

## AWS CCP Training 2020 (YT) Notes

[ORIGINAL SOURCE](#) - Credit Andrew Brown

### What is Cloud Computing

- Cloud Computing - the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than on a local server or personal computer
  - Traditional Approach (On-premise)
    - You own the servers
    - You hire the IT people
    - You pay or rent the real-estate
    - You take all of the risk
  - Cloud Providers
    - Someone else owns the servers
    - Someone else hires the IT people
    - Someone else pays or rents the real-estate
    - You are responsible for configured cloud services and code, and someone else takes care of the rest
- 6 Advantages of Cloud Computing
  - Trade capital expense for variable expense
    - No upfront cost
      - Instead of paying for data centers and servers
    - Pay on-demand
      - Pay only when you consume computing resources
  - Benefit from massive economies of scale
    - Usage from hundreds of thousands of customers aggregated in the cloud
    - You are **sharing the cost** with other customers to save money
  - Stop Guessing Capacity
    - Eliminate guesswork about infrastructure capacity needs
    - Instead of paying for idle or under-utilized servers, scale up and down to meet requirements
  - Increase Speed and Agility
    - Launch resources within a few clicks in minutes instead of days or weeks on site
  - Stop spending money on running and maintaining data centers
    - Focus on your own customers, rather than racking, stacking, and powering servers
  - Go global in minutes
    - Deploy your app in **multiple regions around the world** immediately
    - Provide lower latency and a better experience for your customers at minimal cost

## Types of Cloud Computing

- SaaS - a complete product that is run and managed by the service provider (Salesforce, Gmail, Office 365)
  - You don't have to worry about how the service is maintained, it just works and remains available
- PaaS (Platform as a Service) - Removes the need to manage the underlying infrastructure and allows you to focus on deployment and managing your applications
  - Don't worry about provisioning, configuring, or understanding the hardware or OS
  - Heroku, AWS Elastic Beanstalk, Engines for Google
- IaaS (Infrastructure as a Service) - the basic building blocks for cloud IT. Provides access to networking features, computers, and data storage space
  - Don't worry about IT staff, data centers, or hardware

## Cloud Computing Deployment Models

- Cloud - fully utilizing cloud computing
  - Squarespace, Basecamp, Dropbox
  - Good for startups, SaaS offerings, new projects and companies
- Hybrid - using both Cloud and On-Premise
  - Good for banks, Fintech, Large Professional Service providers, Legacy on-premise (sensitive data)
- On-Premise - deploying resources on-premises, using virtualization and resource management tools, sometimes called "private cloud"
  - Good for public sector (government), sensitive data (hospitals), large enterprises with heavy regulation (insurance companies)

## AWS Global Infrastructure

- 69 Availability Zones (with many more Edge locations than AZs)
  - AZs are one or more discrete data centers
- 22 Geographic Regions
  - Regions are a physical location in the world with multiple AZs
- Serves over a million active customers in more than 190 countries
- AWS is expanding global infrastructure to help customers achieve lower latency and higher **throughput**
- **Edge Location** is a datacenter owned by a trusted AWS partner

## Regions

- A **geographically distinct** location with multiple AZs (data centers)
  - Every region is **physically isolated** from and independent of every other region in terms of location, power, and water supply

- Each region has **at least 2 AZs**
- New services almost always become available in the US-EAST first
- Not all services are available in all regions
- US-EAST-1 is the region where you see all of the billing information
- Most companies have to operate in at least 3 AZs
  - Amazon is working on this

## AZs

- An AZ is a datacenter owned and operated by AWS
- Each region has at least 2 AZs
- AZs are represented by a Region Code, followed by a letter identifier
  - Ex. us-east-1a
- Multi-AZ Distributing spreads your instances across multiple AZs, and allows failover configuration for handling requests when one instance goes down
- **There is less than 10ms latency between AZs**

## Edge Locations (EL)

- Used for getting or uploading data fast to AWS
- EL is a datacenter owned by a trusted partner of AWS and has a **direct connection** to the AWS network
- These locations serve requests for **CloudFront** and **Route53**
  - Requests going to either of these services will be routed to the nearest EL automatically
- **S3 Transfer Acceleration** traffic and **API Gateway** endpoint traffic also use the AWS Edge Network
- ELs allow for low latency, no matter where the end user is geographically located

## GovCloud Regions (GCR)

- AWS GovCloud Regions allow customers to host sensitive Controlled Unclassified Information and other types of regulated workloads
- GCRs are only operated by employees who are US citizens on US soil
- GCRs are **only** accessible to US entities and root account holders who pass a screening process
- Customers can architect secure cloud solutions that comply with
  - FedRAMP High baseline
  - DOJ Criminal Justice Information Systems (CJIS) Security Policy
  - US International Traffic in Arms Regulation (ITAR)
  - Export Administration Regulations (EAR)
  - Department of Defense Cloud Computing Security Requirements Guide

## PowerUsers

- Provides full access to AWS services and resources, but does not allow the user to manage other Users and groups

### When Creating a New Instance

- Add permissions through IAM Management Console
  - AmazonEC2RoleforSSM
  - Simple Systems Manager (SSM)
- You can STOP an instance to save money (not the same as terminating)

### Sessions Manager

- Under SSM in AWS
- Advantage: it logs every time someone creates a session

### Amazon Machine Image (AMI)

- Snapshot or copy of the entire server
- In EC2 > Instances, do Actions > Image > Create Image
- Once we have an AMI, we can launch another copy of this server/instance

### CloudFront

- Used as a CDN (content distribution network)
- Can share static files across the globe by copying them to multiple edge locations across the world and will be accessible from those ELs
- Traffic will hit the domain name, and then it will route the traffic to the nearest EL

### Relational Database Service (RDS)

- Amazon Aurora is one of the most-expensive options
- Has 3 templates
  - Production
  - Dev/Test
  - Free tier
- If you do not specify the initial database name, the db is not created
- Turn backup retention period to 0 days
- Turn off performance insights

### Lambda

- Create a function in the preferred language
- With Lambda, you don't have to worry about servers, you just have to run your code
- Has integration with third-party Amazon partners

### EC2 Pricing Model

- On-Demand
- Spot
- Reserved
- Dedicated

### On-Demand Pricing (LEAST COMMITMENT)

- When you launch an EC2 instance, it is by default using On-Demand
- On-Demand has **no upfront payment and no long-term contract**
- You are charged by the **hour** or by the **minute** (varies based on EC2 Instance Types)
- On-Demand is for applications where the workload is short-term, spiky, or unpredictable
  - When you have a new app for development or you want to run an experiment

### (RI) Reserved Instances (BEST LONG-TERM)

- Best long term savings
- Reserved Instances can be shared between multiple accounts within an organization
  - Unused Reserved instances can be sold in the **Reserved Instance Marketplace**
- Designed for applications that have a steady-state, predictable usage, or require reserved capacity
- Reduced pricing is based on **Term x Class Offering x Payment Option**
- **Terms**
  - You commit to a 1 or 3 year contract
    - The longer the contract, the more savings
- **Payment Options (greater upfront, greater savings)**
  - All upfront
  - Partial upfront
  - No upfront
    - Good way to save money
- **Class Offerings**
  - Standard - up to 75% reduced pricing compared to on-demand
    - Cannot change RI Attributes (ex. cannot change the number of instances)
  - Convertible - up to 54% reduced pricing compare to on-demand
    - Allows you to change RI Attributes if greater or equal in value
  - Scheduled - reserve instances for specific time periods, e.g. once a week for a few hours
    - Savings vary

### Spot Instances (BIGGEST SAVINGS)

- Designed for applications that have flexible start and end times or applications that are only feasible at very low compute costs
- **AWS Batch is an easy way to use Spot Pricing**
- AWS has unused compute capacity that they want to maximize the utility of for their idle servers
  - Similar to when a hotel offers discounts to fill vacant rooms
- Spot instances provide a **discount of 90%** as compared to On-Demand Pricing
- Spot Instances can be terminated if the computing capacity is needed by on-demand customers

- **Termination Conditions**
  - Instances can be terminated by AWS **at anytime**
  - If your instance is terminated by AWS, **you don't get charged for a partial hour of usage**
  - **If you terminate**, you will still be charged for any hours in which it ran

### Dedicated Host Instances (MOST EXPENSIVE)

- Designed to meet regulatory requirements when you have strict server-bound licensing that won't support multi-tenancy or cloud deployments
- Offered in both **On-Demand** and **Reserved (70% off On-Demand Pricing)**
- Enterprises and large orgs may have security concerns or obligations about sharing the same hardware with other AWS customers

### Multi-Tenant vs Single Tenant

- Multi Tenant
  - When multiple customers are running workloads on the same hardware. **Virtual Isolation** is what separates customers
- Single Tenant
  - When a single customer has dedicated hardware. **Physical Location** is what separates customers



