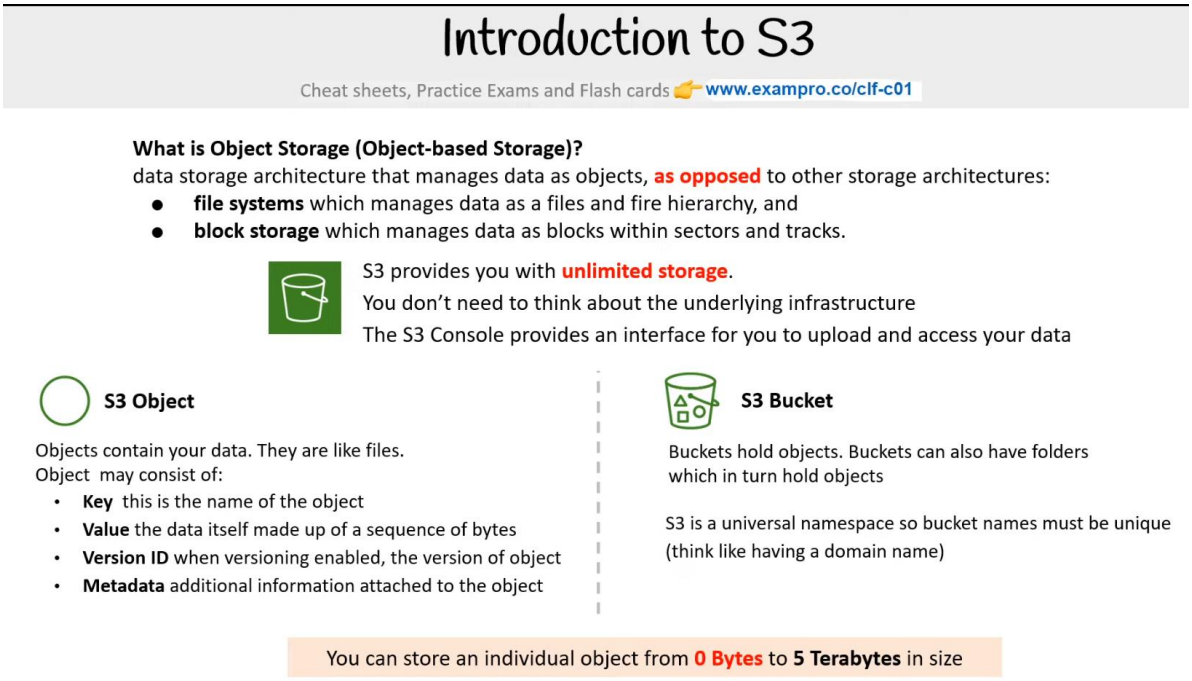


Introduction to S3 - What is Object Storage (Object-based Storage)? - Data storage architecture that manages data as objects, **as opposed** to other storage architectures:

- file systems which manage data as files and fire hierarchy, and
- block storage which manages data as blocks within sectors and tracks.

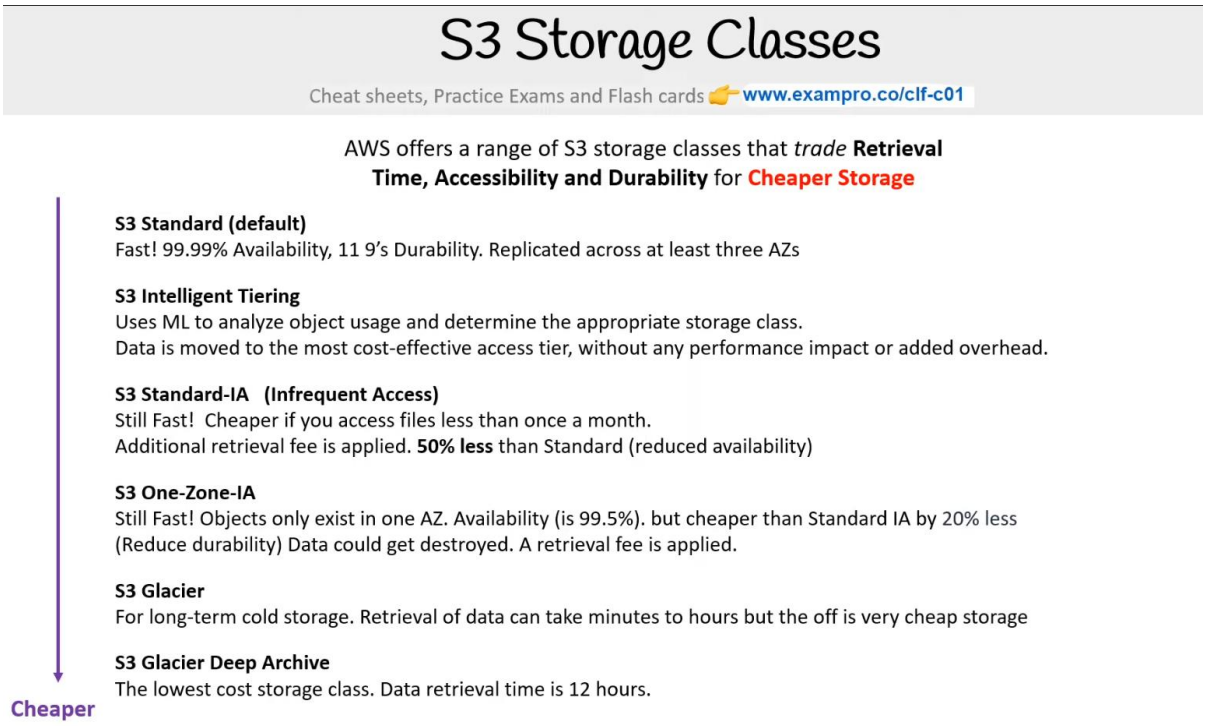
S3 provides you with **unlimited storage**. You don't need to think about the underlying infrastructure. The S3 Console provides an interface for you to upload and access your data

S3 Object



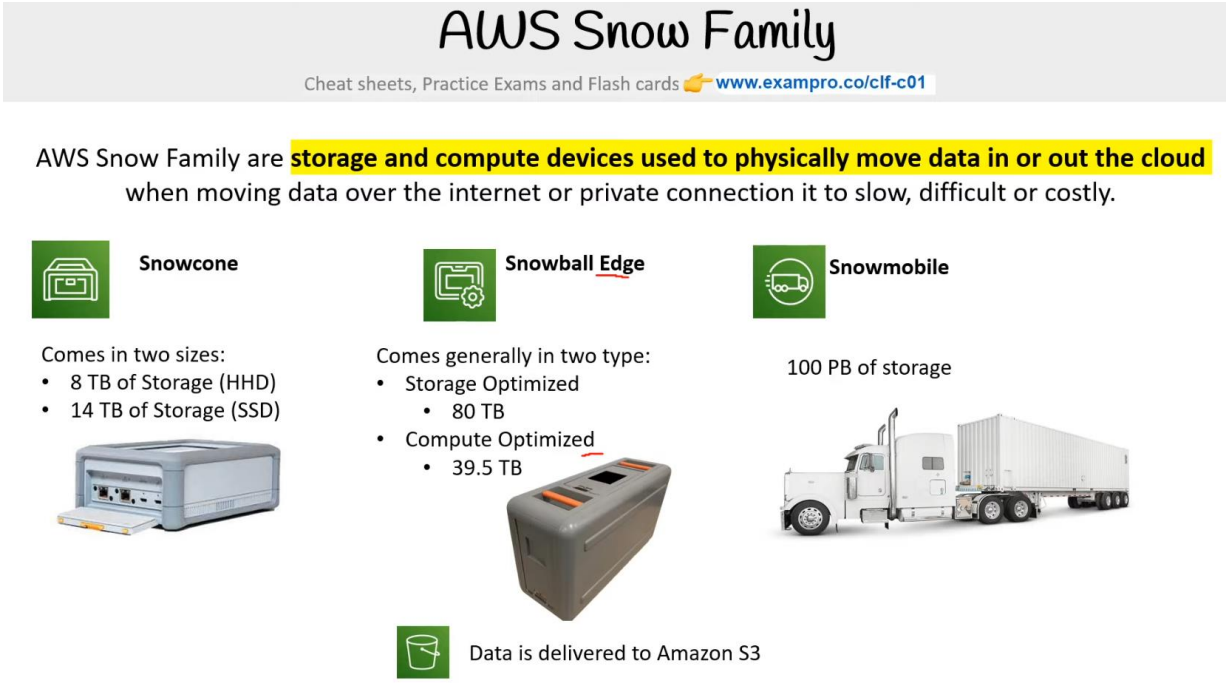
Reference - [Object storage]

S3 Storage Classes



Reference - [Storage classes]

AWS Snow Family

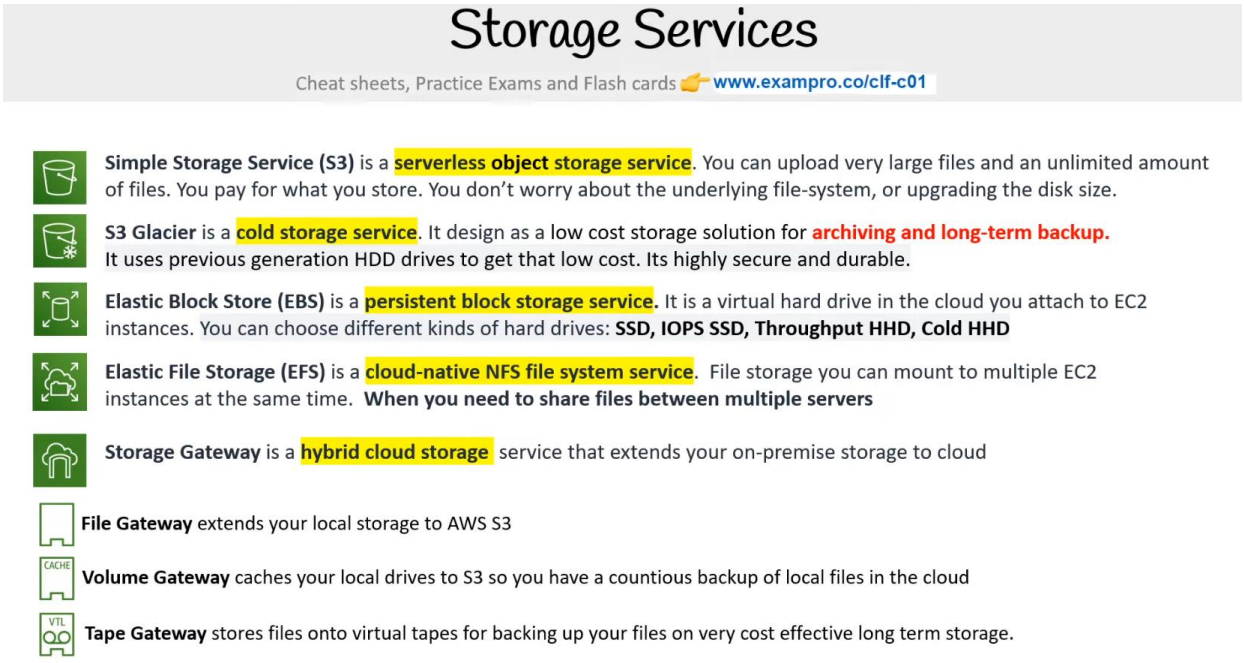


Reference

[AWS re:Invent recap: Optimize your data migration with AWS Snow Family]

[AWS Snowball Edge Device Differences]

Storage Services:



Storage Services

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

AWS Snow Family are **storage devices used to physically migrate large amounts of data** to the cloud.

- ~~Snowball and~~ **Snowball Edge** are briefcase size data storage devices. **50-80 Terabytes**
- **Snowmobile** is a cargo container filled with racks of storage and compute that is transported via semi-trailer tractor truck to transfer up to **100PB** of data per trailer.
- **Snowcone** is a very small version of Snowball that can transfer **8TB** of data.

AWS Backup a fully **managed backup service** that makes it easy to centralize and automate the backup of data across multiple AWS services eg. EC2, EBS, RDS, DynamoDB, EFS, Storage Gateway. You create backup plans.

CloudEndure Disaster Recovery continuously replicates your machines into a low-cost staging area in your target AWS account and preferred Region enabling fast and reliable recovery in case of IT data center failures.

Amazon FSx is a **feature rich and highly-performant file system.** That can be used for Windows (SMB) or Linux (Lustre)

Amazon FSx for Window File Server uses the SMB protocol and allows you to mount FSx to Windows servers

Amazon FSx for Lustre uses Linux's Lustre file system and allows you to mount FSx to Linux servers

Provide scalable cloud-based storage solutions for your workloads on AWS.

- **S3 (Simple Storage Service)** - is an object storage service that offers industry-leading scalability, data availability, security, and performance. Think of it as a "hard drive in the cloud" with a lot of available space.
- **S3 Glacier** - low cost storage for archiving and long-term backup Trade-off: You may have to wait several hours to access data stored here. Use case: for data that you must hold on to but are unlikely to look at often. Example: an enterprise company that must store records for many years under a litigation hold.
- **EBS** - `Elastic Block Storage- is a persistent block storage service. It is a virtual hard drive in the cloud you attach to EC2 instances. You can choose different kinds of hard drives: **SSD, IOPS SSD, Throughput HHD, Cold HHD**
- **EFS** - Elastic File Storage- file storage mountable to multiple EC2 instances at the same time
- **Storage Gateway** - hybrid cloud storage with local caching. Expand your on-premises storage capacity into the cloud.
- **File Gateway** extends your local storage to AWS S3
- **Volume Gateway** caches your local drives to S3 so you have a continuous backup of local files in the cloud
- **Tape Gateway** stores files onto virtual tapes for backing up your files on very cost-effective long-term storage.
- **AWS Snow Family** are storage devices used to physically migrate large amounts of data to the cloud.
- Snowball and Snowball Edge are briefcase-size data storage devices. 50-80 Terabytes
- **Snowball edge** - A version of Snowball for even larger sets of data - 100 TB
- **Snowmobile** is a cargo container filled with racks of storage and compute that is transported via semi-trailer tractor truck to transfer up to 100PB of data per trailer.
- **Snowcone** is a very small version of Snowball that can transfer 8TB of data.

What is a Database?

What is a Database?

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

A database is a **data-store that stores semi-structured and structured data**.

A database is more **complex data stores** because it **requires using formal design and modeling techniques**

Databases can be generally categorized as either:

- **Relational databases**
  - Structured data that strongly represents tabular data (tables, rows and columns)
    - Row-oriented or Columnar-oriented
- **Non-relational databases**
  - Semi-structured that may or may not distantly resemble tabular data.

Databases have a rich set of functionality:

- specialized language to query (retrieve data)
- specialized modeling strategies to optimize retrieval for different use cases
- more fine tune control over the transformation of the data into useful data structures or reports

Reference - Database

What is 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**

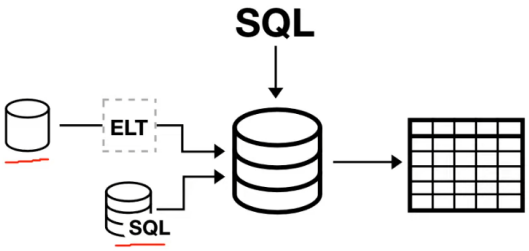
- aggregation is grouping data eg. find a total or average
- Data warehouses are optimized around columns since they need to quickly aggerate column data

Data warehouses are generally designed be HOT

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

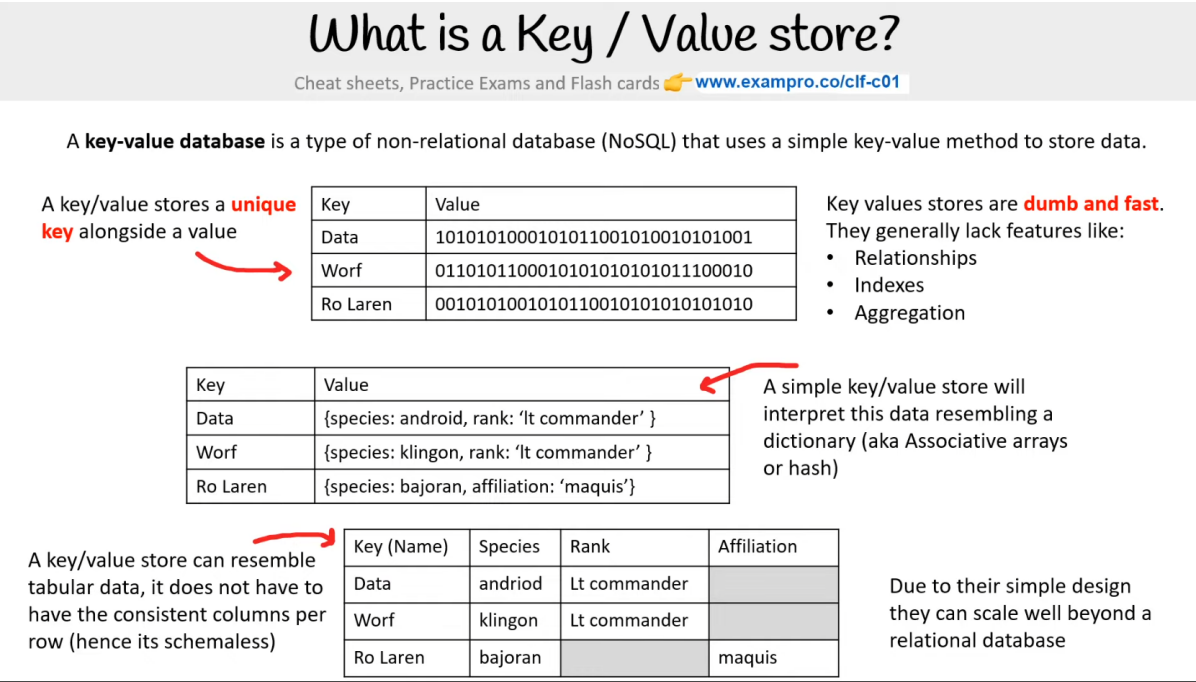
Data warehouses are infrequently accessed meaning they aren't intended for real-time reporting but maybe once or twice a a day or once a week to generate business and user reports.

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

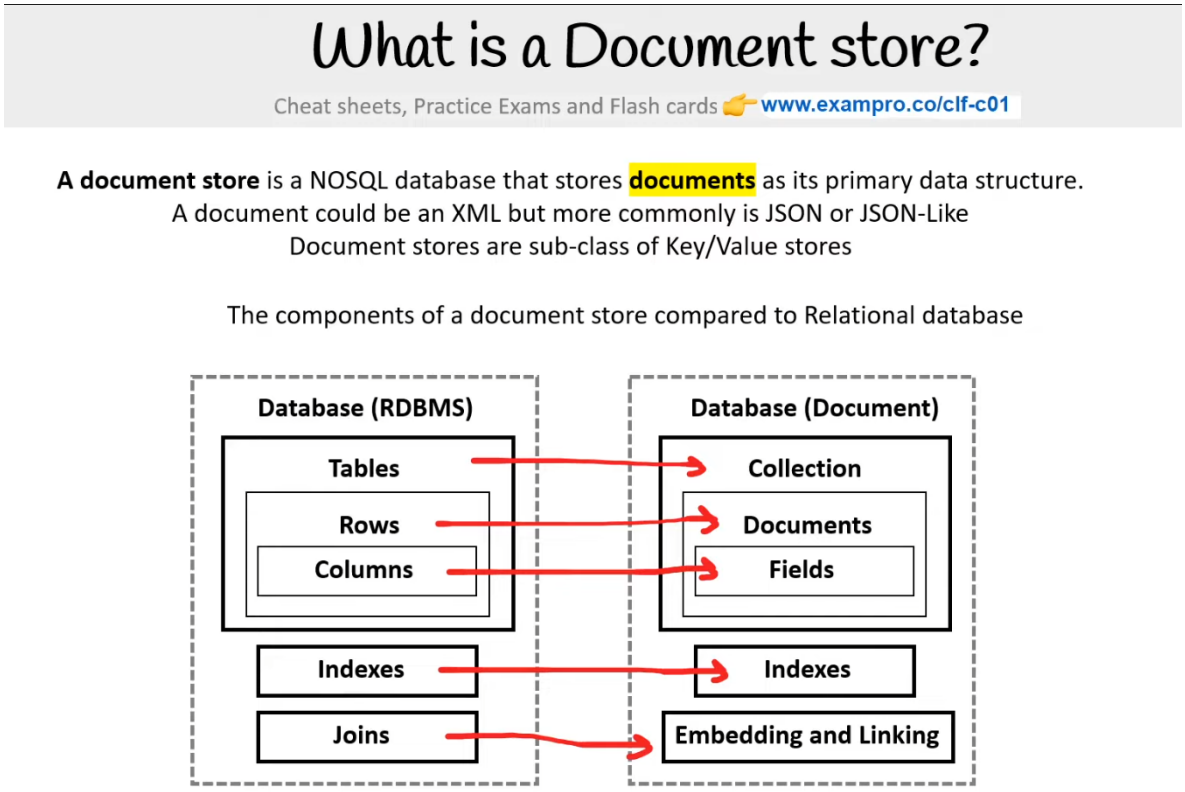


Reference - What is Data Warehouse? Types, Definition & Example

What is a Key / Value store?



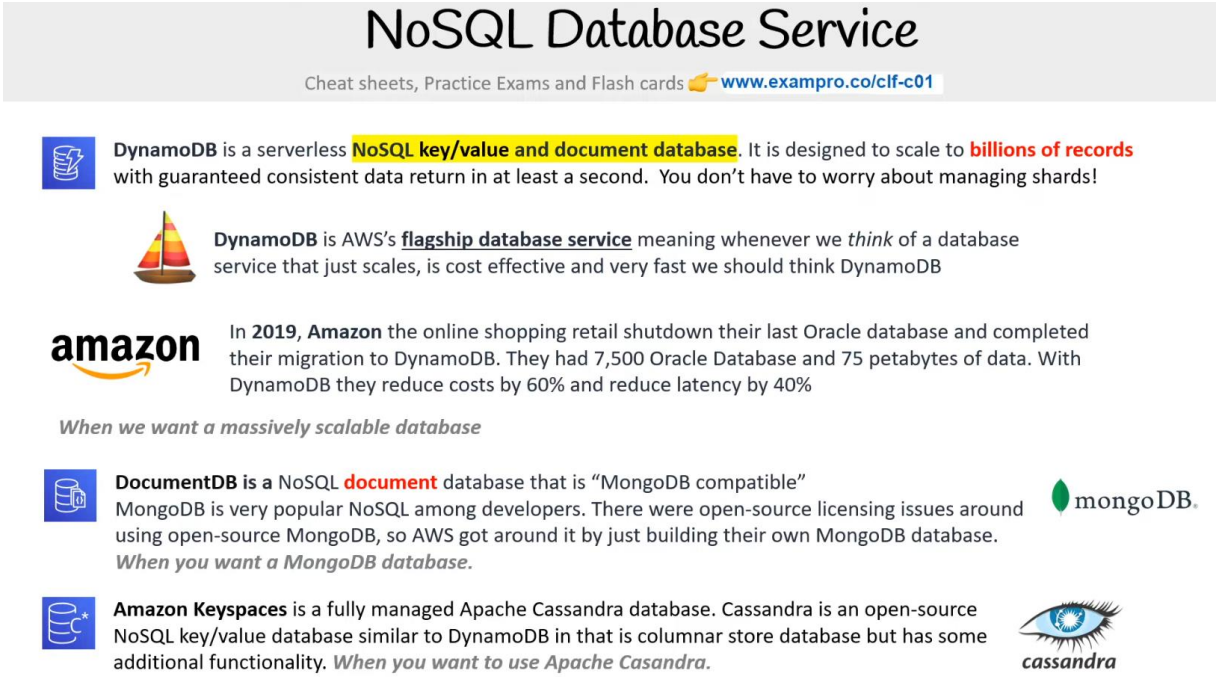
What is a Document store?



A document store is a NoSQL database that stores **documents** as its primary data structure. A document could be an XML but more commonly is JSON or JSON-Like Document stores are a sub-class of Key/Value stores. The components of a document store compared to a Relational database

Reference - Document-oriented database

NoSQL



DynamoDB - is a serverless NoSQL key/value and document database. It is designed to scale to billions of records with guaranteed consistent data return in at least a second. You don't have to worry about managing shards!

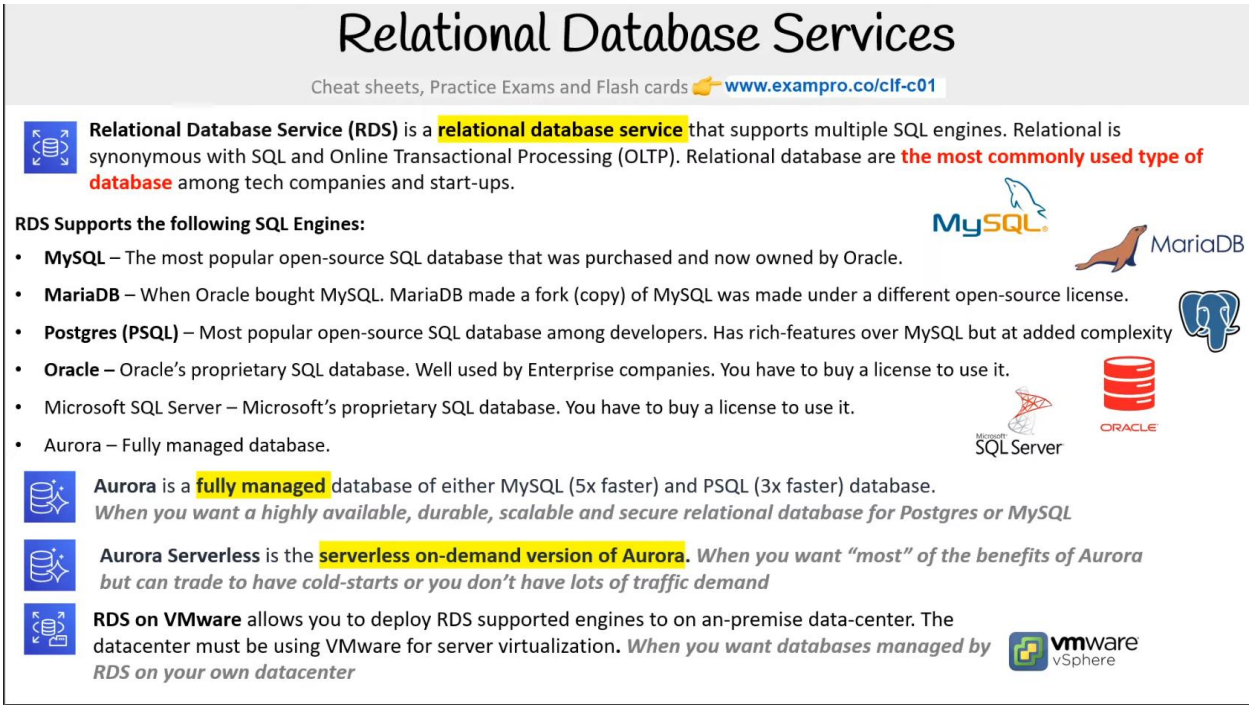
- DynamoDB is AWS's flagship database service meaning whenever we think of a database service that just scales, is cost effective and very fast we should think DynamoDB

DocumentDB - is a NoSQL document database that is "MongoDB compatible"

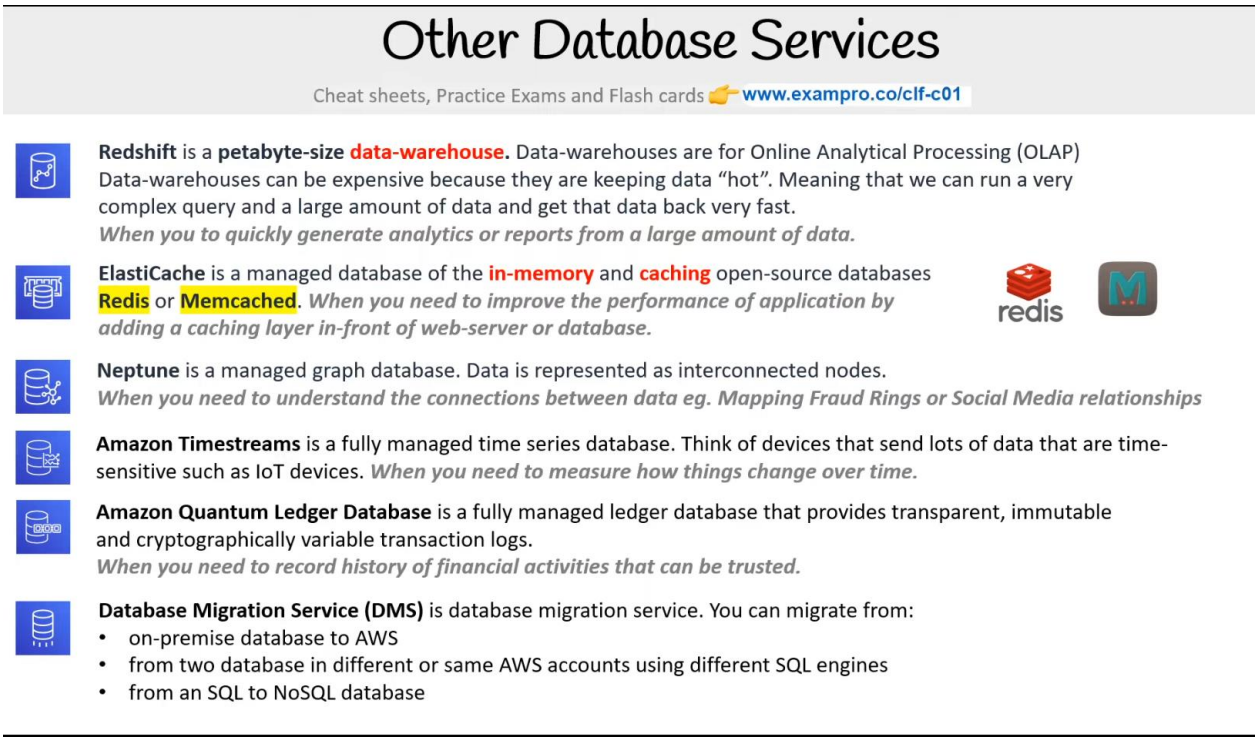
- MongoDB is very popular NoSQL among developers. There were open-source licensing issues around using open-source MongoDB, so AWS got around it by just building their own MongoDB database.

Amazon Keyspaces - is a fully managed Apache Cassandra database. Cassandra is an open-source NoSQL key/value database similar to DynamoDB in that is columnar store database but has some additional functionality. When you want to use Apache Casandra.

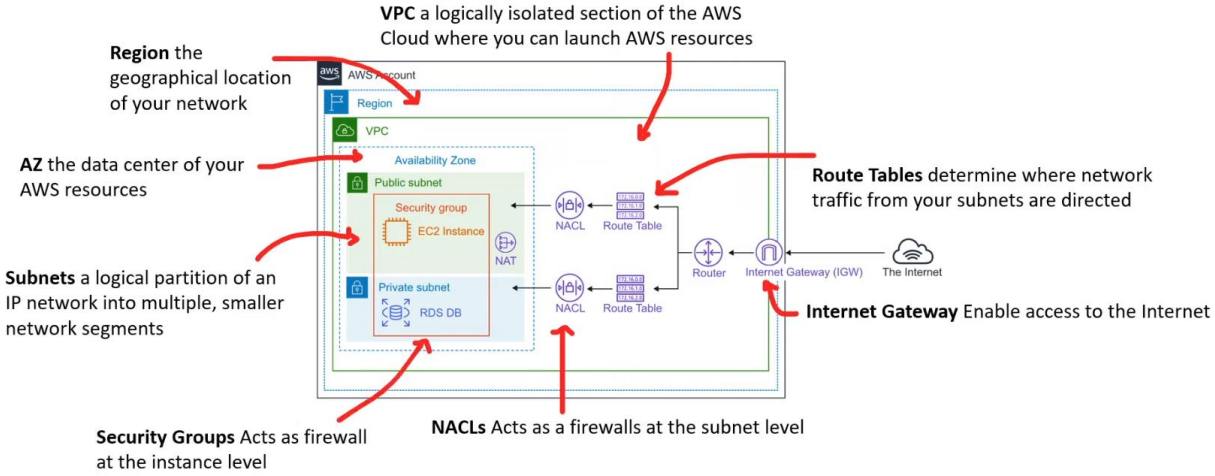
Relational Database Service (RDS)



Other databases



Cloud-Native Networking Services



Key definitions:

Region - the geographical location of your network

Availability Zone (AZ) - a data center containing your AWS resources

Virtual Private Cloud (VPC)- a logically isolated section of the AWS Cloud where you can launch AWS resources

Internet Gateway- enables access to the Internet for your VPC

Route Tables- determines where network traffic from your subnets are directed

NACLs- *Network Access Control Lists.* Act as a firewall at the subnet level

Security Groups- Act as firewall at the instance level

Subnets- a logical partition of an IP network into multiple, smaller network segments

Availability Zones: Availability Zones are the **data centers** where you launch your AWS resources into. Each AZs is associated with a specific region

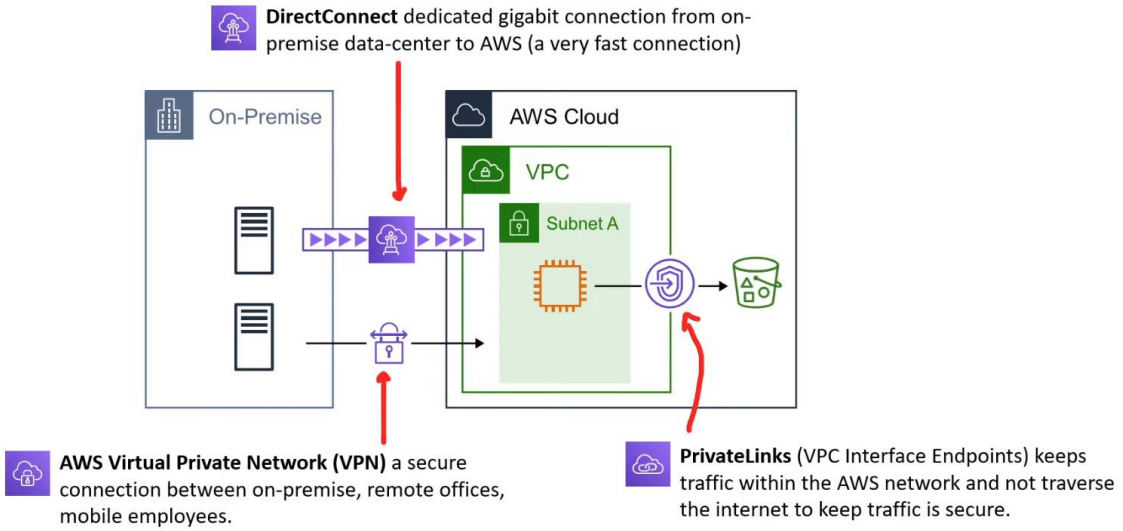
Key VPC Components: A virtual private cloud (VPC) network is your own personal isolated section of the AWS cloud. A route table contains a set of rules (called routes), that are used to determine where network traffic from your subnet or gateway is directed.

Internet Gateway- Allows you to grant internet access to resources inside of your VPC. But you also need a **route table** which routes the traffic from the VPC network out to the IGW

You can think of it as a door from your VPC outward.

Reference - Internetwork traffic privacy in Amazon VPC | VPC networking components

Enterprise/Hybrid Networking Services



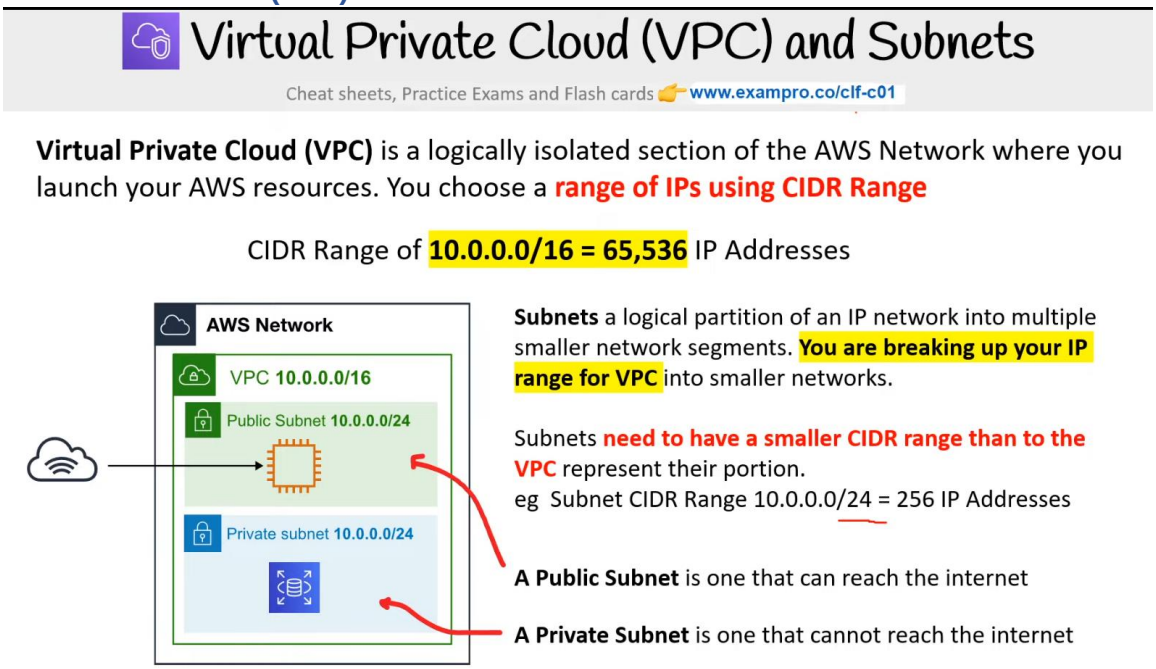
Direct Connect - is a dedicated Gigabit network connection from your premises location to AWS. Provides a direct fiber optic cable running straight to the AWS network

VPN - establishes a secure connection to your AWS network

- Site-to-Site VPN - connecting your on-premise to your AWS network
- Client VPN - connecting a Client (ie users laptop) to your AWS network

PrivateLinks (VPC Interface Endpoints) - keeps traffic within the AWS network and not traverse the internet to keep traffic is secure.

Virtual Private Cloud (VPC) & Subnets

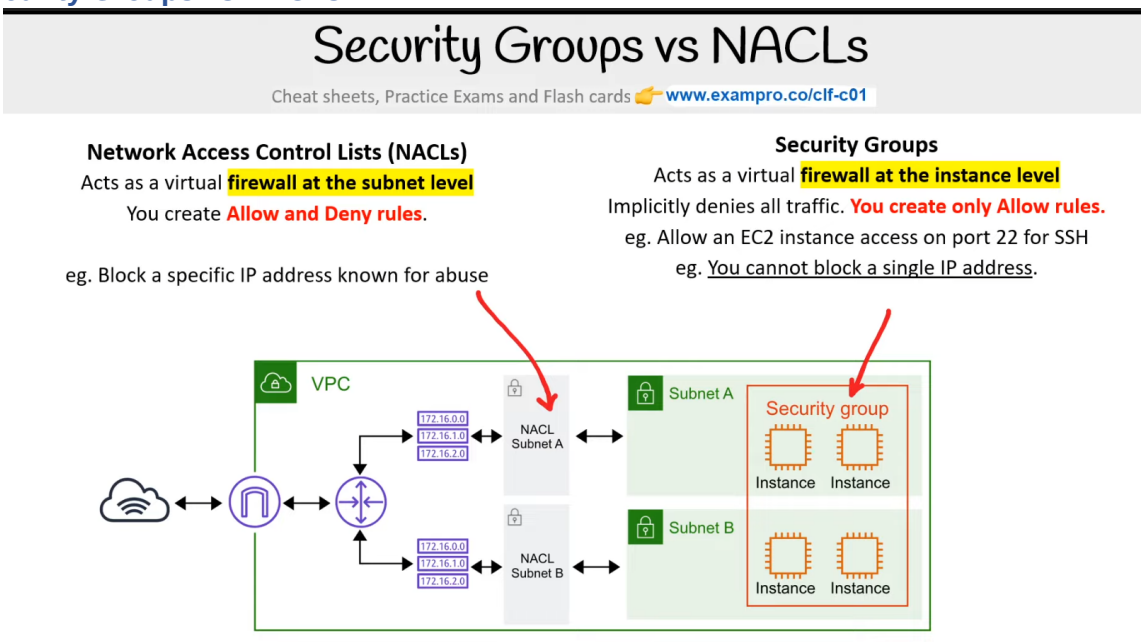


Subnets a logical partition of an IP network into multiple smaller network segments. You are breaking up your IP range for VPC into smaller networks.

- Subnets need to have a smaller CIDR range than to the VPC represent their portion. eg Subnet CIDR Range 10.0.0.0/24 = 256 IP Addresses

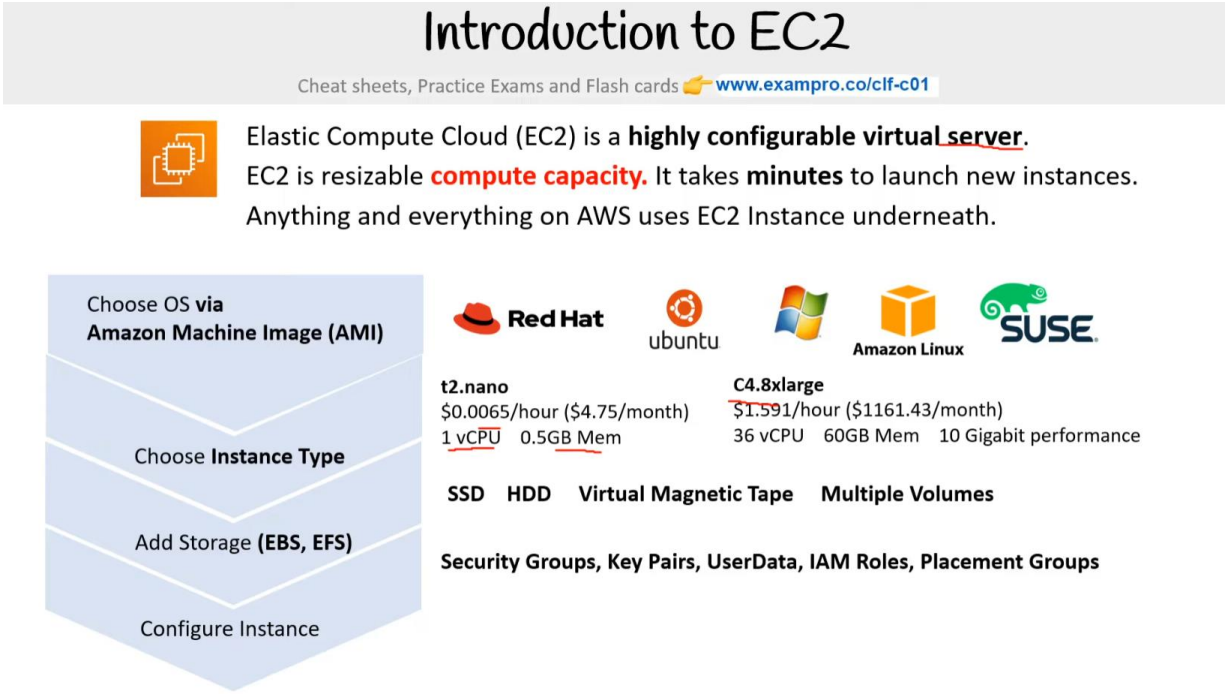
Public vs Private Subnets: - Public subnets are generally used for placing resources which are accessible on the internet. Private subnets are used when you need resources to be more secured and only accessible through tightly filtered traffic into the subnet

Security Groups vs NACLs

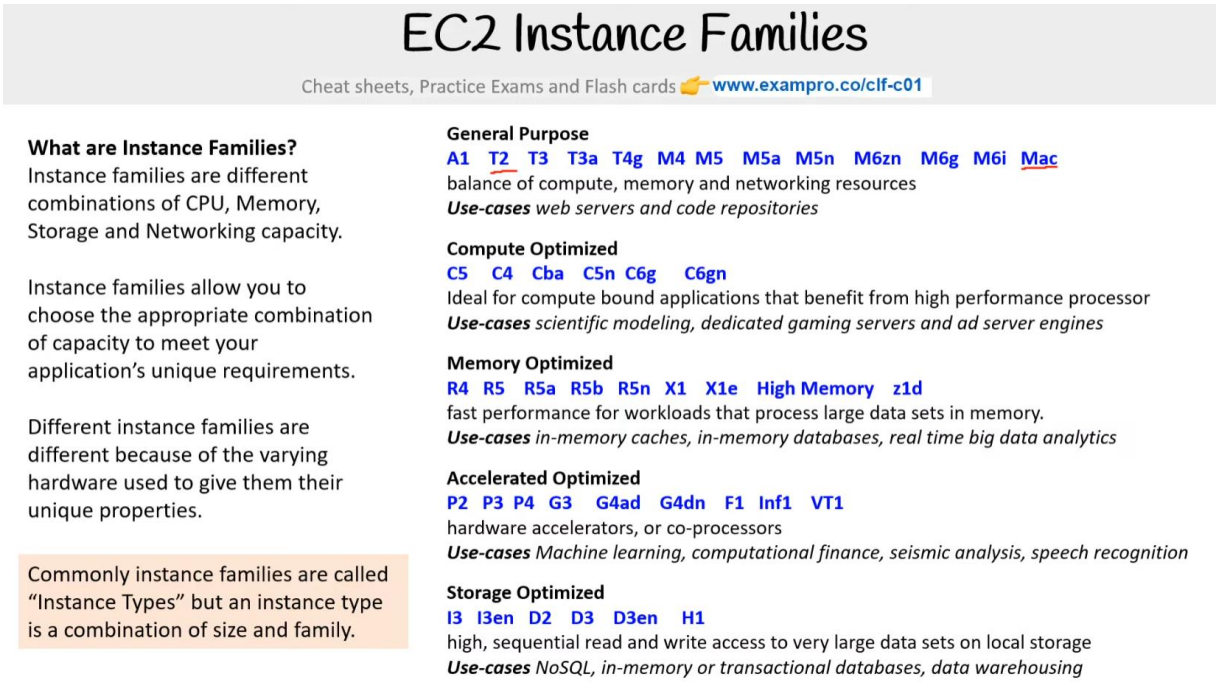


Reference- [Security groups for your VPC]

Introduction to EC2



EC2 Instance Families



Reference - [Amazon EC2 Instance Types]

EC2 Instance Types

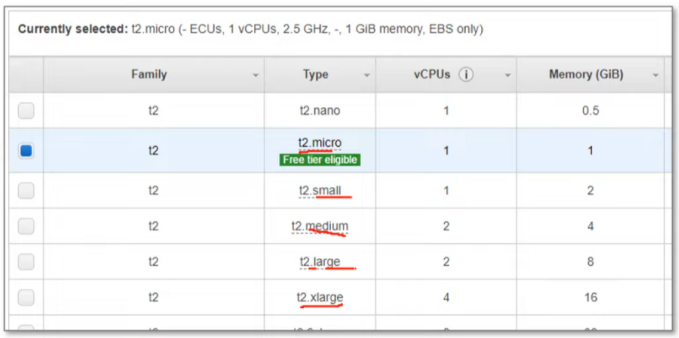
EC2 Instance Types

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

An instance type is a particular **instance size and instance family**:

A common pattern for instance sizes:

- nano
- micro
- small
- medium
- large
- xlarge
- 2xlarge
- 4xlarge
- 8xlarge
- ....



