AWS Notes

From: AWS Certified Cloud Practitioner Certification Course (CLF-C02) - Pass the Exam!
This Google Docs Link :
https://docs.google.com/document/d/1C1L4y3WAtvDSDdVIYOIi56OLHOBAcD1bBAieJxFVv08/edit?usp=sharing

1. Cloud Computing:
    - The practice of using a network of remote servers hosted on the internet to store, manage and process data, rather than a local server or a personal computer
2. Evolution Of Cloud Hosting:
    - Back then:
        1) Dedicated server (costly, high maintenance but high security)
        2) Virtual Private Server (Better utilisation and isolation of resources)
        3) Shared Hosting (very cheap, limited functionality, poor isolation)
        4) Cloud hosting (flexible, scalable, secure, cost-effective, high configurability)

3. AWS Timeline
    - Simple Queue Service (SQS) - launched in 2004
    - Simple Storage Service (S3) - launched in Mar 2006
    - Elastic Compute Cloud (EC2) - launched in Aug 2006
    - All services migrated to AWS in Nov 2010

4. What is a Cloud Service Provider (CSP)?
    - Cloud services can be chained together to create cloud architectures
    - Services are accessible via Single Unified API eg AWS API
    - Services utilised metered billing based on usage per second, per hour
    - Services have monitoring built-in eg AWS CloudTrail
    - Have an infrastructure as a service (IaaS)
    - Offer automation via infrastructure as Code (IaC)
    - If a company does not meet all the requirements, it would be referred to as a Cloud Platform eg Twilio, Hashicorp
5. Gartner Magic Quadrant for Cloud
    - Magic Quadrant is a series of market research reports published by IT consulting firm Gartner that rely on proprietary qualitative data analysis methods. To demonstrate, market trends, such as direction, maturity and participants.

6. 4 Core Cloud Services
    - Compute (EC2)
    - Networking (VPC)
    - Storage (EBS)
    - Databases (RDS)

- AWS has over 200+ cloud services

7. Evolution of Computing
    - Dedicated
        1) Physical server wholly utilized by a single customer
        2) Have to guess your capacity
        3) Will have to overpay if you underutilize the server
        4) Can't vertical scale, need a manual migration
        5) Replacing it is very difficult
        6) Limited by your OS
        7) Multiple apps can result in conflicts in resource sharing
        8) Have a guarantee of security, privacy and full utility of underlying resources
    - Virtual Machines (VM)
        1) Can run multiple VMs on one machine
        2) Hypervisor is the software layer that lets you run the VMs
        3) A physical server shared by multiple customers
        4) Pay a fraction
        5) Overpay for underutilised VM
        6) Limited by your OS
        7) Resource sharing can cause conflicts
        8) Easy to export/import images for migration
        9) Easy to vertically and horizontally scale
    - Containers
        1) VMs running multiple containers
        2) Docker Deamon is the name of the software layer that lets you run multiple containers
        3) Maximise the utilisation of cost-effective
        4) Containers share the same OS so they are more efficient than multiple VMs
        5) Multiple apps can run side by side without being limited to the same OS requirements and will not cause conflicts
    - Functions
        1) Are managed VMs running managed containers
        2) Known as serverless compute
        3) Upload a piece of code, choose the amount of memory and duration
        4) Only responsible for code and data, nothing else
        5) Very cost-effective, only pay for the time code is running, VMs only run when there is code to be executed
        6) Cold Starts are a side effect of this setup

8. Types of Cloud computing
    - Software as a Service (SaaS) - for customers eg Gmail, office 365
    - Platform as a Service (Paas) - for developers Heroku
    - Infrastructure as a Service (IaaS) - for Admins eg AWS, Azure

9. Types of Deployment Models
    - Public Cloud - Basecamp, Dropbox
    - Private Cloud / On-Premise - Hospitals, Govt
    - Hybrid - Deloitte, DBS
    - Cross-Cloud / Multiple Cloud

10. 6 Advantages of AWS Cloud
    - Trade Capital expense for variable expense
        1) Pay On-Demand
    - Benefit from massive economies of scale
        1) Sharing the cost with other customers
    - Stop guessing capacity
        1) Scale up or down
    - Increase speed and agility
        1) Launch resources within a few clicks
    - Stop sending money on running and maintaining data
        1) Focus on your customers
    - Go global in minutes
        1) Deploy your app in multiple regions around the world with a few clicks

11. AWS Global Infrastructure
    - I globally distributed hardware and data centres that are physically networked together to act as one large resource for the end customer

    - 32 Launched regions
        1) Isolated
        2) Eg us-East-1b the “East-1” denotes the region
        3) Different regions have different pricing, services and performance

    - 102 Availability Zones
        1) A data centre in a secured building that contains hundreds of thousands of computers
        2) Generally 3 AZs in a region
        3) You choose the AZs by choosing the subnets
        4) Eg . us-East- 1b the “b” denotes the AZ
        5) Multi-AZ won't be affected by power issues

    - 115 Direct Connection Locations
    - 550+ Points of Presence

    - 35 Local Zones
        1) Datacenters located close to densely populated areas
        2) Provides low latency performance (7ms)
        3) Eg us-west-2-lax-1a

- 29 Wavelength Zones
    1) Allows for edge computing for low latency
    2) EC2 instances

12. Fault Domains (Failure Zone)
    - It 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
    - Many fault domains (AZs) = fault level (Region)
    - Fault domains can be in specific servers in a rack, an entire rack, an entire room or even the entire data centre

13. AWS Global Network
    - Represent the interconnection between Global INfrastrucyt
    - Edge Locations can act as on and off-ramps to the Global Network
    - VPC Endpoints

14. Point of Presence (PoP)
    - Centre owned by AWS or a trusted partner for content or expedited delivery
    - Edge Locations
        1) Datacenters that hold cached(copy) on the popular files (webpages, images and videos)
    - Regional Edge Caches
        1) Datacenter that holds much larger aches of less popular files
    - AWS services using PoP
        1) Amazon CloudFront
        2) Amzaon S3 Transfer Acceleration
        3) Amazon Global Accelerator

15. AWS Direct Connect
    - A private/dedicated connection between your data centre, office, co-location and AWS
    - 2 high-speed network
        1) Lower Bandwidth 50MBps - 500 MBps
        2) Higher Bandwidth 1GBps - 10GBps
    - Reduce network costs and increase bandwidth throughput
    - More consistent network experience

16. Data Residency
    - Physical or geographical of where an organization or cloud resources reside
    - Compliance Boundaries
        1) Regulatory/legal requirement where the govt tells the organisation
    - Data Sovereignty
        1) Jurisdictional control or legal authority that can be asserted over data

- AWS Outpost
    1) Physical rack of servers that you can put in your data centre which means your data will reside where the outpost is
- AWS Config
    1) Policy Code Service
    2) Can create a rule to check AWS resources configuration continuously
    3) If they deviate you are alerted or the AWS config does auto-remediate
- IAM Policies
    1) can be written explicitly to deny access to specific AWS regions
    2) Service Control Policy (SCP) are permissions applied organisation-wide

17. AWS Government
- AWS can be utilised by the Public sector because AWS achieves this by meeting regulatory compliance programs through special regions called GovCloud
- AWS GovCloud (Global)
    1) A CSP generally will offer an isolated region to run FedRAMP workloads
    2) Only for US entities and root account holders
- AWS in China
    1) Is completely isolated intentionally from AWS Global to meet regulatory compliance for Mainland China
    2) Own domain at Amazon.cn
    3) It operates in China, you need a Chinese Business License (ICP License)
    4) Not all services are available eg route 53
    5) Running in China means you would not need to transverse The Great Firewall
    6) 2 Regions: Ningxia and Sinnet

18. Sustainability
- Co-founded the Climate Pledge to achieve Net-Zero Carbon Emissions by 2040
- AWS Cloud's Sustainability goal
    1) Renewable Energy - powered by 100% renewable energy by 2025 RECs and GOs
    2) Cloud Efficiency - 3.6 times more efficient than the median of US enterprise DCs
    3) Water Stewardship - Direct Evaporatiov Tech and using non-potable water for cooling

19. AWS Ground Station
- Lets you control satellite communication, process data and scale your operation without manning and infrastructure
- Use cases:
    1) Weather forecasting
    2) Surface imaging
    3) Comms and video broadcasts
- To use a ground station

1) Schedule a contact (select satellite, start and end time, ground location)
2) 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

20. AWS Outposts

- Rack of servers running AWS infrastructure on your physical location
- 3 Form Factors:
    1) 42U - Full rack of servers by AWS
    2) 1U - place into your existing racks
    3) 2U - place into your existing racks

21. Cloud Architecture Terminologies
- Solutions Architect
    1) Architects' technical solution using multiple systems via research, and documentation
- Cloud Architect
    1) Solutions architect that is focused solely on architecting solutions using cloud services
- Cloud Architect - business factors:
    1) Availability - Highly Available(HA)
    2) Scalability - the ability to grow rapidly or unimpeded
    3) Elasticity - the ability to shrink and grow to meet the demand
    4) Fault Tolerance - the ability to prevent a failure
    5) Disaster Recovery - Highly Durable (HR)
    6) Cost
    7) Security

22. Cloud Architect
- High Availability
    1) Ensuring there is no single point of failure
    2) Run your workload across multiple AZs to ensure that if 1 or 2 AZ become unavailable your service remains available
    3) Elastic Load Balancer allows you to evenly distribute multiple servers in one or more datacentre like making backup
- Scalability
    1) Increase your capacity based on the increasing demand for traffic, memory and computing power
    2) Scaling Up (Upgrade to a bigger server) or Scaling Out (Add more servers of the same size - increases your availability too)
- High Elasticity
    1) Automatically increase or decrease your capacity based on the current demand of traffic
    2) Horizontal Scaling Out or In

3) Auto Scaling Groups (ASG) is an AWS feature that automatically adds or removes servers based on scaling rules defined by you

- Fault Tolerance
    1) Prevent the chance of failure
    2) Fail-overs are when you have a plan to shift traffic to a redundant system in case the primary system fails, have a copy of the database
    3) RDS Multi-AZ is when you run a standby database in another AZ in case your primary fails
- High Durability
    1) CloudEndure Disaster Recovery continuously replicates your machines into a low-cost staging area in your AWS account and preferred region
    2) A business Continuity Plan (BCP) outlines how a business will continue operating during an unplanned disruption in services
    3) RPO - the maximum acceptable amount of data loss, units is time
    4) RTO - the maximum amount of downtime your business can tolerate without financial loss
    5) Backup&Restore < Pilot Light < Warm Standby < Multi-Site Active (how fast can you recover and the cost of it)

23. AWS Application Programming Interface (API)
    - An API is a software that allows two applications/services to talk to each other, the most common type of API is via HTTP/S requests
    - Each AWS Service has its endpoint which you send a request, and then you need to generate a signed request (complicated)
    - Rarely do users directly send HTTP requests to AWS API, it's much easier to interact with the API via a variety of developer tools
        1) HTTP Request - directly interact with the AWS API
        2) AWS CLI - interact via terminal/shell program
        3) AWS SDK - interact using your favourite programming language
        4) AWS Management Console - A WISWIG Web Interface

24. AWS Management Console aka ClickOps
    - Web-based unified console builds, manages and monitors everything

25. AWS Tools for PowerShell
    - Built on top of the .NET
    - Lets you interact with AWS API

26. AWS Resource Names (ARNs)
    - Partition
        1) Aws - AWS Regions
        2) Aws-cn - China Regions
        3) Aws-us-gov - AWS GovCloud (US) regions
    - Service

    1) Ec2
    2) S3
    3) iam
- Region
    1) Us-east-1
    2) Ca-central-1
- Account ID
- Resource ID
- Wildcard (*)
- Example:
    1) Arn:aws:s3:::my-bucket

27. AWS CLI
    - Go to AWS CloudShell (logo found at the top bar) to install CLI
    - Then you can add or create S3 buckets and other services

28. AWS Software Development Kit (SDK)
    - A collection of software development tools in one package
    - Use it to programmatically create, modify, delete or interact with AWS resources
    - AWS Cloud9 (AWS IDE)
    - Offerings:
        1) Java
        2) Python
        3) Node.js
        4) Ruby
        5) Go
        6) .NET
        7) PHP
        8) JavaScript
        9) C++

29. AWS CloudShell
    - Browser-based shell built into AWS Management Console
    - Has pre-installed tools eg AWS CLI,python,Node.js etc
    - Can seamlessly switch between PowerShell or other shells

30. Infrastructure as Code (IaC)
    - Write a configuration script to automate creating, updating or destroying cloud infrastructure
    - IaC is a blueprint of your infrastructure
    - Allows you to easily share, version or inventory of your cloud infrastructure
    - AWS has two offerings for writing it:

1) AWS CloudFormation (CFN) - is a declarative IaC tool (Explicit - what you see is what you get, zero chance of misconfiguring)
2) AWS Cloud Development Kit (CDK) - is an imperative IaC tool (Implicit - you say what you want and the rest is filled in, could end up misconfiguring)

31. CloudFormation (CFN)
    - Allows you to write IaC as either JSON or YAML file
    - CDK generates it so easier for DevOps to read and debug any errors

