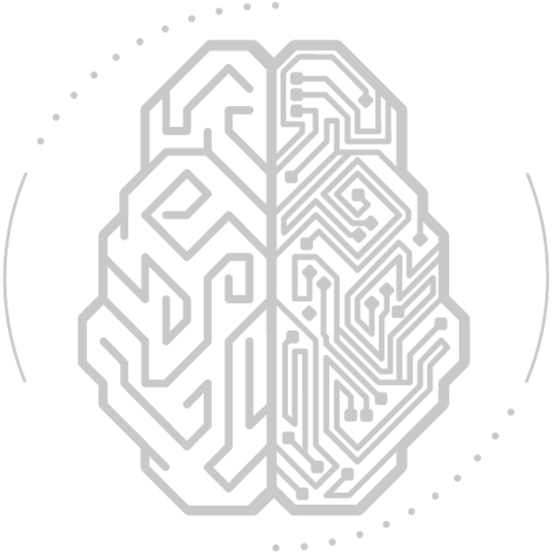
Cloud Practitioner



Date: 25th Sept 2021

What's in it for you

AWS Cloud Practitioner	
S.No.	Agenda
1	AWS Services - Serverless
2	AWS Services - Database
3	AWS Services - Glue
4	AWS Services - VPC
5	AWS Services - Cloudformation
6	AWS Services - Cloud Integration
7	AWS Services - Developer Tools
8	AWS Services - Monitoring
9	AWS Shared Responsibility
10	AWS Well Architected Review

aws CERTIFIED

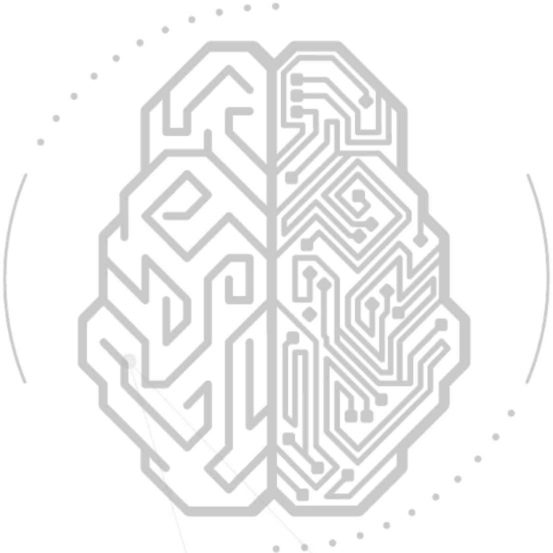
Cloud Practitioner

Speaker

Sanchit Jain

Lead Architect - AWS at Quantiphi
AWS APN Ambassador

AWS Services - Serverless



What is serverless?

What is Serverless?

a cloud-native platform

for

short-running, stateless computation

and

event-driven applications

which

scales up and down instantly and automatically

and

charges for actual usage at a millisecond granularity

Greater Agility

Less Overhead

Better Focus

Increased Scale

More Flexibility

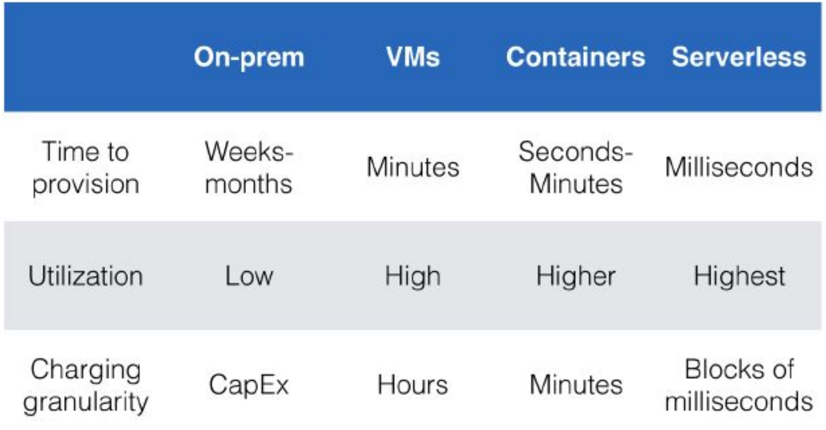
Faster Time To Market

Why is Serverless attractive?

- Server-less means no servers? Or worry-less about servers?
- Runs code **only** on-demand on a per-request basis
- Making app development & ops dramatically faster, cheaper, easier
- Drives infrastructure cost savings

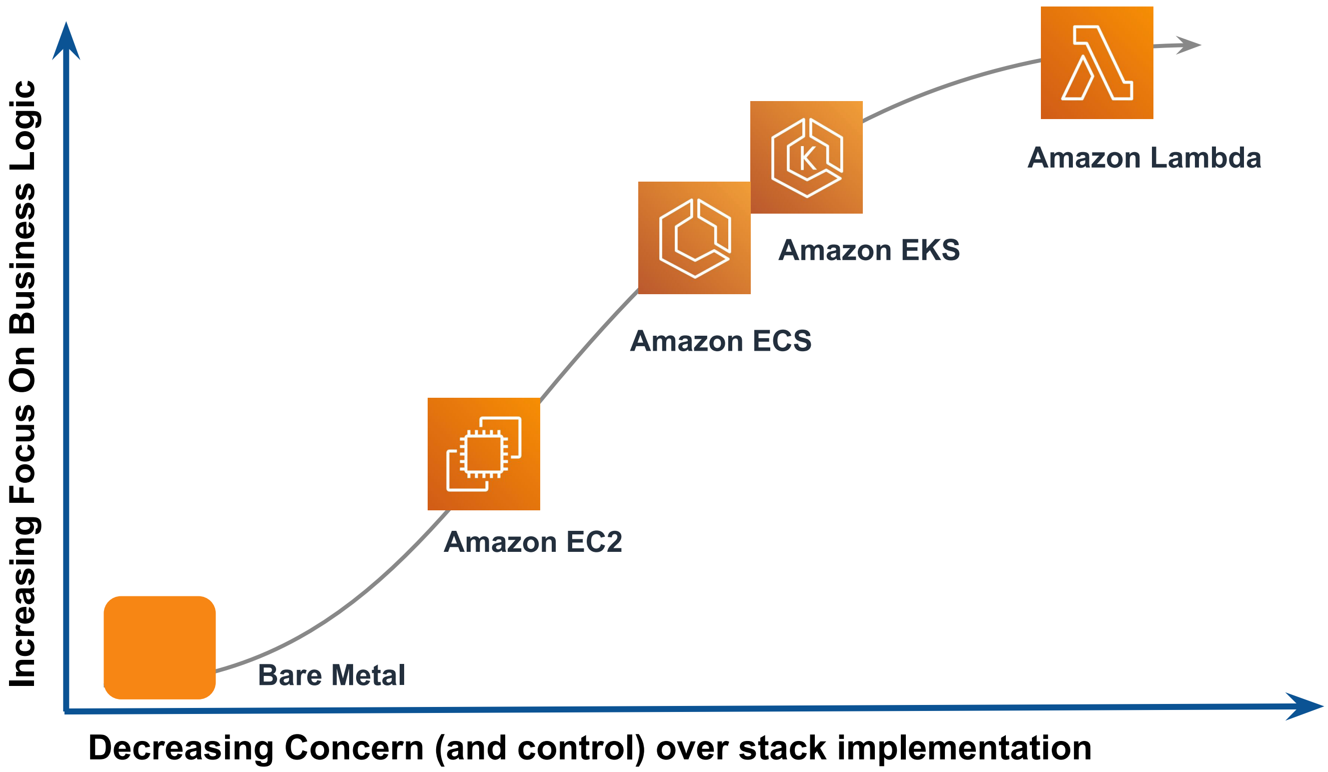
No servers

Just code



	On-prem	VMs	Containers	Serverless
Time to provision	Weeks-months	Minutes	Seconds-Minutes	Milliseconds
Utilization	Low	High	Higher	Highest
Charging granularity	CapEx	Hours	Minutes	Blocks of milliseconds