There are many exceptions to this pattern for sizes e.g.

- c6g.metal – is a bare metal machine.
- C5.9xlarge – Is not a power of 2 or even number size

EC2 – Dedicated Host

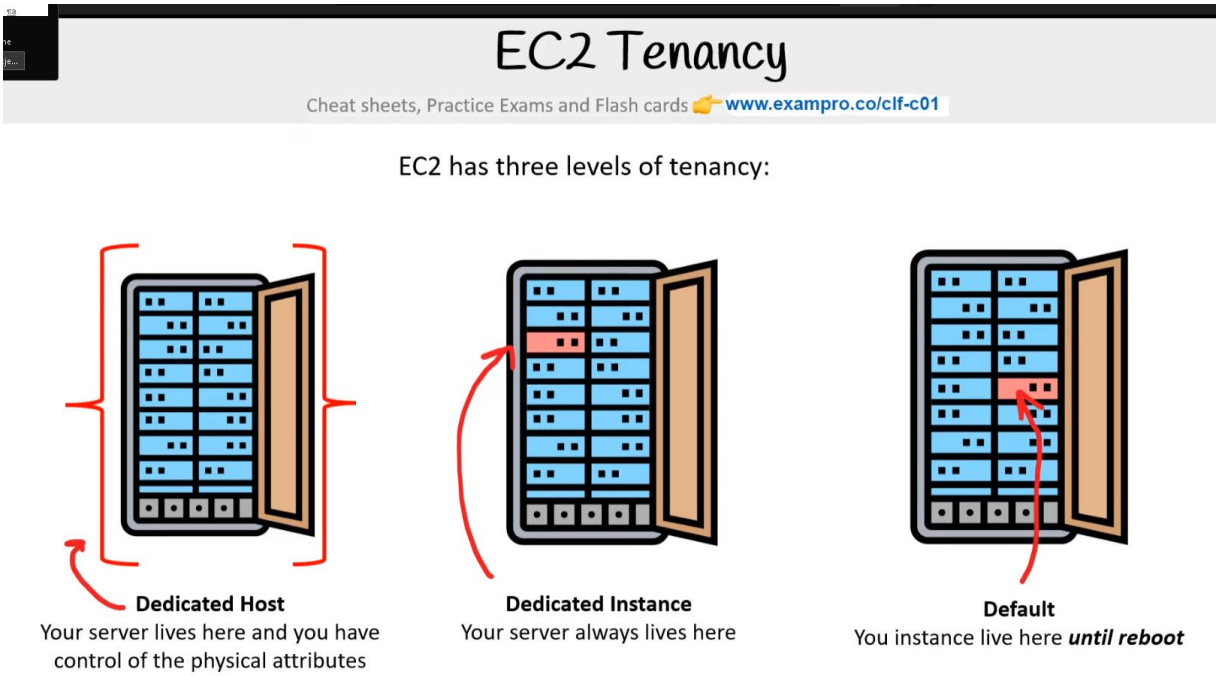
EC2 – Dedicated Host

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

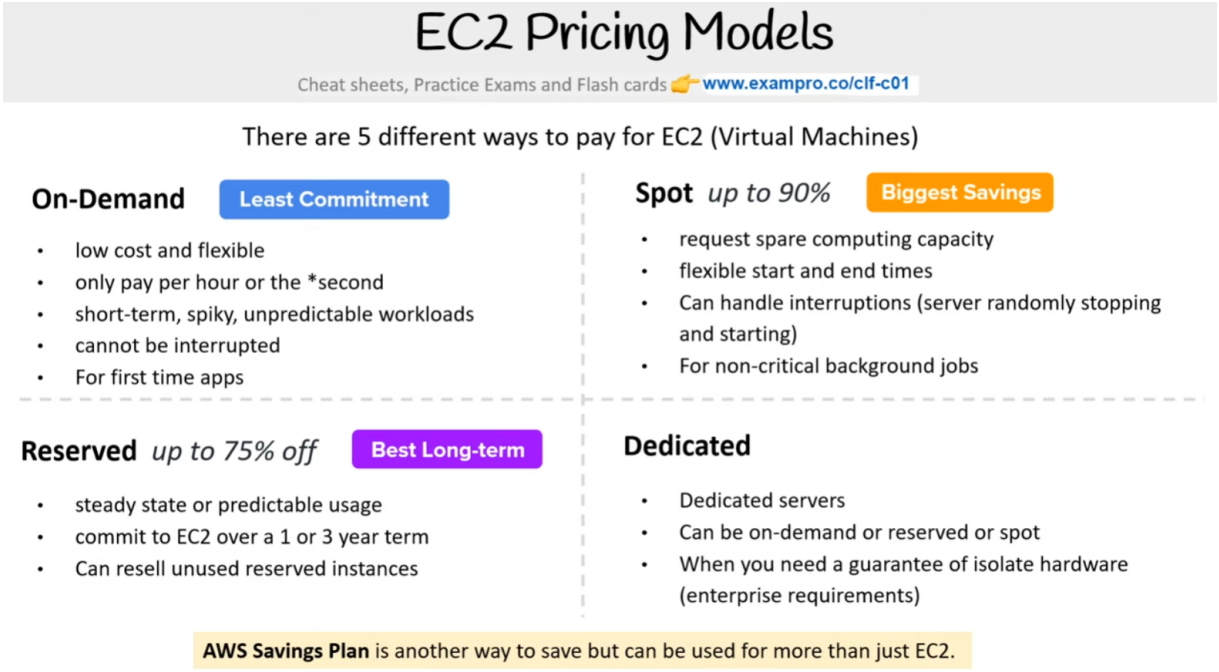
Dedicated Hosts are single-tenant EC2 instances designed to let you Bring-Your-Own-License (BYOL) based on **machine characteristics**

	Dedicated Instance	Dedicated Hosts
Isolation	Instance Isolation	Physical Server Isolation
Billing	Per instance billing (+$2 per region fee)	Per host billing
Visibility of Physical characteristics	No Visibilities	**Sockets, cores, host ID**
Affinity between a host and instance	No Affinity	Consistency deploy to the same instances to the same physical server
Targeted instance placement	No control	Additional control over instance placement on physical server
Automatic instance placement	Yes	Yes
Add capacity using an allocation request	No	Yes

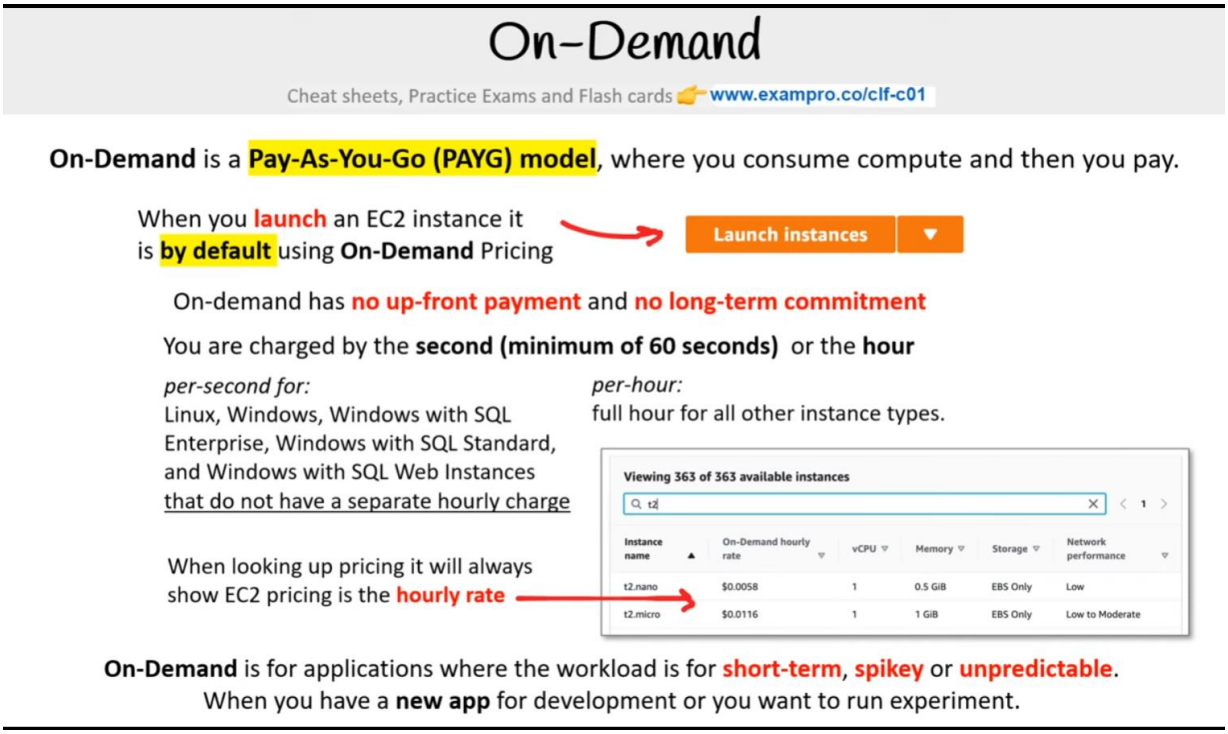
EC2 Tenancy



EC2 - Pricing Model



On Demand



On-Demand is a Pay-As-You-Go (PAYG) model, where you consume compute and then you pay.. When you launch an EC2 instance it is by default On-Demand Pricing

Key Points:

- On-Demand has no up-front payment and no long-term commitment
- You are charged by the **hour** or by the **minute** (varies based on EC2 Instance Types

per-second for:

- Linux, Windows, Windows with SQL Enterprise, Windows with SQL Standard, and Windows with SQL Web Instances that do not have a separate hourly charge

per-hour:

- full hour for all other instance types.

When looking up pricing it will always show EC2 pricing is the hourly rate

- On-Demand is for applications where the workload is for **short-term, spikey,** or **unpredictable.**
- Used for when you have a **new app** for development or you want to run an experiment

Reference - Amazon EC2 On-Demand Pricing

New – Per-Second Billing for EC2 Instances and EBS Volumes

On-Demand Instances

EC2- Reserved Instances (RI)

Reserved Instances (RI)

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

Designed for applications that have a **steady-state**, **predictable usage**, or require **reserved capacity**.
Reduced Pricing is based on **Term** x **Class Offering** x **RI Attributes** x **Payment Option**

Term — The longer the term the greater savings.

You commit to a **1 Year** or **3 Year** contract.
Reserved Instances do not renew automatically

When the expire your instance will use On-Demand with no interruption to service

Class — The less flexible the greater the savings

Standard Up to **75%** reduced pricing compared to on-demand. You can modify **RI Attributes.**

Convertible Up to **54%** reduced pricing compared to on-demand. You can exchange RI based on **RI Attributes** if greater or equal in value.

~~**Scheduled**~~ AWS no longer offers Scheduled RI

Payment Options — The greater upfront the great the savings

All Upfront
Full payment is made at the start of the term

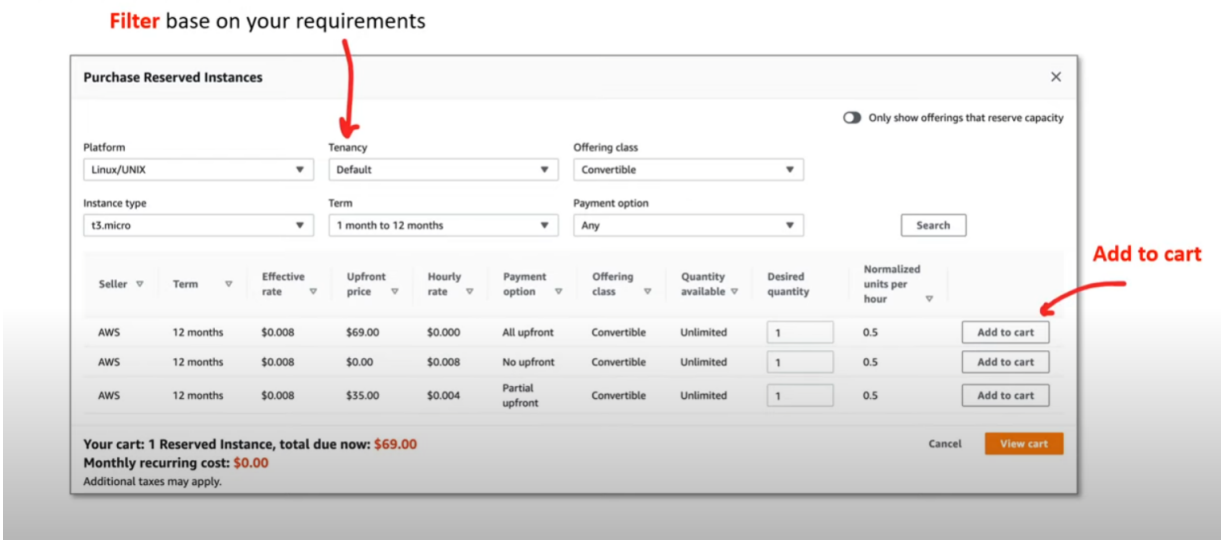
Partial Upfront
A portion of the cost must be paid upfront and the remaining hours in the term are billed at a discounted hourly rate

No Upfront
You are billed a discounted hourly rate for every hour within the term, regardless of whether the Reserved Instance is being used

RIs can be **shared between multiple accounts within an AWS Organization**

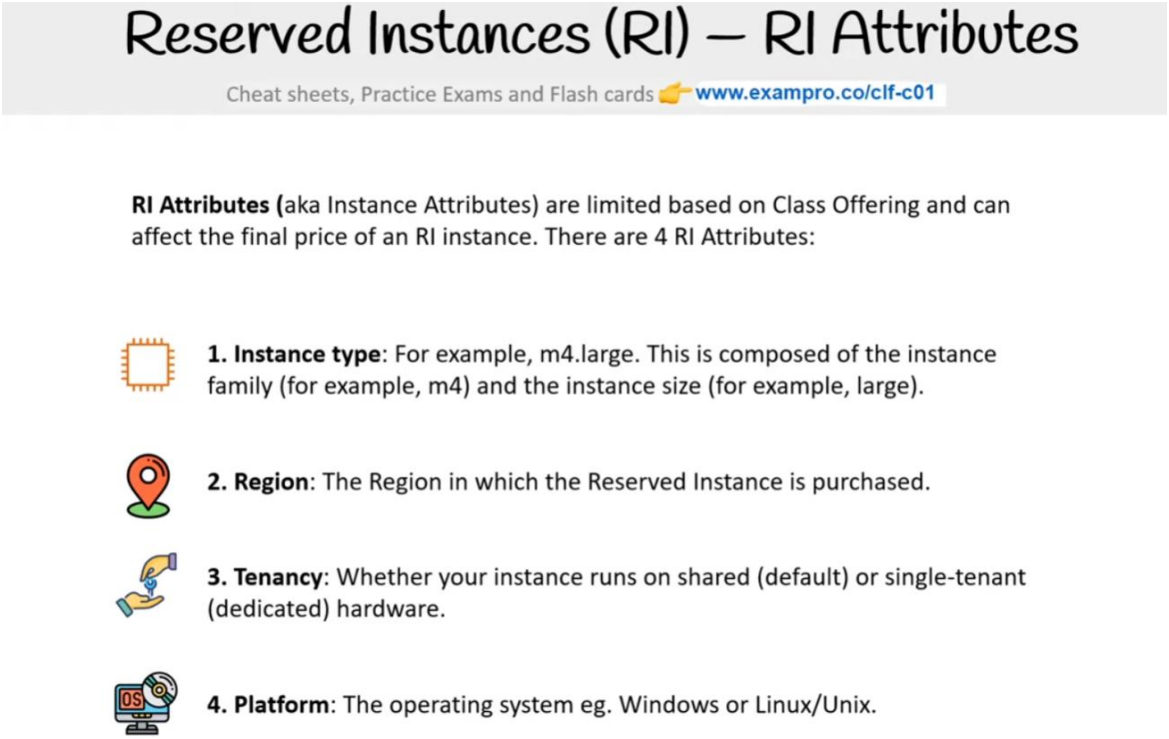
Reserved Instances (RI)

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

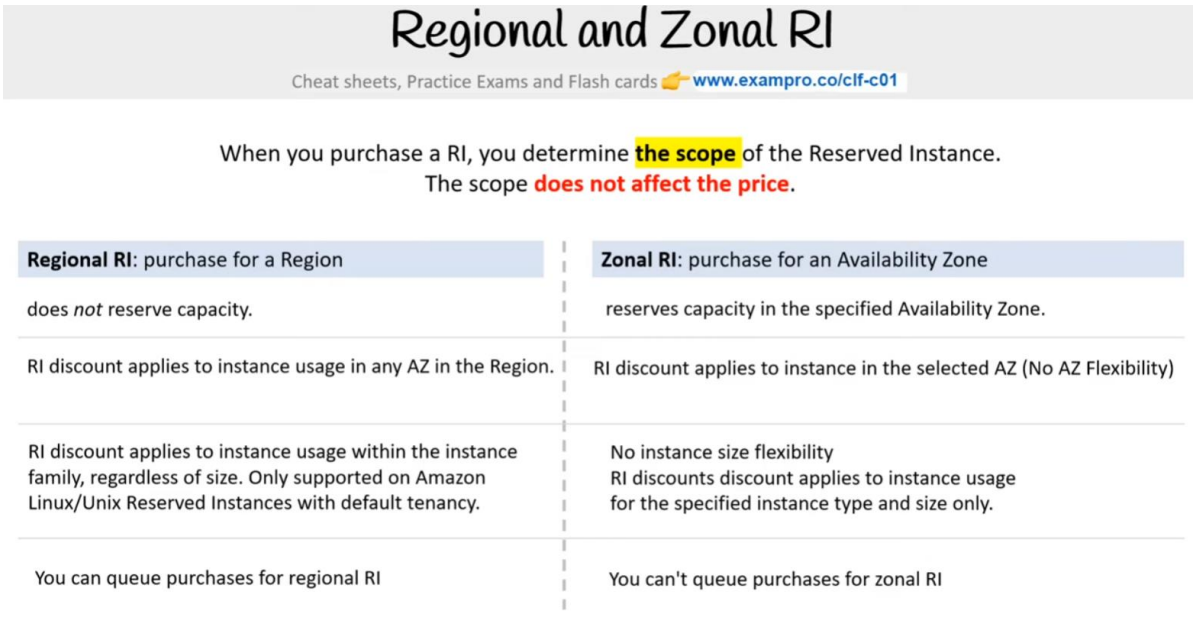


Reference - [Amazon EC2 Reserved Instances | Types of Reserved Instances (offering classes)]

Reserved Instances (RI) — RI Attributes

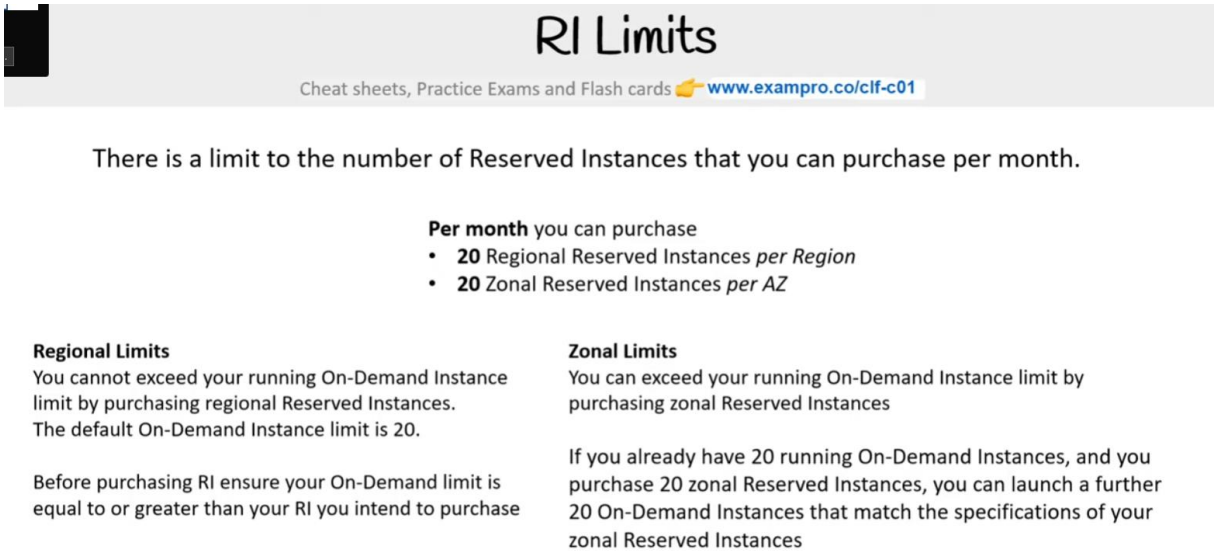


Regional and Zonal RI



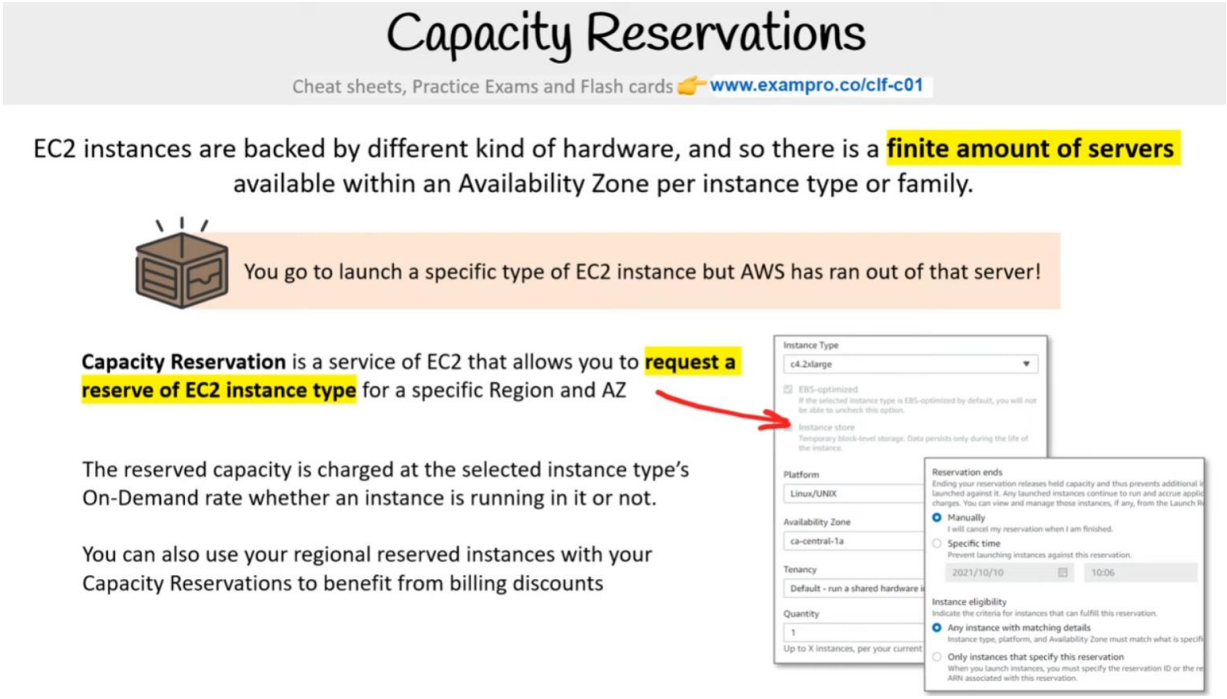
Reference - Regional and zonal Reserved Instances (scope) | Work with Capacity Reservations

RI Limits



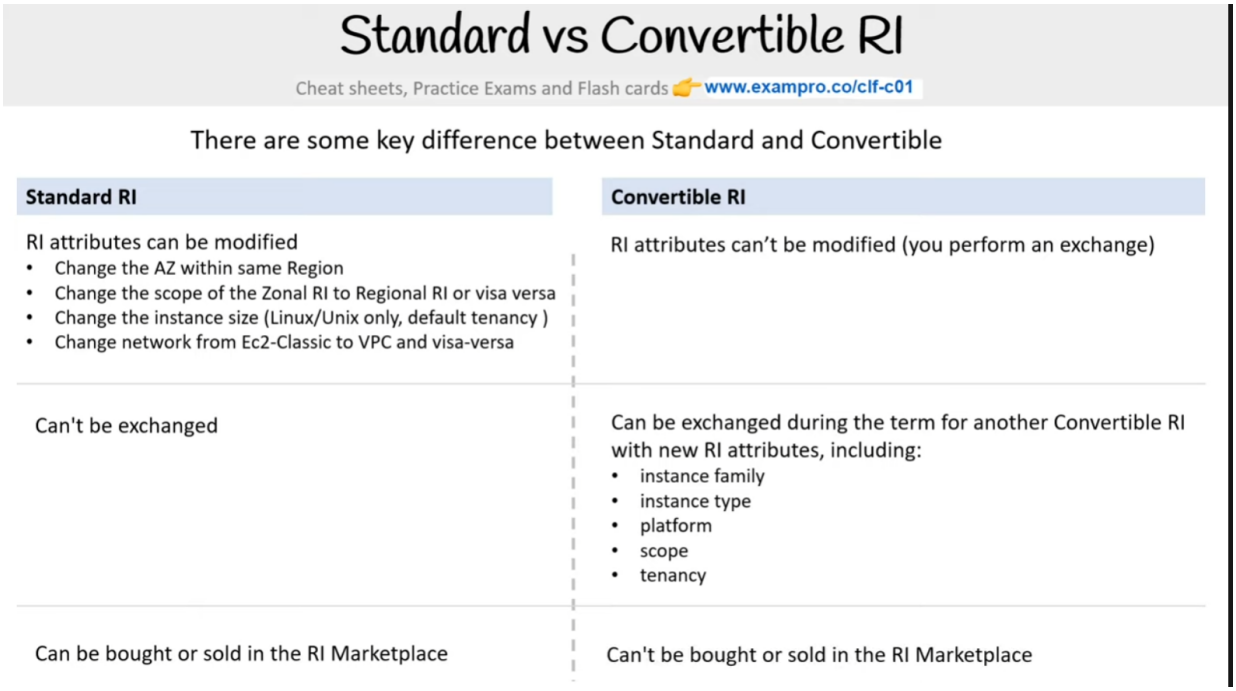
Reference - Reserved Instances

Capacity Reservations



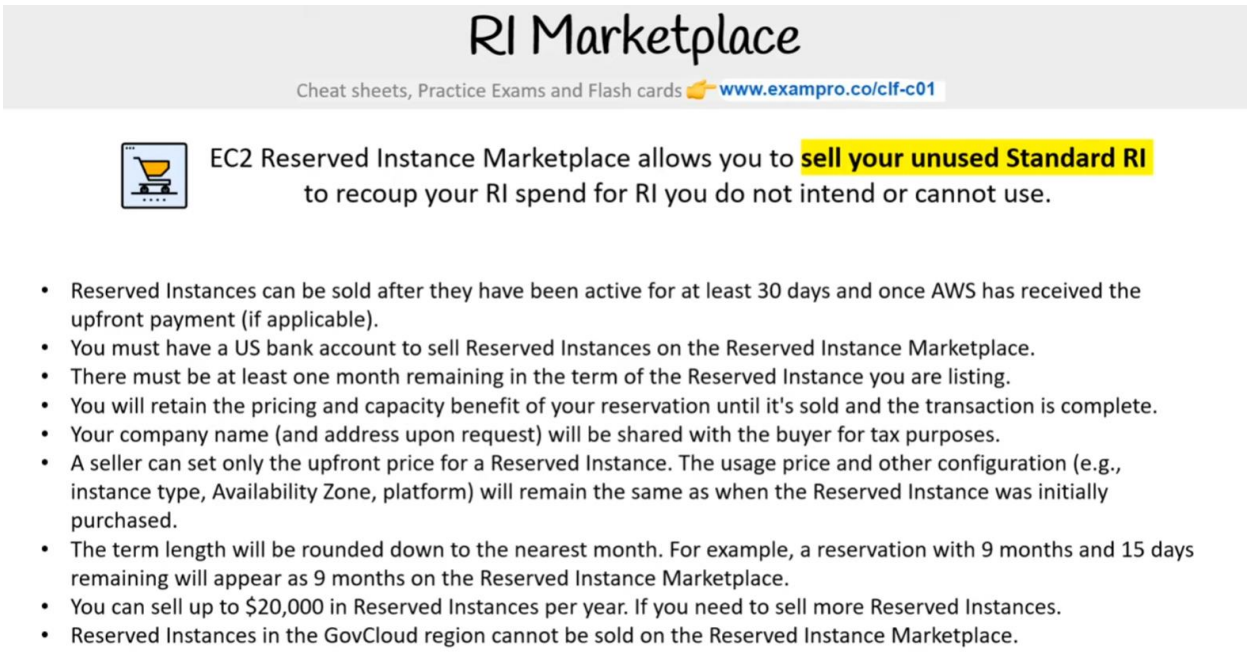
Reference- Work with Capacity Reservations

Standard vs Convertible RI

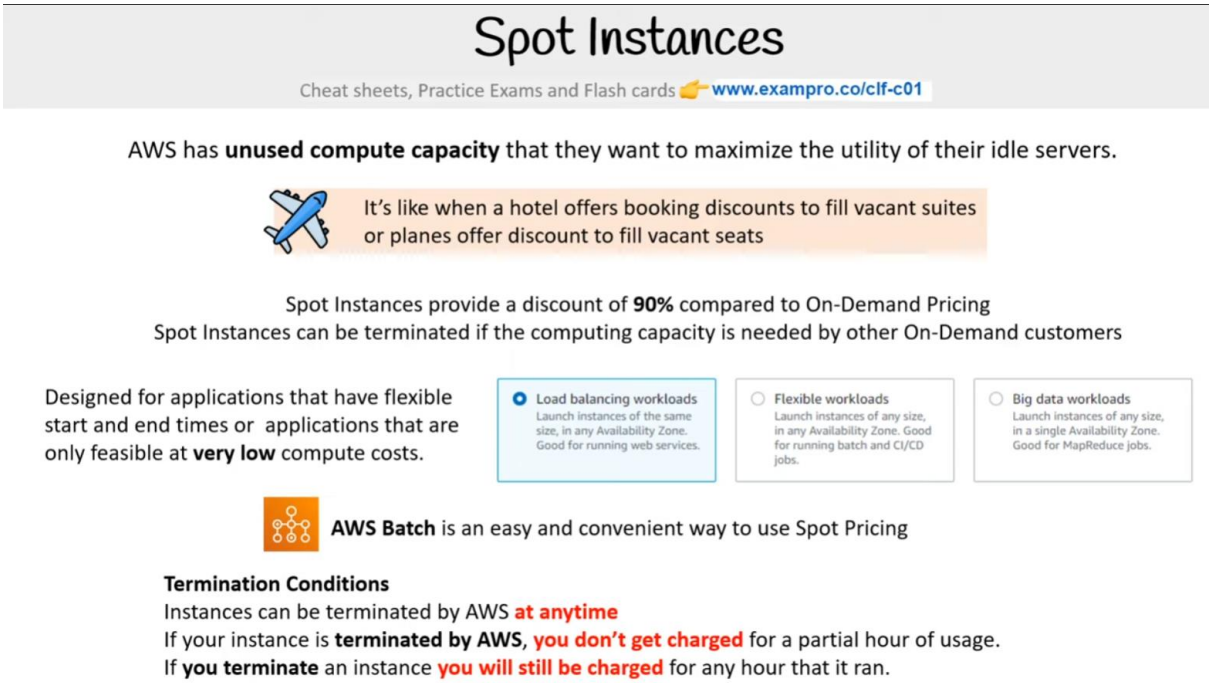


Reference - [Types of Reserved Instances (offering classes)](#) | [Modify Reserved Instances](#)

RI Marketplace



Spot Instances



AWS has unused compute capacity that they want to maximize the utility of their idle servers. It's like when a hotel offers booking discounts to fill vacant suites or planes offer discounts to fill vacant seats

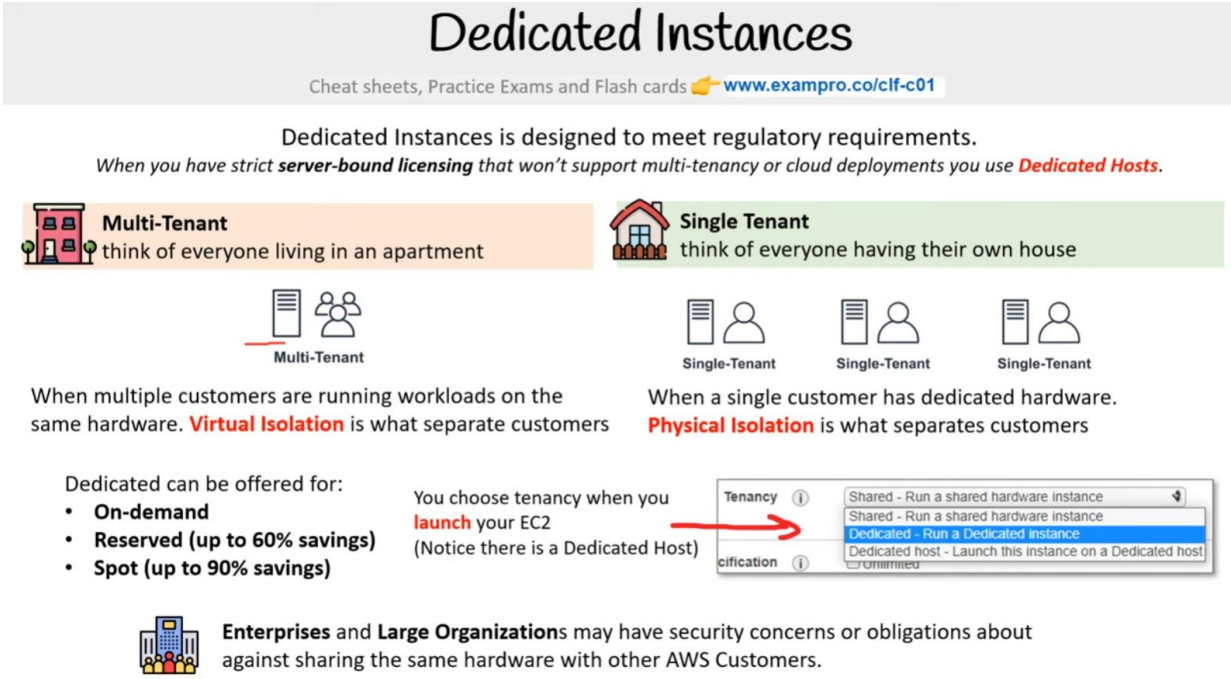
Amazon EC2 Spot Instances provide a discount of 90% compared to On-Demand Pricing. Spot Instances can be terminated if the computing capacity is needed by other On-Demand customers. Amazon EC2 Spot Instances let you take advantage of **unused EC2 capacity** in the AWS cloud.. Designed for applications that have flexible start and end times or applications that are only feasible at **very low** compute costs.

AWS Batch is an easy and convenient way to use Spot Pricing

Termination Conditions:

- Instances can be terminated by AWS **at any time.**
- If your instance is terminated by AWS, **you don't get charged** for a partial hour of usage.
- If you terminate an instance **you will still be charged** for an hour that it ran.

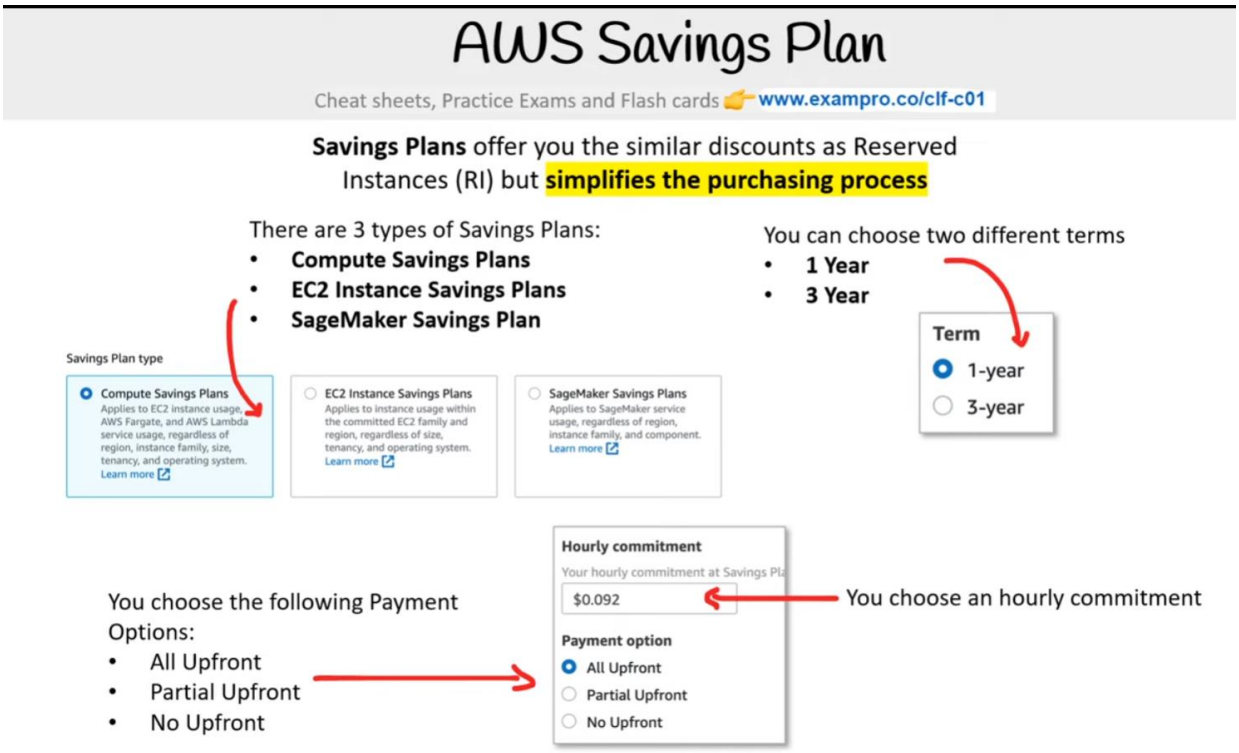
Dedicated Host Instances



Dedicated Host Instances are designed to meet regulatory requirements. When you have strict server-bound licensing that won't support multi-tenancy or cloud deployments you use Dedicated Hosts.

Reference - Amazon EC2 Dedicated Instances

AWS Savings Plan



AWS Savings Plan

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

AWS Savings Plan has 3 different savings types:

Compute
Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage, AWS Fargate, and AWS Lambda service usage regardless of instance family, size, AZ, region, OS, or tenancy.

EC2 Instances
provide the lowest prices, offering savings up to 72% in exchange for commitment to usage of individual instance families in a region.
automatically reduces your cost on the selected instance family in that region regardless of AZ, size, OS or tenancy.
give you the flexibility to change your usage between instances within a family in that region.

SageMaker
Helps you reduce SageMaker costs by up to 64%.
automatically apply to SageMaker usage regardless of instance family, size, component, or AWS region.

Reference - Savings Plans | New – Savings Plans for AWS Compute Services

The Ultimate Guide To Reserved Instance And AWS Savings Plan

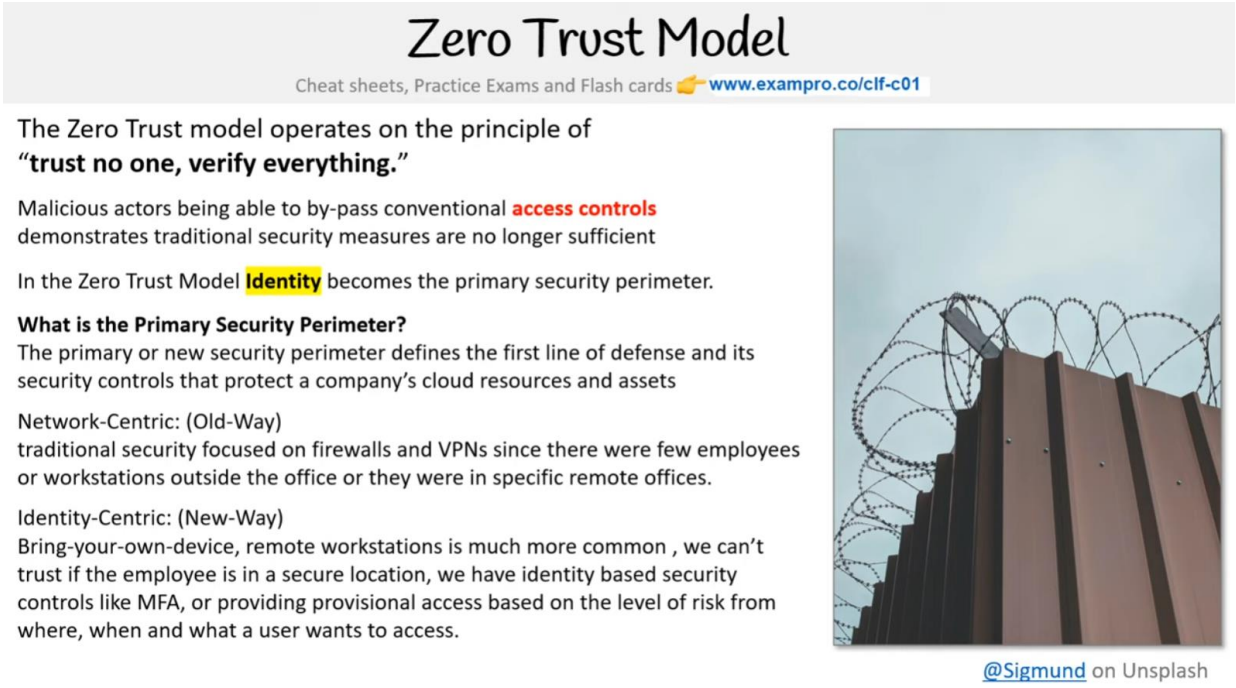
Cheat Sheet

- **EC2 has 4 pricing models**
    0. On-Demand
    1. Spot
    2. Reserved Instances (RI)
    3. Dedicated
- **On-Demand** (Least commitment)
    0. Low cost and flexible
    1. Only pay per hour
    2. Use Case: short-term, spiky, unpredictable workloads, and first time apps
    3. Ideal when your workloads cannot be interrupted.
- **Reserved Instances**- up to 75% off (Best long-term value)
    0. **Use case:** steady state or predictable usage
    1. Can resell unused reserved instances (Reserved Instance Marketplace)
    2. Reduced Pricing is based on **Term x Class Offering x Payment Option**
    3. **Payment Terms:** 1 year or 3 years
    4. **Payment Options:** All Upfront, Partial Upfront, No Upfront
    5. **Class Offerings:**
        - Standard: Up to 75% reduced pricing compared to on-demand. Cannot change RI attributes
        - Convertible: Up to 54% reduced pricing compared to on-demand. Allows you to change RI Attributes if greater than or equal in value.
        - Scheduled: You reserve instances for specific times periods. Savings vary.
- **Spot Pricing**- up to 90% off (Biggest Savings)
    0. Request spare computing capacity
    1. Flexible start and end times
    2. **Use case:** Can handle interruptions like a server randomly stopping and starting

3. **Use case:** For non-critical background jobs
4. Instances can be terminated by AWS **at anytime**
5. If your instance is **terminated by AWS**, you don't get charged for a partial hour of usage.
6. If **you terminate** an instance you will still be charged for any hour that it ran.