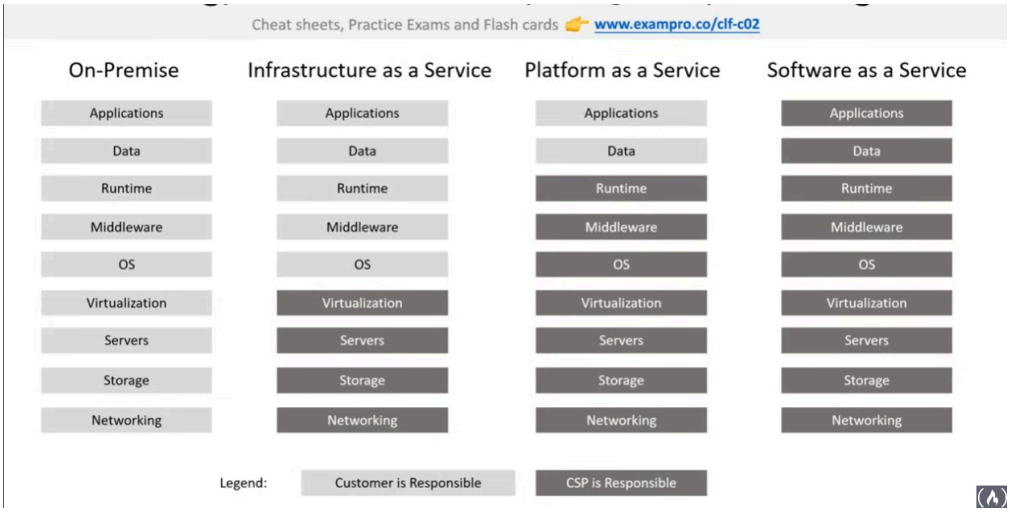
32. Cloud Development Kit (CDK)
    - Allows you to use your favourite programming language to write infrastructure as Code
    - CDK generates CloudFormation templates
    - Has a large library of reusable cloud components called CDK construct https://constructs.dev
    - comes with its own CLI
    - pipelines to quickie setup CI/CD pipelines for CDK projects
    - has a testing framework for unit and integration Testing
    - AWS SDK and CDK might look similar but CDK ensures idempotent of your infrastructure

33. AWS Toolkit for VSCode
    - Open source plugin for VSCode to create, debug, and deploy AWS resources
    - AWS Explorer
    - AWS CDK Explorer
    - Amazon Elastic Container Service
        1) Provide IntelliSense for EC2- task-defined files
    - Serverless Application

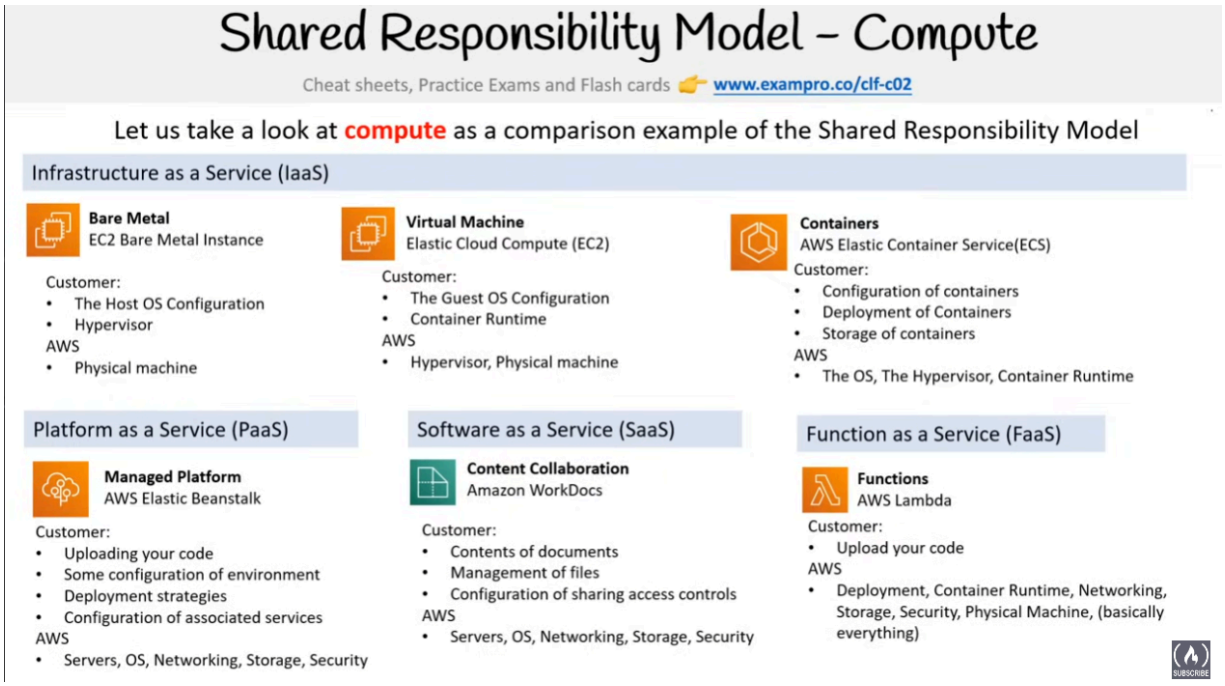
34. Introduction to the Shared Responsibility Model
    - Is a cloud security framework that defines the security obligations of the customer and versa the CSP

35. AWS Shared Responsibility Model
    - Customers are responsible for Security In the Cloud
        1) Data
        2) Configuration
    - AWS is responsible for Security of the Cloud
        1) Hardware
        2) Operation of Managed Services
        3) Global Infrastructure

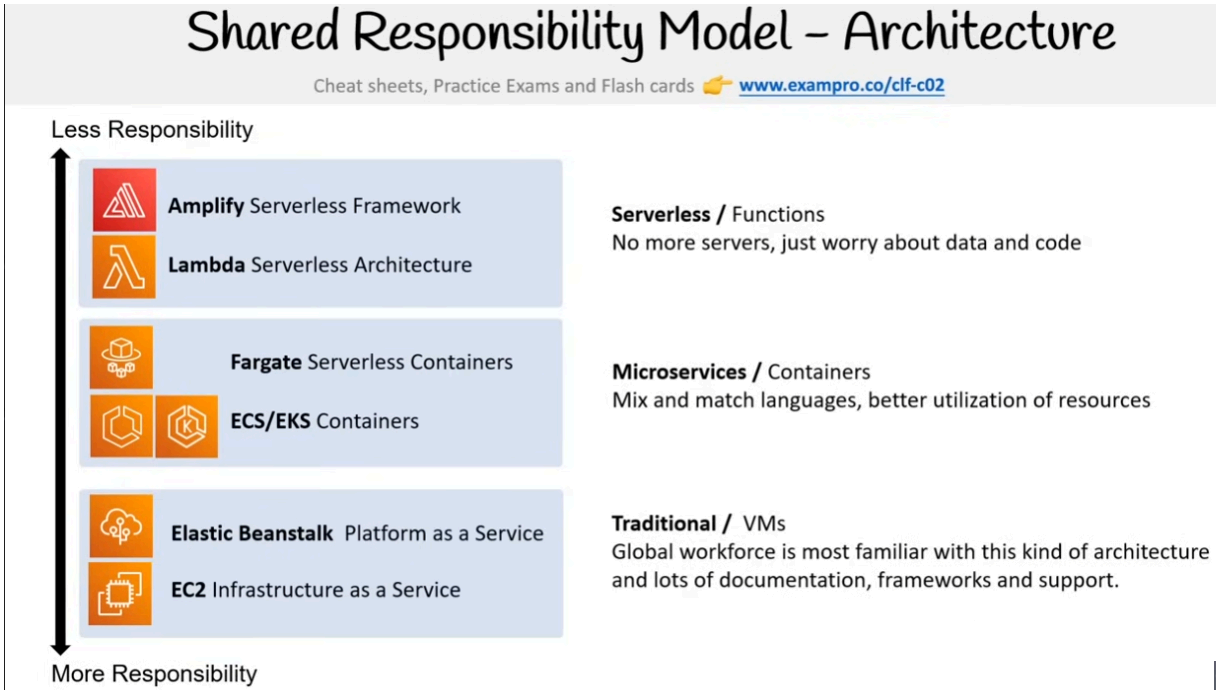
36. Types of Responsibilities



37. Shared Responsibility Model - Compute



38. Shared Responsibility Model Architecture



39. Computing Services - Elastic Compute Cloud (EC2)
    - Allows you to launch Virtual Machines (VM)
    - Amazon Machine Image (AMI) is a predefined configuration for a VM
    - Server virtualisation allows you to create, copy, resize or migrate your server
    - EC2 is highly configurable where you can choose AMI that affects options such as
        1) Amount of CPUs
        2) RAM
        3) Network Bandwidth
        4) OS
        5) Attach multiple virtual hard-drive for storage eg Elastic Block Store (EBS)
    - EC2 is the backbone of AWS, majority AWS services use EC2 as their underlying servers, S3, RDS, DynamoDB, Lambdas

40. VMs, Containers and Serverless Functions

    - Virtual Machines - emulation of a physical computer using software

        1) Amazon LightSail - manages virtual server service to launch a Windows server but don't know how or don't know WordPress

    - Containers - virtualising an OS to run multiple workloads on a single OS instance, microservice architecture when you divide your application into smaller applications that talk to each other

1) Elastic Container Service (ECS) - is a container orchestration service that launches a cluster of servers on EC2 instances with docker installed (when you need docker or need to run containers
2) Elastic Container Registry (ECR) - is a repository for container images, you need an image to launch containers
3) ECS Fargate - serverless orchestration container service, ECS but serverless and pay on-demand
4) Elastic Kubernetes Service (EKS) - is a fully managed Kubernetes Service, when you need to run Kubernetes which id form Google and a standard for managing Microservices

- Serverless - underlying servers managed by AWS, you dont worry or configure servers

    1) AWS Lambda - is a serverless function service

41. High-Performance Computing Services

- The Nitro System - dedicated hardware and lightweight hypervisor, all new EC2 instances use this
    1) Nitro Cards - specialised cards for VPC, EBS and instance storage and controller card
    2) Nitro Security Chips - integrated into motherboards, protects hardware resources
    3) Nitri Hypervisor - lightweight hypervisor Memory and CPU allocation Bare Mtel-Like performance

- Bare Metal Instance - EC2 Instance without hypervisor to run workloads directly on hardware for max performance and control. M5 and R5 are bare metal EC2 instances
    1) Bottlerocket is a Linux-based open-source operation system that is purpose-built by AWS for running containers on VMs or bare metal hosts

- High Performance Computing (HPC)
    1) Cluster of hundreds of thousands of servers with fast connection between each of them, boosting computing capacity
    2) AWS ParallelCluster - AWS-supported open source cluster management tool easy for you to deploy and manage HPC

42. Edge and Hybrid Computing
- Edge Computing
    1) When you push your computing workloads outside of your network to run close to the destination location eg pushing computing to run on phones, IoT devices or external servers, not within your cloud network
- Hybrid Computing
    1) Run workloads on both your on-premise datacenter and AWS VPC

- AWS Outposts
    1) physical rack of servers that you can put in your data center, allows you use AWS API and Services such as EC2 right in your datacenter
- AWS Wavelength
    1) allows you to build and launch your application in a telecom datacenter, ultra-low latency since they pushed over 5G Network
- VMWare Cloud on AWS
    1) manage on-premise VMs using VMWare as EC2 instances, only for VMWare virtualised date canter
- AWS Local Zones
    1) edge datacenter located outside of an AWS region so you can use AWA closer to destination

43. Cost & Capacity Management of Computing Services
- EC2 Spot Instances, Reserved Instances and Savings Plan
- AWS Batch
    1) Plans, schedules and executes your batch computing workloads across the full range of AWS compute services, can utilise Spot instances to save money
- AWS Compute Optimiser
    1) Suggesting how to reduce costs and improve performance by using Machine Learning (ML) to analyse your previous usage history
- EC2 Autoscaling Groups (ASGs)
    1) 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 number of servers you need
- Elastic Load Balancer (ELB)
    1) Distributed traffic to multiple instances, can re-route traffic from unhealthy to healthy instances, can router traffic to EC2 instances running different AZs
- AWS Elastic Beanstalk
    1) Easily deployed for web-applications without developers having to worry about setting up and understanding underlying AWS services, similar to Heroku

44. Types of Storage Services
- Elastic Block Store (EBS) - Block
    1) Manages data as blocks within sectors and tracks
    1) When you need a virtual hard drive attached to a VM
    2) Data is split into evenly split blocks, directly accessed by the OS
    3) Supports only a single write volume
- AWS Elastic File Storage (EFS) - File
    1) Manages data as files and file hierachy
    1) When you need a file-share where multiple users or VMs need to access the same drive
    2) File is stored with data and metadata, multiple connections via network share
    3) Supports multiple reads, writing locks the file

- Amazon Simple Storage Service (S3) - Object
    1) When you just want to upload files and not to have worry about the underlying infrastructure
    2) Object stores with data,metadata and Unique ID, scaled wil limited no file limit or storage limit
    3) Supports multiple reads and writes (no locks)
    4) Not intended for IOPs (Input and Output per second)

45. Simple Storage Service (S3)
- Can store 0 bytes to 5 TB per object
- S3 Object
    1) Object contains your data, like your files
    2) Key - name
    3) Value - data in a sequence of bytes
    4) Version ID - version of the object
    5) Metadata - additional information attached to the data
- S3 Bucket
    1) Buckets hold objects, buckets can also have folders which in turn have objects
    2) S3 is a universal namespace so bucket names must be unique, kinda like having a domain name

46. S3 Storage Classes (Expensive - Cheap)
- S3 Standard (default)
    1) Fast, 99.99% availability, replicated across at least 3 AZs
- S3 Intelligent Tiering
    1) Uses ML to analyse object usage and determine the appropriate storage class
- S3 Standard-IA - (Infrequent Access)
    1) Still fast, cheaper by 50% than standard if you access files less than once a month
    2) Additional retrieval fees applied
- S3 One-Zone-IA
    1) Still Fast, objects only exist in one AZ, availability 99.5% 20% cheaper than standard-IA
    2) Data could get destroyed, retrieval fees applied
- S3 Glacier
    1) long -term cold storage, retrieval of data can take minutes to hours
- S3 Glacier Deep Archive
    1) Lowest cold storage class, data retrieval time is 12 hours

47. AWS Snow Family
- Storage and compute devices used to physically move data in or out of the cloud when moving data over the internet or private connection is too slow, difficult or costly
- Snowcone
    1) 8TB of Storage (HHD)