## EC2 Pricing - *CheatSheet*

---

- EC2 has four pricing models: **On-Demand**, **Spot**, **Reserved Instances (RI)**, and **Dedicated**
- **On-Demand** (least commitment)
  - low cost and flexible
  - only pay per hour
  - **Use case:** short-term, spiky, unpredictable workloads, first-time apps
  - Ideal when your workloads cannot be interrupted
- **Reserved Instances** up to 75% off (Best long-term value)
  - **Use case:** steady state or predictable usage
  - Can resell unused reserved instances (Reserved Instance Marketplace)
  - Reduced Pricing is based on **Term x Class Offering x Payment Option**
  - **Payment Terms:** 1 year or 3 year
  - **Payment Options:** All Upfront, Partial Upfront, and No Upfront
  - **Class Offerings**
    - **Standard** Up to 75% reduced pricing compared to on-demand. Cannot change RI Attributes.
    - **Convertible** Up to 54% reduced pricing compared to on-demand. Allows you to change RI Attributes if greater or equal in value.
    - **Scheduled** You reserve instances for specific time periods e.g. once a week for a few hours. Savings vary



## EC2 Pricing - *CheatSheet*

- **Spot Pricing** upto 90% off (Biggest Savings)
  - request spare computing capacity
  - flexible start and end times
  - **Use case:** Can handle interruptions (server randomly stopping and starting)
  - **Use case:** For non-critical background jobs
  - Instances can be terminated by AWS **at anytime**
  - If your instance is **terminated by AWS**, **you don't get charged** for a partial hour of usage.
  - If you **terminate** an instance **you will still be charged** for any hour that it ran.
- **Dedicated Hosting** (Most Expensive)
  - Dedicated servers
  - Can be on-demand or reserved (upto 70% off)
  - **Use case:** When you need a guarantee of isolate hardware (enterprise requirements)

### Billing and Pricing - Free Services

- The following services are free, but **can provision AWS services that DO cost money**
  - The resources they setup will cost you
- Examples (in bold are ones to focus on)
  - **IAM**
  - **Amazon VPC**
  - **Auto Scaling**
  - **CloudFormation**
    - The service itself is free, but it can provision other services
  - **Elastic Beanstalk**
  - Opsworks
  - Amplify
  - AppSync
  - CodeStar
  - Organizations and Consolidated Billing
  - AWS Cost Explorer

### Billing and Pricing - AWS Support Plans

- Four Support Plans
  - Basic (default)
    - Email support only for billing and account management
    - NO third-party support (Express, Django, Node, etc.)
  - Developer
    - \$20/month
  - Business
    - \$100/month

- Enterprise
  - \$15,000/month
  - Personal Concierge
  - Personal Technical Account Manager (TAM)
  - Respond in less than 15 mins for critical issues
- \*\*Advisor Checks

#### For Exam

- Know difference in pricing for different tiers
- Know response times
- Know when people are assigned to your account (only in enterprise)
- Know when third-party support is available in each tier (business and enterprise)

AWS Support Plans			
Basic	Developer	Business	Enterprise
Email Support only For Billing and Account	Tech Support via Email ~24 hours until reply  No third party support	Tech Support via Chat, Phone Anytime 24/7  General Guidance < 24 hrs System Impaired < 12 hrs	Production System Impaired < 4 hrs Production System DOWN! < 1 hrs  Business-Critical System DOWN! < 15m  Personal Concierge TAM
7 Trusted Advisor Checks		All Trusted Advisor Checks	
\$0 USD /month	\$20 USD /month	\$100 USD / month	\$15,000 USD / month <small>()</small>

#### Billing and Pricing - AWS Marketplace

- AWS Marketplace is a curated digital catalog with thousands of software listings from independent software vendors
- Easy to find, buy, test, and deploy software that already runs on AWS
- The product can be **free**, or have an **associated charge**
  - The charge is added to the AWS bill, and, once you pay, AWS Marketplace pays the provider
- The sales channel for ISVs (independent software vendors) and Consulting Partners **allows you to sell your solutions** to other AWS customers
- Products can be offered as
  - AMIs

- AWS CloudFormation templates
- SaaS offerings
- Web ACL
- AWS WAF rules

## Billing and Pricing - AWS Trusted Advisor

- Advises you on security, **saving money**, performance, service limits, and fault tolerance
- Think of it like an automated checklist of best practices on AWS
- Free Tier gets 7 Trusted Advisor Checks
- Business/Enterprise - All Trusted Advisor Checks

The screenshot shows the AWS Trusted Advisor interface. At the top right is the title "AWS Trusted Advisor" next to a purple shield icon. Below the title are two columns of service categories and specific checks:

 Cost Optimization	 Security
Amazon EC2 Reserved Instances Optimization	AWS CloudTrail Logging
Low Utilization Amazon EC2 Instances	IAM Password Policy
Underutilized Amazon EBS Volumes	<b>MFA on Root Account</b>
Amazon EC2 Reserved Instance Lease Expiration	Security Groups - Specific Ports Unrestricted
Amazon RDS Idle DB Instances	Security Groups - Unrestricted Access
Amazon Route 53 Latency Resource Record Sets	Amazon S3 Bucket Permissions
<b>Idle Load Balancers</b>	<b>IAM Access Key Rotation</b>
<b>Unassociated Elastic IP Addresses</b>	Amazon EBS Public Snapshots
Underutilized Amazon Redshift Clusters	Amazon RDS Public Snapshots
 	Amazon RDS Security Group Access Risk
 Performance	Amazon Route 53 MX Resource Record Sets and Sender Policy Framework
CloudFront Alternate Domain Names	CloudFront Custom SSL Certificates in the IAM Certificate Store
Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration	CloudFront SSL Certificate on the Origin Server
Amazon EC2 to EBS Throughput Optimization	ELB Listener Security
Amazon Route 53 Alias Resource Record Sets	ELB Security Groups
CloudFront Content Delivery Optimization	Exposed Access Keys
CloudFront Header Forwarding and Cache Hit Ratio	IAM Use
<b>High Utilization Amazon EC2 Instances</b>	
Large Number of EC2 Security Group Rules Applied to an Instance	
Large Number of Rules in an EC2 Security Group	
Overutilized Amazon EBS Magnetic Volumes	

In the bottom right corner of the interface is a small "SUBSCRIBE" button with a gear icon.

## Cost Optimization Advisor Checks

- **Idle Load Balancers**
  - Will give you feedback on when Load Balancers are not being used (no instances)
- **Unassociated Elastic IP Addresses**
  - If you have an instance with a static IP, you can reserve an IP through AWS (which costs money)
  - If it is not attached to an EC2 instance, it costs money (because AWS wants to release the IP to be used by other customers potentially)

## Performance

- High Utilization EC2 Instances

- Advises on upgrading to bigger instances if CPU usage is high to get better performance

## Security

- MFA on Root Account
- IAM Access Key Rotation
  - Advises to rotate access keys to keep the instances secure

The screenshot shows the AWS Trusted Advisor interface. At the top right, there is a shield icon and the text "AWS Trusted Advisor". Below this, there are two main sections: "Fault Tolerance" and "Service Limits".

**Fault Tolerance:**

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

**Service Limits:**

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

## Fault Tolerance

- Amazon RDS Backups
  - Recommends that you have backups in place or turned on in case db goes down

## Service Limits

- If you go beyond the capacity of a service, you will have to ask for a Service Limit Increase
  - Ex. SES Daily Sending Quota for emails
    - If you send more than 5,000 allotted emails per day, you will have to increase the Service Limit

## Billing and Pricing - Consolidated Billing

- Allows for **one bill** for all of your accounts
  - AWS treats all accounts in an organization as if they were one account
  - Happens by default for the master account

- You can designate the **Master account** in charge of paying for all member accounts under it
- Offered at no additional cost
- Use **Cost Explorer** to visualize usage for consolidated billing
- \*Note: if you have a member account that leaves the organization, the Cost Explorer data will no longer be available

### Consolidated Billing Volume Discounts

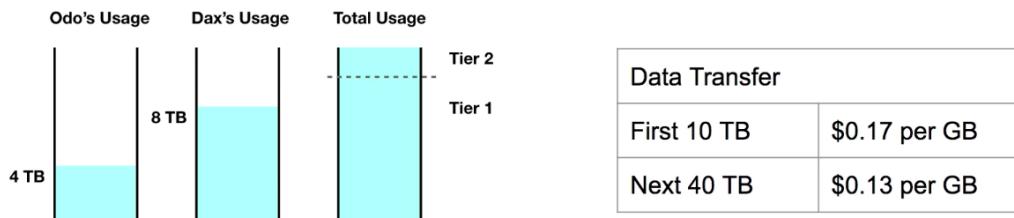
- The more you use, the more you save
- Consolidated Billing lets you take advantage of Volume Discounts

## Consolidated Billing – Volume Discounts

AWS has **Volume Discounts** for many services

The more you use, the more you save.

Consolidated Billing lets you take advantage of Volume Discounts



Odo	$(4 \times 1024) \times 0.17$	= \$696.32
Dax	$(8 \times 1024) \times 0.17$	= \$1392.64
<b>Unconsolidated</b>	$696.32 + 1392.64$	<b>= \$2088.96</b>
<b>Consolidated</b>	$((10 \times 1024) \times 0.17) + ((2 \times 1024) \times 0.13)$	<b>= \$2007.04</b>

$$1 \text{ TB} = 1024 \text{ GB}$$

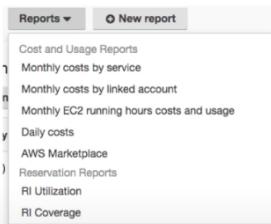
### AWS Cost Explorer

- Cost Explorer lets you visualize, understand, and manage your AWS costs and usage over time
- If you have multiple AWS accounts within an AWS Organization, costs will be consolidated in the **master account**
- Default Reports give insight into cost drivers and usage trends
- Use **forecasting** to get an idea of future costs
- You can view data at a **monthly or daily level of granularity**
- Use **filter** and **grouping** functionalities to dig even deeper into your data



**AWS Cost Explorer** lets you **visualize, understand, and manage** your AWS costs and usage over time. If you are have multiple AWS accounts within an AWS Organization costs will be consolidated in the **master account**.