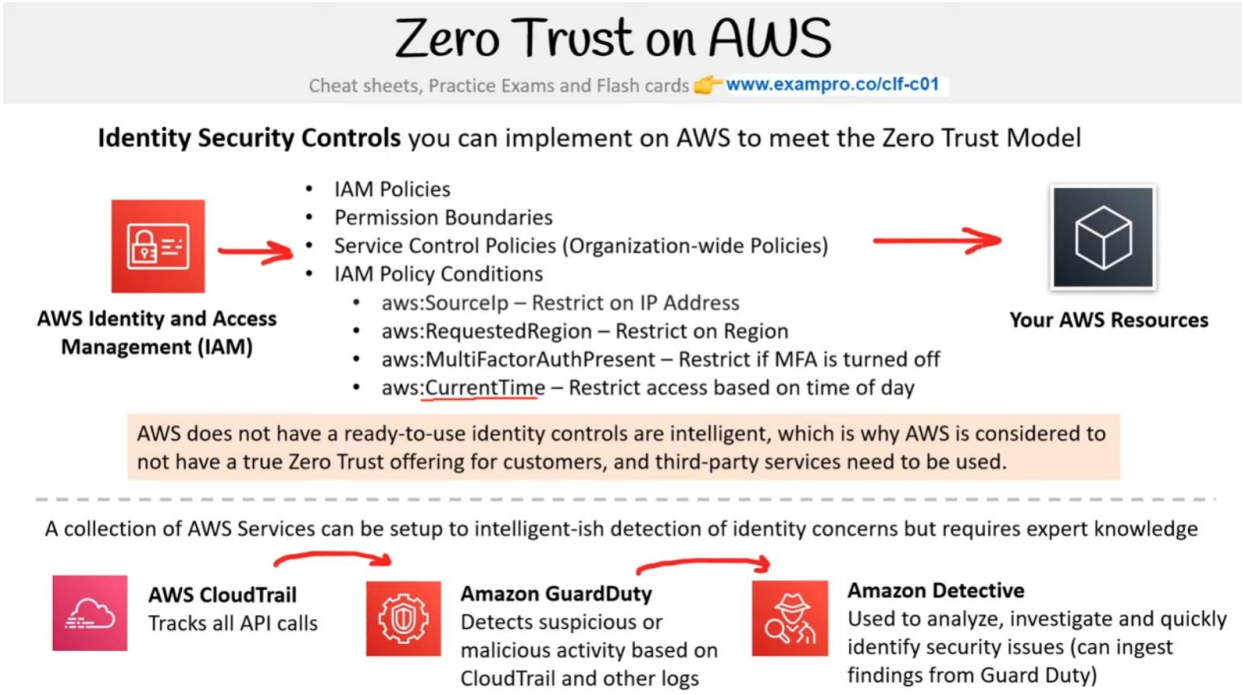
- **Dedicated Hosting** (Most Expensive)
    0. Dedicated servers
    1. Can be on-demand or reserved (up to 70% off)
    2. **Use case**: When you need a guarantee of isolated hardware (enterprise requirements)

Zero Trust Model



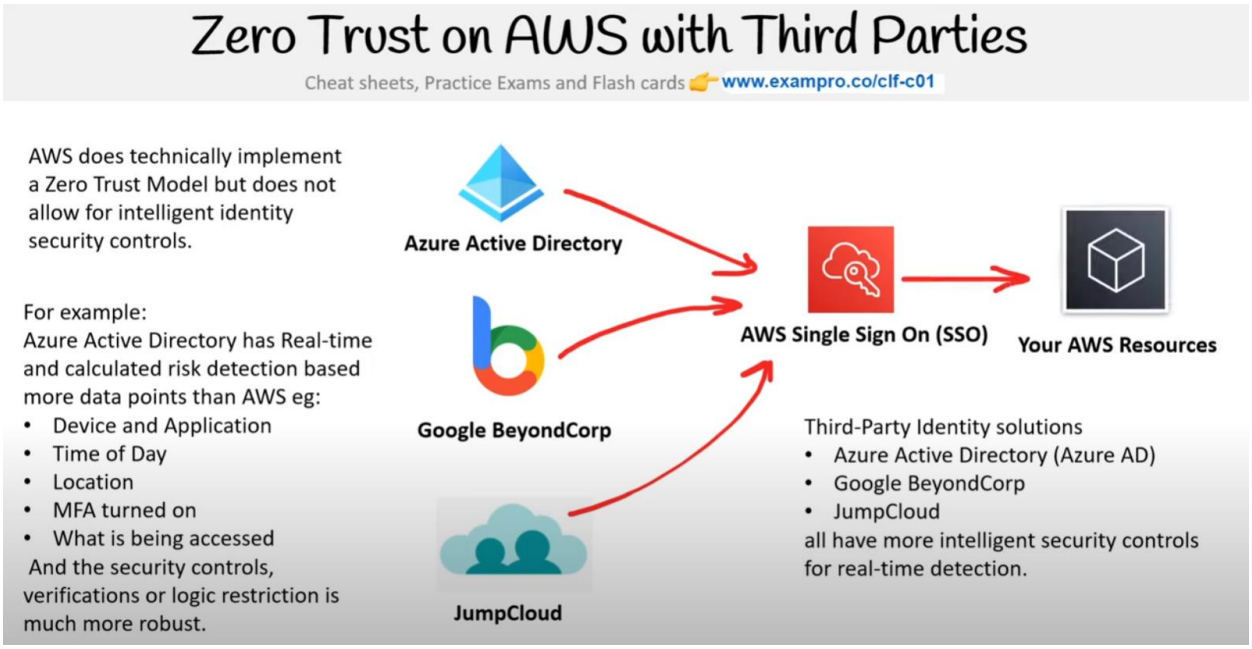
Reference - Zero Trust on AWS

Zero Trust on AWS



Reference - [Zero Trust on AWS](#) | [AWS re:Invent 2020: Zero Trust: An AWS perspective](#)

Zero Trust on AWS with Third Parties



Directory Service

Directory Service

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

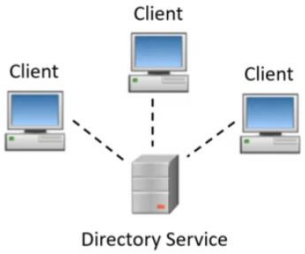
What is a directory service?
A directory service maps the **names of network resources to their network addresses.**

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

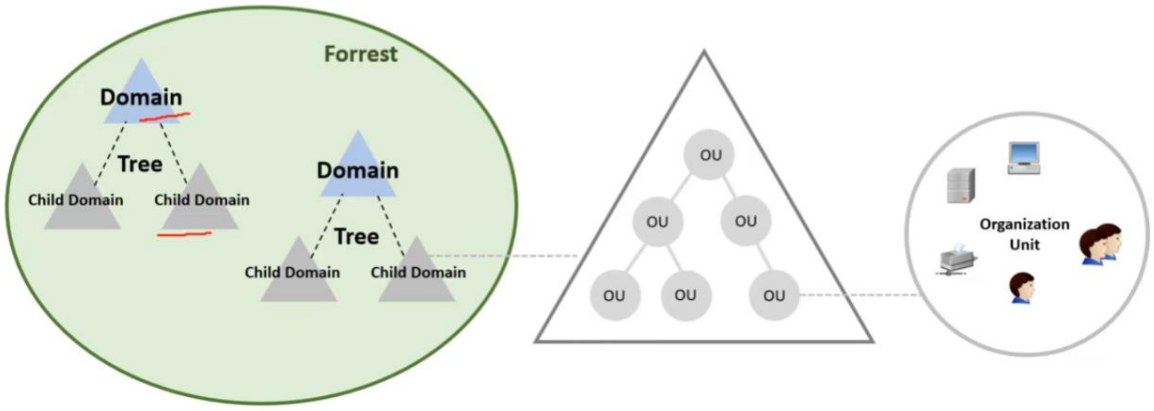
Reference - About Google Cloud Directory Sync

Active Directory

Active Directory

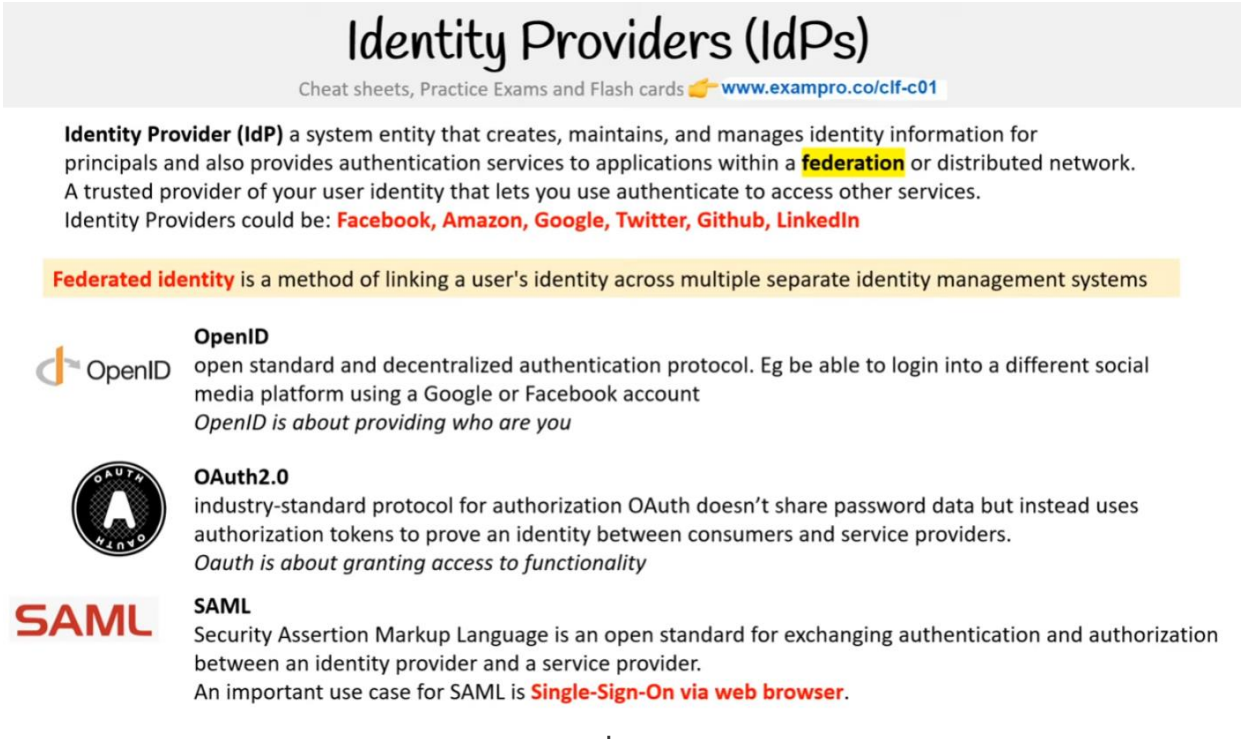
Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Microsoft introduced **Active Directory** Domain Services in **Windows 2000** to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.



Reference - The Difference Between Active Directory and LDAP

Identity Providers (IdP)

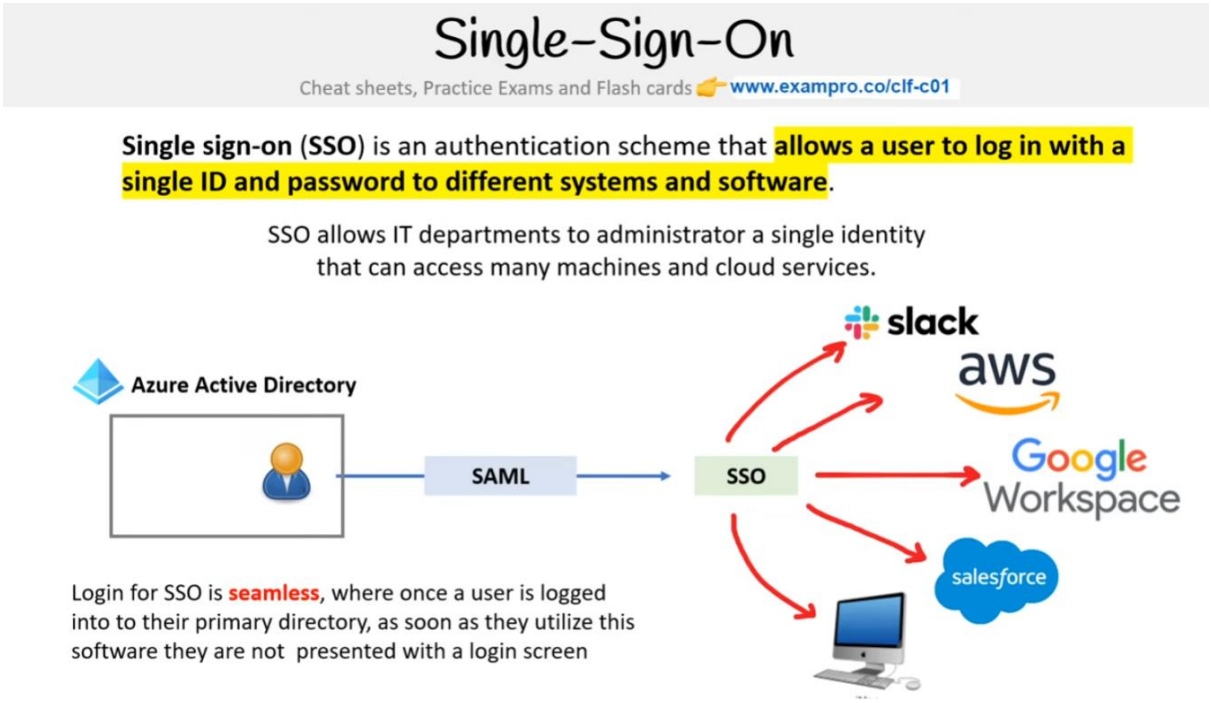


References - Identity provider | Oauth | Identity provider (SAML)

What's the Difference Between OAuth, OpenID Connect, and SAML?

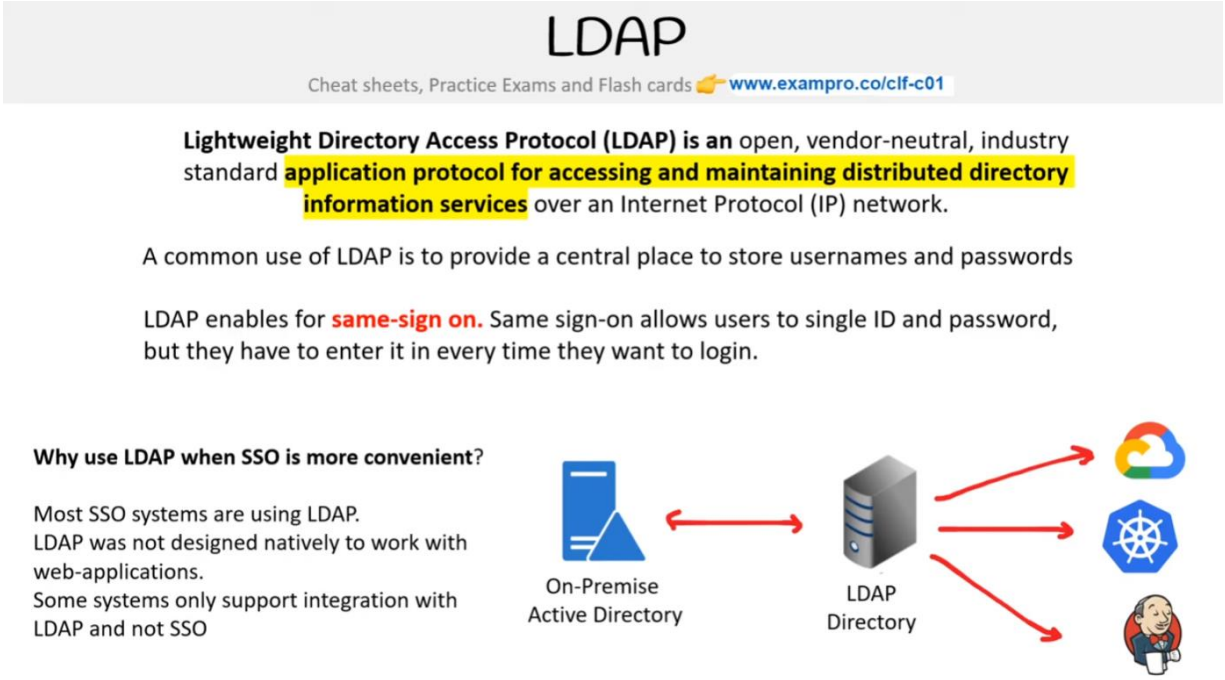
What's the difference between OpenID and OAuth?

Single-Sign-On



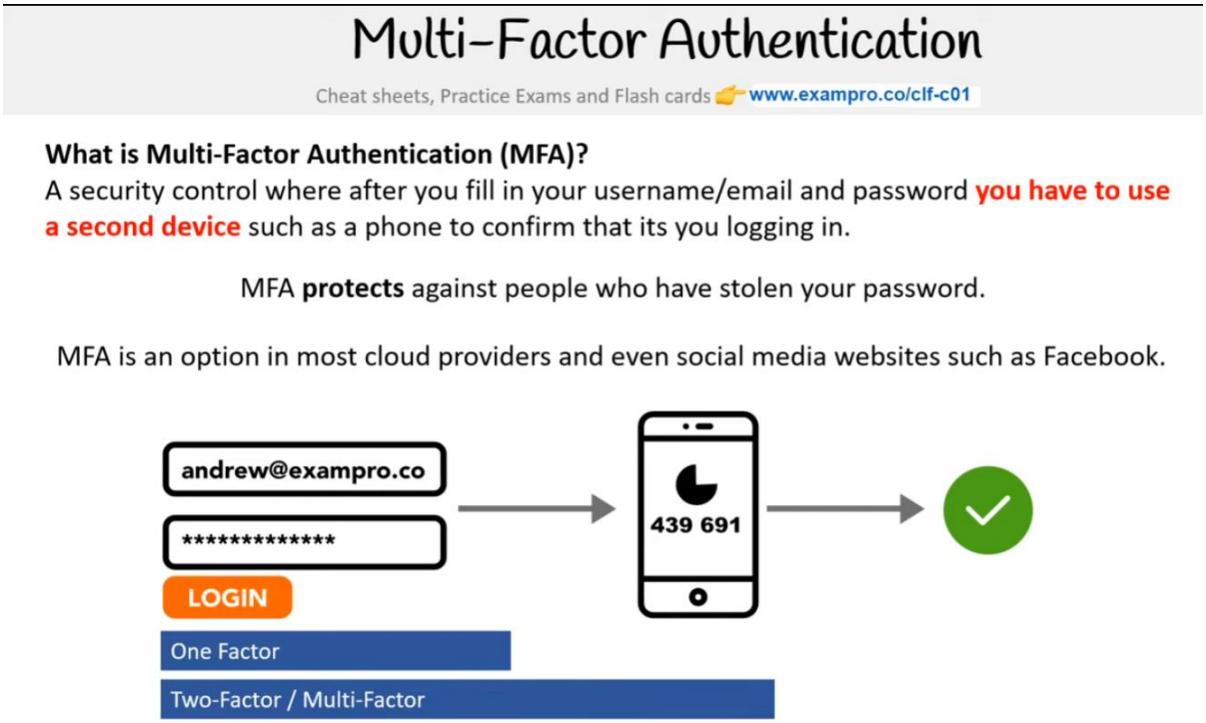
Reference - About Google Cloud Directory Sync

LDAP

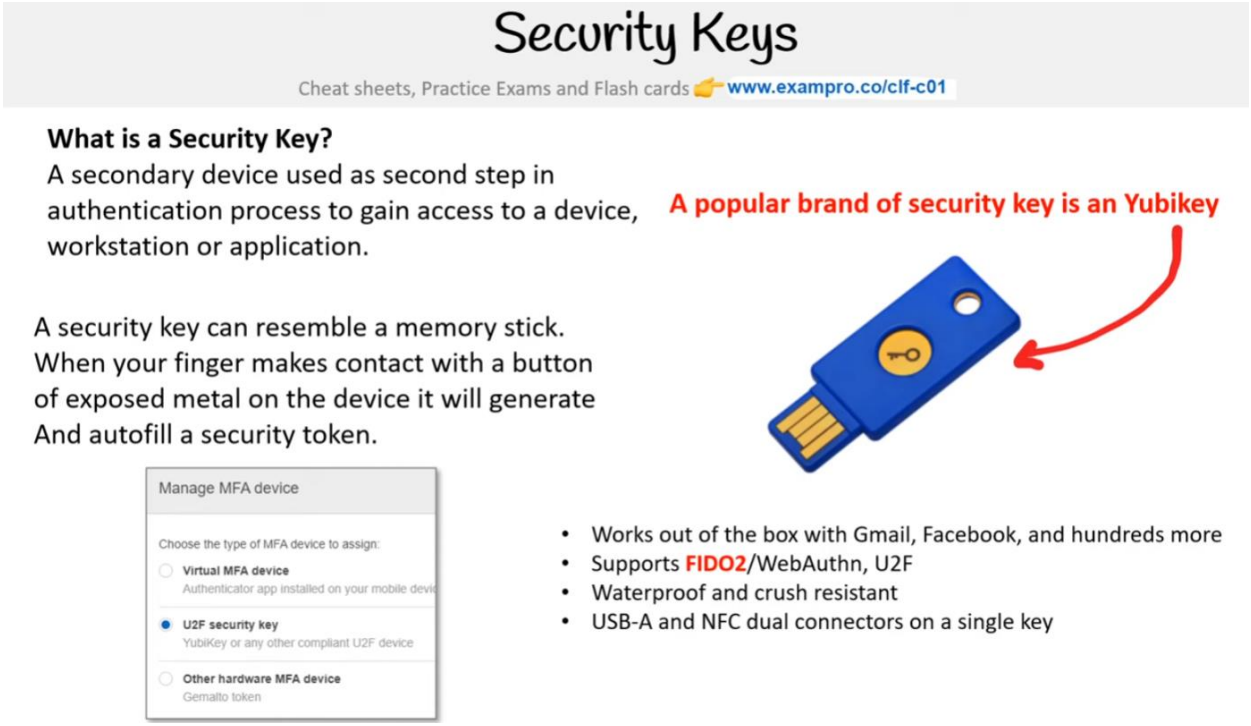


Reference - Office 365: Single Sign-on vs. Same Sign-on | What Is LDAP & How Does It Work? | Difference Between SSO and LDAP | SAML SSO vs. LDAP — Which Protocol Is Right for You?

Multi-Factor Authentication

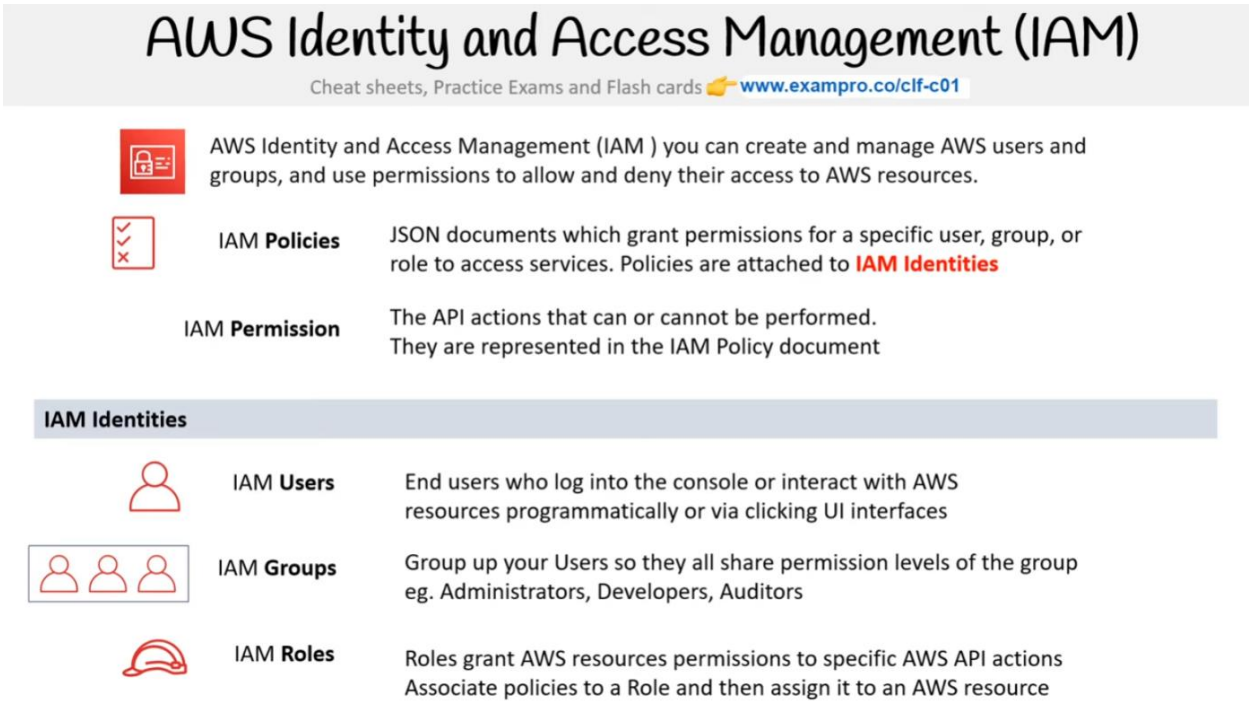


Security Keys



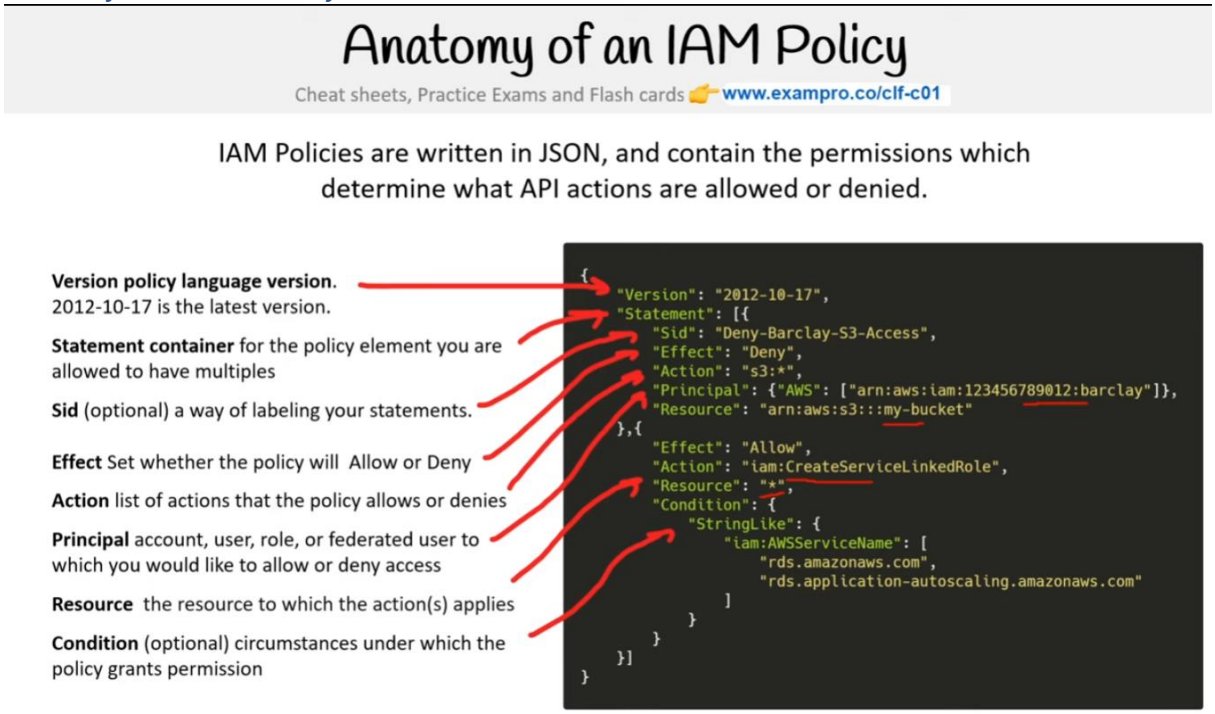
Reference - Alliance Overview - FIDO Alliance Specifications Overview

AWS Identity and Access Management (IAM)

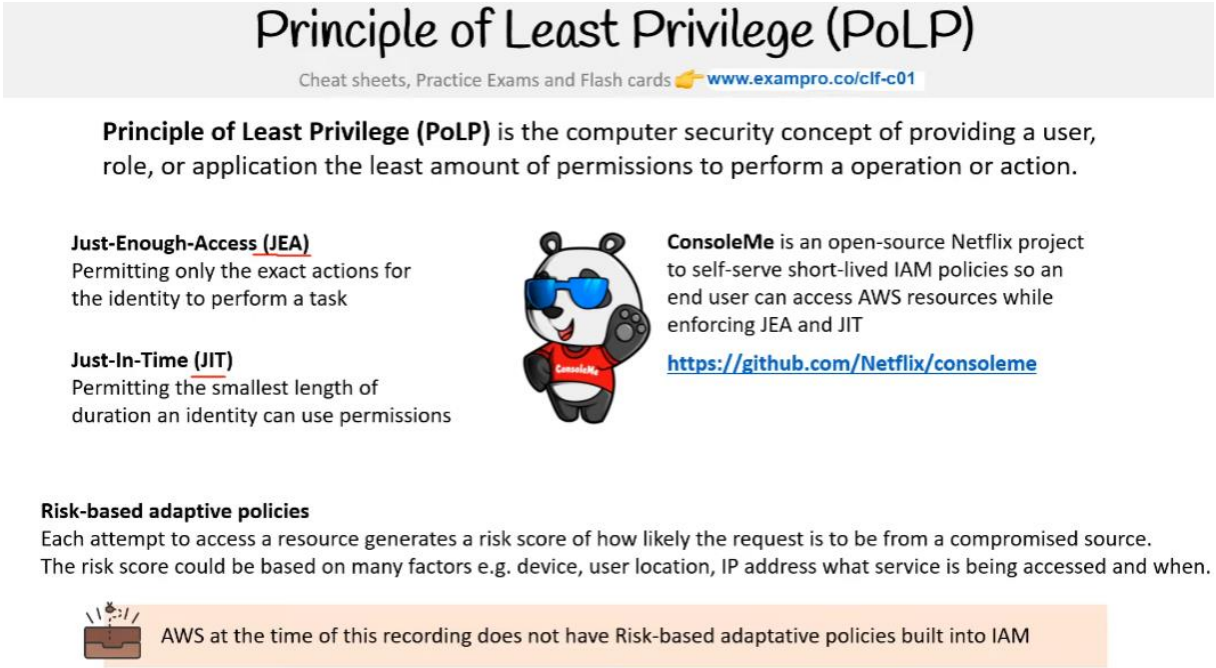


Reference - https://aws.amazon.com/iam/

Anatomy of an IAM Policy



Principle of Least Privilege (PoLP)



Principle of Least Privilege (PoLP) is the computer security concept of providing a user, role, or application the least amount of permissions to perform an operation or action.

Just-Enough-Access (JEA)

Permitting only the exact actions for the identity to perform a task

Just-In-Time (JIT)

Permitting the smallest length of duration an identity can use permissions

ConsoleMe is an open-source Netflix project to self-serve short-lived IAM policies so an end-user can access AWS resources while enforcing JEA and JIT

https://github.com/Netflix/consoleme

Risk-based adaptive policies

Each attempt to access a resource generates a risk score of how likely the request is to be from a compromised source. The risk score could be based on many factors e.g. device, user location, IP address what service is being accessed, and when.

AWS at the time of this recording does not have Risk-based adaptative policies built into IAM

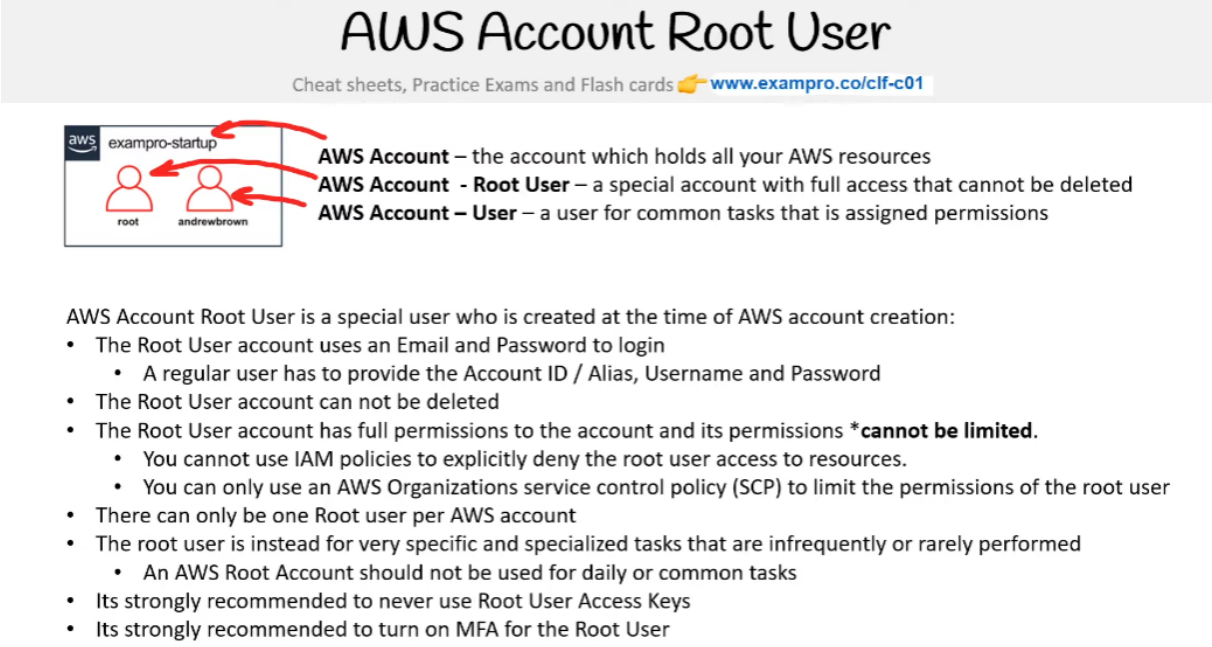
Reference

Principle of least privilege

Using adaptive authentication

ConsoleMe: A Central Control Plane for AWS Permissions and Access

AWS Account Root User



AWS Account Root User is a special user who is created at the time of AWS account creation:

- The Root User account uses an Email and Password to login
  - A regular user has to provide the Account ID / Alias, Username and Password
- The Root User account can not be deleted
- The Root User account has full permissions to the account and its permissions ***cannot be limited**.
  - You cannot use IAM policies to explicitly deny the root user access to resources.
  - You can only use an AWS Organizations service control policy (SCP) to limit the permissions of the root user
- There can only be one Root user per AWS account
- The root user is instead for very specific and specialized tasks that are infrequently or rarely performed
  - An AWS Root Account should not be used for daily or common tasks
- Its strongly recommended to never use Root User Access Keys
- Its strongly recommended to turn on MFA for the 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.

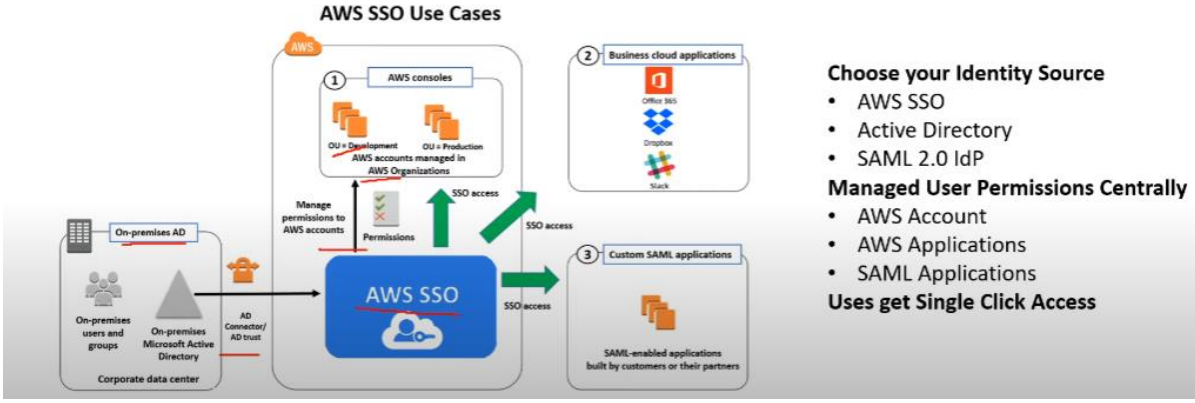
Reference - AWS account root user

AWS Single-Sign On

AWS Single-Sign On

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

AWS Single Sign-On (AWS SSO) is where you create, or connect, your workforce identities in AWS **once** and manage access centrally across your AWS organization.



Reference - Introducing AWS Single Sign-On - AWS Single Sign-On

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

Queueing

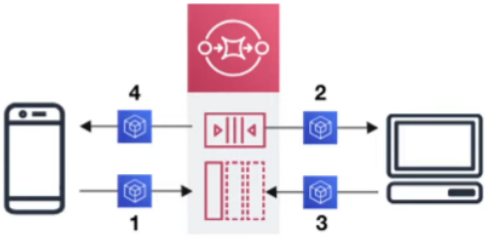
Queueing

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.

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.

Pub/Sub

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.

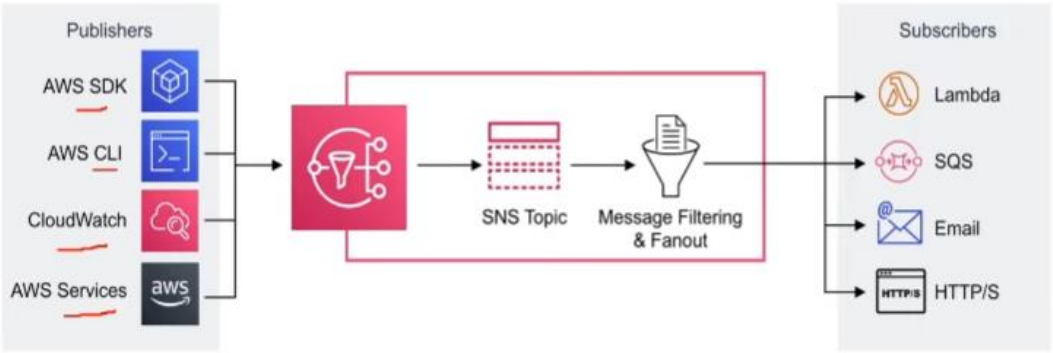
Use Case: a real-time chat system. A web-hook system

- 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.



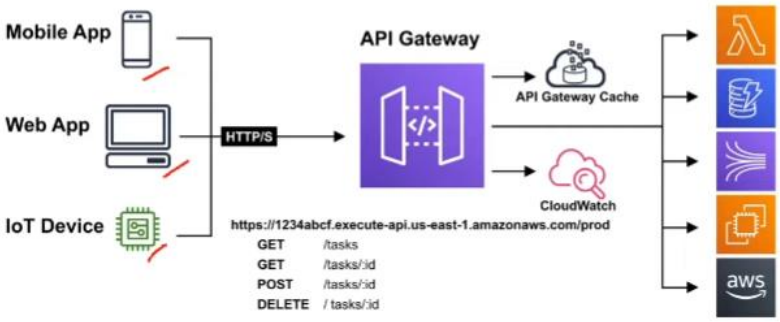
API Gateway

API Gateway

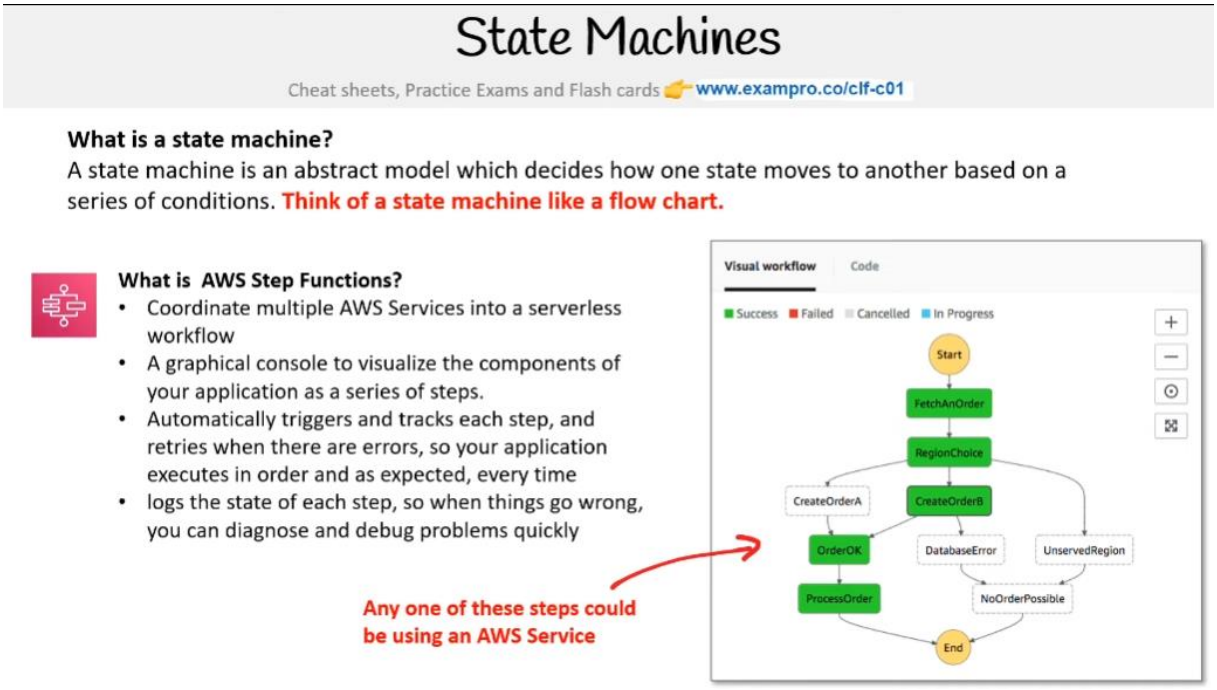
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

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.



State Machines



Event Bus

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.

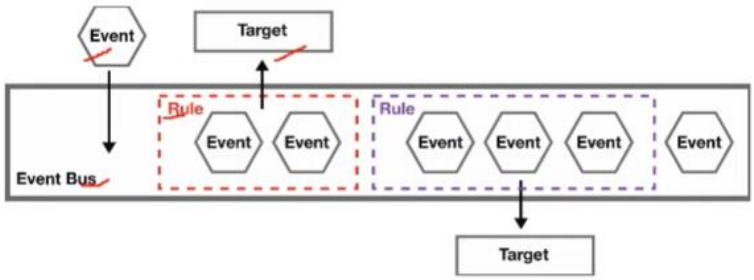
Amazon Event Bridge

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

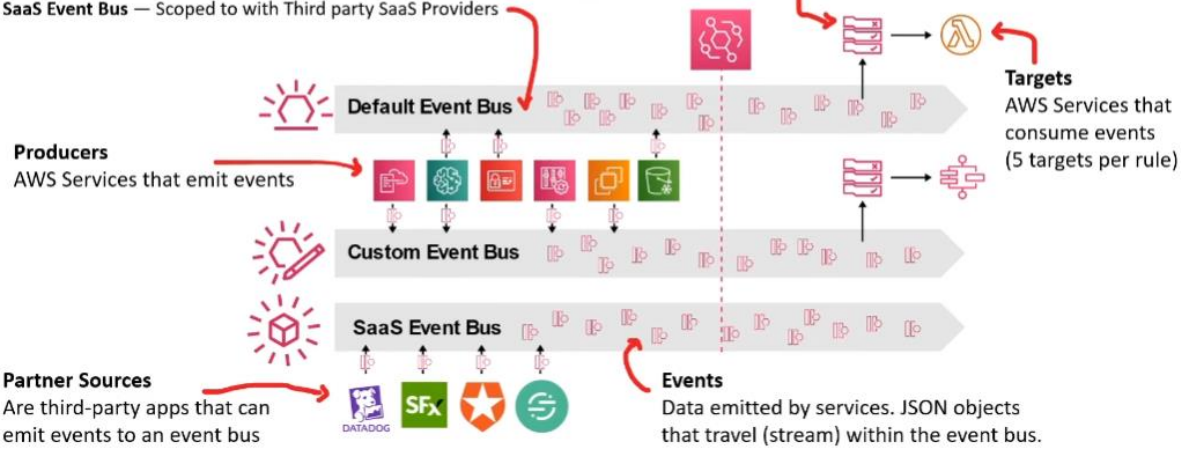
EventBridge was *formerly* called **Amazon CloudWatch** Events.

