

# AWS Cloud Practitioner

⌚ Category	
📎 Files	
🕒 Created	@June 26, 2022 4:24 PM
📅 Reminder	
⌚ Status	<span style="background-color: #c8e6c9; padding: 2px 10px; border-radius: 5px;">Open</span>
🔗 URL	
🕒 Updated	@December 30, 2022 7:24 PM

## ▼ 1. Cloud Concepts

### ▼ 1. What is AWS

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

### ▼ 2. Timelines of AWS Services

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

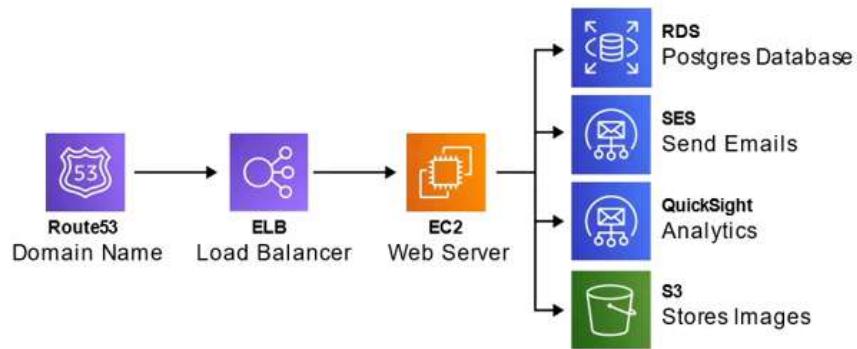
2006(March) - S3( Simple Storage Service) which is still in use.

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

2010 - Amazon started using AWS

2013- Emerged as a Certification

### ▼ 3. Cloud Service Provider Architecture diagram.



## ▼ 4. 4 most Common Cloud Services

### Common Cloud Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

	<b>Compute</b> Imagine having a virtual computer that can run application, programs and code.		<b>Networking</b> Imagine having virtual network defining internet connections or network isolations between services or outbound to the internet
	<b>Storage</b> Imagine having a virtual hard-drive that can store files		<b>Databases</b> Imagine a virtual database for storing reporting data or a database for general purpose web-application

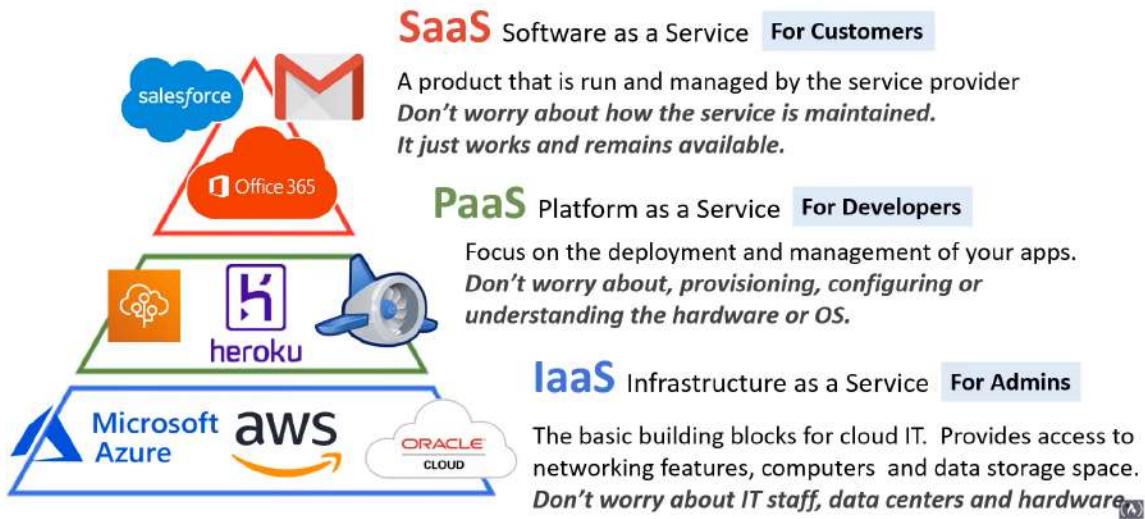
AWS has over **200+** cloud services

The term "Cloud Computing" can be used to refer to all categories, even though it has "compute" in the name. [\(A\)](#)

## ▼ 5. Types of Cloud Computing

## Types of Cloud Computing

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## ▼ 6. Cloud Computing Deployment Models

### Cloud Computing Deployment Models

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Cloud	Hybrid	On-Premise
Fully utilizing cloud computing   	Using both Cloud and On-Premise   	Deploying resources on-premises, using virtualization and resource management tools, is sometimes called "private cloud".   
Companies that are starting out today, or are small enough to make the leap from a VPS to a CSP. <ul style="list-style-type: none"><li>• Startups</li><li>• SaaS offerings</li><li>• New projects and companies</li></ul>	Organizations that started with their own datacenter, can't fully move to cloud due to effort of migration or security compliance. <ul style="list-style-type: none"><li>• Banks</li><li>• FinTech, Investment Management</li><li>• Large Professional Service providers</li><li>• Legacy on-premise</li></ul>	Organizations that cannot run on cloud due to strict regulatory compliance or the sheer size of their organization <ul style="list-style-type: none"><li>• Public Sector eg. Government</li><li>• Super Sensitive Data eg. Hospitals</li><li>• Large Enterprise with heavy regulation eg. Insurance Companies</li></ul>
		<p>There really isn't reason to be fully on-premise</p>

## ▼ 2. Digital Transformation

### ▼ 1. Evolution of Computing

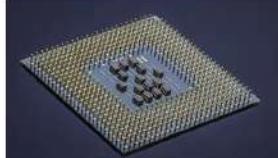
### Evolution of Computing Power

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

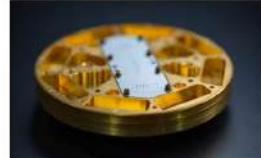
**What is Computing Power?**  
The throughput measured at which a computer can complete a computational task.



**General Computing**  
Xeon CPU Processor



**GPU Computing**  
\*50x faster than traditional CPUs



**Quantum Computing**

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

---

AWS Service Offering

 Elastic Compute Cloud EC2

 AWS Inferentia (Inf1)

 AWS Bracket  
Via CalTech

## ▼ 3. Benefits of Cloud

### ▼ 1. 7 Advantages of Cloud

### Seven Advantages to Cloud

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

## ▼ 4. AWS Global Infrastructure

### ▼ 1. What is AWS Global Infrastructure

### AWS Global Infrastructure

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**What is the AWS Global Infrastructure?**

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

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

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



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



### ▼ 2. Regions

### Global Infrastructure – Regions

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Each region generally has three Availability Zones

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

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

Not all AWS Services are available in all regions

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

The cost of AWS services vary per region

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

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



Region	Availability Zones	Launched
US East (Ohio) Region	3*	2016
US West (Oregon) Region	4	2011
US West (Northern California) Region	3*	2009
GovCloud (US-West) Region	3	2011
GovCloud (US-East) Region	3	2018
Canada (Central) Region**	3	2016
US East (Northern Virginia) Region	6	2006
	8	2020

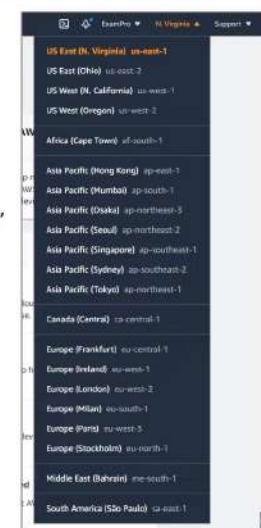
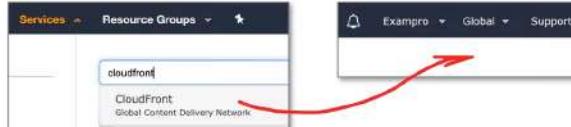
## ▼ 3. Regions vs Global

### Global Infrastructure – Regional vs Global Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

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



For these global services at the time of creation:

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

## ▼ 4. Availability Zones

### Global Infrastructure – Availability Zones

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

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

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

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

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

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



# Global Infrastructure – Availability Zones

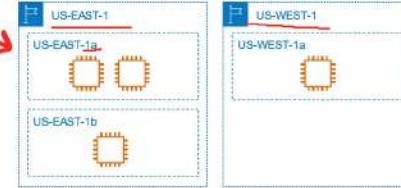
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

A Subnet is associated with an Availability Zone.

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

Subnet	ⓘ	✓ No preference (default subnet in any Availability Zone) subnet-d9de91f7   Default in us-east-1c subnet-d0c28f8c   Default in us-east-1a subnet-349fd53   Default in us-east-1b subnet-a8c2f8a7   Default in us-east-1f subnet-b9db4cb7   Default in us-east-1e subnet-13869659   Default in us-east-1d
Public IP	ⓘ	
Ant group	ⓘ	
servation	ⓘ	

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



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



# Global Infrastructure – Availability Zones

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

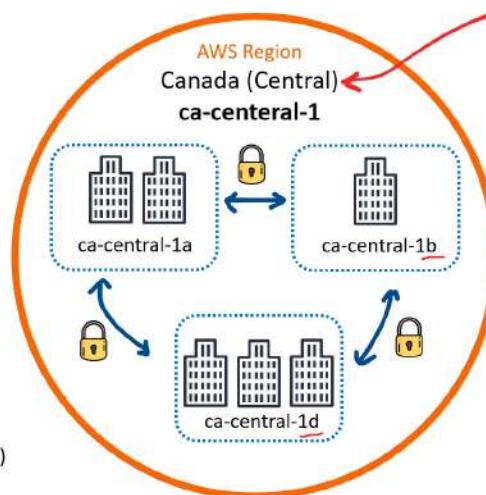
A region has multiple Availability Zones

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

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

All traffic between AZs is encrypted

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



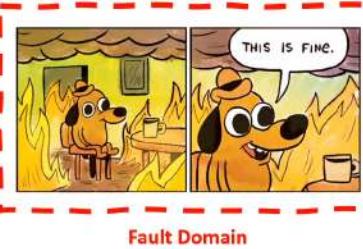
Montreal



## ▼ 5. Fault Tolerance

## Global Infrastructure - Fault Tolerance

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



### What is a fault domain?

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

You can have fault domains nested inside fault domains.

### What is a fault level?

A fault level is a collection of fault domains.

The scope of a fault domain could be:

- specific servers in a rack
  - an entire rack in a datacenter
  - an entire room in a datacenter
  - the entire data center building
- It's up to the Cloud Service Provider (CSPs) to define the boundaries of a domain

An AWS Region would be a **Fault Level** →

Fault Level  
us-east-1 (Region)

A Availability Zone would be a **Fault Domain** →

Fault Domain  
us-east-1a (AZ)      Fault Domain  
us-east-1b (AZ)



## Global Infrastructure - Fault Tolerance

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Each Amazon Region is designed to be completely **isolated** from the other Amazon Regions.

- This achieves the greatest possible fault tolerance and stability

Each Availability Zone is **isolated**, but the Availability Zones in a Region are connected through low-latency links

Each Availability Zone is designed as an **independent failure zone**

- *A "Failure Zone" is AWS describing a Fault Domain.*

### Failure Zone

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



### Multi-AZ for High Availability

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



## ▼ 6. Point of Presence(POPs)

## Global Infrastructure – Point of Presence (PoP)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

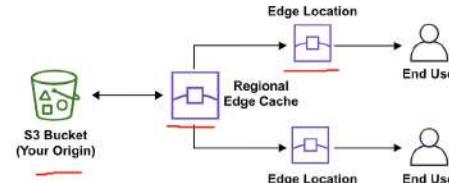
**Points of Presence (PoP)** is an intermediate location between an AWS Region and the end user, and this location could be a datacenter or collection of hardware.

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

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

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

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



(A)

## ▼ 7. Services that use POPs

### Global Infrastructure – Point of Presence (PoP)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

The following AWS Services use PoPs **for content delivery or expedited 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 return 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.

(A)

## ▼ 8. AWS Direct Connect

## Global Infrastructure – Direct Connect Locations

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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



You would use the **AWS Direct Connect** service to order and establish a connection



## ▼ 9. Local Zones

### Global Infrastructure – Local Zones

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**Local Zones** are datacenters located very close to a densely 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 the support highly-demanding applications sensitive to latencies:

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



## ▼ 10. Data Residency

# Global Infrastructure – Data Residency

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is Data Residency?

The physical or geographic location of where an organization or cloud resources reside.

## What is Compliance Boundaries?

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

## What is Data Sovereignty?

Data Sovereignty is the jurisdictional control or legal authority that can be asserted over data because its physical location is within jurisdictional boundaries

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



### AWS Config

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



### IAM Policies

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



### AWS Outposts

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



## ▼ 11. GovCloud

# Global Infrastructure – GovCloud (US)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## Federal Risk and Authorization Management Program (FedRAMP)

a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

## What is GovCloud?

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



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

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

Customers can architect secure cloud solutions that comply with:

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



## ▼ 12. AWS China

## Global Infrastructure – AWS in China

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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](http://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:



## ▼ 13. AWS Ground Station

### Global Infrastructure – AWS Ground Station

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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: To use Ground Station:

- weather forecasting
- surface imaging
- communications
- video broadcasts
- 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

## ▼ 14. AWS Outposts

## Global Infrastructure – AWS Outposts

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

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

42U Rack



### What is a Server Rack?

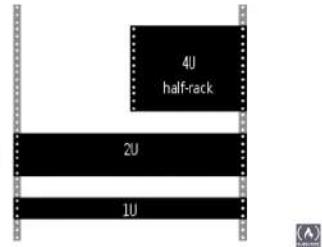
A frame design to hold and organize IT equipment.

### Rack Heights

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

full-size rack cage is 42U high

- equipment is typically 1U, 2U, 3U, or 4U high



## Global Infrastructure – AWS Outposts

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

This a full rack of servers provided by AWS

42U



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 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.



## ▼ 5. Cloud Architecture

### ▼ 1. Cloud Architect and Solution Architect

# Cloud Architecture Terminologies

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## 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 need to understand the following terms and factor them into their designed architecture based on the business requirements.

- **Availability** - Your ability to ensure a service remains available eg. **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 eg. **Highly 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?

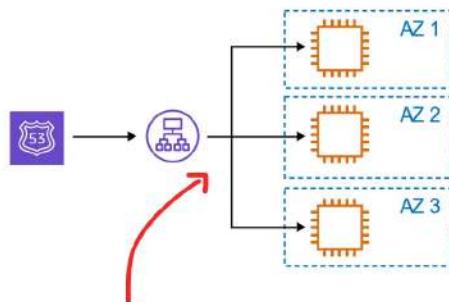


## ▼ 2. What is high availability

### High Availability

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Your ability for your service to **remain available** by ensuring there is **\*no single point of failure** and/or ensure a certain level of performance



#### Elastic Load Balancer

A load balancer allows you to evenly distribute traffic to multiple servers in one or more datacenter. If a datacenter or server becomes unavailable (unhealthy) the load balancer will route the traffic to only available datacenters with servers.

Running your workload across multiple **Availability Zones** ensures that if 1 or 2 AZs become unavailable your service / applications remains available.



## ▼ 3. What is high scalability

## High Scalability

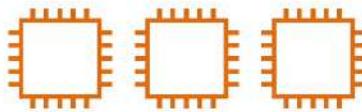
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Your ability to **increase your capacity** based on the increasing demand of traffic, memory and computing power



**Vertical Scaling**  
Scaling **Up**

Upgrade to a bigger server



**Horizontal Scaling**  
Scaling **Out**

Add more servers of the same size

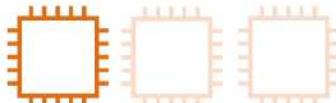


## ▼ 4. What is high elasticity

### High Elasticity

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

#### Horizontal 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.



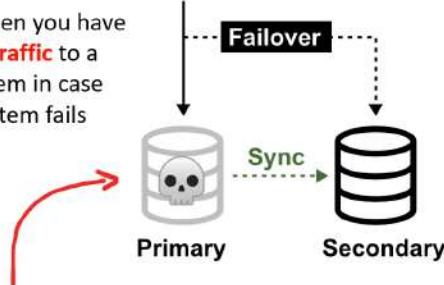
## ▼ 5. What is high fault tolerance

## Highly Fault Tolerant

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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



RDS Multi-AZ is when you run a duplicate standby database in another Availability Zone in case your primary database 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.



## ▼ 6. What is high durability

### High Durability

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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.

