AWS Cloud Practitioner Cert

MAC OS Tools

Connect to EC2 instances via terminal - built into macs

Install a Text Editor -VSCode

AWS EC2 instances authentication is done differently rather than username and password, they use username and key pair file or \*.ppk

EC2 uses public-key cryptography to encrypt and decrypt login information public key to decrypt the data. The public and private keys are known as a key pair.

Create a Key Pair in AWS exported in \*.pem format

* Ues Putty Key Generator to \*.pem -> \*.ppk (Putty)
* Use putty or ObaXterm to SSH into EC2

EXAM FORMAT

Multiple Choice, Multiple Answer

90min

100USD

Around 65 Questions

CLF-01

Cloud Concepts

Security

Technology

Billing and Pricing

Cloud Computing is the on demand delivery of computing power , database storage, applications, and other IT resources through a cloud services platform via the internet with a pay-as-you-go pricing

AWS provides rapid access to flexible and low cost IT Resources

Applications and services are typically run on servers which are comprised of CPU, RAM, HDD/SSD

While cloud computing you don’t need large upfront investments in hardware and spend a lot of time provisioning the hardware

You provision exactly the right type and size of computing resources you need to power and rund your services

AWS is

Elastic means it can easily adapt to different situations and scale up or down to meet the demands that your business has.

Three major types of cloud services:

* IaaS - Infastructure as a Service
* PaaS - Platform as a Service
* SaaS - Software as a Service

The differences between them consist of:

* Functionality
* Tasks’ ownership and flexibility

ON-Prem DC

* You own the car
* However when you upgrade you have to buy a new car

PaaS

* You get a Taxi
* You get to tell the taxi where you want to go but you do not drive
* Platform as a service removes the need for your organization to manage the underlying infrastructure (hardware and operating systems) and allows you to focus on the deployment and management of your applications.
  + This helps to be more efficient as you don’t need to worry about resource procurement, capacity planning, software maintenance or patching,
  + An example would be AWS Lambda

IaaS

* You lease the car
* You get to choose the kind of car you want but you still do not own the car
* Infrastructure as a Service contains the basic building blocks for cloud IT and typically access to networking features, computers and data storage space.
  + IaaS provide the highest level of flexibility and management control over the infrastructure an example is Amazon EC2

SaaS

* You get the bus
* You don’t own the bus, nor can you tell where the bus to go and you share it with others
* Software as a Service provides you a complete product that is run and managed by other service providers.
  + With SaaS you do not have to think about how the service is maintained of how the underlying infrastructure is managed; you only need to think about how you will use the APP
  + A common example of a SaaS application is web-based email.

Cloud Computing Deployment Models

* Three Cloud Deployment Models are currently available:
  + On-Premises: you run everything from a data center you own
    - Also known as “private cloud”, resources are deployed in you on-premises DC, using virtualization and resource management tools like VMware HyperV or Openstack
    - Private cloud option offers the ability to provide dedicated resources, not split between users or end customers(only your apps sit on the actual hardware) this means on a public cloud that the hardware sever that you run off of may also service other applications.
    - You have full control over your infrastructure and are responsible for management and OS patching
  + Hybrid: You runs some of your Apps in your Data Center and some in the AWS Public Cloud
    - The hybrid deployment can be an intermediate step, while you are on your way to fully migrating to the AWS cloud.
    - A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud
    - The most common method of hybrid deployment is between the cloud and your existing on-premises infrastructure in order to extend or grow your organization’s infrastructure
  + Cloud: You run all you Apps in AWS public cloud
    - The applications are fully deployed in the cloud and all components of the application run in the cloud
    - Applications in the cloud have either been created in the cloud or have migrated from an existing infrastructure to take advantage of the cloud benefits
    - Migrating an App from on-prem to cloud is typically called “lift-and-shift” this refers to taking the App as is without modifying it and running it on cloud-native resources.