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)



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

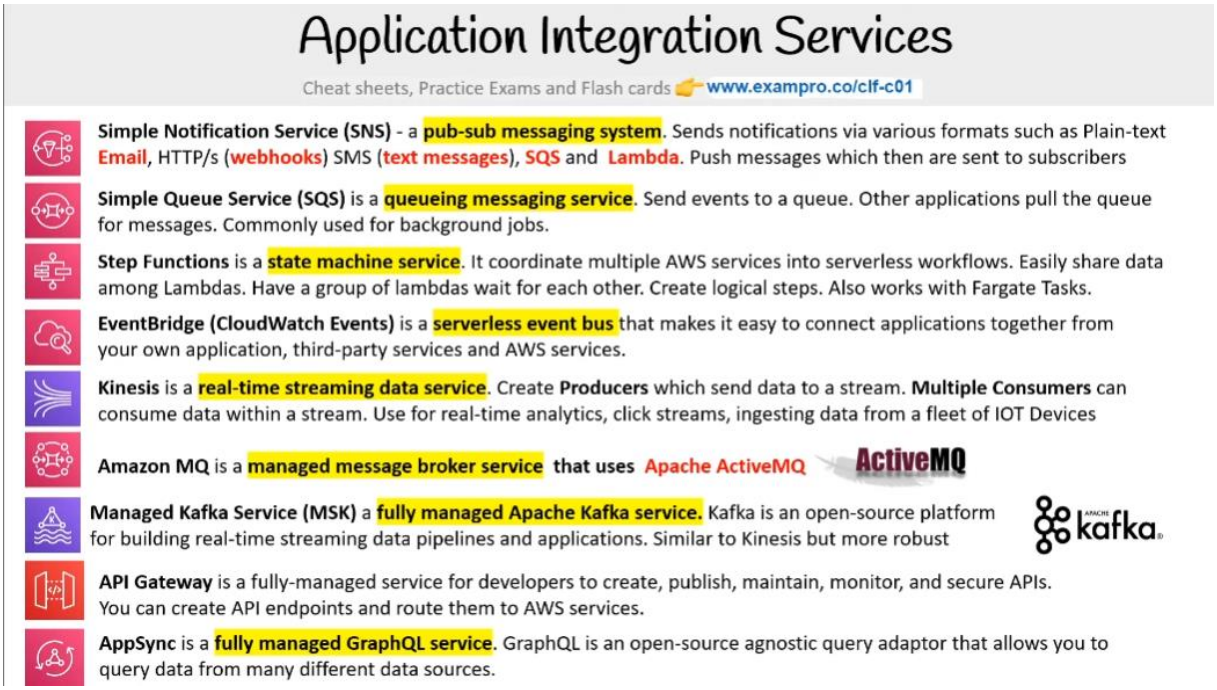
Producers
AWS Services that emit events

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

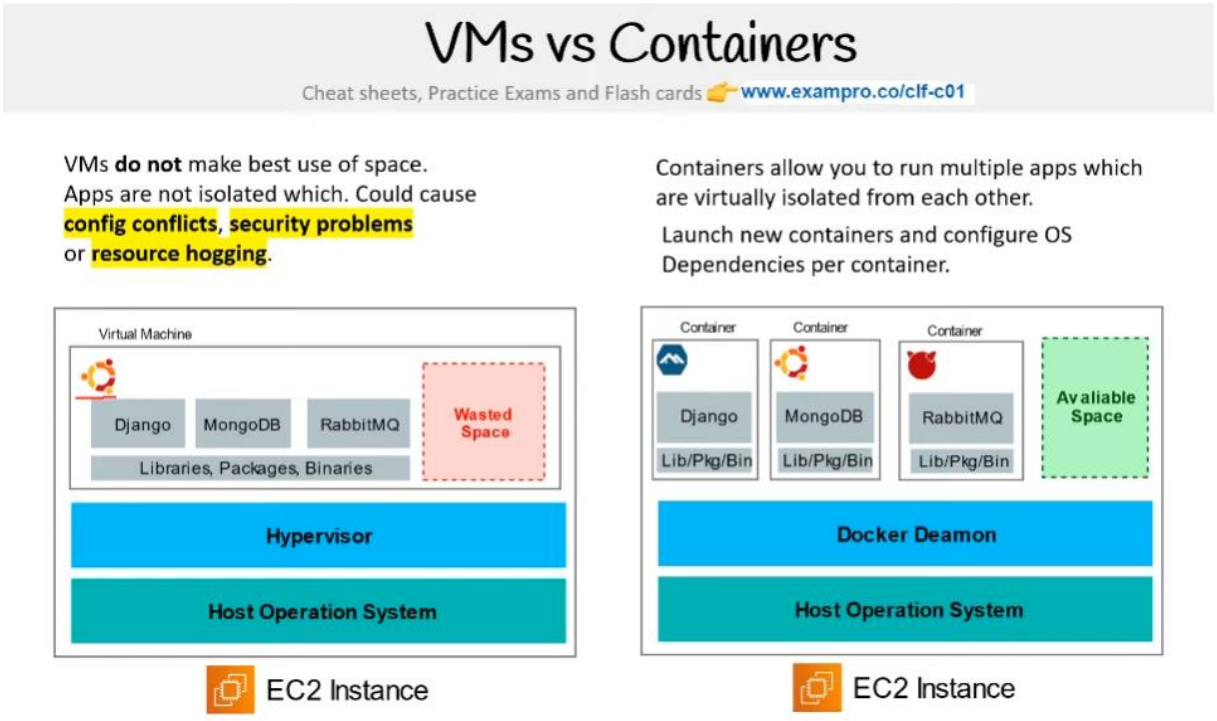
Events
Data emitted by services. JSON objects that travel (stream) within the event bus.

Reference - [EventBus]

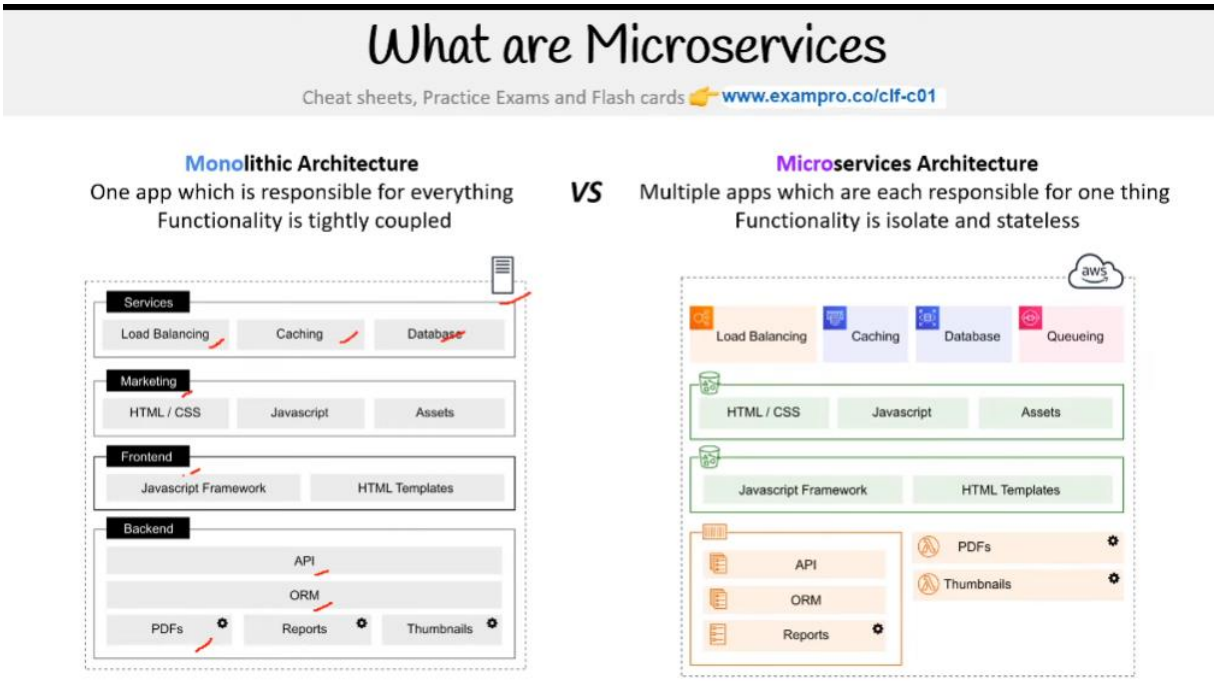
Application Integration Services



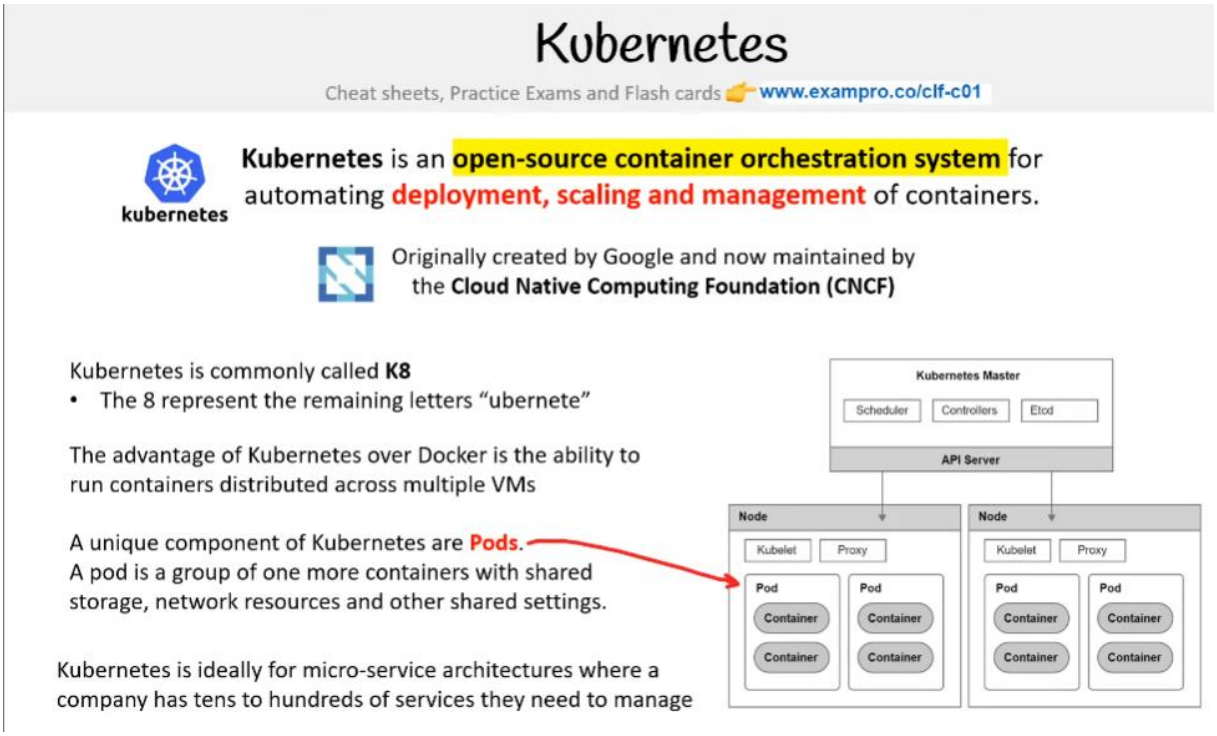
VMs vs Containers



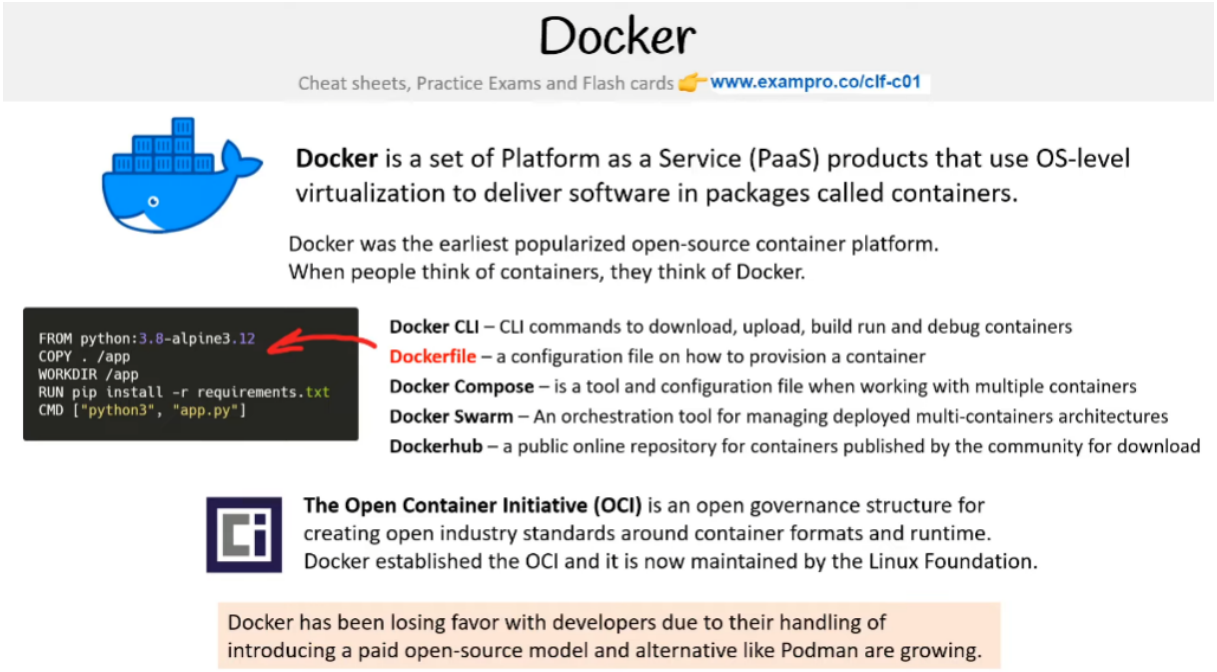
What are Microservices



Kubernetes

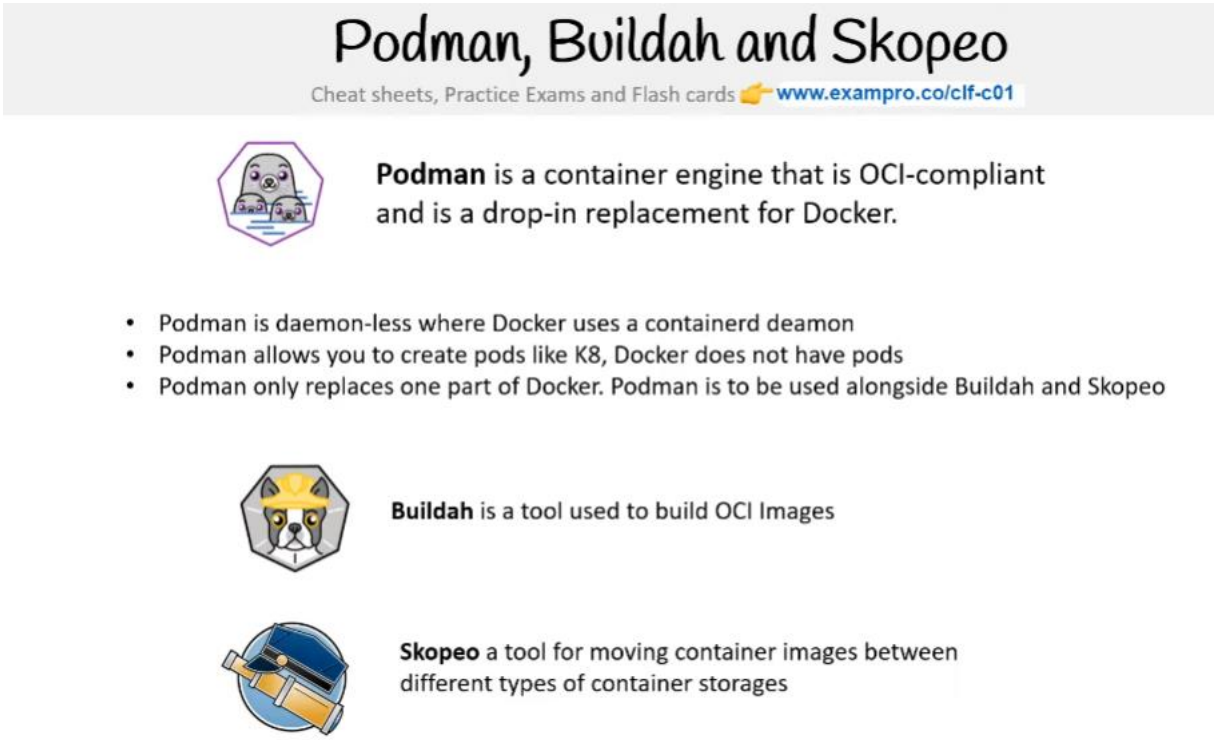


Docker



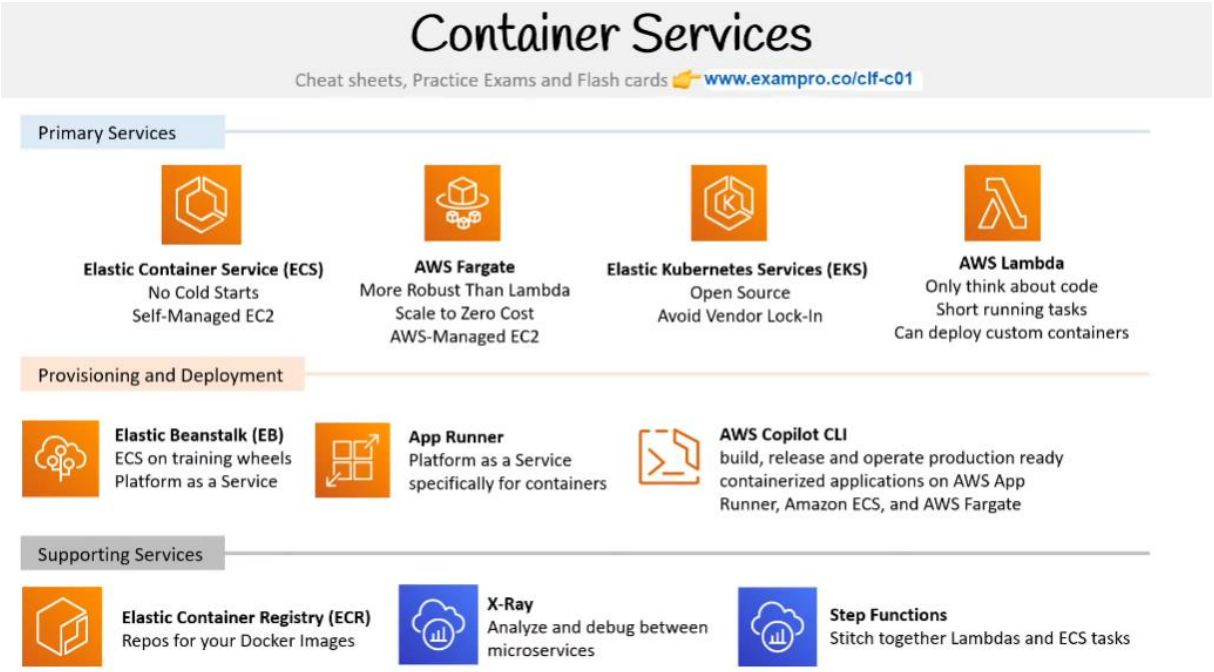
Reference - [Docker (software) | Open Container Initiative]

Podman, Buildah and Skopeo

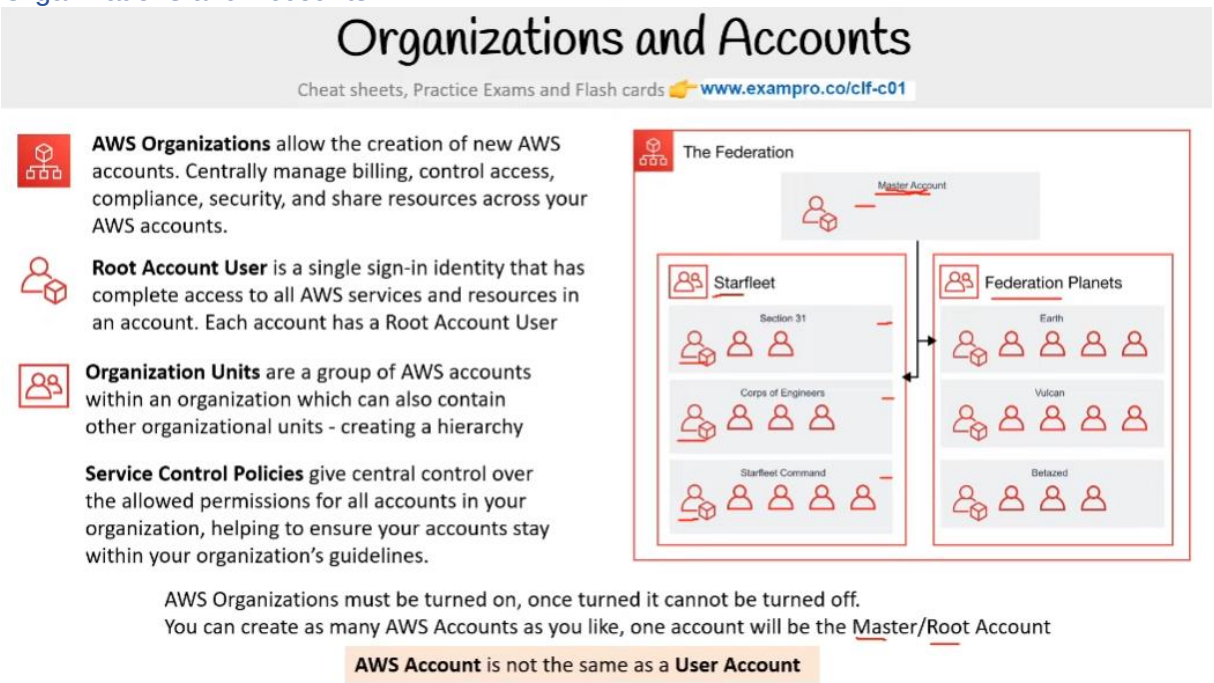


Reference - [podman | skopeo | Daemonless Container Engine]

Container Services



Organizations and Accounts



- **Organizations** allow the creation of new AWS accounts. Centrally manage billing, control access, compliance, security, and share resources across your AWS accounts.
- **Root Account User** is a single sign-in identity that has complete access to all AWS services and resources in an account. Each account has a Root Account User
- **Organization Units** are a group of AWS accounts within an organization which can also contain other organizational units - creating a hierarchy

- **Service Control Policies** give central control over the allowed permissions for all accounts in your organization, helping to ensure your accounts stay within your organization's guidelines.

AWS Organizations must be turned on, once turned it cannot be turned off.

You can create as many AWS Accounts as you like, one account will be the Master/Root Account

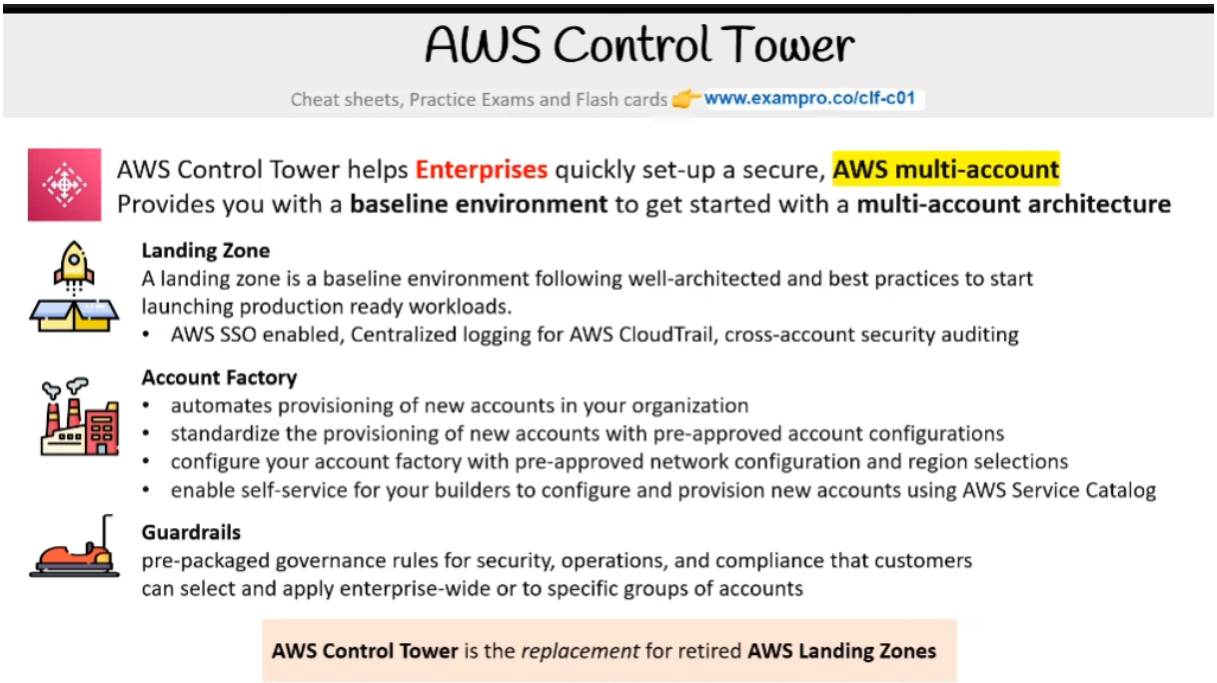
AWS Account is not the same as a User Account

Key Points:

- In AWS you can have more than one account managed through a single account using Organizations
- Organizations allow you to setup consolidated billing where 1 account pays the AWS bill for all
- The payer account is the root level account in an Organization
- You can create isolated AWS accounts for different teams under the payer account - and place them inside Organizational Units (OU)
- The separation of accounts into OUs allows you to set customized permission boundaries on the accounts using Service Control Policies (SCPs)

Reference - Service control policies (SCPs) | AWS Organizations FAQs | AWS account root user | AWS Organizations

AWS Control Tower



Reference - AWS Landing Zone | AWS Control Tower features

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:

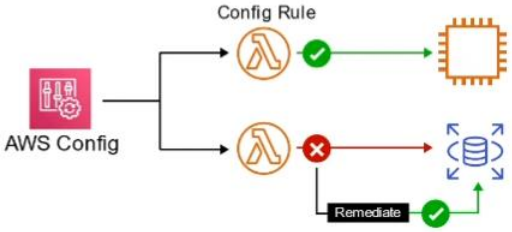
- monitor changes
- enforce changes
- Remediate changes

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.



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

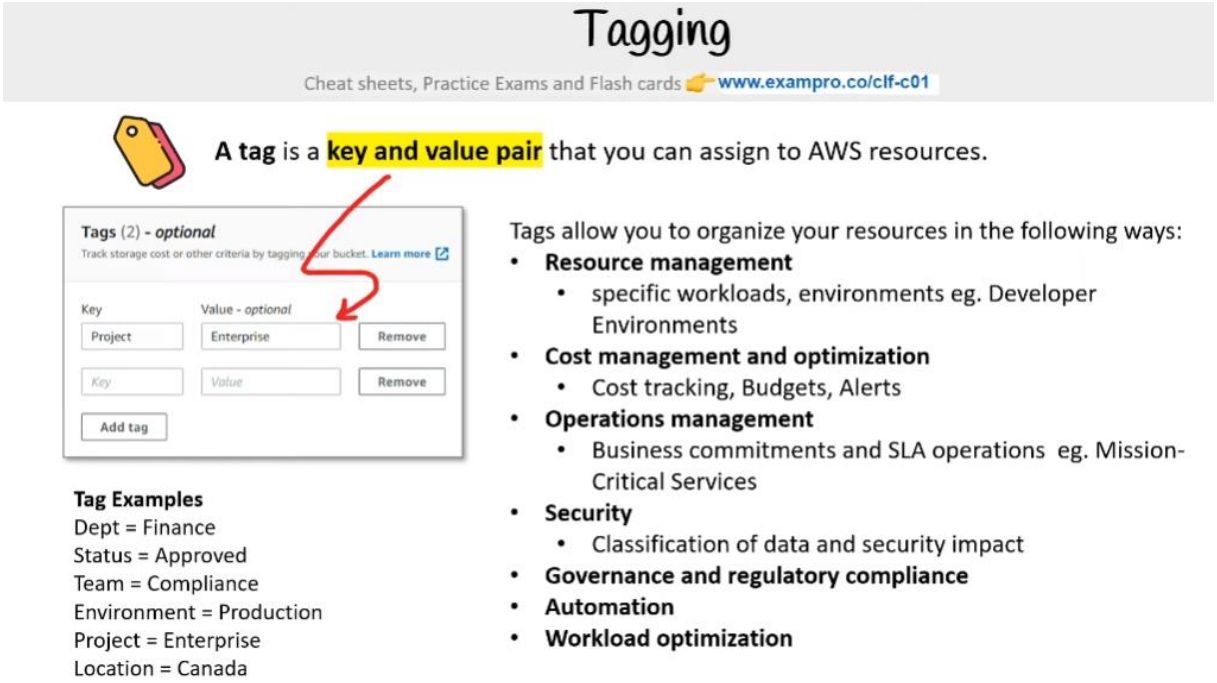
A Quick Start is composed of **3** parts

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!

Reference - [Amazon EC2 Reserved Instances | Amazon EC2 Reserved Instances Pricing | Amazon EC2 Reserved Instance Marketplace | AWS Quick Starts FAQ]

Tagging

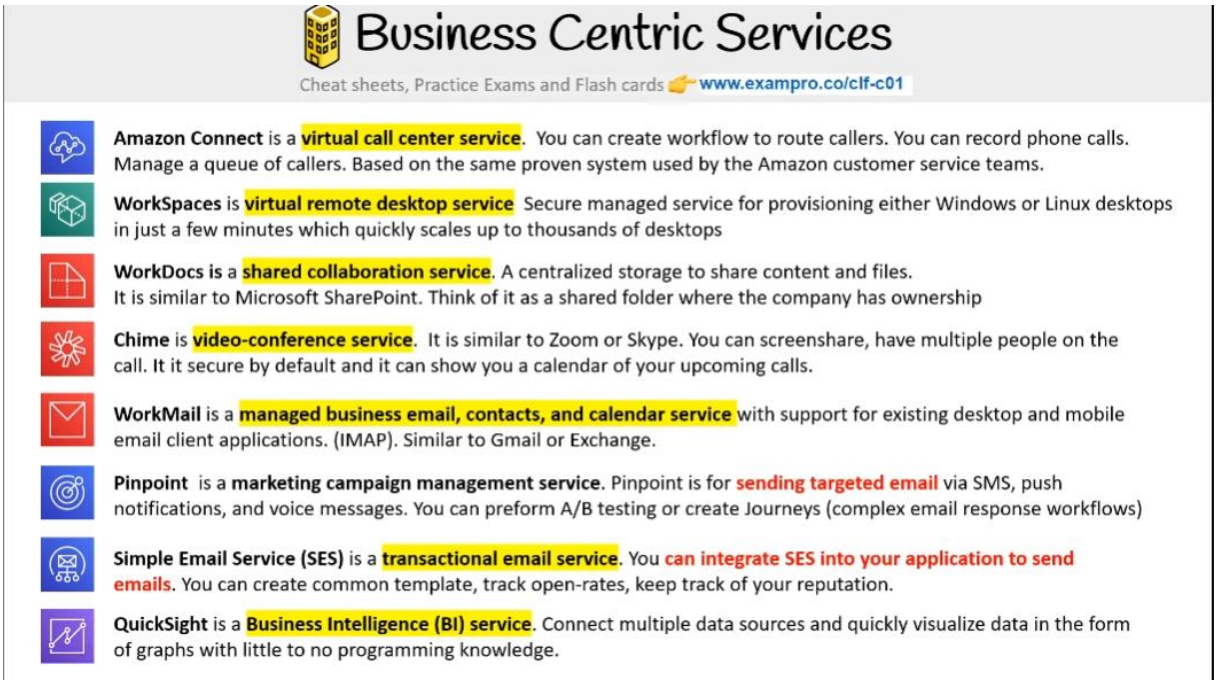


Reference - [What is the AWS Management Console?]

Resource Groups

Reference - [What is the AWS Management Console?]

Business Centric Services



Amazon Connect - Call center as a self-service - cloud-based contact center service that makes it easy for any business to deliver better customer service at lower cost.

WorkSpaces - Virtual Remote Desktops - a fully managed, secure cloud desktop service. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.

WorkDocs - a content creation and collaboration service. Easily create, edit, and share content saved centrally in AWS

Chime - AWS platform for online meetings, video conferencing, and business calling which elastically scales to meet your capacity needs.

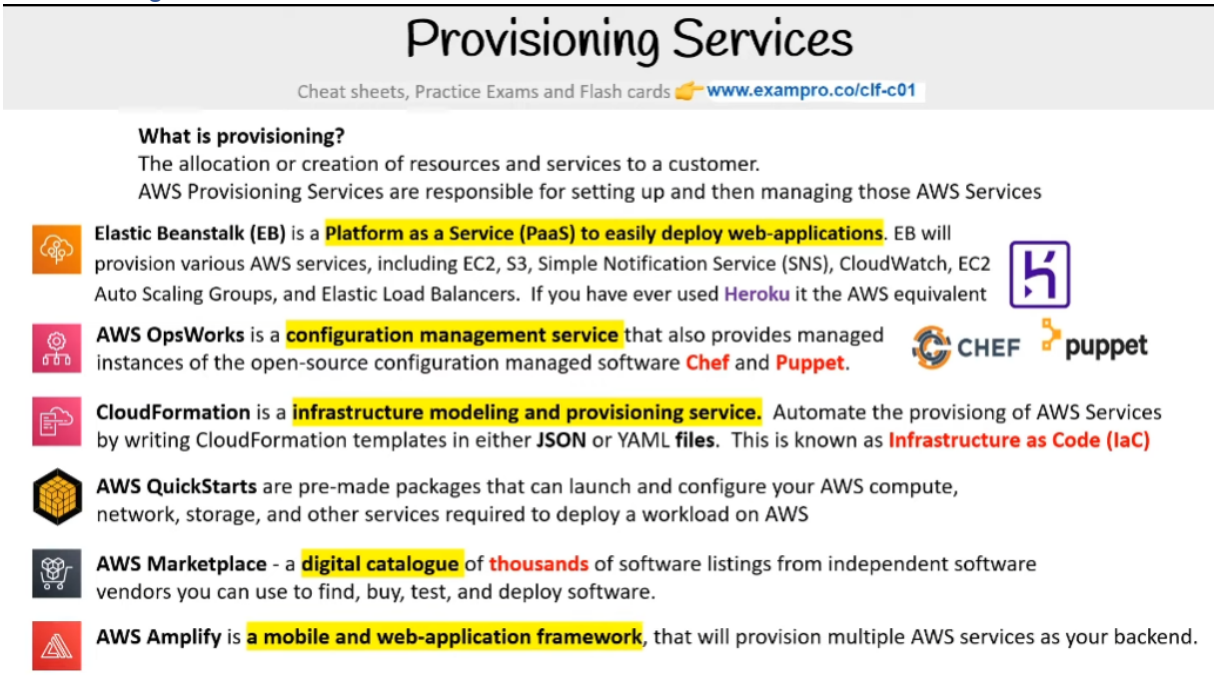
WorkMail - Managed business email, contacts, and calendar service with support for existing desktop and mobile email client applications

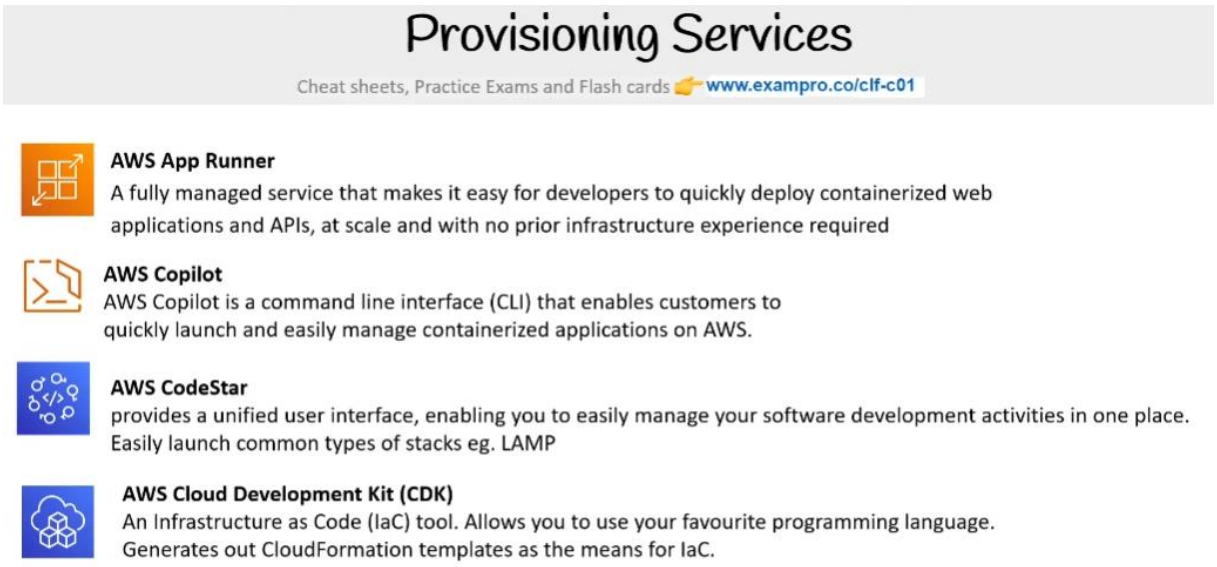
Pinpoint - Marketing campaign management system you can use for sending targeted email, SMS, push notifications, and voice messages.

SES - Simple Email Service- A cloud based email sending service designed fro marketers and application developers to send marketing, notifications, and emails.

QuickSight - A Business Intelligence (BI) service. Connect multiple datasource and quickly visualize data in the form of graphs with little to no programming knowledge.

Provisioning Services:





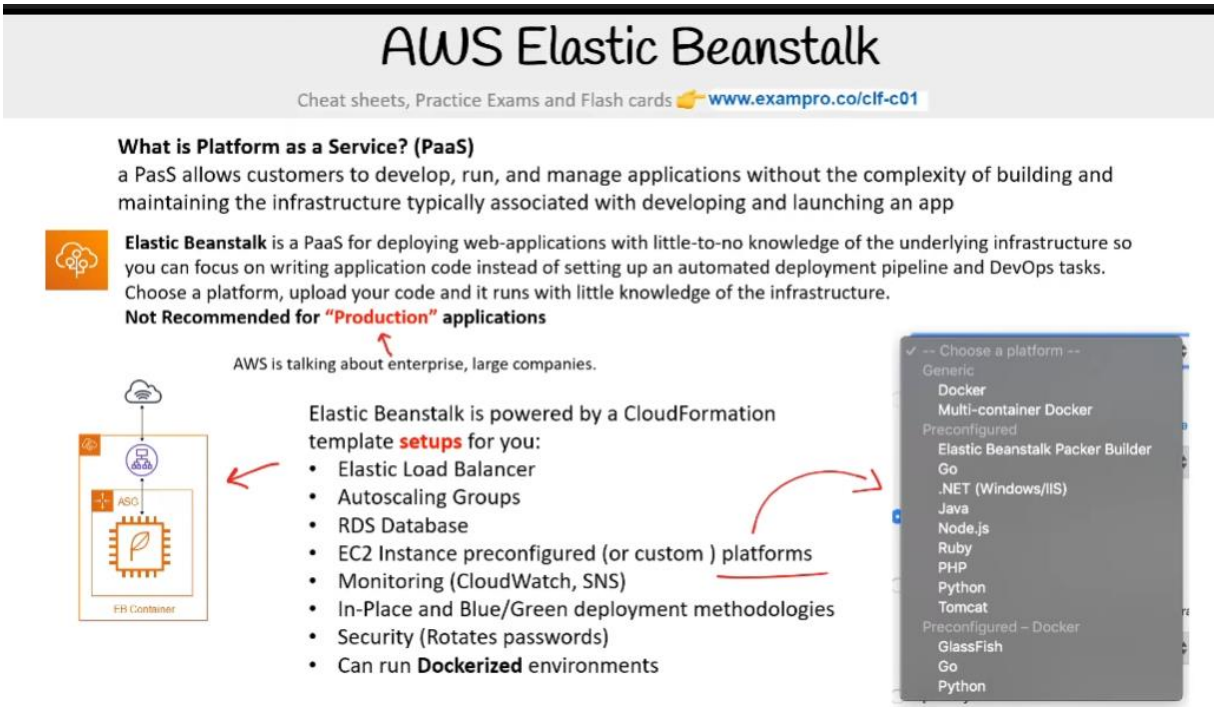
Provisioning is the allocation or creation of resources and services to a customer. AWS Provisioning Services are responsible for setting up and then managing those AWS Services

Types of Services:

- **Elastic Beanstalk** - an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and Internet Information Services (IIS).
- **OpWorks** - configuration management service that provides managed instances of **Chef** and **Puppet**
- **CloudFormation** - lets you deploy your cloud resources using infrastructure-as-code with **JSON** and **YAML** templates

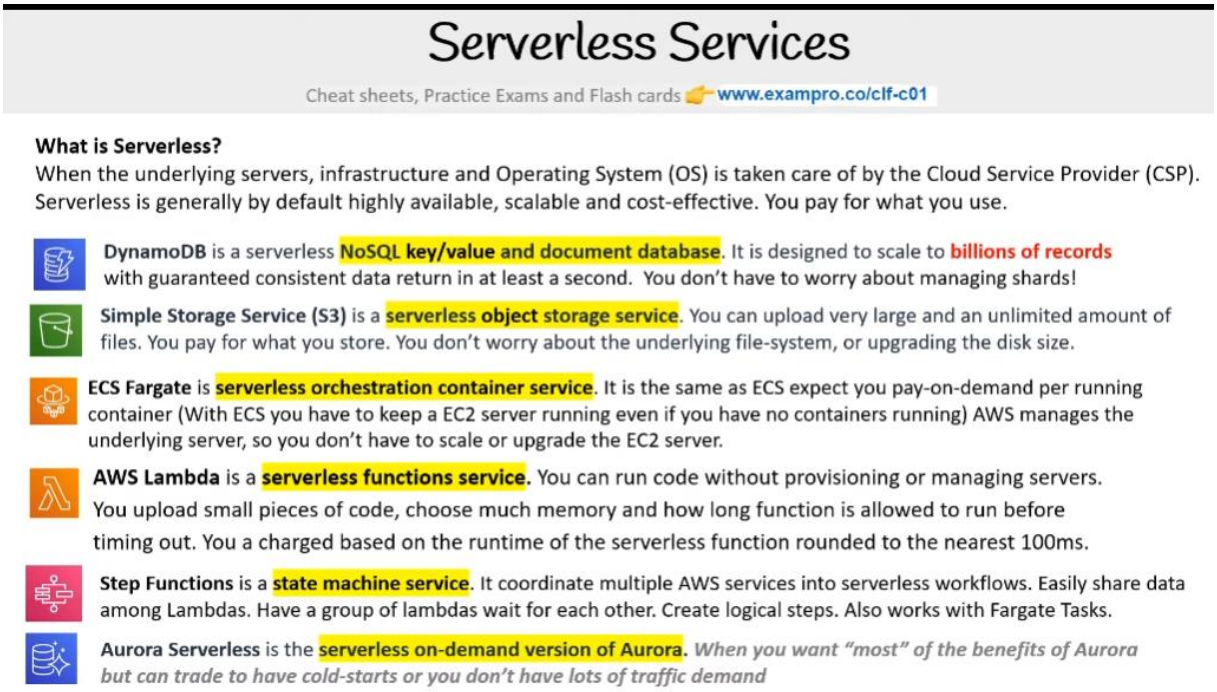
- **AWS QuickStarts** - pre-made packages that can launch and configure your AWS compute, network, storage, and other services required to deploy a workload on AWS
- **AWS Marketplace** - a digital catalogue containing **thousands** of software listings from independent software vendors you can use to find, buy, test, and deploy software.
- **AWS Amplify** - is a mobile and web-application framework, that will provision multiple AWS services as your backend.

AWS Elastic Beanstalk

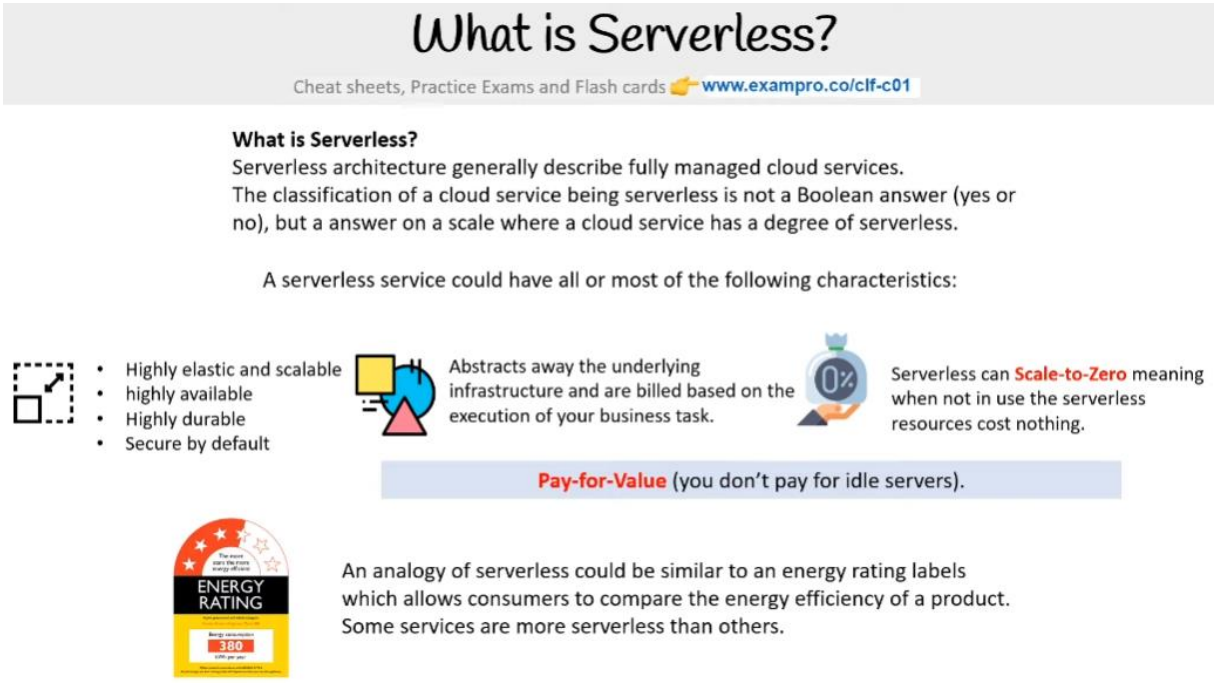


Reference - [AWS OpWorks | AWS Elastic Beanstalk | AWS CloudFormation | AWS AppSync | Amplify Framework Documentation | AWS Quick Starts]

What is Serverless?