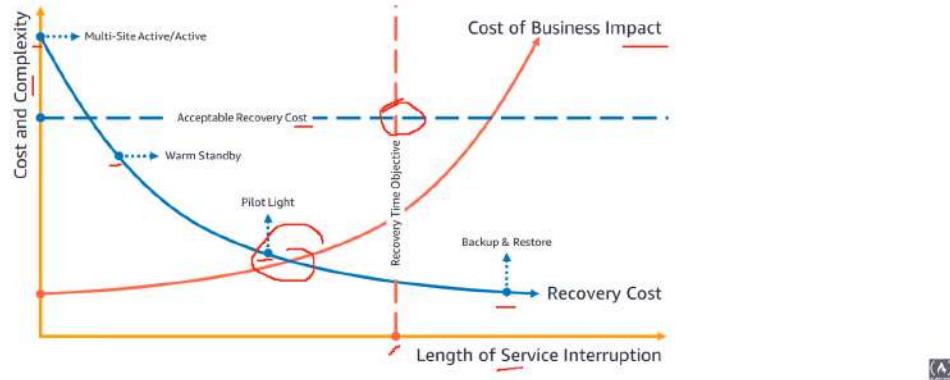


## ▼ 7. Recovery Time Objective (RTO)

# RTO

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

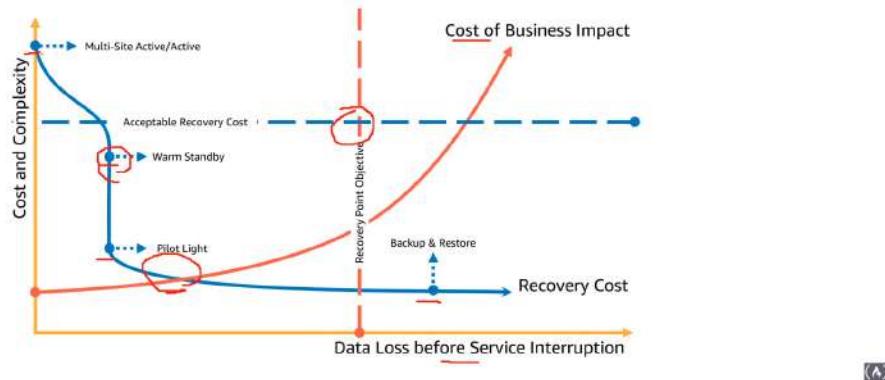


## ▼ 8. Recovery Point Objective (RPO)

# RPO

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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



## ▼ 6. Management and AWS Tools

### ▼ 1. AWS API

# AWS Application Programming Interface (API)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## 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 

## ▼ 2. Service Console

# AWS Management Console – Service Console

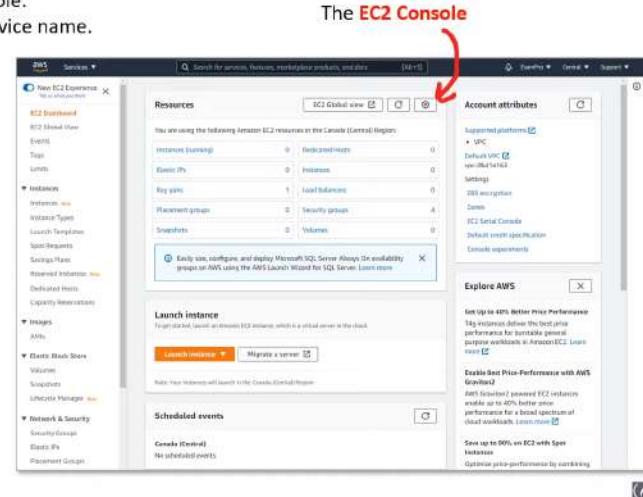
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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: eg

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

A screenshot of the EC2 Service Console. At the top, there is a navigation bar with the "AWS Services" dropdown set to "EC2". The main dashboard shows various EC2 resources: 0 Dedicated networks, 0 Instances, 0 Key pairs, 4 Placement groups, and 0 Snapshots. Below this, there is a "Launch instance" section with a "Launch instance" button and a "Migrate a server" button. On the right side of the dashboard, there is a sidebar titled "Account attributes" and a "Explore AWS" section with links to "Optimize Price-Performance with AWS Graviton2" and "Save up to 50% on EC2 with Spot Instances".

## ▼ 3. Amazon Resource Name

## Amazon Resource Name (ARNs)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**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

### Resource ID

Could be a number name or path:

- user/Bob
- instance/i-1234567890abcdef0

### Service – Identifies the service

- ec2
- s3
- iam

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



arn:aws:s3:::my-bucket

### Region – which AWS resource

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

### Account ID

- 121212121212
- 123456789012

### Name

my-webserver-alb

### ARN

arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/my-webserver-alb/31e9d2ce26643cd8

Copied

(A)

## ▼ 4. AWS Command Line Interface (CLI)

## AWS Command Line Interface (CLI)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

```
aws ec2 describe-instances \
--filters Name=tag-key.Values=Name \
--query 'Reservations[*].Instances[*].
{Instance:InstanceId,AZ:Placement.AvailabilityZone,Name:Tags[?
Key== "Name"]|[0].Value}' \
--output table
```

DescribeInstances		
AZ	Instance	Name
us-east-2b	i-057750d42936e468a	my-prod-server
us-east-2a	i-001efd250faaa6ffa	test-server-1
us-east-2a	i-027552a73f021f3bd	test-server-2



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**

(A)

## ▼ 5. AWS SDK

# AWS Software Development Kit (SDK)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

A Software Development Kit (SDK) is a collection of software development tools in one installable package.



You can use the AWS SDK to programmatically create, modify, delete or interact with AWS resources.

AWS SDK is offered in various programming languages:

- Java
- Python
- Node.js
- **Ruby**
- Go
- .NET
- PHP
- JavaScript
- C++

```
s3 = Aws::S3::Resource.new({
  region: aws_default_region,
  credentials: Aws::Credentials.new(
    aws_access_key_id,
    aws_secret_access_key
  )
})
bucket = s3.bucket s3.bucket
file = File.open file_path
md5 = Digest::MD5.hexdigest file.read
md5 = Base64.encode64([md5].pack("H*")).strip
attrs = {
  key: data["path"],
  body: IO.read(file),
  content_md5: md5
}
resp = bucket.put_object(attrs)
```

(A)

## ▼ 6. AWS Cloud Shell

### AWS CloudShell

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

AWS CloudShell is a browser-based shell built into the AWS Management Console.

AWS CloudShell is scoped per region, Same credentials as logged in user. Free Service!

#### Preinstalled Tools

AWS CLI, Python, Node.js git, make, pip, sudo, tar, tmux, vim, wget, and zip and more

#### Storage included

1 GB of storage free per AWS region

#### Saved files and settings

Files saved in your home directory are available in future sessions for the same AWS region

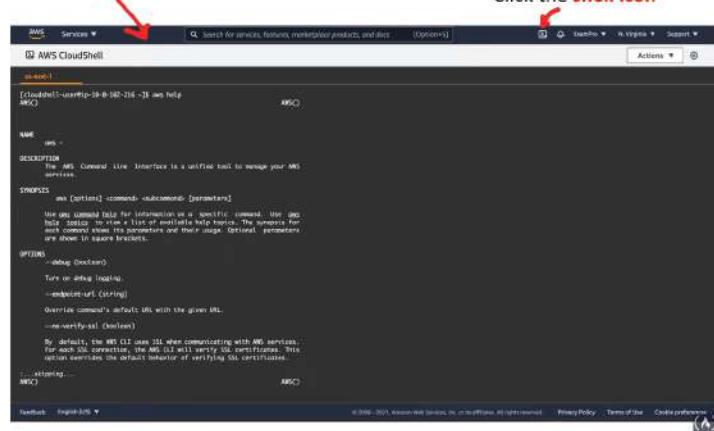
#### Shell Environments

Seamlessly switch between

- Bash
- PowerShell
- Zsh

AWS CloudShell is available in select regions

Click the shell icon



## ▼ 7. Infrastructure as Code (IaC)

## Infrastructure as Code (IaC)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](https://www.exampro.co/clf-c01)

### Infrastructure as Code (IaC)

You write a configuration script to **automate** creating, updating or destroying cloud infrastructure.

- IaC is a **blueprint** of your infrastructure.
- IaC allows you to easily **share, version or inventory** your cloud infrastructure.

AWS has two offerings for writing Infrastructure as Code.



**AWS CloudFormation (CFN)**  
CFN is a Declarative IaC tool



**AWS Cloud Development Kit (CDK)**  
CDK is an Imperative IaC tool.

#### Declarative

- What you see is what you get. **Explicit**
- More verbose, but zero chance of mis-configuration
- Uses scripting languages eg. JSON, YAML, XML

#### Imperative

- You say what you want, and the rest is filled in. **Implicit**
- Less verbose, you could end up with misconfiguration
- Does more than Declarative
- Uses programming languages eg. Python, Ruby, JavaScript



## ▼ 8. Cloud Development Kit (CDK)

## Cloud Development Kit

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](https://www.exampro.co/clf-c01)

AWS CDK allows you to use your favorite programming language to write Infrastructure as Code (IaC)



TypeScript



NodeJS



Python



Java



.NET

```
const bucket = new Bucket(this, 'MyBucket');
const result = bucket.addToResourcePolicy(new iam.PolicyStatement({
  actions: ['s3:GetObject'],
  resources: [bucket.arnForObjects('file.txt')],
  principals: [new iam.AccountRootPrincipal()],
}));
```

- CDK is powered by CloudFormation (it generates out CloudFormation templates)
- CDK has a large library of reusable cloud components called CDK Construct <https://constructs.dev>
- CDK comes with its own CLI
- CDK Pipelines to quickly setup CI/CD pipelines for CDK projects
- CDK has a testing framework for Unit and Integration Testing

AWS SDK looks similar, but the key difference is CDK ensures Idempotent of your Infrastructure



## ▼ 9. Access Keys

# Access Keys

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Access Keys is a **key and secret** required to have programmatic access to AWS resources when interacting with the AWS API outside of the AWS Management Console



An Access Key is commonly referred to as **AWS Credentials**

A user must be **granted access** to use Access Keys

Select AWS credential type\*

**Access key - Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**Password - AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

- Never share your access keys
- Never commit access keys to a codebase
- You can have two active Access Keys
- You can deactivate Access Keys
- Access Keys have whatever access a user has to AWS resources.

**Generate** an Access Key and Secret

Access key ID	Secret access key
AKIAZRJ1QN2ODG55TBXO	jZxt1gj1PE1f/y9k5JVI2TnvvQ6CSwanzg8aUP3O Hide



# Access Keys

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Access Keys are to be stored in `~/.aws/credentials` and follow a TOML file format

**Default** will be the access key used when no profile is specified.

You can store multiple access keys by giving the **profile** names.

You can use the **aws configure** CLI command to populate the credential file.

The AWS SDK will automatically read from these environment variables.

This is the safe way of using an Access Key within your code.

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY
[exampro]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY
region=ca-central-1
```

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