The six advantages of AWS Cloud Computing

* Trade Capital expense for variable expense
  + Instead of having to invest heavily in data centers and servers before you know how you’re going to use them you can pay only when you consume computing resources and pay only for how much you consume.
  + No upfront commitment “‘pay-as-you-use”
  + Example Samsung saved 34 mils with deploying the smart hub app to the cloud
* Benefits from massive economies of scale
  + By using cloud computing, you can achieve a lower variable cost than you can get on your own
  + Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scales, which translates into lower pay as you go prices.
* Stop guessing about capacity
  + Eliminate guessing on your infrastructure capacity needs, remember the black Friday example
  + While guessing you often end up either sitting on expensive idle resources or dealing with limited capacity
  + You can access as much or as little capacity as you need and scale up and down as required
* Increase speed and agility
  + Reduce the time to make IT resources available to your developers from weeks to just minutes
  + This results in a dramatic increase in agility for the organization since the cost and time it takes to experiment and develop is significantly lowered.
  + New server to production time?
* Stop spending money running and maintaining DCs
  + Focus on projects that differentiate your business, not the infrastructure; let AWS take care of the infrastructure
  + AWS will take care of the actual room, power, cooling racks, servers, cabling, storage, networking, security equipment, guards
  + Which allows you to focus on your business!
* Go global in minutes
  + Easily deploy your application in multiple regions around the world with just a few clicks
  + This means you can provide lower latency and a better experience for your customers at minimal cost

AWS Global Infrastructure OverView

Building Blocks:

* Regions
  + An AWS Region is a physical location in the world that consists of multiple Availability zones
  + All AWS regions are completely isolated one from each other
  + Highest fault tolerance and stability
  + Regions are isolated one from each other, AZs are isolated one from each other, BUT… the AZs in the same region are connected through low-latency links and have high bandwidth (2 or more)!
* Availability zones
  + An availability zone represents one or more discrete data centers each DC with redundant power, networking, and connectivity housed in separate facilities
  + What are the benefits for customers?
  + Running your Apps or services in multiple AZs , you can easily achieve high availability, fault tolerance, and scalability
  + This is no possible if running Apps in a single on-prem DC
  + One Availability Zone = One Data Center
  + AZ - one or more data centers
  + What’s inside the “box”
    - Servers
    - Networking
    - Storage
    - Security
    - Balancers
* Edge locations
  + Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, apps to customers globally with low latency and high transfer speeds
  + Amazon CloudFront uses a global network of
  + To deliver content to end-users with lower latency, Amazon CloudFront uses a global network of 210 Points of Presence (199 Edge Locations and 11 Regional Edge Caches) in 78 cities across 37 countries. Amazon CloudFront Edge locations are located in:
  + CloudFront helps one deliver ones web content faster to one end users, thus providing a better user experience
  + CloudFront edge locations bring the web content closer to your viewers and make sure that popular content can be served quickly
  + CloudFront Regional Edge Caches really help when the content is not popular enough to stay at a CloudFront edge location and improve delivery performance for that content.
  + Content Delivery Process
    - User asks for content
    - Route53 looks for the nearest edge location to the webserver.
    - If it has the content it will send it back immediately
    - If not it will ask the regional edge cache
    - If it has the content it will be sent to the edge location and then to the user
    - IF both the edge location and regional edge location do not have the content then the route will ask the webserver directly.
    - Then both the edge location and regional edge cache will store the data and then the content will be delivered to the user

Current Inventory:

* 61 Availability Zones
* 20 Regions

Planned for 2019

* 15 more AZs
* 5 more regions: Bahrain, Cape town, hong Kong, Jakarta, Milan

Current:

* 69 AZs
* 22 Regions

AWS Management Interfaces Overview

* AWS Management Console
  + The AWS Management Console is a GUI for accessing a wide range of AWS Cloud services and managing to compute, storage, and other cloud resources
  + A web application that comprises and refers to a broad collection of service consoles for managing AWS
  + Access the AWS web console from https://console.aws.amazon.com
* AWS Command Line Interface (CLI)
  + The CLI is a unified tool to manage your AWS services
  + With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts
  + After CLI installation you can begin making calls to your AWS services from the command line.
* AWS Software Development Kits(SDKs)
  + An SDK is really nothing more than a set of tools that allow developers to create software or apps for a specific platform, operating system, computer system or device.
  + Using SDKs, you can access and manage AWS services with your preferred development language or platform
  + <https://aws.amazon.com/tools/>

MODULE RECAP MODULE 2

What is cloud computing?

