

# MTPROJECTS Certified Cloud Practitioner Exam Review

Date Last Modified: January 12, 2020

PDF Created based on AWS CPP YouTube video by ExamPro posted on freeCodeCamp.org's channel

Link: <https://www.youtube.com/watch?v=3hLmDS179YE&t=>

## What is cloud computing?

Using remote servers over the internet instead of local server or personal server

**On premise:** owning personal servers, hire own IT people, pay for everything

**Cloud providers:** Someone else owns the hardware, and hires IT etc. You pay fees to use their services.

## 6 advantages of cloud providers over premise:

- 1) Trade capital expense for variable expense: No upfront cost, pay on demand
- 2) Benefit from massive economies of scale: Sharing the cost with other customers to get massive discounts
- 3) Stop guessing capacity: Scale as desired, instead of paying for idles/underutilized servers when you go local.
- 4) Increase speed and agility: Launch software/apps within a few minutes instead of waiting for days to setup hardware etc.
- 5) Stop spending money on running and maintaining data centers: Focus on customer/coding rather than infrastructure.
- 6) Go global in minutes: Launch in multiple areas in the world without having to own hardware etc. Provide low latency to customers.

## Type of cloud computing:

- 1) Software as a service (SAAS) : Fully built applications/products by service providers. Customers just use these products. ie. Office 365, Gmail..
- 2) Platform as a service (PAAS): Do not need to take care of the underline infrastructure. Focus on coding rather than maintaining. ie. Elastic Beanstalk.
- 3) Infrastructure as a service (IAAS): Basic building blocks for cloud IT. No need to worry about IT staff, data centers, hardware etc. ie. AWS, Azure ..

## Cloud computing Deployment Models:

**On-Premise:** Local hardware. Mostly used for public sector ie Government,hospital etc. To protect private data and sensitive data. Sometimes called private cloud.

**Cloud:** Fully utilizing the cloud computing services. All data and functionality is in the cloud.

**Hybrid:** Mix of both cloud and on-premise.

## AWS Global Infrastructure:

**Regions:** Physical location in the world with 2 or more Availability zones. Every region is independent from one another. Largest region is US-EAST (North Virginia). All billing information is in the region US-EAST 1.

**Availability Zones:** One or more discrete data centers. Identifier: us-east-1a = Region: us-east-1, AZ: a. Latency between AZs is less than 10ms.

**Edge Locations:** data centered owned by a trusted partner of AWS that cache data. Serve requests to CloudFront and Route 53.

**GovCloud(US) Region:** Only for US citizens and been in the US. Customers that need to architect secure cloud solutions for the US government body.

**AWS Budgets:** Allows to know if you are going over your desired costs (set amount manually) for services. Also has option to forecast future costs. With free tier you get 2 free budgets. Over that, each budget will cost 2 cents per day. Max 20 000 budgets. Three types of budgets: Cost, Usage or Reservation. Notification to email, chat: Chime or Slack.

**AWS Billing Alarms:** Free tier 10 Free alarms and 1000 free email notifs. per month. Functionality related to AWS Budgets but has less features. Manually set alarms at different stages ie. 100\$, 150\$ 200\$ etc.

## AWS Account setup under IAM initially:

- 1) Delete your root access keys
- 2) Activate MFA on your root account
- 3) Create individual IAM users (initial account created is root account. Root account should be rarely used. Use other created accounts)
- 4) Use groups to assign permissions
- 5) Apply an IAM password policy

## Elastic Compute Cloud - EC2 (Basic server)

You can use stop or terminate the instance, and will not be charged. Every computing service under the hood is using an EC2 instance.

**Simple System Manager (SSM):** Can be used to access an EC2 instance instead of SSH. Much easier, doesn't need any key pair. In the IAM role that is assigned to the EC2 instance, allow SSM. Allows visibility like checking who logged in etc. (Logs)

**Amazon Machine Image (AMI):** Is a snapshot of the service. Example a snapshot of EC2 is a copy of the server that can be used to launch it again.

**Auto Scaling Groups (ASG):** Allows to choose how many servers are running at once. Allows to scale up or down depending on traffic to meet demand. Use AMI to configure it. Scaling policy will allow to setup what the scaling will do. Deleting ASG will delete the instances that it had created.

**Elastic Load Balancer (ELB):** Allows you to distribute traffic between different instances of a server. If you use ELB you will need Auto scaling but for auto scaling you don't need ELB.

