Six Advantages and Benefits of Cloud Computing

Why go with a Cloud Provider over On-Premise?

1 **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

2 **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 get unbeatable savings

3 **Stop guessing capacity**

Eliminate guesswork about infrastructure capacity needs. **Instead of paying for idle or underutilized servers**, you can scale up or down to meet the current need.

4 **Increase speed and agility**

Launch resources **within a few clicks in minutes** instead of waiting days or weeks of your IT to implement the solution on-premise

5 **Stop spending money on running and maintaining data centers**

Focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers

6 **Go global in minutes**

Deploy your app in **multiple regions around the world with a few clicks**.
Provide lower latency and a better experience for your customers at minimal cost.

What is Cloud Computing?

cloud com·put·ing

noun

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.

On-Premise

- You own the servers
- You hire the IT people
- You pay or rent the real-estate
- You take all 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 your configuring cloud services and code, someone else takes care of the rest.

Types of Cloud Computing

SaaS For Customers

Software as a Service

A completed product that is run and managed by the service provider

Don't worry about how the service is maintained. It just works and remains avaliable.

PaaS For Developers

Platform as a Service

Removes the need for your organization to manage the underlying infrastructure. Focus on the deployment and management of your applications

Don't worry about, provisioning, configuring or understanding the hardware or OS.

IaaS For Admins

Infrastructure as a Service

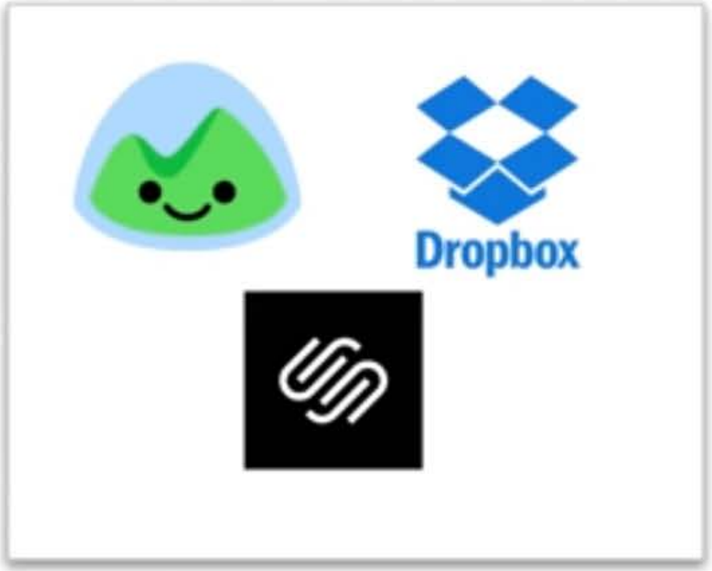
The basic building blocks for cloud IT. Provides access to networking features, computers and data storage space.

Don't worry about IT staff, data centers and hardware.

Cloud Computing Deployment Models

Cloud

Fully utilizing cloud computing



- Startups
- SaaS offerings
- New projects and companies

Hybrid

Using both Cloud and On-Premise

- Banks
- FinTech, Investment Management
- Large Professional Service providers
- Legacy on-premise

On-Premise

Deploying resources on-premises, using virtualization and resource management tools, is sometimes called “private cloud”.

- Public Sector eg. Government
- Super Sensitive Data eg. Hospitals
- Large Enterprise with heavy regulation eg. Insurance Companies

AWS Global Infrastructure

Where does all this Cloud Computing Run?

69 Availability Zones within **22 Geographic Regions** around the world

Way More **Edge Locations** than AZs!

AWS serves over **a million** active customers in **more than 190 countries**

Steadily **expanding** global infrastructure to help customers achieve lower latency and higher throughput

Regions physical location in the world with multiple Availability Zones

Availability Zones one or more discrete data centers

Edge Location datacenter owned by a trusted partner of AWS

Regions

A **geographically distinct** location which has multiple datacenters (AZs)

Every region is **physically isolated** from and independent of every other region in terms of location, power, water supply

Each region has at least ✌️ two AZs

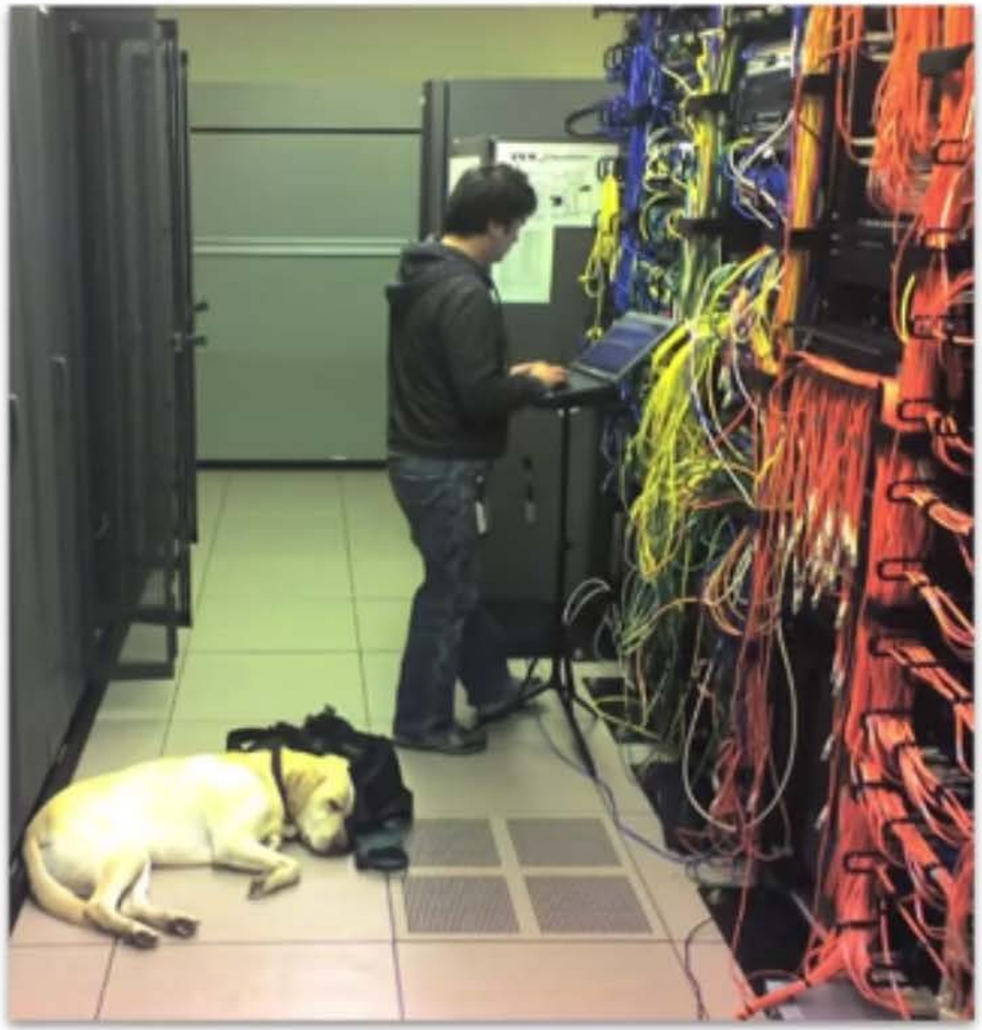
AWS largest region is **US-EAST**

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

Not all services are available in all regions

US-EAST-1 is the region where you see all your billing information

Availability Zones (AZs)



An AZ is a datacenter owned and operated by AWS in which AWS services run

Each region has at least ✌️ two AZs

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

Multi-AZ Distributing your instances across multiple AZs allows failover configuration for handling requests when one goes down.

< 10ms latency between AZs

Edge Locations

Get Data Fast or Upload Data Fast to AWS

An Edge Location is a datacenter owned by a trusted partner of AWS which has a **direct connection** to the AWS network.


These locations serve requests for **CloudFront** and **Route 53**. Requests going to either of these services will be routed to the nearest edge location automatically.


S3 Transfer Acceleration traffic and **API Gateway** endpoint traffic also use the AWS Edge Network.

This allows for **low latency** no matter where the end user is geographically located.