* Cloud computing is the on-demand delivery of computing power, db storage, applications, and other IT resources through a cloud service platform via the internet with a pay as you go pricing
* Think of cloud computing as renting the hardware with no initial investment, but pay as you go and as you grow

Cloud Computing Models

* IaaS = Infrastructure as a Service (EC2)
  + It contains basic building blocks for cloud IT and typically provides access to networking features, computers and data storage space.
* PaaS = Platform as a Service (AWS Lambda)
  + Removes the need for your organization to manage the underlying infrastructure and allows you to focus on the deployment and mgmt. Of your applications.
* Saas = Software as a Service (Gmail)
  + Provides you a complete product that is run and managed by another application

Cloud Computing Deployment Models

* On-Premises = You run everything in your own DC
* Hybrid = You run some of your apps in your DC and some in the AWS Public Cloud
* Cloud - You run all you Apps in AWS Public Cloud

Six Advantages of Cloud Computing

* Trade capital expense for variable expense
* Benefit from massive economies of scale
* Stop guessing about capacity
* Increase speed and agility
* Stop spending money running and maintaining DCS
* Go Global in minutes

Global Infrastructures

* An AZ is one or more discrete data centers each Dc with redundant power, networking, and connectivity, housed in separate facilities
* A Region is a physical location in the world that consists of multiple AZs
* Edge Locations are AWS endpoints that cache content locally
* Regional Edge Caches store even more cache locally

AWS Management Interfaces

* AWS Management Console
* CLI Command Line Interface
* SDKs Software Developer Kits.

Module 3

* Billing Alarm for AWS
  + Allow Billing Alerts
    - Navigate to Username → My Account
    - Navigate to Billing Preferences and check to receive billing alerts
  + Create Alarms
    - AWS Management Console → Management & Governance → CloudWatch
    - Alarms → Billing → Create Alarm → Billing → Total Estimated Charge → USD
    - Conditions → Threshold Type → Conditional Statement → Define Threshold Value
    - Next → Notification → Alarm State → Select an SNS topic
* Identity Access Management (IAM)
  + AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources
  + You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use what resources
  + The key to understanding IAM is represented by these two concepts: authentication and authorization.
  + In order to understand IAM we need to define and understand the following concepts
    - Authentication
      * PERMANENT
        + USER

A User is a permanently named operator; it can be a human or it can be a machine or another AWS service

* + - * + GROUP

A group is a collection of users and usually contains multiple users; a user can belong to multiple groups

* + - * TEMPORARY
        + ROLE

A role is an operator too, another authentication method just like a user; a role can be as well a human or another AWS service

* + Once a user/role is authenticated by AWWS, it will be given permissions (authorized) based on policy documents that are attached to it.
    - Authorization
      * POLICY DOCUMENT
        + Policy documents (JSON [JavaScript Object notation] Format) can be attached to a user group or role; if the policy is attached to the group, once a user joins the group, it will inherit the attached policies
  + Complete Picture
    - A principal (or operator), human or AWS service , makes a request for action on an AWS resource(API Call)
      * First, the user is authenticated, based on username/password pair or access key ID/ secret access key (programmatic access - CLI, API, SDK)
      * Second The user’s action will be permitted or denied (authorization) based on attached policies
      * Third Every API call will be recorded in AWS by CloudTrail
  + IAM Configuration
    - IAM does not need a region to be selected, it is a global feature
    - Add a USER → User Name → Access Types → Password (if desired) → Add USER to a group.
    - Account Settings you can enforce a password policy for users on the AWS
    - In IAM dashboard you can also change the link that users use to login.
* Virtual Private Cloud (VPC)
  + Amazon Virtual Private Cloud enables you to launch AWS resources into a virtual network that you define
  + This virtual network is similar to a traditional network that you would operate in your own data center with the benefits using the scalable infrastructure of AWS
  + A virtual private cloud(VPC) is a virtual network dedicated to your AWS account
  + A subnet is a range of Ip addresses ion your VPC
  + A routing table contain a set of rules, called routes that are used to determine where network traffic is directed
  + An internet gateway allows communication for your instances to the internet
  + Creating a VPC
    - Inside a VPC it has a Main Route Table this route table which is associated with each subnet in the VPC
    - The internet gateway provides the VPC and its routes internet access
* Elastic Compute Cloud(EC2)
  + Amazon Elastic Compute Cloud (EC2) provides scalable computing capacity in the Amazon Web Services Cloud
  + AWS virtual compute environments are called instances
  + Amazon Machine Images (AMIs) are available to choose from
    - Preconfigured templates for EC2 instances
  + Instance types - different configurations of CPU, memory, storage, and networking capacity
  + Secure login to EC2 instances with key pairs( you store the private key, and amazon stores the public key)
  + You can attach storage volumes to your EC2 instances - instance storage volumes - ephemeral storage
  + Persistent storage volumes for your data are available through elastic block store (EBS) - Amazon EBS Volumes
  + Store data in multiple locations (regions and AZs)
  + You can define basic security using AWS built-in firewall security group; protocol, port, source IPs that you permit or deny to reach you EC2 instances
  + Elastic IP address - static IPv4 public address that you can attach to your EC2 instance (i.E. For a website)
  + Create and attach tags or labels to your EC2 instances
  + **First steps for EC2**
    - First, you have to select an AMI, which basically represents software selection
      * All AMIs are categorized as either backed by Amazon EBS or backed by instance store
      * For AMIs with root volume backed by EBS, data is deleted when the instance terminates vs instance store volumes, where data persists only while the instance is live.
    - Next step is to select the hardware - instance type
      * Each instance type offers different compute, memory and storage capabilities and grouped in instance families based on these capabilities
    - Decide on a payment plan (4 ways)
      * On-Demand Instances
        + With On-Demand Instances, you pay for compute capacity per hour or per second, depending on which instances you run
      * Reserved Instances
        + Provide you with a significant discount (up to 75%) compared to On-Demand
        + Common Use Cases:

For applications that have predictable usage, and can provide significant savings compared to on-demand instances

Best for customers that commit to using ec2 over a 1-3 year term to reduce their total computing costs

* + - * Spot Instances
        + You can request spare EC2 computing capacity for up to 90% off the on-demand price. The price is not fixed therefore it is an option. You can put a threshold on the use of spot pricing in the management console.
        + Common Use Cases:

Applications that have flexible start and end times

Applications that are only feasible at very low compute prices. (eg: Big Data)

Users with urgent computing needs for a lot of additional capacity.

* + - * Dedicated Hosts
        + An amazon dedicated host is a physical ec2 server dedicated for your use
        + Dedicated hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, incl. Windows server, sql server, etc
        + They can also help meet compliance requirements
  + Launching EC2
    - Management Console → computing services → ec2 → launch instance → choose amazon machine image (AMI)
      * Important things for the AMI
        + Root device type: EBS + Instance Store
        + Virtualization type: Hardware Virtual Machine (HVM) or Paravirtual (PV)

<https://cloudacademy.com/blog/aws-ami-hvm-vs-pv-paravirtual-amazon/>

* + - * + ENA (Elastic Network Adapter) Enabled: yes or no
    - Select appropriate AMI → to select the appropriate instance → to configure instance details
      * Choose VPC within the region you are working from
      * Choose a subnet where the EC2 will run on
      * Have amazon provide an auto-assign public IP allowing it to be reachable from the internet
    - Select Storage
    - Add Tags
    - Add EC2 instance to a security group
      * Built-in firewalls provided by AWS
        + NOTE\* if the source is 0.0.0.0/0 anyone can connect to it from anywhere
    - Review and Launch → SAVE KEY PAIR VERY IMPORTANT
  + Connecting to EC2
    - In instances select the instance you want to connect to make sure to copy the IPv4 Public DNS Address then click the connect button next to launch instance
    - Open a terminal:
      * Navigate to folder where the key pair was saved
      * Chmod 400 \*.pem
      * Ssh -i \*.pem ec2-user@(public DNS IPv4)
      * BEST PRACTICE
        + Sudo su (to change to root user)
        + Yum update -y (update all files)
      * WEB SERVER
        + Yum install httpd -y