**Simple Storage Service (S3):** Storage system for AWS cloud. Can store files. You would create a bucket that will allow you to store files. A bucket name must be unique.

**CloudFront:** Is used as a CDN (Content Distributed Network). Copies to multiple edge locations in the world, so customers all over the world has fast access to your static content.

**Relational Database Service (RDS):** Database system for AWS. Allows to have multiple engines ie. MySQL, PostgreSQL, MSSQL, Aurora, Oracle etc. 3 different templates: Production, Dev/Test, Free Tier.

**Lambda:** A function that allows you to handle the business logic/back end. It allows users to go serverless. It will compute the function and then stop working. You are only charged for the time used for the computation. Set a trigger to start the function.

## PRICING:

### 4 pricing models

1) **On-Demand pricing:** Charged by the hour or minute without any long term commitment or up front payment.

2) **Reserved Instances (RI):** Reserve an amount of time and save money.

- a. **Standard:** Save up to 75% compared to On Demand. Cannot change anything in the configurations
- b. **Convertible:** Save up to 54% compared to On Demand. Allows to change RI attributes if greater or equal in value
- c. **Schedules:** You reserve instances for specific time periods. Ie. A week for a few hours. Savings vary.

Terms: 1 or 3 year contract.

Payment options: All upfront, partial upfront or no upfront.

Can sell the RI if not needed to someone else that wants to use it.

3) **Spot Instances:** Up to 90% discount compared on demand pricing. No stability. Another customer that wants to pay higher price, your instance can be terminated at any given time. If AWS terminates your instance, you don't get charged for a partial hour of usage. You get charged if you terminate it.

4) **Dedicated Host Instances:** Strict server bound licensing that won't support multi tenancy. Isolated hardware.

a. **Multi Tenant:** Sharing same hardware with other AWS customers

b. **Single Tenant:** Having your own hardware and not sharing.

Most expensive option

Can be demand or reserved.

## Free services:

Certain services are free themselves, but the resources they setup will cost you.

The services are free	 <b>IAM - Identity Access Management</b>
	 <b>Amazon VPC</b>
However they can provision AWS services which cost money	 <b>Auto Scaling</b>  <b>CloudFormation</b>  <b>Elastic Beanstalk</b>  <b>Opsworks</b>  <b>Amplify</b>  <b>AppSync</b>  <b>CodeStar</b>
	 <b>Organizations &amp; Consolidated Billing</b>
	 <b>AWS Cost Explorer</b>

## AWS Support Plans:

### Basic:

- Email support only for billing and account
- 7 Trusted Advisor Checks
- \$0 USD / Month

### Developer:

- Tech support via Email 24 hours until reply
- No third party support (frameworks etc.)
- General Guidance < 24hours
- System Impaired < 12 hours
- 7 Trusted advisor checks
- \$20 USD / Month

### Business:

- Tech support via Email 24 hours until reply
- Tech Support via Chat, Phone anytime 24/7
- General Guidance < 24 hours
- System Impaired < 12 hours
- Production System Impaired < 4 hours
- Production System Down < 1 hour
- All Trusted Advisor Checks
- \$100 USD / Month

### Enterprise:

- Tech support via Email 24 hours until reply
- Tech Support via Chat, Phone anytime 24/7
- General Guidance < 24 hours
- System Impaired < 12 hours
- Production System Impaired < 4 hours
- Production System Down < 1 hour
- Business Critical System DOWN! < 15 min
- Personal Concierge
- TAM (Technical Account Manager)
- All Trusted Advisor Checks
- \$15 000 USD / Month

## AWS Marketplace:

Digital Catalogue with thousand of software listing from independent software vendors. You can buy and sell software over here.

## AWS Trusted Advisor:

Advices you on security, saving money, performance, service limits and fault tolerance. Automated checklist for best practices on AWS. Ie. If you have a static IP sitting without use, it will tell you to release the IP so you can save money.

## Consolidated Billing:

Feature turned on by default. One account is your master account, and other accounts under it. Master account is in charge for billing for all the accounts. No additional cost for this service. It has an option for volume discounts. With consolidated billing, you can combine service usage from multiple accounts and apply discounts. The more you use a service, the bigger the discounts, so combining the service usage, you will save more.

## AWS Cost Explorer:

Lets you visualize, understand and manage AWS Costs and usage over time. Use master account if you have many accounts. You can pull out reports. You can view data monthly or daily. Information can be filtered and grouped.

**TCO Calculator (Tool Cost Ownership):** Allows you to cost how much it will cost to transition to AWS. It is an approximation, not exact price.