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



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



Choose if you want to view your data at a **monthly** or **daily** level of granularity



Use **filter** and **grouping** functionalities to dig even deeper into your data!



- Create budgets for
  - Cost - dollar amount
  - Usage - e.g. EC2 running hours
  - Reservation - for Reserved Instances
- Tracked **monthly, quarterly, or yearly**, with customizable start and end dates
- Alerts support EC2, RDS, Redshift, and ElastiCache reservations
- Can be managed via the Dashboard or Budgets API
- Get notified of by providing an email or Chatbot, and check how close to the threshold of the current or forecasted budget you are
- Based on fixed cost OR plan on upfront based on your chosen level (tier)



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

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

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

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

Usage unit(s)
<input checked="" type="radio"/> Usage Type Group
EC2: Running Hours (hrs) *
<input type="radio"/> Usage Type

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



Budgeted amount	100	Hrs	Last month's usage 2260.54 Hrs
-----------------	-----	-----	--------------------------------

Budget based on a fixed cost or plan your upfront based on your chosen level

Can be easily manage from the **AWS Budgets** dashboard or via the **Budgets API**.

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

#### Billing and Pricing - TCO Calculator

- Total Cost of Ownership - allows you to estimate how much you would save when moving from on-premise to AWS
- Provides a detailed set of reports that can be used in **executive presentations**
- Built on underlying calculation models that generate fair assessments of value that you can achieve given the data provided
- Helps to reduce the need to invest in large capital expenditures (datacenters, hard disks, IT staff)
- **ONLY FOR APPROXIMATION** - not exact
- Three Steps
  - 1. Describe your environment
  - 2. View 3 Year Summary of Cost Comparisons

- 3. Download a detailed report

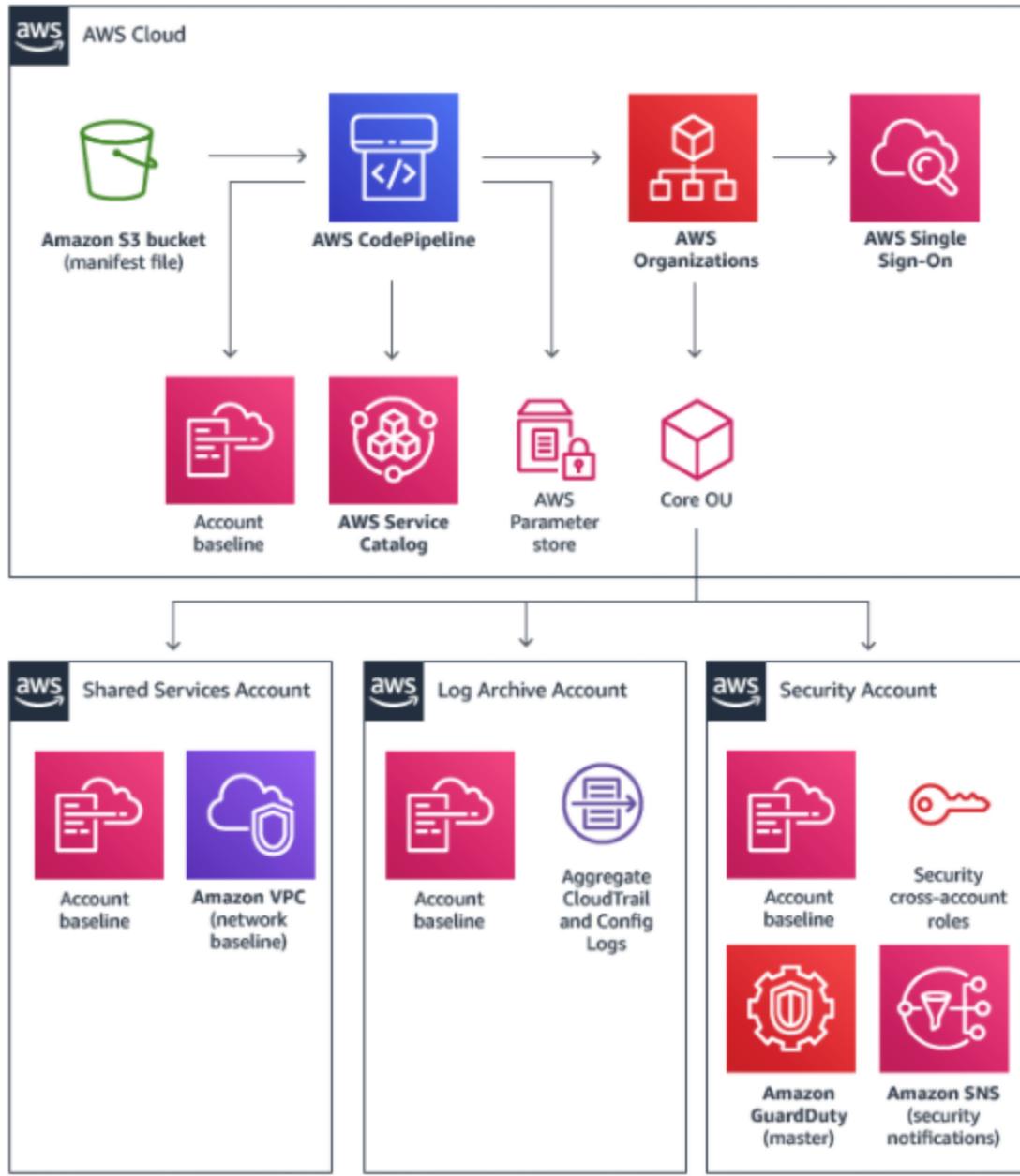
#### Billing and Pricing AWS Landing Zone - [Diagrams](#)

- Helps **enterprises** quickly set up a secure, AWS multi-account
- Provides a **baseline environment** to get started with a **multi-account architecture**
- **AWS Account Vending Machine (AVM)**
  - Automatically provisions and configures new accounts via a Service Catalog Template
  - Uses Single Sign On (SSO) for managing and accessing accounts
    - Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.
- The environment is customizable to allow customers to implement their own account baselines through a Landing Zone configuration and update pipeline

#### Notes

- When setting up an AWS Organization account, always have an isolated Log In Account and an isolated Security Account
  - Better for auditing purposes
  - This is done by AWS Landing Zone

The AWS Landing Zone solution includes four accounts, and add-on products that can be deployed using the AWS Service Catalog such as the Centralized Logging solution and AWS Managed AD and Directory Connector for AWS SSO.



#### Billing and Pricing - Resource Groups and Tagging

- **Tags** - words or phrases that act as metadata for organizing AWS resources
- **Resource Groups** - collections of resources that share one or more **TAGS**

- Helps to organize and consolidate information based on your project and resources that you use
- Resource Groups can display details about a group of resources based on:
  - Metrics
  - Alarms
  - Configuration Settings
- At any time, you can modify the settings of your resource groups to change which resources appear
- Ex. If you have a database, a server, and an S3 Bucket, you would give them the same tag and put them in the same Resource Group

#### Billing and Pricing - AWS Quick Starts

- **Prebuilt templates** by AWS and AWS Partners that help to **deploy popular stacks** on AWS
  - Reduces hundreds of manual procedures into a few steps
- Composed of 3 Parts
  - A reference architecture for the deployment
  - AWS **CloudFormation** templates that automate and configure the deployment
  - A deployment guide that explains the architecture and implementation in detail
- Most Quick Starts reference deployments enable you to spin up a fully functional architecture in less than an hour

#### Billing and Pricing - Cost and Usage Report

- Generates a detailed spreadsheet that enables you to better analyze and understand your AWS costs
- Places report into S3 Bucket
- Use **Athena** to turn the report into a queryable database
- Use **QuickSight** to visualize your billing data as graphs