GovCloud (US)

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

GovCloud Regions are only operated by employees who are U.S. citizens, on U.S. soil.

They are **only** accessible to U.S. entities and root account holders who pass a screening process

Customers can architect secure cloud solutions that comply with:

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

EC2 – Pricing Model

On-Demand **Least Commitment**

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

Spot upto 90% **Biggest Savings**

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

Reserved upto 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

Dedicated **Most Expensive**

- Dedicated servers
- Can be on-demand or reserved (upto 70% off)
- When you need a guarantee of isolate hardware (enterprise requirements)

we need to know for lambda so we're gonna take a look at the ec2

EC2 – Reserved Instances (RI)

Best Long-term

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**

Platform: Linux/UNIX | Tenancy: Default | Offering Class: Standard

Instance Type: t2.micro | Term: 12 months - ... | Payment Option: Partial Upfront | Search

Seller	Term	Effective Rate	Upfront Price	Hourly Rate	Payment Option	Offering Class	Quantity Available	Desired Quantity	Normalized units per hour	
AWS	36 months	$0.005	$66.00	$0.002	Partial Upfront	standard	Unlimited	1	0.5	Add to Cart

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 eg. once a week for a few hours. Savings vary

Terms
You commit to a **1 Year** or **3 Year** contract.
The longer the term the greater savings.

Payment Options
All Upfront, **Partial Upfront**, and **No Upfront**
The greater upfront the great the savings

RIs can be **shared between multiple accounts** within an org

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

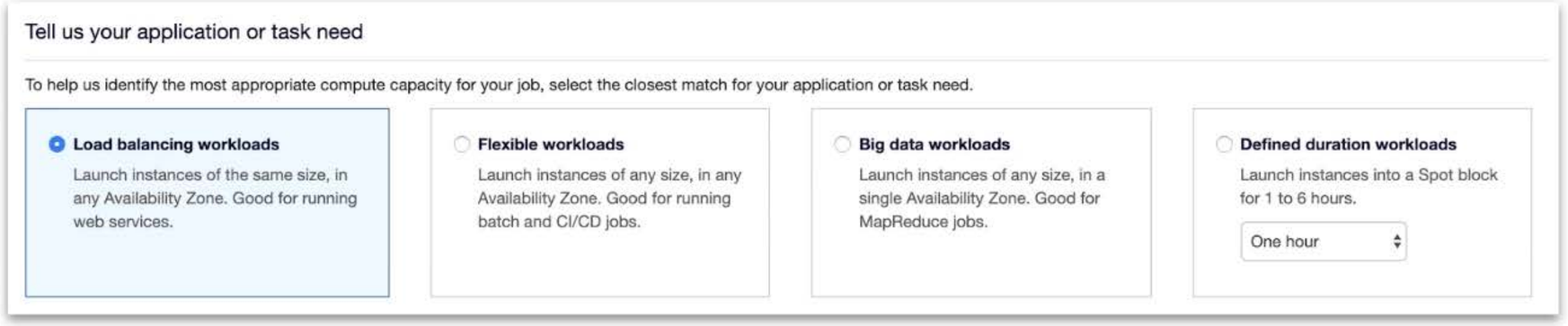
EC2 – Spot Instances

Biggest Savings

AWS has **unused compute capacity** that they want to maximize the utility of their idle servers.
It's like when a hotel offers discounts for to fill vacant suites or planes offer discount to fill vacant seats.

Spot Instances provide a discount of **90%** compared to On-Demand Pricing
Spot Instances can be terminated if the computing capacity is needed by on-demand customers.

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 and convenient way to use Spot Pricing

Termination Conditions

Instances can be terminated by AWS **at anytime**
If your instance is **terminated by AWS**, **you don't get charged** for a partial hour of usage.
If **you terminate** an instance **you will still be charged** for any hour that it ran.

EC2 – 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.

Multi-Tenant vs Single Tenant

When multiple customers are running workloads on the same hardware. **Virtual Isolation** is what separate customers. (think apartment)

Multi-Tenant

When a single customer has dedicated hardware. **Physical Isolation** is what separates customers (think house)

Single-Tenant **Single-Tenant** **Single-Tenant**

Offered in both **On-demand** and **Reserved** (70% off on-demand pricing)

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

EC2 Pricing – *CheatSheet*

- EC2 has for 4 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** upto 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 eg. once a week for a few hours. Savings vary

The Free Services

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

The services are free

However they can provision AWS services which cost money


IAM - Identity Access Management


Amazon VPC


Auto Scaling


CloudFormation


Elastic Beanstalk


Opsworks


Amplify


AppSync


CodeStar


Organizations & Consolidated Billing


AWS Cost Explorer

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

AWS Marketplace

AWS Marketplace is a curated digital catalogue with **thousands** of software listings from independent software vendors.

Easily find, buy, test, and deploy software that already runs on AWS.

The product can be **free** to use or can have an **associated charge**. The charge becomes part of your AWS bill, and once you pay, AWS Marketplace pays the provider.

The sales channel for ISVs and Consulting Partners allows you to **sell your solutions** to other AWS customers.

Products can be offered as

- Amazon Machine Images (AMIs)
- AWS CloudFormation templates
- Software as a service (SaaS) offerings
- Web ACL
- AWS WAF rules

AWS Trusted Advisor

FREE - 7 Trusted Advisor Checks
Business, Enterprise - All Trusted Advisor Checks

Advises you on **security**, **saving money**, **performance**, **service limits** and **fault tolerance**

Think of it like an automated checklist of best practices on AWS

AWS Trusted Advisor

Cost Optimization

Amazon EC2 Reserved Instances Optimization
Low Utilization Amazon EC2 Instances
Underutilized Amazon EBS Volumes
Amazon EC2 Reserved Instance Lease Expiration
Amazon RDS Idle DB Instances
Amazon Route 53 Latency Resource Record Sets
Idle Load Balancers
Unassociated Elastic IP Addresses
Underutilized Amazon Redshift Clusters

Performance

CloudFront Alternate Domain Names
Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration
Amazon EC2 to EBS Throughput Optimization
Amazon Route 53 Alias Resource Record Sets
CloudFront Content Delivery Optimization
CloudFront Header Forwarding and Cache Hit Ratio
High Utilization Amazon EC2 Instances
Large Number of EC2 Security Group Rules Applied to an Instance
Large Number of Rules in an EC2 Security Group
Overutilized Amazon EBS Magnetic Volumes

Security

AWS CloudTrail Logging
IAM Password Policy
MFA on Root Account
Security Groups - Specific Ports Unrestricted
Security Groups - Unrestricted Access
Amazon S3 Bucket Permissions
IAM Access Key Rotation
Amazon EBS Public Snapshots
Amazon RDS Public Snapshots
Amazon RDS Security Group Access Risk
Amazon Route 53 MX Resource Record Sets and Sender Policy Framework
CloudFront Custom SSL Certificates in the IAM Certificate Store
CloudFront SSL Certificate on the Origin Server
ELB Listener Security
ELB Security Groups
Exposed Access Keys
IAM Use

AWS Trusted Advisor

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
ENA 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

Consolidated Billing

One bill for all of your accounts

Consolidate your billing and payment methods **across** multiple AWS accounts into **one bill**

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

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

Consolidated billing is offered at no additional cost!