```
$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
$ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY
$ export AWS_DEFAULT_REGION=us-west-2
```

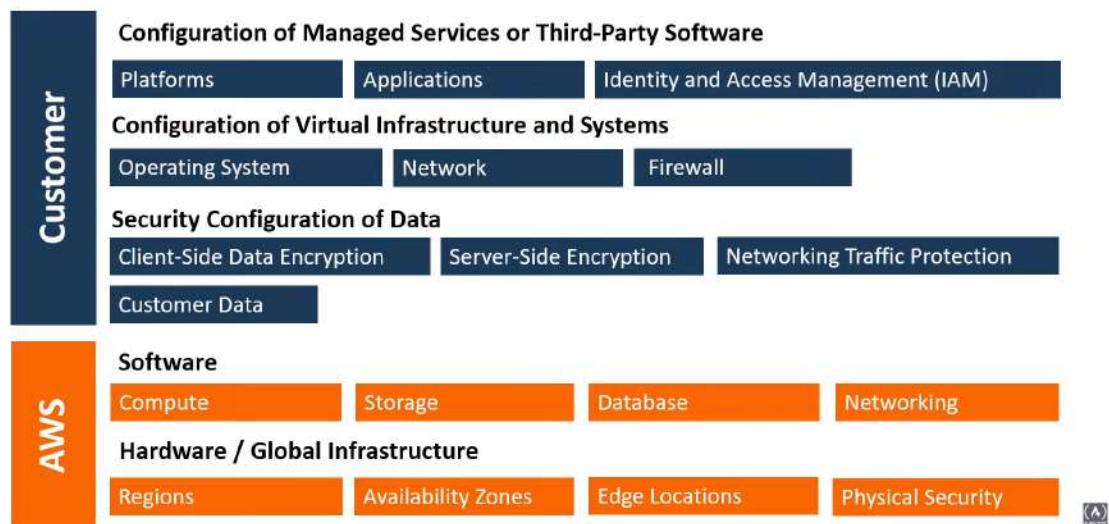


## ▼ 7. Shared Responsibility Model

### ▼ 1. What is Shared Responsibility Model

# AWS Shared Responsibility Model

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



# AWS Shared Responsibility Model

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Customers are responsible for Security **in** the Cloud



**Data Configuration**



**Hardware  
Operation of Managed Services  
Global Infrastructure**

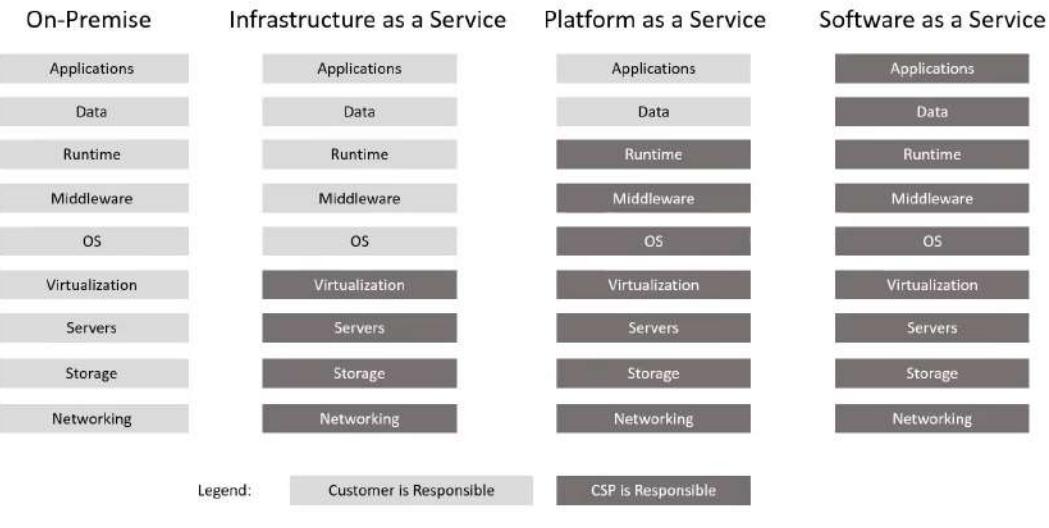
AWS is responsible for Security **of** the Cloud



## ▼ 2. Types of Cloud Computing Responsibility

# Types of Cloud Computing Responsibility

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## ▼ 3. Shared Responsibility Model Compute

### Shared Responsibility Model – Compute

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Let us take a look at **compute** as a comparison example of the Shared Responsibility Model

#### Infrastructure as a Service (IaaS)



##### Bare Metal EC2 Bare Metal Instance

- Customer:
- The Host OS Configuration
  - Hypervisor
- AWS
- Physical machine



##### Virtual Machine Elastic Cloud Compute (EC2)

- Customer:
- The Guest OS Configuration
  - Container Runtime
- AWS
- Hypervisor, Physical machine



##### Containers AWS Elastic Container Service(ECS)

- Customer:
- Configuration of containers
  - Deployment of Containers
  - Storage of containers
- AWS
- The OS, The Hypervisor, Container Runtime

#### Platform as a Service (PaaS)



##### Managed Platform AWS Elastic Beanstalk

- Customer:
- Uploading your code
  - Some configuration of environment
  - Deployment strategies
  - Configuration of associated services
- AWS
- Servers, OS, Networking, Storage, Security

#### Software as a Service (SaaS)



##### Content Collaboration Amazon WorkDocs

- Customer:
- Contents of documents
  - Management of files
  - Configuration of sharing access controls
- AWS
- Servers, OS, Networking, Storage, Security

#### Function as a Service (FaaS)



##### Functions AWS Lambda

- Customer:
- Upload your code
- AWS
- Deployment, Container Runtime, Networking, Storage, Security, Physical Machine, (basically everything)



## ▼ 4. Shared Responsibility Model for IaaS, Paas and SaaS

## Shared Responsibility Model

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

The **Shared Responsibility Model** is a simple visualization that helps determine what the customer is responsible for and what the CSP is responsible for related to AWS.

The customer is responsible for the data and the **configuration** of access controls that resides in AWS.

The customer is responsible for the **configuration** of cloud services and granting access to users via permissions.

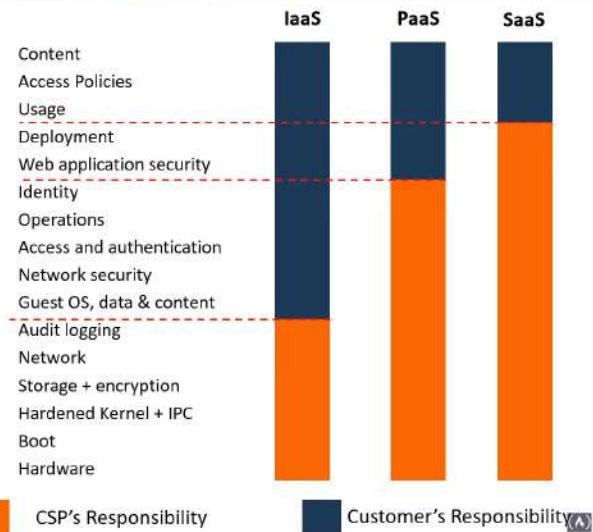
CSP is generally responsible for the underlying Infrastructure.

### Responsibility of in the cloud

If you can configure or store it then you (the customer) are responsible for it.

### Responsibility of the cloud

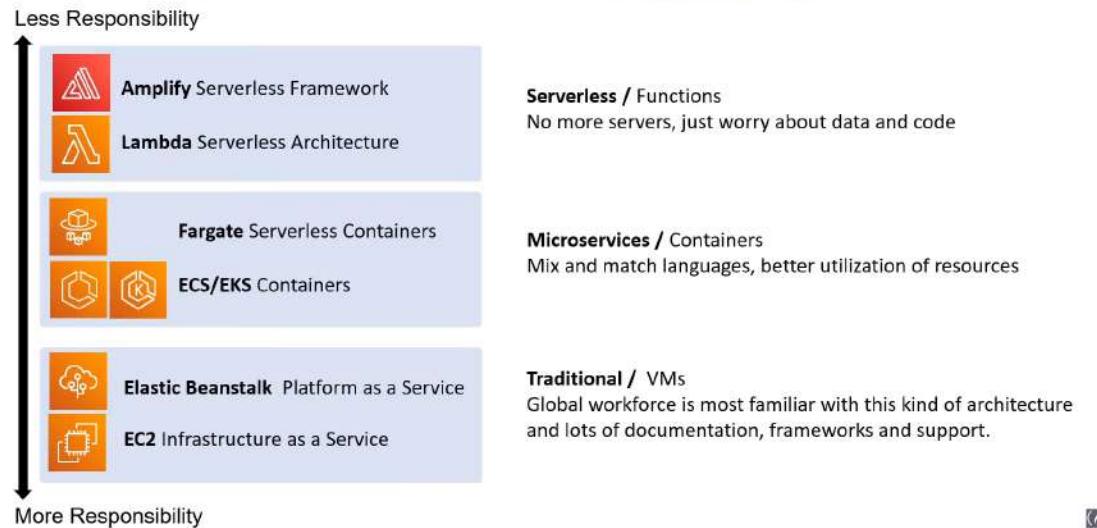
If you can not configure it then CSP is responsible for it



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

## Shared Responsibility Model - Architecture

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## ▼ 8. Compute

### ▼ 1. EC2 Overview

# Computing Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## Elastic Compute Cloud (EC2) allows you to launch Virtual Machines (VM)

### What is a Virtual Machine?

A Virtual Machine (VM) is an emulation of a physical computer using software.

Server Virtualization allows you to easily **create, copy, resize or migrate** your server.

Multiple VMs can run **on the same physical server** so you can share the cost with other customers.

*Imagine if your server or computer was an executable file on your computer*

When we launch a Virtual Machine we call it an "**instance**"

EC2 is **highly configurable** where you can choose **AMI** that affects options such as:

- The amount of CPUs
- The amount of Memory (RAM)
- The amount of Network Bandwidth
- The Operation System (OS) eg. Windows 10, Ubuntu, Amazon Linux 2
- Attach multiple virtual hard-drives for storage eg. Elastic Block Store (EBS)



An Amazon Machine Image (AMI) is a predefined configuration for a Virtual Machine.



EC2 is also considered **the backbone of AWS** because the majority of AWS services are using EC2 as their underlying servers. eg. S3, RDS, DynamoDB, Lambdas



## ▼ 2. Computing Services

# Computing Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**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

*When you need to launch a Linux or Windows server but don't have much AWS knowledge. eg. Launch a Wordpress*

**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 **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 Lambda is 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 are charged based on the runtime of the serverless function rounded to the nearest 100ms. 

## ▼ 3. High Computing Services

## Higher Performance Computing Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

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

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



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

**What is High Performance Computing (HPC)?**

A cluster of hundreds of thousands of servers with fast connections between each of them with the purpose of boosting computing capacity.  
*When you need a supercomputer to perform computational problems too large to run on a standard computers or would take to long.*



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



## ▼ 4. Edge and Hybrid Computing Services

### Edge and Hybrid Computing Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**What is Edge Computing?**

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

**What is Hybrid Computing?**

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



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



**AWS Wavelength** allows you to **build and launch your applications in a telecom datacenter**. By doing this your applications will 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 be 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*



## ▼ 5. Cost and Capacity Management



## Cost and Capacity Management Computing Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**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 Instances 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



**AWS 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**.



(A)

## ▼ 9. Storage

### ▼ 1. Types of Storage Services

#### Types of Storage Services

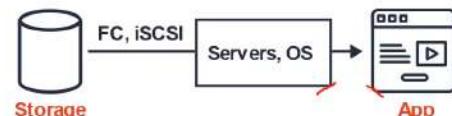
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



##### Elastic Block Store (EBS) - Block

Data is split into evenly split blocks  
Directly accessed by the Operation System  
Supports only a single write volume

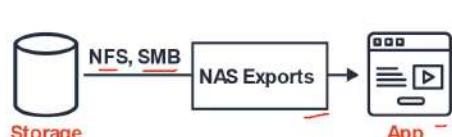
When you need a virtual hard drive attached to a VM



##### AWS Elastic File Storage (EFS) - File

File is stored with data and metadata  
Multiple connections via a network share  
Supports multiple reads, writing locks the file.

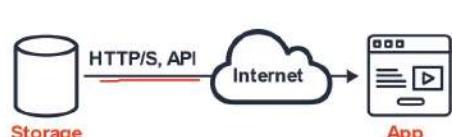
When you need a file-share where multiple users or VMs need to access the same drive



##### Amazon Simple Storage Service (S3) - Object

Object is stored with data, metadata and Unique ID  
Scales with limited no file limit or storage limit  
Supports multiple reads and writes (no locks)

When you just want to upload files, and not have to worry about underlying infrastructure. Not intended for high IOPs



(A)

### ▼ 2. What is S3

# Introduction to S3

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is Object Storage (Object-based Storage)?

data storage architecture that manages data as objects, as opposed to other storage architectures:

- **file systems** which manages data as a files and file 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

Objects contain your data. They are like files.

Object may consist of:

- **Key** this is the name of the object
- **Value** the data itself made up of a sequence of bytes
- **Version ID** when versioning enabled, the version of object
- **Metadata** additional information attached to the object



### S3 Bucket

Buckets hold objects. Buckets can also have folders which in turn hold objects

S3 is a universal namespace so bucket names must be unique  
(think like having a domain name)

You can store an individual object from **0 Bytes** to **5 Terabytes** in size



## ▼ 3. S3 Storage Classes

# S3 Storage Classes

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

AWS offers a range of S3 storage classes that trade **Retrieval Time, Accessibility and Durability** for **Cheaper Storage**

### S3 Standard (default)

Fast! 99.99% Availability, 11 9's Durability. Replicated across at least three AZs

### S3 Intelligent Tiering

Uses ML to analyze object usage and determine the appropriate storage class.

Data is moved to the most cost-effective access tier, without any performance impact or added overhead.

### S3 Standard-IA (Infrequent Access)

Still Fast! Cheaper if you access files less than once a month.

Additional retrieval fee is applied. **50% less** than Standard (reduced availability)

### S3 One-Zone-IA

Still Fast! Objects only exist in one AZ. Availability (is 99.5%). but cheaper than Standard IA by 20% less  
(Reduce durability) Data could get destroyed. A retrieval fee is applied.

### S3 Glacier

For long-term cold storage. Retrieval of data can take minutes to hours but the off is very cheap storage

### S3 Glacier Deep Archive

The lowest cost storage class. Data retrieval time is 12 hours.

S3 Outposts has its own storage class.



↓  
Cheaper

## ▼ 4. AWS Snow Family

## AWS Snow Family

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

AWS Snow Family are **storage and compute devices used to physically move data in or out the cloud** when moving data over the internet or private connection it is slow, difficult or costly.



**Snowcone**

Comes in two sizes:

- 8 TB of Storage (HHD)
- 14 TB of Storage (SSD)



**Snowball Edge**

Comes generally in two types:

- Storage Optimized
  - 80 TB
- Compute Optimized
  - 39.5 TB



**Snowmobile**

100 PB of storage



Data is delivered to Amazon S3



## ▼ 5. Storage Services

### Storage Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**Simple Storage Service (S3)** is a **serverless object storage service**. You can upload very large files 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.



**S3 Glacier** is a **cold storage service**. It designs as a low cost storage solution for **archiving and long-term backup**. It uses previous generation HDD drives to get that low cost. It's highly secure and durable.



**Elastic Block Store (EBS)** 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**



**Elastic File Storage (EFS)** is a **cloud-native NFS file system service**. File storage you can mount to multiple EC2 instances at the same time. **When you need to share files between multiple servers**



**Storage Gateway** is a **hybrid cloud storage** service that extends your on-premise storage to 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.



## ▼ 10. Database

### ▼ 1. Data Warehouse

## What is Data Warehouse?

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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**

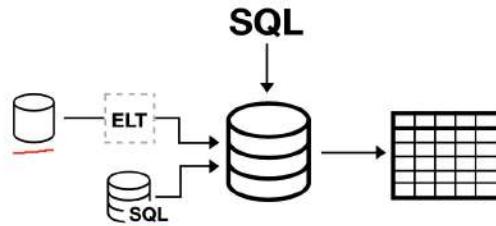
- aggregation is grouping data eg. find a total or average
- Data warehouses are optimized around columns since they need to quickly aggregate column data

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 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.



(A)

## ▼ 2. Key/Value Store

### What is a Key / Value store?

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

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

Key	Value
Data	101010100010101100101001010101001
Worf	0110101100010101010101011100010
Ro Laren	001010100101011001010101010101010

Key values stores are **dumb and fast**.

They generally lack features like:

- Relationships
- Indexes
- Aggregation

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

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

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

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

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

(A)

## ▼ 3. Document Store

## What is a Document store?

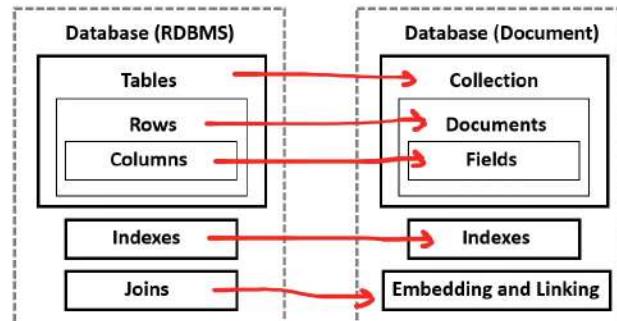
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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 sub-class of Key/Value stores

The components of a document store compared to Relational database



(A)

## ▼ 4. No SQL Database Service

### NoSQL Database Service

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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