# AWS Cost and Usage Report

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

M	N	O	P	Q	R	S	T
	Invoice/Period/Cycle	Invoice/Logistics	Invoice/Period	Invoice/Period/AvailabilityZone	Invoice/Usage/Annual	Invoice/Currency/Code	Invoice/Description
1	AmazonEC2	CW:AmazonMetricLog	Unsorted		0.00134400	\$0.00	\$0.00 per alarm metric - first 10 alarms
2	AmazonEC2	Requests 1hr	Unsorted		0.00134400	\$0.00	\$0.00 per request - PUT, COPY, POST or GET requests under the monthly global free tier
3	AmazonEC2	Unsorted	Unsorted		0.00134400	\$0.00	\$0.00 per API call - first 100 API calls
4	AmazonEC2	APSL:EBI:VolumeLog:gp2	Unsorted		0.00134400	\$0.00	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
5	AmazonEC2	APSL:EBI:VolumeLog:io1	Unsorted		0.00134400	\$0.00	\$0.00 per GB-month of Provisioned IOPS (SSD) storage under monthly free tier
6	AmazonEC2	UVW:2:BlockUsage:CL002	un-west-2a		0.00134400	\$0.00	\$0.00 per Windows 12. metro instance-hour (or partial hour) under monthly free tier
7	AmazonEC2	UVW:2:BlockUsage:CL002	un-west-2a		0.00134400	\$0.00	\$0.00 per GB - data transfer out under the monthly global free tier
8	AmazonEC2	UVW:2:UVEI:AWS-Out-Bytes	PublicOut		0.00000000	\$0.00	\$0.00 per byte - data transfer out from US West (Oregon) to US West (Northern California)
9	AmazonEC2	UVW:2:UVEI:AWS-In-Bytes	PublicIn		0.00000000	\$0.00	\$0.00 per byte - data transfer in from US West (Oregon) to US West (Northern California)
10	AmazonEC2	UVW:2:UVEI:AWS-In-Bits	PublicIn		0.00000000	\$0.00	\$0.00 per bit - data transfer in under the monthly global free tier
11	AmazonEC2	UVW:2:UVEI:AWS-Out-Bits	PublicOut		0.00000000	\$0.00	\$0.00 per bit - data transfer out under the monthly global free tier
12	AmazonEC2	UVW:2:DataTransfer:Clip-Bytes	Unsorted		0.00001344	\$0.00	\$0.00 per byte - data transfer under the monthly global free tier
13	AmazonEC2	UVW:2:UVW:AWS-Out-Bits	PublicOut		0.00000000	\$0.00	\$0.00 per byte - data transfer out under the monthly global free tier
14	AmazonEC2	UVW:2:UVW:AWS-In-Bits	PublicIn		0.00000000	\$0.00	\$0.00 per bit - data transfer in under the monthly global free tier
15	AmazonEC2	UVW:2:UVW:AWS-In-Bytes	PublicIn		0.00000000	\$0.00	\$0.00 per byte - data transfer in from US West (Northern California) to US West (Oregon)
16	AmazonEC2	UVW:2:UVW:AWS-Out-Bytes	PublicOut		0.00000000	\$0.00	\$0.00 per byte - data transfer out from US West (Northern California) to US West (Oregon)
17	AmazonEC2	UVW:2:UVW:AWS-In-Bits	PublicIn		0.00000000	\$0.00	\$0.00 per bit - data transfer in from US West (Northern California) to US West (Oregon)
18	AmazonEC2	APSL:EBI:VolumeLog:gp2	Unsorted		0.00134400	\$0.00	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
19	AmazonEC2	UVW:2:UVW:AWS-Out-Bits	PublicOut		0.00000000	\$0.00	\$0.00 per bit - data transfer under the monthly global free tier
20	AmazonEC2	UVW:2:BlockUsage:CL002	un-ws2a		0.00134400	\$0.00	\$0.00 per Windows 12. metro instance-hour (or partial hour) under monthly free tier
21	AmazonEC2	UVW:2:BlockUsage:CL002	un-ws2a		0.00134400	\$0.00	\$0.00 per GB - data transfer out under the monthly global free tier
22	AmazonEC2	UVW:2:DataTransfer:Clip-Bytes	Unsorted		0.00000000	\$0.00	\$0.00 per byte - data transfer in per month under the monthly global free tier
23	AmazonEC2	UVW:2:DataTransfer:Regional-Bytes	Unsorted		0.00000000	\$0.00	\$0.00 per byte - regional data transfer under the monthly global free tier
24	AmazonEC2	UVW:2:UVW:AWS-Out-Bits	PublicOut		0.00000000	\$0.00	\$0.00 per bit - data transfer out under the monthly global free tier
25	AmazonEC2	UVW:2:DataTransfer:Clip-Bytes	Unsorted		0.00000000	\$0.00	\$0.00 per byte - data transfer out under the monthly global free tier
26	AmazonEC2	UVW:2:UVW:AWS-In-Bits	PublicIn		0.00000000	\$0.00	\$0.00 per bit - data transfer in under the monthly global free tier
27	AmazonEC2	UVW:2:UVW:AWS-In-Bytes	PublicIn		0.00000000	\$0.00	\$0.00 per byte - data transfer in from Asia Pacific (Seoul) to US West (Oregon)
28	AmazonEC2	UVW:2:APSL:AWS-Out-Bytes	PublicOut		0.00000000	\$0.00	\$0.00 per byte - data transfer out under the monthly global free tier
29	AmazonEC2	UVW:2:UVW:AWS-Out-Bits	PublicOut		0.00000000	\$0.00	\$0.00 per bit - data transfer out from Asia Pacific (Seoul) to US West (Oregon)
30	AmazonEC2	UVW:2:DataTransfer:Clip-Bytes	Unsorted		0.00000000	\$0.00	\$0.00 per byte - data transfer out under the monthly global free tier
31	AmazonEC2	UVW:2:UVW:AWS-In-Bits	PublicIn		0.00000000	\$0.00	\$0.00 per bit - data transfer in under the monthly global free tier
32	AmazonEC2	UVW:2:UVW:AWS-Out-Bytes	PublicOut		0.00000000	\$0.00	\$0.00 per byte - data transfer out under the monthly global free tier
33	AmazonEC2	UVW:2:DataTransfer:Clip-Bytes	Unsorted		0.00000000	\$0.00	\$0.00 per byte - data transfer in under the monthly global free tier



Places the reports into S3



Use Athena to turn the report into a queryable database



Use QuickSight to visualize your billing data as graphs



## Technology Overview - AWS Organizations and Accounts

- Organizations allow you to centrally manage billing, control access, compliance, security, and share resources across your AWS accounts
- Root Account User is a single, sign-in identity that has complete access to all AWS services and resources in an account.
  - Each account has a root user
- Organization Units are a group of AWS accounts within an organization which can also contain other organizational units - creating a hierarchy
- Service Control Policies give central control over the allowed permissions for all accounts in your organization, helping to ensure your accounts stay within your organization's guidelines

## Tech Overview - AWS Networking

- Region - the geographical region of your network
- AZ - the data center of your AWS resources
- VPC (Virtual Private Cloud) - a logically isolated section of the AWS Cloud where you can launch AWS resources
- Internet Gateway - enable access to the internet
- Route Tables - determine where network traffic from your subnets is directed
- NACLs (Network Access Control List) - act as firewalls at the subnet level
- Security Groups - act as firewalls at the instance level
- Subnets - a logical partition of an IP network into multiple, smaller network segments
  - Public vs Private Subnets

- Public - accessible to the internet (Ex. EC2 Instance)
- Private - secure, not accessible to the internet (Ex. RDS DB)



**Region** the geographical location of your network

**AZ** the data center of your AWS resources

**VPC** a logically isolated section of the AWS Cloud where you can launch AWS resources

**Internet Gateway** Enable access to the Internet

**Route Tables** determine where network traffic from your subnets are directed

**NACLs** Acts as a firewalls at the subnet level

**Security Groups** Acts as firewall at the instance level

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

## Tech Overview - DB Services

### Database Services



**DynamoDB** - NoSQL **key/value** database



**DocumentDB** - NoSQL **Document** database that is MongoDB compatible



**RDS** - **Relational** Database Service that supports multiple engines

ENGINES: MySQL, Postgres, Maria DB, Oracle, Microsoft SQL Server, Aurora



**Aurora** MySQL (5x faster) and PSQL (3x faster) database **fully managed**



**Aurora Serverless** - only runs when you need it, like AWS Lambda



**Neptune** - Managed **Graph** Database



**Redshift** - **Columnar** database, **petabyte** warehouse **1000 TB = 1 PB!!!!**



\*\*Probably just know DynamoDB, RDS, Aurora, Redshift

- When you run Aurora is highly available and durable, and when you have a cluster, it will run 6 copies of the DB across 3 AZs (more expensive than RDS)
- Aurora Serverless - much less expensive than Aurora (need to basis)
  - Good for development or infrequently used apps
- Neptune - Managed **Graph** DB
- Redshift - Columnar DB, petabyte warehouse (1000 TB = 1PB)
  - Instead of reading via rows, it reads via columns
  - Good for working with large amounts of data for reports, analytics
  - Handles PBs of data!!!
- ElastiCache - Redis or Memcached database
  - For caching
- Caching
  - Caching is an area of a computer's memory devoted to temporarily storing recently used information. The content, which includes HTML pages, images, files and Web objects, is stored on the local hard drive in order to make it faster for the user to access it, which helps improve the efficiency of the computer and its overall performance.

## Provisioning Services

- Provisioning - the allocation or creation of resources and services to a customer
- Elastic Beanstalk - service for deploying and scaling web apps and services developed with Java, .NET, PHP, Node, Python, Ruby, Go, Docker
  - Similar to Heroku, Netlify
- OpsWorks - configuration management service that provides managed instances of **Chef** and **Puppet**
  - Chef and Puppet programmatically set up a server
    - Chef uses Ruby to define *recipes* to set up servers, dependencies, pull code
  - OpsWorks has **layers for infrastructure**
    - DB layer, network layer, application layer
- CloudFormation - infrastructure as code, JSON or YAML
  - Create a JSON or YAML file that defines all AWS Resources and how you want to configure them, and this will set up everything that you want in one go
  - CloudFormation is the most complex option/most flexible option (more powerful than Opsworks)
- AWS QuickStart - pre-made packages that can launch and configure your AWS compute, network, storage, and other services required to deploy a workload on AWS
- AWS Marketplace - a digital catalogue of **thousands** of software listings from independent software vendors to find, buy, test, and deploy software

# Provisioning

## What is provisioning?

The allocation or creation of resources and services to a customer

-  **Elastic Beanstalk** - service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker 
-  **OpsWorks** - configuration management service that provides managed instances of **Chef** and **Puppet**.
-  **CloudFormation** - infrastructure as code, **JSON** or **YAML**
-  **AWS QuickStart** - pre-made packages that can launch and configure your AWS compute, network, storage, and other services required to deploy a workload on AWS
-  **AWS Marketplace** - a digital catalogue of **thousands** of software listings from independent software vendors you can use to find, buy, test, and deploy software.