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

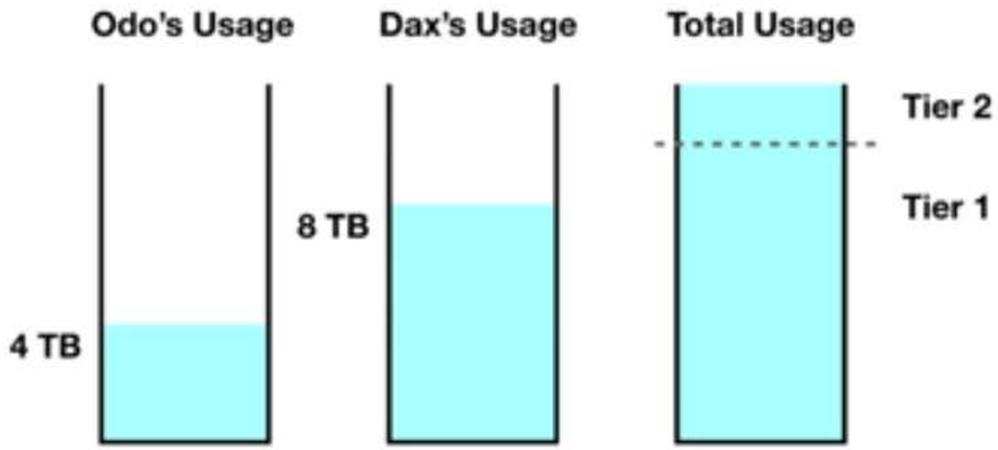
that is all you really need to know for
trust advisors - there you go

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



Data Transfer	
First 10 TB	$0.17 per GB
Next 40 TB	$0.13 per GB

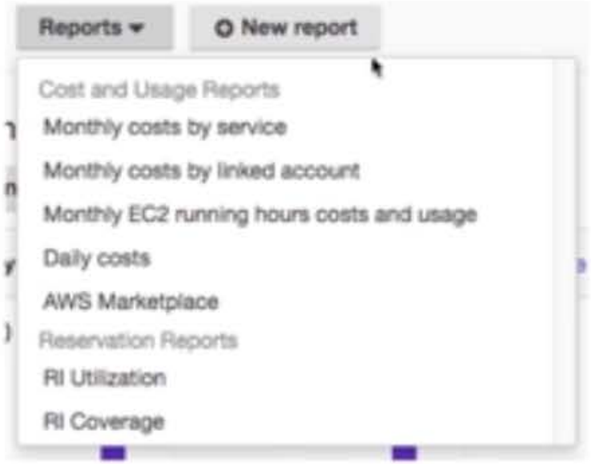
Odo	(4*1024)*0.17	= $696.32
Dax	(8*1024)*0.17	= $1392.64
Unconsolidated	696.32+1392.64	= **$2088.96**
Consolidated	((10*1024)*0.17)+((2*1024)*0.13)	= **$2007.04**

1 TB = 1024 GB

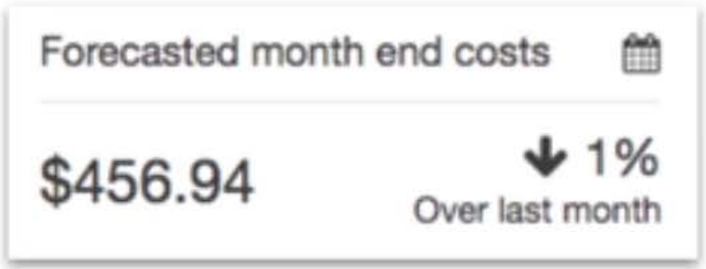
AWS Cost Explorer

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.

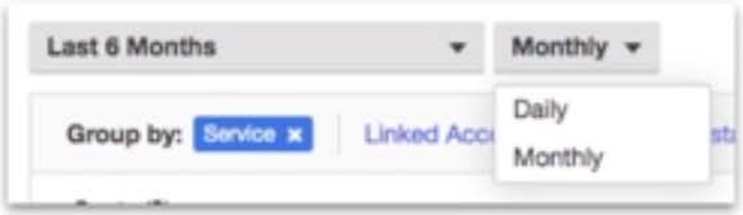


Use **forecasting** to get an idea of future costs

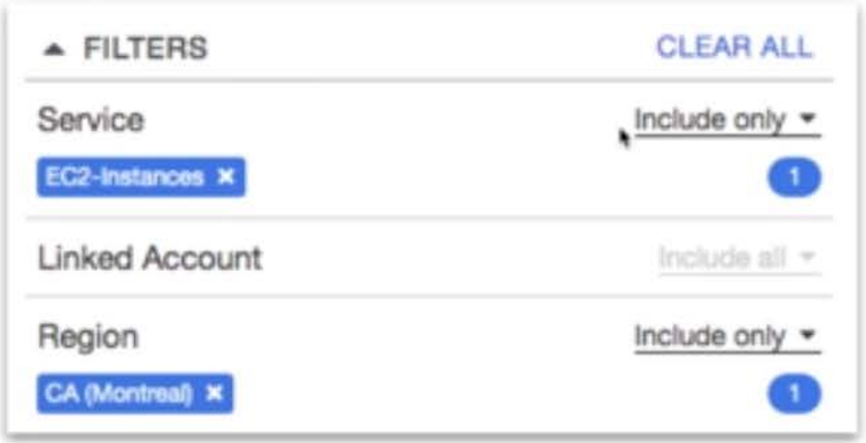


AWS Cost Explorer

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!



there's tons of different ways and you
can also filter based on a lot

AWS Budgets

first two budgets are **free** of charge
Each budget is **$0.02** per day **~0.60 USD / mo**
20,000 budgets limit

Plan your **service usage, service costs and Instance reservations**

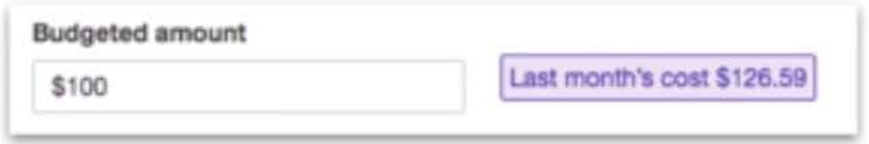
Think of it like an billing alarms on steroids

instance reservations I like to think of
it as building alarms on steroids and

AWS Budgets

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

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



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

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

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

here a little bit more detail and so the
idea here is that you

TCO Calculator

The **T**otal **C**ost of **O**wnership allows you to estimate how much you would save when moving to AWS from on-premise

Provides you **a detailed set of reports** that **can be used in executive presentations**

The tool is built on underlying calculation models that generate fair assessments of value that you can achieve given the data provided.

This TCO helps by reducing the need to invest in large capital expenditures

The tool is for **approximation purposes** only!

Launch the TCO Calculator »

1. Describe Your Environment
2. View 3 Year Summary Of Cost Comparisons
3. Download a full detailed report

AWS Landing Zone

Helps **Enterprises** quickly set-up a secure, AWS multi-account

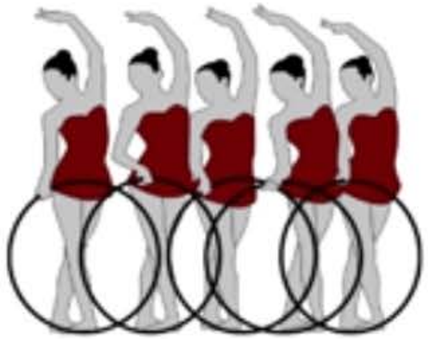
Provides you with a **baseline environment** to get started with a **multi-account architecture**

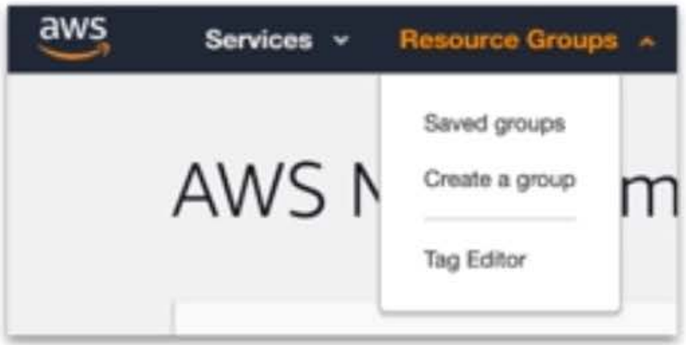
AWS Account Vending Machine (AVM)
Automatically provisions and configure new accounts via  Service Catalog Template
Uses Single Sign-on (SSO) for managing and accessing accounts.