    2) 14TB of Storage (SSD)
- Snowball Edge
    1) 80TB storage optimised
    2) 39.5 TB compute optimised
- Snowmobile
    1) 100 PB of storage
- All data is delivered to Amazon S3

48. Storage Services
    1) Simple Storage services
        - Serverless object storage service
    2) S3 Glacier
        - Cold storage, low-cost service for archiving and long-term backup
        - Uses previous generation HDD drives to get that low-cost, highly secure and durable
    3) Elastic Block Store (EBS)
        - Persistent block storage service
        - Virtual hard drive in the cloud you attach to EC2 instances
        - SSD, IOPS SSD, throughput HHD, Cold HHD
    4) Elastic File Storage (EFS)
        - Cloud-native NFS file system, mounts to multiple EC2 instances at the same time
        - Share files between multiple servers
    5) Storage Gateway
        - Hybrid cloud storage (includes on-premise storage to the cloud)
        - File Gateway extends your local storage 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 files on very cost-effective long-term storage
    6) AWS Snow Family
        - Storage devices used to physically migrate large amounts of data
        - Snowcone is a tiny version of snowball (8TB)
        - Snowball Edge are briefcase size data storage devices (50-80 TB)
        - Snowmobile is a cargo container filled with racks of storage and compute that is transported via a truck (100PB per trailer)
    7) AWS Backup
        - Fully managed backup service that makes it easy to centralise and automate the backup of data across multiple AWS services
    8) AWS CloudEndure Disaster Recovery
        - Continuously replicate 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
    9) Amazon FSx

- Feature-rich and highly performant file system that can used for Windows or Linux
- Amazon FSx for Windows File Server uses the SMB protocol and allows you to mount FSx to Windows servers
- Amazon FSx for Lustre uses Linux's Lustre file system and allows you to mount FSx to Linux servers

49. Databases
    - The data store that stores semi-structured and structured data
    - More complex data stores because it requires using formal design and modelling techniques
    - Relational Database
        1) Structured data, represents tabular data, row-oriented and column-oriented
    - Non-Relational Database
        1) Semi-structured that may or may not represent tabular data
    - Normally databases infer someone is using a relational row-oriented data store

50. Data Warehouse
    - Relational datastore for analytic workloads, generally column-oriented data store
    - Perform aggregation
    - Generally designed to be HOT, means return queries very fast with vast amount of data

51. Key-Value store (NoSQL)
    - Non-relational database (NoSQL)
    - Dumb and fast
    - Uses key-value method to store
        1) Interpret data resembling dictionary(python concept)

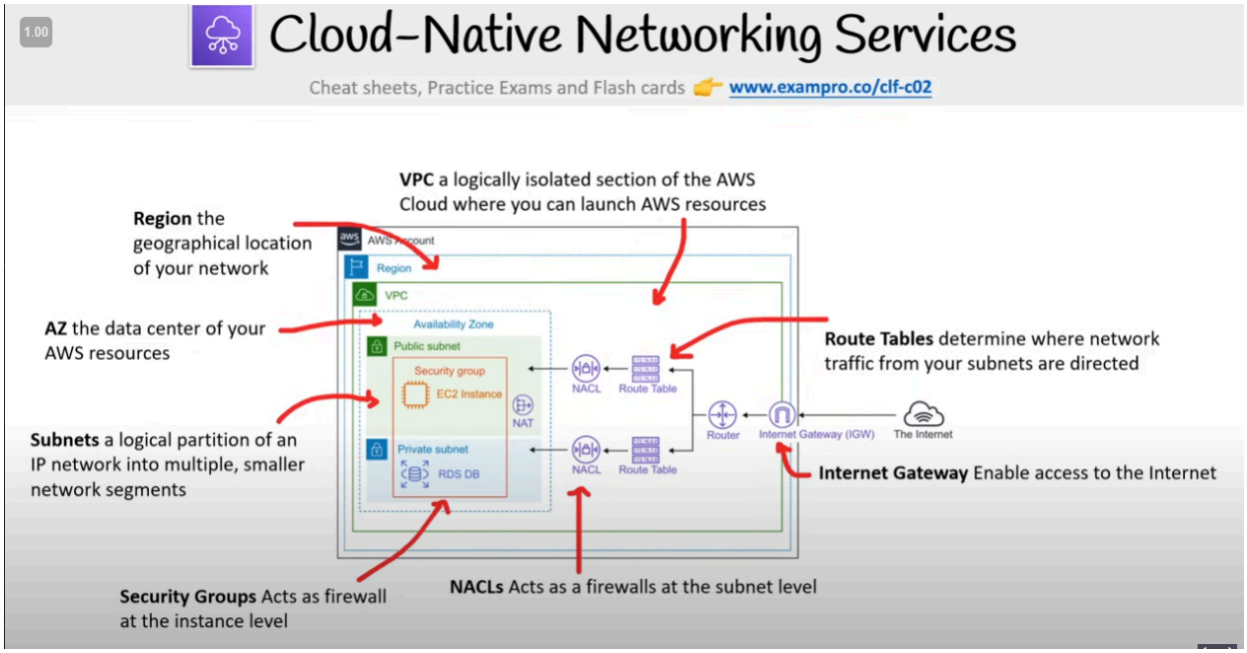
52. Document Store (NoSQL)
    - Is a NoSQL database that stores document
    - Could be an XML, more commonly JSON/JSON-Like
    - Sub-class of key/value

53. NoSQL Database Service on AWS
    1) DynamoDB (NoSQL)
        - Serverless NoSQL key/value and document database
        - AWS's flagship database service, a service that just scales and cost-effective
    2) DocumentDB
        - NoSQL document database like MongoDB (compatible too)
        - When you want to use MongoDB
    3) Amazon Keyspaces
        - Basically an Apache Cassandra Database
        - Columnar store database

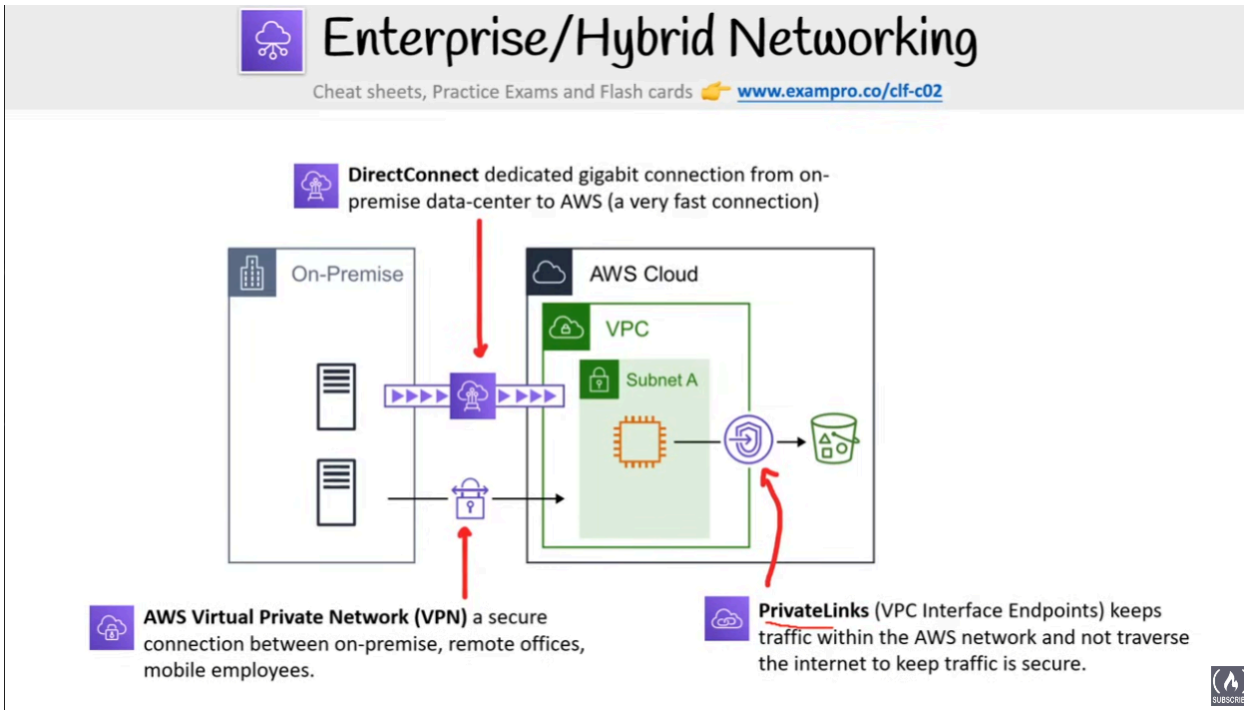
54. Relational Database Services
    1) Relational Database Service (RDS)
        - Relational synonymous with SQL and Online Transactional Processing (OLTP)
        - Aurora - fully managed database of either MySQL(5xfaster) or PSQL(3xfaster) when you want a highly available, durable, scalable and secure relational database
        - 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 font have lots of traffic demand
        - RDS on VMWare - allows you to deploy RDS-supported engines to an on-premise data centre, it has to be virtualised by VMWare when you want databases managed by RDS on your datacentre

55. Other database services
    1) Redshift
        - Is a petabyte-size data warehouse
        - When you need to quickly generate analytics or reports from a large amount of data
    2) ElastiCache
        - In-memory and caching open-source databases Redis or Memcached
        - When you need to improve the performance of an application by adding a caching layer in front of a web server or database
    3) Neptune
        - Managed graph database, data represented as interconnected nodes
        - When you need to understand the connection between data
    4) Amazon Timestreams
        - Time series database, devices that send lots of data that are time-sensitive
        - When you need to measure how things change over time
    5) Amazon Quantum Ledger Database
        - Transparent, immutable and cryptographically variable transactional logs
        - When you need to record the history of financial activities that can be trusted
    6) Database Migration Service (DMS)
        - On-premise database to AWS
        - From two databases in different or the same AWS accounts using different SQL engines
        - From an SQL to NoSQL database

56. Cloud-Native Networking Services



57. Enterprise/Hybrid Networking



58. VPC & Subnets

1) Virtual Private Cloud (VPC)
    - Is a logically isolated section of the AWS Network where you launch your AWS resources

- Choose a range of IPs using CIDR range
- CIDR Range of 10.0.0.0 / 16 = 65,536 IP Adresses

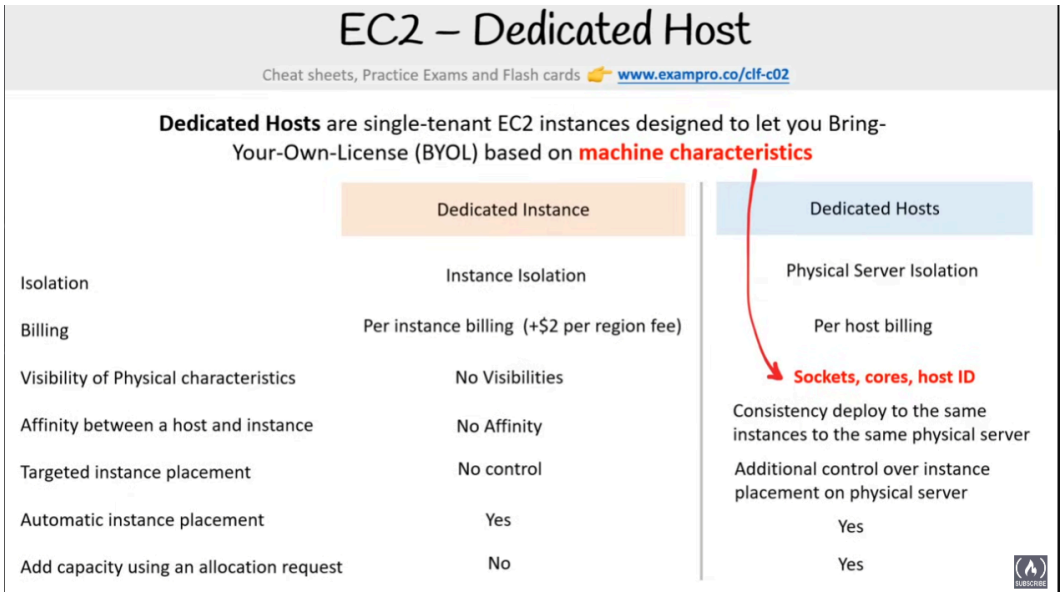
2) Subnets
   - Logical partition of an IP network into multiple smaller network segments
   - Breaking up your IP range for VPC into smaller networks
   - Need to have a smaller CIDR range than VPC ro represent their portion
   - Public Subnet - can reach internet
   - Private Subnet - cannot reach internet

59. Security Groups vs NACLs
    1) Network Access Control Lists (NACLs)
       - Virtual firewall at the subnet level
       - Create allow and deny rules
       - Eg block a specific IP address knows for abuse
    2) Security Groups
       - Virtual firewall at the instance level
       - Denies all traffic, create only allow rules
       - Eg cannot block a single IP Address

60. EC2
    - Elastic Compute Cloud (EC2) is a highly configurable virtual server (aka VMs)
    - Resizable computable capacity, takes minutes to launch anew instance
    - Steps to Launch:
      1) Choose OS via Amazon Machine Image (AMI)
      2) Choose Instance Type - t2.nano / t2.mocro / C4.8xlarge
      3) Add Storage (EBS, EFS) - SSD / HDD / Virtual Magnetic Tape / Multiple Vo;umes
      4) Configure Intsance - Security Groups, Key Pairs, UserData, IAM roles, Placement Groups

61. EC2 Tenancy
    1) Dedicated Host
       - You get the whole rack
       - Your server lives here and you have control of the physical attributes
    2) Dedicated instance
       - Yoru server in a shared rack with other customers' servers
       - Always lives there
    3) Default
       - Instance lives here until reboot
       - Always changes from server/rack to server/rack

62. Dedicated Host vs Dedicated Instance
    - Dedicated hosts are single-tenant EC2 sinatces designed to let you Bring-Your-Own-License (BYOL) based on machine characteristics
    -