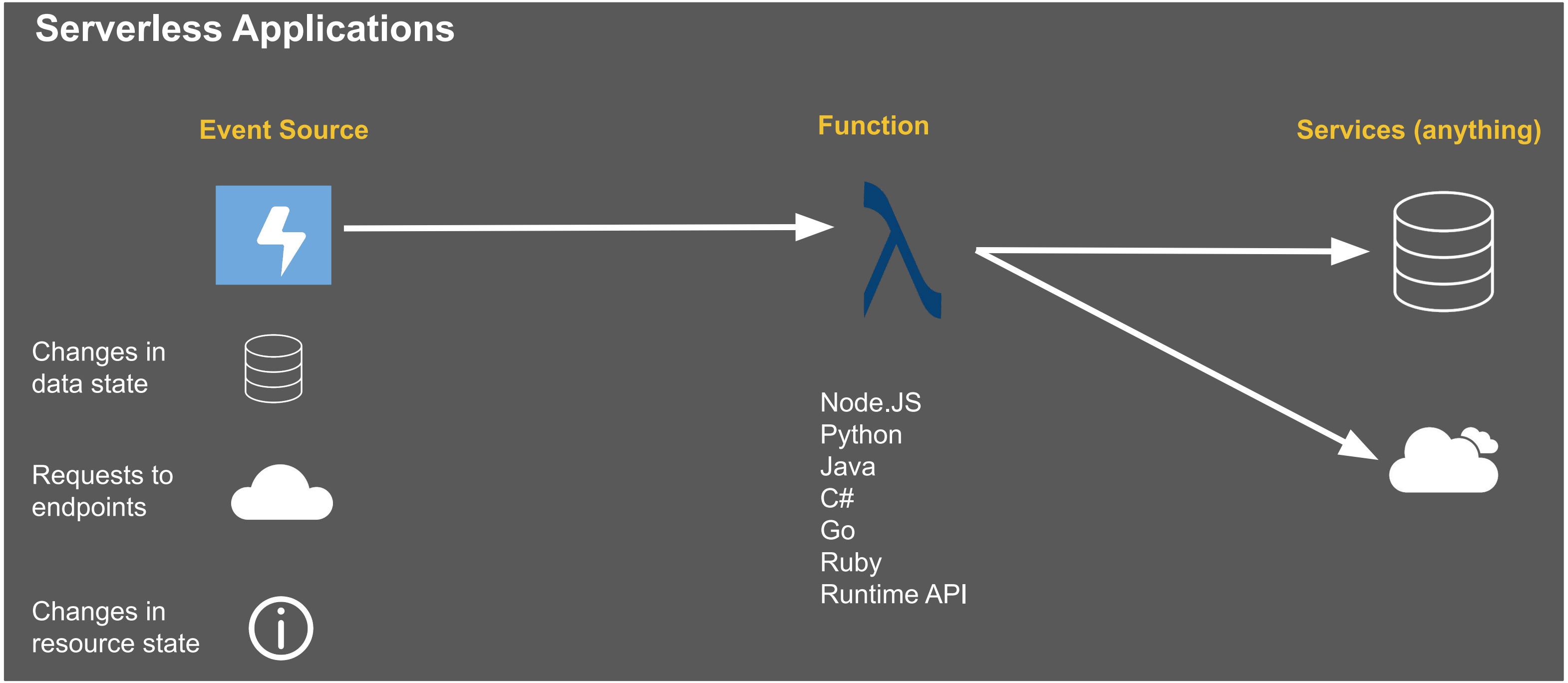
Where Serverless Stands?



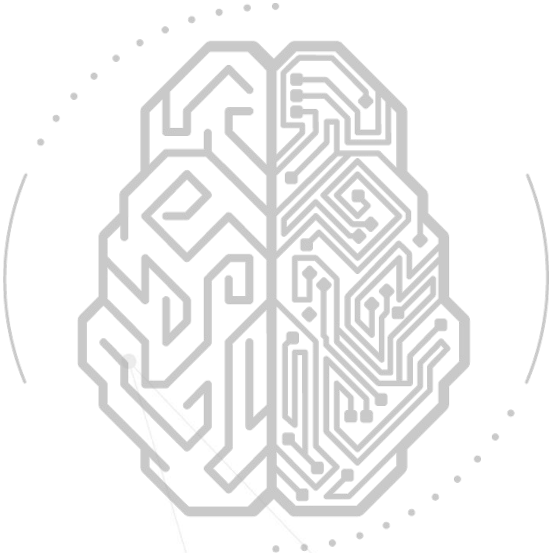
Amazon Lambda
Amazon EKS
Amazon ECS
Amazon EC2
Bare Metal
Increasing Focus On Business Logic
Decreasing Concern (and control) over stack implementation

What triggers code execution?

- Runs code in response to events
- Event-programming model



AWS Services - Database



AWS Services - Database: RDS

- Amazon Relational Database Service (Amazon RDS) is a service that makes it easier to operate, and scale a relational database in the cloud.

- It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

- It manages backups, software patching, automatic failure detection, and recovery by itself. You can have automated backups performed when you need them, or manually create your own backup snapshot

- In addition to the security in your database package, you can help control who can access your RDS databases by using AWS Identity and Access Management (IAM) to define users and permissions

- Different Database Engine - Amazon Aurora, Microsoft SQL Server, MySQL, MariaDB, PostgreSQL, and Oracle

- High Availability (Multi-AZ) - Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support.
  - Multi-AZ deployments : Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology
  - SQL Server DB instances use SQL Server Mirroring

- **Backup -** Amazon RDS creates and saves automated backups of your DB instance during the specified backup window. Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Automated backups follow these rules:
  - DB instance must be in the ACTIVE state for automated backups to occur.
  - Automated backups don't occur while a copy is executing in the same region for the same DB instance

AWS Services - Athena

- Amazon Athena is a Serverless Interactive Query Service. You can accomplish these tasks using the AWS Management Console, which is a simple and intuitive web interface.
- Amazon Athena uses Presto, a distributed SQL engine, works with a variety of standard data formats
- Amazon Athena stores tables as objects in S3. Define a schema for the file and start querying
- Types of standard data formats supported - CSV, json, AVRO, Apache Parquet, and ORC
- Athena queries works faster by compressing or partitioning the data, cost incurred is less since less amount of data is scanned.
- Athena Pricing
  - Charges for Athena is per query
  - You are billed according to amount of data scanned by the query. Minimum 10MB
  - $5 per 1TB of data scanned. Compression/ partitioning reduces amount of data scanned
  - No charges for failed queries. Cancelled queries charged for amount of data scanned
  - Amazon Athena queries data directly from Amazon S3, so your source data is billed at S3 rates.

AWS Services - Redshift

- Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. Its datasets range from 100s of gigabytes to a petabyte.
- The Amazon Redshift service manages all of the work of setting up, operating, and scaling a data warehouse. These tasks include provisioning capacity, monitoring and backing up the cluster, and applying patches and upgrades to the Amazon Redshift engine.
- An Amazon Redshift cluster is a set of nodes, which consists of a **leader node** and one or more **compute nodes**.
- The type and number of compute nodes that you need depends on the size of your data, the number of queries you will execute, and the query execution performance that you need.
- Features of Amazon Redshift – Supports VPC, Encryption at Rest, Encryption in Transit, Scalable, and Cost-effective
- Backup - Snapshots are point-in-time backups of a cluster. There are two types of snapshots: automated and manual.
- Cost Optimization - On-Demand pricing, Amazon Redshift Spectrum, Concurrency Scaling pricing, and Reserved Instance pricing

AWS Services - DynamoDB

- Amazon DynamoDB is a key-value and document database (NoSql) that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-active, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications.