## Computing Services

- EC2 (Elastic Compute Cloud) - highly configurable server in terms of CPU, Memory, Network, OS
  - **Every service under the hood is running on EC2 instances**
- ECS (Elastic Container Service) - **Docker as a Service** - highly scalable, high-performance container orchestration service that supports Docker containers, pay for EC2 instances
- Fargate - Microservices with which you don't have to think about infrastructure
  - Pay per task (runtime and CPU utilized when running)
  - You don't choose EC2 instances, just define containers within a task or service, and AWS will run it
- EKS - Kubernetes as a Service - easy to deploy, manage, and scale containerized applications using Kubernetes
  - Kubernetes is a standard in the industry
- Lambda serverless functions run code without provisioning or managing servers
  - Pay for compute time that you consume (how long it runs)
- Elastic Beanstalk - orchestrates various AWS services, including EC2, S3, Simple Notification Service (SNS), CloudWatch, autoscaling, and Elastic Load Balancers (ELBs)
- AWS Batch - plans, schedules, and executes batch computing workloads across the full range of AWS compute services and features, such as Amazon EC2 and Spot Instances
  - Saves a lot of money \$\$\$

## Computing



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



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



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



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



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



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



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



## Storage Services

### Storage



**S3 - Simple Storage Service** - **object** storage



**S3 Glacier** - low cost storage for **archiving and long-term backup**



**Storage Gateway** - hybrid cloud storage with local caching



File Gateway



Volume Gateway



Tape Gateway



**EBS - Elastic Block Storage** - hard drive in the cloud you attach to EC2 instances  
SSD, IOPS SSD, Throughput HDD, Cold HDD



**EFS - Elastic File Storage** - file storage mountable to multiple EC2 instances at the same time



**Snowball** - Physically migrate lots of data via a computer suitcase 50-80 TB



**Snowball Edge** A better version of Snowball - 100 TB



**Snowmobile** Shipping container, pulled by a semi-trailer truck - 100 PB



- Storage Gateway - hybrid cloud storage with local caching
  - An extension of on-premise storage in the cloud
- EBS (Elastic Block Storage) - hard drive in the cloud you attach to EC2 instances

- Different choices include SSD, IOPS SSD, Throughput HHD, Cold HHD
- Snowball - physically migrate lots of data via a computer suitcase 50-80 TB
  -
- Snowball Edge - a better version of Snowball (100TB)
- Snowmobile - shipping container, pulled by a semi-trailer truck (100PB)
  - Actually in a truck!!!!

## Business Centric Services

- Amazon Connect
  - Accept inbound calls and dial outbound
  - Record calls and store them in S3 (run analysis through Amazon Comprehend)
  - Set up workflows
- WorkSpaces
  - Virtual, remote desktop
  - Spin up Windows 10 server from AWS
- WorkDocs
  - Sharepoint competitor
- Chime
  - Ex. Slack + Skype
- Workmail
  - Gmail for AWS
- Pinpoint
  - Email marketing
  - Create campaigns
  - Do A/B testing
- SES Simple Email Service
  - Cloud-based email for developers
  - For when you are building an app and want to send out emails FROM that application
  - Supports HTML emails
  - SNS can also send emails, but only plain text
- QuickSight
  - Connect data from S3, Aurora, RDS
    - Creates graph from this data

## Business Centric Services



**Amazon Connect - Call Center** - Cloud-based call center service you can setup in just a few clicks - based on the same proven system used by the Amazon customer service teams.



**WorkSpaces - Virtual Remote Desktop** - Secure managed service for provisioning either Windows or Linux desktops in just a few minutes which quickly scales up to thousands of desktops



**WorkDocs** - A content creation and collaboration service - easily create, edit, and share content saved centrally in AWS. (the AWS version of Sharepoint)



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



**WorkMail** - Managed **business email**, contacts, and calendar service with support for existing desktop and mobile email client applications. (IMAP)



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



**SES - Simple Email Service** - A cloud-based email sending service designed for marketers and application developers to **send marketing, notification, and emails**



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



(A)

## Enterprise Integration

- Going Hybrid! (On-premise + Cloud)
- Direct Connect
  - Low latency, dedicated connection
- VPN
- Storage Gateway
  - Ex. extends on-prem hard drives onto AWS
- Active Directory

# Enterprise Integration

## Going Hybrid!



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



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



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



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

### Logging Services

- CloudTrail
  - Determines who we should blame for something on AWS (which employee)
  - Detect developer misconfiguration ^
  - Detect malicious actors
  - Automate response (everytime something is created, create a notification)
- CloudWatch
  - CloudWatch Logs\*\*\*\*

# Logging Services



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

Who created this bucket?

- Detect developer misconfiguration

Who spun up that expensive EC2 instance?

- Detect malicious actors

Who launched this SageMaker Notebook?

- Automate responses



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

**CloudWatch Logs**

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

**CloudWatch Metrics**

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

**CloudWatch Events**

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

**CloudWatch Alarms**

triggers notifications based on metrics

**CloudWatch Dashboard**

create visualizations based on metrics

## Quick Guide

## Know your Initialisms

**IAM** Identity and Access Management

**ELB** Elastic Load Balancer

**S3** Simple Storage Service

**ALB** Application Load Balancer

**SWF** Simple Workflow Service

**NLB** Network Load Balancer

**SNS** Simple Notification Service

**EC2** Elastic Cloud Compute

**SQS** Simple Queue Service

**ECS** Elastic Container Service

**SES** Simple Email Service

**ECR** Elastic Container Repository

**SSM** Simple Systems Manager

**EBS** Elastic Block Storage

**RDS** Relational Database Service

**EFS** Elastic File Storage

**VPC** Virtual Private Cloud

**EMR** Elastic MapReduce

**VPN** Virtual Private Network

**EB** Elastic Beanstalk

**CFN** CloudFormation

**ES** Elasticsearch

**WAF** Web Application Firewall

**EKS** Elastic **Kubernetes** Service

**MQ** Amazon ActiveMQ

**MKS** Managed **Kafka** Service

**ASG** Auto Scaling Groups

**IoT** Internet of Things

**TAM** Technical Account Manager

**RI** Reserved Instances

## Shared Responsibility Model

- Customers are responsible for security IN the cloud
  - Any data that you put into AWS
  - If you do not secure it, that is your fault

- If you do not monitor sensitive data, that is your fault
- AWS is responsible for Security of the CLOUD
- Just know the first model\*\*

## Shared Responsibility Model

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



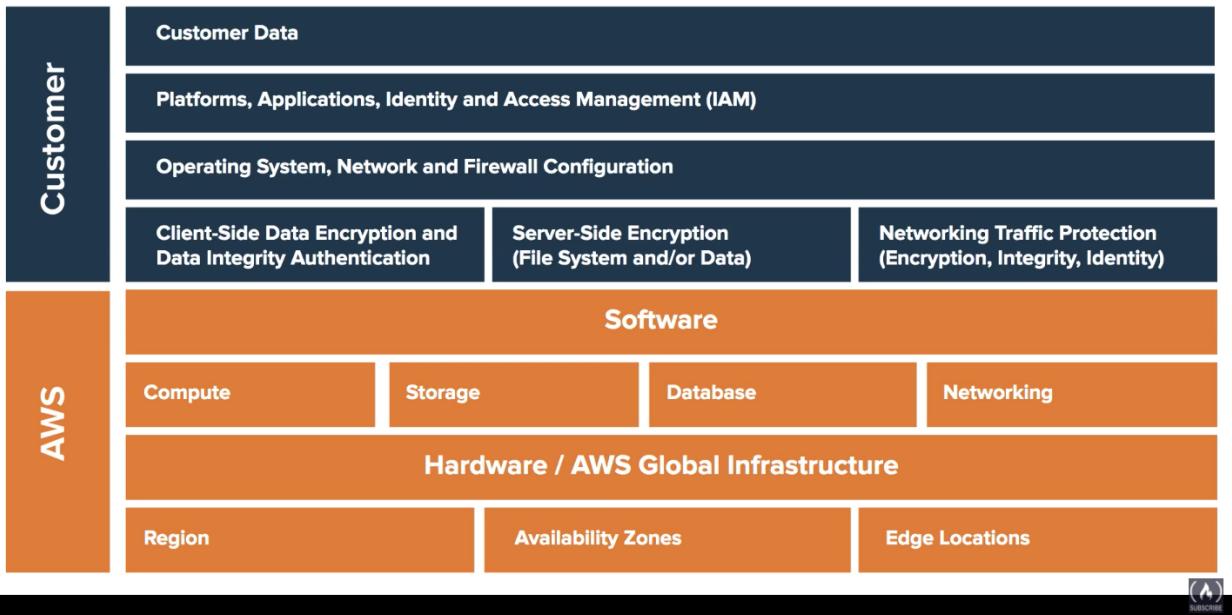
**Data Configuration**



**Hardware  
Operation of Managed Services  
Global Infrastructure**

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

## Shared Responsibility Model



AWS Compliance Programs

- Set of internal policies and procedures of a company to comply with laws, rules, and regulations, or to uphold business reputation
- Ex.
  - HIPAA
    - Safeguards medical information
  - PCI DSS
    - When you want to sell things online and handle credit card information

## AWS Compliance Programs

**Compliance Programs**  
A set of internal policies and procedures of a company to comply with laws, rules, and regulations or to uphold business reputation.