What is Serverless?



When the underlying servers, infrastructure, and Operating System (OS) is taken care of by the Cloud Service Provider (CSP).

Serverless is generally by default highly available, scalable and cost-effective. You pay for what you use.

DynamoDB - is a serverless NoSQL key/value and document database. It is designed to scale to billions of records with guaranteed consistent data return in at least a second. You don't have to worry about managing shards!

Simple Storage Service (S3) - is a serverless object storage service. You can upload very large and an unlimited amount of files. You pay for what you store. You don't worry about the underlying file-system, or upgrading the disk size.

ECS Fargate - is serverless orchestration container service. It is the same as ECS except you pay-on-demand per running container (With ECS you have to keep an EC2 server running even if you have no containers running) AWS manages the underlying server, so you don't have to scale or upgrade the EC2 server.

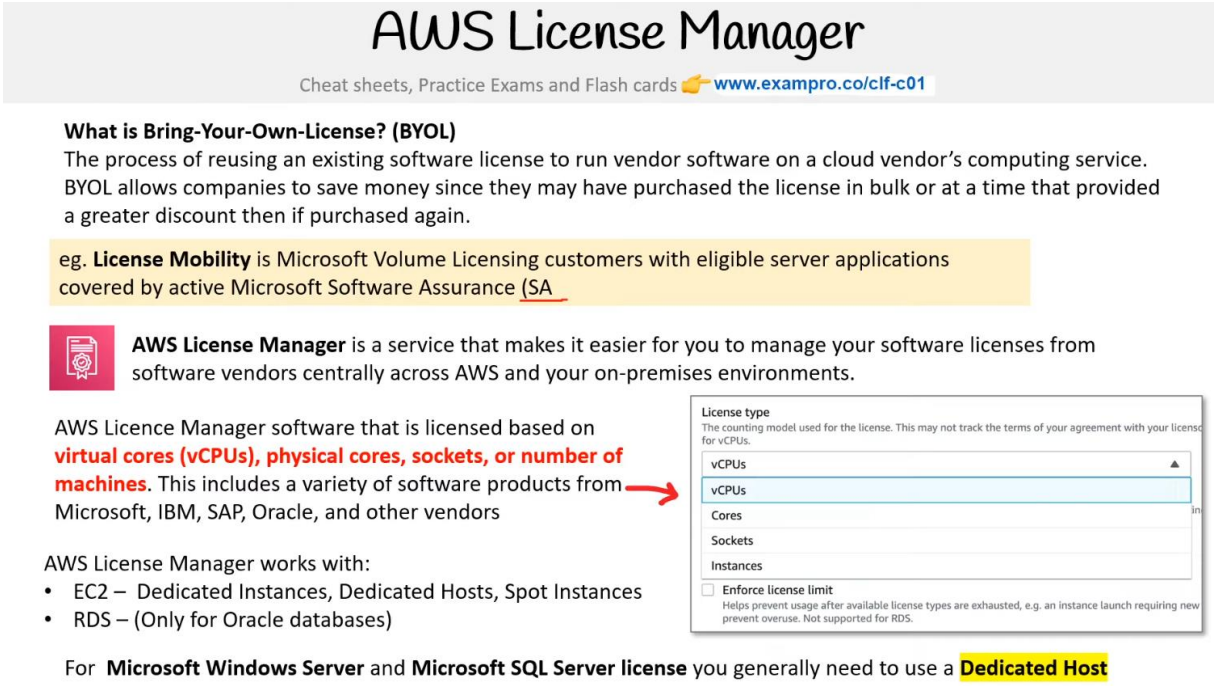
AWS Lambda - is a serverless functions service. You can run code without provisioning or managing servers. You upload small pieces of code, choose how much memory, and how long the function is allowed to run before timing out. You a charged based on the runtime of the serverless function rounded to the nearest 100ms.

Step Functions - is a state machine service. It coordinates multiple AWS services into serverless workflows. Easily share data among Lambdas. Have a group of lambdas wait for each other. Create logical steps. Also works with Fargate Tasks.

Aurora Serverless - is the serverless on-demand version of Aurora. When you want "most" of the benefits of Aurora but can trade to have cold-starts or you don't have lots of traffic demand

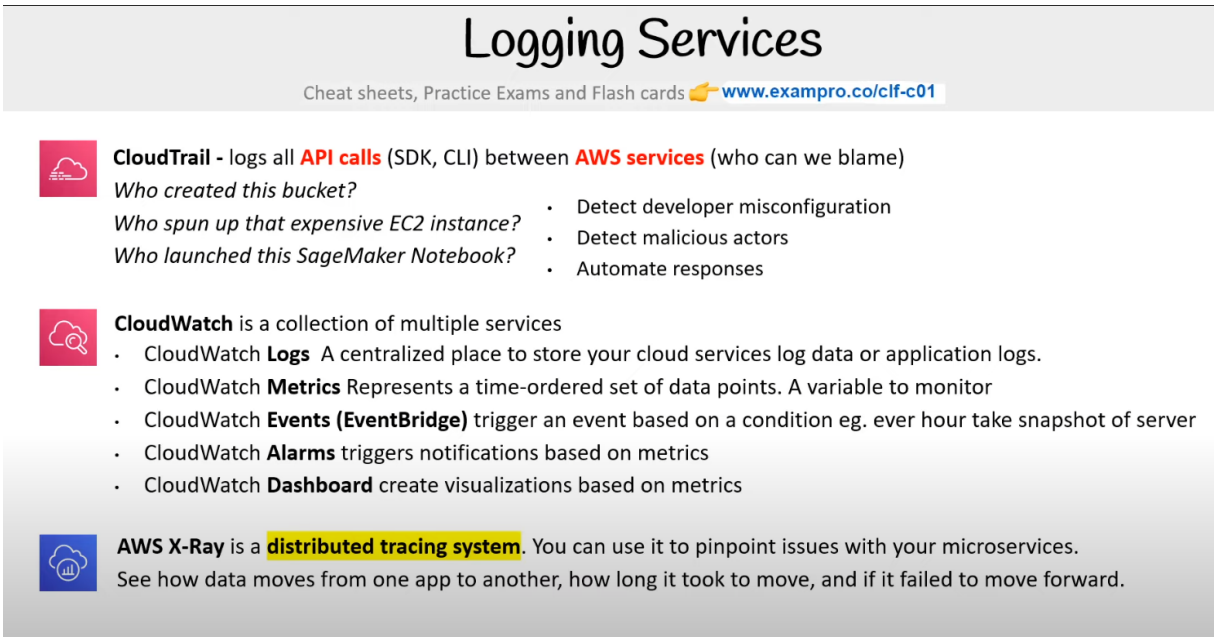
Windows on AWS

AWS License Manager



Reference - [AWS License Manager](#) | [Bring your own license](#)

Logging Services



Amazon Web Services (AWS) provides service-specific operational metrics and log files to give customers insight into how the service is operating.

CloudTrail - logs all API calls(SDK, CLI) between various AWS services

Questions that CloudTrail can answer:

Who create this bucket? - detect developer mis-configuration

Who spun up that expensive EC2 instance? - Detect malicious actors

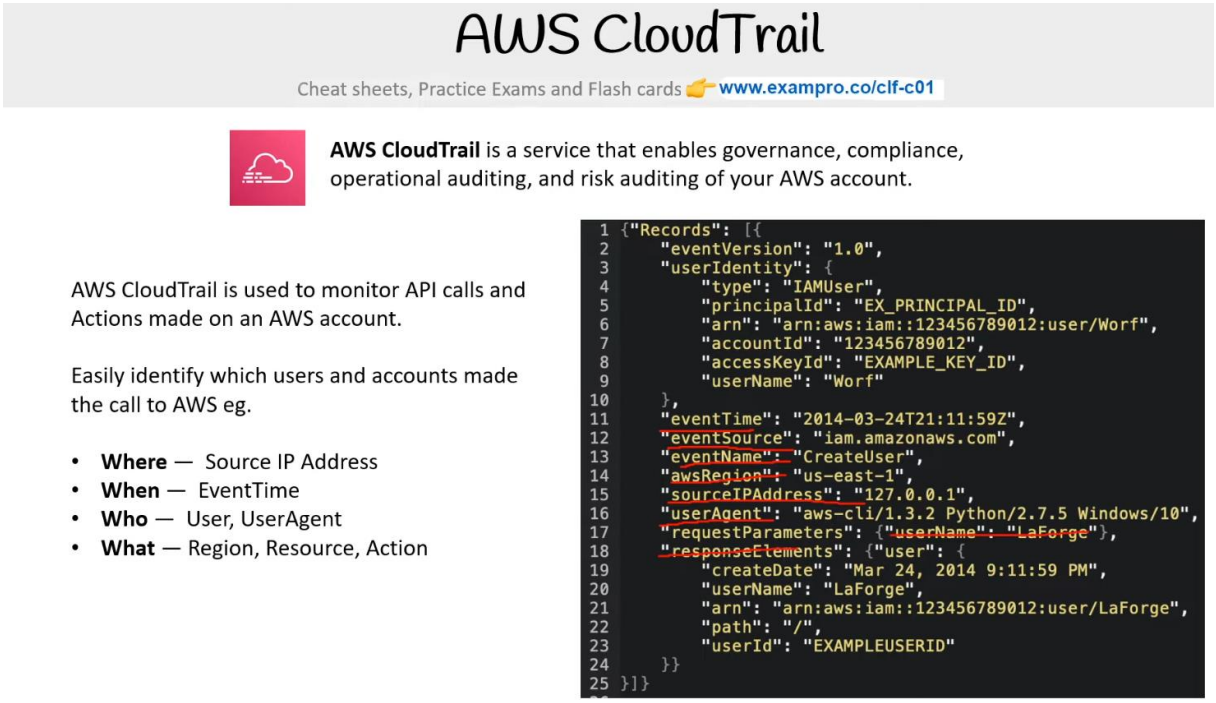
Who launched this SageMaker notebook? - Automate responses

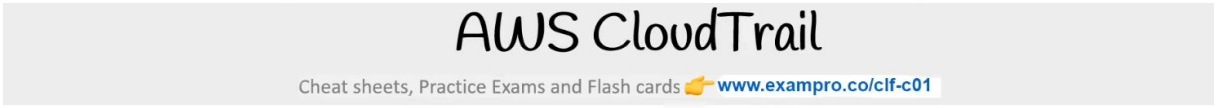
CloudWatch - is a collection of multiple services

- CloudWatch **Logs** : Performance data about AWS Services eg. CPU Utilization, Memory, Network in Application Logs eg. Rails, Nginx Lambda Logs
- CloudWatch **Metrics**: Represents a time-ordered set of data points. A variable to monitor
- CloudWatch **Events**: trigger an event based on a condition eg. every hour take a snapshot of the server
- CloudWatch **Alarms**: triggers notifications based on metrics
- CloudWatch **Dashboard**: create visualizations based on metrics

AWS X-Ray is a distributed tracing system. You can use it to pinpoint issues with your microservices. See how data moves from one app to another, how long it took to move, and if it failed to move forward.

AWS CloudTrail

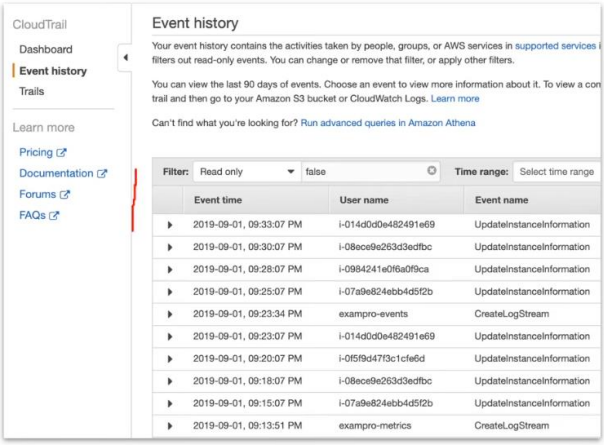




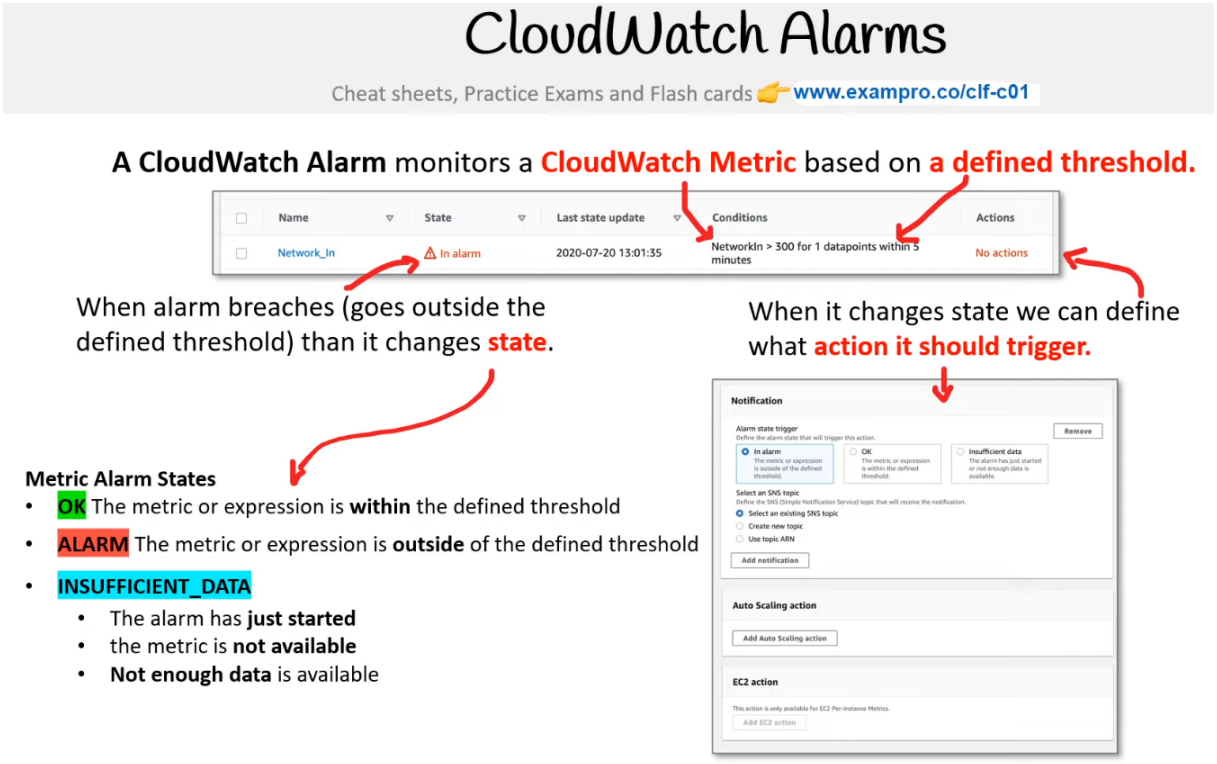
CloudTrail is already logging by default and will collect logs for **last 90 days** via **Event History**

If you need more than 90 days you need to create a **Trail**

Trails are output to S3 and do not have GUI like Event History. To analyze a Trail you'd have to use **Amazon Athena**.



CloudWatch Alarms



A CloudWatch Alarm monitors a **CloudWatch Metric** based on **a defined threshold.**

When alarm breaches (goes outside the defined threshold) then it changes **state.**

Metric Alarm States

- **OK** The metric or expression is **within** the defined threshold
- **ALARM** The metric or expression is **outside** of the defined threshold

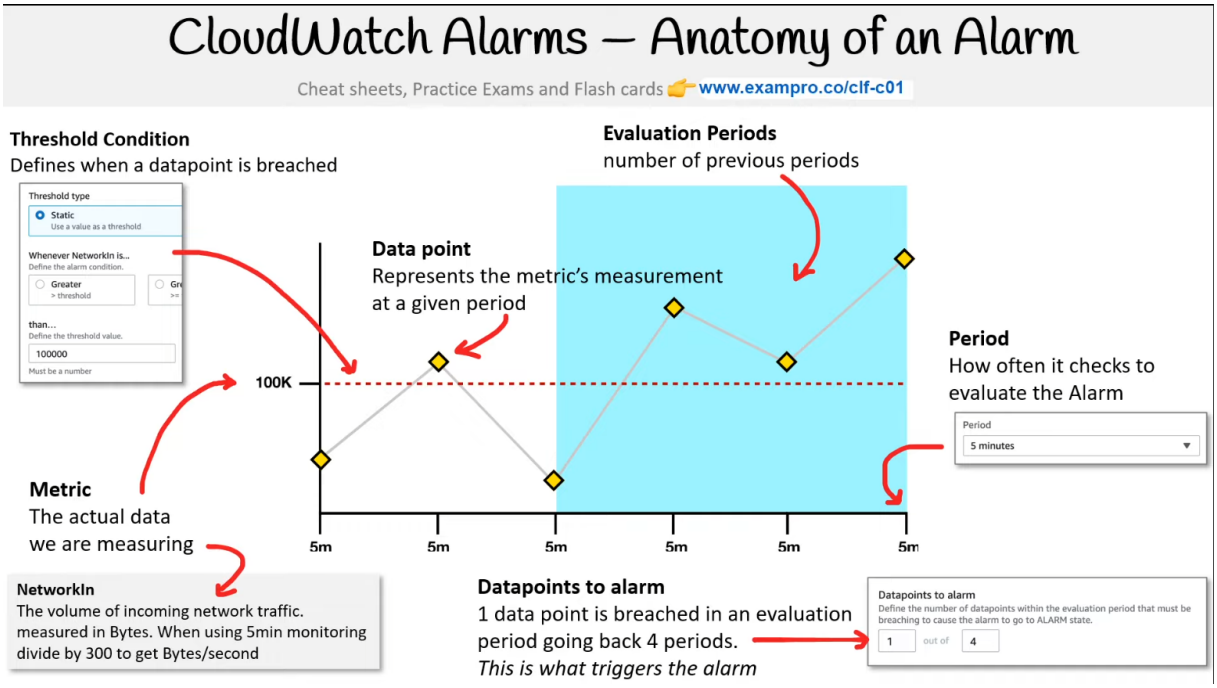
- **INSUFFICIENT_DATA**
    - The alarm has just started
    - the metric is not available
    - Not enough data is available

When it changes state we can define what **action it should trigger.**

- Notification
- Auto Scaling Group
- EC2 Action

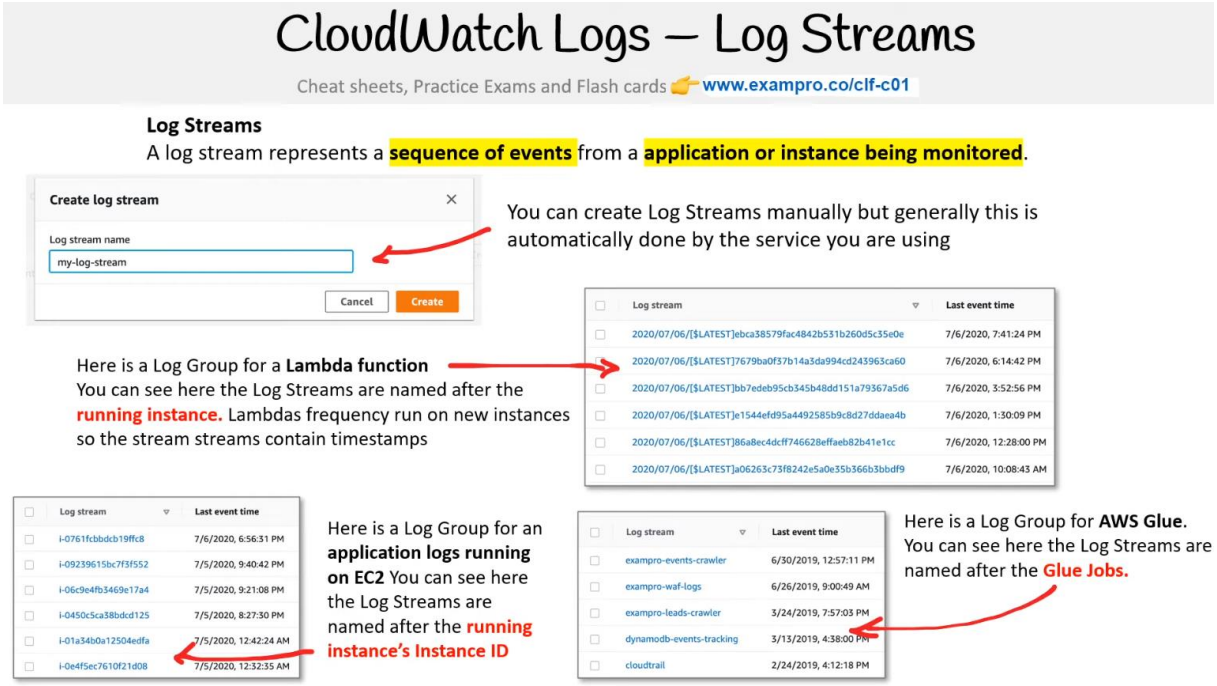
Reference - [Using Amazon CloudWatch alarms]

CloudWatch Alarms — Anatomy of an Alarm

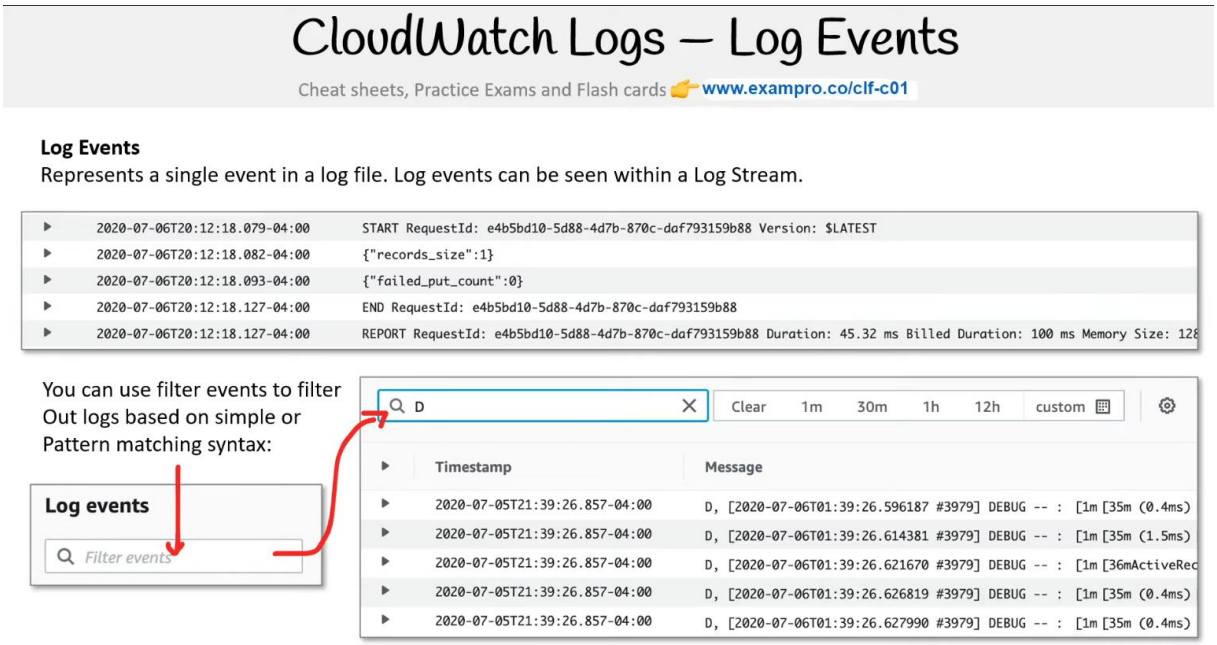


Reference - [Using Amazon CloudWatch alarms | What is Amazon EC2?]

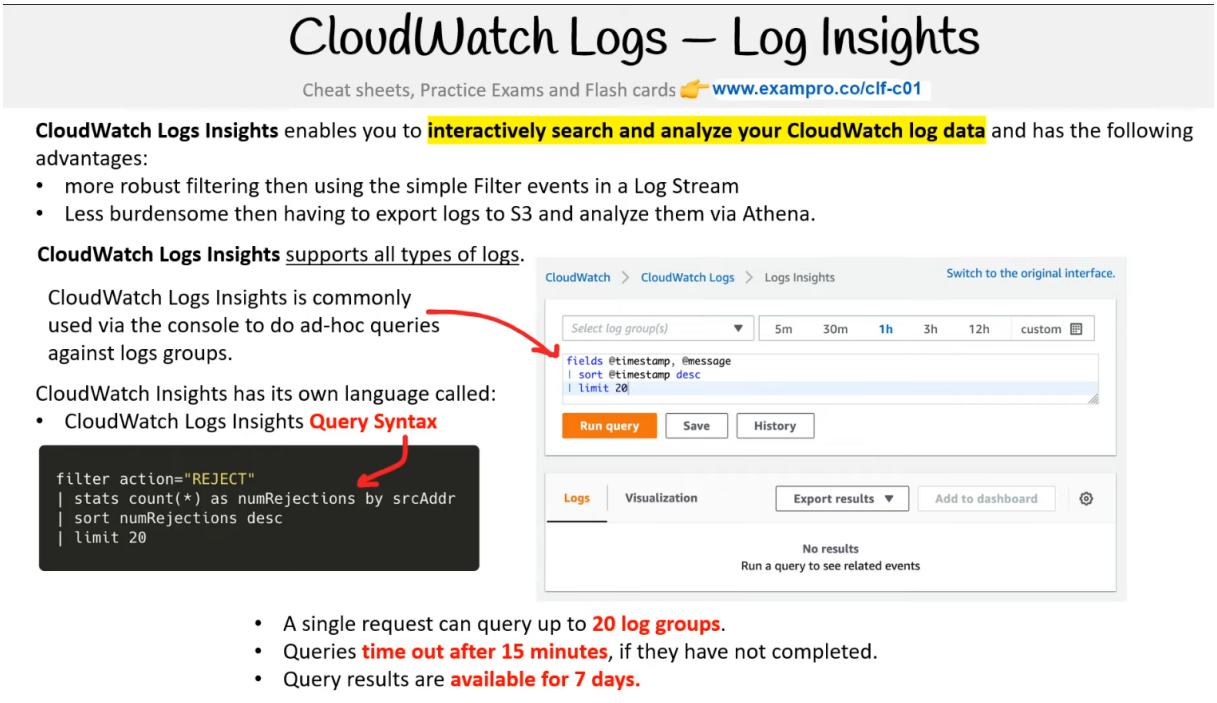
CloudWatch Logs — Log Streams

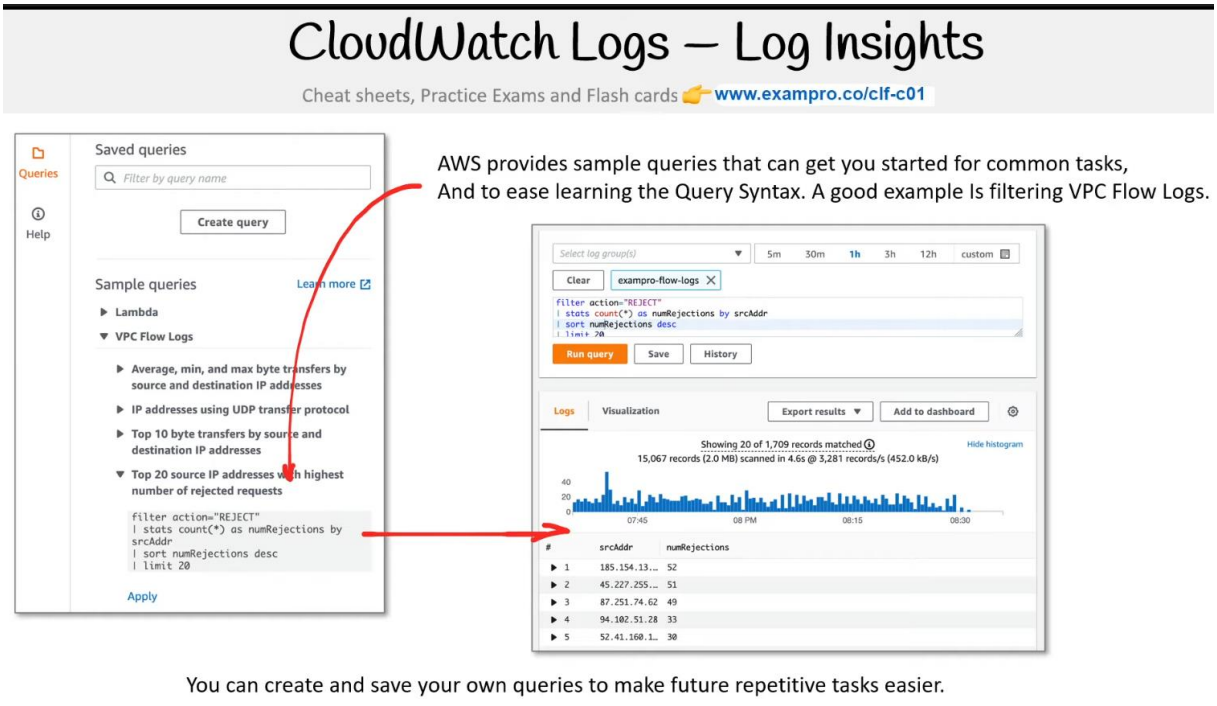


CloudWatch Logs — Log Events



CloudWatch Logs — Log Insights





CloudWatch Logs Insights enables you to **interactively search and analyze your CloudWatch log data** and has the following advantages:

- More robust filtering than using the simple Filter events in a Log Stream
- Less burdensome than having to export logs to S3 and analyze them via Athena.

CloudWatch Logs Insights supports all types of logs.

CloudWatch Logs Insights is commonly used via the console to do ad-hoc queries against logs groups.

CloudWatch Insights has its own language called:

- CloudWatch Logs Insights **Query Syntax**

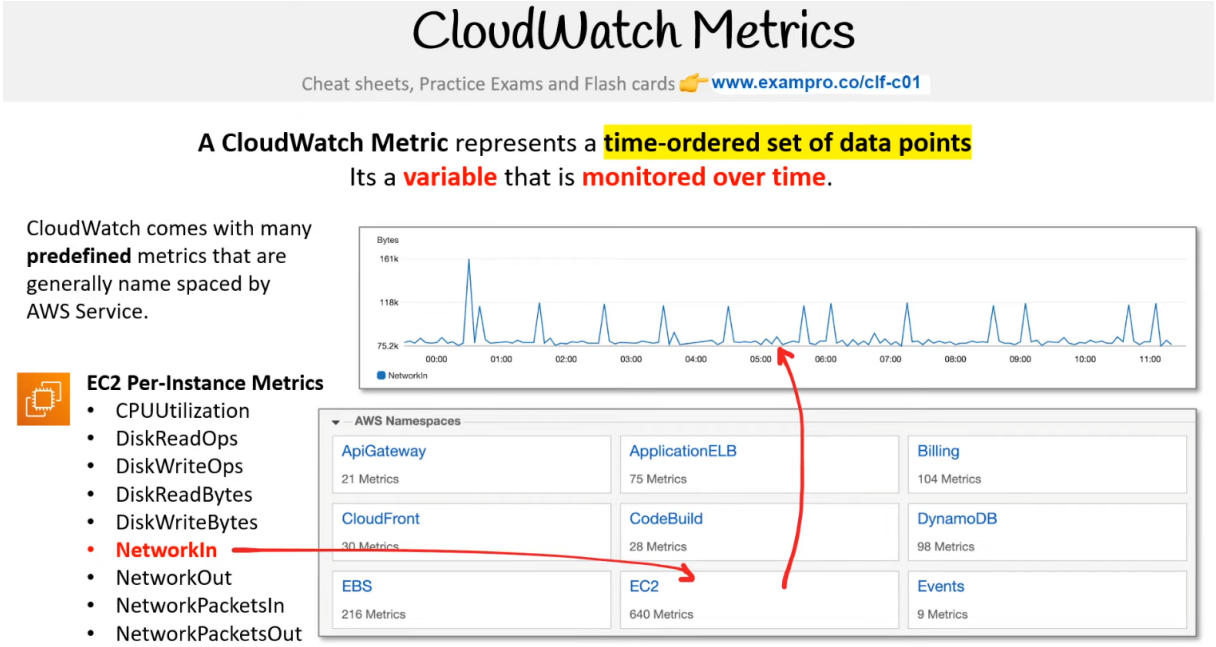
- A single request can query up to **20 log groups.**
- Queries **time out after 15 minutes**, if they have not been completed.
- Query results are **available for 7 days.**

AWS provides sample queries that can get you started for common tasks,

And to ease learning the Query Syntax. A good example Is filtering VPC Flow Logs.

You can create and save your own queries to make future repetitive tasks easier.

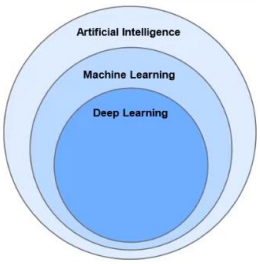
CloudWatch Metrics



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

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.

Machine Learning and AI Services

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

Amazon Forecast is a **time-series forecasting service**. Forecast business outcomes such as product demand, resource needs or financial performance.

AWS Deep Learning AMIs Amazon EC2 instances **pre-installed with popular deep learning frameworks** and interfaces such as TensorFlow, PyTorch, Apache MXNet, Chainer, Gluon, Horovod, and Keras

AWS Deep Learning Containers Docker images instances pre-install with popular deep learning frameworks and interfaces such as TensorFlow, PyTorch, and Apache MXNet.

AWS DeepComposer is **machine-learning enabled musical keyboard**

AWS DeepLens is a **video-camera that uses deep-learning**.

AWS DeepRacer a **toy race car** that can be powered with machine-learning to perform **autonomous driving**.

Amazon Elastic Inference allows you to attach low-cost GPU-powered acceleration to EC2 instances to reduce the cost of running deep learning inference by up to 75%.

Amazon Fraud Detector is a **fully managed fraud detection a service**. identify potentially fraudulent online activities such as online payment fraud and the creation of fake accounts.

Amazon Kendra **enterprise machine learning search engine service**. Uses natural language to suggest answers to question instead of just simple keyword matching

Big Data and Analytics Services

Big Data and Analytics Services

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

What is BigData?
A term used to describe **massive volumes of structured/unstructured data** that is so large it is difficult to **move and process** using traditional database and software techniques.

Amazon Athena is a **serverless interactive query service**. It can take a bunch of CSV or JSON files in a S3 Bucket and load them into temporary SQL tables so you can run SQL queries. ***When you want to query CSV or JSON files***

Amazon CloudSearch is a fully managed **full-text search service**. ***When you want add search to your website***

Amazon Elasticsearch Service (ES) is a **managed Elasticsearch cluster**. Elasticsearch is a open-source full-text search engine. It is more robust than CloudSearch but requires more server and operational maintaince.

Amazon Elastic MapReduce (EMR) is for data processing and analysis. Its can be used for creating reports just like Redshift, but is more suited when you need to transform unstructured data into structured data on the fly.

Kinesis Data Streams is a **real-time streaming data service**. Create **Producers** which send data to a stream. **Multiple Consumers** can consume data within a stream. Use for real-time analytics, click streams, ingesting data from a fleet of IOT Devices

Kinesis Firehose is serverless and a simpler version of Data Streams, You pay-on-demand based on how much data is consumed through the stream and you don't worry about the underlying servers.

Amazon Kinesis Data Analytics allows you to run queries against data that is flowing through your real-time stream so you can create reports and analysis on emerging data.

Amazon Kinesis Video Streams allows you to analyze or apply processing on real-time streaming video.

Big Data and Analytics Services

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

Managed Kafka Service (MSK) a **fully managed Apache Kafka service.** Kafka is an open-source platform for building real-time streaming data pipelines and applications. It is similar to Kinesis but with more robust functionalities

Redshift is a **petabyte-size data-warehouse.** Data-warehouses are for Online Analytical Processing) OLAP Data-warehouses can be expensive because they are keeping data "hot". Meaning that we can run a very complex query and a large amount of data and get that data back very fast.
When you to quickly generate analytics or reports from a large amount of data.

Amazon QuickSight is **business intelligence (BI) dashboard**. You can use it to create business dashboards to power business decisions. It requires little to no programming knowledge and connect and ingest to many different types of databases

AWS Data Pipeline automates the movement of data. You can reliably move data between compute and storage services.

AWS Glue is an **Extract, Transform, Load (ETL) service**. Moving data from one location to another and where you need to perform transformations before the final destination. Similar to Database Migration Service (DMS) but more robust

AWS Lake Formation is as a **centralized, curated, and secured repository that stores all your data.**
A **data lake** is a storage repository that holds a vast amount of raw **data** in its native format until it is needed.

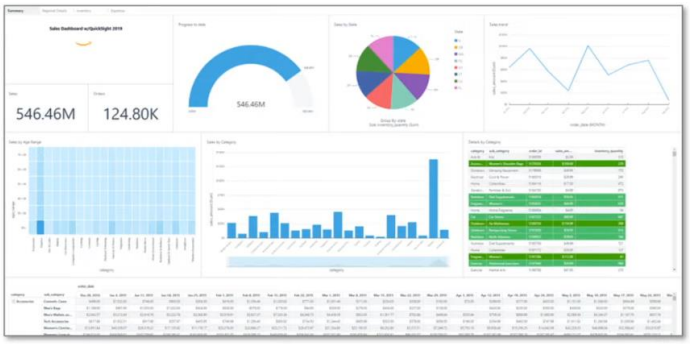
AWS Data Exchange is a catalogue of third-party datasets. You can download for free subscribe or purchase datasets.
Eg. COVID-19 Foot Traffic Data, IMDB TV and Movie data, Historical Weather Data

Amazon QuickSight

Amazon QuickSight

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

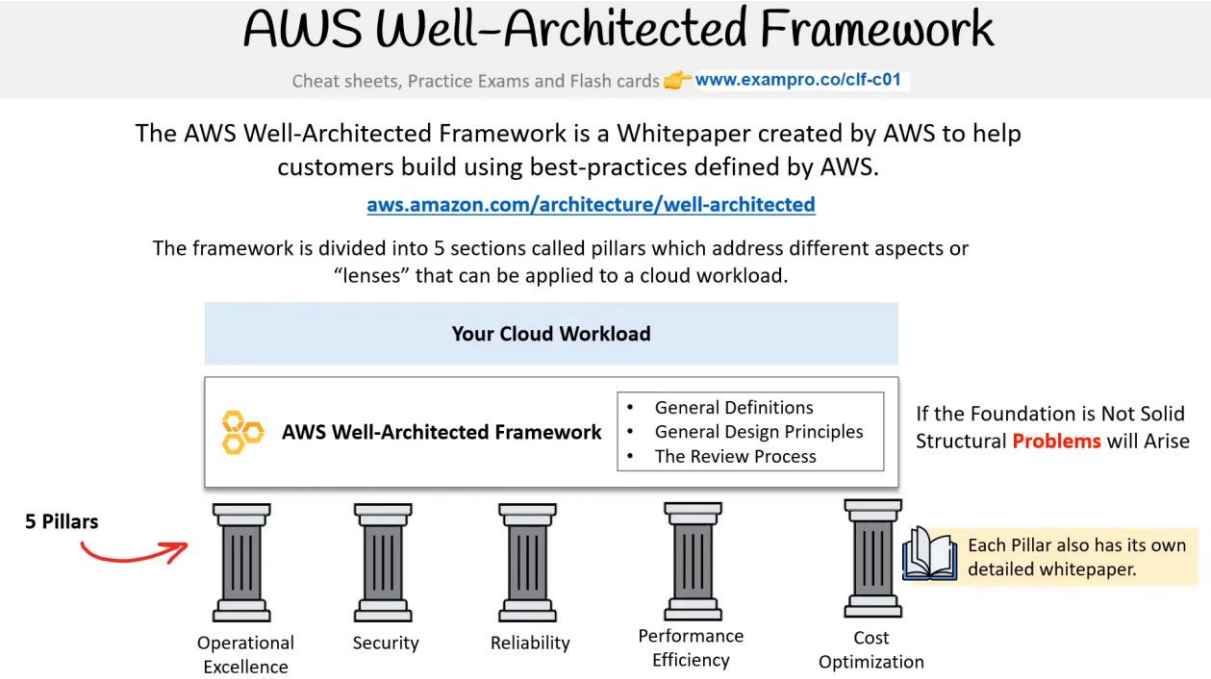
Amazon QuickSight is a **Business Intelligence (BI) Dashboard** that allows you to ingest data from various AWS storage or database services to **quickly visualize business data** with minimal programming or data formula knowledge.



QuickSight uses **SPICE** (super-fast, parallel, in-memory, calculation engine) to achieve blazing fast performance at scale

Amazon QuickSight ML Insights – Detect Anomalies, Perform accurate forecasting, Generate Natural Language Narratives.
Amazon QuickSight Q - Ask question using natural language, on all your data, and receive answers in seconds.

AWS Well-Architected Framework



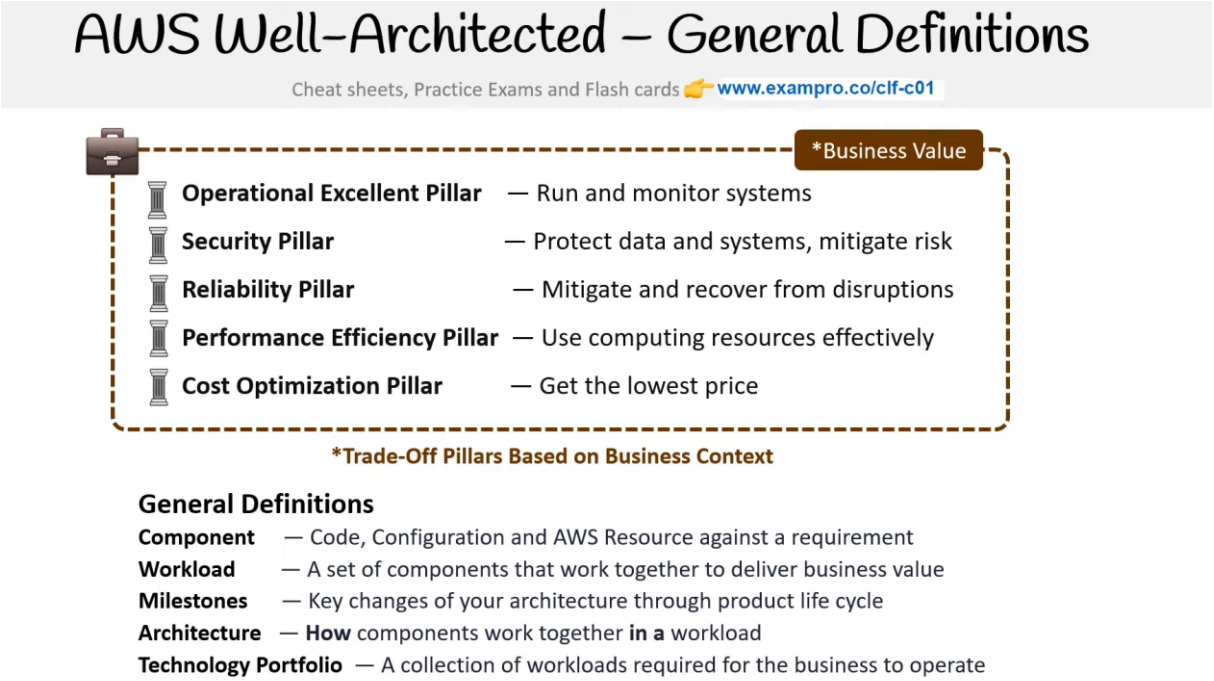
Note: On Dec 2, 2021, AWS introduced a new AWS Well-Architected Sustainability Pillar to help organizations learn, measure, and improve workloads using environmental best practices for cloud computing.