The environment is customizable to allow customers to implement their own account baselines through a Landing Zone configuration and update pipeline

AWS Resource Groups and Tagging

Tags are words or phrases that act as metadata for organizing your AWS resources
Resource Groups are a collection of resources that share one or more **tags**





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

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

- Metrics
- Alarms
- Configuration Settings

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

AWS Quick Starts

Prebuilt templates by AWS and AWS Partners to **help you deploy popular stacks** on AWS

Reduce hundreds of manual procedures into just a few steps

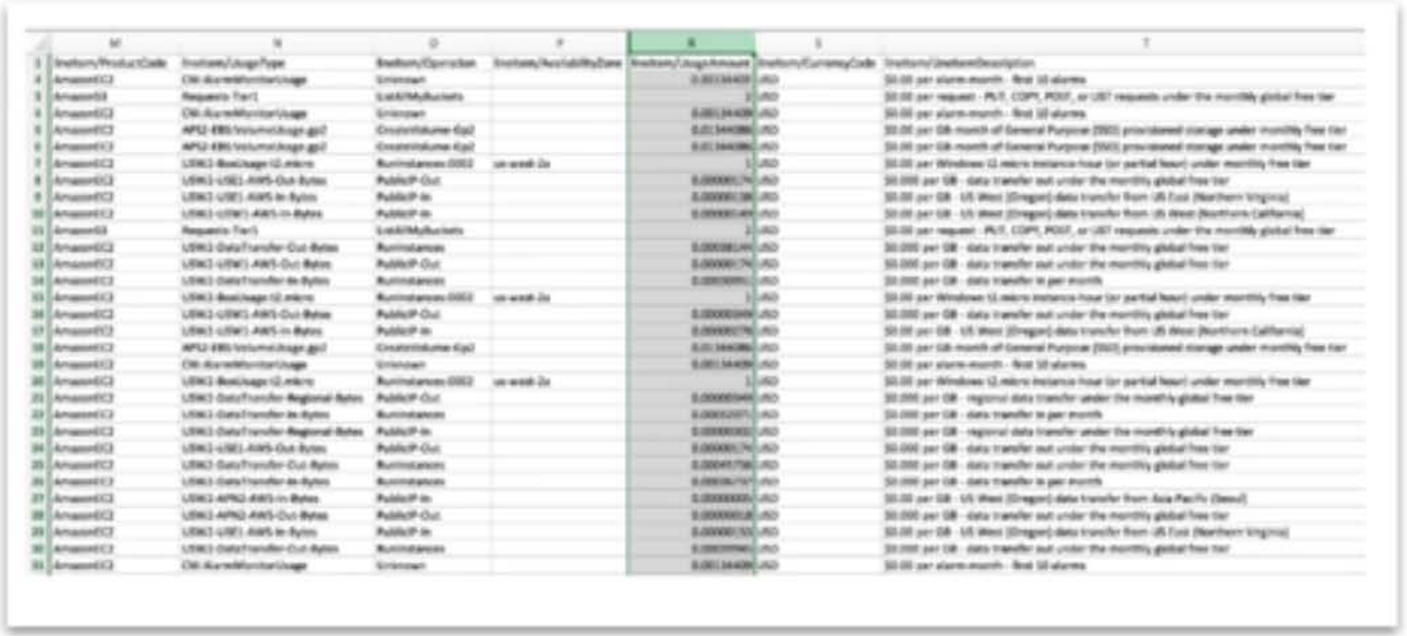
A Quick Start is composed of **3** parts

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

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

AWS Cost and Usage Report

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



Places the reports into S3

Use Athena to turn the report into a queryable database

Use QuickSight to visualize your billing data as graphs

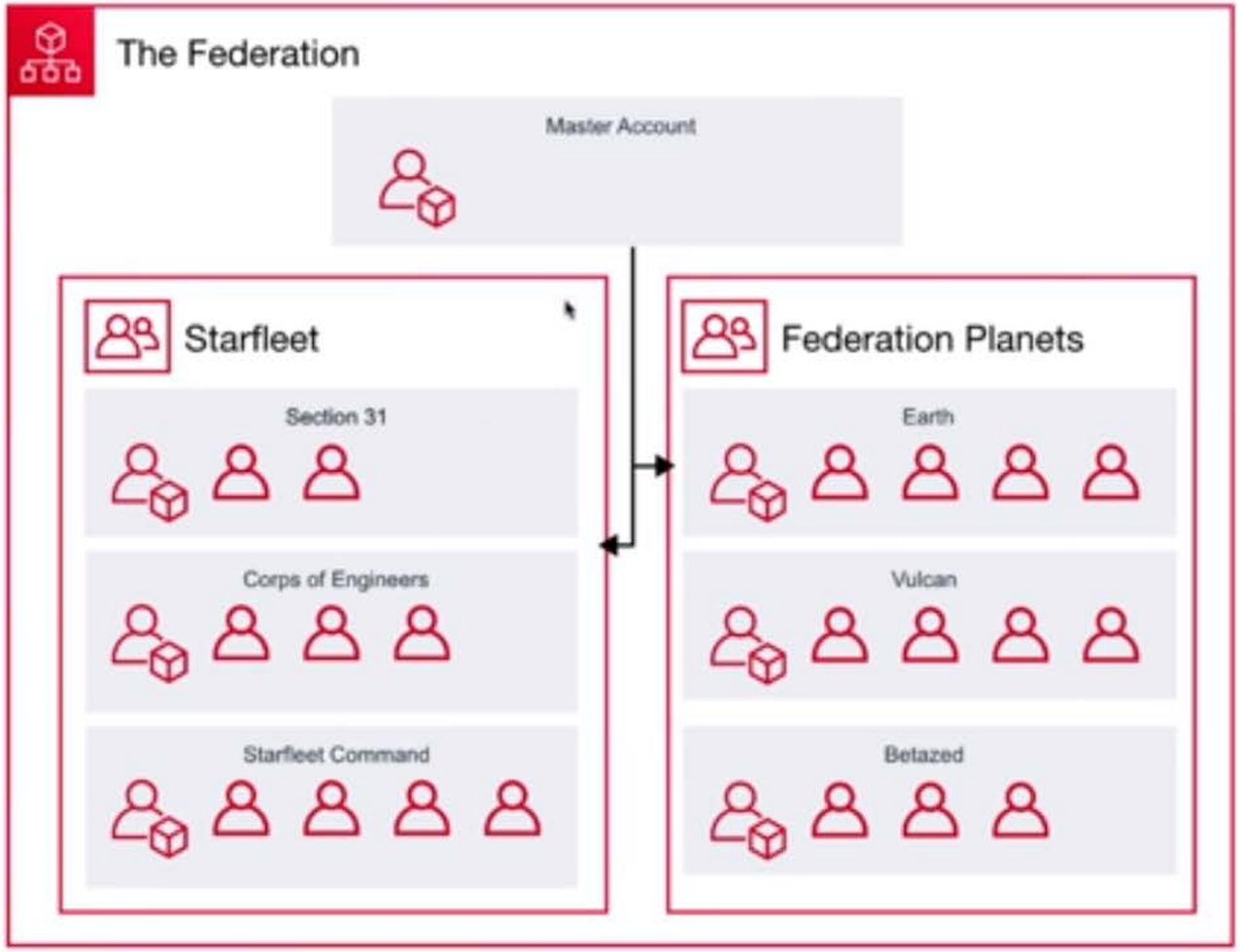
Organizations and Accounts

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 Account User

Organization Units are a group of AWS accounts within an organization which can also contain other organizational units - creating a hierarchy

Service Control Policies give central control over the allowed permissions for all accounts in your organization, helping to ensure your accounts stay within your organization's guidelines.