**Health Insurance Portability and Accountability Act of 1996** is United States legislation that provides data privacy and security provisions for safeguarding medical information.

The Payment Card Industry Data Security Standard (PCI DSS)

When you want to sell things online and you need to handle credit card information.

### AWS Artifact

- How do we prove AWS meets a compliance?
- Go into AWS Artifacit, choose package or Artifact, it will generate a PDF, and within this PDF you will click a link to get the files that you want



## AWS Artifact



### How do we prove AWS meets a compliance?

No cost, self-service portal for on-demand access to AWS' compliance reports

On-demand **access to AWS' security and compliance reports** and select online agreements

These checks are based on **global compliance frameworks**



Government of Canada (GC) Partner Package  
Reporting period: Valid beginning 08/25/2017

The Government of Canada (GC) Partner Package is intended for use by partners and customers when building applications and solutions on AWS that need to meet the GC requirements based on the Protected B/Medium Integrity/Medium Availability (PBMM) profile. The documents available in this package include: Partner Package Playbook, Controls Implementation Summary (CIS)/Customer Responsibility Matrix (CRM), and Government of Canada PBMM Security Assessment and Letter of Attestation.

[Get this artifact](#)



### Amazon Inspector

- How do we prove an EC2 Instance is **hardened**?
- Hardening - the act of eliminating as many security risks as possible
- Runs a **Security Benchmark** against specific EC2 instances
  - You can run a variety of these
- CIS - Center of Internet Security - a benchmark that runs over 699 checks
- Network Assessment - checking whether ports are open and whether they're reachable to the internet
- Host - checks the applications and OS



## Amazon Inspector

### How do we prove an EC2 Instance is hardened?

#### Hardening

The act of eliminating as many **security** risks as possible.

AWS Inspector runs a **security benchmark** against specific EC2 instances.  
You can run a variety of security benchmarks.

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

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

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



### AWS WAF (Web Application Firewalls)

- WAF has to be attached to either **CLOUDFRONT or APPLICATION LOAD BALANCER (ALB)**



## AWS WAF

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

Write your own **rules** to ALLOW or DENY traffic based on the contents of an HTTP requests

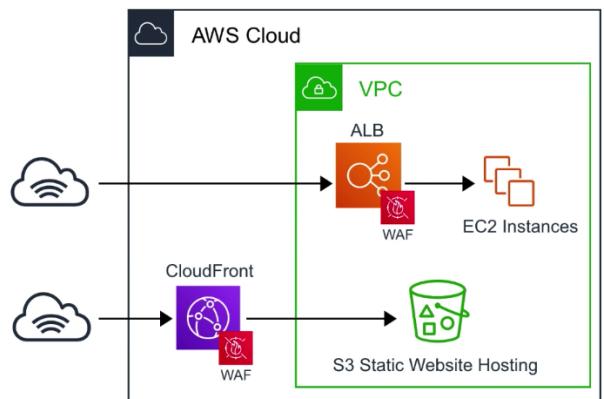
Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Rules Marketplace

WAF can be attached to either **CloudFront** or an **Application Load Balancer**

Protect web applications from attacks covered in the

**OWASP Top 10** most dangerous attacks:

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring



### AWS Shield

- DDOS Attack - a malicious attempt to disrupt normal traffic by flooding a website with a large amount of fake traffic
- DDOS = Distributed Denial of Service
- AWS Shield is a managed DDOS protection service that safeguards applications on AWS
- You should always be routing your traffic through Route53 or CloudFront (Automatically come with AWS Shield Standard)
- Protects against Layer 3,4, and 7 attacks
  - 7 = Application
  - 4 = transport
  - 3 = network



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

#### What is a DDOS attack?

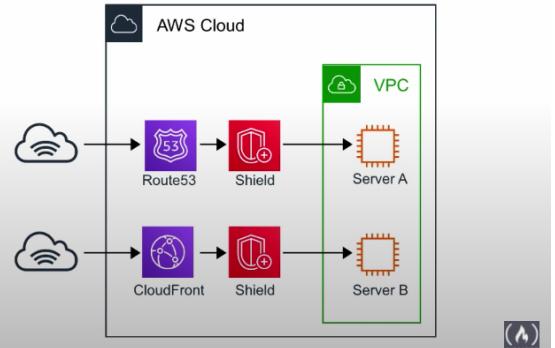
A malicious attempt to disrupt normal traffic by flooding a website a large amount of fake traffic

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge

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

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

- 7 Application
- 4 Transport
- 3 Network



#### AWS Shield Plans

- Shield Standard - Free
  - Protects again most common DDOS attacks
- Shield Advanced - \$3000/year
  - Additional protection against larger and more sophisticated attacks
  - Available for:
    - Route53
    - CloudFront
    - ELB
    - AWS Global Accelerator
    - Elastic IP (Amazon Elastic Compute Cloud and Network Load Balancer)



## AWS Shield

### Shield Standard

Free

For **protection against most common DDoS attacks**, and access to tools and best practices to build a DDoS resilient architecture.

Automatically available on all AWS services.

### Shield Advanced

3000 USD / Year

For **additional protection against larger and more sophisticated attacks**, visibility into attacks, and 24x7 access to DDoS experts for complex cases.

Available on:

- Amazon Route 53
- Amazon CloudFront
- Elastic Load Balancing
- AWS Global Accelerator
- Elastic IP (Amazon Elastic Compute Cloud and Network Load Balancer)

## Security - Penetration Testing

- PenTesting - authorized simulated cyberattack on a computer system, performed to evaluate the security of a system
- You CAN do this on AWS for some services

## Penetration Testing

### What is PenTesting?

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

*Can you perform PenTesting on AWS? Yes!*

#### Permitted Services

1. EC2 instances, NAT Gateways, and ELB
2. RDS
3. CloudFront
4. Aurora
5. API Gateways
6. AWS Lambda and Lambda@Edge functions
7. Lightsail resources
8. Elastic Beanstalk environments

#### Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

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



## AWS Security - Guard Duty

- IDS = Intrusion Detection System
- IPS = Intrusion Protection System
- How do you detect whether someone is attempting to gain access to your AWS account or resources
- Guard Duty is a threat detection service that uses machine learning to analyze:
  - CloudTrail logs
  - VPC Flow logs
  - DNS logs



### Amazon Guard Duty

#### What is IDS/IPS?

Intrusion Detection System and Intrusion Protection System.

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

*How do we detect if someone is attempting to gain  
access to our AWS account or resources?*

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

- CloudTrail Logs
- VPC Flow Logs
- DNS logs



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

## Key Management Service (KMS)

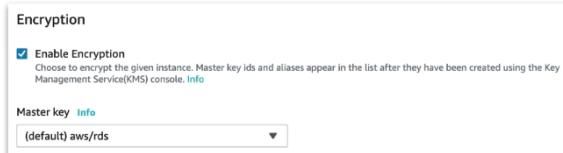
- Makes it easy to create and control encryption keys to encrypt your data
- KMS is a multi-tenant hardware security module (HSM)
  - An actual piece of hardware that is used by multiple AWS customers that are isolated using virtual software
- Many AWS services use KMS to encrypt data with a simple checkbox
- KMS uses Envelope Encryption
  - Envelope Encryption - when you encrypt your data, your data is protected, but you have to protect your **data/encryption key**. When you encrypt your data key with a **master key**, you have an additional layer of security
    - Like putting your key in an envelope so others can't see



## Key Management Service (KMS)

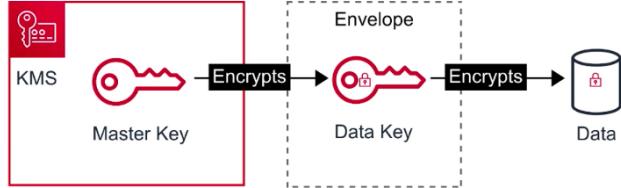
A managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

- KMS is a multi-tenant HSM (hardware security module)
- Many AWS services are integrated to use KMS to encrypt your data with a simple checkbox
- KMS uses Envelope Encryption.



### Envelope Encryption

When you encrypt your data, your data is protected, but you have to protect your encryption key. When you encrypt your data key with a master key as an additional layer of security.