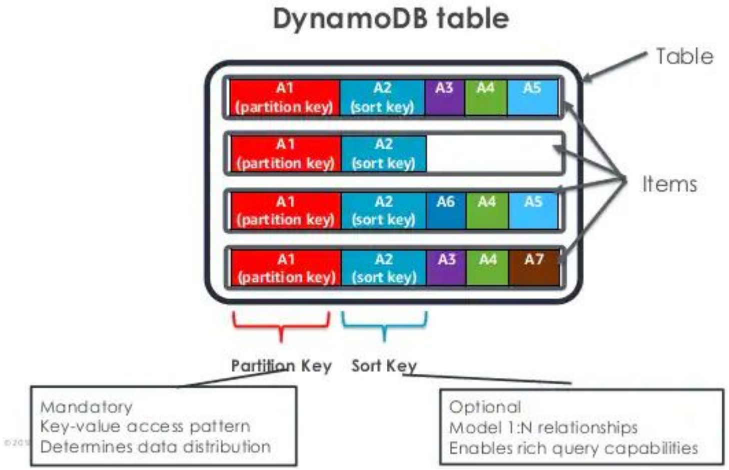
- DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second

- **Primary Key -** Two types of primary key
  - Partition Key (Hash Key) will help determine the physical location of data.
  - Composite key: Partition Key (Hash Key) & Sort Key (Range key – e.g date)

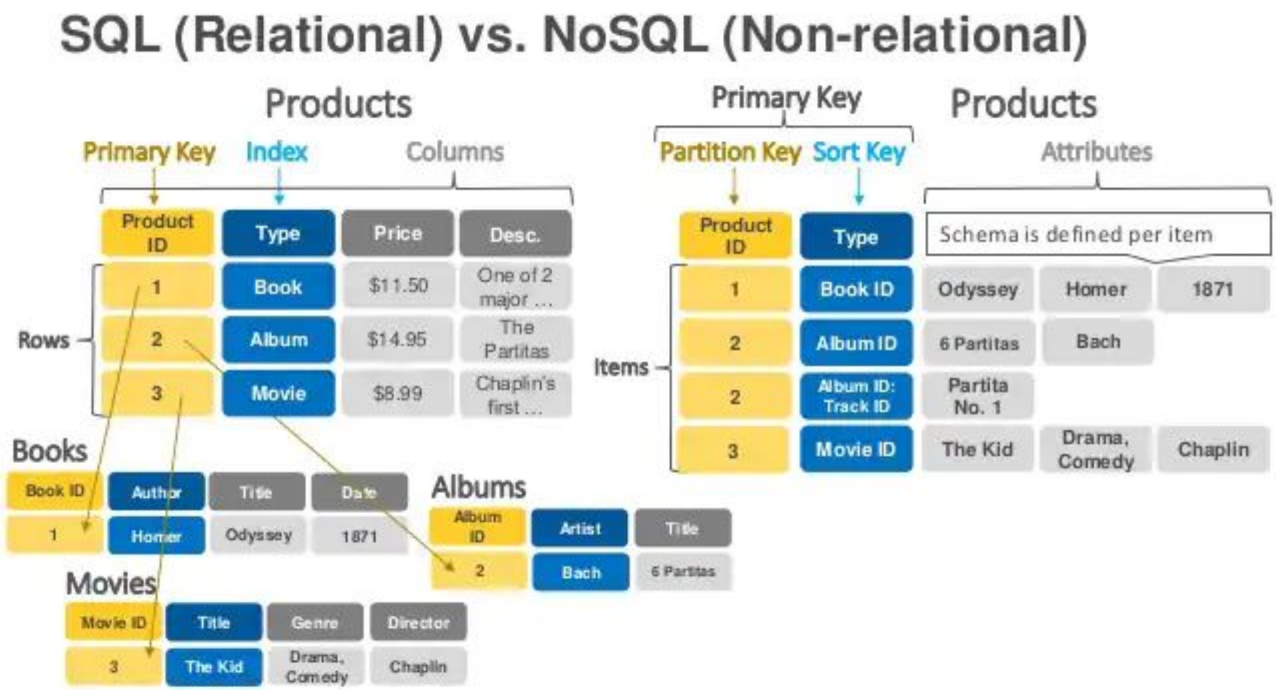
- Secondary Indexes: Secondary indexes allow you to perform queries on attributes that are not part of the table's primary key

- Local Secondary Index – Same Partition Key + Different Sort Key (can only be created while creating the table, cannot be added/removed or modified later)

- Global Secondary Index – Different Partition Key + Different Sort Key (can be created during the table creation or can be added later or removed / modified later)



SQL (Relational) vs. NoSQL (Non-Relational)



SQL (Relational) vs. NoSQL (Non-relational)

Products

Product ID	Type	Price	Desc.
1	Book	$11.50	One of 2 major …
2	Album	$14.95	The Partitas
3	Movie	$8.99	Chaplin's first …

Books

Book ID	Author	Title	Date
1	Homer	Odyssey	1871

Albums

Album ID	Artist	Title
2	Bach	6 Partitas

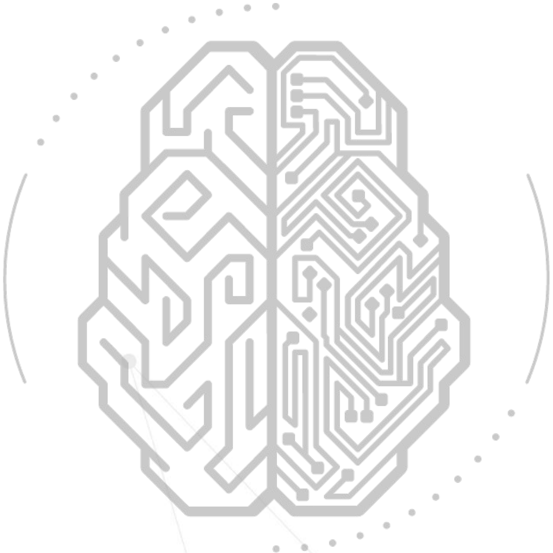
Movies

Movie ID	Title	Genre	Director
3	The Kid	Drama, Comedy	Chaplin

Products

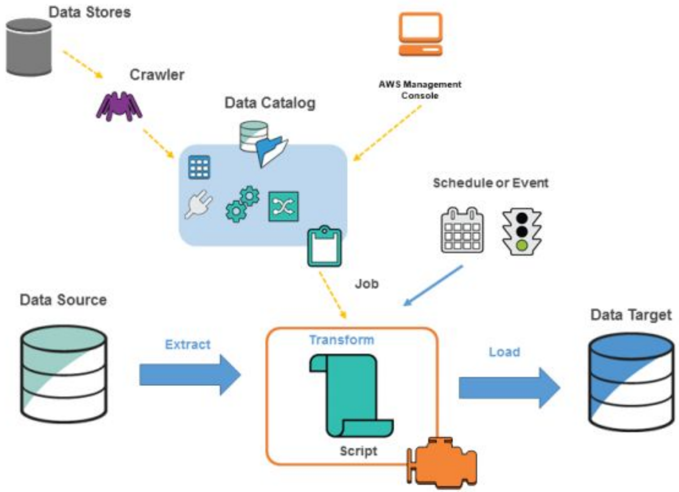
Product ID	Type	Schema is defined per item		
1	Book ID	Odyssey	Homer	1871
2	Album ID	6 Partitas	Bach	
2	Album ID: Track ID	Partita No. 1		
3	Movie ID	The Kid	Drama, Comedy	Chaplin

AWS Services - Glue

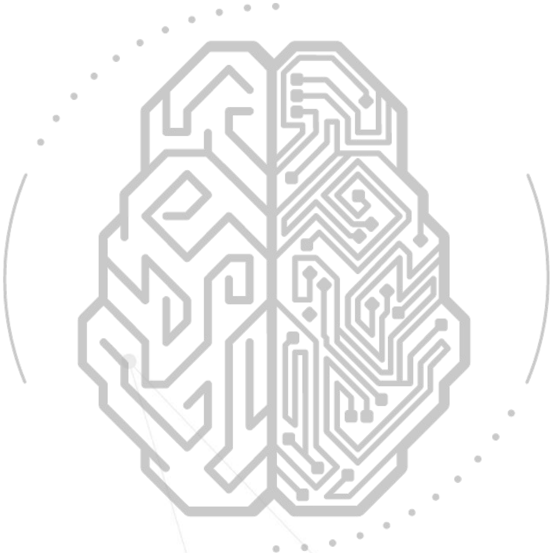


AWS Services - Glue

- AWS Glue is a fully managed ETL (extract, transform, and load) service.
- Categorize your data, clean it, enrich it and move it reliably between various data stores.
- Once catalogued, your data is immediately searchable and queryable across your data.
- Simple and cost-effective.
- Serverless; runs on a fully managed, auto-scaling Spark environment.
- AWS Glue consists of a central metadata repository known as the AWS Glue Data Catalog, an ETL engine that automatically generates Python or Scala code, and a flexible scheduler that handles dependency resolution, job monitoring, and retries.
- Glue Components
  - Databases - Tables and Connections
  - Data Catalog - Crawler and Classifiers
  - ETL - Jobs and Triggers