AWS Networking

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

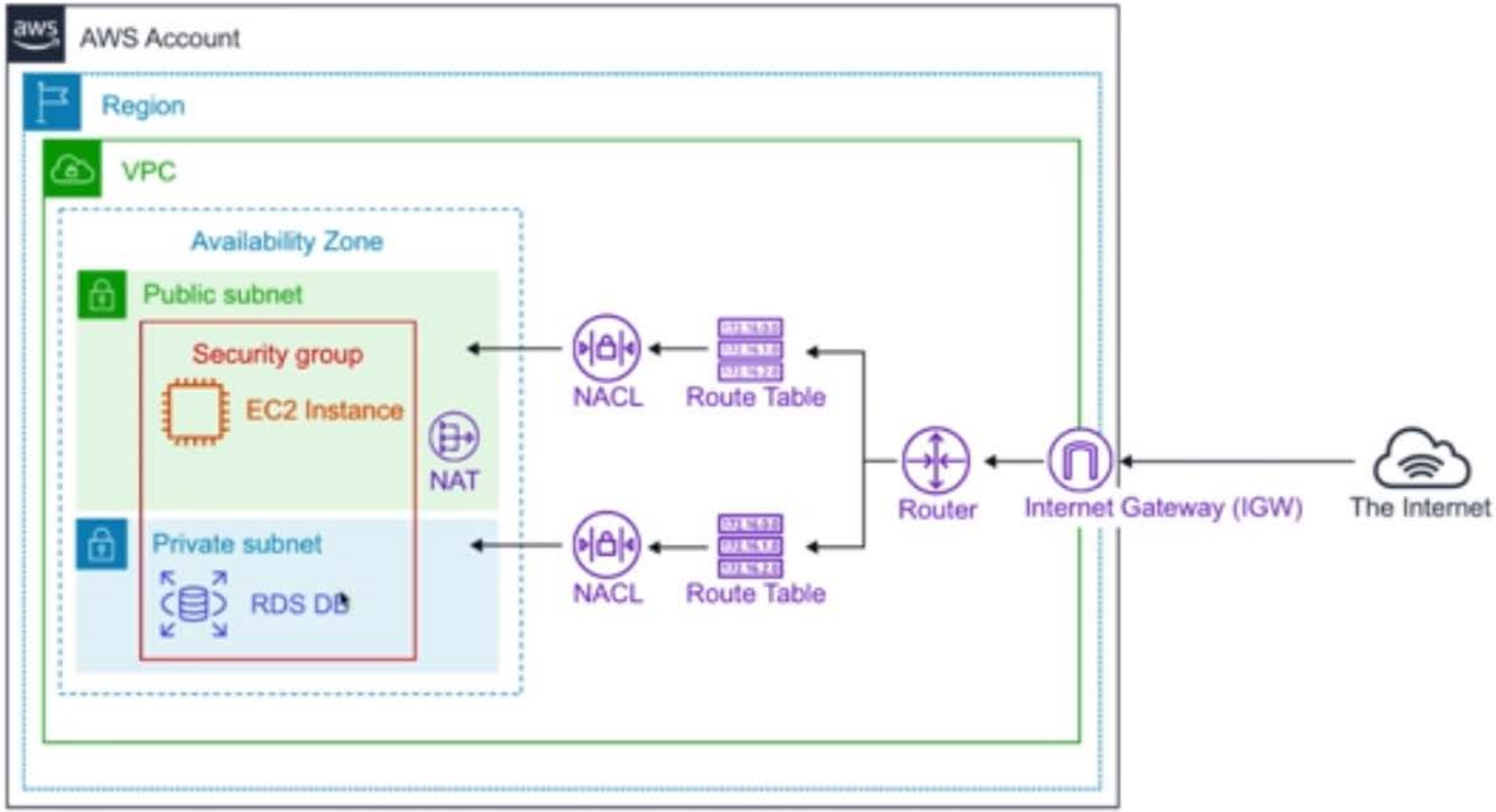
Internet Gateway Enable access to the Internet

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



Database Services

DynamoDB - NoSQL **key/value** database

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

mongoDB

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!!!!!**

ElastiCache - **Redis** or, **Memcached** database

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

heroku

CHEF puppet

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

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. Play 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

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 HHD, Cold HHD

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

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.

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

Who created this bucket?
Who spun up that expensive EC2 instance?
Who launched this SageMaker Notebook?

- Detect developer misconfiguration
- Detect malicious actors
- Automate responses

CloudWatch - is a collection of multiple services

CloudWatch **Logs**	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

Know your Initialisms

IAM Identity and Access Management

S3 Simple Storage Service

SWF Simple Workflow Service

SNS Simple Notification Service

SQS Simple Queue Service

SES Simple Email Service

SSM Simple Systems Manager

RDS Relational Database Service

VPC Virtual Private Cloud

VPN Virtual Private Network

CFN CloudFormation

WAF Web Application Firewall

MQ Amazon ActiveMQ

ASG Auto Scaling Groups

TAM Technical Account Manager

ELB Elastic Load Balancer

ALB Application Load Balancer

NLB Network Load Balancer

EC2 Elastic Cloud Compute

ECS Elastic Container Service

ECR Elastic Container Repository

EBS Elastic Block Storage

EFS Elastic File Storage

EMR Elastic MapReduce

EB Elastic Beanstalk

ES Elasticsearch

EKS Elastic **Kubernetes** Service

MKS Managed **Kafka** Service

IoT Internet of Things

RI Reserved Instances

Shared Responsibility Model

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

IN

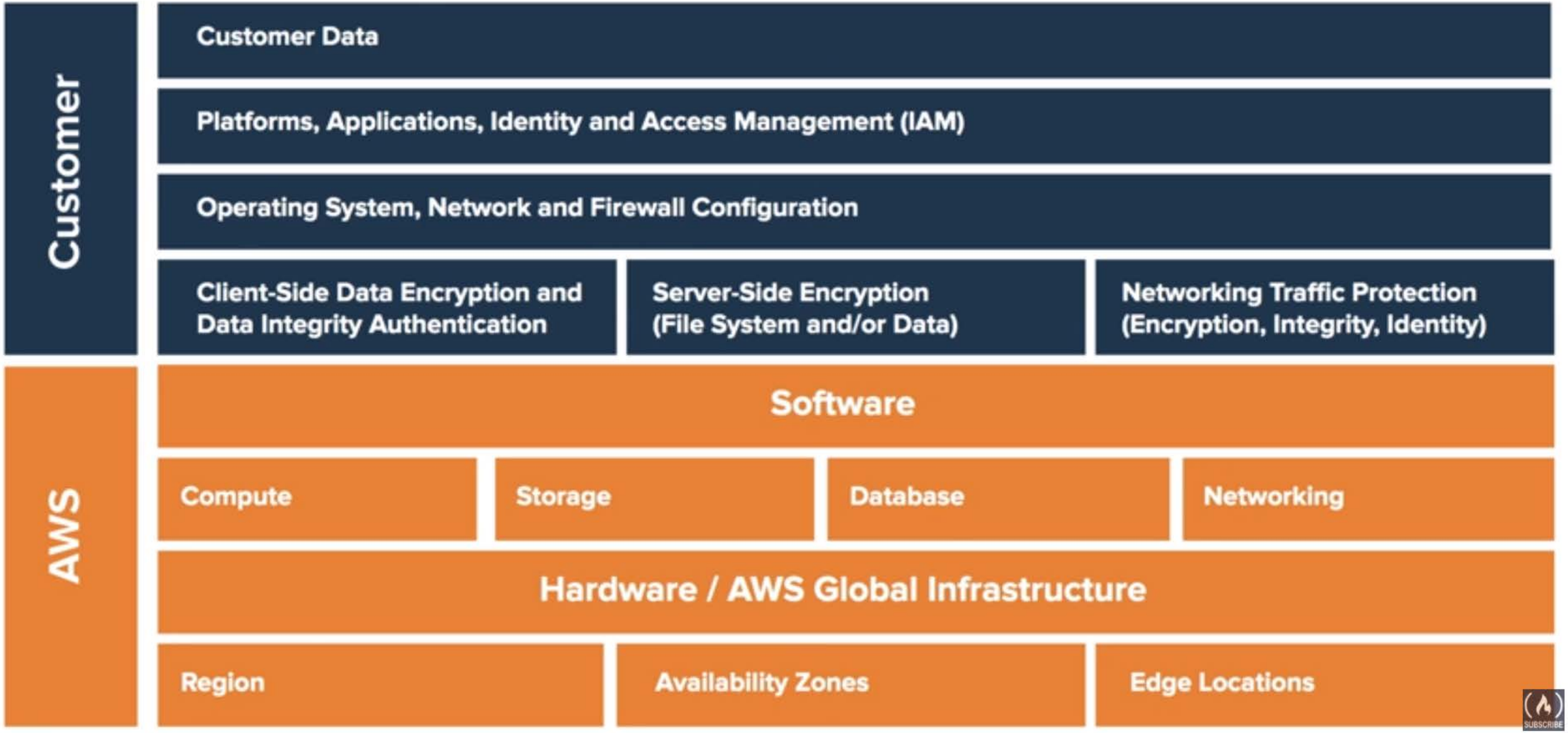
- Data
- Configuration

OF

- Hardware
- Operation of Managed Services
- Global Infrastructure

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

Shared Responsibility Model



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?