## Amazon Macie

- Macie is a fully managed service that continuously monitors S3 data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks
  - Uses Machine Learning to analyze your CloudTrail logs
  - When you put data in your S3 Data, like credit card numbers, Macie detects sensitive data and whether that data is exposed or can be compromised
    - Ex. if credit card numbers are stored as plain text, Macie will alert you that you should encrypt that data
- Will identify your most at-risk users
  - Ranked by badges
    - The nicer the badge, the worse the user is at best practices



## Amazon Macie

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

Macie works by uses Machine Learning to Analyze your CloudTrail logs

Macie has a variety of alerts

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

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



- Ransomware - locking you out of your data and asking for money
- Privilege Escalation - someone getting access to stuff they're not supposed to
- Identity Enumeration - trying to enumerate over data to figure out what they can steal
- Credential Loss

Security Groups vs. NACLs

- Security Groups are firewalls at the **instance level**
- NACLs are a firewall at the **subnet level**

# Security Groups vs NACLs

## Security Groups

Acts as a firewall at the **instance** level  
Implicitly denies all traffic. You create Allow rules.

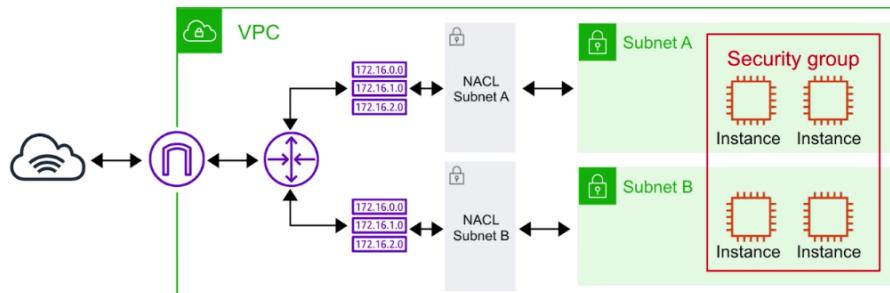
Eg. Allow an EC2 instance access on port 22 for SSH

## NACLs

Network Access Control Lists

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

Eg. Block a specific IP address known for abuse



## AWS VPN

- Lets you establish a **secure and private tunnel** from your network or device to the AWS Global Network
- Site-to-Site VPN
  - Securely connect on-premises network or branch office site to VPC
  - Ex. connect an entire office or network
- AWS Client VPN
  - Securely connect users to AWS or on-premises networks
  - Connect individual employees

# Security Groups vs NACLs

## Security Groups

Acts as a firewall at the **instance** level  
Implicitly denies all traffic. You create Allow rules.

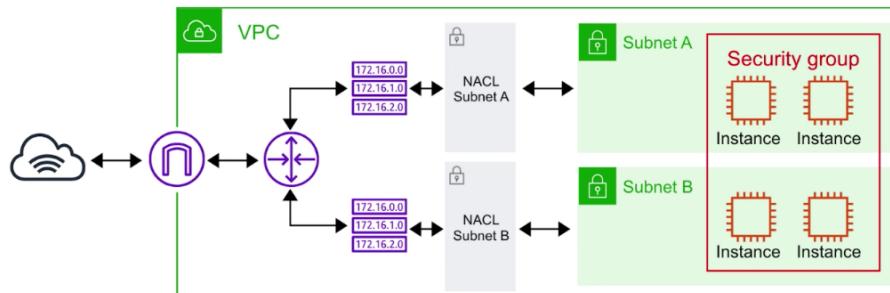
Eg. Allow an EC2 instance access on port 22 for SSH

## NACLs

Network Access Control Lists

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

Eg. Block a specific IP address known for abuse



## Cloud Service Variation Study

- CloudFormation - infrastructure as code, sets up services via templating script via JSON and YML
- CloudTrail - who you can blame - logs all API calls between AWS Services
- CloudFront - Content Distribution Network (CDN) creates a cached copy of your website and copies to servers located near people trying to download the website
- CloudWatch - a collection of services
  - CloudWatch logs
    - Any custom log data, Memory Usage, Rails Logs, Nginx Logs
  - CloudWatch Metrics
    - Metrics based off of logs, i.e. Memory Usage
  - CloudWatch Events
    - Trigger an event based on a condition, i.e. every hour take a snapshot of the server
  - CloudWatch Alarms
    - Triggers notifications based on metrics
  - CloudWatch Dashboard
    - Create visualizations based on metrics
- CloudSearch
  - Search engine for when you have an ecommerce website and you want a search bar

# Cloud\* Services

## Similar names, completely different services.



**CloudFormation** - infrastructure as code, set up services via templating script eg. yml,json



**CloudTrail** - logs all api calls between aws services (who can we blame)  
eg. aws s3api create-bucket --bucket my-bucket-ash-test-123



**CloudFront** - Content Distribution Network, It create a cached copy of your website and copies to server located near people trying download website



**CloudWatch** - is a collection of multiple services  
CloudWatch Logs - any custom log data, Memory Usage, Rails Logs, Nginx Logs  
CloudWatch Metrics - metrics that are based off of logs eg. Memory Usage  
CloudWatch Events - trigger an event based on a condition eg. ever hour take snapshot of server  
CloudWatch Alarms - triggers notifications based on metrics  
CloudWatch Dashboard - create visualizations based on metrics



**CloudSearch** - search engine, you have an ecommerce website and you want to add a search bar

## Connect Service Variation Study

- Direct Connect - dedicated fiber optics connections from DataCenter to AWS
  - A large enterprise has their own datacenter and they need an insanely fast connection directly to AWS. If you need security, you can apply a VPN on top of Direct Connect
- Amazon Connect - Call Center Service
  - A call center in the cloud
  - Toll free number, accept inbound and outbound calls, setup automated phone payments
- Media Connect - New version of Elastic Transcoder, Converts Videos to different Video Types

## \*Connect Services



### **Direct Connect** Dedicated Fiber Optics Connections from DataCenter to AWS

A large enterprise has their own datacenter and they need an insanely fast connection directly to AWS. If you need to security you can apply a VPN connect on-top of Direct Connect



### **Amazon Connect** Call Center Service

Get a toll free number, accept inbound and outbound calls, setup automated phone systems.



### **Media Connect** New Version of Elastic Transcoder, Converts Videos to Different Video Types

You have 1000 of videos you and you need to transcode them into different videos format, maybe you need to apply watermarks, or insert introduction video in front of every video

#### Elastic Transcoder vs. MediaConvert (Same price)

- **Both services transcode videos**
- Elastic Transcoder is the old way
  - Transcodes videos to streaming formats
- AWS Elemental MediaConvert (new way)
  - Transcodes videos to streaming formats
  - Overlays images
  - Insert video clips
  - Extracts captions data
  - Robust UI

#### SNS vs SQS (They both connect apps via Messages)

- SNS - Simple Notification Service
  - Passes along messages using PubSub (Publisher - Subscriber)
  - Send notifications to subscribers on topics via HTTP, email, SQS, SMS
  - Used for **plain text emails (cannot do HTML emails)**, ex. Billing alarms
- SQS - Simple Queue Service
  - Queue up messages, guaranteed delivery
  - Places messages into a queue - applications pull queue using the AWS SDK (Software Development Kit)
  - Retains message up to 14 days
  - Sends messages in sequential order
  - Ensure only one message is sent
  - Ensure messages are delivered at least ONCE
  - Good for delayed tasks, i.e. queueing up emails



## SNS vs SQS



### The Both Connect Apps via Messages

#### Simple Notifications Service

Pass Alongs Messages eg. PubSub

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

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

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

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



PUSHER  
POWERING REALTIME

PubNub

#### Simple Queue Service

Queue Up Messages, Guaranteed Delivery

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

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

Really good for delayed tasks, queueing up emails



### Inspector vs. Trusted Advisor (Both security tools to perform audits)

- Amazon Inspector (Only for EC2 instances)
  - Audits a **SINGLE** EC2 instance that you have selected
  - Generates reports from a long list of checks... 699 checks
- Trusted Advisor (Multiple AWS services and security practices)
  - Doesn't generate a PDF report
  - Gives a holistic view of recommendations across **multiple services** and best practices
    - Ex. you have open ports on these security groups
    - Ex. you should enable MFA on your root account when using trusted advisor



## Amazon Inspector vs AWS Trusted Advisor



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

### Amazon Inspector

Audits **a single EC2 instance** that you've selected

Generates a report from a long list of security checks i.e 699 checks.

### Trusted Advisor

Trusted Advisor **doesn't generate out a PDF report**.

Gives you a **holistic view** of recommendations across multiple services and best practices

eg.  
You have open ports on these security groups

You should enable MFA on your root account when using trusted advisor.

## ALB v. NLB v. CLB



## ALB vs NLB vs CLB

### Application

**Layer 7 Requests**

**HTTP and HTTPS traffic**

**Routing Rules**, more usability from one load balancer.



Can attach WAF

### Network

**Layer 4 IP protocol data.**

**TCP and TLS traffic** where extreme performance is required.

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

### Classic

**OLD**

**Layer 4 and Layer 7**

Intended for applications that were built within the **EC2-Classic network**

Doesn't use Target Groups



Can attach Amazon Certification Manager (ACM) SSL Certificate

## SNS vs. SES



### SNS vs SES



#### They Both Send Emails

##### Simple Notifications Service

Practical and Internal

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.

Most exam questions are going to be talking about SNS because lots of services can trigger SNS for notifications.

You Need to Know what are **Topics** and **Subscriptions** regarding **SNS**

##### Simple Email Service

Professional, Marketing, Emails

A cloud based email service. eg. **SendGrid**

SES sends **html emails**, SNS cannot.