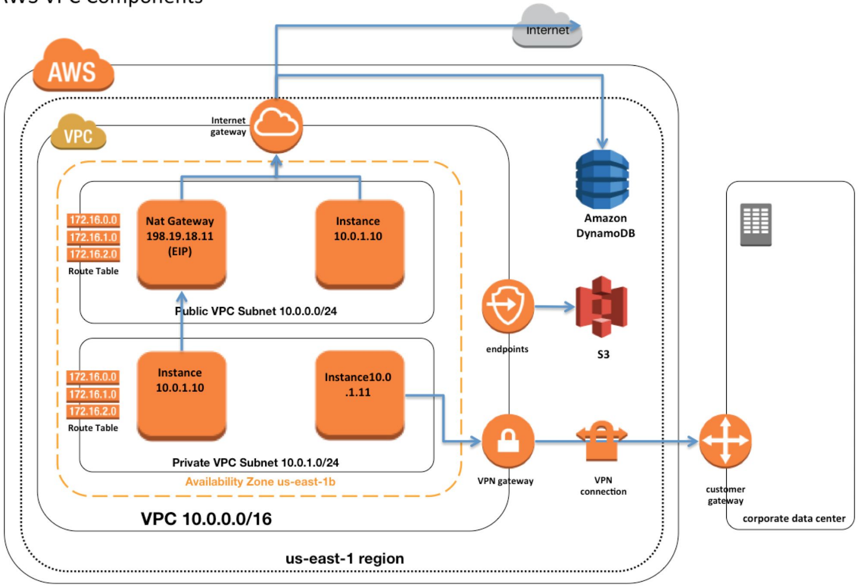
AWS Services - VPC



AWS Services - VPC: Introduction

- Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.
- It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.
- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.
- Your account comes with a default VPC that has a default subnet in each Availability Zone. A default VPC has the benefits of the advanced features provided by EC2-VPC, and is ready for you to use.
- If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC
- When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a **/16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)**

AWS VPC Components



AWS Services - VPC: Components

- **Internet Gateway** - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

- **Subnet** - Subnet is logical Isolation of your network i.e dividing your VPC into smaller network . Each subnet must be associated with a route table, which specifies the allowed routes for outbound traffic leaving the subnet. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets.

- **Route Tables** - A route table tells network packets which way they need to go to get to their destination. There are certain rules defined within this table. You can choose which subnets to be associated with a single route table. One subnet can be associated with only one RT, unlike RTs which can be associated with multiple subnets.

- **NAT Gateway** - NAT is a networking technique commonly used to give an entire private network access to the internet without assigning each host a public IPv4 address. When a host in the private network initiates an internet-bound connection, the NAT device public IP address becomes the source IP address for the outbound traffic. The response traffic from the internet therefore uses that public IP address as the destination IP address. The NAT device then routes the response to the host in the private network that initiated the connection

- **Egress only Internet Gateway** - An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the internet, and prevents the internet from initiating an IPv6 connection with your instances.

- **Elastic IP** - When an EC2 instance is launched, it is associated with a public IP address. When that instance is stopped and started again, a new IP address gets attached to that. Now comes Elastic IP into the picture. When an elastic IP is created and is associated with an EC2 instance, even if the instance is stopped and started again, same IP address retains. We can disassociate elastic ip of a terminated/stopped instance and associate with another instance until the former one is started again

AWS Services - VPC: Components

- **Security Groups** - Automatically default security group is created when a VPC is created, Instance-level security, Default security group, Custom security group, Second line of defense, and Stateful

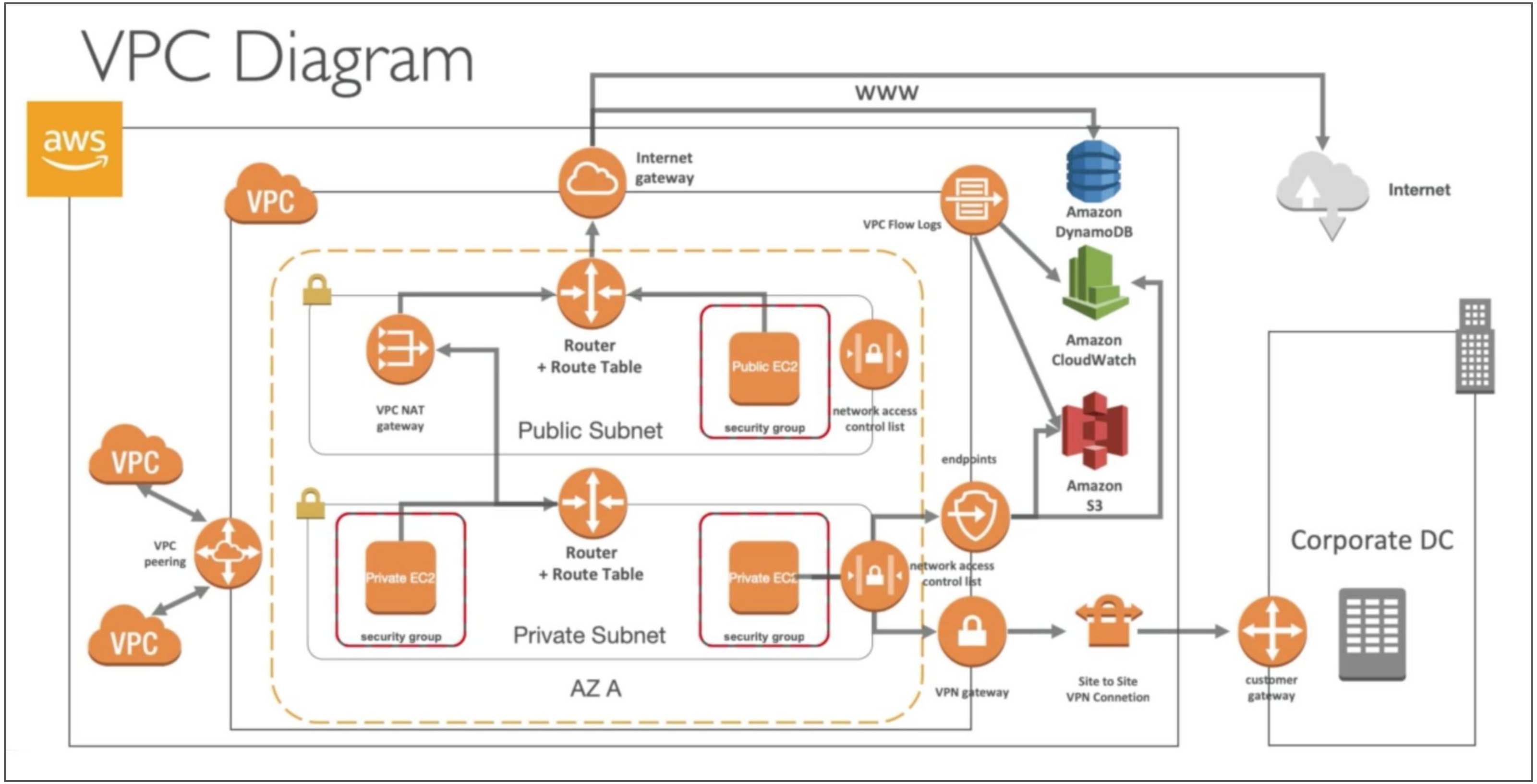
- **NACL** - Automatically default NACL is created when a VPC is created, Subnet-level security, Default NACL, Custom NACL, First line of defense, and Stateless

- **VPC Endpoints** - To prevent data from being unnecessarily exposed to the internet. VPC endpoint enables creation of a private connection between VPC to supported VPC Gateway (AWS services) and VPC endpoint services powered by PrivateLink using its private IP address.