Apache HTTP Server

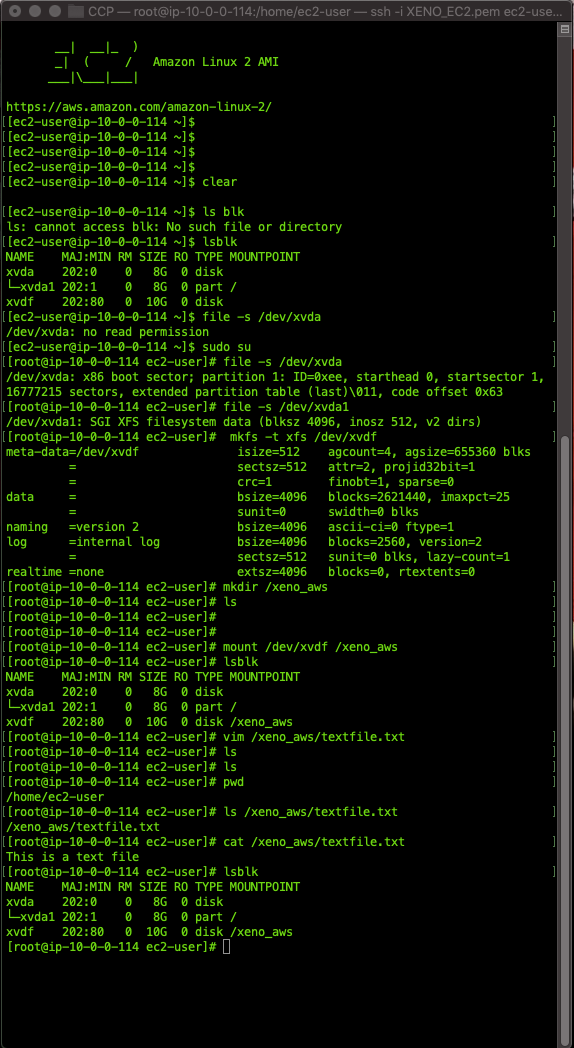
* + - * + service httpd status

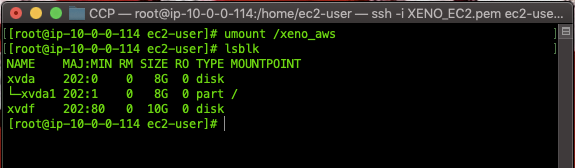
Know if the server is running or inactive

If inactive

service httpd start

* Security Groups (SGs)
  + AWS security groups act as a virtual firewall for your EC2 instances to control inbound and outbound traffic
  + Security groups enforce security at the instance level, not the subnet different EC2 instances can have different SGs applied
  + In a SG you add rules that control inbound traffic to instances and separate rules that control outbound traffic
  + Creating a security groups
    - When you first create a security group, it has no inbound rules => no traffic is permitted to EC2
    - When defining rules, you can only specify allow rules and no dny rules
    - By default all outbound traffic is permmi=itted
    - What rules can you actually define in a SG
      * Inbound rules:
        + Type, protocol, Port Range, Source, Description
      * Outbound rules
* Elastic Block Store(EBS)
  + Amazon Elastic Block Store (EBS provides block level storage volumes for use with EC2 instances. This is different than s3 and is more like installing HD to your computer
  + EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same AZ
  + EBS volumes that are attached to an EC2 instance are exposed as storage g volumes that persist independently from the life of the instance
  + Amazon EBS provides two types, which differ in performance characteristics and price
    - SSD volumes high IIOPS
      * General-purpose SSD (gp2
        + A balance between price and performance
      * Provisioned IOPS SSD (iol)
        + Highest performance SSD volume
    - HDD volumes throughput over iops
      * Throughput optimized HDD (st1)
        + Low cost HDD volume designed for frequently accessed throughput-intensive workloads
      * Cold HDD (sc1)
        + Lowest cost HDD volume designed for less frequently accessed workloads.
    - For security reasons data stored on EBS volumes needs to be encrypted; you can launch your ebs volumes an encrypted volumes
    - If you choose to create an encrypted EBS volume and attach it to your EC2, data store and snapshots are encrypted (“at rest”)
    - WIth data encrypted on your EBS volumes you are also ensuring security for data “in-transit”
    - You can take point-in-time snapshots of data on your Amazon EBS volumes and store them in AWS S3
      * Snapshot are incremental backups, which means that only data on the volume that has changed after you las snapshot is saved
      * Each snapshot contains all of the information needed to restore your data to a new EBS volume
    - Amazon EBS pricing
      * Volumes
        + Total storage of all EBS volumes, charged as GB/month
      * Snapshots
        + Total snapshot storage consumed in AWS S3
        + EBS snapshot copying between regions is charged
      * Data Transfer - inbound is free outbound is charged.
  + Creating EBS volume and attaching it to the EC2 instance.
    - EC2 management console → volumes → create volume → pick volume type based on needs → size of the volume in GiB → availability zone (as volumes are stored in AZs and) → identify a snapshot if you are formatting a volume from an existing snapshot → and chosen to either add encryption or key/value pairs or tags
    - After creation, you have to attach it to the EC2 instance you want and define the file path for the drive in the ec2 instance.
  + Identify storage in the terminal with the command
    - Lsblk
    - File -s /dev/xvda (identify the
    - If the mountpoint is blank you have to establish one
    - Command
      * Sudo su
      * Mkfs -t xfs name of path
      * Mkdir /mount\_path
      * Mount name of path and name of mount path