63. EC2 Instance Family
    - Different families have different combinations of CPU, Memory, storage and networking capacity
    - Choose appropriate combination
    - Varying hardware used to give them unique properties
    1) General Purpose
        - A1, T2, T3, T3a, T4g, M4, M5, M5a, M5n, M6zn, M6i, Mac
        - Balance : web servers and code repositories
    2) Compute Optimised
        - C5, C4, Cba, C5n, C6g, C6gn
        - High-performance : scientific modelling, dedicated gaming servers and ad server engines
    3) Memory Optimised
        - R4, R5, R5a, R5b, R5n, X1, X1e, High Memory, z1d#
        - Fast process large datasets in memory : in-memory caches, in-memory databases, realtime big data analytics
    4) Accelerated Optimised
        - P2, P3, P4, G3, G4ad, G4dn, F1, Inf1, VT1
        - Hardware accelerators/co-processors : ML, computational finance, seismic analysis, speech recognition
    5) Storage Optimised
        - I3, I3en, D2, D3, D3en, H1
        - Large datasets on local storage : NoSQL, data warehousing

64 EC2 Instance Types

- Instance size and family, t2.micro
- Sizes: Nano, micro, small, medium, large, xlarge, 2xlarge, 4xlarge, 8xlarge
- Exceptions: c6g.metal is a bare metal machine
- Instance sizes generally double in prices and key attributes

65. EC2 Pricing Models

1) On-Demand - least commitment
    - Low cost and flexible
    - Pay per hour/second
    - Short-term, spiky, unpredictable
    - Uninterrupted
    - First-time apps

2) Spot (up to 90% off) - biggest savings
    - Request spare computing capacity
    - Flexible start and end times
    - The server randomly stops and starts
    - For non-critical background jobs

3) 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

4) Dedicated - most expensive
    - Dedicated servers
    - Can be on-demand / reserved / spot
    - Guarantee of isolated hardware

66. On-Demand

- Pay-As-You-Go (PAYG) model
- When you launch an EC2 instance it is by default On-Demand pricing
- No-upfront and long term payment
- Per second and per hour charging

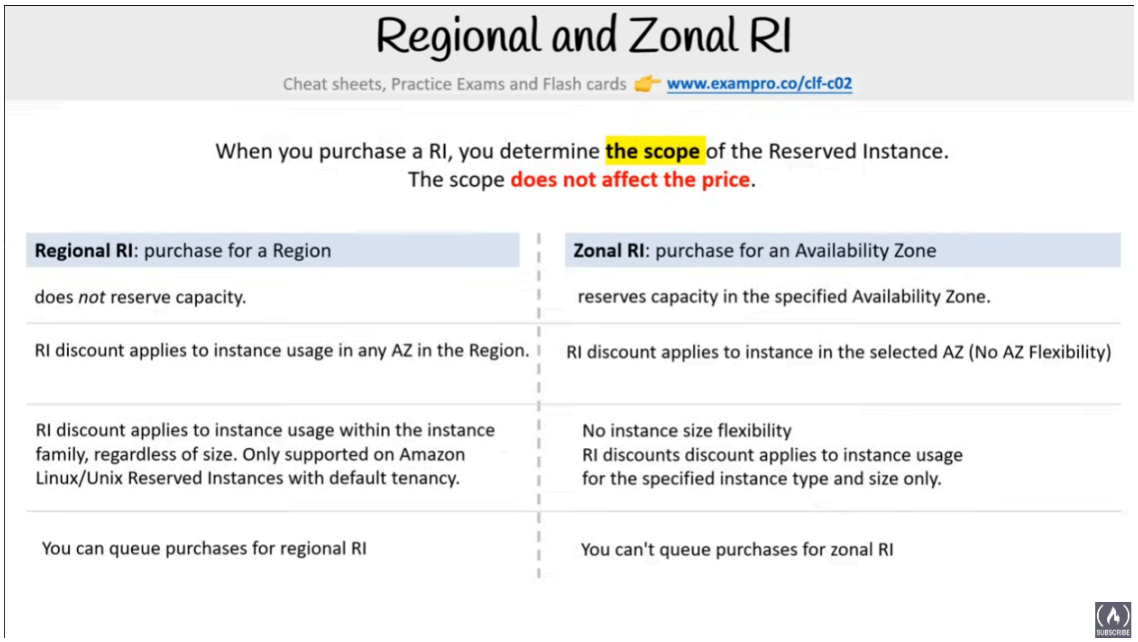
67. Reserved Instances (RI)

- RIs can be shared between multiple accounts within an AWS organisation
- Unused RIs can be sold in the RI Marketplace
- Reduced Pricing based on = Term x Class Offering x RI Attributes x Payment Option

1) Term
    - Longer-term, greater savings
    - 1-year or 3 Year contract
    - RI do not renew automatically, once expiration changed to on-demand with no interruption
2) Class
    - Less flexible, greater savings
    - Standard: up to 75% off from on-demand, can modify RI attributes
    - Convertible: up to 54% off from on-demand, exchange RI based on RI attributes if greater or equal in value
    - Scheduled: Cancelled
3) Payment Options
    - Greater upfront, greater savings
    - All Upfront: full payment made at the start of the term
    - Partial Upfront: portion paid upfront, remaining hours billed at a discounted hourly rate
    - No Upfront: billed at a discounted hourly rate regardless of the RI is being used

68. RI Attributes (Instance Attributes)
    1) Instance Type
    2) Region
    3) Tenancy
    4) Platform - OS

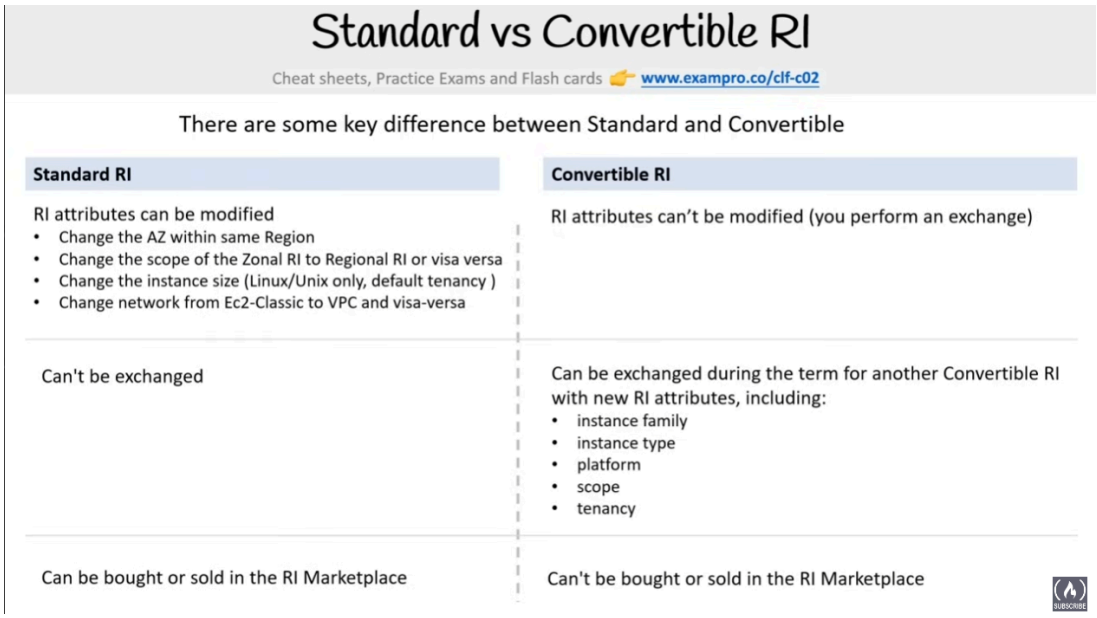
69. Regional VS Zonal RI



70. RI Limits
    - Regional Limits
        1) 20 regional RIs per Region
        2) Cannon exceed your running on-demand instances
        3) The default limit for on-demand instances is 20
    - Zonal Limits
        1) 20 Zonal RIs per AZ
        2) Can exceed running on-demand instance limit by purchasing zonal reserved instances
        3) 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 specification of your zonal RIs

71. Capacity Reservations
    - Backed by hardware so there is a finite amount of servers available within an AZ per instance type or family
    - To solve this: Capacity Reservation
    - Allows you to request a reserve of EC2 instance type
    - Charged at the selected instance type's on-demand rate whether an instance running in it or not
    - Can also use regional RIs with your capacity reservations to benefit from billing discounts

72. Standard VS Convertible RI



73. RI Marketplace
    - Sell your unused standard RI
    - Sold after active for at least 30 days and once AWS has received the upfront payment
    - Must have a US bank account
    - At least one month remaining in the term
    - Seller company name will be shared with the buyer for tax purposes
    - The seller can set only the upfront price, other configurations remain same
    - Term length rounded down to nearest month
    - Sell up to $20,000 in RI per year
    - GovCloud RIs cannot be sold here

74. Spot Instances
    - Unused compute capacity
    - Can be terminated if the computing capacity if needed by other on-demand customers
    - AWS Batch is an easy and convenient way to use Spot Pricing
    - Termination Conditions
        1) Can be terminated by AWS anytime
        2) Once termination by AWS you won't get charged for a partial hour of usage
        3) If you terminate, you will be charged for any hour that it ran

75. Dedicated Instances
    - To meet regulatory requirements
    - Enterprises may have security concerns or obligations giants sharing the same hardware with other AWS customers (server-bound licensing that won't support multi-tenancy)
    - Single-tenant - like having your own house

- A single customer has dedicated hardware
- Physical isolation between customers
- Offered to: On-Demand, Reserved, Spot

76. AWS SavingsPlan
    - Savings plans offer you similar discounts as Reserved Instances (RI) but simplify the purchasing process
    - 3 different savings plans:
        1) Compute Savings Plan
            - Up to 66% off
            - Automatically apply for EC2 instance usage AWS Fargate / AWS Lambda service usage regardless of instance family, size, AZ, region, OS, tenancy
        2) EC2 Instances
            - 72% in exchange for a commitment to the usage of individual instance families in a region
            - Automatically reduces the cost on selected instance family in that region regardless of AZ, size, OS or tenancy give
            - Flexibility to change your usage between instances within a family in that region
        3) SageMaker (AWS's ML services)
            - Reduce SageMaker costs up to 64%
            - Automatically apply to SageMaker usage regardless of instance family, size, component or AWS region
    - 2 different terms
        1) 1 Year
        2) 3 Year
    - Payment Options
        1) All Upfront
        2) Partial Upfront
        3) No Upfront

77. Zero Trust Model
    - "Trust no one, verify everything"
    - Primary Security Perimeter - the first line of defence protects the company's cloud resources and assets
    - Identity becomes the Primary security perimeter
    - Identity-Centric does not replace but augments Network-Centric Security
    1) Network-Centric (Old-Way)
        - Traditional security focused on firewalls and VPNs since there were few employees or workstations outside the office or they were in specific remote offices
    2) Identity-Centric (New-Way)
        - Bring-your-own-device, remote workstations becoming more common
        - Can't trust employees in a secure location

- Identity-based security controls like MFA

78. Zero Trust on AWS
    1) AWS Identity and Access Management (IAM)
        - IAM Policies
        - Permission Boundaries
        - Service Control Policies (Organisation-wide Policies)
        - IAM Policy Conditions
            1. aws:SourceIp - Restrict on IP Address
            2. aws:RequestedRegion - Restrict Region
            3. aws:MultiFactorAuthPresent - Restrict if MFA is turned off
            4. aws:CurrentTime - Restrict access based on time of day

    - AWS does not have ready-to-use identity controls that are intelligent, which is why AWS is considered to not have a Zero Trust offering for customers and third-party services need to be used

    - A collection of AWS services can be set to intelligent-ish detection of identity concerns but requires expert knowledge
        1) AWS CloudTrail -> Amazon GuardDuty -> Amazon Detective
        1) AWS CloudTrail - tracks all API calls
        2) Amazon GuardDuty - detects suspicious or malicious activity based on CloudTrail and other logs
        3) Amazon Detective - used to analyse, investigate and quickly identify security issue (can ingest findings from GuradDuty)

79. Zero-Trust on AWS with third parties (actual Zero Trust)
    - Third Parties
        1) Azure Active Directory
        2) Google BeyondCorp
        3) JumpCloud
    - Use the AWS Single Sign On (SSO) to use these third parties in your AWS to give it a Zero Trust Model

80. Directory Service
    - Shared information infrastructure for locating, managing, administering and organising resources
    - Eg. Domain Name Service (DNS) for the internet, Microsoft Active Directory
    - Microsoft Active Directory
        1) Domains have Child Domains
        2) Child Domains have Organisation Units (OUs)

81. Identity Providers (IdPs)

- IdPs a system entity that creates, maintain and manage identity information for principals and also provide 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
- IdPs 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
    1) OpenID
        - Login into different social media platforms using a Google or Facebook account
        - OpenID is about providing who you are
    2) OAuth2.0
        - Doesn't share password data instead uses authorisation tokens to prove an identity between consumers and service providers
        - OAuth is about granting access to functionality
    3) SAML
        - Security Assertion Markup Langauge
        - Exchanging authentication and authorisation between an identity and service provider
        - Single Sign-On (SSO) via web browser uses SAML

82. Single-Sign-On
- Allows a user to log in with a single ID and password to different systems and software
- Allows IT departments to administrate a single identity that can access many machines and cloud services
- Once you are logged in SSO, into their primary directory,you don't need to log in again
- E.g You have Azure Active Directory, use SAML to get SSO then use Slack/AWS/ Google Workspace/workstation