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

AICPA SOC · ISO 27001 · PCI · C5 · irap · FedRAMP

Amazon Inspector

How do we prove an EC2 Instance is harden?

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

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

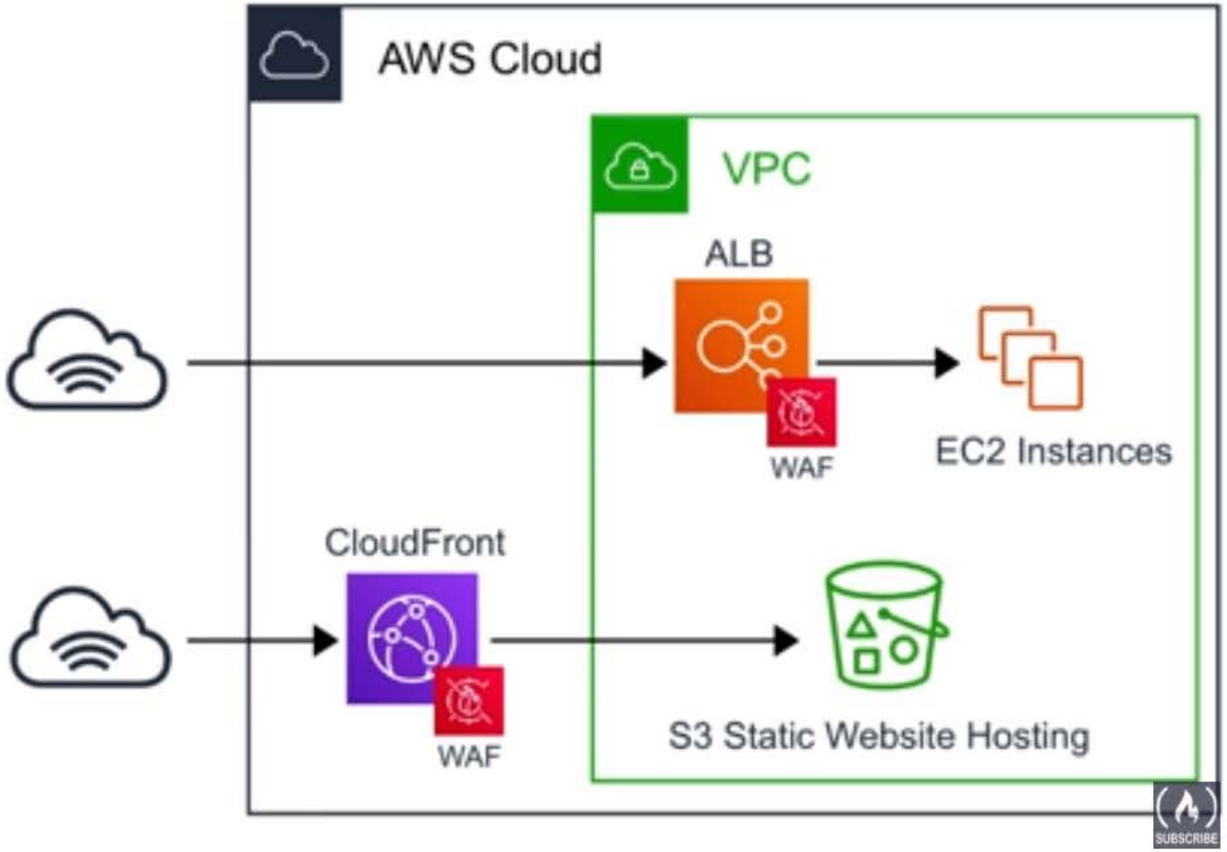
Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Rules Marketplace

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:

OWASP Open Web Application Security Project

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

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

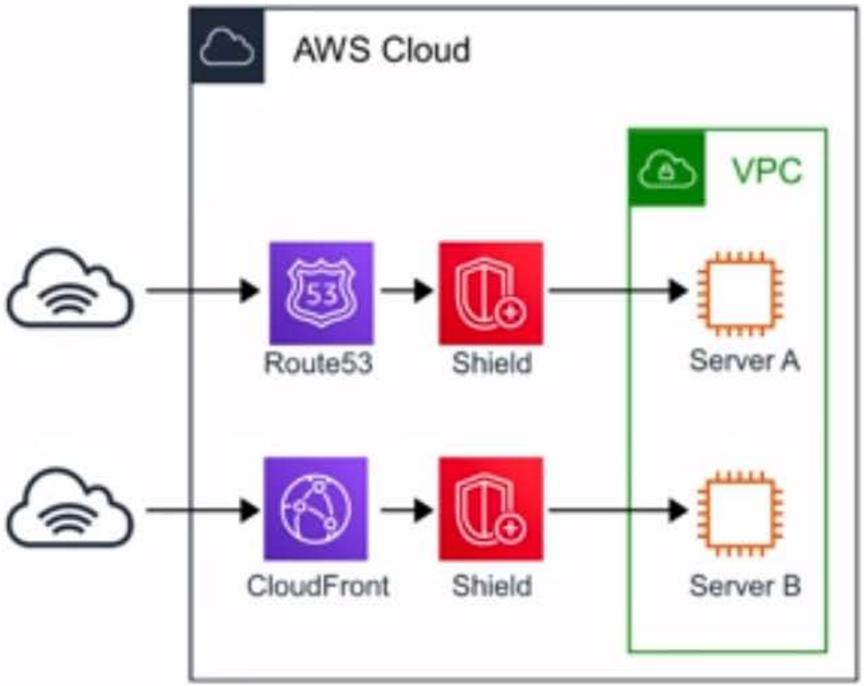
What is a DDOS attack?
A malicious attempt to disrupt normal traffic by flooding a website a large amount of fake traffic

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

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)

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.

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

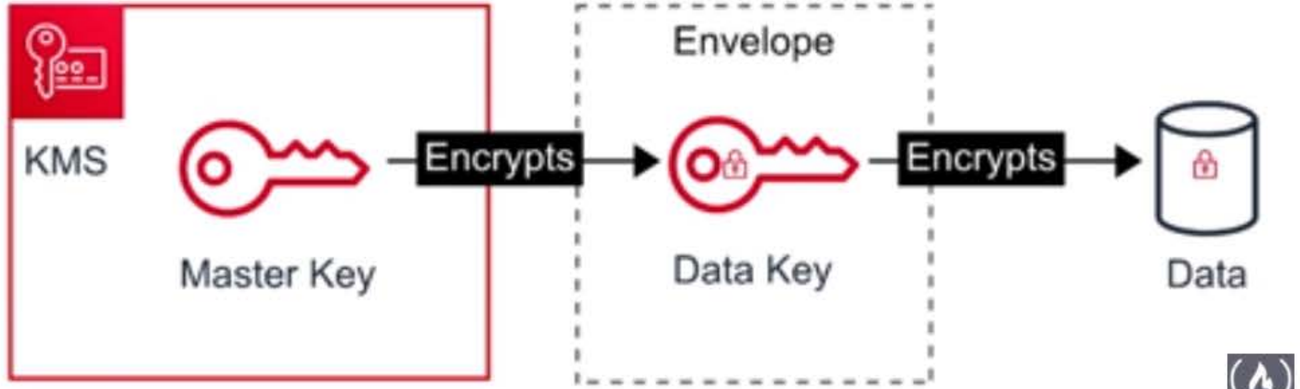
It will alert you of **Findings** which you can automate a incident response via CloudWatch Events or with 3rd Party Services

Key Management Service (KMS)

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.