In 2019, **Amazon** the online shopping retail shutdown their last Oracle database and completed their migration to DynamoDB. They had 7,500 Oracle Database and 75 petabytes of data. With DynamoDB they reduce costs by 60% and reduce latency by 40%

*When we want a massively scalable database*



**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.

*When you want a 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.*



(A)

## ▼ 5. Relational Database Services

# Relational Database Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**Relational Database Service (RDS)** is a **relational database service** that supports multiple SQL engines. Relational is synonymous with SQL and Online Transactional Processing (OLTP). Relational database are **the most commonly used type of database** among tech companies and start-ups.

## RDS Supports the following SQL Engines:

- **MySQL** – The most popular open-source SQL database that was purchased and now owned by Oracle.
- **MariaDB** – When Oracle bought MySQL. MariaDB made a fork (copy) of MySQL was made under a different open-source license.
- **Postgres (PSQL)** – Most popular open-source SQL database among developers. Has rich-features over MySQL but at added complexity
- **Oracle** – Oracle's proprietary SQL database. Well used by Enterprise companies. You have to buy a license to use it.
- **Microsoft SQL Server** – Microsoft's proprietary SQL database. You have to buy a license to use it.
- **Aurora** – Fully managed database.



MariaDB



Microsoft  
SQL Server



**Aurora** is a **fully managed** database of either MySQL (5x faster) and PSQL (3x faster) database.

*When you want a highly available, durable, scalable and secure relational database for Postgres or MySQL*



**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*



**RDS on VMware** allows you to deploy RDS supported engines to on **an-premise** data-center. The datacenter must be using VMware for server virtualization. *When you want databases managed by RDS on your own datacenter*



## ▼ 6. Other Database Services

# Other Database Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**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.*



**ElastiCache** is a managed database of the **in-memory** and **caching** open-source databases **Redis** or **Memcached**. *When you need to improve the performance of application by adding a caching layer in-front of web-server or database.*



**Neptune** is a managed graph database. Data is represented as interconnected nodes. *When you need to understand the connections between data eg. Mapping Fraud Rings or Social Media relationships*



**Amazon Timestreams** is a fully managed time series database. Think of devices that send lots of data that are time-sensitive such as IoT devices. *When you need to measure how things change over time.*



**Amazon Quantum Ledger Database** is a fully managed ledger database that provides transparent, immutable and cryptographically variable transaction logs. *When you need to record history of financial activities that can be trusted.*



**Database Migration Service (DMS)** is database migration service. You can migrate from:

- on-premise database to AWS
- from two database in different or same AWS accounts using different SQL engines
- from an SQL to NoSQL database



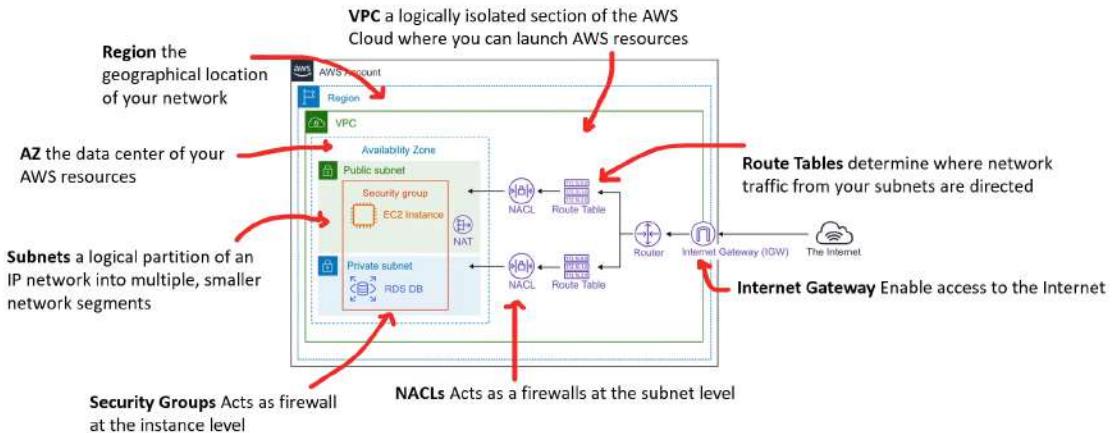
## ▼ 11. Networking

### ▼ 1. Cloud Native Networking Services



## Cloud-Native Networking Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

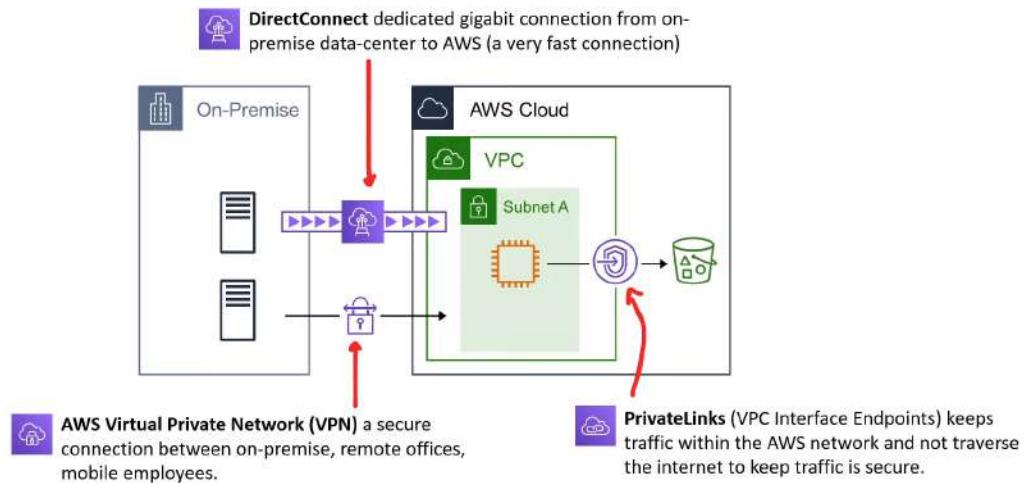


## ▼ 2. Enterprise/Hybrid Networking



## Enterprise/Hybrid Networking

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## ▼ 3. VPC and Subnets

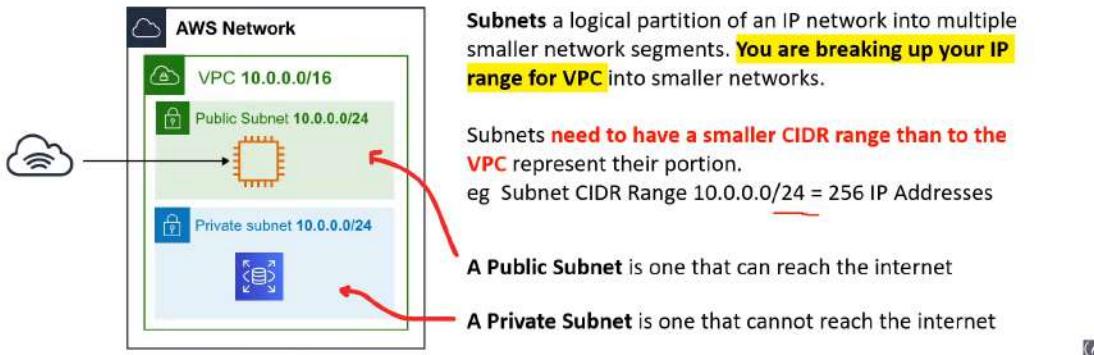


## Virtual Private Cloud (VPC) and Subnets

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**Virtual Private Cloud (VPC)** is a logically isolated section of the AWS Network where you launch your AWS resources. You choose a **range of IPs using CIDR Range**

CIDR Range of **10.0.0.0/16 = 65,536** IP Addresses



(A)

## ▼ 4. Security Group vs NACL

### Security Groups vs NACLs

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

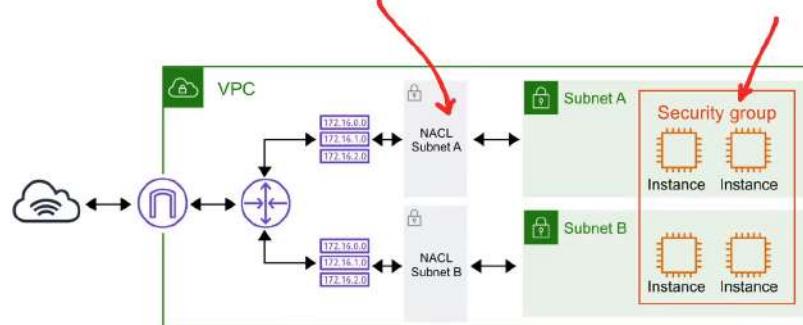
#### Network Access Control Lists (NACLs)

Acts as a virtual **firewall at the subnet level**  
You create **Allow and Deny rules**.

eg. Block a specific IP address known for abuse

#### Security Groups

Acts as a virtual **firewall at the instance level**  
Implicitly denies all traffic. **You create only Allow rules**.  
eg. Allow an EC2 instance access on port 22 for SSH  
eg. You cannot block a single IP address.



(A)

## ▼ 12. EC2

## ▼ 1. Introduction to EC2

### Introduction to EC2

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Elastic Compute Cloud (EC2) is a **highly configurable virtual server**. EC2 is resizable **compute capacity**. It takes **minutes** to launch new instances. Anything and everything on AWS uses EC2 Instance underneath.

AMI	Red Hat	ubuntu	Windows	Amazon Linux	SUSE
t2.nano \$0.0065/hour (\$4.75/month) 1 vCPU 0.5GB Mem	C4.8xlarge \$1.591/hour (\$1161.43/month) 36 vCPU 60GB Mem 10 Gigabit performance				
SSD HDD Virtual Magnetic Tape Multiple Volumes					
Security Groups, Key Pairs, UserData, IAM Roles, Placement Groups					

## ▼ 2. EC2 Instance Families

### EC2 Instance Families

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**What are Instance Families?**  
Instance families are different combinations of CPU, Memory, Storage and Networking capacity.

Instance families allow you to choose the appropriate combination of capacity to meet your application's unique requirements.

Different instance families are different because of the varying hardware used to give them their unique properties.

Commonly instance families are called "Instance Types" but an instance type is a combination of size and family.

**General Purpose**  
**A1 T2 T3 T3a T4g M4 M5 M5a M5n M6zn M6g M6i Mac**  
balance of compute, memory and networking resources  
*Use-cases* web servers and code repositories

**Compute Optimized**  
**C5 C4 Cba C5n C6g C6gn**  
Ideal for compute bound applications that benefit from high performance processor  
*Use-cases* scientific modeling, dedicated gaming servers and ad server engines

**Memory Optimized**  
**R4 R5 R5a R5b R5n X1 X1e High Memory z1d**  
fast performance for workloads that process large data sets in memory.  
*Use-cases* in-memory caches, in-memory databases, real time big data analytics

**Accelerated Optimized**  
**P2 P3 P4 G3 G4ad G4dn F1 Inf1 VT1**  
hardware accelerators, or co-processors  
*Use-cases* Machine learning, computational finance, seismic analysis, speech recognition

**Storage Optimized**  
**I3 I3en D2 D3 D3en H1**  
high, sequential read and write access to very large data sets on local storage  
*Use-cases* NoSQL, in-memory or transactional databases, data warehousing

## ▼ 3. EC2 Instance Types

## EC2 Instance Types

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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
  - ....



Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)				
	Family	Type	vCPUs	Memory (GiB)
	t2	t2.nano	1	0.5
■	t2	<b>t2.micro</b> <small>Free tier eligible</small>	1	1
	t2	t2.small	1	2
	t2	t2.medium	2	4
	t2	t2.large	2	8
	t2	t2.xlarge	4	16

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

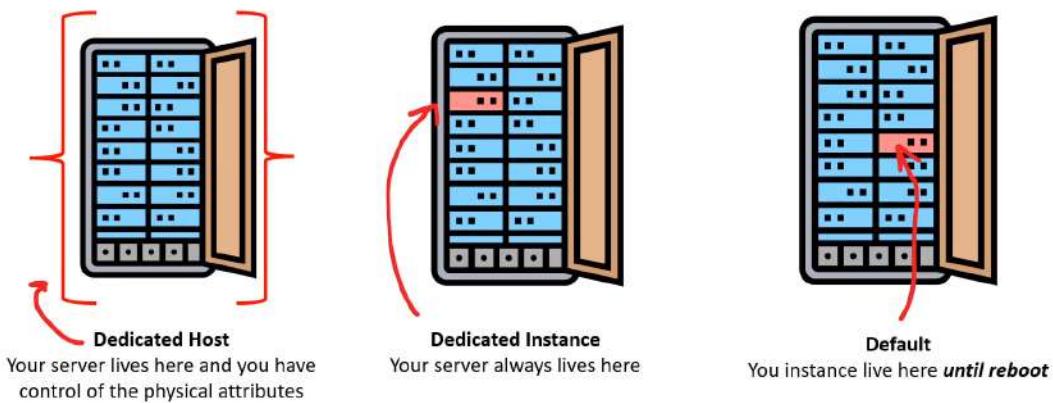


## ▼ 4. EC2 Tenancy

### EC2 Tenancy

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

EC2 has three levels of tenancy:



## ▼ 13. EC2 Pricing Model

### ▼ 1. EC2 Pricing Model

# EC2 Pricing Models

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

There are 5 different ways to pay for EC2 (Virtual Machines)

## On-Demand

Least Commitment

- low cost and flexible
- only pay per hour or the second
- short-term, spiky, unpredictable workloads
- cannot be interrupted
- For first time apps

## Reserved up to 75% off

Best Long-term

- steady state or predictable usage
- commit to EC2 over a 1 or 3 year term
- Can resell unused reserved instances

## Spot up to 90%

BIGGEST SAVINGS

- request spare computing capacity
- flexible start and end times
- Can handle interruptions (server randomly stopping and starting)
- For non-critical background jobs

## Dedicated

Most Expensive

- Dedicated servers
- Can be on-demand or reserved or spot
- When you need a guarantee of isolate hardware (enterprise requirements)

AWS Savings Plan is another way to save but can be used for more than just EC2.



## ▼ 2. On Demand

# On-Demand

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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** using **On-Demand** Pricing

[Launch instances](#)

On-demand has **no up-front payment** and **no long-term commitment**

You are charged by the **second (minimum of 60 seconds)** or the **hour**

*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.

Viewing 363 of 363 available instances						
Instance name	On-Demand hourly rate	vCPU	Memory	Storage	Network performance	
t2.nano	\$0.0058	1	0.5 GB	EBS Only	Low	
t2.micro	\$0.0116	1	1 GB	EBS Only	Low to Moderate	

On-Demand is for applications where the workload is for **short-term, spiky or unpredictable**.

When you have a **new app** for development or you want to run experiment.



## ▼ 3. Reserved Instance

# Reserved Instances (RI)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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 they 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 greater 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**

**Unused RIs** can be sold in the **Reserved Instance Marketplace**



## ▼ 4. Reserved Instance Attributes

### Reserved Instances (RI) – RI Attributes

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**RI Attributes** (aka Instance Attributes) are limited based on Class Offering and can affect the final price of an RI instance. There are 4 RI Attributes:



**1. Instance type:** For example, m4.large. This is composed of the instance family (for example, m4) and the instance size (for example, large).



**2. Region:** The Region in which the Reserved Instance is purchased.



**3. Tenancy:** Whether your instance runs on shared (default) or single-tenant (dedicated) hardware.



**4. Platform:** The operating system eg. Windows or Linux/Unix.



## ▼ 5. RI Limits

## RI Limits

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

### Per month you can purchase

- 20 Regional Reserved Instances *per Region*
- 20 Zonal Reserved Instances *per AZ*

#### Regional Limits

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

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

#### Zonal Limits

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

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



## ▼ 6. Standard vs Convertible RI

### Standard vs Convertible RI

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

There are some key difference between Standard and Convertible

#### Standard RI

RI attributes can be modified

- Change the AZ within same Region
- Change the scope of the Zonal RI to Regional RI or visa versa
- Change the instance size (Linux/Unix only, default tenancy )
- Change network from Ec2-Classic to VPC and visa-versa

Can't be exchanged

Can be bought or sold in the RI Marketplace

#### Convertible RI

RI attributes can't be modified (you perform an exchange)

Can be exchanged during the term for another Convertible RI with new RI attributes, including:

- instance family
- instance type
- platform
- scope
- tenancy

Can't be bought or sold in the RI Marketplace



## ▼ 7. RI MarketPlace

## RI Marketplace

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



EC2 Reserved Instance Marketplace allows you to **sell your unused Standard RI** to recoup your RI spend for RI you do not intend or cannot use.

- Reserved Instances can be sold after they have been active for at least 30 days and once AWS has received the upfront payment (if applicable).
- You must have a US bank account to sell Reserved Instances on the Reserved Instance Marketplace.
- There must be at least one month remaining in the term of the Reserved Instance you are listing.
- You will retain the pricing and capacity benefit of your reservation until it's sold and the transaction is complete.
- Your company name (and address upon request) will be shared with the buyer for tax purposes.
- A seller can set only the upfront price for a Reserved Instance. The usage price and other configuration (e.g., instance type, Availability Zone, platform) will remain the same as when the Reserved Instance was initially purchased.
- The term length will be rounded down to the nearest month. For example, a reservation with 9 months and 15 days remaining will appear as 9 months on the Reserved Instance Marketplace.
- You can sell up to \$20,000 in Reserved Instances per year. If you need to sell more Reserved Instances.
- Reserved Instances in the GovCloud region cannot be sold on the Reserved Instance Marketplace.



## ▼ 8. Spot Instances

### Spot Instances

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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 discount to fill vacant seats