* Unmount volumes
  + 
  + Once you have unmountd the volume you can detach it and delete it or attach it to something else from the volumes option within the EC2 dashboard.
* Simple Storage Service(S3)
  + Amazon S3 provides object storage through a web service interface
  + With amazon s3 you can store and retrieve any amount of data, at any time, from anywhere on the web
    - Bucket
      * A bucket is a container for objects store in S3
      * Every object in s3 is contained by a bucket
      * Which will have url of
        + Https: //s3.<bucket\_name>.amazonaws.com/object\_name
        + Think of a bucket as a folder you can store files in
        + Bucket names are globally unique
    - Objects
      * Objects are the fundamental entities stored in Amazon S3
      * Objects consist of object data and metadata’ object data is the actual data, while metadata is just data about the data.
      * When you create an object you specify the key name, which uniquely ident5ifies the object in the bucket
      * Every object in a bucket has exactly one key = name
    - Data Consistency Model
      * Amazons S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all regions
      * This means you can access the object immediately after it was copied or put in an s3 bucket
      * S3 offers eventual consistency for overwriting puts and deletes in all regions
      * If you update or delete an object in s3 the change will eventually be propagated and visible everywhere
    - Storage classes
      * S3 offers a range of storage classes for the objects that you store
      * You choose a class depending on your use case scenario and performance access requirements and all of these storage classes offer high durability
      * Each object in s3 has a storage class associated with it
      * TYPES:
        + Standard -default storage class

Standard storage class is used for performance-sensitive use cases ( those that require milliseconds access time) and frequently accessed data

Suitable for objects larger than 128k that you plan to store for at least 30 days

S3 stores the object data re4dundantly across multiple geographically separated AZs; objects are resilient to the loss of an AZ

* + - * + Standard\_IA and Onezone\_Ia - Infrequently accessed

Designed for long-lived and infrequently accessed data

Amazon s3 charges a retrieval fee for these objects, so they are most suitable for infrequently accessed data

S3 stores the object data in only one AZ; however the data is not resilient to the physical loss of the AZ it is in.

* + - * + Storage classes for low-cost data archiving objects (glacier and deep\_archive
        + Glacier

Data stored in this storage class has a minimum storage duration period of 90 days and can be accessed in 1-5 minutes using expedited retrieval

* + - * + Deep\_Archive

The minimum storage duration period of 1800 days and a default retrieval time of 12 hours; lowest cost storage option in AWS

* + - * Bucket Policies
        + Provide permissions across a centralized access control to the buckets and objects based on a variety of conditions
        + With bucket policies, you can add or deny permissions across all ( or a subset ) of objects based on a variety of conditions
        + With bucket policies, you can add or deny permissions across all ( or a subset) of objects within a bucket
        + Only the bucket owner is allowed to associate a policyu with a bucket.
      * Cross-Region Replication
        + Enables automatic, asynchronous copying of objects across buckets in different AWS regions
      * Pricing
        + Pay only buy the storage you use and will depend on the following

Storage Class

Start with standard and move data to standard-IS and reduce your cost for infrequently accessed data and move to the glacier for archiving data a very low costs

Storage

Depends on the number and size of objects

Requests

GET requests to come with charges

Data Transfer

Amount of data transferred out of s3 region.

TYPES:

Glacier

Starts at .004$/GB/month and allows you to archive large amounts of data at av very low cost

You only pay only for what you need, with no minimum commitments or upfront fees

Other factors determining pricing include requests and data transfers out of amazon glacier (incoming transfers are free).