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

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

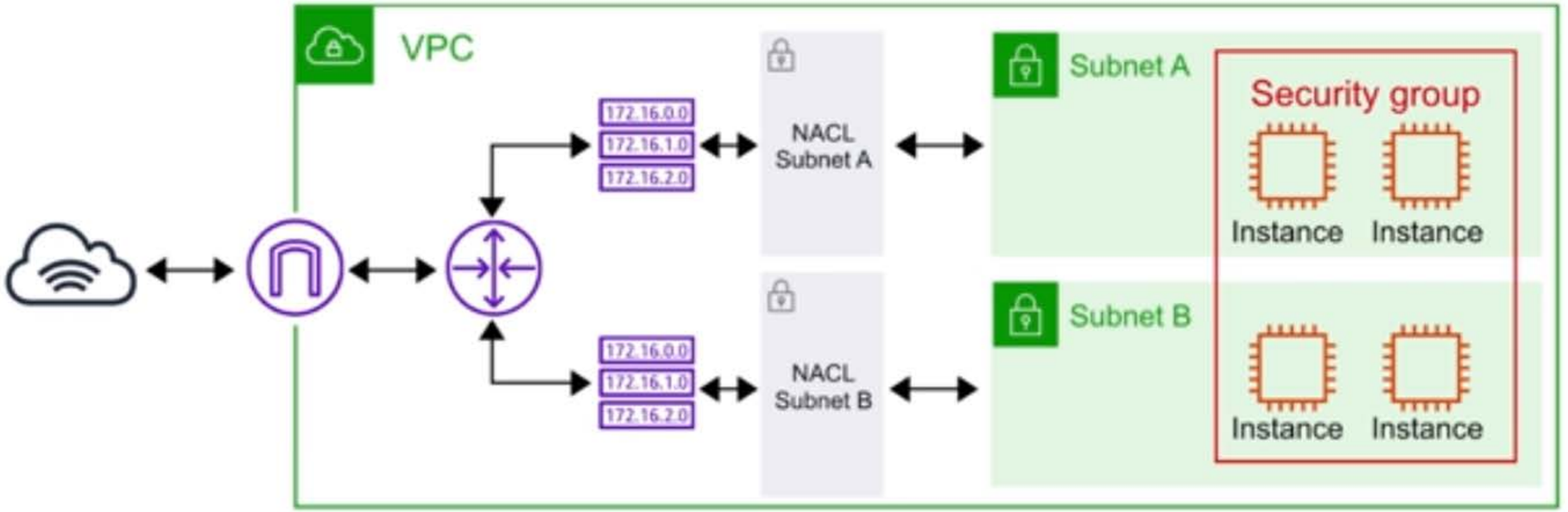
NACLs

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* 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 servers 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

Virtual Private Network (VPN)

lets you establish a secure and **private tunnel** from your network or device to the AWS global network

AWS Site-to-Site VPN

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

AWS Client VPN

securely connect users to AWS or on-premises networks

*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 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

Both services transcodes videos

Elastic Transcoder

The old way

Transcodes videos to streaming formats

AWS Elemental MediaConvert

The new way

Transcodes videos to streaming formats

Overlays images

Insert videos clips

Extracts captions data

Robust UI

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

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

RabbitMQ

Sidekiq

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

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

RabbitMQ

Sidekiq

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 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

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 receives inbound emails

SES can create Email Templates

Custom domain name email

Monitor your email reputation

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

VPC endpoint

A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses. Traffic between your VPC and the other service does not leave the Amazon network. A VPC endpoint does not require an internet gateway, virtual private gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service.

VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components. They allow communication between instances in your VPC and services without imposing availability risks.

The following are the different types of VPC endpoints. You create the type of VPC endpoint that's required by the supported service.

Interface endpoints - An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service. Interface endpoints are powered by AWS PrivateLink. You can also view all of the available AWS service names.

Gateway Load Balancer endpoints - A Gateway Load Balancer endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. Gateway Load Balancer endpoints are powered by AWS PrivateLink. This type of endpoint serves as an entry point to intercept traffic and route it to a service that you've configured using Gateway Load Balancers, for example, for security inspection. You specify a Gateway Load Balancer endpoint as a target for a route in a route table. Gateway Load Balancer endpoints are supported for endpoint services that are configured for Gateway Load Balancers only.

Gateway endpoints - A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. Gateway endpoints are supported for AWS services only. The following AWS services are supported:

- Amazon S3
- DynamoDB

5 PILLARS OF AWS WELL-ARCHITECTED FRAMEWORK

1. Operational Excellence

The Operational Excellence pillar includes the ability to support development and run workloads effectively, gain insight into their operation, and continuously improve supporting processes and procedures to delivery business value. You can find prescriptive guidance on implementation in the Operational Excellence Pillar whitepaper.

Design Principles

There are five design principles for operational excellence in the cloud:

- Perform operations as code
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

Best Practices

Operations teams need to understand their business and customer needs so they can support business outcomes. Ops creates and uses procedures to respond to operational events, and validates their effectiveness to support business needs. Ops also collects metrics that are used to measure the achievement of desired business outcomes.

Everything continues to change—your business context, business priorities, customer needs, etc. It's important to design operations to support evolution over time in response to change and to incorporate lessons learned through their performance.

2. Security

The Security pillar includes the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security. You can find prescriptive guidance on implementation in the Security Pillar whitepaper.

Design Principles - There are seven design principles for security in the cloud:

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Best Practices

Before you architect any workload, you need to put in place practices that influence security. You'll want to control who can do what. In addition, you want to be able to identify security incidents, protect your systems and services, and maintain the confidentiality and integrity of data through data protection.

You should have a well-defined and practiced process for responding to security incidents. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

The AWS Shared Responsibility Model enables organizations that adopt the cloud to achieve their security and compliance goals. Because AWS physically secures the infrastructure that supports our cloud services, as an AWS customer you can focus on using services to accomplish your goals. The AWS Cloud also provides greater access to security data and an automated approach to responding to security events.

3. Reliability

The Reliability pillar encompasses the ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle. You can find prescriptive guidance on implementation in the Reliability Pillar whitepaper.

Design Principles

There are five design principles for reliability in the cloud:

- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change in automation

Best Practices

To achieve reliability, you must start with the foundations—an environment where service quotas and network topology accommodate the workload. The workload architecture of the distributed system must be designed to prevent and mitigate failures. The workload must handle changes in demand or requirements, and it must be designed to detect failure and automatically heal itself.

Before architecting any system, foundational requirements that influence reliability should be in place. For example, you must have sufficient network bandwidth to your data center. These requirements are sometimes neglected (because they are beyond a single project's scope).

This neglect can have a significant impact on the ability to deliver a reliable system. In an on-premises environment, these requirements can cause long lead times due to dependencies and therefore must be incorporated during initial planning.

With AWS, most of these foundational requirements are already incorporated or may be addressed as needed. The cloud is designed to be essentially limitless, so it is the responsibility of AWS to satisfy the requirement for sufficient networking and compute capacity, while you are free to change resource size and allocation, such as the size of storage devices, on demand.

4. Performance Efficiency

The Performance Efficiency pillar includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve. You can find prescriptive guidance on implementation in the Performance Efficiency Pillar whitepaper.

Design Principles

There are five design principles for performance efficiency in the cloud:

- Democratize advanced technologies
- Go global in minutes
- Use serverless architectures
- Experiment more often
- Consider mechanical sympathy

Best Practices

Take a data-driven approach to building a high-performance architecture. Gather data on all aspects of the architecture, from the high-level design to the selection and configuration of resource types.

Reviewing your choices on a regular basis ensures you are taking advantage of the continually evolving AWS Cloud. Monitoring ensures you are aware of any deviance from expected performance. Make trade-offs in your architecture to improve performance, such as using compression or caching, or relaxing consistency requirements

The optimal solution for a particular workload varies, and solutions often combine multiple approaches. Well-Architected workloads use multiple solutions and enable different features to improve performance

5. Cost Optimization

The Cost Optimization pillar includes the ability to run systems to deliver business value at the lowest price point. You can find prescriptive guidance on implementation in the Cost Optimization Pillar whitepaper.

Design Principles

There are five design principles for cost optimization in the cloud:

- Implement cloud financial management
- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on undifferentiated heavy lifting
- Analyze and attribute expenditure

Best Practices

As with the other pillars, there are trade-offs to consider. For example, do you want to optimize for speed to market or for cost? In some cases, it's best to optimize for speed—going to market quickly, shipping new features, or simply meeting a deadline—rather than investing in up-front cost optimization.

Design decisions are sometimes directed by haste rather than data, and as the temptation always exists to overcompensate rather than spend time benchmarking for the most cost-optimal deployment. This might lead to over-provisioned and under-optimized deployments. Using the appropriate services, resources, and configurations for your workloads is key to cost savings

Conclusion - The AWS Well-Architected Framework provides architectural best practices across the five pillars for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. The framework provides a set of questions that allows you to review an existing or proposed architecture. It also provides a set of AWS best practices for each pillar.