**AWS Landing Zone:** Provides you with a baseline environment to get started with a multi account architecture. Uses AWS Account Vending Machine (AVM). Pretty much quickly set up the account structure. Additional accounts can be created with AVM.

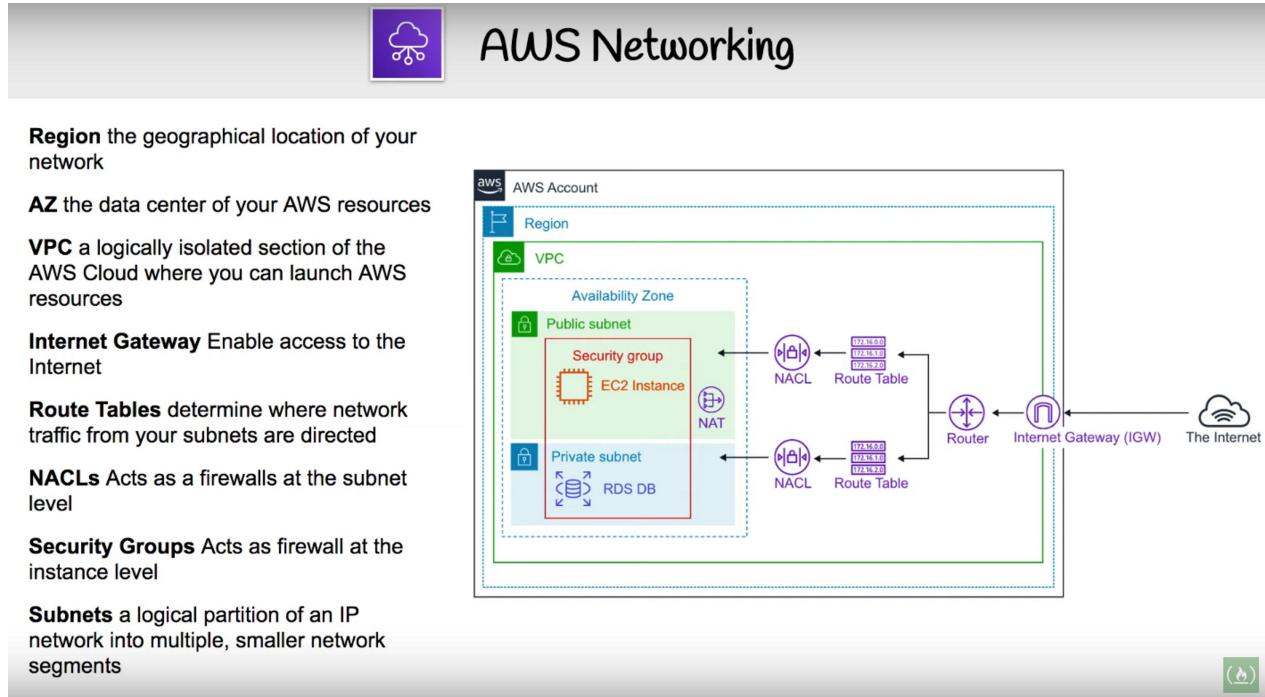
**Resource Groups and Tagging:** Words and phrases that act as metadata. You will tag certain services with a specific tag and then you can group them all in a resource group with the same tag.

**AWS Quickstarts:** Prebuilt templates by AWS and AWS partners to help you deploy a fully functional architecture quickly. Uses AWS CloudFormation.

**AWS Cost And Usage Report:** Generates a detailed spreadsheet to allow you to analyze and better understand AWS costs. 24 hours for the first report.

**AWS Organizations:** Allows you to organize the different accounts and create different sections in the organization. Different sections allows to apply different policy to each of the sections. You can only suspend accounts on AWS and not delete them.

## AWS Networking:



## Database Services:

	<b>DynamoDB</b> - NoSQL <b>key/value</b> database	
	<b>DocumentDB</b> - NoSQL <b>Document</b> database that is MongoDB compatible	
	<b>RDS</b> - <b>Relational</b> Database Service that supports multiple engines <b>ENGINES:</b> MySQL, Postgres, Maria DB, Oracle, Microsoft SQL Server, Aurora	
	<b>Aurora</b> MySQL (5x faster) and PSQL (3x faster) database <b>fully managed</b>	
	<b>Aurora Serverless</b> - only runs when you need it, like AWS Lambda	
	<b>Neptune</b> - Managed <b>Graph</b> Database	
	<b>Redshift</b> - <b>Columnar</b> database, <b>petabyte</b> warehouse <b>1000 TB = 1 PB!!!!</b>	
	<b>ElastiCache</b> - <b>Redis</b> or, <b>Memcached</b> database	