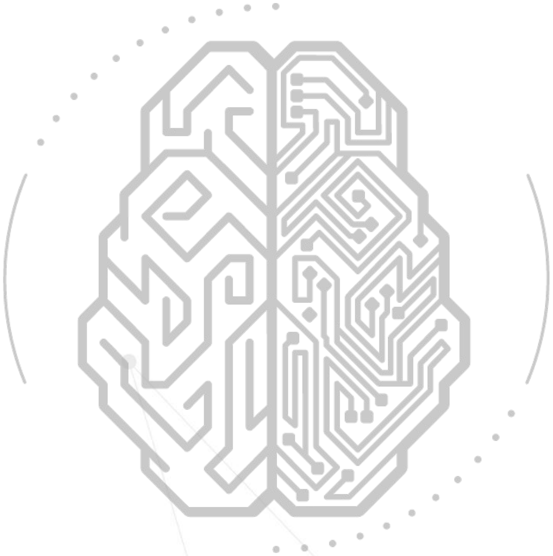
- **VPC Peering** - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 or IPv6 CIDR blocks

- **Security and Best Practices** -
  - Always try to use custom VPC over default VPC
  - Launch EC2, RDS, etc resources in Private Subnet Only
  - For Connecting to Instances in Private Subnet use Bastion Host / Jump Server
  - Use NAT Gateway for Internet connection of EC2 in Private Subnet
  - Always try to use restricted IP address in Security Group Inbound
  - Do not Open port 22 to 0.0.0.0/0
  - Never Share Your Public Key Over GitHub

AWS Services - VPC: End to End



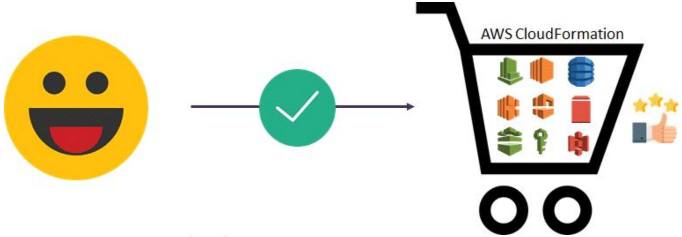
AWS Services - Cloudformation



What is AWS CloudFormation?

AWS CloudFormation provides users a simple way to create and manage a collection of AWS resources by provisioning and updating them in an orderly and predictable way

Create and manage AWS resources



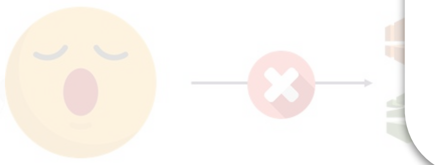
In simple terms, it allows you to create and model your infrastructure and applications without having to perform manual actions

What is AWS CloudFormation?

AWS CloudFormation provi imple way to create and manage a collection of AWS resources by provisioning and updating them in an orderly and predictable way

For Example

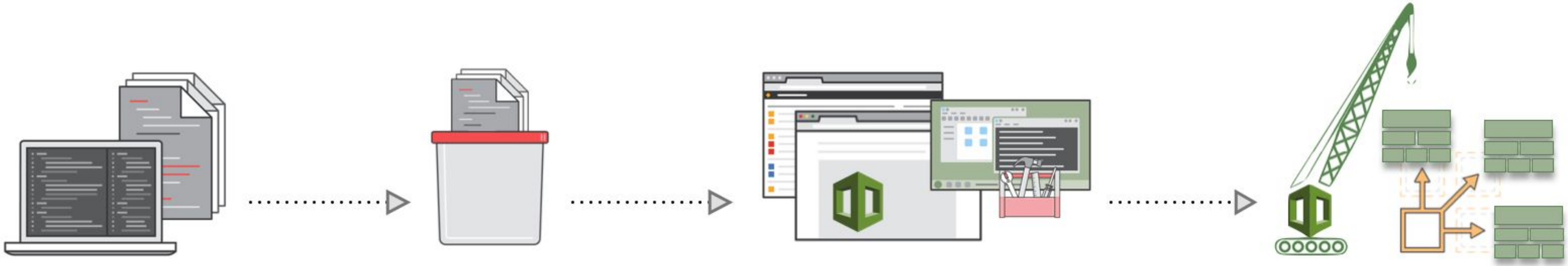
With AWS CloudFormation, Expedia is able to deploy and easily manage its entire front and backend AWS resources into its cloud environment



Create and manage AWS resources

In simple terms, it allows you to create and model your infrastructure and applications without having to perform manual actions

How AWS CloudFormation work?



Code your infrastructure from scratch with the CloudFormation template language, in either YAML or JSON format, or start from many available sample templates

Check out your template code locally, or upload it into an S3 bucket

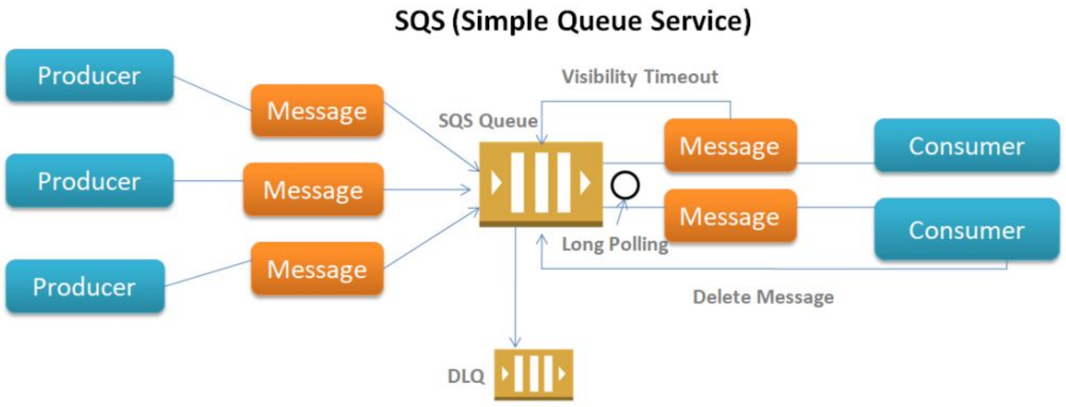
Use AWS CloudFormation via the browser console, command line tools or APIs to create a stack based on your template code

AWS CloudFormation provisions and configures the stacks and resources you specified on your template

AWS Services - Cloud Integration

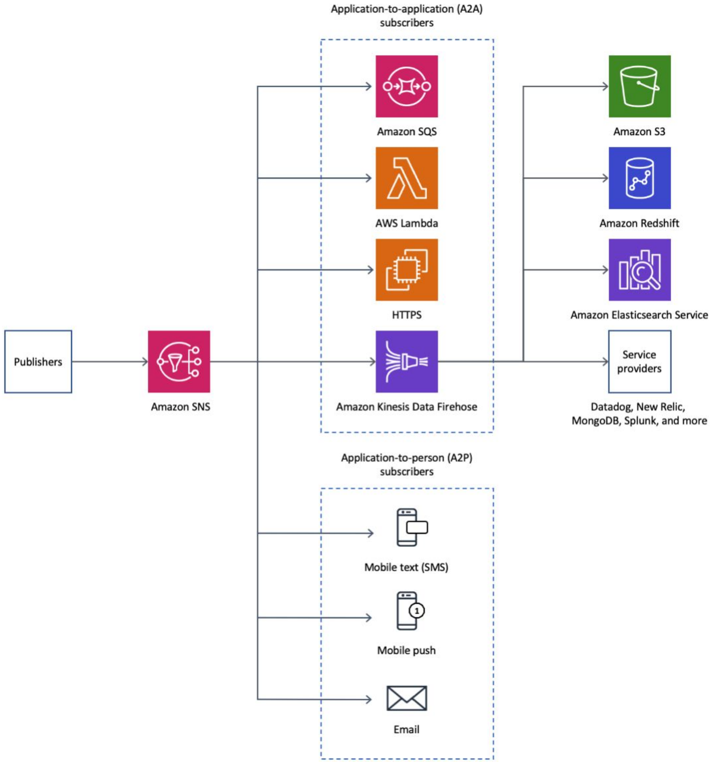
AWS Services - Cloud Integration: SQS

- Oldest AWS offering (over 10 years old)
- Fully managed service, use to decouple applications
- Scales from 1 message per second to 10,000s per second, and Low latency (<10 ms on publish and receive)
- Default retention of messages: 4 days, maximum of 14 days
- No limit to how many messages can be in the queue, and messages are deleted after they’re read by consumers
- Consumers share the work to read messages & scale horizontally