Using the Framework in your architecture helps you produce stable and efficient systems, which allows you to focus on functional requirements.

SHARED RESPONSIBILITY MODEL

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.
AWS responsibility "Security of the Cloud" - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required. Below are examples of controls that are managed by AWS, AWS Customers and/or both.

Inherited Controls – Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

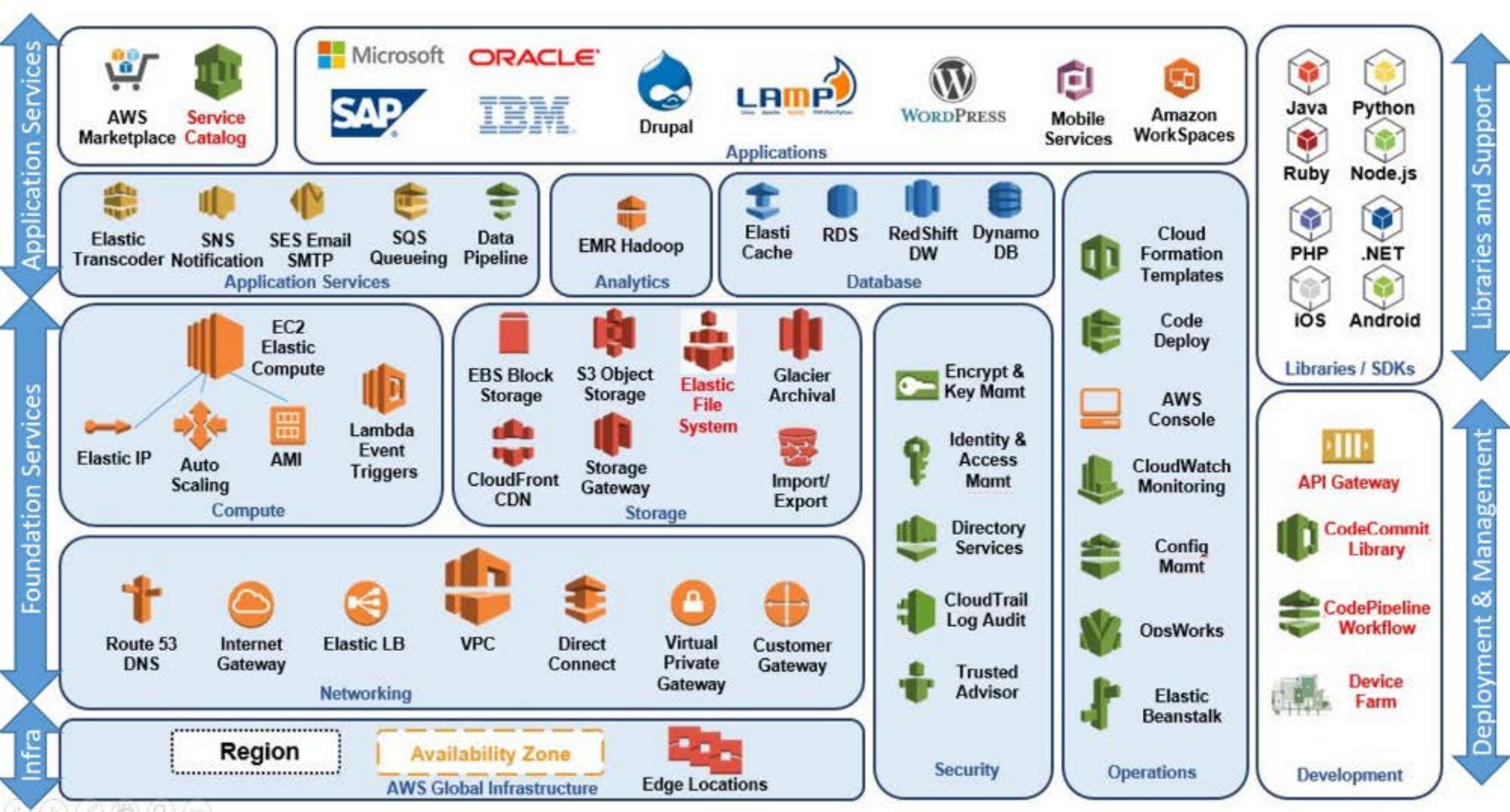
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

Customer Specific – Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

	Basic	**Developer**	**Business**	**Enterprise**
Non-technical Customer Service and Communities	Business hours* access to customer service, documentation and whitepapers	Business hours* access to customer service, documentation and whitepapers	Business hours* access to customer service, documentation and whitepapers	Business hours* access to customer service, documentation and whitepapers
Best Practices	Access to 2 core Trusted Advisor checks	Access to 2 core Trusted Advisor checks	Access to full set of Trusted Advisor checks	Access to full set of Trusted Advisor checks
Technical Support		Business hours* access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat & phone	24x7 access to Sr. Cloud Support Engineers via email, chat & phone
Who Can Open Cases	One primary contact/ Unlimited cases	One primary contact/ Unlimited cases	Unlimited contacts/ Unlimited cases (IAM supported)	Unlimited contacts/ Unlimited cases (IAM supported)
Case Severity/Response Times	General Guidance: < 24 business hours	System Impaired: < 12 business hours General Guidance: < 24 business hours	Production System Down: < 1 hour Production System Impaired: < 4 hours System Impaired: < 12 hours General Guidance: < 24 hours	Business-Critical System Down: < 15 minutes Production System Down: < 1 hour Production System Impaired: < 4 hours System Impaired: < 12 hours General Guidance: < 24 hours
Architecture Support		General guidance	Contextual guidance based on your use-case	Consultative review and guidance based on your applications and solutions
Launch Support			Infrastructure Event Management (Available for additional fee)	Infrastructure Event Management (Included)

Programmatic Case Management			AWS Support API	AWS Support API
Third-Party Software Support			Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting
Operations Support				Operational reviews, recommendations, and reporting
Account Assistance				Assigned Support Concierge
Proactive Guidance				Designated Technical Account Manager
Pricing**	Included	Greater of ¥299 - or - 3% of monthly AWS charges	Greater of ¥599 - or - • 10% of monthly AWS charges for the first ¥0 to ¥60,000 • 7% of monthly AWS charges above ¥60,000 to ¥500,000 • 5% of monthly AWS charges above ¥500,000 to ¥1,500,000 • 3% of monthly AWS charges above ¥1,500,000	Greater of ¥100,000 - or - • 10% of monthly AWS charges for the first ¥0 to ¥1,000,000 • 7% of monthly AWS charges above ¥1,000,000 to ¥3,000,000 • 5% of monthly AWS charges above ¥3,000,000 to ¥6,000,000 • 3% of monthly AWS charges above ¥6,000,000


Application Services
Foundation Services
Infra
AWS Marketplace
Service Catalog
Microsoft
ORACLE
SAP
IBM
Drupal
LAMP
WordPress
Mobile Services
Amazon WorkSpaces
Applications
Elastic Transcoder
SNS Notification
SES Email SMTP
SQS Queueing
Data Pipeline
Application Services
EMR Hadoop
Analytics
Elasti Cache
RDS
RedShift DW
Dynamo DB
Database
Java
Python
Ruby
Node.js
PHP
.NET
iOS
Android
Libraries / SDKs
Libraries and Support
EC2 Elastic Compute
Elastic IP
Auto Scaling
AMI
Lambda Event Triggers
Compute
EBS Block Storage
S3 Object Storage
Elastic File System
Glacier Archival
CloudFront CDN
Storage Gateway
Import/ Export
Storage
Encrypt & Key Mgmt
Identity & Access Mgmt
Directory Services
CloudTrail Log Audit
Trusted Advisor
Security
Cloud Formation Templates
Code Deploy
AWS Console
CloudWatch Monitoring
Config Mgmt
OpsWorks
Elastic Beanstalk
Operations
API Gateway
CodeCommit Library
CodePipeline Workflow
Device Farm
Development
Deployment & Management
Route 53 DNS
Internet Gateway
Elastic LB
VPC
Direct Connect
Virtual Private Gateway
Customer Gateway
Networking
Region
Availability Zone
AWS Global Infrastructure
Edge Locations