~~5~~ 6 Pillars

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization
- **[New] Sustainability**

Reference - AWS Well-Architected | New Sustainability Pillar for the AWS Well-Architected Framework

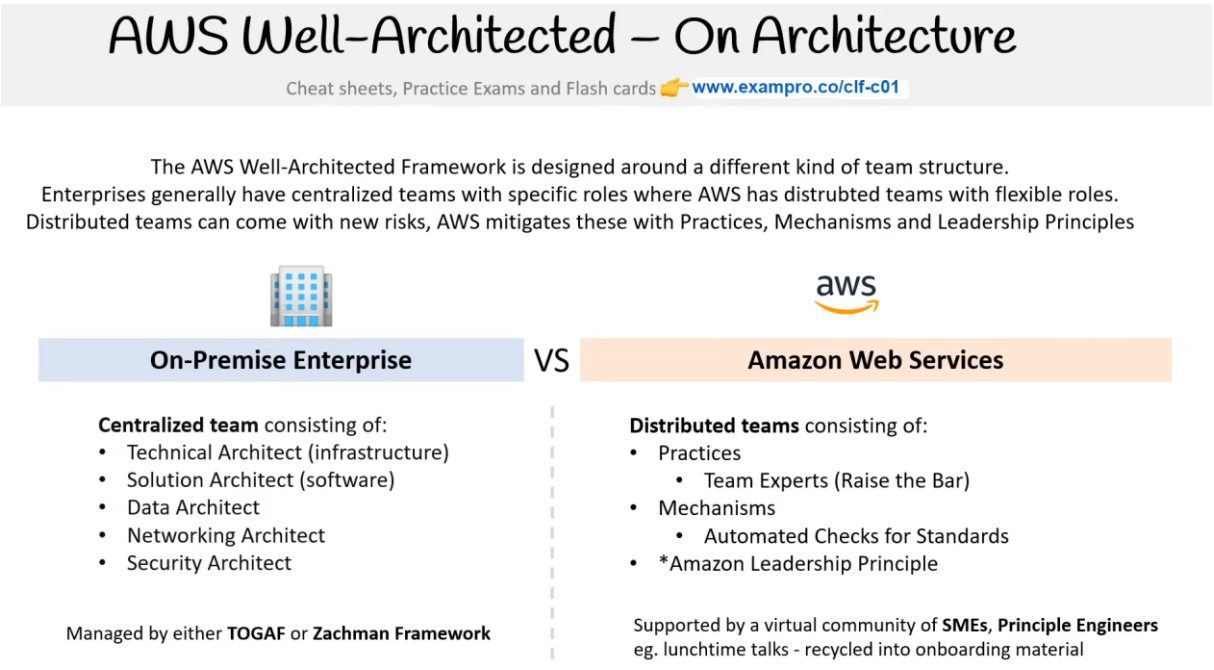
AWS Well-Architected – General Definitions



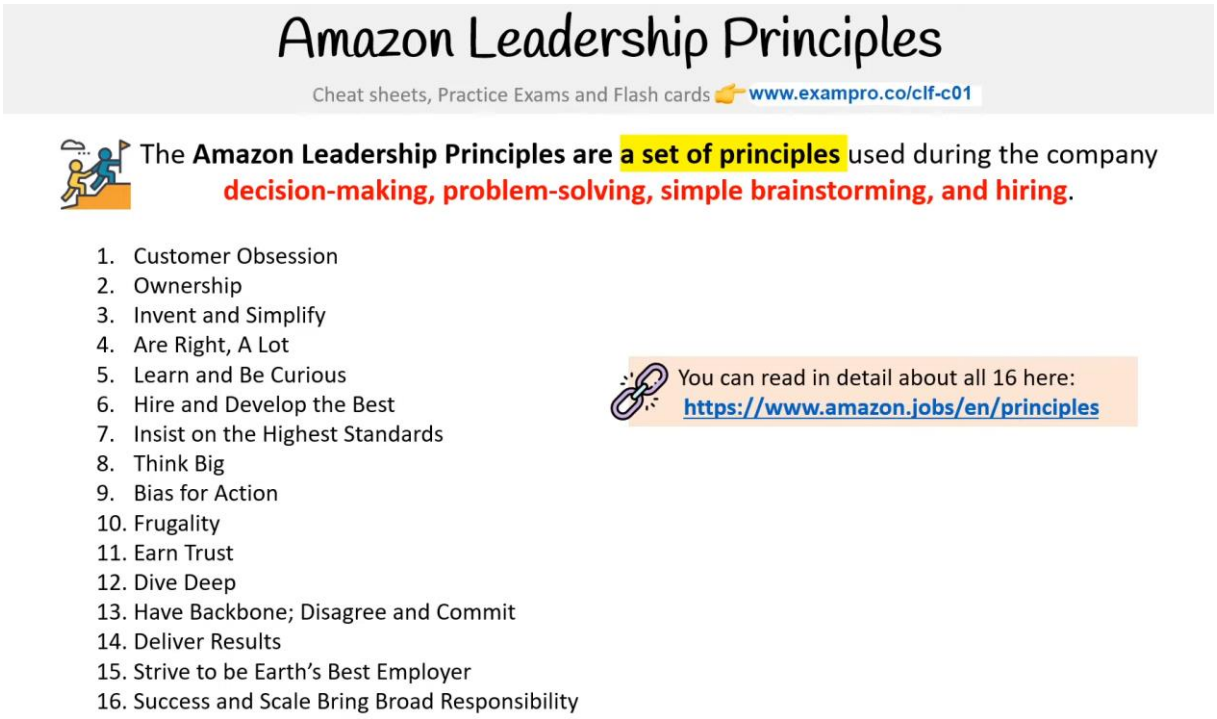
Note: On Dec 2, 2021, AWS introduced a new AWS Well-Architected Sustainability Pillar to help organizations learn, measure, and improve workloads using environmental best practices for cloud computing.

Reference - AWS Well-Architected | New Sustainability Pillar for the AWS Well-Architected Framework

AWS Well-Architected – On Architecture



Amazon Leadership Principles



You can read in detail about all 16 here:

https://www.amazon.jobs/en/principles

Reference - Leadership Principles

AWS Well-Architected – General Design Principles

Stop guessing your capacity needs
eg. Cloud computing you use as little or much based **on demand.**

Test systems at production scale
eg. Clone production env to testing, Tear down testing not in use to save money.

Automate to make architectural experimentation easier
eg. Using CloudFormation with ChangeSets, StackUpdate and Drift Detection

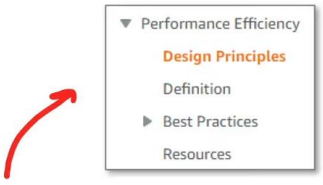
Allow for evolutionary architectures
eg. CI/CD, rapid or nightly releases, Lambdas deprecating run-times forcing you to evolve

Drive architectures using data
eg. CloudWatch, Cloud Trail automatically turned on collecting data

Improve through game days
eg. simulate traffic on production or purposely kill EC2 instances to see test recovery

Reference - [AWS Well-Architected]

WS Well-Architected - Anatomy of a Pillar



Performance Efficiency

A Pillar of the Well-Architected Framework is **structured** as follows:

- Design Principles
  - A list of design principles that need to be considered during implementation
- Definition
  - overview of the best practice categories
- Best Practices
  - detailed information about each best practice with AWS Services
- Resources
  - Additional documentation, whitepapers and videos to implement this pillar

AWS Well-Architected - Design Principles

AWS Well-Architected – Design Principles

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

Operational Excellence Design Principles

Perform operations as code
Apply the same engineering discipline you would to application code to your cloud infrastructure.
By treating your operations as code you can limit human error and enable consistent responses to events.
eg. Infrastructure as Code

Make frequent, small, reversible changes
Design workloads to allow components to be updated regulary.
eg. rollbacks, incremental changes, Blue/Green, CI/CD

Refine operations procedures frequently
Look for continuous opportunities to improve your operations
eg. Use game days to simulate traffic or event failure on your production workloads

Anticipate failure
Perform post-mortems on system failures to better improve, write test code, kill production serves to test recovery

Learn from all operational failures
share lessons learned in a knowledge base for operational events and failures across your entire organization

AWS Well-Architected - Design Principles

AWS Well-Architected – Design Principles

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

Security Design Principles

Implement a strong identity foundation
Implement Principle of Least Privilege (PoLP). Use Centralized identity. Avoid Long-lived credentials

Enable traceability
Monitor alert and audit actions and changes to your environment in real-time
Integrate log and metric collection and automate investigation and remediation

Apply security at all layers
Take Defense in depth approach with multiple security controls for everything eg. Edge Network, VPC, Load Balancing Instances, OS, Application Code

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events
Incident management systems and investigation policy and processes. Tools to detect, investigate and recover from incidences

AWS Well-Architected - Design Principles

AWS Well-Architected – Design Principles

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

Reliability Design Principles

Automatically recover from failure
Monitor Key Performance Indicators (KPIs) and trigger automation when threshold is breached.

Test recovery procedures
Test how your workload fails, and you validate your recovery procedures.
You can use automation to simulate different failures or to recreate scenarios that led to failures before.

Scale horizontally to increase aggregate system availability
Replace one large resource with multiple small resources to reduce the impact of a single failure on the overall workload.
Distribute requests across multiple, smaller resources to ensure that they don't share a common point of failure.

Stop guessing capacity
In on-premise it takes a lot of guess work to determine the elasticity of your workload demands.
With Cloud you don't need to guess how much you need because you can request the right size of resources on-demand.

Manage change in automation
Making changes via Infrastructure as Code, will allow for a formal process to track and review infrastructure

AWS Well-Architected - Design Principles

AWS Well-Architected – Design Principles

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

Performance Efficiency Design Principles

Democratize advanced technologies:
Focus on product development rather than procurement, provisioning and management of services.
Take advantage of advanced technology specialized and optimized for your use-case with on-demand cloud services.

Go global in minutes
Deploying your workload in multiple AWS Regions around the world allows you to provide lower latency and a better experience for your customers at minimal cost.

Use serverless architectures:
Serverless architectures remove the need for you to run and maintain physical servers for traditional compute activities.
Removes the operational burden of managing physical servers, and can lower transactional costs because managed services operate at cloud scale.

Experiment more often:
With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.

Consider mechanical sympathy
Understand how cloud services are consumed and always use the technology approach that aligns best with your workload goals. For example, consider data access patterns when you select database or storage approaches.

AWS Well-Architected - Design Principles

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.

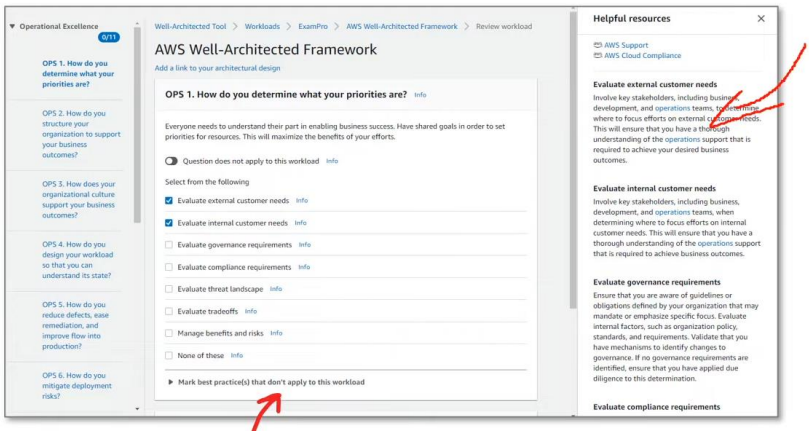
Analyze and attribute expenditure
The cloud makes it easier to accurately identify the usage and cost of systems, which then allows transparent attribution of IT costs to individual workload owners. This helps measure return on investment (ROI) and gives workload owners an opportunity to optimize their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

AWS Well-Architected Tool

AWS Well-Architected Tool

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

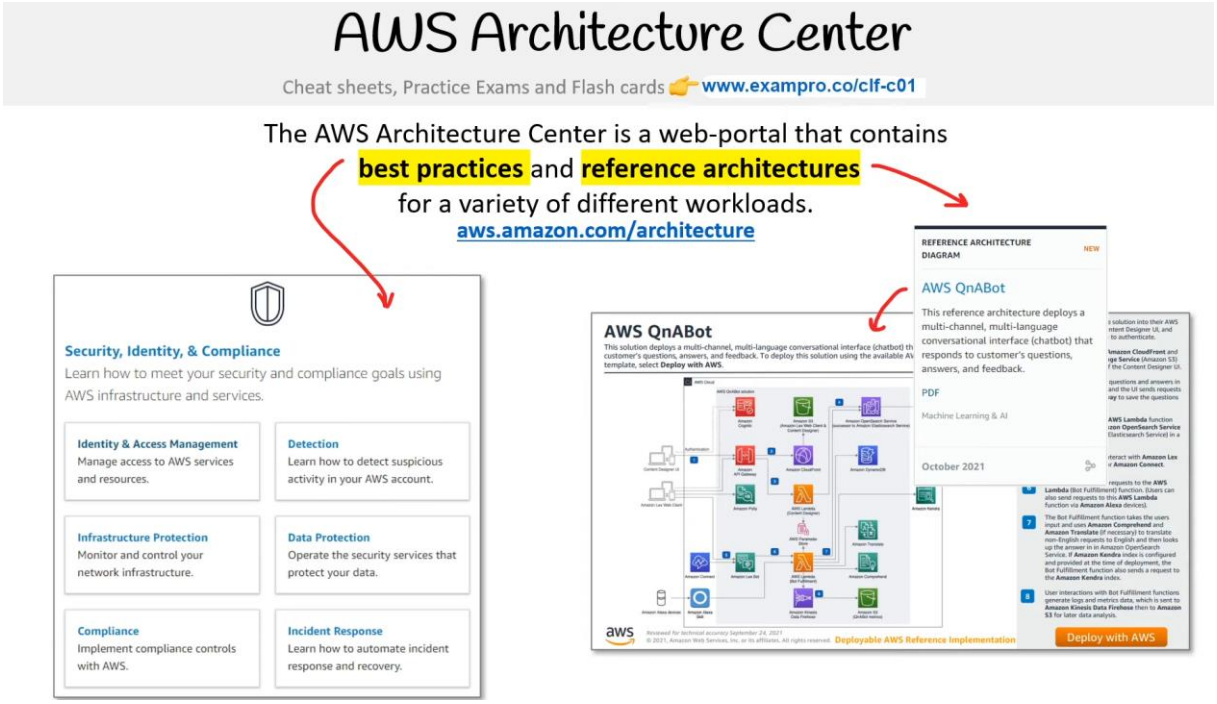
The Well-Architected Tool is **an auditing tool** to be used to asset your cloud workloads for alignment with the AWS Well Architected Framework.



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

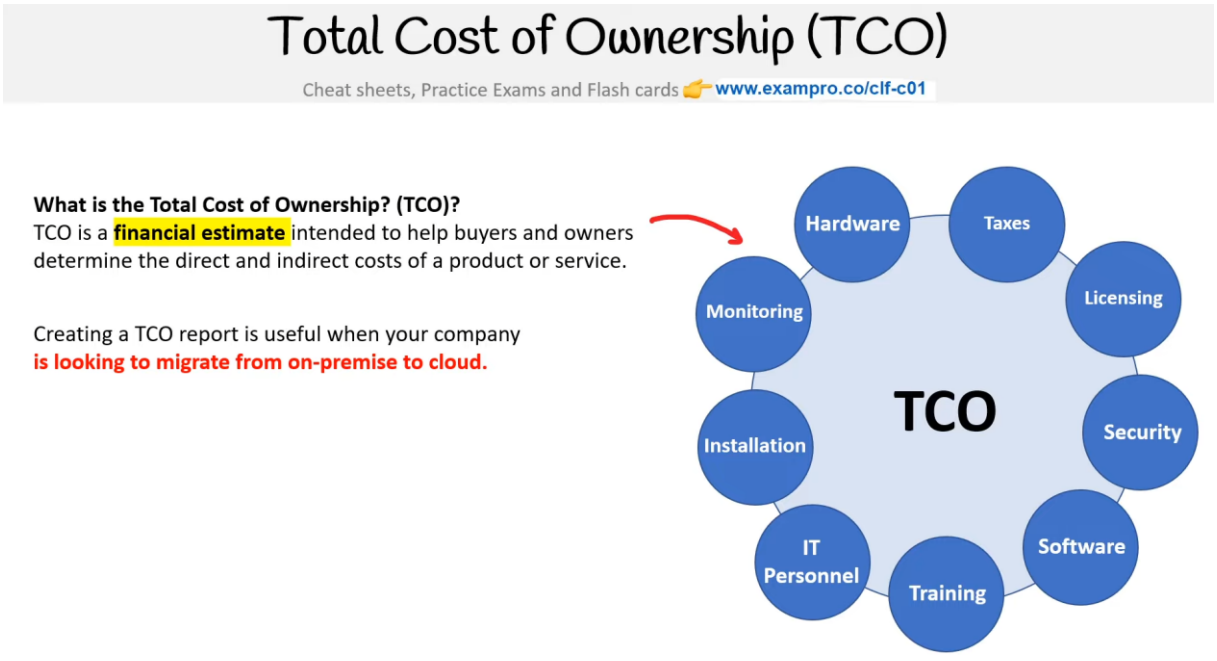
Reference - [AWS Well-Architected]

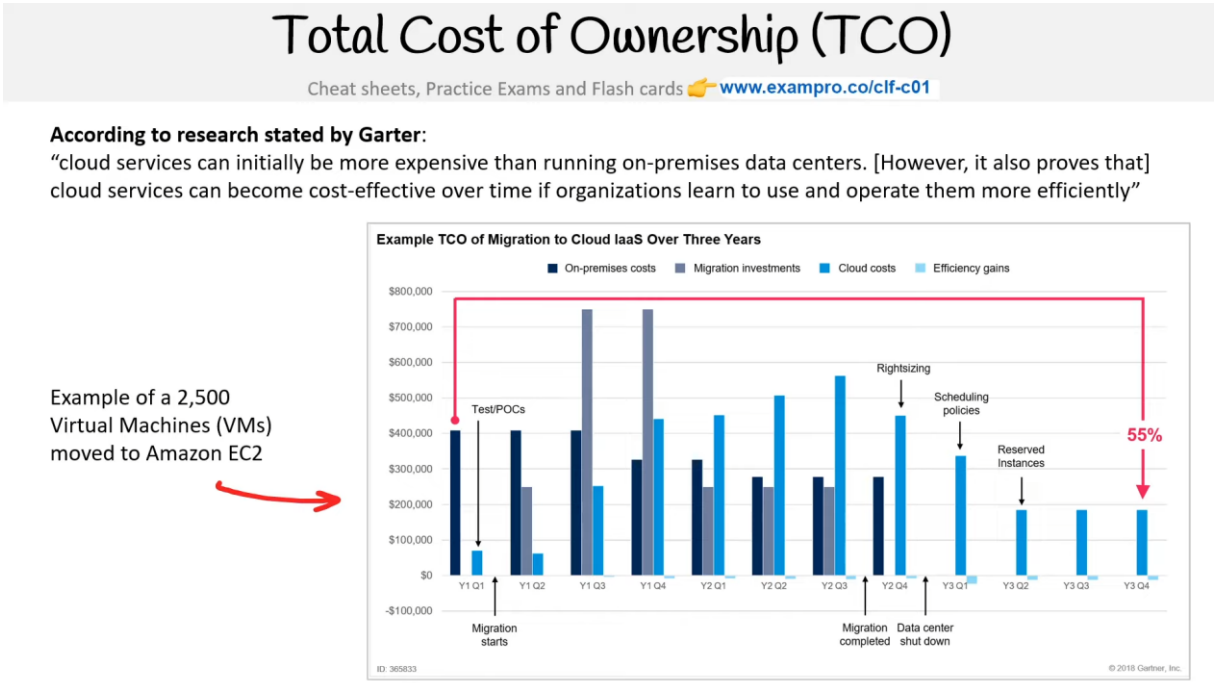
AWS Architecture Center

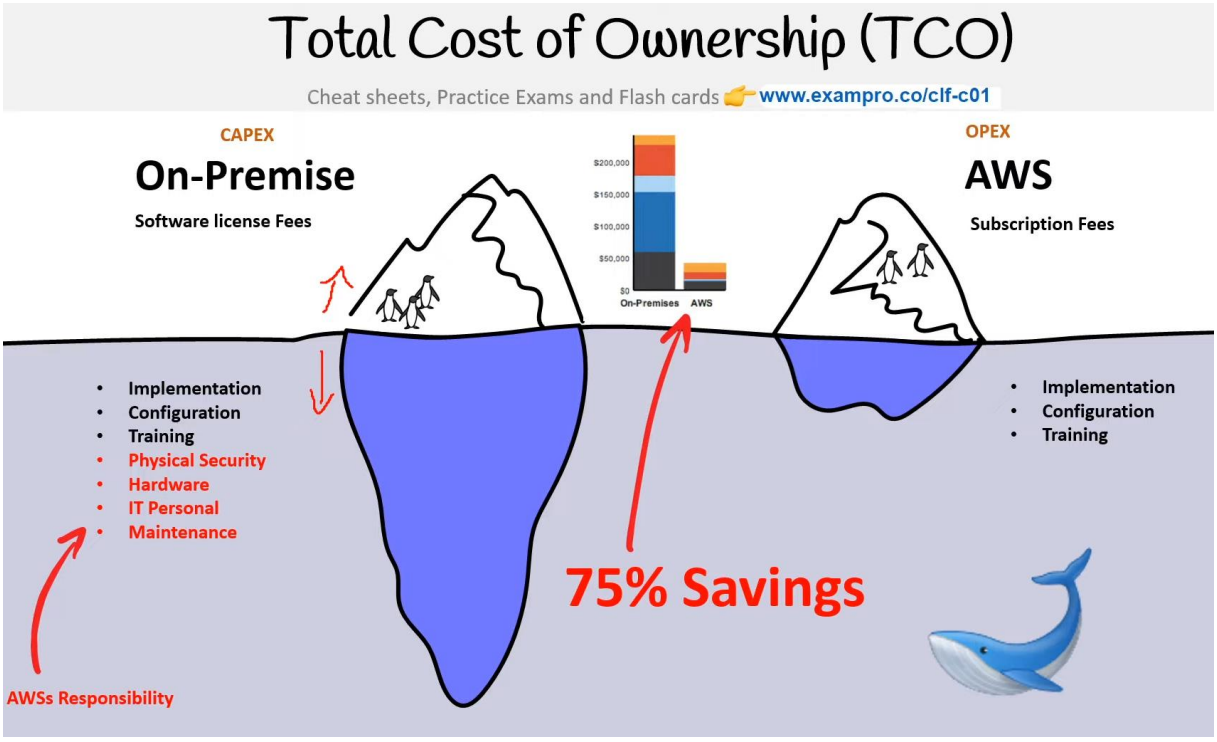


Reference - [AWS Architecture Center]

Total Cost of Ownership (TCO)







What is the Total Cost of Ownership (TCO)?

TCO is a **financial estimate** intended to help buyers and owners determine the direct and indirect costs of a product or service.

Creating a TCO report is useful when your company **is looking to migrate from on-premise to cloud**.

According to research stated by Garter:

“cloud services can initially be more expensive than running on-premises data centers. [However, it also proves that] cloud services can become cost-effective over time if organizations learn to use and operate them more efficiently”

Example of a 2,500 Virtual Machines (VMs) moved to Amazon EC2

CAPEX

On-Premise

Software License Fees

- Implementation
- Configuration
- Training
- Physical Security
- Hardware
- IT Personal
- Maintenance

AWS's Responsibility

OPEX

AWS (75% Savings)

Subscription Fees

- Implementation
- Configuration
- Training

CAPEX vs OPEX

Capital vs Operational Expenditure

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

Capital Expenditure (CAPEX)

Spending money upfront on **physical infrastructure**
Deducting that expense from your tax bill over time.

- Server Costs (computers)
- Storage Costs (hard drives)
- Network Costs (Routers, Cables, Switches)
- Backup and Archive Costs
- Disaster Recovery Costs
- Datacenter Costs (Rent, Cooling, Physical Security)
- Technical Personal

With Capital Expenses **you have to guess upfront** what you plan to spend

Operational Expenditure (OPEX)

The costs associated with an on-premises datacenter that has shifted the cost to the service provider. The customer only has to be concerned with **non-physical costs**.

- Leasing Software and Customizing features
- Training Employees in Cloud Services
- Paying for Cloud Support
- Billing based on cloud metrics eg.
  - compute usage
  - storage usage

With Operation Expenses you can try a product or service **without investing in equipment**

Does Cloud Make IT Personnel Redundant?

Does Cloud Make IT Personnel Redundant?

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

A company is considering migrating their workloads from on-premise to the cloud to take advantage of the savings. There is a concern among the staff that there will be mass layoffs. Does cloud make IT Personnel redundant?

***Shifting* your IT Team**

- A company needs IT personnel during the migration phase
- A company can transition some roles to new cloud roles:
  - Networking to Cloud Networking
- A company may decide to take a Hybrid approach so they'll always need to have a traditional IT team and a Cloud IT Team
- A company can change employees activities from **Managing Infrastructure to Revenue Generating**

AWS Pricing Calculator

AWS Pricing Calculator

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

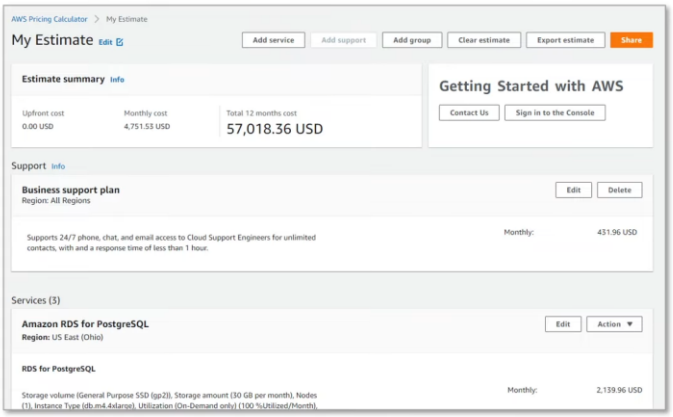
The **AWS Pricing Calculator** is a **free cost estimate tool** that can be used within your **web-browser** without the need for an AWS Account to estimate the cost of a various AWS services.

calculator.aws

The AWS Pricing Calculator contains 100+ services that you can configure for cost estimate.

To calculate Total Cost of Ownership an organization needs to compare their existing cost against the AWS costs and so the AWS Pricing Calculator can be used to determine that cost.

You can export your final estimate to a CSV.



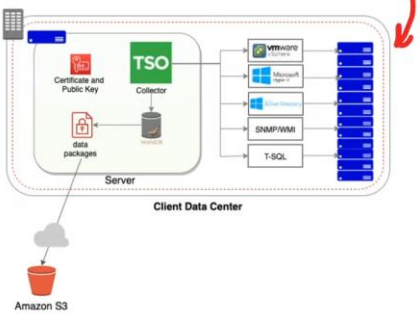
Migration Evaluator

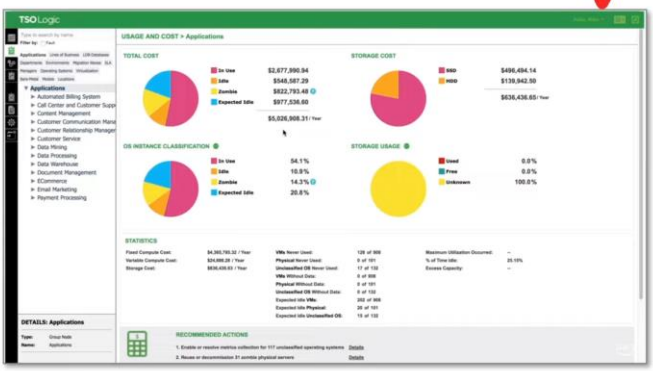
Migration Evaluator

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

AWS Migration Evaluator (formally known as TSO Logic) is an **estimate tool** used to determine an organization existing on-premise cost so it can compare it against AWS Costs for planned cloud migration

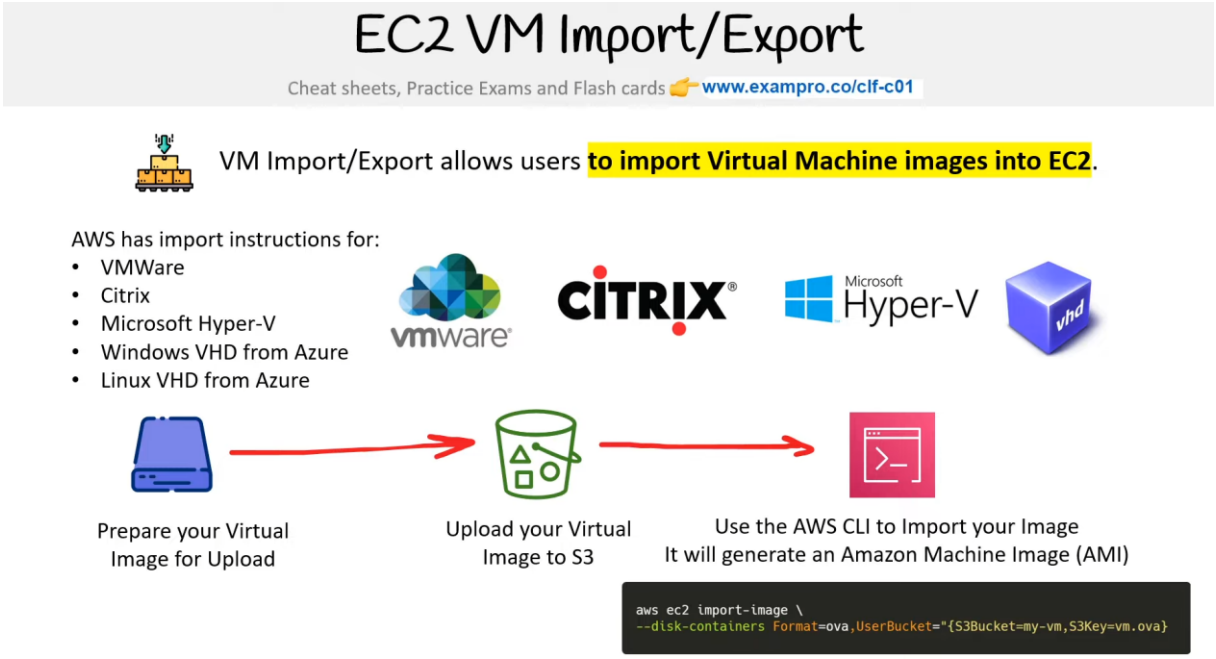
Migration Evaluator uses an **Agentless Collector** to collect data from your on-premise infrastructure to extract your on-premise costs



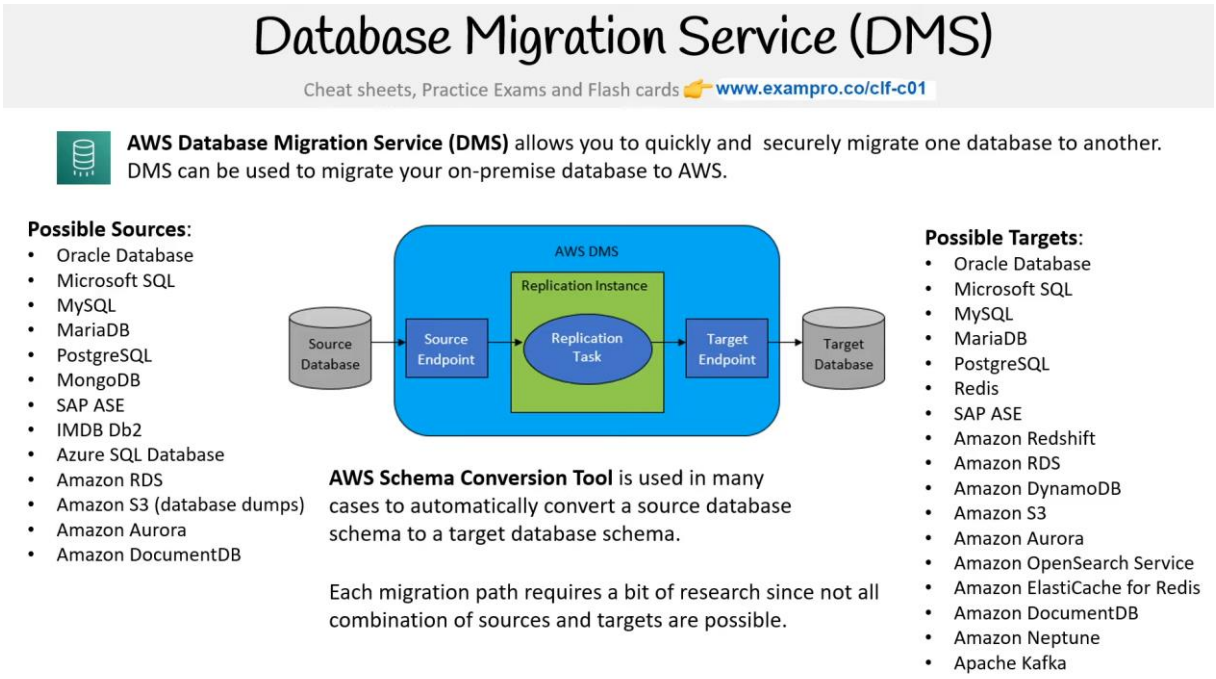


Reference - Migration Evaluator | TSO Logic: Software Demo

EC2 VM Import/Export



Database Migration Service (DMS)



Reference - What is AWS Database Migration Service? | AWS Schema Conversion Tool

AWS Cloud Adoption Framework (CAF)

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.

Reference - AWS Cloud Adoption Framework (AWS CAF) | Introduction

AWS Free Services

AWS Free Services

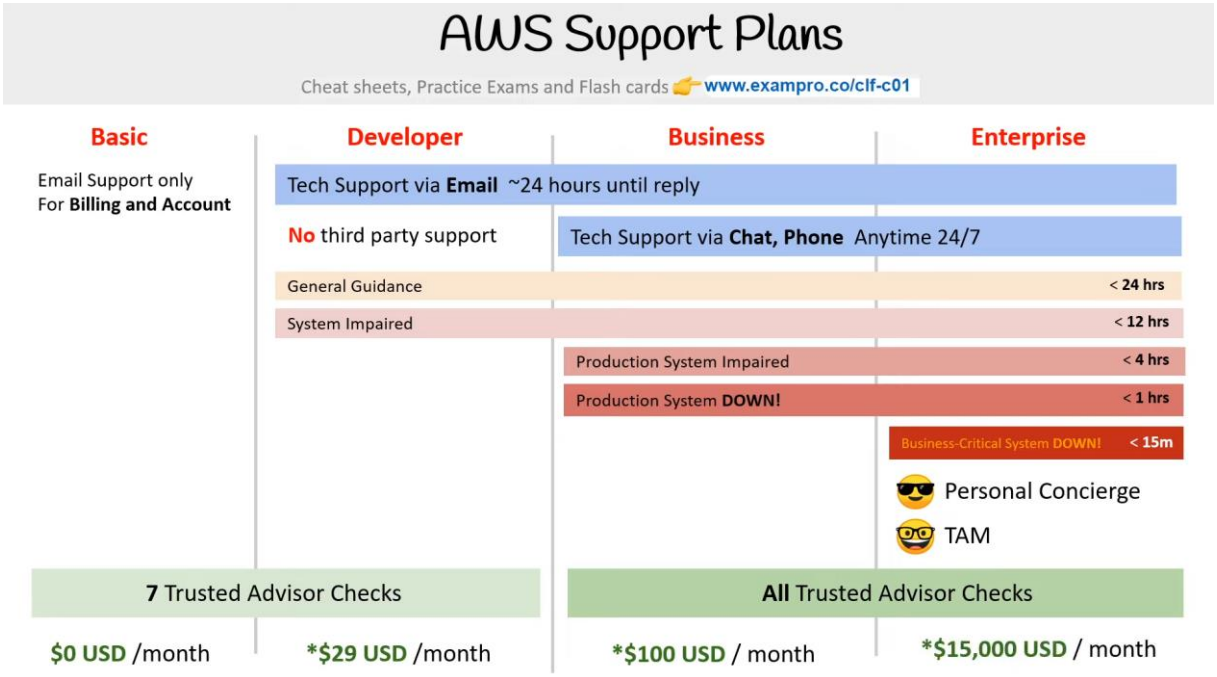
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

AWS Free services are free forever, unlike the "free-tier" that are up to a point of usage or time

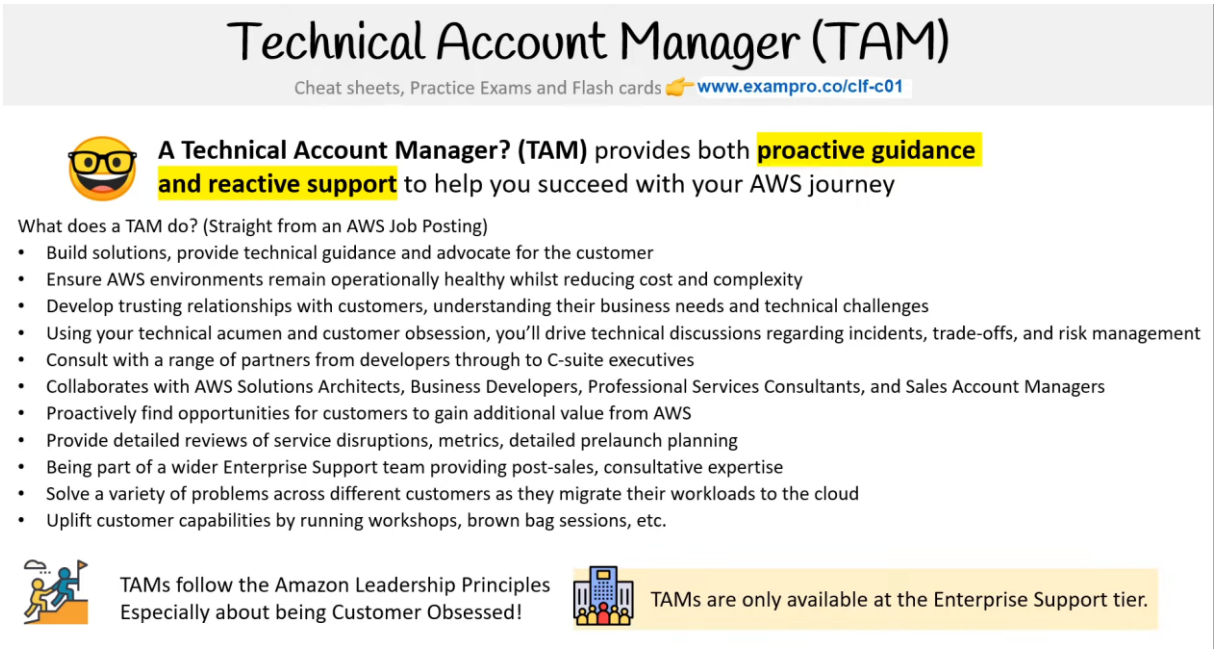
The AWS services are also free. however these AWS Services provision other services which may cost money

- **IAM - Identity Access Management**
- **Amazon VPC**
- **Auto Scaling**
- **CloudFormation**
- **Elastic Beanstalk**
- Opsworks
- Amplify
- AppSync
- CodeStar
- Organizations & Consolidated Billing
- AWS Cost Explorer

AWS Support Plans

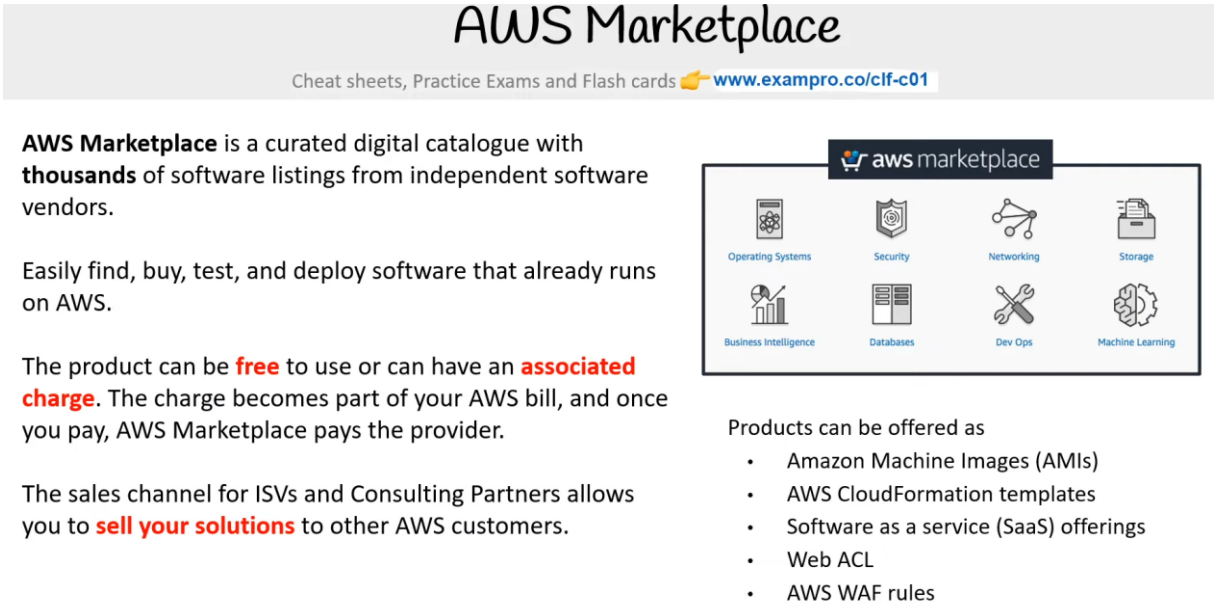


Technical Account Manager (TAM)



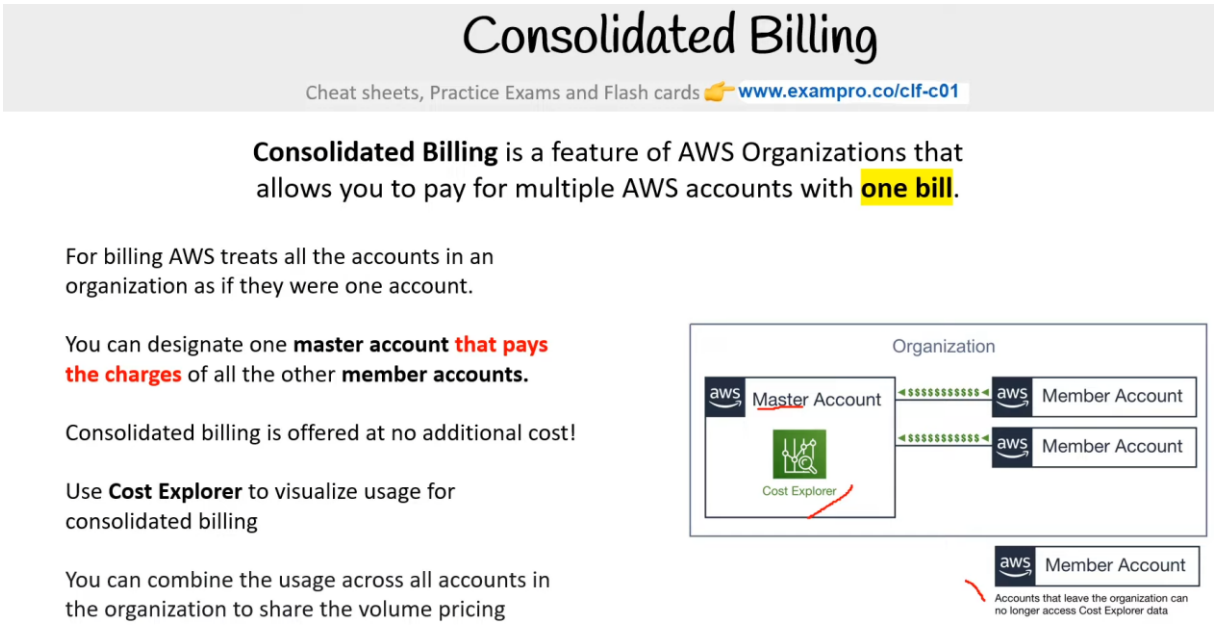
Reference - [Technical Account Manager](#) | [What is the role of a Technical Account Manager? Meet our ANZ Team](#)

AWS Marketplace



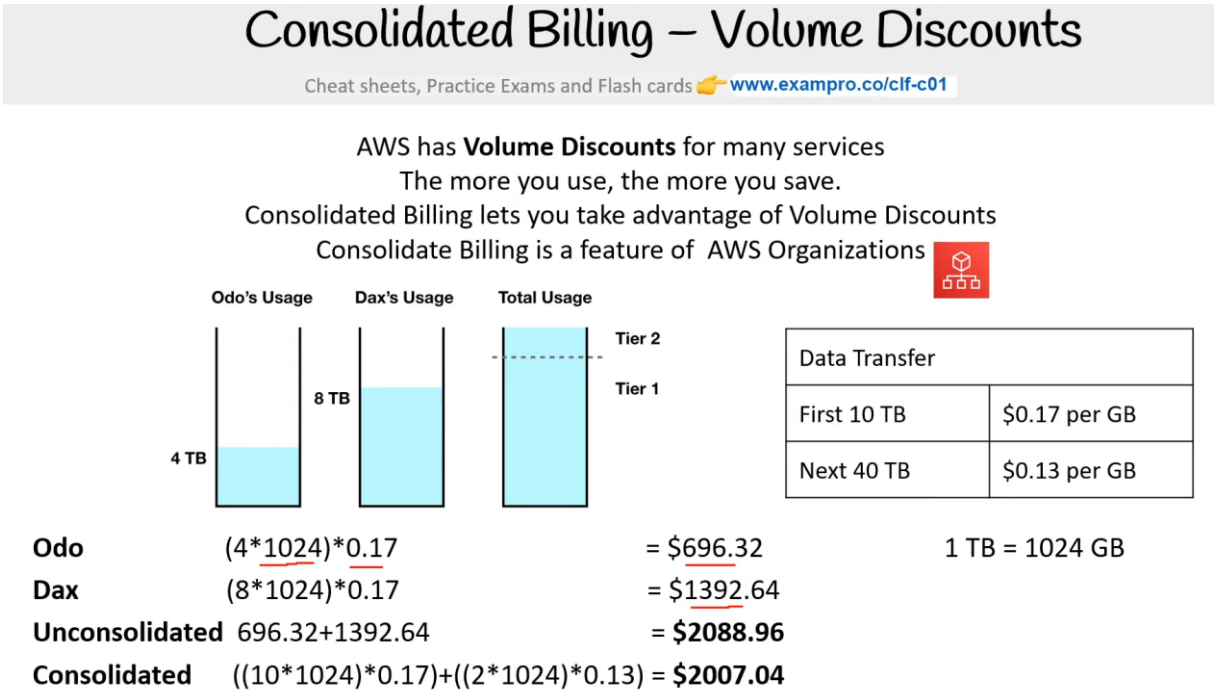
Reference - [What is AWS Marketplace?](#)