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

Designed for applications that have flexible start and end times or applications that are only feasible at **very low** compute costs.

**Load balancing workloads**  
Launch instances of the same size, in any Availability Zone.  
Good for running web services.

**Flexible workloads**  
Launch instances of any size, in any Availability Zone. Good for running batch and CI/CD jobs.

**Big data workloads**  
Launch instances of any size, in a single Availability Zone. Good for MapReduce jobs.



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

#### Termination Conditions

Instances can be terminated by AWS **at anytime**

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 any hour that it ran.



## ▼ 9. Dedicated Instances

## Dedicated Instances

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Dedicated Instances is 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**.



**Multi-Tenant**

think of everyone living in an apartment



**Single Tenant**

think of everyone having their own house



Multi-Tenant



Single-Tenant



Single-Tenant

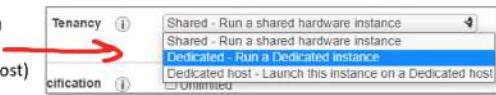
When multiple customers are running workloads on the same hardware. **Virtual Isolation** is what separates customers

When a single customer has dedicated hardware. **Physical Isolation** is what separates customers

Dedicated can be offered for:

- **On-demand**
- **Reserved (up to 60% savings)**
- **Spot (up to 90% savings)**

You choose tenancy when you **launch** your EC2  
(Notice there is a Dedicated Host)



**Enterprises and Large Organizations** may have security concerns or obligations about against sharing the same hardware with other AWS Customers.



## ▼ 10. AWS Savings Plan

### AWS Savings Plan

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.



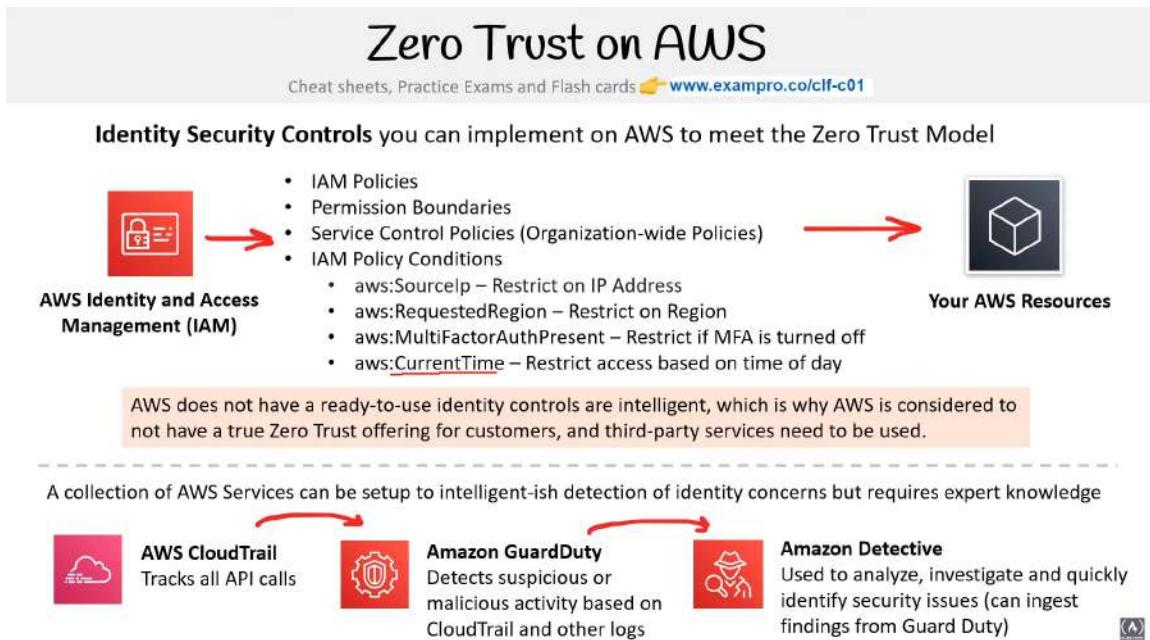
**SageMaker**

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

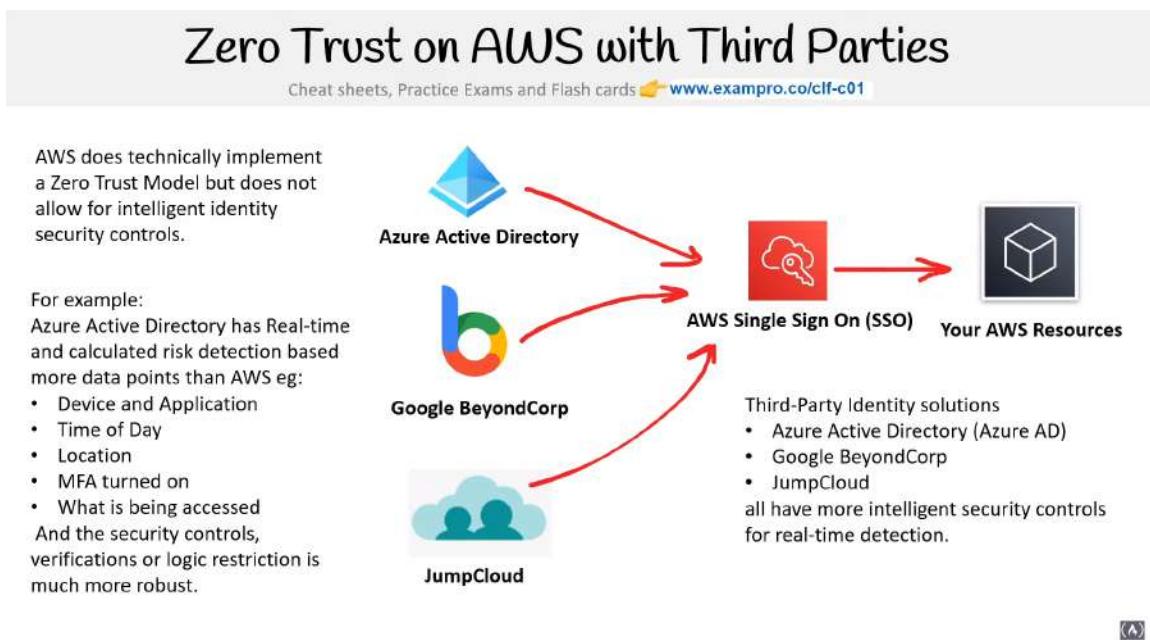


## ▼ 14. Identity

## ▼ 1. Zero Trust Model



## ▼ 2. Zero Trust Model on Third Parties



## ▼ 3. Directory Service

# Directory Service

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is a directory service?

A directory service maps the **names of network resources to their network addresses.**

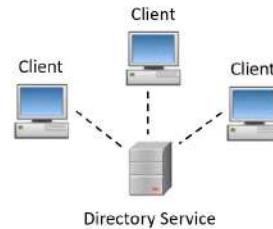
A directory service is shared information infrastructure for **locating, managing, administering and organizing** resources:

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

A directory service is a critical component of a network operating system

A directory server (name server) is a server which provides a directory service

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



## Well known directory services:

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



## ▼ 4. Internet Providers

# Identity Providers (IdPs)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

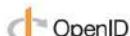
**Identity Provider (IdP)** a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to applications within a **federation** or distributed network.

A trusted provider of your user identity that lets you use authenticate to access other services.

Identity Providers could be: **Facebook, Amazon, Google, Twitter, Github, LinkedIn**

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

### OpenID



open standard and decentralized authentication protocol. Eg be able to login into a different social media platform using a Google or Facebook account

*OpenID is about providing who are you*

### OAuth2.0

industry-standard protocol for authorization OAuth doesn't share password data but instead uses authorization tokens to prove an identity between consumers and service providers.

*Oauth is about granting access to functionality*

### SAML

Security Assertion Markup Language is an open standard for exchanging authentication and authorization between an identity provider and a service provider.

An important use case for SAML is **Single-Sign-On via web browser.**



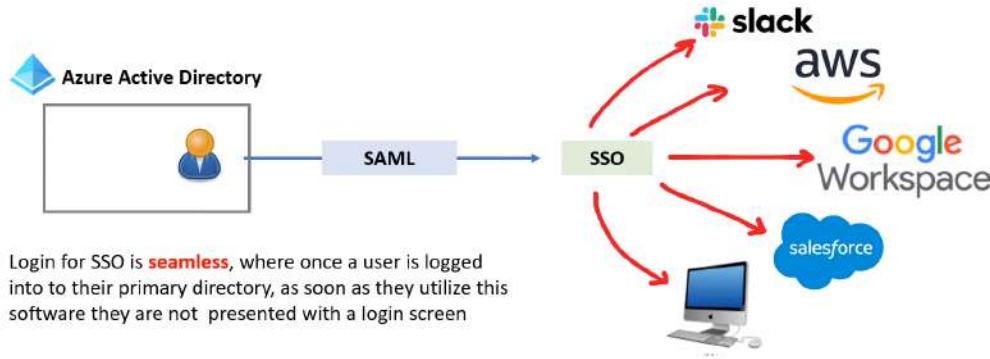
## ▼ 5. Single Sign On (SSO)

## Single-Sign-On

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**Single sign-on (SSO)** is an authentication scheme that **allows a user to log in with a single ID and password to different systems and software.**

SSO allows IT departments to administer a single identity that can access many machines and cloud services.



## ▼ 6. Lightweight Directory Access Protocol ( LDAP )

### LDAP

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

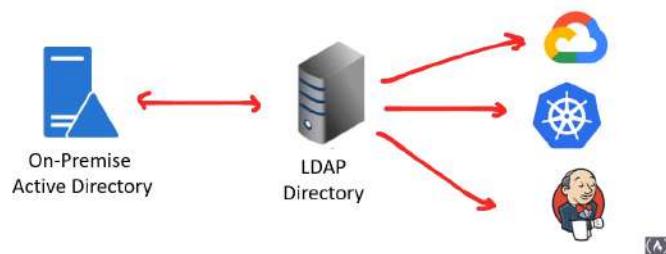
**Lightweight Directory Access Protocol (LDAP)** is an open, vendor-neutral, industry standard **application protocol for accessing and maintaining distributed directory information services** over an Internet Protocol (IP) network.

A common use of LDAP is to provide a central place to store usernames and passwords

LDAP enables for **same-sign on**. Same sign-on allows users to single ID and password, but they have to enter it in every time they want to login.

Why use LDAP when SSO is more convenient?

Most SSO systems are using LDAP.  
LDAP was not designed natively to work with web-applications.  
Some systems only support integration with LDAP and not SSO



## ▼ 7. Multi Factor Authentication ( MFA )

# Multi-Factor Authentication

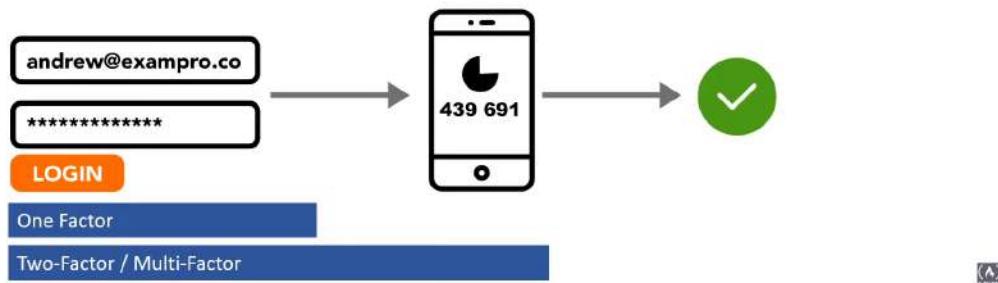
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is Multi-Factor Authentication (MFA)?

A security control where after you fill in your username/email and password **you have to use a second device** such as a phone to confirm that its you logging in.

MFA **protects** against people who have stolen your password.

MFA is an option in most cloud providers and even social media websites such as Facebook.



## ▼ 8. Security Keys

### Security Keys

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

#### What is a Security Key?

A secondary device used as second step in authentication process to gain access to a device, workstation or application.

**A popular brand of security key is an Yubikey**

A security key can resemble a memory stick. When your finger makes contact with a button of exposed metal on the device it will generate And autofill a security token.



- Works out of the box with Gmail, Facebook, and hundreds more
- Supports **FIDO2**/WebAuthn, U2F
- Waterproof and crush resistant
- USB-A and NFC dual connectors on a single key

## ▼ 9. AWS Identity Access Management ( IAM )

# AWS Identity and Access Management (IAM)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



AWS Identity and Access Management (IAM ) you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.



**IAM Policies** JSON documents which grant permissions for a specific user, group, or role to access services. Policies are attached to **IAM Identities**

**IAM Permission**

The API actions that can or cannot be performed.  
They are represented in the IAM Policy document

## IAM Identities



**IAM Users**

End users who log into the console or interact with AWS resources programmatically or via clicking UI interfaces



**IAM Groups**

Group up your Users so they all share permission levels of the group  
eg. Administrators, Developers, Auditors



**IAM Roles**

Roles grant AWS resources permissions to specific AWS API actions  
Associate policies to a Role and then assign it to an AWS resource



## ▼ 10. Principal of Least Privilege ( PoLP )

### Principle of Least Privilege (PoLP)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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



## ▼ 11. AWS Account Root User

# AWS Account Root User

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

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



## ▼ 15. Application Integration

### ▼ 1. What is Application Integration.

#### Application Integration

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



##### What is Application Integration?

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



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

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

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



### ▼ 2. Queuing

# Queueing

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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?

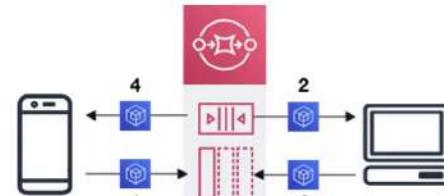
A Queueing system is a messaging system that generally will delete messages once they are consumed.  
Simple communication. **Not Real-time.** Have to pull. Not reactive.



### 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.



(A)

## ▼ 3. Streaming

# Streaming

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

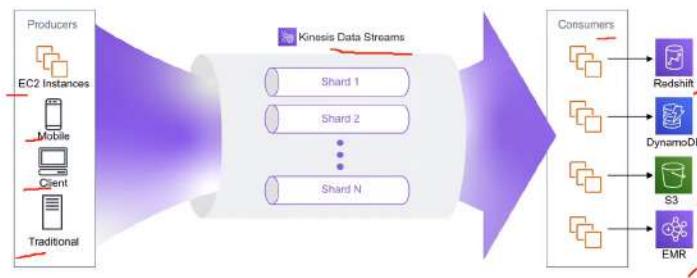
## What is streaming?

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.



(A)

## ▼ 4. Pub/Sub ( Publisher/Subscriber )

## Pub/Sub

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.



- Publishers 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

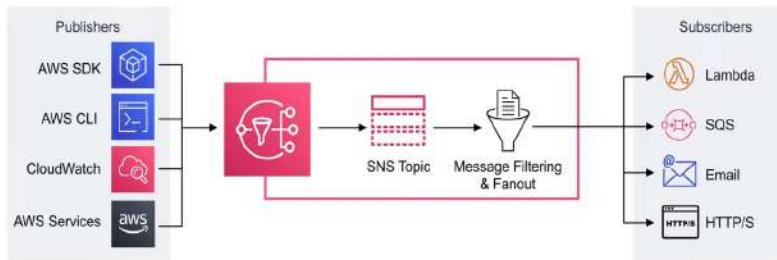
(A)

## Pub/Sub

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.



(A)

## ▼ 5. API Gateway

# API Gateway

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

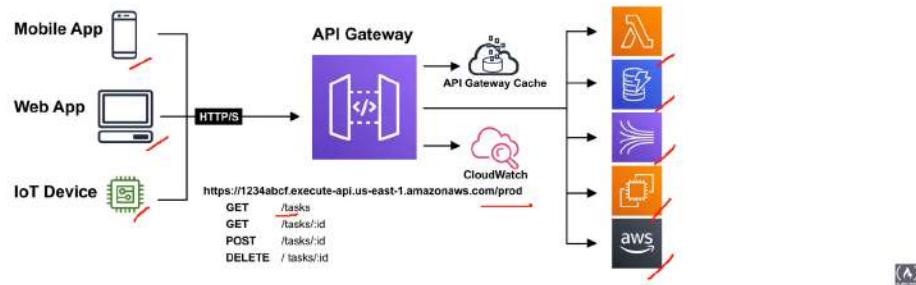
## What is an API Gateway?

An API Gateway is a program that sits between a single-entry point and multiple backends.

API Gateway allows for throttling, logging, routing logic or formatting of the request and response



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



## ▼ 6. State Machines

# State Machines

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is a state machine?

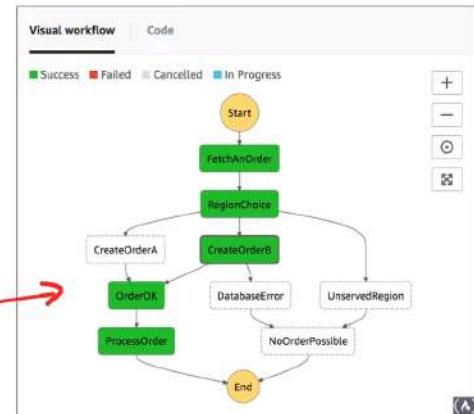
A state machine is an abstract model which decides how one state moves to another based on a series of conditions. **Think of a state machine like a flow chart.**



### What is AWS Step Functions?

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

Any one of these steps could be using an AWS Service



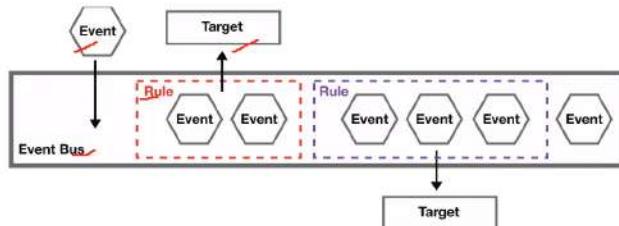
## ▼ 7. Event Bus and Amazon Event Bridge

# Event Bus

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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](http://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 work with Third party SaaS Providers

## Rules

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

## Producers

AWS Services that emit events

Default Event Bus

Custom Event Bus

SaaS Event Bus

## Targets

AWS Services that consume events (5 targets per rule)



Events

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

## Partner Sources

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



## ▼ 16. Containers

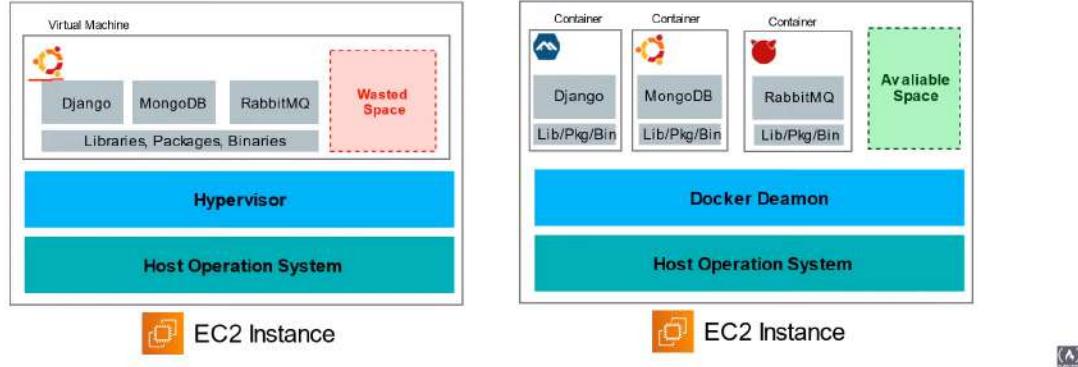
### ▼ 1. VMs vs Containers

## VMs vs Containers

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

VMs **do not** make best use of space.  
Apps are not isolated which. Could cause  
**config conflicts, security problems**  
or **resource hogging**.

Containers allow you to run multiple apps which  
are virtually isolated from each other.  
Launch new containers and configure OS  
Dependencies per container.



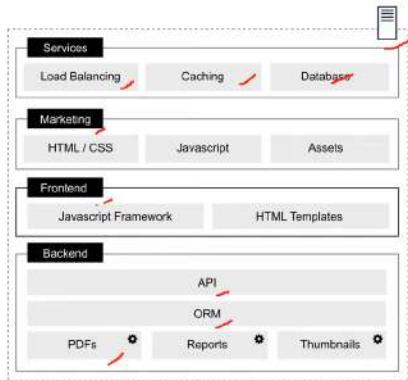
## ▼ 2. What are Microservices

### What are Microservices

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

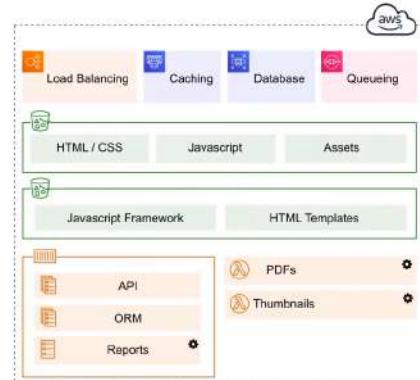
#### Monoistic Architecture

One app which is responsible for everything  
Functionality is tightly coupled



#### Microservices Architecture

VS    Multiple apps which are each responsible for one thing  
Functionality is isolate and stateless



## ▼ 3. Kubernetes

# Kubernetes

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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



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

Kubernetes is commonly called **K8s**

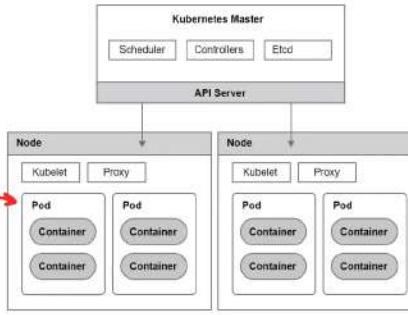
- The 8 represent the remaining letters "ubernete"

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

A unique component of Kubernetes are **Pods**.

A pod is a group of one or more containers with shared storage, network resources and other shared settings.

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



(A)

## ▼ 4. Docker

# Docker

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

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

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

Docker CLI – CLI commands to download, upload, build, run and debug containers

Dockerfile – a configuration file on how to provision a container

Docker Compose – is a tool and configuration file when working with multiple containers

Docker Swarm – An orchestration tool for managing deployed multi-containers architectures

Dockerhub – a public online repository for containers published by the community for download



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

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

(A)

## ▼ 5. PodMan

## Podman, Buildah and Skopeo

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**Podman** is a container engine that is OCI-compliant and is a drop-in replacement for Docker.

- Podman is daemon-less where Docker uses a containedr deamon