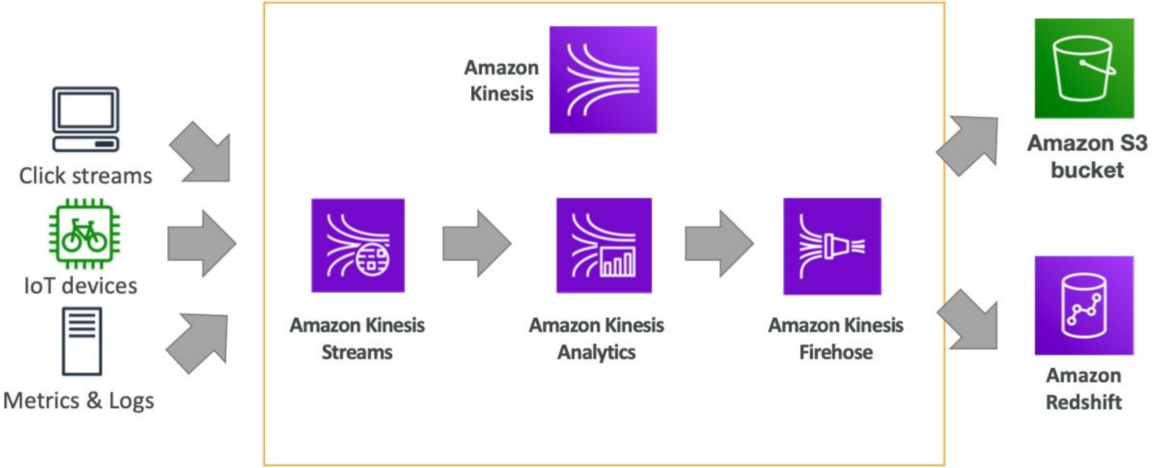
AWS Services - Cloud Integration: SNS

- Publishers sends message to a SNS topic and multiple subscribers listen to the SNS topic notifications
- Each subscriber to the topic will get all the messages
- Up to 10,000,000 subscriptions per topic, 100,000 topics limit
- SNS Subscribers can be:
  - HTTP / HTTPS (with delivery retries – how many times)
  - Emails,SMS messages,Mobile Notifications
  - SQS queues (fan-out pattern), Lambda Functions (write-your-own integration)

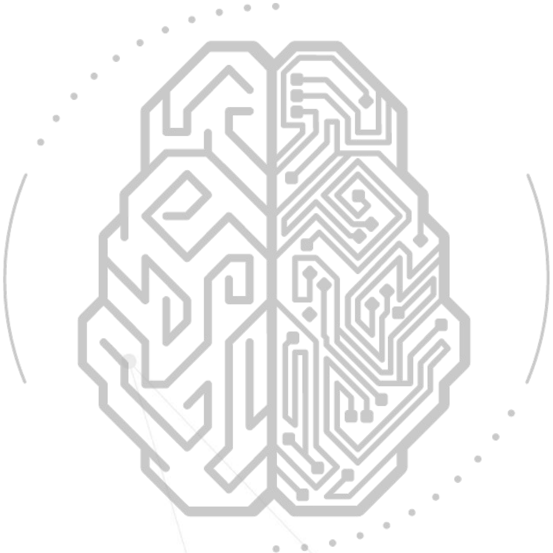

Application-to-application (A2A) subscribers
Amazon SQS
AWS Lambda
HTTPS
Amazon Kinesis Data Firehose
Amazon S3
Amazon Redshift
Amazon Elasticsearch Service
Service providers
Datadog, New Relic, MongoDB, Splunk, and more
Publishers
Amazon SNS
Application-to-person (A2P) subscribers
Mobile text (SMS)
Mobile push
Email

AWS Services - Cloud Integration: Kinesis

- For the exam: Kinesis = real-time big data streaming
- Managed service to collect, process, and analyze real-time streaming data at any scale
- Too detailed for the Cloud Practitioner exam but good to know:
  - Kinesis Data Streams: low latency streaming to ingest data at scale from hundreds of thousands of sources
  - Kinesis Data Firehose: load streams into S3, Redshift, ElasticSearch, etc
  - Kinesis Data Analytics: perform real-time analytics on streams using SQL
  - Kinesis Video Streams: monitor real-time video streams for analytics or ML