Consolidated Billing



Reference - [Consolidated billing for AWS Organizations]

Consolidated Billing – Volume Discounts



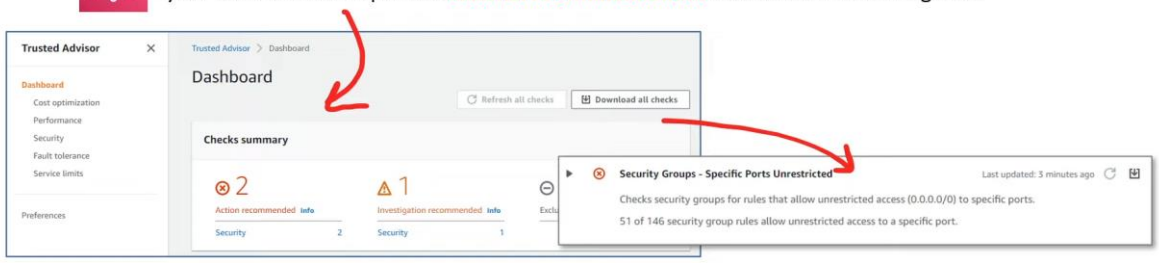
Reference - [Consolidated billing for AWS Organizations]

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

AWS Trusted Advisor providers different level of checks based on your AWS Support Plan

Basic	Developer	Business	Enterprise
7 Trusted Advisor Checks		**All** Trusted Advisor Checks	

AWS providers the following checks for free:

1. MFA on Root Account
2. Security Groups – Specific Ports of Unrestricted
3. Amazon S3 Bucket Permissions
4. Amazon EBS Public Snapshots
5. Amazon RDS Public Snapshots
6. IAM Use - discourage the use of root access
7. Service Limits (All Service limits checks are free)

Six security checks

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

AWS Trusted Advisor

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

Fault Tolerance

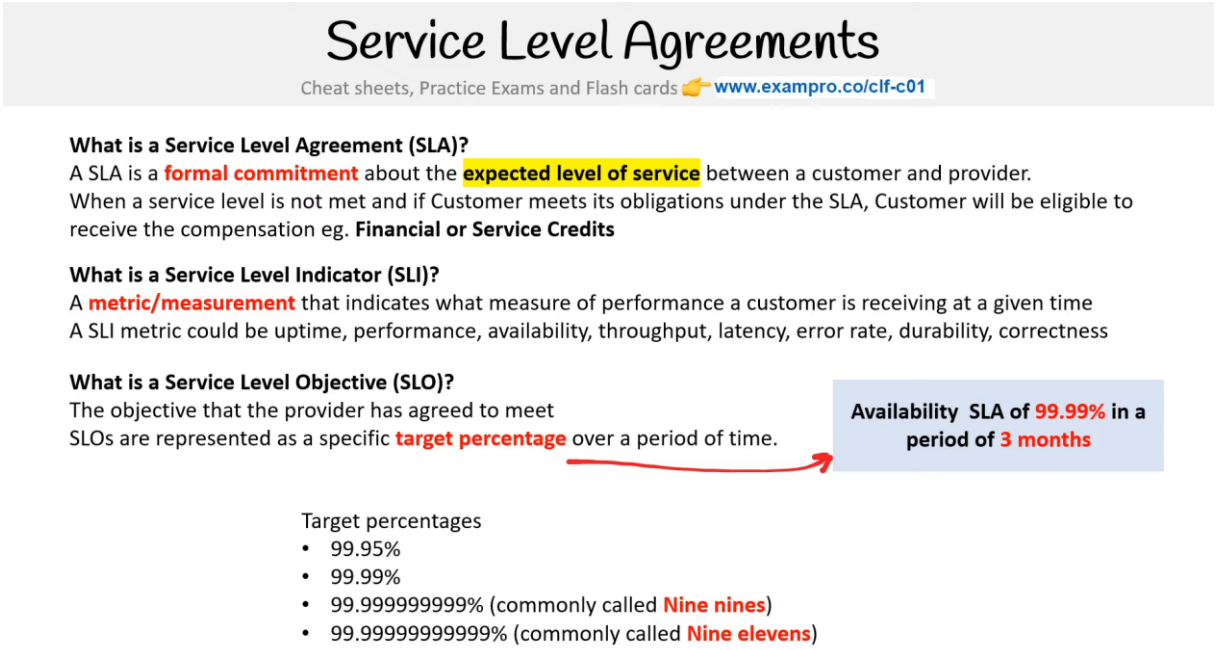
Amazon EBS Snapshots
Amazon RDS Multi-AZ
Amazon S3 Bucket Logging
Amazon S3 Bucket Versioning
Amazon Aurora DB Instance Accessibility
Amazon EC2 Availability Zone Balance
Amazon RDS Backups
Amazon Route 53 Deleted Health Checks
Amazon Route 53 Failover Resource Record Sets
Amazon Route 53 High TTL Resource Record Sets
Amazon Route 53 Name Server Delegations
Auto Scaling Group Health Check
Auto Scaling Group Resources
ELB Connection Draining
ELB Cross-Zone Load Balancing
Load Balancer Optimization
VPN Tunnel Redundancy
AWS Direct Connect Connection Redundancy
AWS Direct Connect Location Redundancy
AWS Direct Connect Virtual Interface Redundancy
EC2Config Service for EC2 Windows Instances
ENA Driver Version for EC2 Windows Instances
NVMe Driver Version for EC2 Windows Instances

Service Limits

Auto Scaling Groups
Auto Scaling Launch Configurations
CloudFormation Stacks
DynamoDB Read Capacity
DynamoDB Write Capacity
EBS Active Snapshots
EBS Active Volumes
EBS Cold HDD (sc1) Volume Storage
EBS General Purpose SSD (gp2) Volume Storage
EBS Magnetic (standard) Volume Storage
EBS Provisioned IOPS (SSD) Volume Aggregate IOPS
EBS Provisioned IOPS SSD (io1) Volume Storage
EBS Throughput Optimized HDD (st1) Volume Storage
EC2 Elastic IP Addresses
EC2 On-Demand Instances
EC2 Reserved Instance Leases
ELB Active Load Balancers
IAM Group
IAM Instance Profiles
IAM Policies
IAM Roles
IAM Server Certificates
IAM Users
Kinesis Shards per Region
RDS Cluster Parameter Groups
RDS Cluster Roles
RDS Clusters
RDS DB Instances
RDS DB Parameter Groups
RDS DB Security Groups
RDS DB Snapshots Per User
RDS Event Subscriptions
RDS Max Auths per Security Group
RDS Option Groups
RDS Read Replicas per Master
RDS Reserved Instances
RDS Subnet Groups
RDS Subnets per Subnet Group
RDS Total Storage Quota
Route 53 Hosted Zones
Route 53 Max Health Checks
Route 53 Reusable Delegation Sets
Route 53 Traffic Policies
Route 53 Traffic Policy Instances
SES Daily Sending Quota
VPC
VPC Elastic IP Address
VPC Internet Gateways

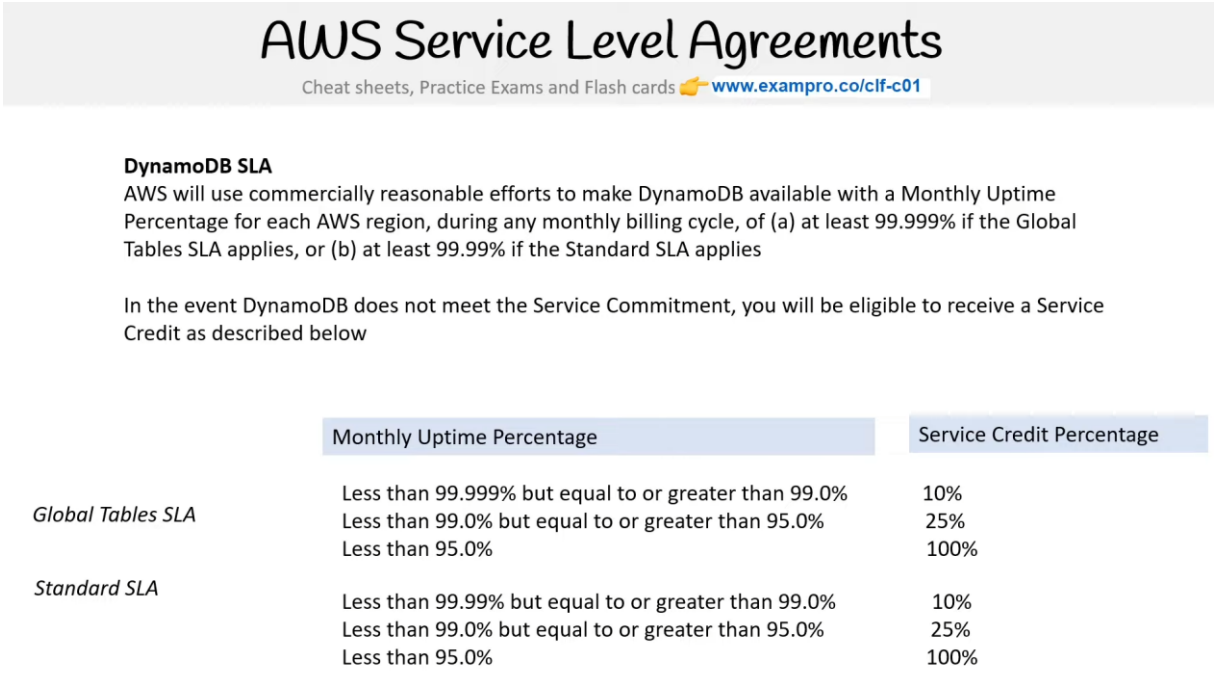
Reference - [AWS Trusted Advisor check reference]

Service Level Agreements



Reference - [SLA vs. SLO vs. SLI: What's the difference?]

AWS Service Level Agreements



AWS Service Level Agreements

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

Compute SLAs

- Amazon Elastic Compute Cloud (Amazon EC2)*
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate for Amazon ECS and Amazon EKS

AWS makes two SLA commitments for the Included Services:

1. a Region-Level SLA that governs Included Services deployed across multiple AZs or regions, and
2. an Instance-Level SLA that governs Amazon EC2 instances individually.

	Monthly Uptime Percentage	Service Credit Percentage
Region-Level SLA	Less than 99.99% but equal to or greater than 99.0%	10%
	Less than 99.0% but equal to or greater than 95.0%	30%
	Less than 95.0%	100%
Instance-Level SLA	Less than 99.5% but equal to or greater than 99.0%	10%
	Less than 99.0% but equal to or greater than 95.0%	30%
	Less than 95.0%	100%

AWS Service Level Agreements

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

RDS SLA

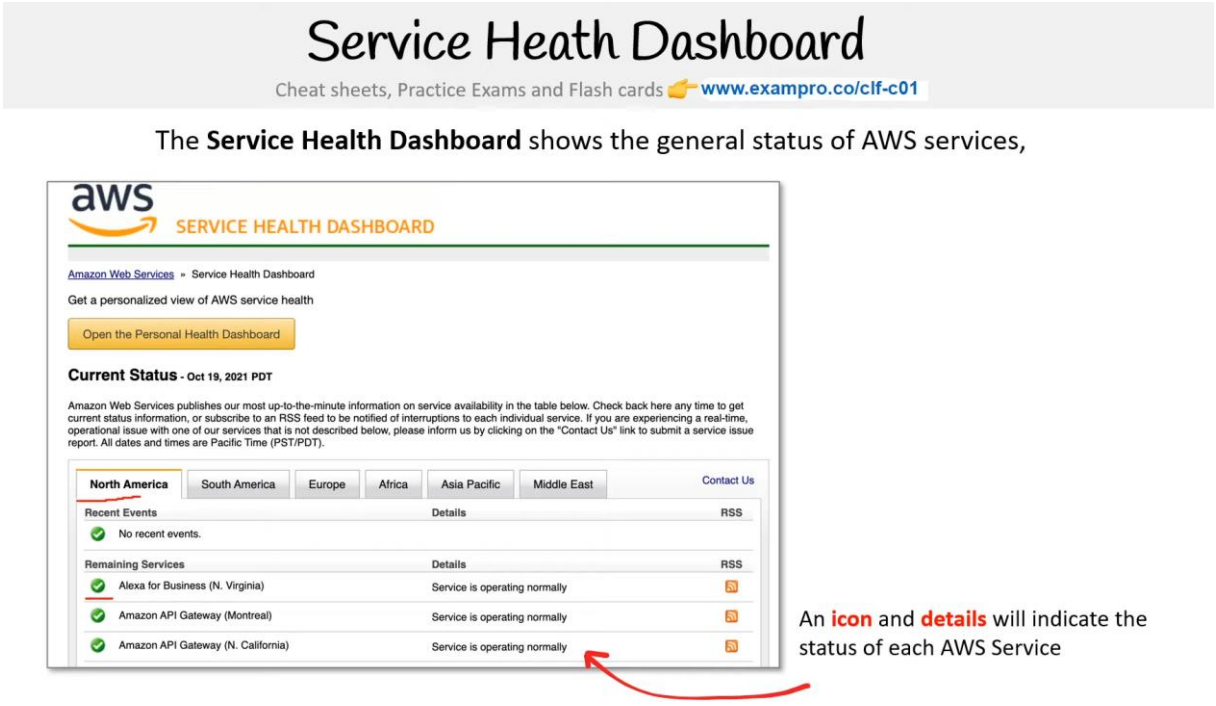
AWS will use commercially reasonable efforts to make Multi-AZ instances available with a Monthly Uptime Percentage of at least 99.95% during any monthly billing cycle

In the event Amazon RDS does not meet the Monthly Uptime Percentage commitment, you will be eligible to receive a Service Credit as described below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

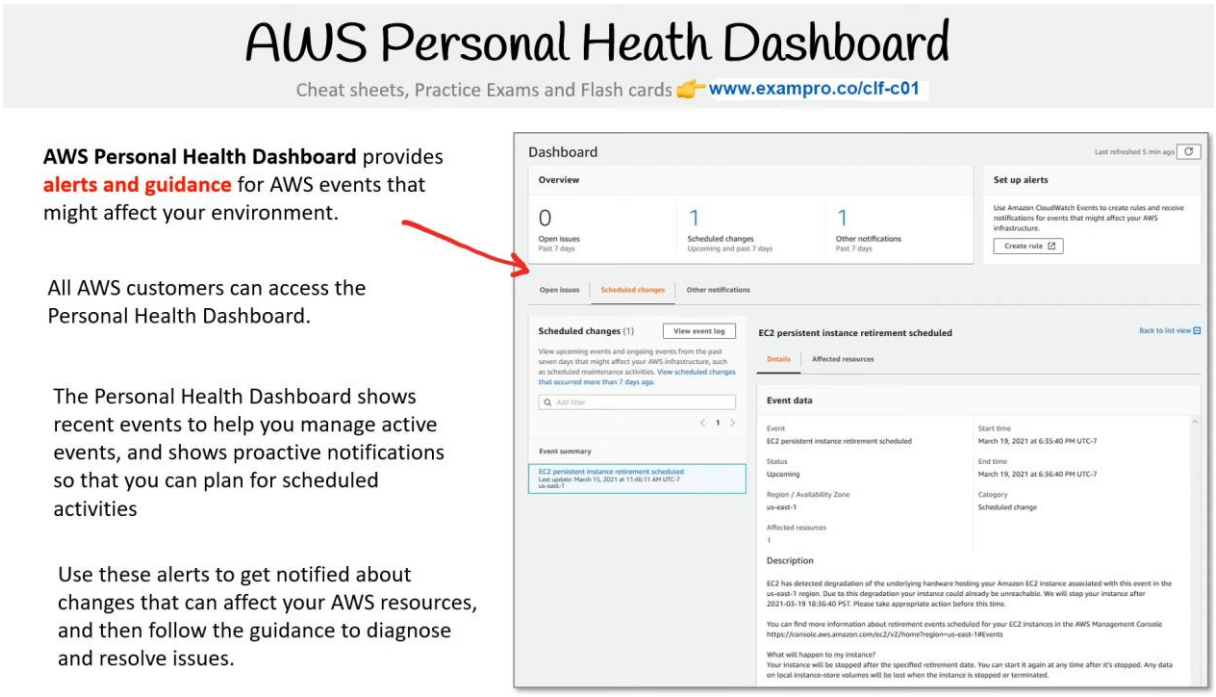
Reference - AWS Service Level Agreements (SLAs) | Amazon DynamoDB Service Level Agreement | Amazon Compute Service Level Agreement

Service Heath Dashboard



Reference - [AWS Personal Health Dashboard]

AWS Personal Health Dashboard



Reference - [Automating processes for handling and remediating AWS Abuse alerts] | [AWS Personal Health Dashboard]

AWS Abuse

AWS Abuse

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

AWS Trust & Safety is a team that specifically deals with abuses occurring on the AWS platform for the following issues:

Spam
You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are used to spam websites or forums.

Port scanning
Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server. You also believe this is an attempt to discover unsecured ports.

Denial-of-service (DoS) attacks
Your logs show that one or more AWS-owned IP addresses are used to flood ports on your resources with packets. You also believe that this is an attempt to overwhelm or crash your server or the software running on your server.

Intrusion attempts:
Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.

Hosting prohibited content:
You have evidence that AWS resources are used to host or distribute prohibited content, such as illegal content or copyrighted content without the consent of the copyright holder.

Distributing malware
You have evidence that AWS resources are used to distribute software that was knowingly created to compromise or cause harm to computers or machines that it's installed on.

AWS Support does not deal with Abuse tickets. You need to contact abuse@amazonaws.com or fill out the Report Amazon AWS abuse form.

Reference - [Automating processes for handling and remediating AWS Abuse alerts](#) | [How do I report abuse of AWS resources?](#) | [Report Amazon AWS abuse](#)

AWS Free-Tier

AWS Free-Tier

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

AWS has a free-tier which allows you to use AWS at no cost
- for the first 12 months of signup
- Or free usage up to a certain monthly limit forever

The Best Deals

EC2 Web Server
t2.micro 750 hours per month for 1 year

RDS Database (MySQL or Postgres)
t2.db.micro 750 hours per month for 1 year

ELB Load Balancer
750 hours per month for 1 year

Amazon CloudFront Homepage Video
50 GB data-transfer out in total for 1 year

Amazon Connect Toll Free Number
90 minutes of call-time per month for 1 year

Amazon ElastiCache Caching
cache.t3.micro 750 hours per month for 1 year

Amazon ElasticSearch Service Full Text Search
750 hours per month for 1 year

PinPoint Campaign / Marketing Emails
5,000 targeted users per month for 1 year

SES Emails sent by your web-application
62,000 emails per month forever

AWS CodePipeline CI/CD
1 Pipeline free

AWS CodeBuild Building Code
100 build minutes per month forever

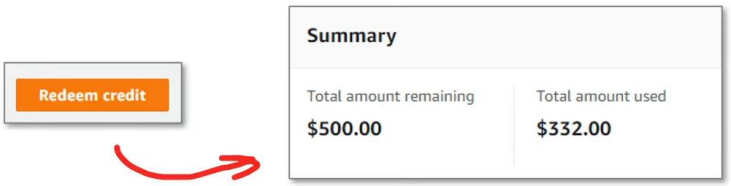
AWS Lambda Serverless Compute
1M free request per month
3.2M seconds of compute time per month

Reference - [AWS Free Tier]

AWS Credits

AWS Promotional Credits (or AWS Credits for short) are the equivalent to USD dollars on the AWS platform. AWS Credits can be earned several ways:

- Joining the AWS Activate startup program
- Winning Hackathons
- Participating in Surveys
- ...

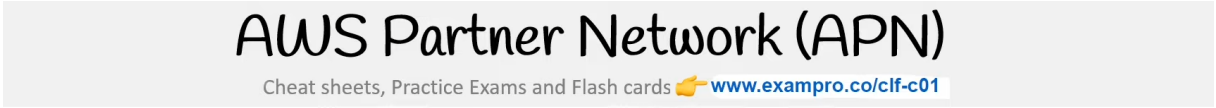


AWS Credits generally have an expiry date attached to them.

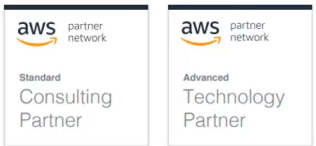
AWS Credits can be used for most services but there are exceptions where AWS Credits cannot be used eg. Purchasing a domain via Route53

Reference - [AWS credits]

AWS Partner Network (APN)



The AWS Partner Network (APN) is a global partner program for AWS.
Joining the APN will open your organization up to business opportunities and allows exclusives trainings and marketing events

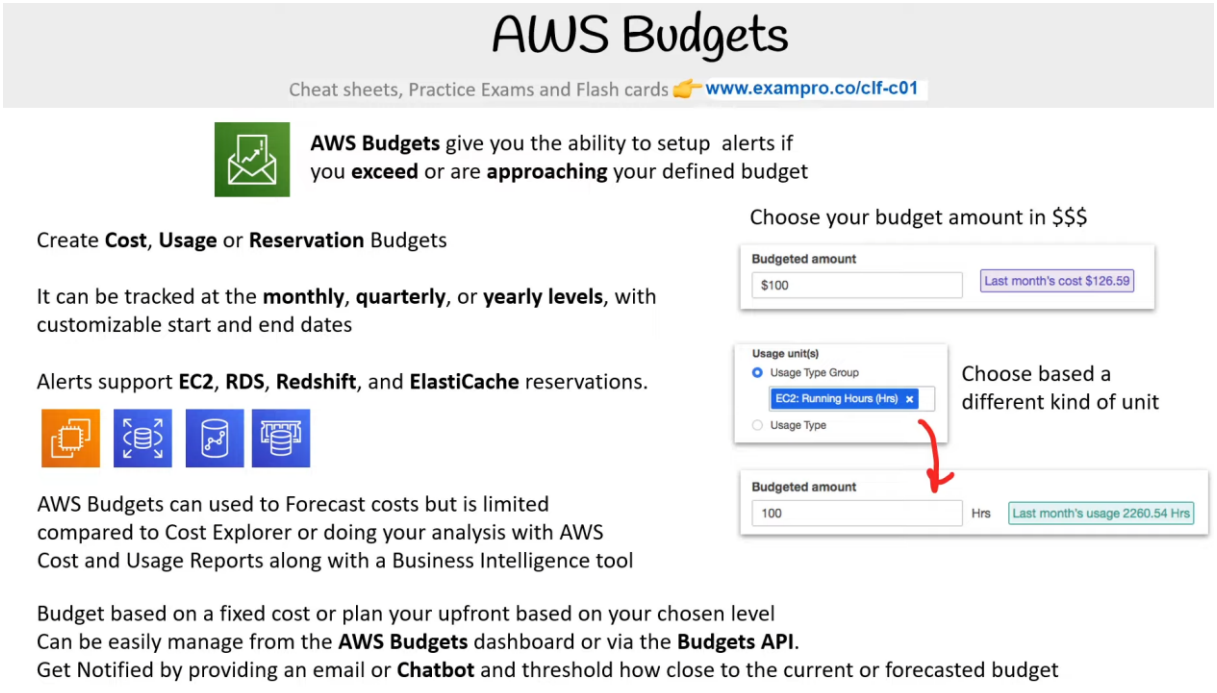


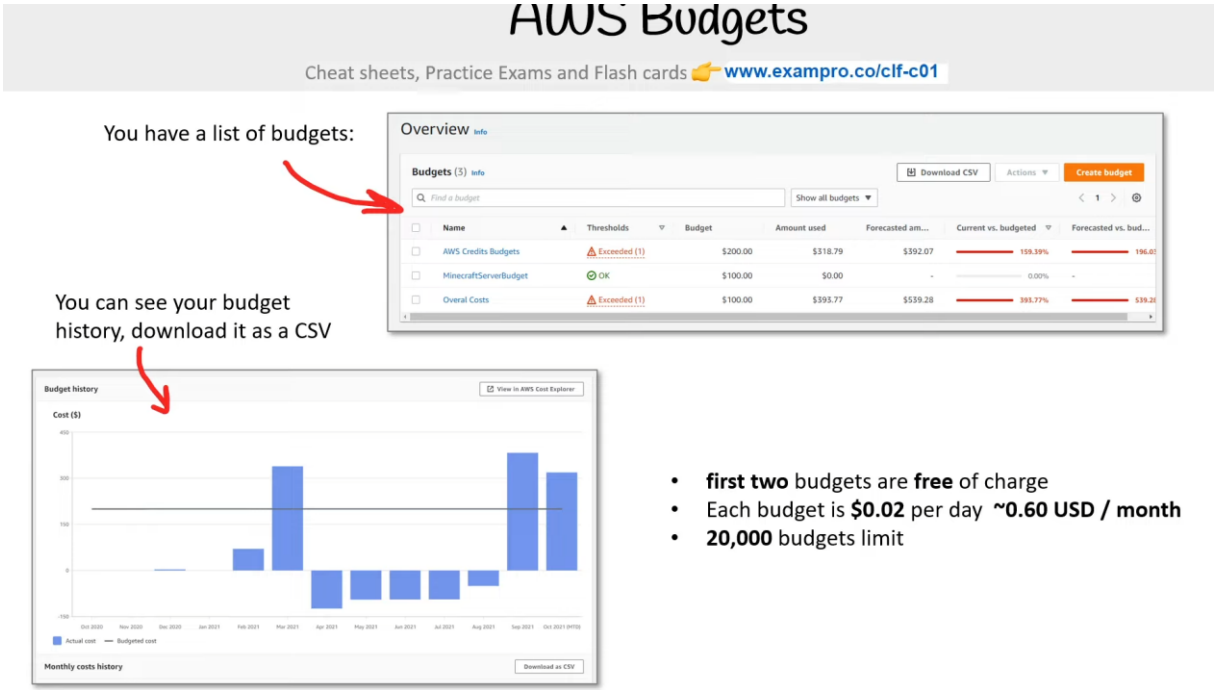
When joining the APN you can either be a:
Consulting Partner – you help companies utilize AWS
Technology Partner – you build technology ontop of AWS as a service offering

- A partner belongs to a specific Tier: Select, Advanced or Premier
- Different tiers have different Annual fee commitments
- Different tiers have different Knowledge requirements
  - AWS Certification
  - AWS APN-Exclusive Certifications
- You can get back Promotional AWS Credits
- You can have unique speaking opportunities in the official AWS marketing channels. Eg blogs, webinars
- Being part of the APN is a requirement to be a Sponsor with a vendor booth at AWS Events

Reference - [AWS Partner Network](#) | [Why AWS Partner Network Badges Matter for Customers and APN Partners](#) | [AWS Consulting Partners](#)

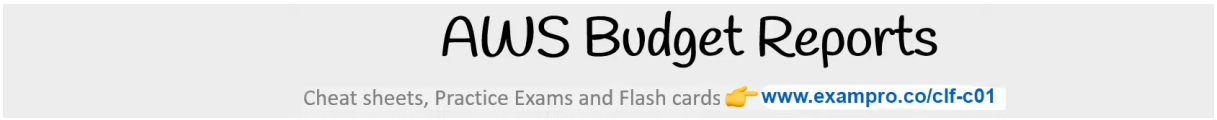
AWS Budgets



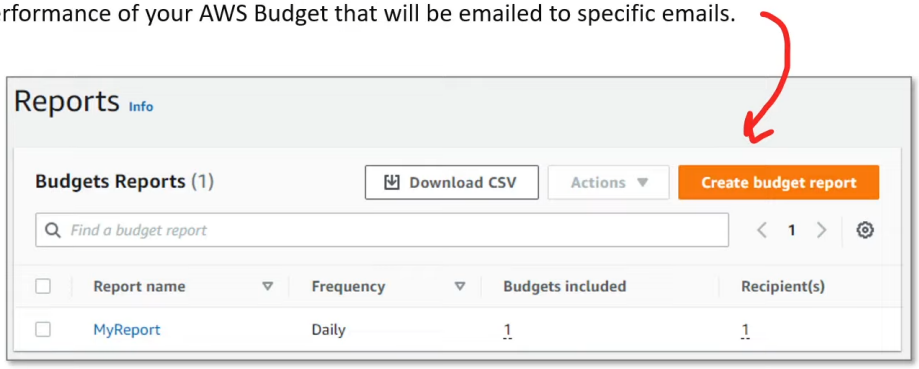


Reference - [AWS Budgets](#)

AWS Budget Reports



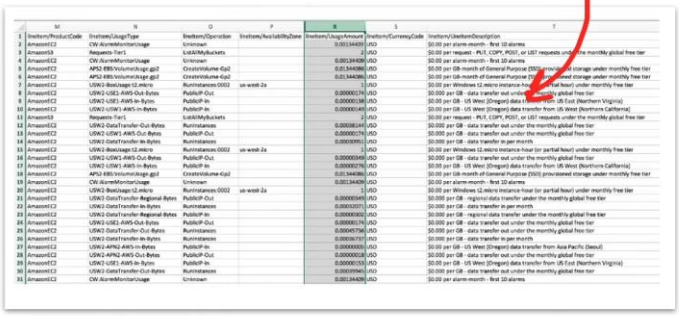
AWS Budget Report is used alongside AWS Budgets to create and send daily, weekly, or monthly reports to monitor the performance of your AWS Budget that will be emailed to specific emails.



AWS Budget Reports serve as a more convenient way of staying on top of reports since they are delivered to your email instead of logging into the AWS Management Console

AWS Cost and Usage Reports (CUR)

Generate a **detailed spreadsheet**, enabling you to **better analyze and understand your AWS costs**



choose the granularity of your data by selecting hourly, daily or monthly

The report will contain Cost Allocation Tags

CUR data is stored in a CSV (GZIP) or Parquet format in your selected S3 bucket

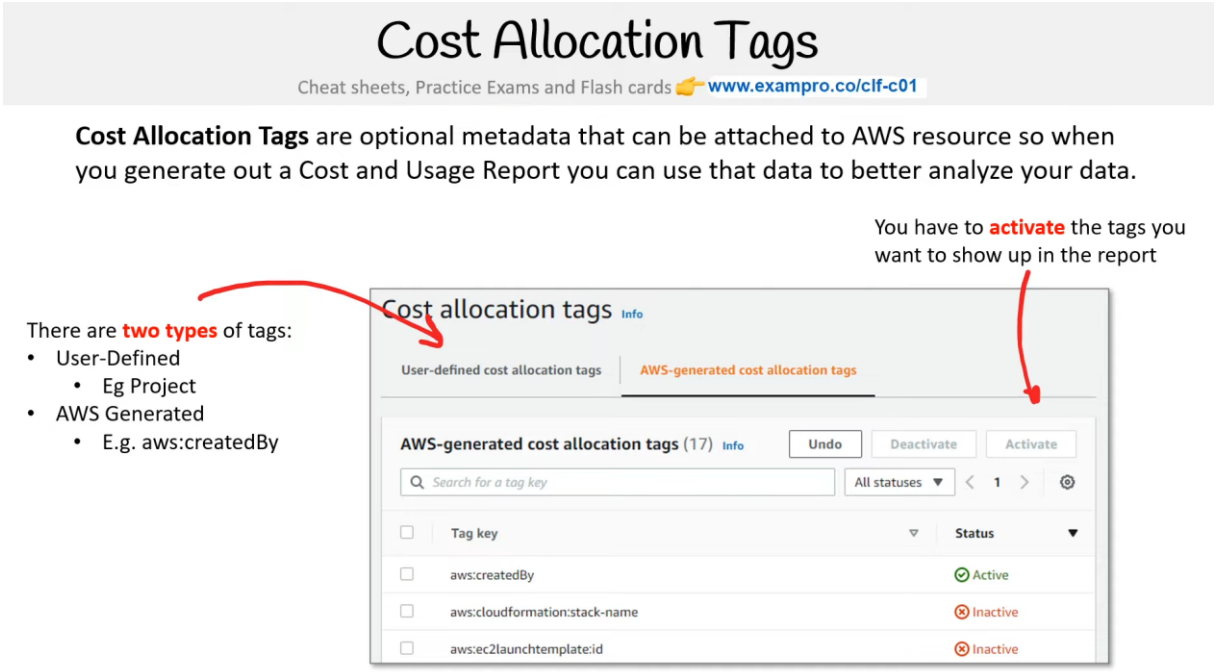
Places the reports into S3

Use Athena to turn the report into a queryable database

Use QuickSight to visualize your billing data as graphs

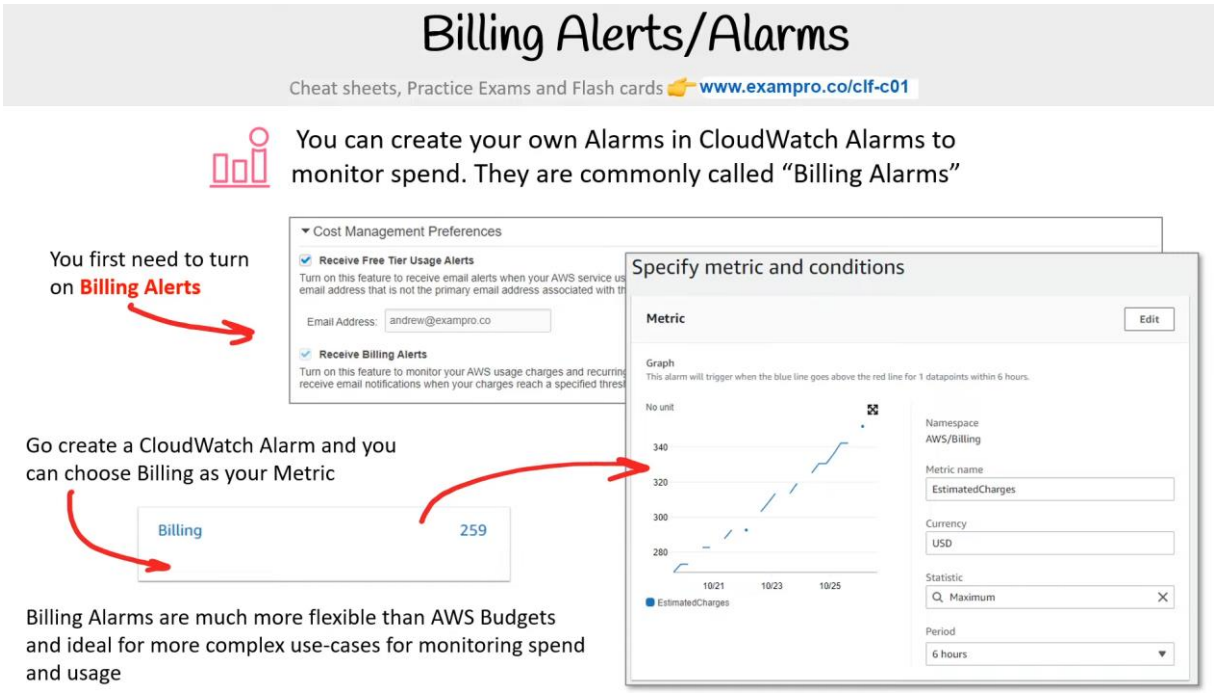
Reference - Amazon EC2 Reserved Instances

Cost Allocation Tags

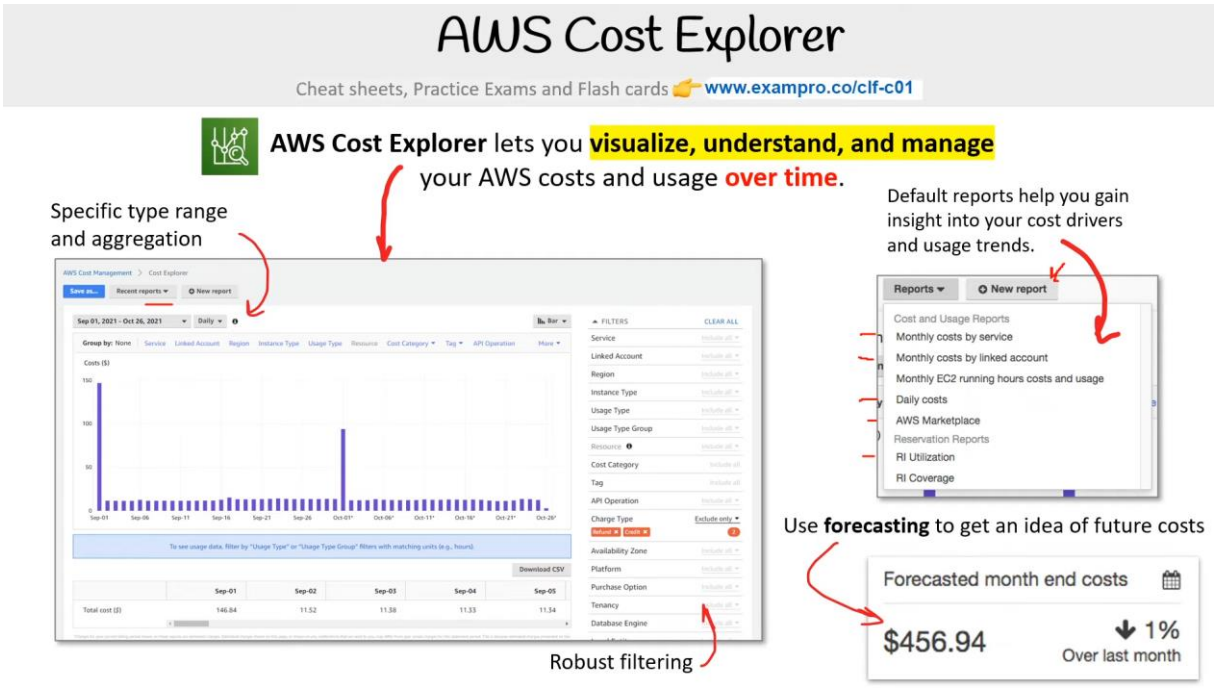


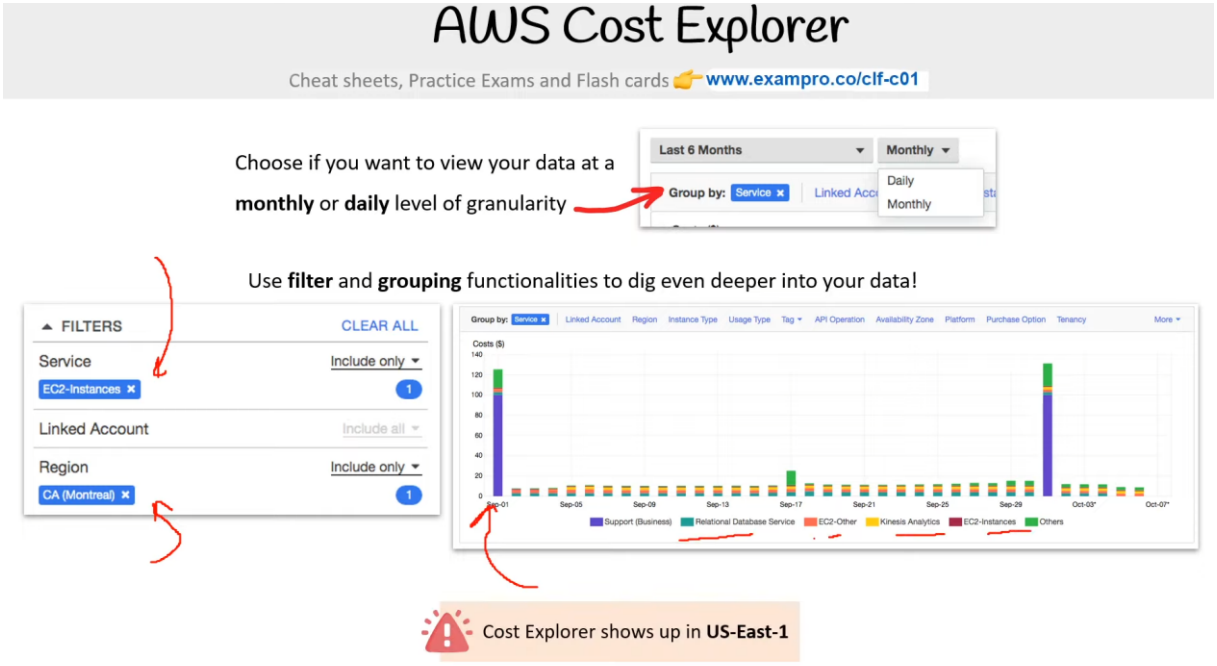
Reference - [Using Cost Allocation Tags]

Billing Alerts/Alarms



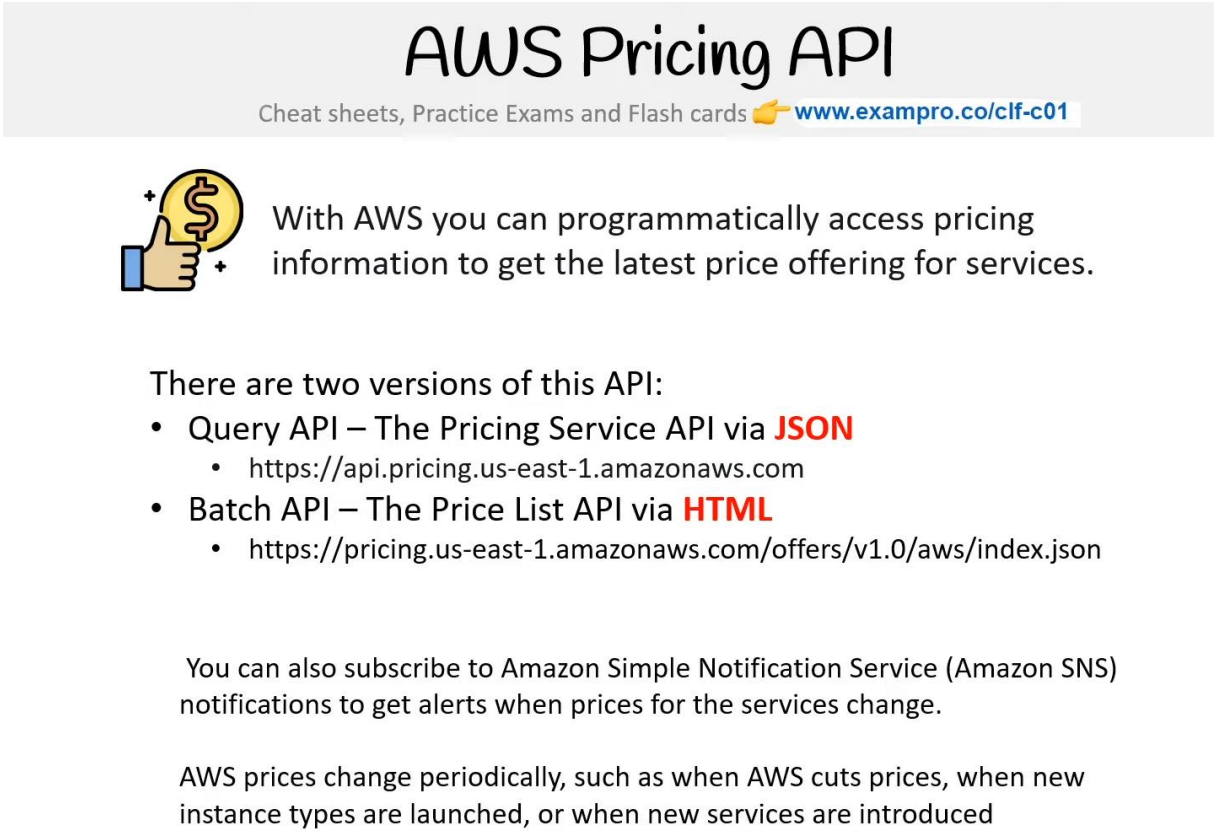
AWS Cost Explorer





Reference - [AWS Cost Explorer]

AWS Pricing API



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

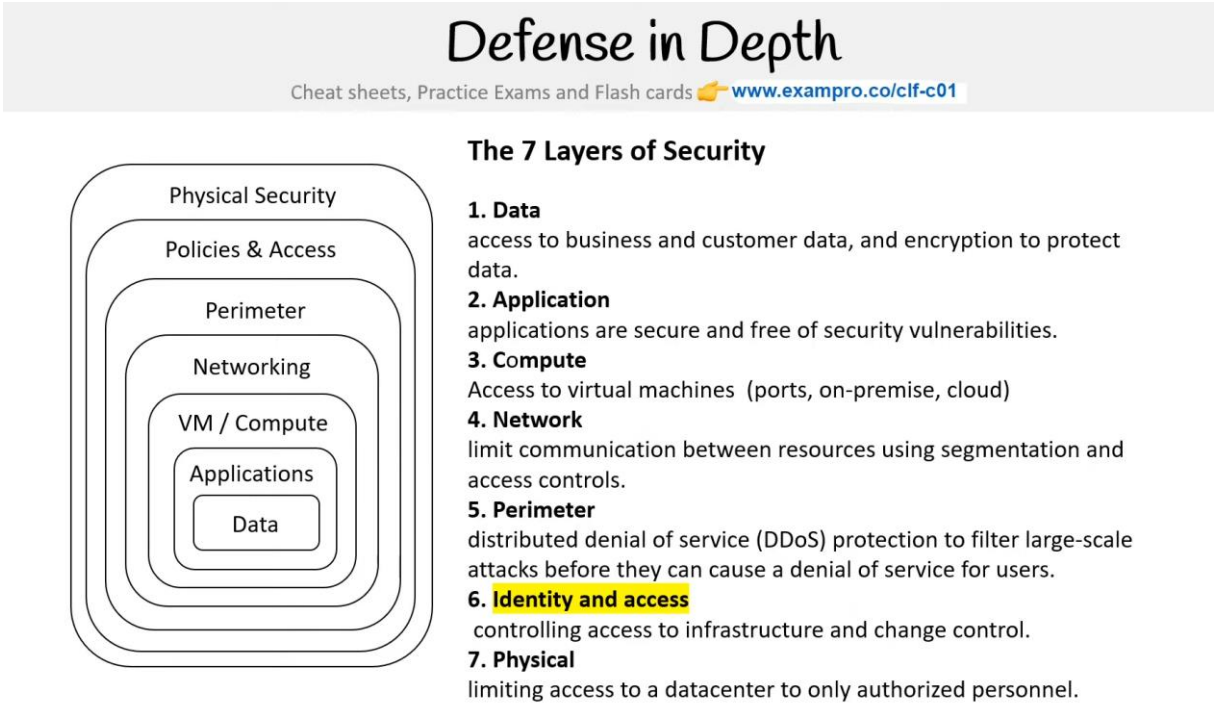
There are two versions of this API:

- 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.