- Podman allows you to create pods like K8, Docker does not have pods
- Podman only replaces one part of Docker. Podman is to be used alongside Buildah and Skopeo



**Buildah** is a tool used to build OCI Images



**Skopeo** a tool for moving container images between different types of container storages

(A)

## ▼ 6. Container Services

### Container Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

#### Primary Services



**Elastic Container Service (ECS)**  
No Cold Starts  
Self-Managed EC2



**AWS Fargate**  
More Robust Than Lambda  
Scale to Zero Cost  
AWS-Managed EC2



**Elastic Kubernetes Services (EKS)**  
Open Source  
Avoid Vendor Lock-In



**AWS Lambda**  
Only think about code  
Short running tasks  
Can deploy custom containers

#### Provisioning and Deployment



**Elastic Beanstalk (EB)**  
ECS on training wheels  
Platform as a Service



**App Runner**  
Platform as a Service specifically for containers



**AWS Copilot CLI**  
build, release and operate production ready containerized applications on AWS App Runner, Amazon ECS, and AWS Fargate

#### Supporting Services



**Elastic Container Registry (ECR)**  
Repos for your Docker Images



**X-Ray**  
Analyze and debug between microservices



**Step Functions**  
Stitch together Lambdas and ECS tasks

(A)

## ▼ 17. Governance

### ▼ 1. AWS Organizations and Accounts

# Organizations and Accounts

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**AWS Organizations** allow the creation of new AWS accounts. Centrally manage billing, control access, compliance, security, and share resources across your AWS accounts.

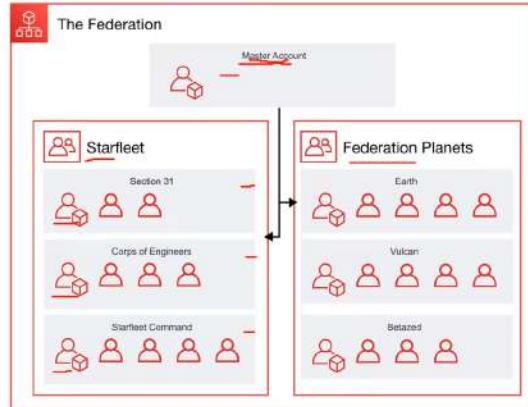


**Root Account User** is a single sign-in identity that has complete access to all AWS services and resources in an account. Each account has a Root Account User



**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



## ▼ 2. AWS Control Tower

### AWS Control Tower

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



AWS Control Tower helps **Enterprises** quickly set-up a secure, **AWS multi-account** Provides you with a **baseline environment** to get started with a **multi-account architecture**



#### Landing Zone

A landing zone is a baseline environment following well-architected and best practices to start launching production ready workloads.

- AWS SSO enabled, Centralized logging for AWS CloudTrail, cross-account security auditing



#### Account Factory

- automates provisioning of new accounts in your organization
- standardize the provisioning of new accounts with pre-approved account configurations
- configure your account factory with pre-approved network configuration and region selections
- enable self-service for your builders to configure and provision new accounts using AWS Service Catalog



#### Guardrails

pre-packaged governance rules for security, operations, and compliance that customers can select and apply enterprise-wide or to specific groups of accounts

AWS Control Tower is the *replacement* for retired AWS Landing Zones



## ▼ 3. AWS Config

# AWS Config

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.

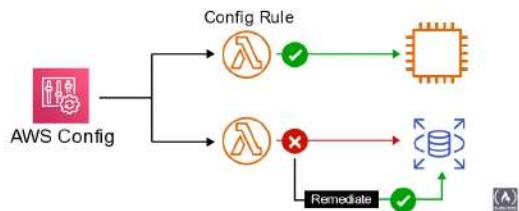


## What is AWS Config?

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

### When should you use AWS Config?

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



## ▼ 4. AWS Quick Starts

# AWS Quick Starts

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

Reduce hundreds of manual procedures into just a few steps

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

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



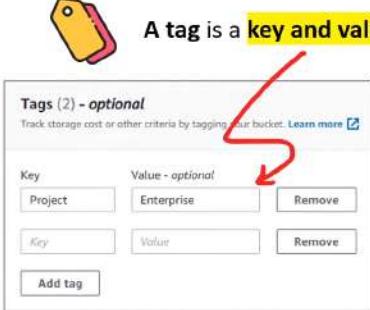
Most Quick Start reference deployments enable you to spin up a fully functional architecture in less than an hour!



## ▼ 5. Tagging

## Tagging

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



A tag is a **key and value pair** that you can assign to AWS resources.

Tags allow you to organize your resources in the following ways:

- Resource management**
  - specific workloads, environments eg. Developer Environments
- Cost management and optimization**
  - Cost tracking, Budgets, Alerts
- Operations management**
  - Business commitments and SLA operations eg. Mission-Critical Services
- Security**
  - Classification of data and security impact
- Governance and regulatory compliance**
- Automation**
- Workload optimization**

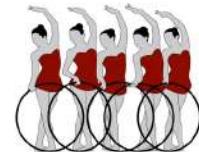
**Tag Examples**

- Dept = Finance
- Status = Approved
- Team = Compliance
- Environment = Production
- Project = Enterprise
- Location = Canada

## ▼ 6. Resource Groups

### Resource Groups

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



Resource Groups are a collection of resources that share one or more **tags**

Helps you organize and consolidate information based on your project and the resources that you use.

Resource Groups can display details about a group of resource based on

- Metrics
- Alarms
- Configuration Settings

At any time you can modify the settings of your resource groups to change what resources appear.

Resource Groups appears in the **Global Console Header** and Under **Systems Manager**



## ▼ 7. Business Centric Services

 **Business Centric Services**

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

-  **Amazon Connect** is a **virtual call center service**. You can create workflow to route callers. You can record phone calls. Manage a queue of callers. Based on the same proven system used by the Amazon customer service teams.
-  **WorkSpaces** is **virtual remote desktop service** Secure managed service for provisioning either Windows or Linux desktops in just a few minutes which quickly scales up to thousands of desktops
-  **WorkDocs** is a **shared collaboration service**. A centralized storage to share content and files. It is similar to Microsoft SharePoint. Think of it as a shared folder where the company has ownership
-  **Chime** is **video-conference service**. It is similar to Zoom or Skype. You can screenshare, have multiple people on the call. It is secure by default and it can show you a calendar of your upcoming calls.
-  **WorkMail** is a **managed business email, contacts, and calendar service** with support for existing desktop and mobile email client applications. (IMAP). Similar to Gmail or Exchange.
-  **Pinpoint** is a **marketing campaign management service**. Pinpoint is for **sending targeted email** via SMS, push notifications, and voice messages. You can perform A/B testing or create Journeys (complex email response workflows)
-  **Simple Email Service (SES)** is a **transactional email service**. You **can integrate SES into your application to send emails**. You can create common template, track open-rates, keep track of your reputation.
-  **QuickSight** is a **Business Intelligence (BI) service**. Connect multiple data sources and quickly visualize data in the form of graphs with little to no programming knowledge.

(A)

## ▼ 18. Provisioning

### ▼ 1. Provisioning Services

**Provisioning Services**

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**What is provisioning?**  
 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

-  **Elastic Beanstalk (EB)** is a **Platform as a Service (PaaS) to easily deploy web-applications**. EB will provision various AWS services, including EC2, S3, Simple Notification Service (SNS), CloudWatch, EC2 Auto Scaling Groups, and Elastic Load Balancers. If you have ever used **Heroku** it is the AWS equivalent 
-  **AWS OpsWorks** is a **configuration management service** that also provides managed instances of the open-source configuration managed software **Chef** and **Puppet**.  
-  **CloudFormation** is a **infrastructure modeling and provisioning service**. Automate the provisioning of AWS Services by writing CloudFormation templates in either **JSON** or **YAML files**. This is known as **Infrastructure as Code (IaC)**
-  **AWS QuickStarts** are 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** of **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.

(A)

# Provisioning Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## AWS App Runner

A fully managed service that makes it easy for developers to quickly deploy containerized web applications and APIs, at scale and with no prior infrastructure experience required



## AWS Copilot

AWS Copilot is a command line interface (CLI) that enables customers to quickly launch and easily manage containerized applications on AWS.



## AWS CodeStar

provides a unified user interface, enabling you to easily manage your software development activities in one place. Easily launch common types of stacks eg. LAMP



## AWS Cloud Development Kit (CDK)

An Infrastructure as Code (IaC) tool. Allows you to use your favourite programming language. Generates out CloudFormation templates as the means for IaC.



## ▼ 2. AWS Elastic Beanstalk

# AWS Elastic Beanstalk

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

### What is Platform as a Service? (PaaS)

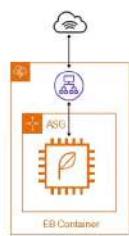
a PaaS allows customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app



Elastic Beanstalk is a PaaS for deploying web-applications with little-to-no knowledge of the underlying infrastructure so you can focus on writing application code instead of setting up an automated deployment pipeline and DevOps tasks.

Choose a platform, upload your code and it runs with little knowledge of the infrastructure.

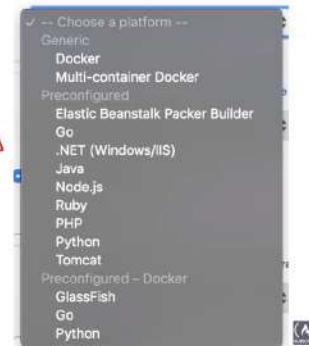
Not Recommended for "Production" applications



AWS is talking about enterprise, large companies.

Elastic Beanstalk is powered by a CloudFormation template **setups** for you:

- Elastic Load Balancer
- Autoscaling Groups
- RDS Database
- EC2 Instance preconfigured (or custom ) platforms
- Monitoring (CloudWatch, SNS)
- In-Place and Blue/Green deployment methodologies
- Security (Rotates passwords)
- Can run **Dockerized** environments



## ▼ 19. Serverless

### ▼ 1. Serverless Services

# Serverless Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## 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 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.



AWS Lambda is 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 are charged based on the runtime of the serverless function rounded to the nearest 100ms.



Step Functions is a **state machine service**. It coordinate 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



## ▼ 2. What is Serverless

# What is Serverless?

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is Serverless?

Serverless architecture generally describes fully managed cloud services. The classification of a cloud service being serverless is not a Boolean answer (yes or no), but a answer on a scale where a cloud service has a degree of serverless.

A serverless service could have all or most of the following characteristics:



- Highly elastic and scalable
- highly available
- Highly durable
- Secure by default



Abstracts away the underlying infrastructure and are billed based on the execution of your business task.



Serverless can **Scale-to-Zero** meaning when not in use the serverless resources cost nothing.

**Pay-for-Value** (you don't pay for idle servers).



An analogy of serverless could be similar to an energy rating label which allows consumers to compare the energy efficiency of a product. Some services are more serverless than others.



## ▼ 20. Windows on AWS

### ▼ 1. Windows on AWS

 **Windows on AWS**

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

AWS has multiple cloud services and tools to make it easy for you run Windows workloads on AWS.

 **Windows Servers on EC2**

You can select from a number of Windows Server versions including the latest version, Windows Server 2019



**SQL Server on RDS** You can select from a number of SQL Server database versions



**AWS Directory Service** lets you run **Microsoft Active Directory (AD) as a managed service**



**AWS License Manager** makes it easier to manage your software licenses from software vendors such as Microsoft.



Amazon FSx for Windows File Server is a **fully managed scalable storage** built for Windows.



**AWS Software Development Kit (SDK)** allows you to write code in your favorite language to interact with AWS API. The SDK supports **.NET** a language favorite for Windows Developers



**Amazon WorkSpaces** allows you to run a virtual desktop. You can launch a **Windows 10 desktop** to a provide secure and durable workstation that is accessible from wherever you have an internet connection.



AWS Lambdas supports **PowerShell** as a programming language to write your serverless functions!

**AWS Migration Acceleration Program (MAP)** for Windows is a migration methodology from moving large enterprise. AWS has Amazon Partners that specialize in providing professional services for MAP.



## ▼ 2. AWS License Manager

### AWS License Manager

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**What is Bring-Your-Own-License? (BYOL)**