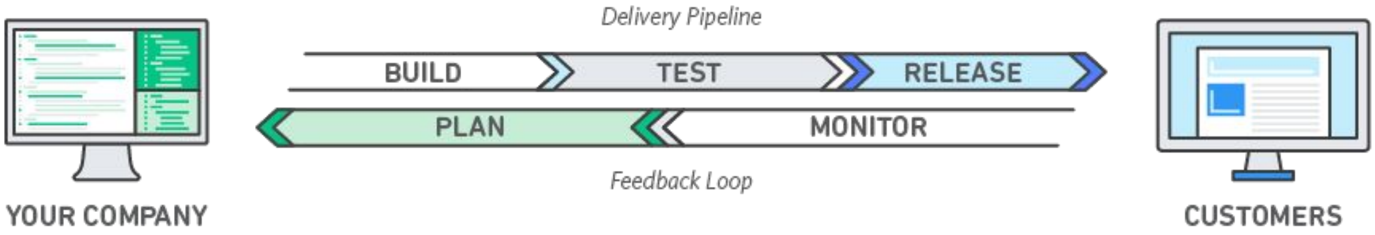


AWS Services - Developer Tools

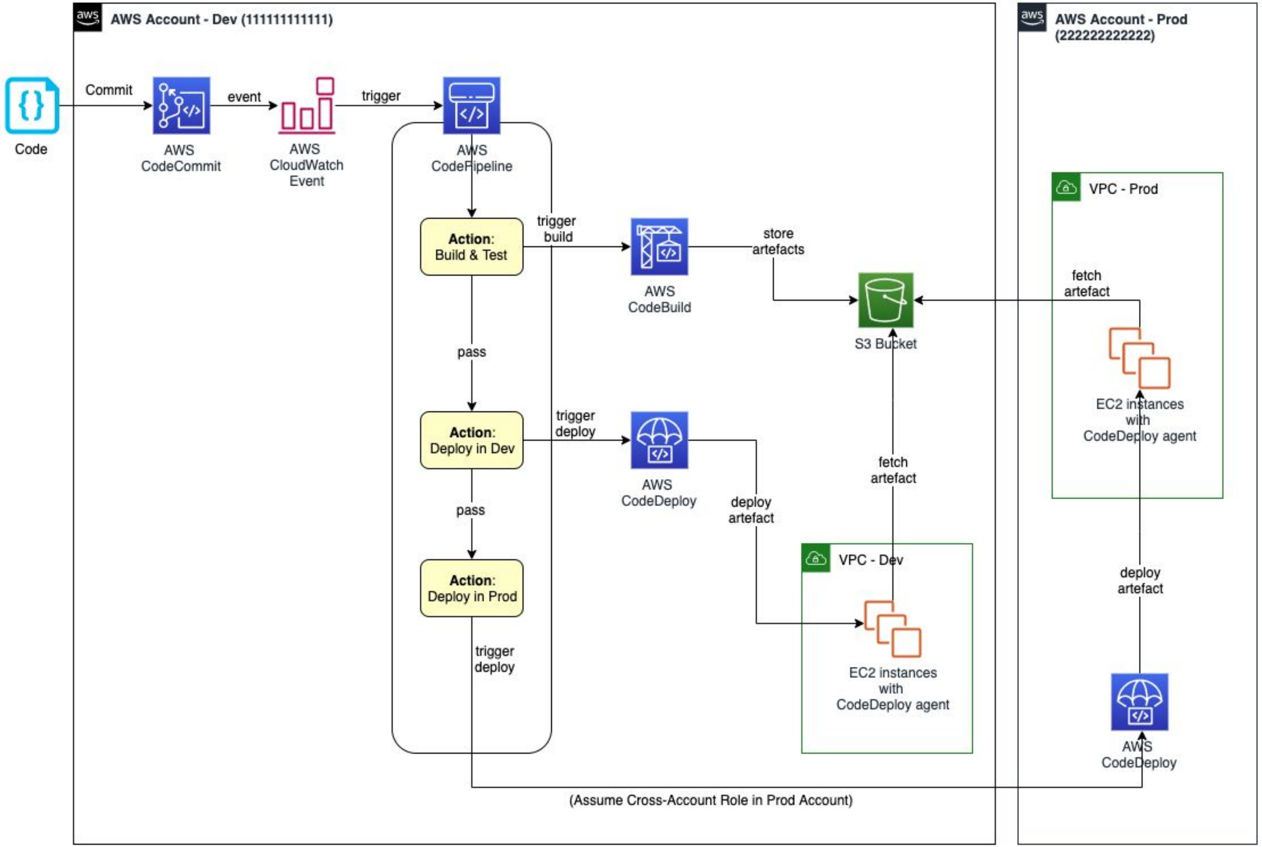


AWS Services - Developer Tools

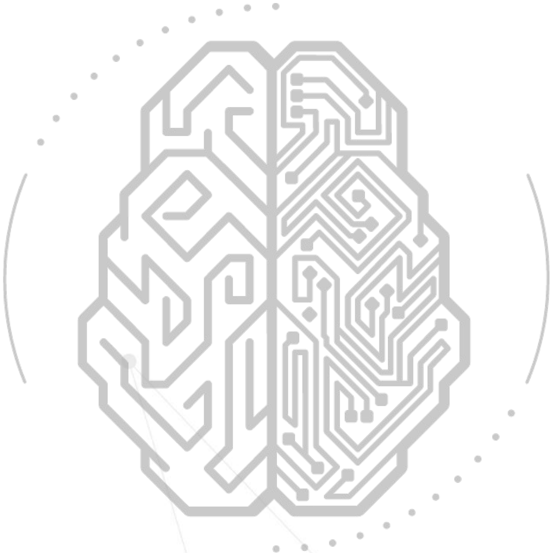
- **AWS CodeCommit** – A fully-managed source control service that hosts secure Git-based repositories. CodeCommit makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem.
- **AWS CodeBuild** – A fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy, on a dynamically created build server.
- **AWS CodeDeploy** – A fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers.
- **AWS CodePipeline** – A fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.



AWS Services - Developer Tools: Workflow



AWS Services - Monitoring



AWS Services - CloudWatch

- Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time
- You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.
- You can additionally create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose
- You can create alarms which watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached
- Example : CloudWatch can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use this data to determine whether you should launch additional instances to handle increased load
- **Cloudwatch Concepts**
  - **Metrics** - Think of a metric as a variable to monitor, and the data points as representing the values of that variable over time example CPU utilization of a particular EC2 instance
  - **Dimensions** - A dimension is a name/value pair that is part of the identity of a metric. You can use dimensions to filter the results that CloudWatch returns. Example filter by specifying the InstanceId dimension
  - **Statistics** - Statistics are metric data aggregations over specified periods of time. Example Min, Max, Average, Sum, SampleCount
  - **Alarms** - You can use an alarm to automatically initiate actions on your behalf
- **CloudWatch Dashboards** - A single view for selected metrics and alarms to help you assess the health of your resources and applications across one or more regions

AWS Services - CloudTrail

- CloudTrail is used to search, download, archive and respond to account activities across AWS infrastructure. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

- You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

- Event history allows you to view, search, and download the past 90 days of activity in your AWS account. CloudTrail is enabled on your AWS account when you create it.

- **Workflow**
  - View event history for your AWS account
  - Download events
  - Create a trail
  - Create and subscribe to an Amazon SNS topic
  - Manage user permissions
  - View your log files
  - Use Amazon S3 to retrieve log files.
  - Log management and data events
  - Log CloudTrail Insights events
  - Enable log encryption
  - Share log files with other AWS accounts

- Two types of Events that can be logged in CloudTrail - Management Events (example AttachRolePolicy, CreateSubnet) and Data Events (example GetObject, DeleteObject, and PutObject)

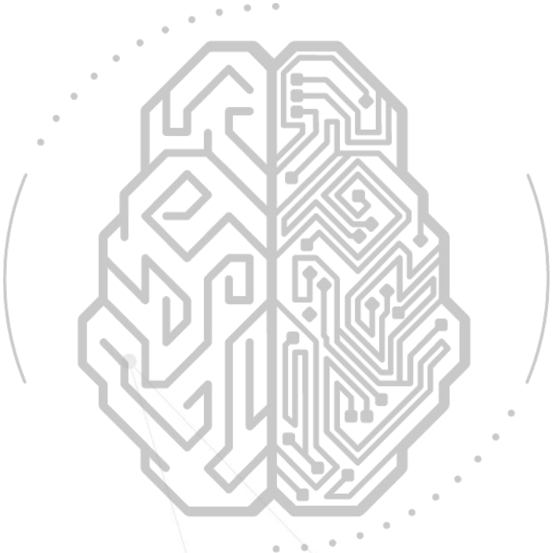
AWS Services - CloudTrail

- Trail Creation - A trail is a configuration that enables delivery of CloudTrail events to an Amazon S3 bucket, CloudWatch Logs, and CloudWatch Events. Two types of CloudTrail trails - A trail that applies to all regions, and A trail that applies to one region

- Insights Events - CloudTrail Insights events capture unusual activity in your AWS account.

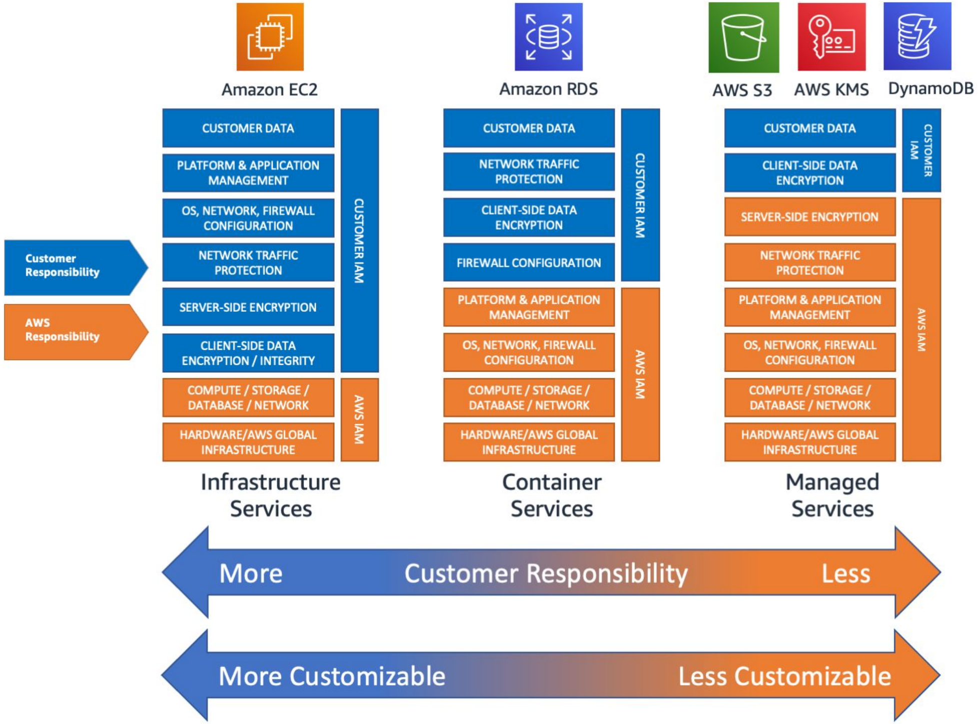
- Best Practices
  - **Detective**
    - Create a trail
    - Apply trails to all AWS Regions
    - Enable CloudTrail log file integrity
    - Integrate with Amazon CloudWatch Logs
  - **Preventative**
    - Log to a dedicated and centralized Amazon S3 bucket
    - Use server-side encryption with AWS KMS managed keys
    - Implement least privilege access to Amazon S3 buckets where you store log files
    - Enable MFA Delete on the Amazon S3 bucket where you store log files
    - Configure object lifecycle management on the Amazon S3 bucket where you store log files
    - Limit access to the AWSCloudTrailFullAccess policy

AWS Shared Responsibility

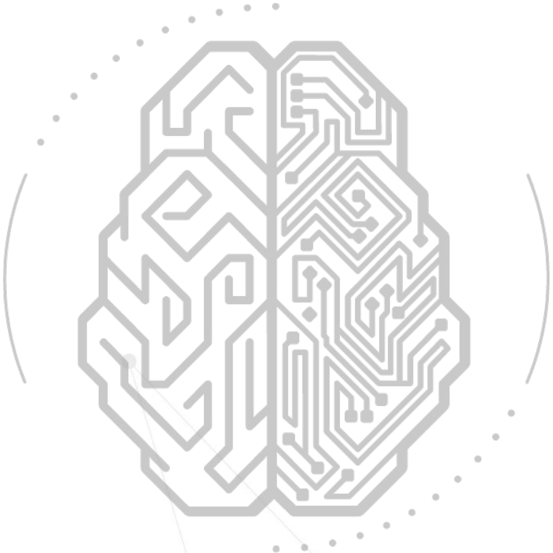


AWS Shared Responsibility

- To help clarify the division of responsibilities and ease the burden of cloud security, Amazon Web Services (AWS) has established the AWS Shared Responsibility Model. Put simply, the AWS Shared Responsibility Model explains what AWS is responsible for securing in the cloud and what the customer is responsible for securing.