SES can receive inbound emails

SES can create Email Templates

Custom domain name email

Monitor your email reputation

#### TOPICS and SUBSCRIPTIONS REGARDING SNS!!!

#### Artifact v. Inspector



### AWS Artifact vs AWS Inspector



Both Artifact and Inspector **compile out PDFs**

##### AWS Artifact

Why should an enterprise trust AWS?

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

Service Organization Control (SOC)

Payment Card Industry (PCI)

##### AWS Inspector

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

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

**Audit tool for security of EC2 instances**



## Last Minute Tips

- Global Accelerator can be used to reduce latency of websites to load faster for users around the world
  - Monitors health with the ability to route traffic to healthy regional endpoints
- VPC Flow Logs can capture information about IPD traffic or any traffic flowing into your VPC
- You can use Snowball or Data Migration Service (DMS) to move data from on-premise to AWS

## Tricky Questions

- S3 Standard Storage Class has 99.99999999% Durability and 99.99% Availability
- What is the main benefit of on-demand EC2 instances?
  - You can create, start, stop, and terminate at any time
- If you are using an on-demand EC2 instance, how are you being charged for it?
  - You are charged per second, based on an hourly rate, and there are no termination fees
- What is benefit of choosing reserved instance over on-demand instance ?
  - Lower cost when compared to on-demand
- Which AWS service can help against DDoS protection ?
  - CloudFront
- Which AWS service can help caching objects ?
  - CloudFront
- You are building online cloud storage platform. Users will be uploading their files for backup to your applications. You are unsure about the capacity requirements. Which AWS service can help you here ?
  - S3
- What is the benefit of using RDS instead of hosting own database in EC2 instance ? Which of the following are benefits of AWS's Relational Database Service (RDS)?
  - Automated patches and backups
- Alice is a DevOps and he wants to ensure that all servers are working perfectly. One of the aspects is monitor the CPU usage. Application tends to slow down when CPU usage is greater than 60%. How can Alice track down when CPU usage goes above 60% for any of the EC2 instance ?
  - Use CloudWatch Alarms
- You have a very critical application which your organization simply can't afford to have it down. What is the architecture strategy you would use to prepare to be used for the application ?
  - Use Multi-region based architectures
- What is one of the advantages of the Amazon Relational Database Service (Amazon RDS)?

- It simplifies relational database administration tasks
- A customer needs to run a MySQL database that easily scales. Which AWS service should they use?
  - Amazon Aurora
- Which of the following is a shared control between the customer and AWS?
  - AWS is responsible for creating awareness and providing training of their employees. Client is responsible to do the same for their employees.
  - Awareness and Training
- How many Availability Zones should compute resources be provisioned across to achieve high availability?
  - Minimum of 2
- Which AWS IAM feature allows developers to access AWS services through the AWS CLI?
  - Access Keys
- Which of the following is a fast and reliable NoSQL database service?
  - Amazon DynamoDB
- What approach to transcoding a large number of individual video files adheres to AWS architecture principles?
  - Using many instances in parallel
- Which of the following is an AWS managed Domain Name System (DNS) web service?
  - Amazon Route 53
- Which storage service can be used as a low-cost option for hosting static websites?
  - Amazon Simple Storage Service (S3)
- What is the AWS customer responsible for according to the AWS shared responsibility model?
  - Data encryption
- Which of the following AWS Cloud services can be used to run a customer-managed relational database?
  - Amazon EC2
- A company is looking for a scalable data warehouse solution. Which of the following AWS solutions would meet the company's needs?
  - Amazon Redshift (warehouse!)
- Which of the following are valid ways for a customer to interact with AWS services?
  - Command line interface
- What is the benefit of using AWS managed services, such as Amazon ElastiCache and Amazon Relational Database Service (Amazon RDS)?
  - They simplify patching and updating underlying OSs
- Which AWS service provides a simple and scalable shared file storage solution for use with Linux-based AWS and on-premises servers?
  - Amazon EFS (Elastic File System) ???

- Under the shared responsibility model, which of the following is a shared control between a customer and AWS?
  - Patch management
- Which AWS service allows companies to connect an Amazon VPC to an on-premises data center?
  - Amazon Direct Connect
- Which AWS service provides alerts when an AWS event may impact a company's AWS resources?
  - AWS Personal Health Dashboard
- Which task is AWS responsible for in the shared responsibility model for security and compliance?
  - Updating Amazon EC2 host firmware
- If a customer needs to audit the change management of AWS resources, which of the following AWS services should the customer use?
  - AWS Config
- What is Amazon CloudWatch?
  - A metrics repository with customizable notification thresholds and channels
- Which design principles for cloud architecture are recommended when re-architecting a large monolithic application?
  - Implement loose coupling
  - Designing loosely-coupled system is one of the very important design principles.
- Which AWS services are defined as global instead of regional?
  - Amazon CloudFront
    - Amazon CloudFront is a Content Distribution Network for global access to data
- Which AWS Cost Management tool allows you to view the most granular data about your AWS bill?
  - AWS Cost and Usage Report
- Which of the following services falls under the responsibility of the customer to maintain operating system configuration, security patching, and networking?
  - Amazon EC2
- Which service is best for storing common database query results, which helps to alleviate database access load?
  - ElastiCache
- How does data get into Glacier ?
  - S3 Lifecycle policy
    - In order to upload to Glacier, S3 LifeCycle policy should be used
- Which of the following AWS services ensures that only authorized and authenticated request are allowed?
  - AWS Identity and Access Management (IAM)

- Small Corp is planning to create a disaster recovery strategy for their workloads in AWS. Which among these is a good DR strategy for worst case scenario?
  - AWS Regions
- Which among the following is true about Availability Zones?
  - Multiple zones across distinct locations in the same region connected by high speed networks
- The use of what AWS feature or service allows companies to track and categorize spending on a detailed level?
  - Cost Allocation tags
- What AWS team assists customers with accelerating cloud adoption through paid engagements in any of several specialty practice areas?
  - AWS Professional Services
- A customer would like to design and build a new workload on AWS Cloud but does not have the AWS-related software technical expertise in-house.
  - AWS Partner Network Consulting Partners
- Which AWS services can host a Microsoft SQL Server database?
  - Amazon RDS
- Which AWS services can host a Microsoft SQL Server database?
  - Amazon EC2
- Which of the following Amazon EC2 pricing models allow customers to use existing server-bound software licenses?
  - Dedicated Hosts
- Which services can be used across hybrid AWS Cloud architectures?
  - Amazon Route 53
  - \*\*Virtual Private Gateways can also be used for hybrid architectures
- A company is considering using AWS for a self-hosted database that requires a nightly shutdown for maintenance and cost-saving purposes. Which service should the company use?
  - Amazon EC2 with Amazon Elastic Block Store (EBS)
- Which is a recommended pattern for designing a highly available architecture on AWS?
  - Ensure that the application is designed to accommodate failure of any single component
- Which AWS services are defined as global instead of regional?
  - Amazon Route 53
  - DNS (Domain Naming System)
- Which of the following features can be configured through the Amazon Virtual Private Cloud (Amazon VPC) Dashboard?
  - Subnets
- Where should users report that AWS resources are being used for malicious purposes?

- AWS Abuse Team
- Which Amazon RDS feature can be used to achieve high availability?
  - Multiple AZs
- What helps a company provide a lower latency experience to its users globally?
  - Using EL (edge locations) to put content closer to all users
- Which activity is a customer responsibility in the AWS Cloud according to the AWS shared responsibility model?
  - Ensuring Amazon EBS volumes are backed up
- Which AWS service allows users to identify the changes made to a resource over time?
  - AWS Config
- A Cloud Practitioner needs a consistent and dedicated connection between AWS resources and an on-premises system. Which AWS service can fulfill this requirement?
  - Amazon Direct Connect
- Which security service automatically recognizes and classifies sensitive data or intellectual property on AWS?
  - Macie
- \*\*\*\*How can a company isolate the costs of production and non-production workloads on AWS? .
  - Use different accounts for production and non-production expenses
- A web application running on AWS has been spammed with malicious requests from a recurring set of IP addresses. Which AWS service can help secure the application and block the malicious traffic?
  - AWS WAF
- What is the advantage of deploying an application across multiple Availability Zones?
  - The application will have higher availability because it can withstand a service disruption in one AZ
- Which AWS service provides inbound and outbound network ACLs to harden external connectivity to Amazon EC2?
  - Amazon VPC
- Access keys in AWS Identity and Access Management (IAM) are used to:
  - Make programmatic calls to AWS from AWS APIs
- A customer runs an On-Demand Amazon Linux EC2 instance for 3 hours, 5 minutes, and 6 seconds. For how much time will the customer be billed?
  - 3 hours, 5 mins, 6 seconds
- A company wants to monitor the CPU usage of its Amazon EC2 resources. Which AWS service should the company use?
  - Amazon CloudWatch
- Which of the following is the responsibility of AWS?

- Physically destroying storage media at the end of life
- Which of the following services is a MySQL-compatible database that automatically grows storage as needed?
  - Amazon Aurora
- What feature of Amazon RDS helps to create globally redundant databases?
  - Cross-region read replicas
- How is asset management on AWS easier than asset management in a physical data center?
  - Users can gather asset metadata reliability with a few API calls
- Which of the following can a customer use to enable single sign-on (SSO) to the AWS Console?
  - AWS Directory Service
- Which services are parts of the AWS serverless platform?
  - AWS Step Functions, Amazon DynamoDB, Amazon SNS