Snowball

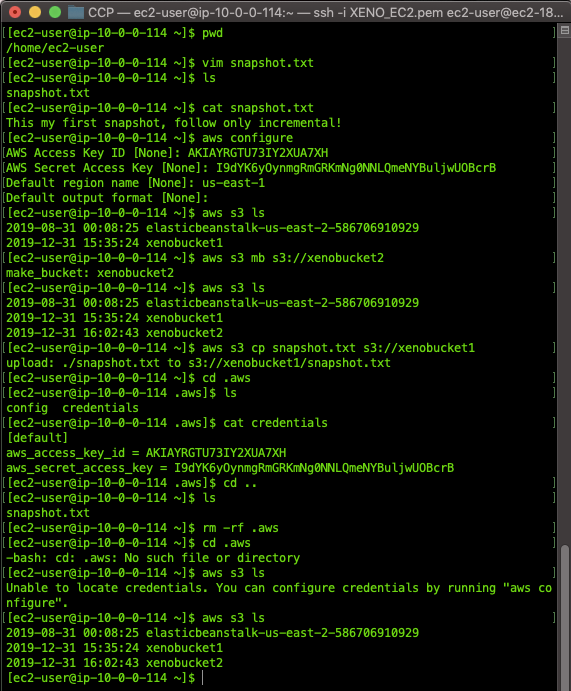
You pay a service fee per data transfer job and the cost of shipping the appliance

Each job includes the use of a snowball appliance for 10 days of onsite usage for free

Dtat transfer in to s3 is free. Data transfer out of s3 is priced by region

Snowball 50TB: 200$

Snowball 80TB: 250$

* 
* Creation of s3 and accessing files from ec2 to s3
* Module Completion& Exam Hints
  + IAM
    - Helps you securely control access to aws resources
    - You use IAM to control who is authenticated (signed in) and authorized ( has permissions) to use what resources
    - IAM authentication and authorization
      * USER ais a permanently named operator, human or aws service with permanent auth. Credentials
      * A groups is a collection os users and usually contains multiple users; a user can belong to multiple groups
      * \a role is an operator just like a user a role can be as well a human or another aws service with temporary auth. Credentials
      * Policy docs enforce authorization
  + Virtual Private Cloud
    - A VPC is a virtual network dedicated to your aws account
    - VPC enables you to launch aws resources into the virtual network that you define
    - Aws vpc is literally our data center in the aws cloud.
  + EC2
    - Provides scalable computing capacity in the aws cloud virtual machines in aws instances
    - There are four ways to pay for amazon ec2 instances
      * On-Demand Instance
        + Pay for computing capacity per hour or per second depending on which instances
      * Reserved instances
        + Provide you with a significant discount upto 75% compared to instance pricing
      * Spot instances
        + Request spare ec2 computing capacity for up to 90% off the on-demand price
      * Dedicated Hosts
        + A physical ec2 server dedicated for your use
  + Security Groups
    - Act as a virtual firewall for your ec2 instances to control inbound and outbound traffic
    - Security groups enforce security at the instance level, not the subnet; different ec2 instances can have different sgs applied
    - In a sg you add rules that control inbound traffic to the instance and separate rules that control outbound traffic
  + Elastic Block Store
    - Proivdes block-level storage volumes for use with ec2 instances
    - Ebs volumes are highly available and reliable storage columns that can be attached to any running instance that is in the same AZ
    - EBS volumes that are attached to an ec2 instance are exposed as storage volumes that persist independently from the lif of the instance
    - TYPES
      * SSD
        + General Purpose gp2

Balance between price and performance

* + - * + Provisioned iops iol

Highest peformance ssd volume

* + - * HDD
        + Throughput optimized stl

Low cost; frequently accesse4d, throughput-intensive

* + - * + Cold HHD scl

Lowest cost; less frequently accessed workloads.

* + - PRICE
      * Volumes,
        + Total storage of all volumes by GB/month
      * Snapshots
        + Total snapshot storage consumed in S3
        + Any copying between regions is also charged
      * Data Transfer
        + Inbound is free
        + Outbound is charged
  + S3
    - Provides object storage through a web service interface
    - Store and retrieve any amount od data at any time from anywhere on the web
    - You can use s3 to store files documents pics, etc as it is object storage not os storage like EBS
    - The bucket is a container for objects
    - Every object is contained in a bucket
    - Bucket names are globally unique