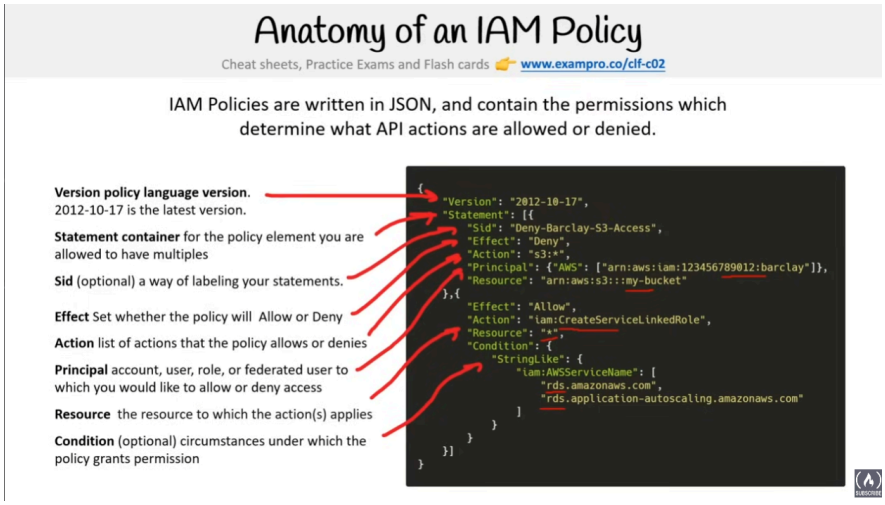
83. LDAP
- Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an IP network
- Commonly used as a central place to store usernames and passwords
- LDAP enable same-sign-on, same sign-on allows users to single ID and password, but they have to enter it in every time they want to log in (the difference from SSO)
- Why LDAP when SSO is more convenient?
    1) Most SSO systems are using LDAP
    2) LDAP was not designed natively to work with web applications
    3) Some systems only support integration with LDAP and not SSO

84. MFA

- After you fill in your username/email and password you have to use a second device such as a phone to confirm that you logging in
- Protects against people who have stolen your password

85. Security Keys
    - Used as a method of MFA
    - Physical auth token, looks like a USB with a button on it

86. AWS IAMs
    1) IAM Policies
        - JSON documents that grant permissions for a specific user, group or role to access services, are attached to IAM Identities
    2) IAM Permissions
        - API actions that can or cannot be informed
        - Represented in the IAM policy document
    3) IAM Identities
        - IAM Users
        - IAM Groups
        - IAM Roles - associate policies to roles
    4) IAM Policy Anatomy



87. Principle-of-Least-Privilege (PoLP)
    - Is the computer security concept of providing a user, role, or application with the least amount of permissions to perform an operation or action
        1) Just-Enough-Access (JEA)
            - Permitting only exact actions for the identity to perform a task
        2) Just-In-Time (JIT)
            - Permitting the smallest length of duration an identity can use permissions

- 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 such as device, user, location, IP address
- AWS currently doesn't have Risk-based policies built in
- 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

88. AWS Account Root User
    1) AWS Account - account that holds all your resources
    2) AWS Account Root User - a special account with full access that cannot be deleted
    3) AWS Account User - for common tasks that is assigned permissions

    - AWS Account Root User
        1) Created at the time of AWS account creation
        2) Uses an Email and Password to log in
        3) Regular users need an Account ID/Alias, Username and Password
        4) Cannot be deleted
        5) Full permissions and not limited, cannot deny it resources however you can use AWS Organisation Service Control Policy to limit permissions for root user
        6) One root user per account
        7) Should not use it for daily and common tasks but for specific and specialised tasks that are infrequently or rarely performed
        8) Strongly recommended to never use Root User Acess Keys
        9) Strongly recommended to turn on MFA for the Root User

    - Roor User-only Tasks
        1) Change your account setting
        2) Restore IAM user permissions
        3) Activate IAM access to the Billing and Cost Management Console
        4) View certain tax invoices
        5) Change or cancel AWS Support Plan
        6) Register as a seller in Reserved Instance Marketplace
        7) Enable MFA Delete on an S3 Bucket
        8) Edit or delete an Amazon S3 Bucket policy that includes an invalid VPC ID or VPC endpoint ID
        9) Sign up for GovCloud
        10) Create the Organisation

89. AWS Single Sign-On (SSO)
    - Where you create or connect your workforce identities in AWS once and manage access centrally across your AWS organisation
    - Choose your identity source
        1) AWS SSO
        2) Active Directory

    3) SAML 2.0 IdP
- Managed User Permissions Centrally
    1) AWS Account
    2) AWS Applications
    3) SAML Applications
- Uses get Single Click Access

90. Application Integration (like a bridge between AWS services)
- Is the process of letting two independent applications communicate and work with each other, commonly facilitated by an intermediating systems
- Cloud workloads encourage systems and services to be loosely coupled and so AWS has many services for the specific purpose of an application integration
- Common systems or design patterns are:
    1) Queuing
    2) Streaming
    3) Pub/Sub
    4) API Gateways
    5) State Machine
    6) Event Bus

91. Queueing and SQS
- Is a messaging system that generally delta messages once they are consumed
- Simple communication, not real-time, have to pull, not reactive
- Messaging system to decouple processes via messages/events
- Simple Queueing Service (SQS) - queueing service that enables you to decouple and scale microservices, distributed systems and serverless applications to not hang up the site
- Uses case: queue up transactional emails to be sent, sign up, reset password

92. Streaming and Kinesis
- Multiple consumers can react to events
- Events live in the stream for long periods, so complex operations can be applied in real-time
- E.g Kinesis Data Streams is between EC2 Instances (Producers) and S3/DynamoDB/Redshift(Consumers)

93. Pub/Sub and SNS
- Publish-Subscribe pattern implemented in messaging systems
- The sender of messages (publishers) sends their message to an event bus
- The event bus categorises their messages into groups
- The receiver of messages (subscribers) subscribe to these groups
- Publishers do not know who their subscribers are
- Subscribers do not pull for messages

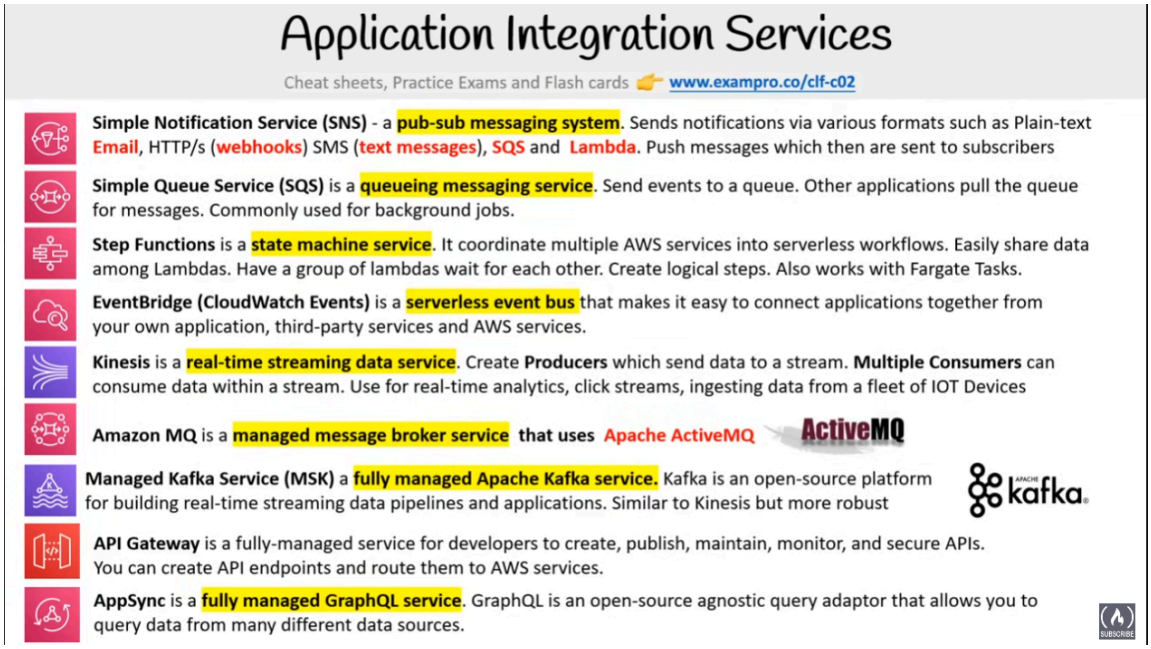
- Messages automatically and immediately pushed to subscribers
- Messages and events are interchangeable terms in pub/sub
- Use case: real-time chat system, web-hook system
- Simple Notification Service (SNS)
- Enables you to decouple microservices, distributed systems and serverless functions

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

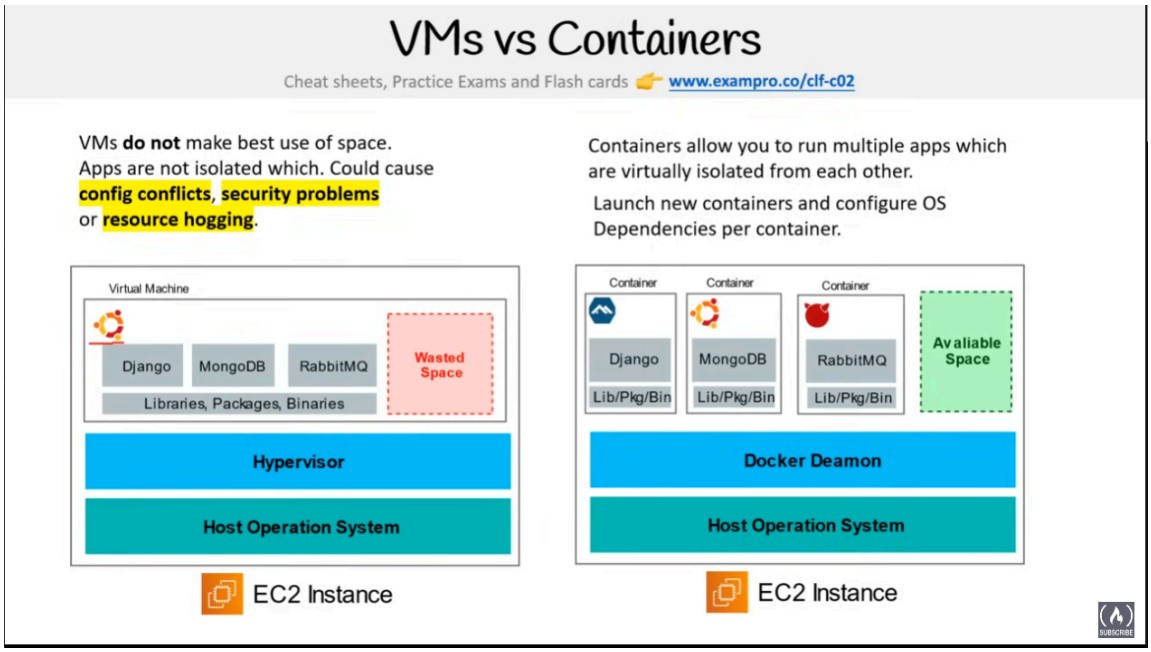
95. State Machines and AWS Step Functions
    - Decides how one state moves to another based on a series of conditions
    - Like a flow chart
    - AWS Step Functions
    - Coordinate multiple AWS Services into a serverless workflow
    - Graphical console to visualise the components of your application
    - Automatically triggers and tracks each step and retries when there are errors
    - Order is executed every time
    - Logs the state of each step so you can diagnose and debug

96. Event Bus and Amazon EventBridge
    - 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 application

97. API Services



98. VMs VS Containers
    - VMs do not make the best use of space
    - Apps are not isolated which could cause conflicts, security problems or resource hogging
    - Containers allow you to run multiple apps wich are virtually isolated from each other
    - Launch new containers and configure OS Dependencies per container



99. Microservices
- Monolithic Architecture: One App which is responsible for everything, functionality is tightly coupled
- Microservices Architecture: Multiple Apps which are each responsible for one thing, functionality is isolated and stateless
- AWS is basically engaging a Microservice Architecture

100. Kubernetes (K8)
- Open-source container orchestration system
- K8 over docker because it can run containers distributed across multiple VMs
- K8 has pods, pods are a group of containers
- Ideally for microservice architecture where a company has tens to hundreds of services

101. Docker
- PaaS products that use OS-level virtualisation to deliver software in packages called containers
- Docker CLI, Dockerfile, Docker Compose, Docker Swarm, Dockerhub
- Created Open Container Initiative (OCI)
- Losing out of favour due to their handling of introducing a paid open source and alternative like Podman growing

102. Podman, Buildah and Skopeo
- Container engine, drop-in replacement for Docker
- Daemon-less unlike Docker
- Allows you to create pods like K8
- Replaces one part of docker, Buildah and Skopeo fill in the other parts

103. Container Services

104. Organisations and Accounts

1. AWS Organisations
    - Allow the creation of new AWS accounts. Centrally manage billing, control access, compliance, security and share resources across your AWS accounts
    - Need to be turned on, once turned off cannot be turned on

1) Root Account User
    - Single sign-in identity that has complete access to all AWS services and resources in an account, there are root account users for each OU
2) Organisation Units (OU)
    - Group of AWS accounts within an organisation which can also contain other organisation units, creating a hierarchy
3) Service Control Policies (SCP)
    - Give central control over that allowed permissions for all accounts

105. AWS Control Tower

- Helps enterprises quickly set secure AWS multi-account
- Provides you with a baseline environment to get started with multi-account architecture

1) Landing Zone
    - Baseline environment following well-architectured
    - AWS SSO enable, Centralised Logging for AWS CloudTrail, cross-account security auditing
2) Account Factory
    - Configure

    - Enable self-service for your builder to configure and provision new accounts using the AWS Service Catalog
3) Guardrails
    - Pre-package governance rules for security, operation and compliance that customers can select and apply enterprise-wide or to specific groups of accounts

106. AWS Config
- Is a Compliance-as-Code framework that allows us to manage changes in your AWS accounts on a per-region basis, normally are lambda functions
- Change management in the context of the cloud is when we monitor, enforce and remediate changes
- When to use?
    1) I want this resource to stay configured in a specific way for compliance
    2) Keep track of configuration changes to resources
    3) List of all resources within a region
    4) Analyse potential security weaknesses needs detailed historical information

107. AWS Quick Starts
- Are prebuilt templates by AWS and AWS Partners to help deploy a wide range of stacks
- Reduce hundreds of manual procedures into just a few steps
- 3 Parts:
    1) Reference Architecture for the deployment
    2) AWS CloudFormation templates that automate and configure the deployment
    3) Deployment guide explaining the architecture and implementation in detail
- Fully functional Architecture can be set up in less than an hour

108. Tagging
- Key and value pair you can assign AWS resources
- Organise your resources
    1) Resource management
    2) Cost Management and Optimisation
    3) Operations Management
    4) Security
    5) Governance and Regulatory Compliance
    6) Automation
    7) Workload Optimisation

109. Resource Groups
- Collections of resources that share one or more tags
- Useful in using in IAM Policies

110. Business Centric Services

Business Centric Services

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c02

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 it 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 preform 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.