## Provisioning Services:

### What is provisioning?

The allocation or creation of resources and services to a customer



**Elastic Beanstalk** - service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker



**OpsWorks** - configuration management service that provides managed instances of **Chef** and **Puppet**.



**CloudFormation** - infrastructure as code, **JSON** or **YAML**



**AWS QuickStart** - 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.

## Computing Services:



**EC2** Elastic Compute Cloud, highly configurable server eg. CPU, Memory, Network, OS



**ECS** Elastic Container Service **Docker as a Service** highly scalable, high-performance container orchestration service that supports Docker containers, pay for EC2 instances



**Fargate** Microservices where you don't think about the infrastructure. Pay per task



**EKS** **Kubernetes as a Service** easy to deploy, manage, and scale containerized applications using Kubernetes



**Lambda** **serverless functions** run code without provisioning or managing servers. You pay only for the compute time you consume



**Elastic Beanstalk** orchestrates various AWS services, including EC2, S3, Simple Notification Service (SNS), CloudWatch, autoscaling, and Elastic Load Balancers



**AWS Batch** plans, schedules, and executes your batch computing workloads across the full range of AWS compute services and features, such as **Amazon EC2** and **Spot Instances**

## Storage Services:

	<b>S3 - Simple Storage Service</b> - <b>object</b> storage
	<b>S3 Glacier</b> - low cost storage for <b>archiving and long-term backup</b>
	<b>Storage Gateway</b> - hybrid cloud storage with local caching
	File Gateway
	Cache
	Volume Gateway
	Tape Gateway
	<b>EBS - Elastic Block Storage</b> - hard drive in the cloud you attach to EC2 instances SSD, IOPS SSD, Throughput HHD, Cold HHD
	<b>EFS - Elastic File Storage</b> - file storage mountable to multiple EC2 instances at the same time
	<b>Snowball</b> - Physically migrate lots of data via a computer suitcase 50-80 TB
	Snowball Edge A better version of Snowball - 100 TB
	Snowmobile Shipping container, pulled by a semi-trailer truck - 100 PB



## Business Centric Services:

	<b>Amazon Connect - Call Center</b> - Cloud-based call center service you can setup in just a few clicks - based on the same proven system used by the Amazon customer service teams.
	<b>WorkSpaces - Virtual Remote Desktop</b> - Secure managed service for provisioning either Windows or Linux desktops in just a few minutes which quickly scales up to thousands of desktops
	<b>WorkDocs</b> - A content creation and collaboration service - easily create, edit, and share content saved centrally in AWS. <b>(the AWS version of Sharepoint)</b>
	<b>Chime</b> - AWS Platform for <b>online meetings, video conferencing</b> , and business calling which elastically scales to meet your capacity needs
	<b>WorkMail</b> - Managed <b>business email</b> , contacts, and calendar service with support for existing desktop and mobile email client applications. (IMAP)
	<b>Pinpoint</b> - Marketing campaign management system you can <b>use for sending targeted email, SMS, push notifications, and voice messages</b>
	<b>SES - Simple Email Service</b> - A cloud-based email sending service designed for marketers and application developers to <b>send marketing, notification, and emails</b>
	<b>QuickSight</b> - A Business Intelligence (BI) service. Connect multiple datasource and quickly visualize data in the form of graphs with little to no programming knowledge.



Enterprise Integration Services:

## Going Hybrid!



**Direct Connect** dedicated Gigabit network connection from your premises to AWS  
Imagine having a direct fibre optic cable running straight to AWS



**VPN** establish a **secure** connection to your AWS network  
Site-to-Site VPN - Connecting your on-premise to your AWS network  
Client VPN - Connecting a Client (a laptop) to your AWS network



**Storage Gateway** A hybrid storage service that enables your on-premises applications to use AWS cloud storage. You can use this for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration.



**Active Directory** The AWS Directory Service for Microsoft Active Directory also known as AWS Managed Microsoft AD - enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

Logging Services:



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

Who created this bucket?

- Detect developer misconfiguration
- Detect malicious actors
- Automate responses

Who spun up that expensive EC2 instance?

Who launched this SageMaker Notebook?