The process of reusing an existing software license to run vendor software on a cloud vendor's computing service. BYOL allows companies to save money since they may have purchased the license in bulk or at a time that provided a greater discount than if purchased again.

eg. **License Mobility** is Microsoft Volume Licensing customers with eligible server applications covered by active Microsoft Software Assurance (SA)



**AWS License Manager** is a service that makes it easier for you to manage your software licenses from software vendors centrally across AWS and your on-premises environments.

AWS Licence Manager software that is licensed based on **virtual cores (vCPUs), physical cores, sockets, or number of machines**. This includes a variety of software products from  Microsoft, IBM, SAP, Oracle, and other vendors

**License type**  
The counting model used for the license. This may not track the terms of your agreement with your license provider.  
For vCPUs.

vCPUs	<input type="text" value="vCPUs"/>
vCPUs	<input type="text" value="vCPUs"/>
Cores	<input type="text"/>
Sockets	<input type="text"/>
Instances	<input type="text"/>

**Enforce license limit**  
Helps prevent usage after available license types are exhausted, e.g. an instance launch requiring new prevent overuse. Not supported for RDS.

AWS License Manager works with:

- EC2 – Dedicated Instances, Dedicated Hosts, Spot Instances
- RDS – (Only for Oracle databases)

For **Microsoft Windows Server** and **Microsoft SQL Server license** you generally need to use a **Dedicated Host**



## ▼ 21. Logging

### ▼ 1. Logging Services

# Logging Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**CloudTrail** - logs all **API calls** (SDK, CLI) between **AWS services** (who can we blame)

*Who created this bucket?*

*Who spun up that expensive EC2 instance?*

*Who launched this SageMaker Notebook?*

- Detect developer misconfiguration
- Detect malicious actors
- Automate responses



**CloudWatch** is a collection of multiple services

- CloudWatch **Logs** A centralized place to store your cloud services log data or application logs.
- CloudWatch **Metrics** Represents a time-ordered set of data points. A variable to monitor
- CloudWatch **Events (EventBridge)** trigger an event based on a condition eg. ever hour take snapshot of 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.



## ▼ 2. Cloud Watch Alarms

### CloudWatch Alarms

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

Name	State	Last state update	Conditions	Actions
Network_in	<span style="color: orange;">In alarm</span>	2020-07-20 13:01:35	NetworkIn > 300 for 1 datapoints within 5 minutes	No actions

When alarm breaches (goes outside the defined threshold) than 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**.

The screenshot shows the 'Actions' section of the CloudWatch Metrics Alarm configuration. It includes fields for selecting an SNS topic, an S3 bucket, or an SNS topic for notifications, and sections for Auto Scaling action and EC2 action.

- Notification
- Auto Scaling Group
- EC2 Action



## ▼ 3. LOG Events

## CloudWatch Logs – Log Events

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

### Log Events

Represents a single event in a log file. Log events can be seen within a Log Stream.

▶ 2020-07-06T20:12:18.079-04:00	START RequestId: e4b5bd10-5d88-4d7b-870c-daf793159b88 Version: \$LATEST
▶ 2020-07-06T20:12:18.082-04:00	{"records_size":1}
▶ 2020-07-06T20:12:18.093-04:00	{"failed_put_count":0}
▶ 2020-07-06T20:12:18.127-04:00	END RequestId: e4b5bd10-5d88-4d7b-870c-daf793159b88
▶ 2020-07-06T20:12:18.127-04:00	REPORT RequestId: e4b5bd10-5d88-4d7b-870c-daf793159b88 Duration: 45.32 ms Billed Duration: 100 ms Memory Size: 128

You can use filter events to filter out logs based on simple or pattern matching syntax:



Timestamp	Message
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.596187 #3979] DEBUG -- : [1m [35m (0.4ms)
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.614381 #3979] DEBUG -- : [1m [35m (1.5ms)
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.621670 #3979] DEBUG -- : [1m [36mActiveRec
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.626819 #3979] DEBUG -- : [1m [35m (0.4ms)
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.627990 #3979] DEBUG -- : [1m [35m (0.4ms)

## ▼ 4. Cloud Watch Metrics

### CloudWatch Metrics

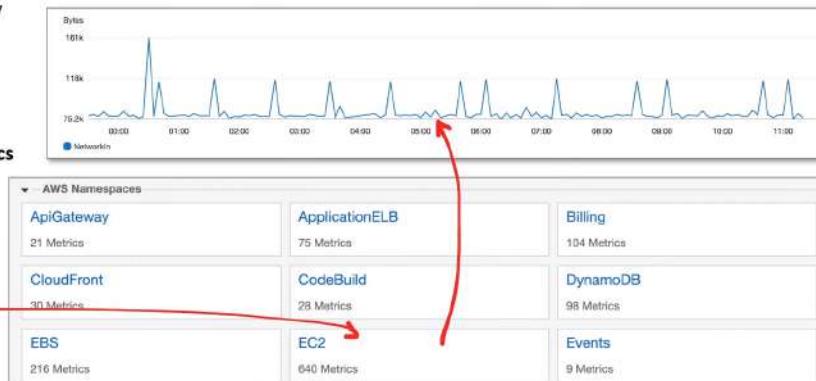
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

A CloudWatch Metric represents a **time-ordered set of data points**  
Its a **variable** that is **monitored over time**.

CloudWatch comes with many **predefined** metrics that are generally name spaced by AWS Service.



- EC2 Per-Instance Metrics**
- CPUUtilization
  - DiskReadOps
  - DiskWriteOps
  - DiskReadBytes
  - DiskWriteBytes
  - **NetworkIn**
  - NetworkOut
  - NetworkPacketsIn
  - NetworkPacketsOut

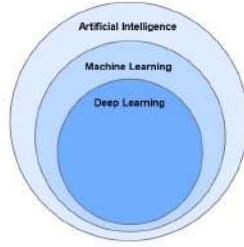


## ▼ 22. ML, AI and Big Data

### ▼ 1. Machine Learning and AI Services

# Machine Learning and AI Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## What is Artificial Intelligence (AI)?

Machines that perform jobs that mimic human behavior

## What is Machine Learning (ML)?

Machines that get better at a task without explicit programming

## What is Deep Learning (DL)?

Machines that have an artificial neural network inspired by the human brain to solve complex problems.



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

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



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



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



# Machine Learning and AI Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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](http://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



## ▼ 2. Big Data and Analysis Service

### Big Data and Analytics Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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 maintenance.



**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](http://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 need 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 connects 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 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



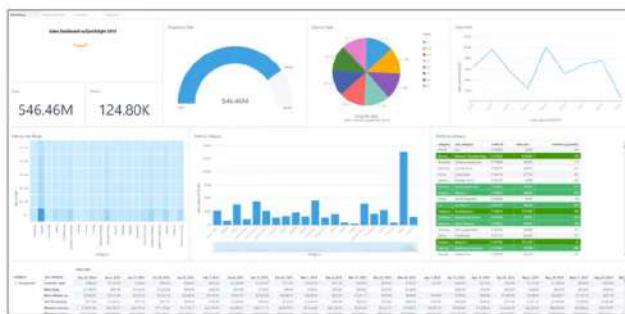
## ▼ 3. Amazon Quick Sight

### Amazon QuickSight

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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 questions using natural language, on all your data, and receive answers in seconds.



## ▼ 23. AWS Well-Architected Framework

### ▼ 1. The 5 Pillars

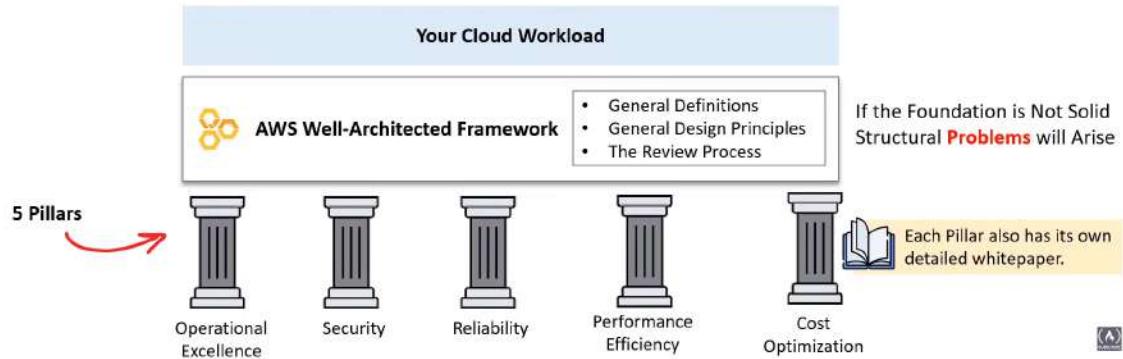
# AWS Well-Architected Framework

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

The AWS Well-Architected Framework is a Whitepaper created by AWS to help customers build using best-practices defined by AWS.

[aws.amazon.com/architecture/well-architected](http://aws.amazon.com/architecture/well-architected)

The framework is divided into 5 sections called pillars which address different aspects or "lenses" that can be applied to a cloud workload.



## ▼ 2. General Definitions

### AWS Well-Architected – General Definitions

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

	*Business Value
	Operational Excellent Pillar — Run and monitor systems
	Security Pillar — Protect data and systems, mitigate risk
	Reliability Pillar — Mitigate and recover from disruptions
	Performance Efficiency Pillar — Use computing resources effectively
	Cost Optimization Pillar — Get the lowest price

\*Trade-Off Pillars Based on Business Context

#### General Definitions

- Component** — Code, Configuration and AWS Resource against a requirement  
**Workload** — A set of components that work together to deliver business value  
**Milestones** — Key changes of your architecture through product life cycle  
**Architecture** — How components work together **in** a workload  
**Technology Portfolio** — A collection of workloads required for the business to operate



## ▼ 3. Operational Excellence Design Principles

## AWS Well-Architected - Design Principles

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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 regularly.  
*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 servers to test recovery

#### Learn from all operational failures

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



## ▼ 4. Security Design Principles

## AWS Well-Architected - Design Principles

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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



## ▼ 5. Reliability Design Principles

## AWS Well-Architected - Design Principles

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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



## ▼ 6. Performance Efficiency Design Principles

## AWS Well-Architected - Design Principles

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.



## ▼ 7. Cost Optimization

# AWS Well-Architected - Design Principles

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



## Cost Optimization Design Principles

### Implement Cloud Financial Management:

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

### Adopt a consumption model

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

### Measure overall efficiency

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

### Stop spending money on undifferentiated heavy lifting

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

### Analyze and attribute expenditure

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



## ▼ 8. AWS Well Architected Tool

# AWS Well-Architected Tool

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.

The screenshot shows the AWS Well-Architected Framework review interface. It includes sections for Operational Excellence, Well-Architected Tool, Workload, Example, AWS Well-Architected Framework, Review checklist, and Helpful resources. The review checklist for OPS 1 is displayed, asking how to determine priorities. The 'Evaluate external customer needs' checkbox is checked. A red arrow points to the 'Mark best practice! What doesn't apply to this workload?' section at the bottom.

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

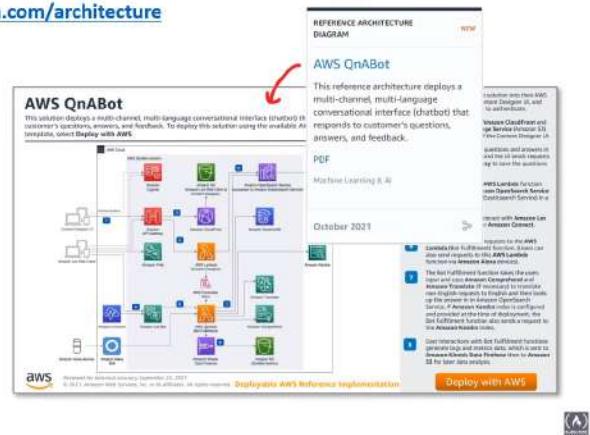


## ▼ 9. AWS Architecture Centre

**AWS Architecture Center**

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

The AWS Architecture Center is a web-portal that contains **best practices** and **reference architectures** for a variety of different workloads.  
[aws.amazon.com/architecture](http://aws.amazon.com/architecture)



## ▼ 24. TCO and Migration

### ▼ 1. Total Cost of Ownership ( TCO )

**Total Cost of Ownership (TCO)**

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**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.



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

### Capital vs Operational Expenditure

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Capital Expenditure (CAPEX)	Operational Expenditure (OPEX)
<p><b>Spending money upfront</b> on <b>physical infrastructure</b> Deducting that expense from your tax bill over time.</p> <ul style="list-style-type: none"><li>• Server Costs (computers)</li><li>• Storage Costs (hard drives)</li><li>• Network Costs (Routers, Cables, Switches)</li><li>• Backup and Archive Costs</li><li>• Disaster Recovery Costs</li><li>• Datacenter Costs (Rent, Cooling, Physical Security)</li><li>• Technical Personal</li></ul> <p>With Capital Expenses <b>you have to guess upfront</b> what you plan to spend</p>	<p>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 <b>non-physical costs</b>.</p> <ul style="list-style-type: none"><li>• Leasing Software and Customizing features</li><li>• Training Employees in Cloud Services</li><li>• Paying for Cloud Support</li><li>• Billing based on cloud metrics eg.<ul style="list-style-type: none"><li>• compute usage</li><li>• storage usage</li></ul></li></ul> <p>With Operation Expenses you can try a product or service <b>without investing in equipment</b></p>

## ▼ 3. AWS Pricing Calculator

### AWS Pricing Calculator

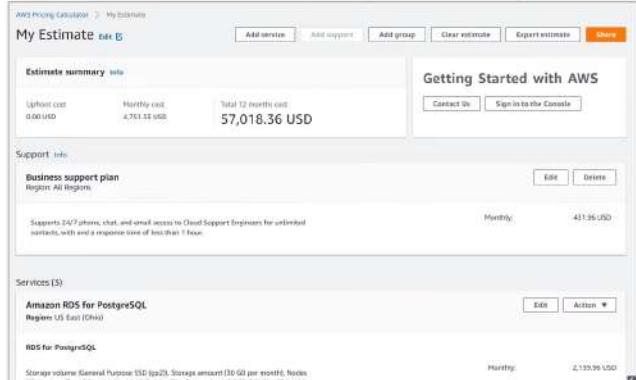
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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.

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.



## ▼ 4. AWS Migration Evaluator

### Migration Evaluator

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

AWS Migration Evaluator (formerly 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

The screenshot shows the TSO Logic interface with several charts and tables. One chart titled 'USAGE AWS COST + Applications' shows total costs for Compute, Storage, and Network. Another chart shows 'US MIGRATION CLASSIFICATION' with categories like Compute, Storage, and Network. Below the charts are detailed tables for 'US SERVICES' and 'DETAILED Applications'.

## ▼ 5. VM Import / Export

### EC2 VM Import/Export

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

VM Import/Export allows users to import Virtual Machine images into EC2.

AWS has import instructions for:

- VMware
- Citrix
- Microsoft Hyper-V
- Windows VHD from Azure
- Linux VHD from Azure