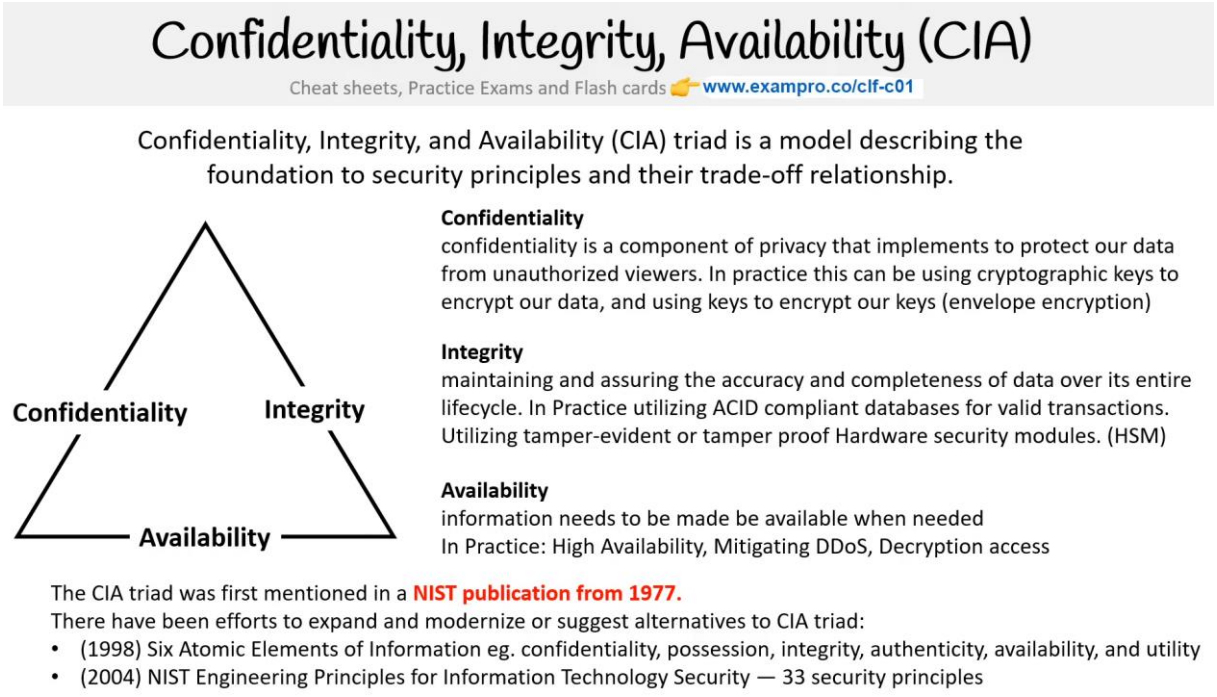
AWS prices change periodically, such as when AWS cuts prices when new instance types are launched, or when new services are introduced

Defense in Depth



Reference - [Azure Essentials: Defense in depth security]

Confidentiality, Integrity, Availability (CIA)



Reference - [Key concepts]

Vulnerabilities

Vulnerabilities

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

What is a vulnerability?
a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application

OWASP

Allowing Domains or Accounts to Expire
Buffer Overflow
Business logic vulnerability
CRLF Injection
CSV Injection
Catch NullPointerException
Covert storage channel
Deserialization of untrusted data
Directory Restriction Error
Doubly freeing memory
Empty String Password
Expression Language Injection
Full Trust CLR Verification issue
Heartbleed Bug
Improper Data Validation
Improper pointer subtraction
Information exposure through query strings
Injection problem
Insecure Compiler Optimization
Insecure Randomness
Insecure Temporary File
Insecure Third Party Domain Access
Insecure Transport
Insufficient Entropy
Insufficient Session-ID Length
Least Privilege Violation
Memory leak
Missing Error Handling
Missing XML Validation
Multiple admin levels
Null Dereference
OWASP .NET Vulnerability Research
Overly Permissive Regular Expression
PHP File Inclusion
PHP Object Injection
PRNG Seed Error
Password Management Hardcoded Password
Password Plaintext Storage
Poor Logging Practice
Portability Flaw
Privacy Violation
Process Control
Return Inside Finally Block
Session Variable Overloading
String Termination Error
Unchecked Error Condition
Unchecked Return Value Missing Check against Null
Undefined Behavior
Unreleased Resource
Unrestricted File Upload
Unsafe JNI
Unsafe Mobile Code
Unsafe function call from a signal handler
Unsafe use of Reflection
Use of Obsolete Methods
Use of hard-coded password
Using a broken or risky cryptographic algorithm
Using freed memory
Vulnerability template
XML External Entity (XXE) Processing

Encryption

Encryption

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

What is cryptography?
The practice and study of techniques for secure communication in the presence of third parties called adversaries

What is encryption?
The process of encoding (scrabbling) information **using** a **key** and a **cypher** to store sensitive data in an unintelligible format as a means of protection. An encryption takes in plaintext and produces **ciphertext**.

The **enigma machine** was used during WW2. A different key for each day was used to set the position of the rotors. It relied on simple cypher substitution.

Reference - Key (cryptography) - A Brief History of Cryptography

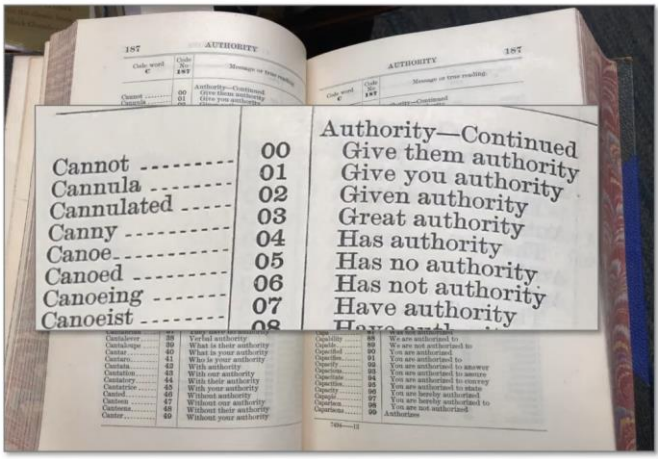
Cyphers

Cyphers

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

What is a cypher?
An algorithm that performs encryption or decryption. Cipher is synonymous with "code"

What is ciphertext
Ciphertext is the result of encryption performed on plaintext via an algorithm



A **codebook** is a type of document used for gathering and storing cryptography codes

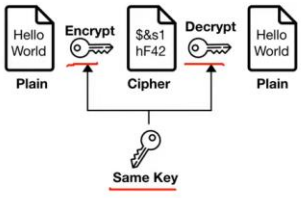
Reference - Key (cryptography) - Codebook

Cryptographic Keys

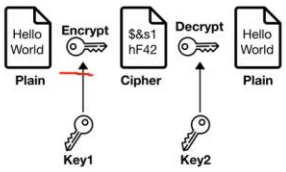
Cryptographic Keys

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

What is a cryptographic key?
A key is a variable used in conjunction with an encryption algorithm in order to encrypt or decrypt data.



What is symmetric encryption?
The same key is used for encoding and decoding.
eg **Advanced Encryption Standard (AES)**



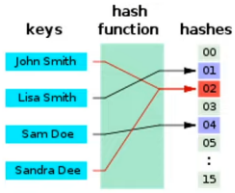
What is asymmetric encryption?
Two keys are used. One to encode and one to decode eg. **Rivest–Shamir–Adleman (RSA)**

Reference - Key (cryptography)

Hashing and Salting

Hashing and Salting

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



What is hashing function?
A function that accepts arbitrary size value and maps it to a fixed-size data structure. Hashing can reduce the size of the store value.

Hashing is a **one-way process** and is **deterministic**
A deterministic function always returns the same output for the same input.

Hashing Passwords
Hashing functions are used to store passwords in database so that a password does not reside in a plaintext format.

To authenticate a user, when a user inputs their password, it is hashed, and the hash is compared to the store hashed. If they match then the user has successful logged in.

Popular hashing functions are **MD5, SHA256 and Bcrypt**
If an attacker knowns what function you are using and stole your database, they could enumerate a dictionary of password to determine the password.

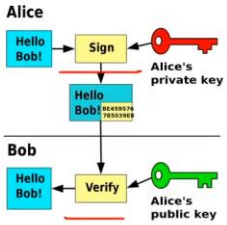
Salting Passwords
A salt is a random string not known to the attacker that the hash function accepts to mitigate the deterministic nature of hashing functions

Reference - Key (cryptography)

Digital Signatures and Signing

Digital Signatures and Signing

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



What is a digital signature
A mathematical scheme for verifying the authenticity of digital messages or documents.

A Digital signature gives us **tamper-evidence** .
- Did someone mess (modify) the data?
- Is this data is not from the expected sender?

There are three algorithms to digital signatures:

- **Key generation** – generates a public and private key.
- **Signing** - the process of generating a digital signature with a **private key** and inputted message
- **Signing verification –** verify the authenticity of the message with a **public key**

```
ssh-keygen -t rsa
```

SSH uses a public and private key to authorize remote access into a remote machine e.g. Virtual Machine. It is common to use RSA
ssh-keygen is a **well known command** to generate a public and private key

What is Code Signing?
When you use a digital signature to ensure **computer code** has not been tampered

In-Transit vs At-Rest Encryption

Encryption In-Transit
Data that is secure when moving between locations
Algorithms: **TLS, SSL**

Encryption At-Rest
Data that is secure when residing on storage or within a database
Algorithms: **AES, RSA**

Transport Layer Security (TLS)
An encryption protocol for data integrity between two or more communicating computer application.
TLS 1.0, 1.1 are deprecated. **TLS 1.2** and **1.3** is the current best practice

Secure Sockets Layers (SSL)
An encryption protocol for data integrity between two or more communicating computer application
SSL 1.0, 2.0 and 3.0 *are deprecated*

Reference - Transport Layer Security

Common Compliance Programs

Common Compliance Programs

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

International Organization for Standardization (ISO) / International Electrotechnical Commission
ISO/IEC 27001 — control implementation guidance
ISO/IEC 27017 — enhanced focus on cloud security
ISO/IEC 27018 — protection of personal data in the cloud. eg. PII
ISO/IEC 27701 — Privacy Information Management System (PIMS) framework
- outlines controls and processes to manage data privacy and protect PII.

System and Organization Controls (SOC)
SOC 1 — 18 standard and report on the effectiveness of internal controls (SSAE) at a service organization
- relevant to their client's internal control over financial reporting (ICFR).

SOC 2 — evaluates internal controls, policies, and procedures that directly relate to the security of a system at a service organization
SOC 3 — A report based on the Trust Services Criteria that can be freely distributed

Payment Card Industry Data Security Standard (PCI DSS)
a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

Federal Information Processing Standard (FIPS) 140-2
US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

Common Compliance Programs

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

Personal Health Information Protection Act (PHIPA)
An Ontario provincial law (Canada) that regulates patient Protected Health Information

Health Insurance Portability and Accountability Act (HIPAA).
US federal law that regulates patient Protected Health Information

Cloud Security Alliance (CSA) STAR Certification
Independent third-party assessment of a cloud provider's security posture

Common Compliance Programs

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

Federal Risk and Authorization Management Program (FedRAMP)
US government standardized approach to security authorizations for Cloud Service Offerings

Criminal Justice Information Services (CJIS)
Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy.

General Data Protection Regulation (GDPR)
A European privacy law. Imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

References | Compliance resource center | Compliance offerings | What's The Difference Between SOC 1, SOC 2, and SOC 3?

Penetration Testing

Penetration Testing

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

What is PenTesting?
An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

Pen Testing **is allowed** to be performed on AWS!

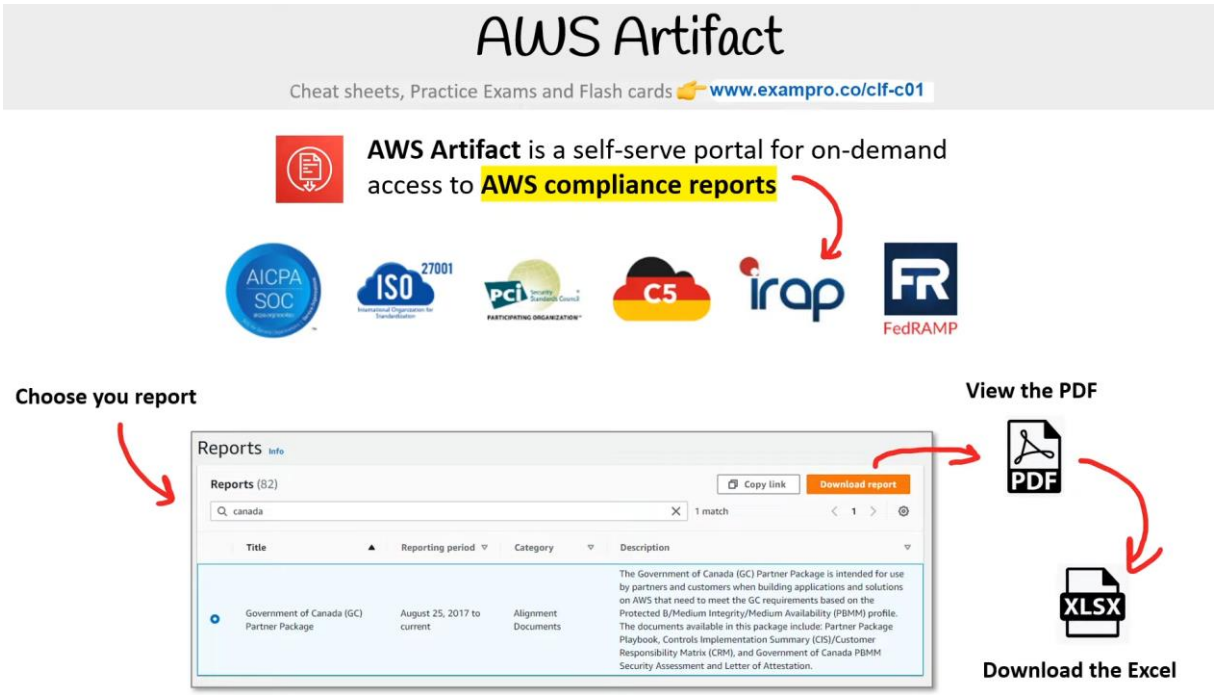
Permitted Services
- Amazon EC2 instances
- NAT Gateways
- Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

- **Prohibited Activities**
- DNS zone walking via Amazon Route 53 Hosted Zones
- *Subject to the **DDoS Simulation Testing policy**
  - Denial of Service (DoS)
  - Distributed Denial of Service (DDoS)
  - Simulated DoS, Simulated DDoS
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

For **Other Simulated Events** you will need to submit a request to AWS. A reply could take up to 7 days.

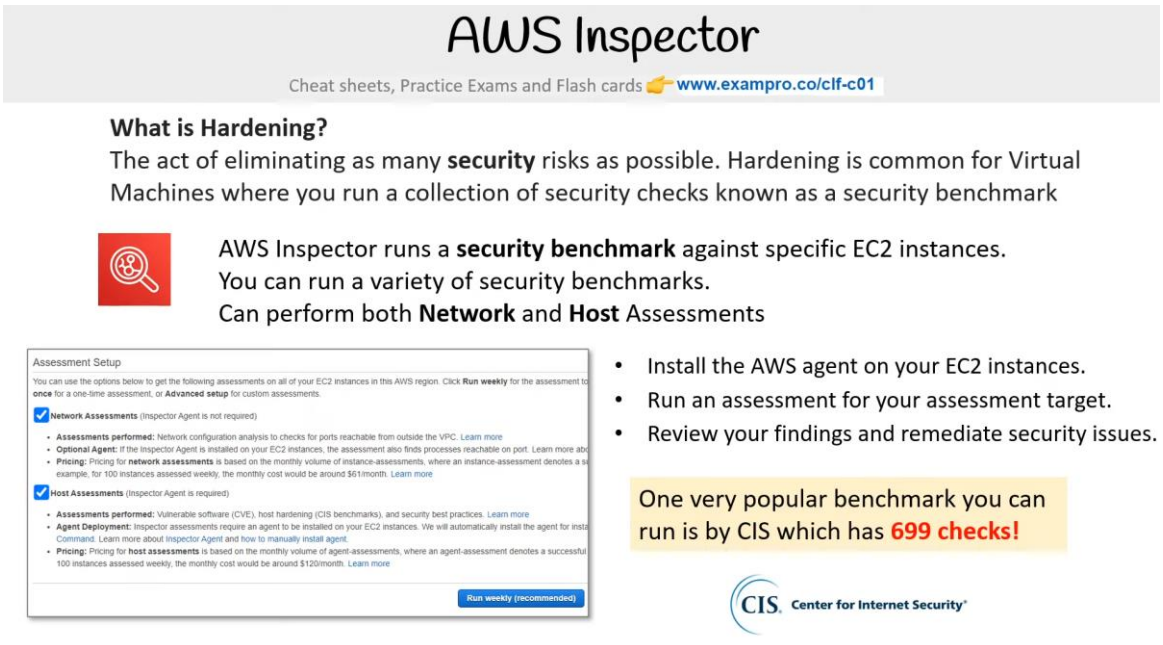
Reference - Penetration Testing

AWS Artifact



Reference - [AWS Artifact]

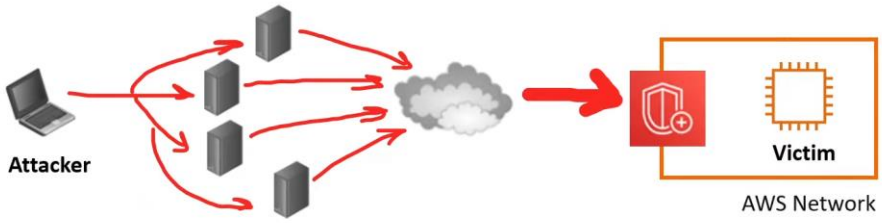
AWS Inspector



Reference - [Amazon Inspector]

Distributed Denial of Service (DDoS)

What is a DDoS (Distributed Denial of Service) Attack?
A malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic.



Reference - AWS Shield

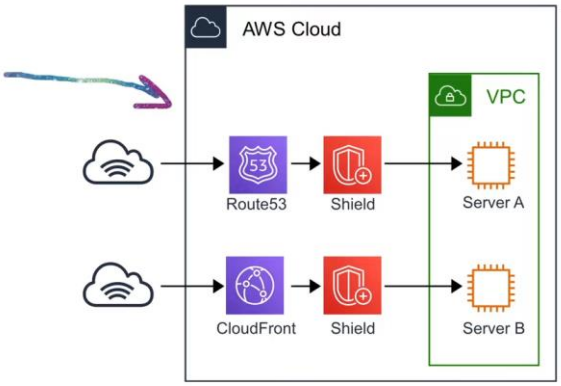
AWS Shield

AWS Shield is a **managed** DDoS (Distributed Denial of Service) protection service that safeguards applications running on AWS

When you route your traffic through **Route53** or **CloudFront** you are using **AWS Shield Standard**

Protects you against **Layer 3, 4** and **7** attacks

- 7 Application
- 4 Transport
- 3 Network



AWS Shield

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

Shield Standard FREE

protection against most common DDoS attacks

- access to tools and best practices to build a DDoS resilient architecture.
- Automatically available on all AWS services.

Shield Advanced *3000 USD / Year

additional protection against larger and more sophisticated attacks

Available On
- Amazon Route 53
- Amazon CloudFront
- Elastic Load Balancing
- AWS Global Accelerator
- Elastic IP (Amazon EC1 and Network Load Balancer)

Notable Features
- Visibility and Reporting on Layer 3,4 and 7
- Access to Team and Support (with Business or Enterprise Support)
- DDoS Cost Protection
- Comes with SLA

Both plans integrate with AWS Web Application Firewall (WAF) to give you Layer 7 (Application) protection

Reference - [Getting Started with AWS Shield]

Amazon Guard Duty

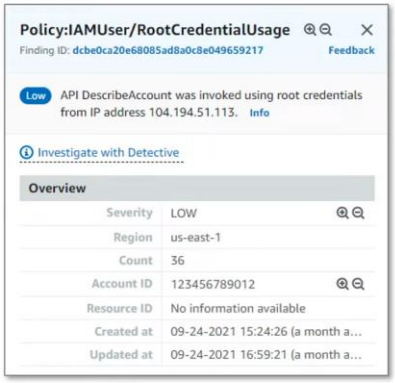
Amazon Guard Duty

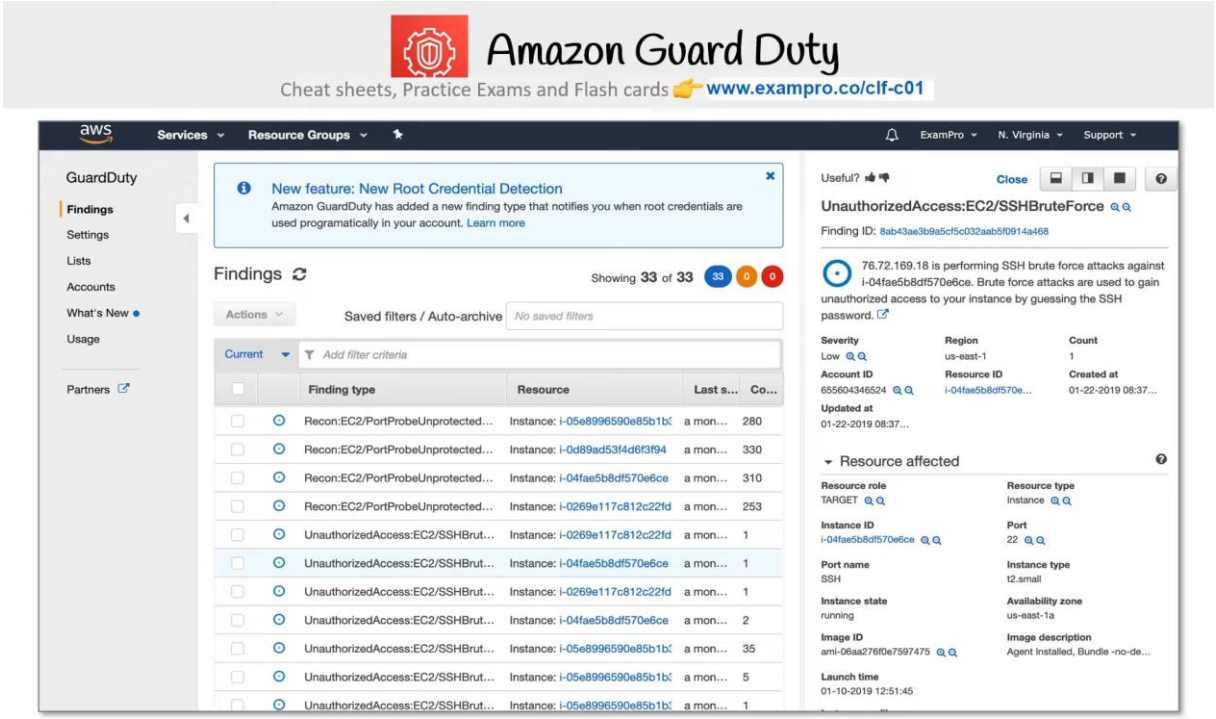
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

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:

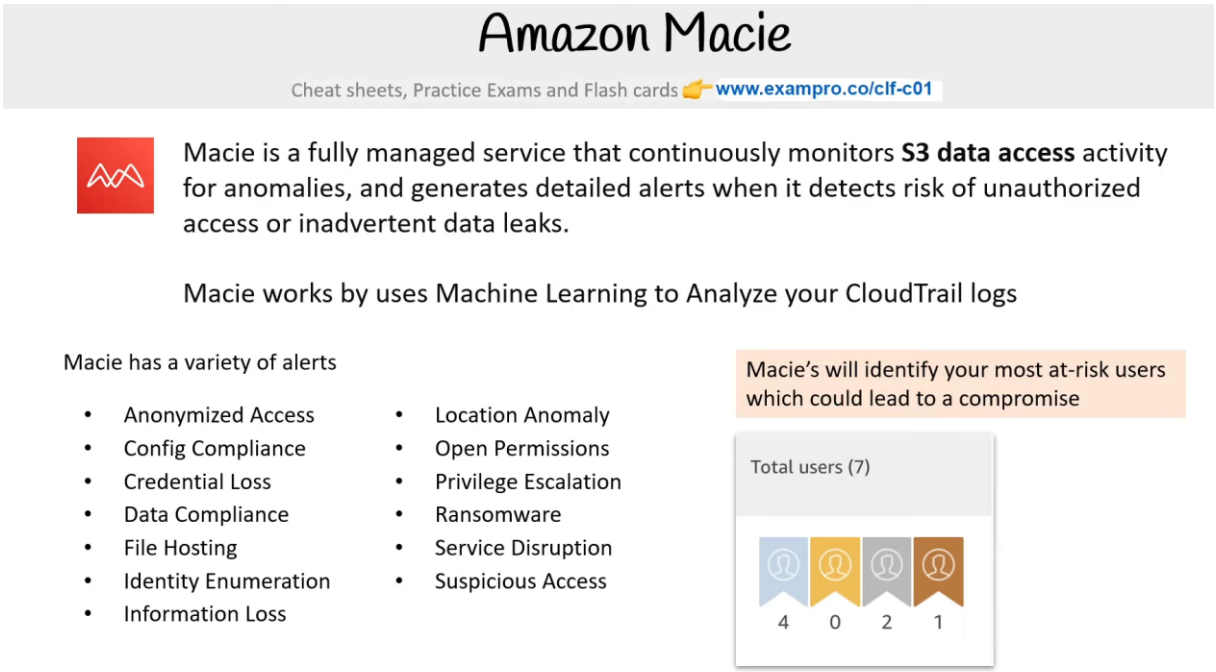
- CloudTrail Logs
- VPC Flow Logs
- DNS logs





Reference - [Amazon GuardDuty]

Amazon Macie



Reference - [Amazon Macie]

AWS Virtual Private Network (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)

AWS WAF

AWS WAF

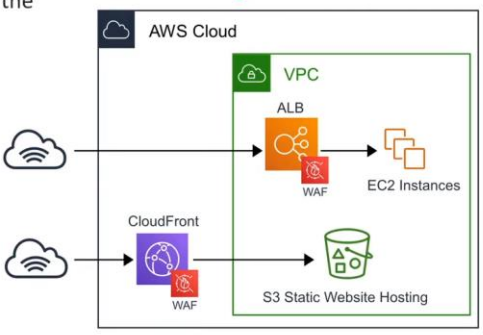
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

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

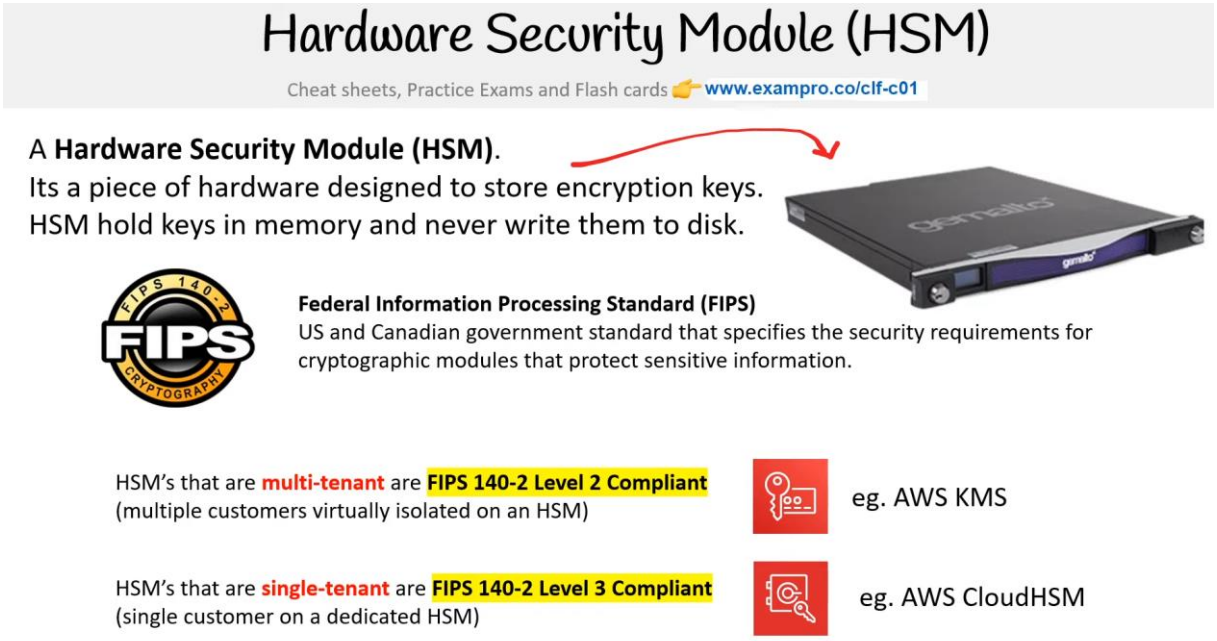
Write your own **rules** to ALLOW or DENY traffic based on the contents of an HTTP requests
Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Rules Marketplace
WAF can be attached to either **CloudFront** or an **Application Load Balancer**

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

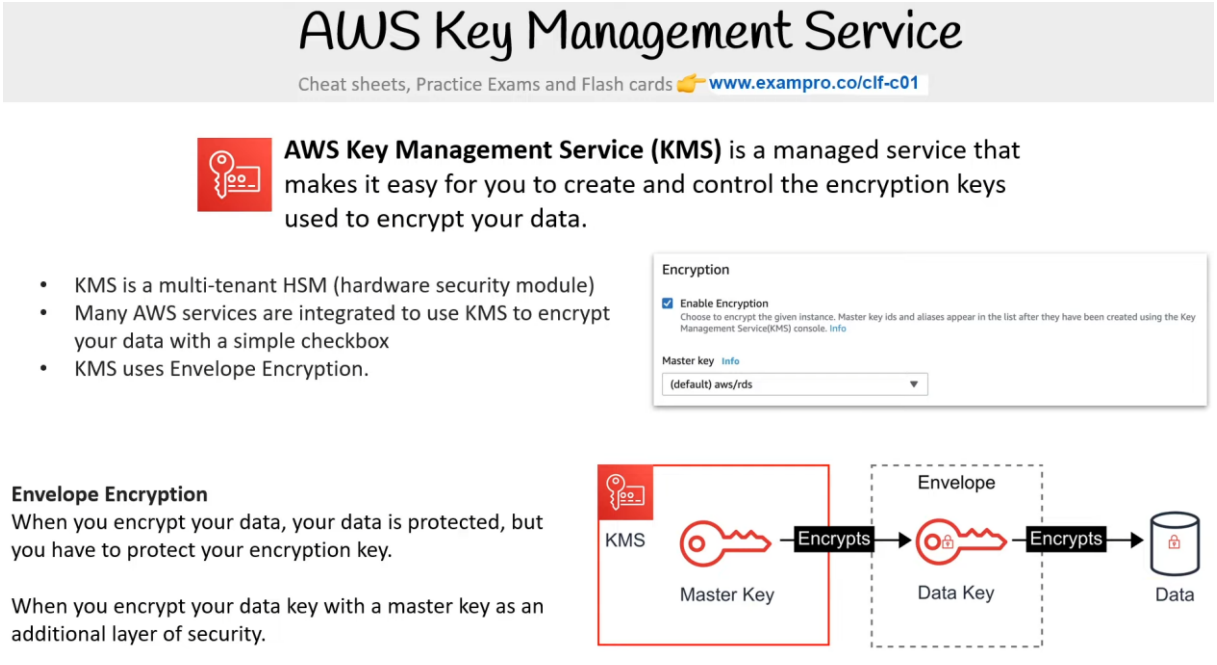


Hardware Security Module (HSM)



Reference - [Key Vault]

AWS Key Management Service



Reference - [AWS Key Management Service (KMS)]

CloudHSM

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.

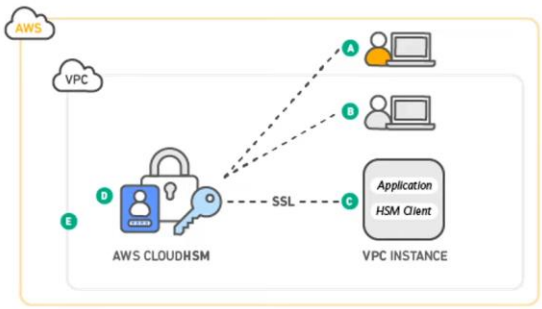
AWS CloudHSM enables you to generate and use your encryption keys on a FIPS 140-2 Level 3 validated hardware.

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.



Know Your Initialisms

Know Your Initialisms

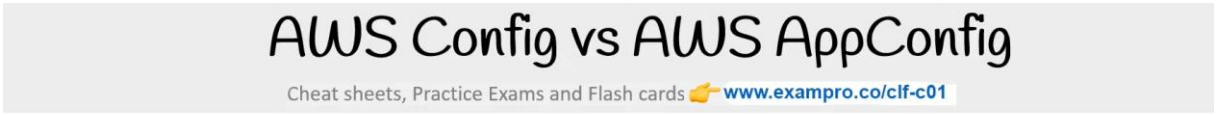
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c01

IAM Identity and Access Management
S3 Simple Storage Service
SWF Simple Workflow Service
SNS Simple Notification Service
SQS Simple Queue Service
SES Simple Email Service
SSM Simple Systems Manager
RDS Relational Database Service
VPC Virtual Private Cloud
VPN Virtual Private Network
CFN CloudFormation
WAF Web Application Firewall
MQ Amazon ActiveMQ
ASG Auto Scaling Groups
TAM Technical Account Manager

ELB Elastic Load Balancer
ALB Application Load Balancer
NLB Network Load Balancer
GWLB Gateway Load Balancer
CLB Classic Load Balancer
EC2 Elastic Cloud Compute
ECS Elastic Container Service
ECR Elastic Container Repository
EBS Elastic Block Storage
EFS Elastic File Storage
EMR Elastic MapReduce
EB Elastic Beanstalk
ES Elasticsearch
EKS Elastic **Kubernetes** Service
MSK Managed **Kafka** Service

RAM AWS Resource Manager
ACM Amazon Certificate Manager
PoLP Principle of Least Privilege
IoT Internet of Things
RI Reserved Instances

AWS Config vs AWS AppConfig



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

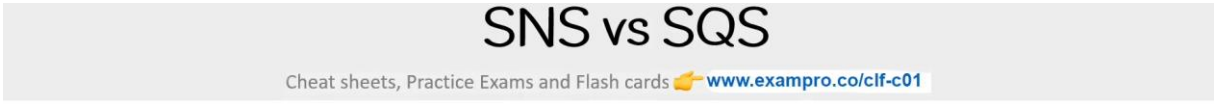
AWS AppConfig

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.

SNS vs SQS



The Both **Connect Apps** via Messages

Simple Notifications Service

Pass Alongs Messages eg. PubSub

Send notifications to **subscribers** of **topics** via multiple protocol. eg, HTTP, **Email**, SQS, SMS

SNS is generally used for sending **plain text emails** which is triggered via other AWS Services. The best example of this is billing alarms.

Can retry sending in case of failure for **HTTPS**

Really good for webhooks, simple internal emails, triggering lambda functions

PUSHER POWERING REALTIME PubNub

Simple Queue Service

Queue Up Messages, Guaranteed Delivery

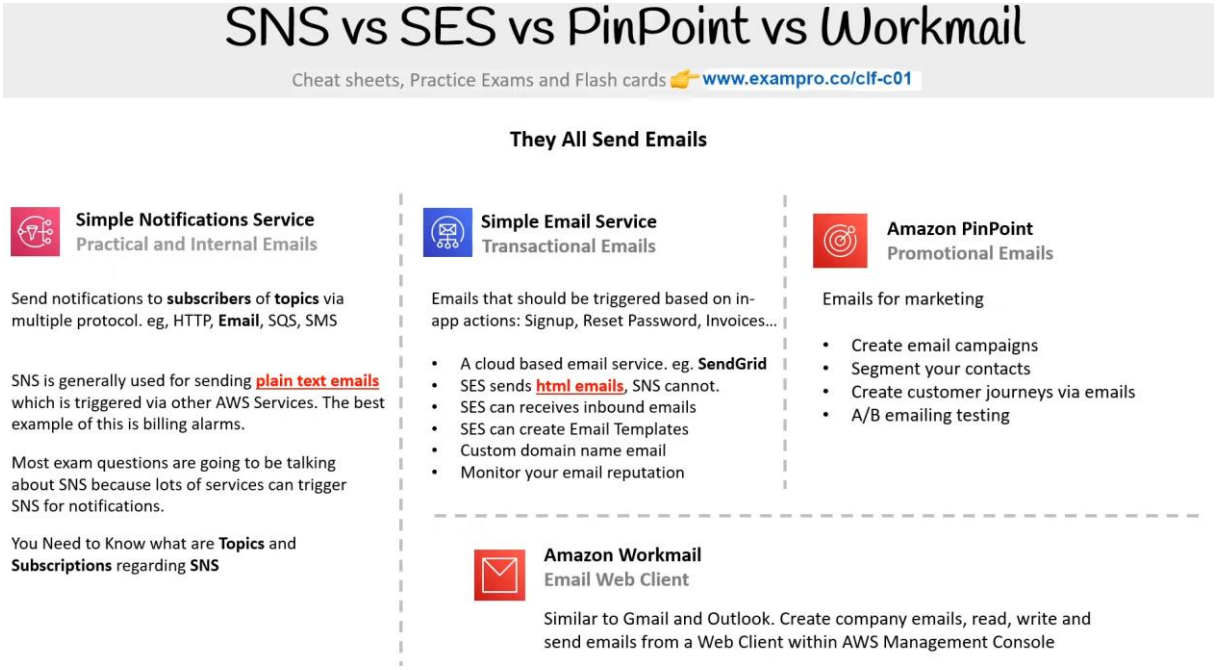
Places messages into a **queue.** Applications pull queue using **AWS SDK**

Can retain a message for up to 14 days
Can send them in sequential order or in parallel
Can ensure only one message is sent
Can ensure messages are delivered at least once

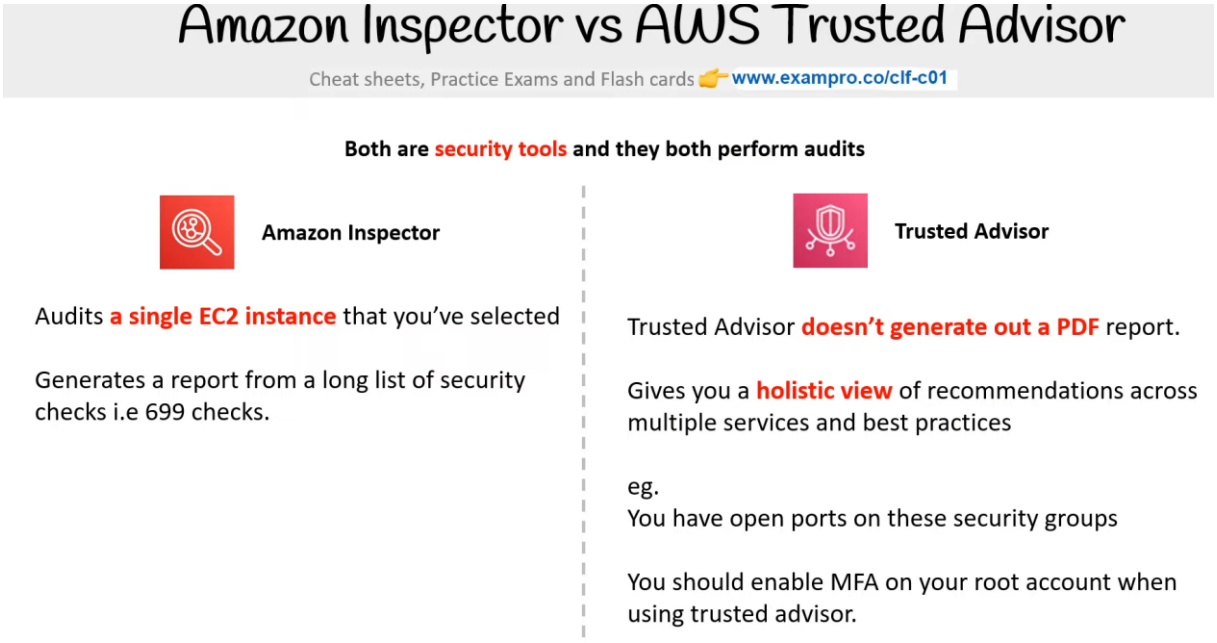
Really good for delayed tasks, queueing up emails

RabbitMQ Sidekiq

SNS vs SES vs PinPoint vs Workmail



Amazon Inspector vs AWS Trusted Advisor



Connect Names Services

Connect Names Services

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

They all have **"Connect"** in the name but they are not related or similar in functionality

Direct Connect

- A Dedicated Fiber Optics Connection from your DataCenter to AWS
- Intended for large enterprises with their own datacenter and they need an insanely fast and *private* connection directly AWS.
- If you need a **secure connection** you need apply a AWS VPN connection on-top of Direct Connect

Amazon Connect

- Call Center as a Service
- Get a toll free number, accept inbound and outbound calls, setup automated phone systems.
- Interactive Voice System (IVS)

Media Connect

- New Version of Elastic Transcoder, Converts Videos to Different Video Types
- You have 1000 of videos you and you need to transcode them into different videos format, maybe you need to apply watermarks, or insert introduction video in front of every video

Elastic Transcoder vs MediaConvert

Elastic Transcoder vs MediaConvert

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

Both services transcodes videos

Elastic Transcoder
The Old Way

Elastic Transcoder was the original transcoding service. It may have programmatic APIs or workflows not available in MediaConvert.

Its exists due to legacy customers still using the platform

- Transcodes videos to streaming formats

AWS Elemental MediaConvert
The New Way

MediaConvert is a more robust transcoding service that can preform various operations during transcoding.

- Transcodes videos to streaming formats
- Overlays images
- Insert videos clips
- Extracts captions data
- Robust UI

AWS Artifact vs Amazon Inspector

AWS Artifact vs Amazon Inspector

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

Both Artifact and Inspector **compile out PDFs**

AWS Artifact

Why should an enterprise trust AWS?

Generates a security report that's based on **global compliance frameworks** such as:

- Service Organization Control (SOC)
- Payment Card Industry (PCI)

Amazon Inspector

How do we know this EC2 instance is Secure? Prove It?

Runs a script that analyzes your EC2 instance, then generates a PDF report telling you which security checks passed.

Audit tool for security of EC2 instances

ELB vs ALB vs NLB vs GWLB vs CLB

ELB vs ALB vs NLB vs GWLB vs CLB

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

Elastic Load Balancer (ELB) has 4 different types of possible load balancers.

Application Load Balancer (ALB)
Layer 7 - HTTP/S
Routing Rules
- create rules to change routing based on information found in a HTTP/S request

Can attach an AWS WAF

Network Load Balancer (NLB)
Layer 3 and 4 – TCP and UDP

Where extreme performance is required for **TCP and TLS traffic**

Capable of handling millions of requests per second while maintaining **ultra-low latencies**

Optimized for **sudden and volatile traffic** patterns while using a single static IP address per Availability Zone

Gateway Load Balancer (GWLB)
When you need to deploy a fleet of third-party virtual appliances that support GENEVE

Classic Load Balancer (CLB)
Layer 3,4 and 7
Intended for applications that were built within the **EC2-Classic network**
Doesn't use Target Groups
Retires on Aug 15, 2022