**CloudWatch** - is a collection of multiple services

CloudWatch **Logs**

Performance data about AWS Services eg. CPU Utilization, Memory, Network In Application Logs eg. Rails, Nginx Lambda logs

CloudWatch **Metrics**

Represents a time-ordered set of data points. A variable to monitor

CloudWatch **Events**

trigger an event based on a condition eg. every hour take snapshot of server

CloudWatch **Alarms**

triggers notifications based on metrics

CloudWatch **Dashboard**

create visualizations based on metrics



## Initialisms:

<b>IAM</b> Identity and Access Management	<b>ELB</b> Elastic Load Balancer
<b>S3</b> Simple Storage Service	<b>ALB</b> Application Load Balancer
<b>SWF</b> Simple Workflow Service	<b>NLB</b> Network Load Balancer
<b>SNS</b> Simple Notification Service	<b>EC2</b> Elastic Cloud Compute
<b>SQS</b> Simple Queue Service	<b>ECS</b> Elastic Container Service
<b>SES</b> Simple Email Service	<b>ECR</b> Elastic Container Repository
<b>SSM</b> Simple Systems Manager	<b>EBS</b> Elastic Block Storage
<b>RDS</b> Relational Database Service	<b>EFS</b> Elastic File Storage
<b>VPC</b> Virtual Private Cloud	<b>EMR</b> Elastic MapReduce
<b>VPN</b> Virtual Private Network	<b>EB</b> Elastic Beanstalk
<b>CFN</b> CloudFormation	<b>ES</b> Elasticsearch
<b>WAF</b> Web Application Firewall	<b>EKS</b> Elastic <b>Kubernetes</b> Service
<b>MQ</b> Amazon ActiveMQ	<b>MKS</b> Managed <b>Kafka</b> Service
<b>ASG</b> Auto Scaling Groups	<b>IoT</b> Internet of Things
<b>TAM</b> Technical Account Manager	<b>RI</b> Reserved Instances

## Shared Responsibility:

Customers: Responsible for security in the cloud --> Data Configuration

AWS: Responsible for hardware, operation of managed services and global infrastructure.

Customers are responsible of security in the cloud whereas AWS is responsible for security of the cloud!

**AWS Compliance Programs:** Set of internal policies and procedure of a company to comply with laws, rules and regulations. Ie. HIPPA for hospitals and PCI for Payment card Industry Data Security Standard

**AWS Artifact:** Allows to check if AWS meets a compliance program. Why should an enterprise trust AWS?

**Amazon Inspector:** Checks if EC2 instance is hardened. Hardening is the act of eliminating as many security risks as possible. This service runs a security benchmark against a specific EC2 instance. Generates a report from a long list of security checks.

**AWS Web Application Firewall (WAF):** Protects web apps from common web exploits. More rule sets can be purchased. Can be attached to either CloudFront or Application Load Balancer.

**AWS Shield:** Managed DDoS protection service that safeguards apps running on AWS. Automatically turned on. There is Shield Standard (Free) and Shield Advanced (\$3000 USD / Year): More advanced and limited to certain services ex. Route 53, CloudFront etc.

**Penetration Testing:** is allowed in AWS but there are certain activities prohibited. All types of flooding is prohibited. Certain simulated events need special request from AWS. Permitted services include: (EC2, RDS, CloudFront, Aurora, API Gateways, Lambda, Lightsail, Elastic Beanstalk).

**Guard Duty:** Threat detection service, continuously monitors for malicious, suspicious and unauthorized behavior. Uses Machine learning to analyze Cloud Trail Logs, VPC Flow Logs, and DNS Logs.

**Key Management Service (KMS):** Stores keys in memory. It is multitenant. KMS uses Envelope Encryption.

**Amazon Macie:** Monitors S3 data access from unauthorized activity. Can also identify your most at risk users.

**Security Groups:** Acts as a firewall at the instance level. Ie. Allows an EC2 instance access on port 22 for SSH.

**Network Access Control Lists (NACLs):** Acts as a firewall at the subnet level. Ie. Blocks a specific IP address.

**VPN:**

**Site to Site VPN:** Securely connect on premise network or branch office site to VPC  
**Client VPN:** Securely connect used to AWS or on premise networks

**Media Connect:** Converts videos to different video types.

**Simple Notification Service (SNS):** Sends notifications to subscribers of topics via multiple protocol. Generally used for sending plain text emails.

**Simple Queue Service (SQS):** Queue up messages, guaranteed delivery. Places messages into a queue, Applications pull queue using AWS SDK.

**Simple Email Service (SES):** A cloud bases email service. Sends html emails, SNS cannot.