111. Provisioning Services

- Are responsible for setting up and then managing those AWS services

Provisioning Services

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c02

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 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 provisiong 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.

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

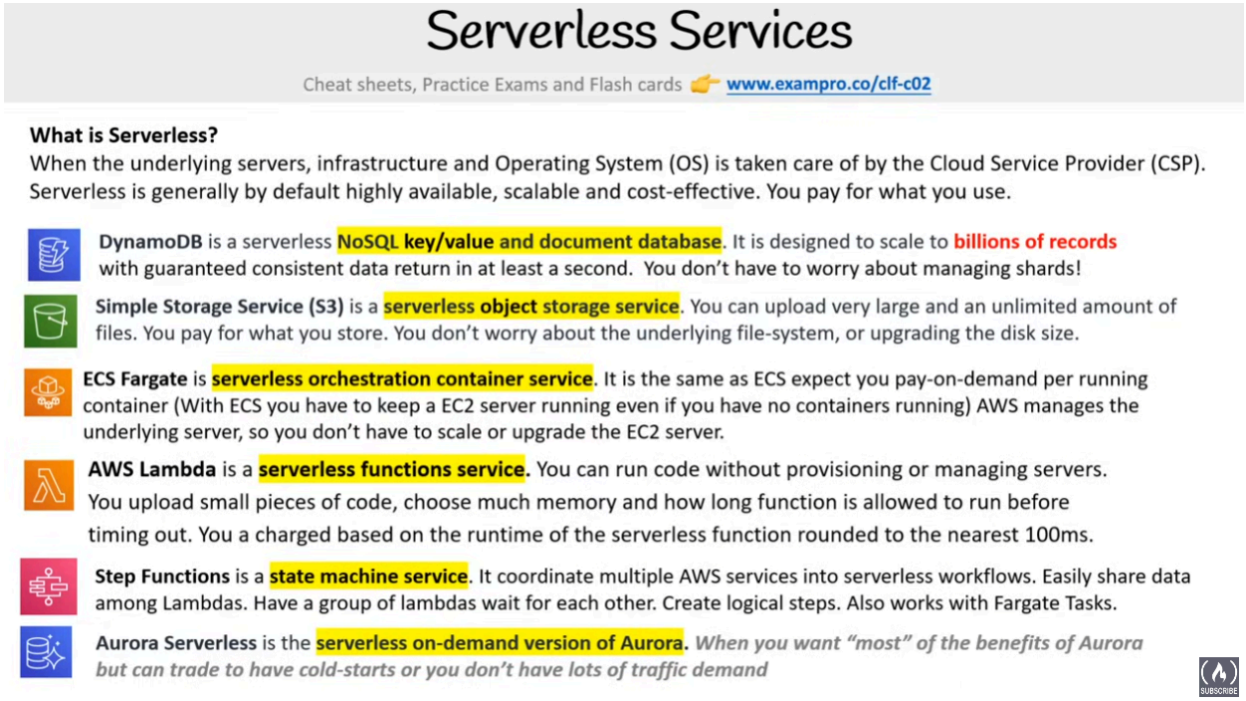
AWS Copilot
AWS Copilot is a command line interface (CLI) that enables customers to quickly launch and easily manage containerized applications on AWS.

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.

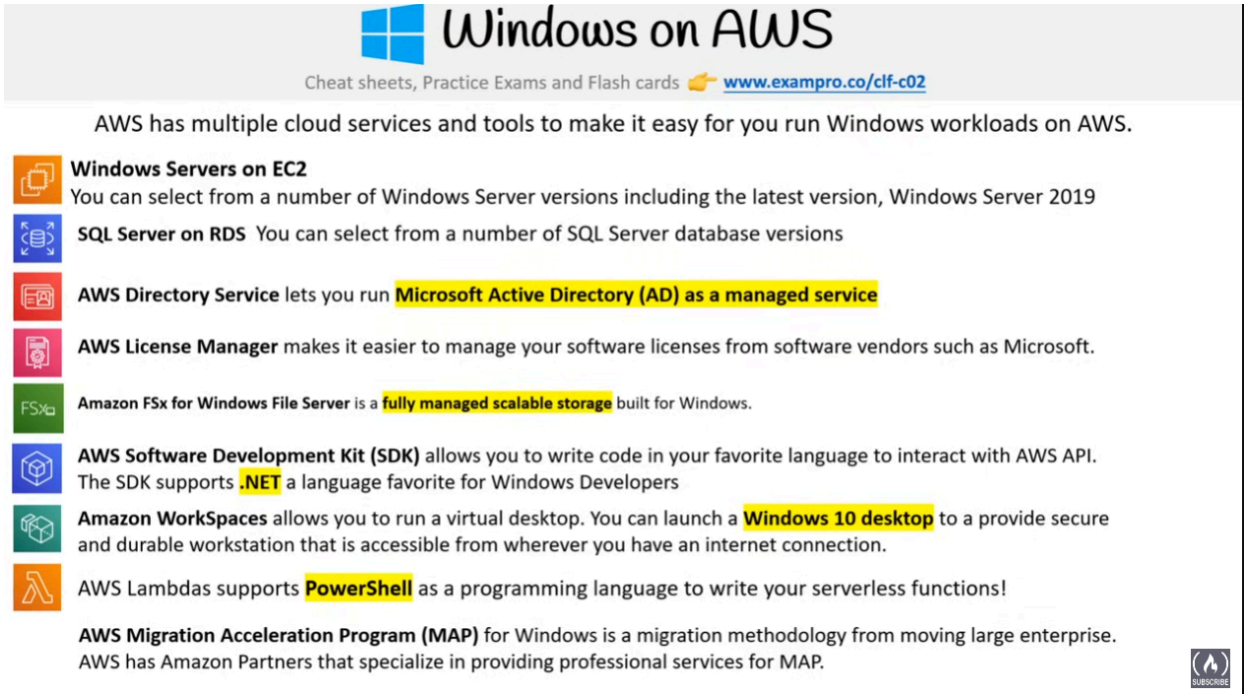
112. Serverless Services

- The underlying server, infrastructure and OS taken care of by the Cloud Service Provider



- What is serverless?
    1) Fully managed cloud services
    2) Answer on a scale where a cloud service has a degree of serverless
    3) Pay-for-Value (you don't pay for idle services)

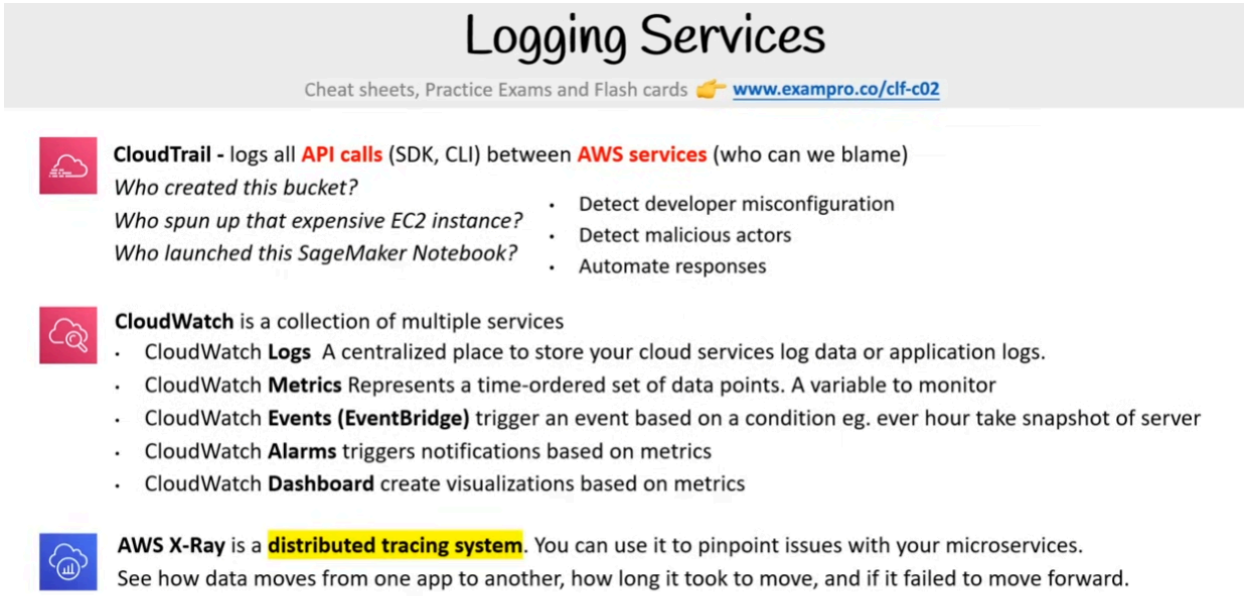
113. Windows on AWS



114. AWS License Manager

- Bring-Your-Own-License (BYOL) - reusing existing software licebses to run vendor software on a cloud vendor's computing service
- Allows companies to save money since they may have purchased the license in bulk or at a time that provided a greater discount then if purchased again
- 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-premise environments.
- For Microsoft Windows Server and Microsoft SQL Server License you need to use a Dedicated Host

115. Logging Services



116. AWS CloudTrail

1) Where - Source IP Address
2) When - EventTime
3) Who - User, UserAgent
4) What - Region, Resource, Action

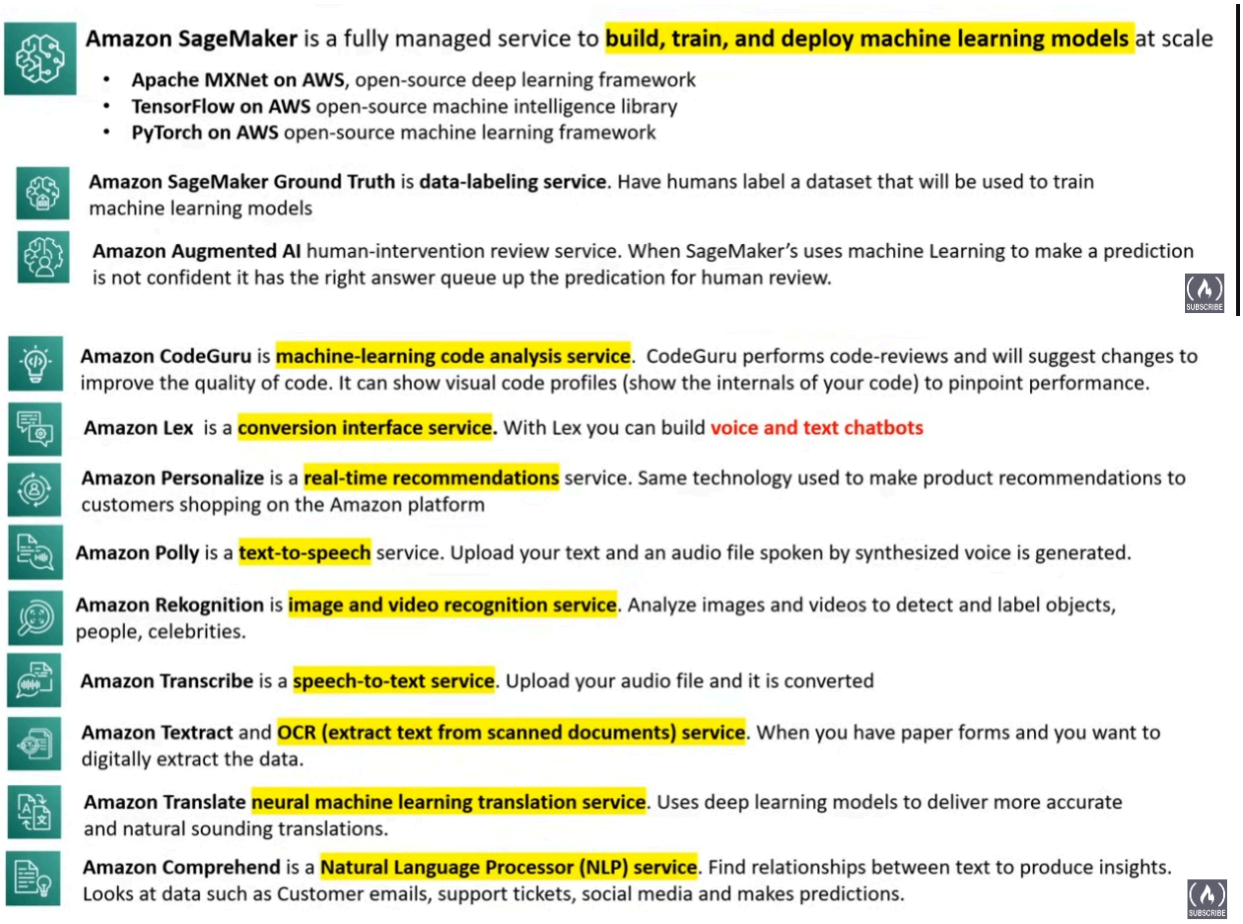
- Logging by default and will collect logs for last 90 days via Event History
- You need more than 90 days you need to create a Trail
- Trails are output to S3 and do not have GUI like Event History
- To analyse a Trail you'd have to use Amazon Athena

117. CloudWatch

- CloudWatch Alarms monitor CloudWatch Metrics based on a Defined Threshold
    1) OK = metric/expression is within the defined threshold
    2) ALARM = outside of the defined threshold
    3) INSUFFICIENT DATA = alarm just started / metric not available / not enough data
- CloudWatch Logs
    1) Log Streams
    2) Log Insights
- CloudWatch Metrics
    1) Time-ordered set of data points
    2) Variable monitored over time
    3) Eg EC2 Instance NetworkIn

118. Introduction to ML and AI Services

- Deep learning is a subset of Machine Learning
- Machine Learning is a subset of AI
- Amazon SageMaker - build, train and deploy machine learning models



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

EXTENDED

Amazon Bedrock
A **Large Language Model (LLM) cloud service offering to** generate text and image responses. ***Think like ChatGPT***

Amazon CodeWhisper
An AI code generator that will predict code to meet your usecase. Think like ***Github Copilot***

Amazon DevOps Guru
Uses ML to analyze your operational data and application metrics and events to detect operational abnormalities. Is there something wrong with our cloud operations?