```
aws ec2 import-image \
--disk-containers Format=ova,UserBucket="{S3Bucket=my-vm,S3Key=vm.ova}"
```

## ▼ 6. Database Migration Service ( DMS )

# Database Migration Service (DMS)

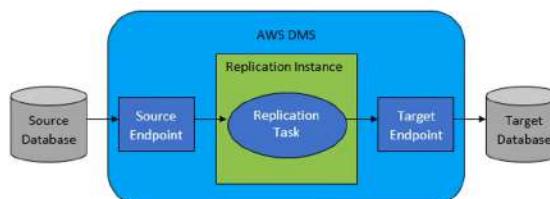
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

## Possible Sources:

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



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

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

## Possible Targets:

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



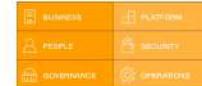
## ▼ 7. AWS Cloud Adoption Framework

### AWS Cloud Adoption Framework (CAF)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

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



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

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

**2 People Perspective** e.g. Human Resources, Staffing, People Managers, how to update the staff skills and organizational processes to optimize and maintain their workforce, and ensure competencies are in place at the appropriate time.

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

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

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

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

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

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

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

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



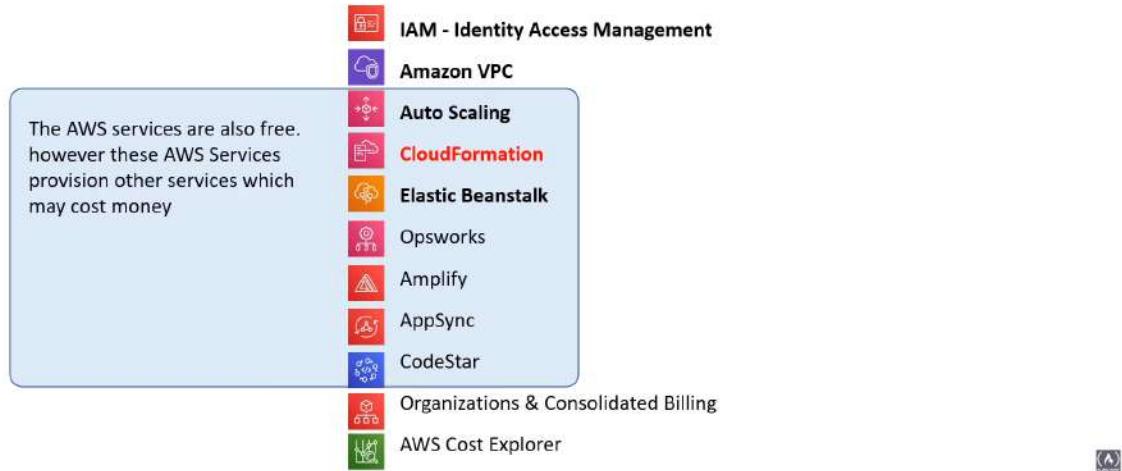
## ▼ 25. AWS Billing and Pricing

### ▼ 1. AWS Free Services

## AWS Free Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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



## ▼ 2. Support Plans

### AWS Support Plans

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Basic	Developer	Business	Enterprise
Email Support only For Billing and Account	Tech Support via <b>Email</b> ~24 hours until reply  No third party support	Tech Support via <b>Chat, Phone</b> Anytime 24/7  General Guidance	Production System Impaired  Production System DOWN!  Business-Critical System DOWN! < 15m  Personal Concierge TAM
		< 24 hrs  < 12 hrs  < 4 hrs  < 1 hrs	
			All Trusted Advisor Checks
7 Trusted Advisor Checks			
\$0 USD /month	*\$29 USD /month	*\$100 USD / month	*\$15,000 USD / month

## ▼ 3. Technical Account Manager

# Technical Account Manager (TAM)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



A Technical Account Manager? (TAM) provides both **proactive guidance** and **reactive support** to help you succeed with your AWS journey

What does a TAM do? (Straight from an AWS Job Posting)

- Build solutions, provide technical guidance and advocate for the customer
- Ensure AWS environments remain operationally healthy whilst reducing cost and complexity
- Develop trusting relationships with customers, understanding their business needs and technical challenges
- Using your technical acumen and customer obsession, you'll drive technical discussions regarding incidents, trade-offs, and risk management
- Consult with a range of partners from developers through to C-suite executives
- Collaborates with AWS Solutions Architects, Business Developers, Professional Services Consultants, and Sales Account Managers
- Proactively find opportunities for customers to gain additional value from AWS
- Provide detailed reviews of service disruptions, metrics, detailed prelaunch planning
- Being part of a wider Enterprise Support team providing post-sales, consultative expertise
- Solve a variety of problems across different customers as they migrate their workloads to the cloud
- Uplift customer capabilities by running workshops, brown bag sessions, etc.



TAMs follow the Amazon Leadership Principles  
Especially about being Customer Obsessed!



TAMs are only available at the Enterprise Support tier.



## ▼ 4. Consolidated Billing

### Consolidated Billing

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**Consolidated Billing** is a feature of AWS Organizations that allows you to pay for multiple AWS accounts with **one bill**.

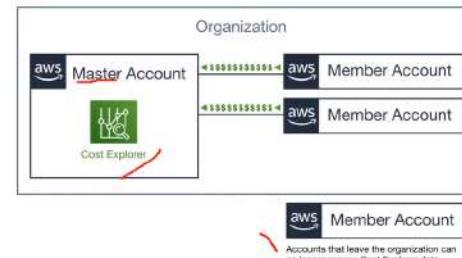
For billing AWS treats all the accounts in an organization as if they were one account.

You can designate one **master account** that pays the charges of all the other **member accounts**.

Consolidated billing is offered at no additional cost!

Use **Cost Explorer** to visualize usage for consolidated billing

You can combine the usage across all accounts in the organization to share the volume pricing discounts



## ▼ 5. AWS Trusted Advisor

# AWS Trusted Advisor

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.

The screenshot shows the AWS Trusted Advisor dashboard. On the left, there's a sidebar with 'Dashboard' selected, followed by 'Cost optimization', 'Performance', 'Security', 'Fault tolerance', and 'Service limits'. Below that is a 'Preferences' section. The main area is titled 'Trusted Advisor > Dashboard' and has a 'Checks summary' section. It displays two items: 'Action recommended' (2) under 'Security' and 'Investigation recommended' (1) under 'Security'. A red arrow points from the top of the page down to the 'Checks summary' section. Another red arrow points from the right side of the 'Checks summary' section to a detailed view of a specific recommendation: 'Security Groups - Specific Ports Unrestricted'. This view includes a description, a link to 'Check details', and a note about last update time.



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 going to hit the maximum limit for a service?



# AWS Trusted Advisor

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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](http://www.exampro.co/clf-c01)

Fault Tolerance	Service Limits	
Amazon EBS Snapshots	Auto Scaling Groups	RDS Cluster Parameter Groups
Amazon RDS Multi-AZ	Auto Scaling Launch Configurations	RDS Cluster Roles
Amazon S3 Bucket Logging	CloudFormation Stacks	RDS Clusters
Amazon S3 Bucket Versioning	DynamoDB Read Capacity	RDS DB Instances
Amazon Aurora DB Instance Accessibility	DynamoDB Write Capacity	RDS DB Parameter Groups
Amazon EC2 Availability Zone Balance	EBS Active Snapshots	RDS DB Security Groups
<b>Amazon RDS Backups</b>	EBS Active Volumes	RDS DB Snapshots Per User
Amazon Route 53 Deleted Health Checks	EBS Cold HDD (sc1) Volume Storage	RDS Event Subscriptions
Amazon Route 53 Failover Resource Record Sets	EBS General Purpose SSD (gp2) Volume Storage	RDS Max Auths per Security Group
Amazon Route 53 High TTL Resource Record Sets	EBS Magnetic (standard) Volume Storage	RDS Option Groups
Amazon Route 53 Name Server Delegations	EBS Provisioned IOPS (SSD) Volume Aggregate IOPS	RDS Read Replicas per Master
Auto Scaling Group Health Check	EBS Provisioned IOPS SSD (io1) Volume Storage	RDS Reserved Instances
Auto Scaling Group Resources	EBS Throughput Optimized HDD (st1) Volume Storage	RDS Subnet Groups
ELB Connection Draining	EC2 Elastic IP Addresses	RDS Subnets per Subnet Group
ELB Cross-Zone Load Balancing	EC2 On-Demand Instances	RDS Total Storage Quota
Load Balancer Optimization	EC2 Reserved Instance Leases	Route 53 Hosted Zones
VPN Tunnel Redundancy	ELB Active Load Balancers	Route 53 Max Health Checks
AWS Direct Connect Connection Redundancy	IAM Group	Route 53 Reusable Delegation Sets
AWS Direct Connect Location Redundancy	IAM Instance Profiles	Route 53 Traffic Policies
AWS Direct Connect Virtual Interface Redundancy	IAM Policies	Route 53 Traffic Policy Instances
EC2Config Service for EC2 Windows Instances	IAM Roles	SES Daily Sending Quota
ENA Driver Version for EC2 Windows Instances	IAM Server Certificates	<b>VPC</b>
NVMe Driver Version for EC2 Windows Instances	IAM Users	VPC Elastic IP Address
PCI DSS Version for EC2 Windows Instances	Kinesis Shards per Region	VPC Internet Gateways



## ▼ 6. Service Level Agreement ( SLA )

### Service Level Agreements

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

#### What is a Service Level Agreement (SLA)?

A SLA is a **formal commitment** about the **expected level of service** between a customer and provider.

When a service level is not met and if Customer meets its obligations under the SLA, Customer will be eligible to receive the compensation eg. **Financial or Service Credits**

#### What is a Service Level Indicator (SLI)?

A **metric/measurement** that indicates what measure of performance a customer is receiving at a given time  
A SLI metric could be uptime, performance, availability, throughput, latency, error rate, durability, correctness

#### What is a Service Level Objective (SLO)?

The objective that the provider has agreed to meet

SLOs are represented as a specific **target percentage** over a period of time.

Availability SLA of **99.99%** in a period of **3 months**



#### Target percentages

- 99.95%
- 99.99%
- 99.99999999% (commonly called **Nine nines**)
- 99.999999999% (commonly called **Nine elevens**)

## ▼ 7. Service Health Dashboard

# Service Health Dashboard

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

The screenshot shows the AWS Service Health Dashboard. At the top, it says "Current Status - Oct 19, 2021 PDT". Below this, there's a table with columns for "Region", "Service", "Status", and "Details". The "Region" column has tabs for North America, South America, Europe, Africa, Asia Pacific, and Middle East. The "Service" column lists services like Alexa for Business (N. Virginia), Amazon API Gateway (Montreal), and Amazon API Gateway (N. California). The "Status" column shows "Service is operating normally" for all listed services. The "Details" column contains links to more information. A red arrow points from the text "An icon and details will indicate the status of each AWS Service" to the "Details" column.

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



## ▼ 8. Personal Health Dashboard

# AWS Personal Health Dashboard

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

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

All AWS customers can access the Personal Health Dashboard.

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

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

The screenshot shows the AWS Personal Health Dashboard. On the left, there's an overview section with metrics for "Open issues", "Scheduled changes", and "Other notifications". On the right, there's a detailed view of a "Scheduled changes" event. The event summary says "EC2 persistent instance retirement scheduled" and "Last update: March 05, 2021 at 11:46:11 UTC-7". The event data section shows details like "Event ID: EC2 persistent instance retirement scheduled", "Start time: March 10, 2021 at 6:00:49 PM UTC-7", and "End time: March 10, 2021 at 6:00:49 PM UTC-7". It also mentions "Affected resources" and "Description". A red arrow points from the text "The Personal Health Dashboard shows recent events to help you manage active events, and shows proactive notifications so that you can plan for scheduled activities" to the "Event summary" section.

## ▼ 9. AWS Abuse

## AWS Abuse

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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](mailto:abuse@amazonaws.com) or fill out the Report Amazon AWS abuse form.



## ▼ 10. AWS Free-Tier

## AWS Free-Tier

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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



### EC2 Web Server

t2.micro 750 hours per month for 1 year

The Best Deals



### 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



## ▼ 11. AWS Credits

## AWS Credits

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**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
- ...

Summary	
Total amount remaining	Total amount used
\$500.00	\$332.00

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



## ▼ 12. AWS Budgets

### AWS Budgets

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**AWS Budgets** give you the ability to setup alerts if you **exceed** or are **approaching** your defined budget

Create **Cost**, **Usage** or **Reservation** Budgets

It can be tracked at the **monthly**, **quarterly**, or **yearly** levels, with customizable start and end dates

Alerts support **EC2**, **RDS**, **Redshift**, and **ElastiCache** reservations.



AWS Budgets can be used to Forecast costs but is limited compared to Cost Explorer or doing your analysis with AWS Cost and Usage Reports along with a Business Intelligence tool

Budget based on a fixed cost or plan your upfront based on your chosen level  
Can be easily managed from the **AWS Budgets** dashboard or via the **Budgets API**.

Get Notified by providing an email or **Chatbot** and threshold how close to the current or forecasted budget

Choose your budget amount in \$\$\$

Budgeted amount  
\$100      Last month's cost \$126.59

Usage unit(s)  
 Usage Type Group  
EC2: Running Hours (Hrs) \*  
 Usage Type

Choose based a different kind of unit

Budgeted amount  
100      Hrs      Last month's usage 2280.54 Hrs



## ▼ 13. AWS Budget Reports

## AWS Budget Reports

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

**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.

The screenshot shows the 'Reports' section of the AWS Management Console. A red arrow points from the text above to the 'Create budget report' button at the top right. Below it, a table lists one report: 'MyReport' with 'Daily' frequency and '1' recipient. There are 'Download CSV' and 'Actions' buttons above the table.

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



## ▼ 14. AWS Cost and Usage Reports (CUR)

### AWS Cost and Usage Reports (CUR)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

The screenshot shows a detailed CUR spreadsheet. A red arrow points from the text above to the first few rows of the table, which list various AWS services and their corresponding costs. The columns include 'Invoice/Logistics Date', 'Invoice/Logistics Type', 'Invoice/Logistics Region', 'Invoice/Logistics Line Item', 'Invoice/Logistics Line Item Description', 'Invoice/Logistics Line Item Unit Price', and 'Invoice/Logistics Line Item Total'. The data includes entries like 'Amazon CloudWatch Metrics' and 'Amazon CloudWatch Metrics Insights'.

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



## ▼ 15. Billing Alerts / Alarms

## Billing Alerts/Alarms

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

You can create your own Alarms in CloudWatch Alarms to monitor spend. They are commonly called "Billing Alarms"

You first need to turn on **Billing Alerts**

Go create a CloudWatch Alarm and you can choose Billing as your Metric

Billing Alarms are much more flexible than AWS Budgets and ideal for more complex use-cases for monitoring spend and usage

The screenshot shows the AWS CloudWatch Metrics & Alarms interface. It includes sections for 'Cost Management Preferences' (with checkboxes for 'Receive Free Tier Usage Alerts' and 'Receive Billing Alarms'), a 'Specify metric and conditions' section with a graph showing 'EstimatedCharges' over time, and a detailed configuration panel for a specific alarm.

## ▼ 16. AWS Cost Explorer

### AWS Cost Explorer

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

AWS Cost Explorer lets you **visualize, understand, and manage** your AWS costs and usage **over time**.

Specific type range and aggregation

Robust filtering

Default reports help you gain insight into your cost drivers and usage trends.

Use **forecasting** to get an idea of future costs

The screenshot shows the AWS Cost Explorer interface. It features a main dashboard with a bar chart, a sidebar for filtering and grouping, a 'Reports' section with various options like 'Monthly costs by service' and 'Daily costs', and a 'Forecasted month end costs' summary at the bottom.

## ▼ 17. AWS Pricing API

## AWS Pricing API

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

There are two versions of this API:

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

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

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



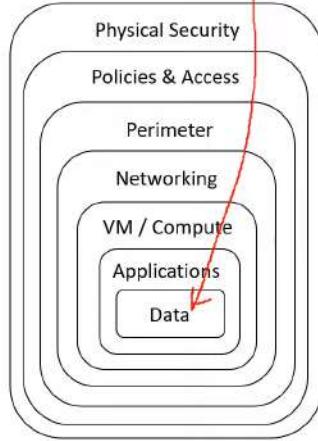
## ▼ 26. Security

### ▼ 1. 7 Layers of Security

## Defense in Depth

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

### The 7 Layers of Security



#### 1. Data

access to business and customer data, and encryption to protect data.

#### 2. Application

applications are secure and free of security vulnerabilities.

#### 3. Compute

Access to virtual machines (ports, on-premise, cloud)

#### 4. Network

limit communication between resources using segmentation and access controls.

#### 5. Perimeter

distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.

#### 6. Identity and access

controlling access to infrastructure and change control.

#### 7. Physical

limiting access to a datacenter to only authorized personnel.

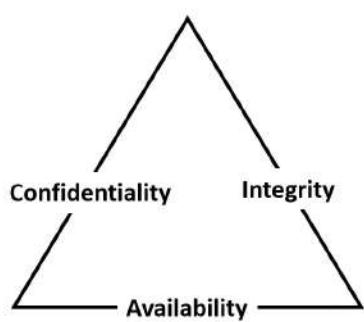


## ▼ 2. CIA Triad

### Confidentiality, Integrity, Availability (CIA)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Confidentiality, Integrity, and Availability (CIA) triad is a model describing the foundation to security principles and their trade-off relationship.



#### Confidentiality

confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. In practice this can be using cryptographic keys to encrypt our data, and using keys to encrypt our keys (envelope encryption)

#### Integrity

maintaining and assuring the accuracy and completeness of data over its entire lifecycle. In Practice utilizing ACID compliant databases for valid transactions. Utilizing tamper-evident or tamper proof Hardware security modules. (HSM)

#### Availability

information needs to be made be available when needed  
In Practice: High Availability, Mitigating DDoS, Decryption access

The CIA triad was first mentioned in a **NIST publication from 1977**.

There have been efforts to expand and modernize or suggest alternatives to CIA triad:

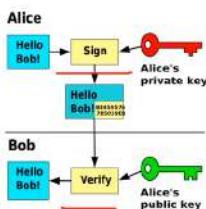
- (1998) Six Atomic Elements of Information eg. confidentiality, possession, integrity, authenticity, availability, and utility
- (2004) NIST Engineering Principles for Information Technology Security — 33 security principles



## ▼ 3. Digital Signature and Signing

### Digital Signatures and Signing

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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



## ▼ 4. Penetration Testing

# Penetration Testing

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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.



## ▼ 5. AWS Artifact

# AWS Artifact

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



AWS Artifact is a self-serve portal for on-demand access to **AWS compliance reports**



Choose your report

Title	Reporting period	Category	Description
Government of Canada (GC) Partner Package	August 25, 2017 to current	Alignment Documents	The Government of Canada (GC) Partner Package is intended for use by partners and customers when building applications and solutions on AWS that need to meet the GC requirements based on the Protection Profile for the Government of Canada profile. The documents available in this package include Partner Package白皮书, Controls Implementation Summary (CIS), Customer Responsibility Matrix (CRM), and Government of Canada (GOC) Security Assessment and Letter of Attestation.

View the PDF



Download the Excel



## ▼ 6. AWS Inspector

# AWS Inspector

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## What is Hardening?

The act of eliminating as many **security** risks as possible. Hardening is common for Virtual Machines where you run a collection of security checks known as a security benchmark



AWS Inspector runs a **security benchmark** against specific EC2 instances.

You can run a variety of security benchmarks.

Can perform both **Network** and **Host** Assessments

Assessment Setup

You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run once for a one-time assessment, or **Advanced setup** for custom assessments.

**Network Assessments** (Inspector Agent is not required)

- Assessments performed: Network configuration analysis to check for ports reachable from outside the VPC. Learn more
- Optional Agent: If the Inspector Agent is installed on your EC2 instances, the assessment also finds processes reachable on port. Learn more about optional agent
- Pricing: Pricing for network assessments is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful scan of 100 instances assessed weekly; the monthly cost would be around \$61/month. Learn more

**Host Assessments** (Inspector Agent is required)

- Assessments performed: Network configuration analysis to check for ports reachable from outside the VPC, host hardening (OS benchmarks), and security best practices. Learn more
- Optional Agent: Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instance commands. Learn more about Inspector Agent and how to manually install agent
- Pricing: Pricing for host assessments is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful scan of 100 instances assessed weekly; the monthly cost would be around \$120/month. Learn more

**Run weekly (recommended)**

- Install the AWS agent on your EC2 instances.
- Run an assessment for your assessment target.
- Review your findings and remediate security issues.

One very popular benchmark you can run is by CIS which has **699 checks!**



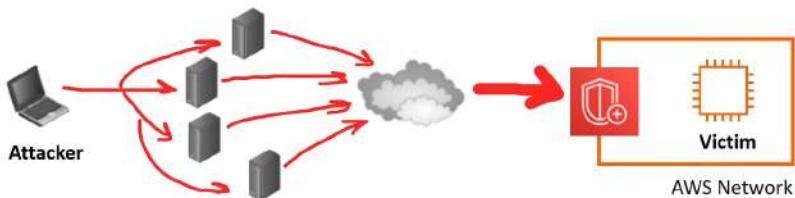
## ▼ 7. DDoS Attack

# Distributed Denial of Service (DDoS)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

## 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.



## ▼ 8. AWS Shield

## AWS Shield

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

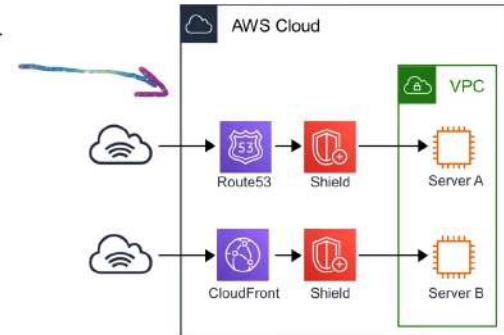


AWS Shield is a **managed** DDoS (Distributed Denial of Service) protection service that safeguards applications running on AWS

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



(A)

## ▼ 9. Shield Standard vs Shield Advanced

### AWS Shield

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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 EC2 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

(A)

## ▼ 10. Guard Duty

## Amazon Guard Duty

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

### What is IDS/IPS?

Intrusion Detection System and Intrusion Protection System.

A device or software application that monitors a network or systems for malicious activity or policy violations.



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

- CloudTrail Logs
- VPC Flow Logs
- DNS logs

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

The screenshot shows a finding titled "Policy: IAMUser/RootCredentialUsage" with a severity of "Low". The finding details state: "API DescribeAccount was invoked using root credentials from IP address 104.194.51.115." A red arrow points to the "Investigate with Detective" button. Below the finding is an "Overview" table with the following data:

Severity	LOW
Region	us-east-1
Count	36
Account ID	123456789012
Resource ID	No information available
Created at	09-24-2021 15:24:26 (a month a...
Updated at	09-24-2021 16:59:21 (a month a...



## ▼ 11. Amazon Macie

## Amazon Macie

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

Macie works by uses Machine Learning to Analyze your CloudTrail logs

Macie has a variety of alerts

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

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



## ▼ 12. VPN

## AWS Virtual Private Network (VPN)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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

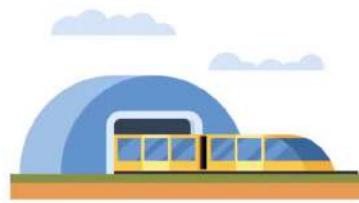
securely connect on-premises network or branch office site to VPC

### 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)



(A)

## ▼ 13. WAF

## AWS WAF

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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

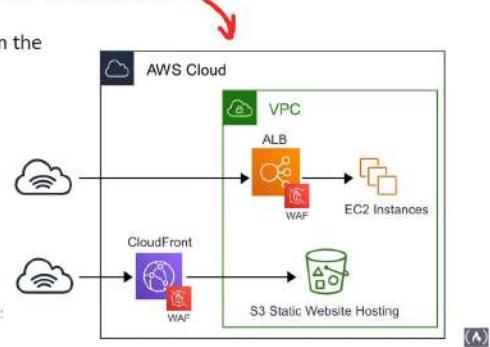
Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Rules Marketplace

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 vulnerabilities
10. Insufficient logging and monitoring



(A)

## ▼ 14. Hardware Security Module

## Hardware Security Module (HSM)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

A Hardware Security Module (HSM).

Its a piece of hardware designed to store encryption keys.  
HSM hold keys in memory and never write them to disk.



Federal Information Processing Standard (FIPS)

US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

HSM's that are **multi-tenant** are **FIPS 140-2 Level 2 Compliant**  
(multiple customers virtually isolated on an HSM)



eg. AWS KMS

HSM's that are **single-tenant** are **FIPS 140-2 Level 3 Compliant**  
(single customer on a dedicated HSM)



eg. AWS CloudHSM



## ▼ 15. AWS KSM

### AWS Key Management Service

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



**AWS Key Management Service (KMS)** is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

Encryption

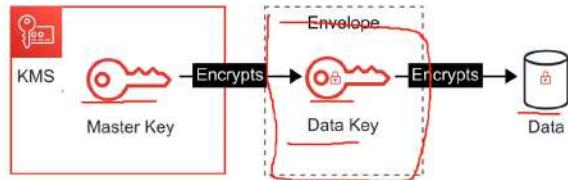
Enable Encryption  
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the Key Management Service(KMS) console. Info

Master key [Info](#)  
(default) aws/kms

#### Envelope Encryption

When you encrypt your data, your data is protected, but you have to protect your encryption key.

When you encrypt your data key with a master key as an additional layer of security.



## ▼ 16. AWS Cloud HSM

## CloudHSM

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



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

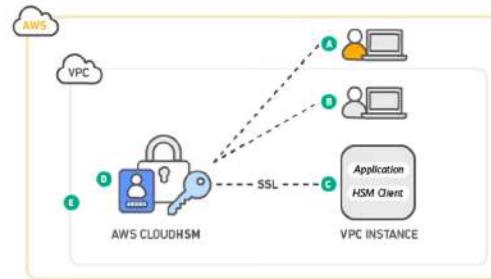
AWS CloudHSM enables you to generate and use your encryption keys on a FIPS 140-2 Level 3 validated hardware.

Built on Open HSM industry standards to integrate with:

- PKCS#11
- Java Cryptography Extensions (JCE)
- Microsoft CryptoAPI (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.



(A)

## ▼ 27. Variation Study

### ▼ 1. AWS Config vs AWS AppConfig

#### AWS Config vs AWS AppConfig

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



##### AWS Config

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

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

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



##### AWS AppConfig

AWS App Config is used to automate 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.

(A)

## ▼ 2. SNS vs SQS

### SNS vs SQS

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

The Both **Connect Apps via Messages**

 <b>Simple Notifications Service</b> Pass Alongs Messages eg. PubSub	 <b>Simple Queue Service</b> Queue Up Messages, Guaranteed Delivery
Send notifications to <b>subscribers</b> of topics via multiple protocol. eg, HTTP, Email, SQS, SMS	Places messages into a <b>queue</b> . Applications pull queue using <b>AWS SDK</b>
SNS is generally used for sending <b>plain text emails</b> which is triggered via other AWS Services. The best example of this is billing alarms.	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
Can retry sending in case of failure for <b>HTTPS</b>	Really good for delayed tasks, queueing up emails
Really good for webhooks, simple internal emails, triggering lambda functions	 <b>RabbitMQ</b>  <b>Sidekick</b>
 <b>PUSHER</b> POWERING REALTIME	 <b>PubNub</b>

## ▼ 3. AWS Inspector vs AWS Trusted Advisor

### Amazon Inspector vs AWS Trusted Advisor

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)

Both are **security tools** and they both perform audits

 <b>Amazon Inspector</b> Audits a <b>single EC2 instance</b> that you've selected Generates a report from a long list of security checks i.e 699 checks.	 <b>Trusted Advisor</b> Trusted Advisor <b>doesn't generate</b> out a PDF report. Gives you a <b>holistic view</b> of recommendations across multiple services and best practices eg. You have open ports on these security groups You should enable MFA on your root account when using trusted advisor.
---	---

## ▼ 4. AWS Artifact vs AWS Inspector

## AWS Artifact vs Amazon Inspector

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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**



## ▼ 5. Types of Load Balancers

### ELB vs ALB vs NLB vs GWLB vs CLB

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/clf-c01](http://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**



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