Amazon Lookout for Equipment / Metrics / Vision
Uses ML models for quality control and performed automated inspections.

Amazon Monitron
Uses ML models to predict unplanned equipment downtime. Monitor has an IOT sensor that captures vibrations and sensor data

AWS Neuron
An SDK used to run deep learning workloads on AWS Inferentia and AWS Trainium based instance

119. Big Data and Analytics Services

- Massive volumes of structured / unstructured data that are too large to move and process using traditional data and software techniques

Big Data and Analytics Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/clf-c02

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

120. Amazon QuickSight

- Amazon's version of PowerBI
- Uses SPICE (super-fast, parallel, in-memory, calculation engine)
- QuickSightML Insights - detects anomalies, accurate forecasting, generates Natural Language Narratives
- QuickSight Q - asks questions using natural language on all your data and receives answers in seconds.

121.Generative AI

- Type of AI capable of generating new content such as text, images and videos

122. ML and DL Frameworks and Tools

- Machine learning and deep learning frameworks
- Used within SageMaker or have direct support

1) Apache MXNet
    - AWS adopted supports both imperative and symbolic
    - Gluon API: imperative programming
    - Module API: symbolic programming
2) PyTorch
    - optimised tensor library for deep learning using GPUs and CPU (by Facebook)
3) TensorFlow -
    - Low-level ML framework
    - Keras: high-level ML framework built on top and shipped with TensorFlow
4) Apache Spark
    - Unified analytics engine for large-scale data processing
    - SparkML: a uniform set of high-level APIs that help users create and tune practical machine learning pipelines
5) Chainer
    - Powerful, flexible and intuitive DL framework, supports CUDA
6) Hugging Face
    - An AI community of ML models and dataset

123. What is Intel

- The inventor of the x86 instruction set uses Assembly Language to program the chip
- There is another popular instruction set called ARM

1) Intel Xeon Scalable Processor
    - high-performance CPU, commonly used in EC2 instances, scalable = gd for ML
2) Intel Habana Gaudi
    - AI training processor developed by Habana Labs, acquired by Intel
    - Training deep learning models
    - Competitor to NVIDIA GPU

124. AWS Well-Architected Framework

- Whitepaper by AWS to help customers build best practices
- AWS Architectire Centre web-portal that contains best practice and reference archetcires
- 5 Sections called Pillars (Trade-off pillars based on business)
    1) Operational Excellence
        - Run and monitor systems
    2) Security
        - Protect data and systems, mitigate risk
    3) Reliability

    - Mitigate and recover from disruptions
4) Performance Efficiency
    - Use computing resources effectively
5) Cost Optimisation
    - Get the lowest price

The AWS Well-Architected Framework upholds six (6) general design principles. The following are:

– Stop guessing your capacity needs.

– Test systems at production scale.

– Automate to make architectural experimentation easier.

– Allow for evolutionary architectures.

– Drive architectures using data.

– Improve through game days.

125. Amazon Leadership Principles

- Set of principles used during the company decision-making, problem-solving, simple brainstorming and hiring

1) Customer Obsession
2) Ownership
3) Invent and Simplify
4) Are Right, A lot
5) Learn and Be Curious
6) Hire and Develop the Best
7) Insist on the Highest Standards
8) Think Big
9) Bias for Action
10) Frugality
11) Earn Trust
12) Dive Deep
13) Have Backbone, Disagree and Commit
14) Deliver Results
15) Strive to be Earth's Best Employer
16) Success and Scale Bring Broad Responsibility

126. Total Cost of Ownership (TCO)

- Financial estimate intended to help buyers and owners determine the direct and indirect costs of a product.

- Might help me when they want to migrate from on-premise to cloud
- AWS promises 75% savings based on their TCO calculator

127. Capital Expenditure (CAPEX) VS Operational Expenditure (OPEX)

1) CAPEX
    - Spending money upfront on physical infrastructure
    - Deducting that expense from your tax bill over time
    - Have to guess upfront what you plan to spend
2) OPEX
    - Cost from shifting on-premise datacentre to the service provider
    - A customer has to be only concerned with non-physical costs
    - You can try a product or service without investing in equipment

128. Does the cloud make IT personnel redundant?

- Bring over to Cloud
- Transition networking to Cloud Networking
- Hybrid approach traditional IT team and Cloud IT team
- Can change employees from Managing Infrastructure to revenue-gathering

129. AWS Pricing Calculator

- free cost estimate tool that can be used within a web browser
- No need AWS Account
- Calculate TCO
- Can export your final estimate to CSV

130. Migration Evaluator

- Formerly known as TCO Logic
- Estimate tool used to determine on-premise cost and compare it against AWS costs for planned cloud migration
- Used an Agentless Collector to collect data from your on-premise infrastructure

131. VM Import Export (Migration Tool)

- Import VMs images into EC2

1) Prepare your virtual image for upload
2) Upload it to S3
3) Use the AWS CLI to import your Image, it will generate an AMI

- Has instructions for:
- VMWare
- Citrix
- Microsoft Hyper-V
- Windows VHD from Azure

- Linux VHD from Azure

132. Database Migration Service
- Allows you to quickly and securely migrate one database to another
- Used to migrate your on-premise database to AWS
- AWS Schema Conversion Tool
- This tool is used in many cases to automatically convert a source database schema to the target database schema

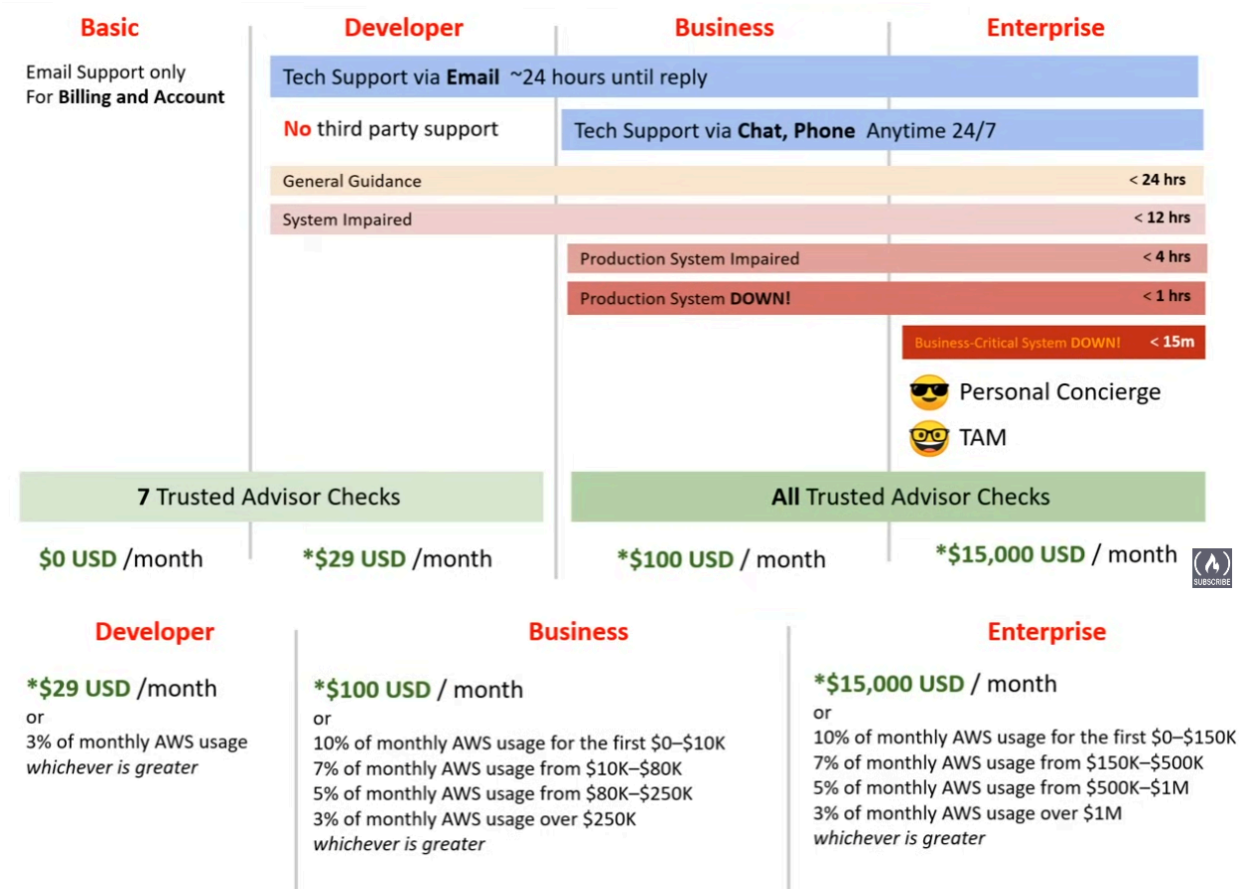
133. Cloud Adoption Framework (CAF)
- Whitepaper to help you plan migration from on-premise to AWS
- Six focus areas
    1) Business Perspective
        - How to update staff skills to optimise business value as they move ops to the cloud
    2) People Perspective
        - How to update skills to optimise and maintain workforce and ensure competencies
    3) Governance Perspective
        - How to update skills to optimise and ensure business governance in the cloud, manage and measure cloud investments
    4) Platform Perspective
        - How to update skills to deliver and optimise cloud solutions and services
    5) Security Perspective
        - Ensure the cloud aligns with the organisation’s security and compliance
    6) Operations Perspective
        - Ensure system health and reliability during the move and then to operate cloud computing best practices

PERSPECTIVE	PURPOSE	STAKEHOLDERS
BUSINESS	Helps ensure that your cloud investments accelerate your digital transformation ambitions and business outcomes	• CEO • COO • CTO • CFO • CIO
PEOPLE	Serves as a bridge between technology & business, accelerating the cloud journey to help organizations more rapidly evolve to a culture of continuous growth, learning, & where change becomes business-as-normal, with focus on culture, organizational structure, leadership &workforce	• CTO • Cloud Directors • COO • Cross-functional Leaders • CIO • Enterprise-wide Leaders
GOVERNANCE	Helps you orchestrate your cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks	• CIO • CFO • CRO • CTO • CDO
PLATFORM	Helps you build an enterprise-grade, scalable, hybrid cloud platform; modernize existing workloads; and implement new cloudnative solutions	• Technology leaders • CTO • Architects • Engineers
SECURITY	Helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads.	• Internal Audit Leaders • CISO • Security Architects • CCO • Engineers
OPERATIONS	Helps ensure that your cloud services are delivered at a level that meets the needs of your business.	• Infrastructure & Operations Leaders • Site Reliability Engineers • IT Service Managers

AWS Cloud Adoption Framework (AWS CAF)

134. AWS Free Services
    - Free forever
    - Free-tier is free up to the point of usage of time

135. AWS Support Plans



136. Technical Account Manager (TAM)
- Proactive guidance and reactive support
- Help and save money
- Reviews and work together with others, collaborate
- Follows Amazon Leadership Principles
- Only for Enterprise Support Tiers

137. AWS Marketplace
- Products can be free or come at a charge
- Sales channel for ISVs and Consulting Partners allows you to sell your solutions to other AWS customers
- Can be AMIs, CloudFormation Templates, Saas offerings, Web ACL, AWS WAF rules

138. Consolidated Billing
- Pay for multiple AWS accounts in an organisation in one bill
- Cost explorer to visualise usage for consolidated billing
- Offered at no additional costs
- Volume Discounts
- The more you use, the more you save

139. AWS Trusted Advisor

- Recommendation tool which automatically and actively monitors your AWS Account to provide actional recommendations
- Like an Automated checklist of Best Practices on AWS
- Different levels based on support plan (The trusted Advisor Checks - 7 vs All)

140. Service Level Agreements

- Formal commitment about the expected level of service between customer and provider
- When the level is not met and the customer meets the obligation under SLA, customer will be eligible to receive the compensation eg financial and Service Credits

1) Service Level Indicator (SLI)
    - SLI is a metric/measurement is a measure of performance a customer is receiving at a given time
2) Service Level Objective (SLO)
    - An objective that the provider has agreed to meet, in the form of a target percentage over some time

141. AWS Abuse

- AWS Trust & Safety is a team that deals with abuses, go to them not AWS Support for these issues:
    1) Spam
    2) Port Scanning
    3) Denial-of-service (Dos) attacks
    4) Intrusion attempts
    5) Hosting prohibited content
    6) Distributing malware

142. AWS Free-Tier

- First 12 months of signup or free usage up to a certain monthly limit forever

143. AWS Partner Network (APN)

- Global partner program for AWS
- Joining it will open your organisation up to business opportunities and allow exclusive and marketing events
- When you join APN you can either be:
    1) Consulting Partner - help companies utilise AWS
    2) Technology Partner - build technology on top of AWS as a service offering
- Tiers: Select, Advanced or Premier
- Require AWS Certification and AWS APN-Exclusive Certifications

144. AWS Budgets
- Gives you the ability to set alerts if you exceed or are approaching your defined budget
- The first 2 budgets are free of charge
- Each budget is $0.02/day
- AWS Budget Reports
    1) Monitor the performance
    2) Emailed specific emails
    3) More convenient as can be seen through emails instead logging into AWS every time

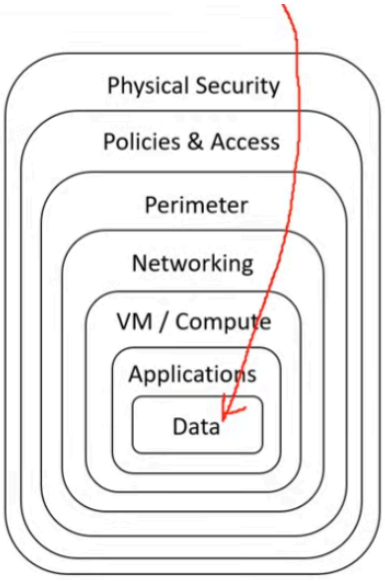
145. AWS Cost and Usage Reports (CUR)
- Detailed spreadsheet, enabling you to better analyse and understand your AWS costs
- Place report into S3
- Use Athena to turn the report into a queryable database
- Use QuickSight to visualise your billing data as graphs
- Will contain cost allocation tags, optional metadata attached to AWS resources

146. Billing Alerts / Alarms CloudWatch
- Have to turn on billing alerts
- Go CloudWatch
- More flexible than aws budget and ideal for complex case

147. AWS Cost Explorer
- Lets you visualise, understand and manage your AWS costs and usage over time
- Shows up in us-east-1

148. AWS Pricing API
- Programmatically access the latest price offering
- Two versions of this API
    1) Query API
        - Pricing service API via JSON
    2) Batch API
        - Price List API via HTML

149. Defence in Depth
- 7 Layers of Security



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.

150. Confidentiality, Integrity, Availability (CIA) Triad
- Foundation to security principles and their trade-off relationship

151. Encryption
- Process of encoding information using a key and a cypher (synonymous to code) to store sensitive data in an unintelligible format as a means of protection.
- Encryption tackles plaintext and produces ciphertext (a result of encryption performed on plaintext)
- Cryptographic Keys
    1) Advanced Encryption Standard (AES)
        - Symmetric encryption, the same key used for encoding and decoding
    2) Rivest-Shamir-Adleman (RSA)
        - Asymmetric Encryption, one for encoding and another for decoding
    3) Transport Layer Security (TLS)
        - For data integrity between two or more communicating computer applications
    4) Secure Sockets Layers (SSL)
        - Same as TLS

152. Hashing and Salting
- Hashing
- One-way process and deterministic always returns the same output for the same input
- Used to store passwords in the database so that passwords do not reside in a plaintext format
- Popular Hashing Functions: MD5, SHA256 and Bcrypt

- Salting Passwords, random strings not known to the attacker the hash function accepts to mitigate the deterministic nature of hashing functions

153. Digital Signatures and Signing
- Mathematical scheme for verifying the authenticity of digital messages or documents
- 3 algorithms:
    1) Key Generation - generates a public and private key
    2) Signing - a process of generating a digital signature with a private key and inputted message
    3) Signing Verification - verify the authenticity of the message with a public key
- Code Signing, when you use a digital signature to ensure computer code has not been tampered with

154. In-Transit vs At-Rest Encryption
- Encryption In-Transit
    1) Data is secure when moving between secure locations
    2) Algorithms: TLS, SSL
- Encryption At- Rest:
    1) Data is secure when residing in storage or within a database
    2) Algorithms: AES, RSA

155. Compliance Programs
- AWS lists out the ones that they are compliant with on their with
- AWS Artifacts, a self-serve portal for on-demand access to AWS compliance re[oprts

156. Penetration Testing (PenTesting)
- Authorised simulated cyberattack on a computer system, performed to evaluate the security of the system
- Allowed to be performed on AWS but with limitations

157. AWS Inspector
- Runs a security benchmark against specific EC2 instances
- Run a variety of security benchmarks
- Can perform both network and host assessments

158. Distributed Denial of Service (DDoS) - AWS Shield
- Malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic
- Built-in protection using AWS Shield
- AWS Shield - managed DDoS protection service that safeguards applications running on AWS
- When you route traffic through Route53 or CloudFront, you are using AWS Shield

1) Shield Standard FREE

2) Shield Advanced USD 3000 / Year
3) Both plans integrate with AWS Web Application Firewall (WAF) to give you Layer 7 application protection

159. AWS Guard Duty
- Intrusion Detection System / Intrusion Protection System (IDS/IPS)
- Threat detection service
- Uses ML to analyse:
    1) CloudTrail Logs
    2) VPC Flow Logs
    3) DNS Logs

160. Amazon Macie
- Continuously monitors S3 Data Access activity for anomalies
- Uses ML to analyse your CloudTrail Logs

161. AWS VPN
- Lets you establish a secure and private tunnel
- Internet Protocol Security (IPsec)

1) Site-to-site VPN (on-premises to VPC)
2) AWS Client VPN (users to AWS/on-premises)

162. AWS WAF
- Protect your web applications from common web exploits
- Write your own rules to allow or deny traffic
- Ruleset from a trusted AWS Security Partner in the AWS WAF Marketplace
- Can be attached to either CloudFront or an Application Load Balancer

163. Hardware Security Module (HSM)
- Hardware designed to store encryption keys
- Hold keys in memory and never write them to disk
- Multi-tenant HSM is FIPS 140-2 Level 2 Compliant (AWS KMS)
- Single-tenant HSM is FIPS 140-2 Level 3 Compliant (AWS CloudHSM)

164 AWS KMS
- Create and control the encryption keys used to encrypt your data
- Multi-tenant HSM
- Uses Envelop encryption - primary keys encrypt your data, master key unlocks your primary key

165. AWS CloudHSM
- Single-tenant HSM
- Built on Open HSM industry standard

- Can also transfer keys to other commercial HSM solutions to make migration easier

167. Know Your Initialisms

168. AWS Config vs AWS AppConfig

AWS Config

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

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

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

AWS AppConfig

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

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

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

169. SNS vs SQS

The Both **Connect Apps** via Messages

Simple Notifications Service

Pass Alongs Messages eg. PubSub

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

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

Can retry sending in case of failure for **HTTP**S

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

Simple Queue Service

Queue Up Messages, Guaranteed Delivery

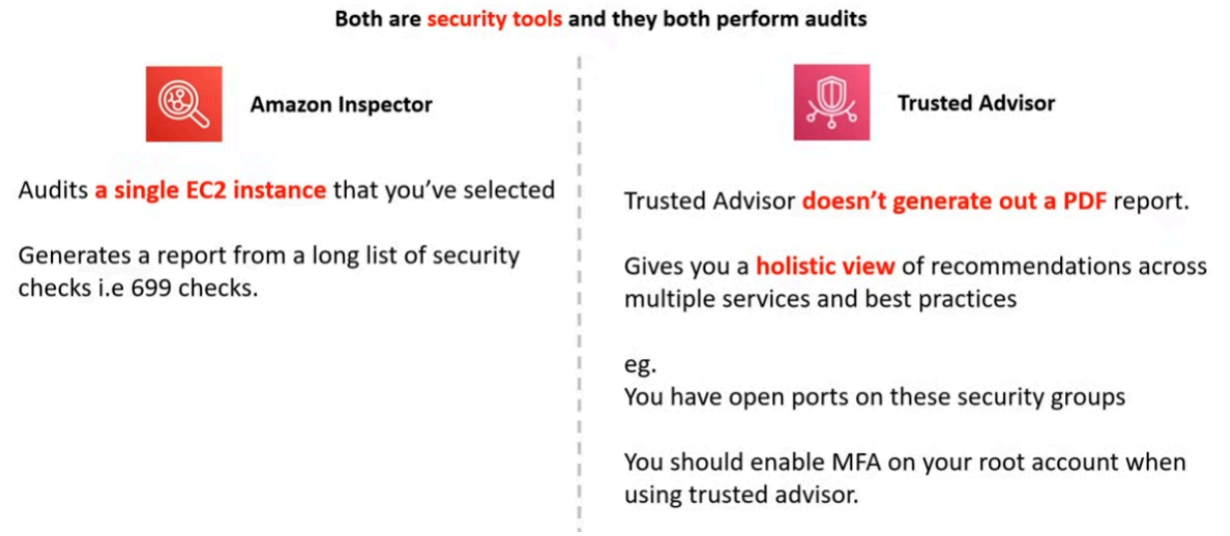
Places messages into a **queue.** Applications pull queue using **AWS SDK**

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

Really good for delayed tasks, queueing up emails

170. SNS vs SES vs PinPoint vs Workmail

171. Amazon Inspector vs AWS Trusted Advisor

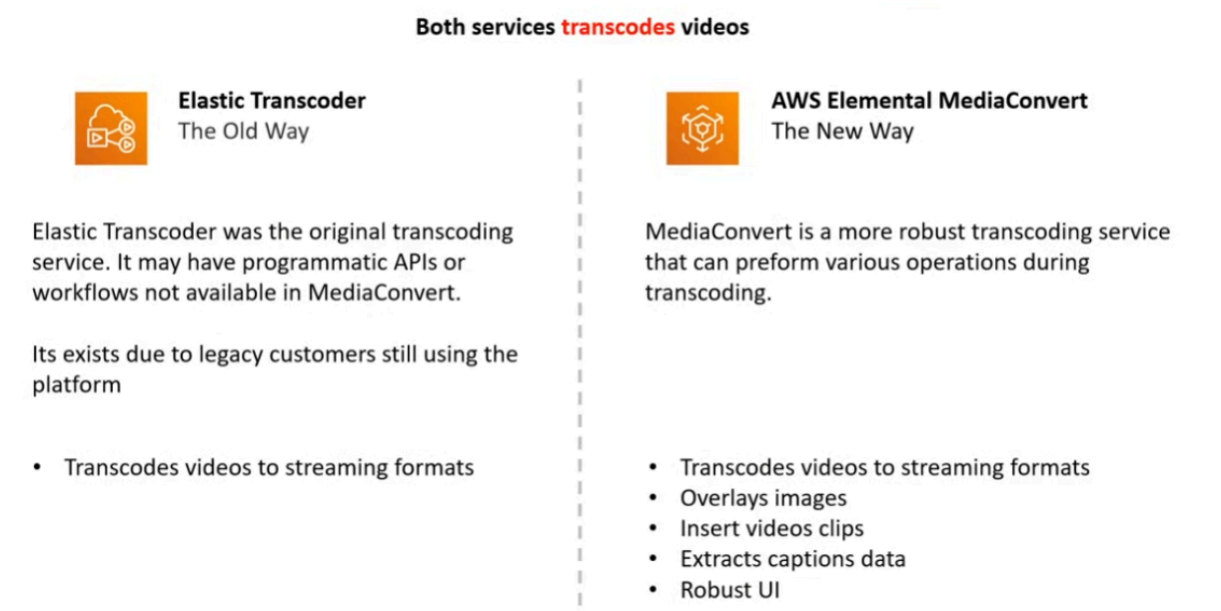


172. Connect Names Services

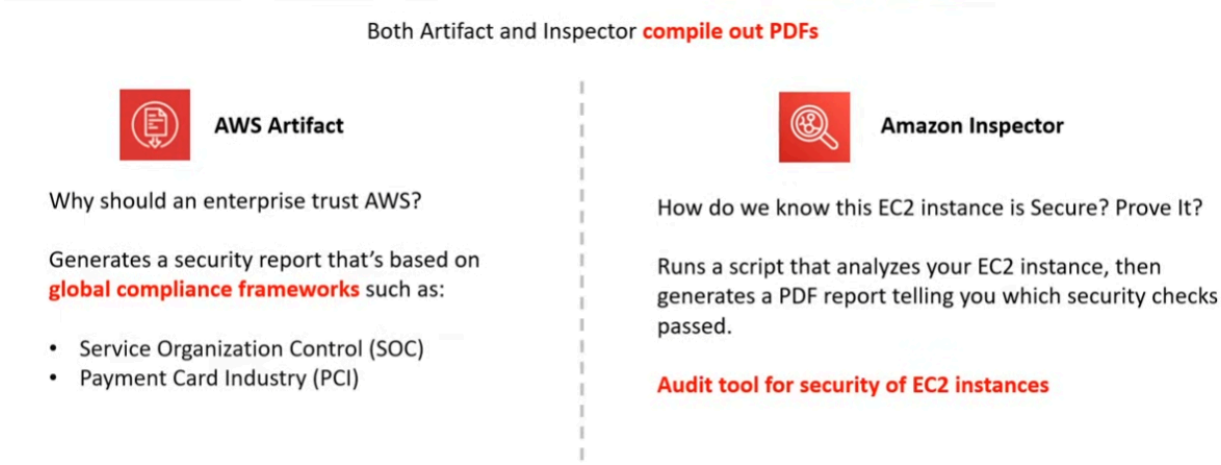
1) Direct Connect
    - Dedicated fibre optics connection from your data centre to AWS
    - Intended for large enterprises with their own data centre and they need fast and private connection
    - For a secure connection, on AWS VPN on top of it
2) Amazon Connect
    - Call centre as a service
    - Toll-free number, set automated phone systems
    - Interactive Voice System (IVS)

3) Media Connect
   - A new version of elastic Transcoder, Converts Videos to Different Video Types

173. Elastic Transcoder vs MediaConvert



174. AWS Artifacts vs Amazon Inspector



175. ELB vs ALB vs NLB vs GWLB vs CLB

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

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

Can attach an AWS WAF

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

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

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

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

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

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