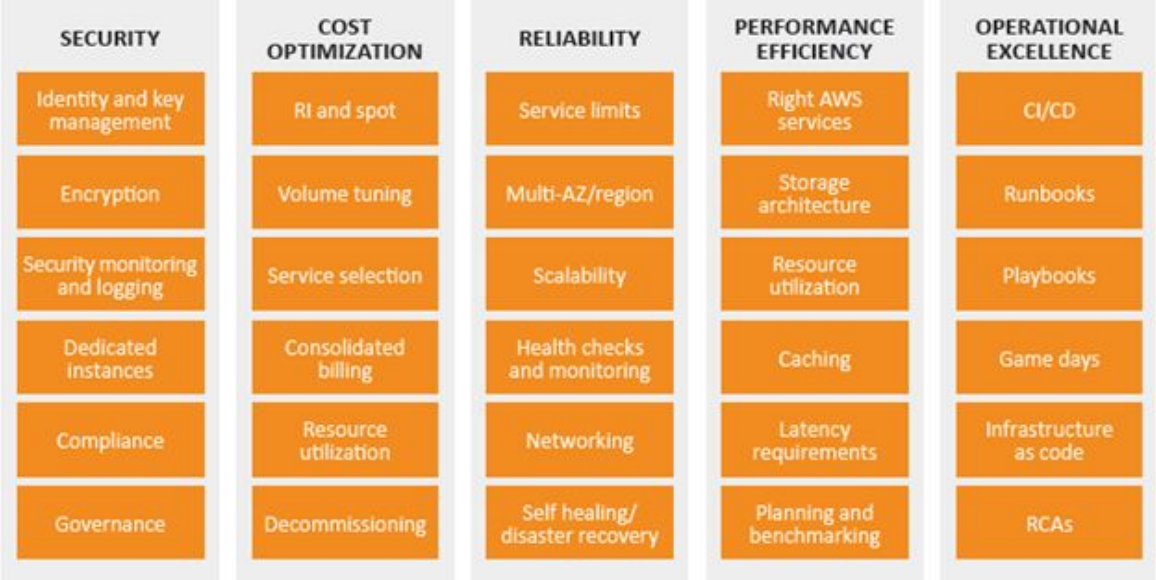

Amazon EC2
Amazon RDS
AWS S3
AWS KMS
DynamoDB
Customer Responsibility
AWS Responsibility
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
NETWORK TRAFFIC PROTECTION
SERVER-SIDE ENCRYPTION
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
NETWORK TRAFFIC PROTECTION
CLIENT-SIDE DATA ENCRYPTION
FIREWALL CONFIGURATION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
CLIENT-SIDE DATA ENCRYPTION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Infrastructure Services
Container Services
Managed Services
More
Customer Responsibility
Less
More Customizable
Less Customizable

AWS Well Architected Review



AWS Well Architected Framework

- AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on five pillars operational excellence, security, reliability, performance efficiency, and cost optimization
- The AWS WA Tool, available at no cost in the AWS Management Console, provides a mechanism for regularly evaluating your workloads, identifying high risk issues, and recording your improvements.

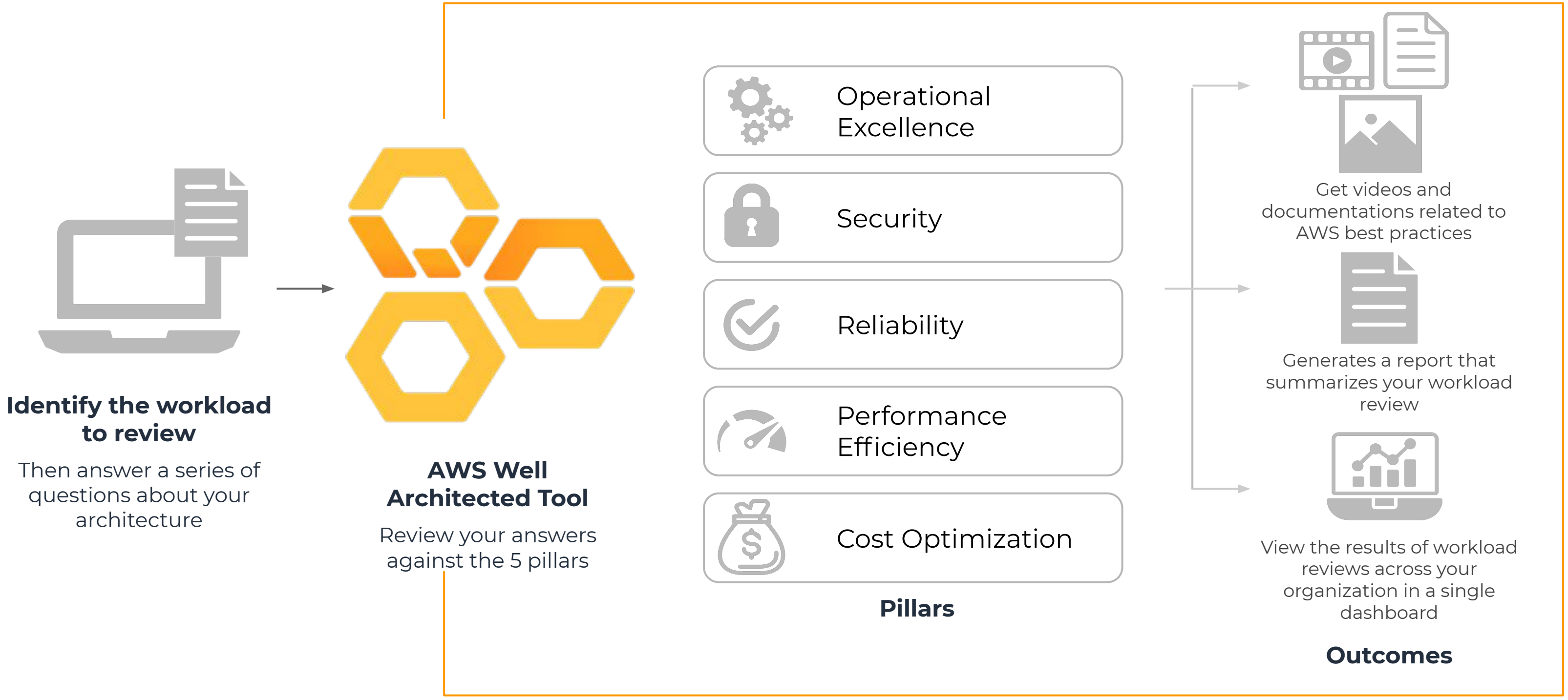


SECURITY	COST OPTIMIZATION	RELIABILITY	PERFORMANCE EFFICIENCY	OPERATIONAL EXCELLENCE
Identity and key management	RI and spot	Service limits	Right AWS services	CI/CD
Encryption	Volume tuning	Multi-AZ/region	Storage architecture	Runbooks
Security monitoring and logging	Service selection	Scalability	Resource utilization	Playbooks
Dedicated instances	Consolidated billing	Health checks and monitoring	Caching	Game days
Compliance	Resource utilization	Networking	Latency requirements	Infrastructure as code
Governance	Decommissioning	Self healing/ disaster recovery	Planning and benchmarking	RCAs

AWS Well Architected Review

AWS Well-Architected Review helps you review the state of your workloads and compares them to the latest AWS architectural best practices.

It is based on the AWS Well Architected Framework, developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure.



Identify the workload to review

Then answer a series of questions about your architecture

AWS Well Architected Tool

Review your answers against the 5 pillars

Operational Excellence

Security

Reliability

Performance Efficiency

Cost Optimization

Pillars

Get videos and documentations related to AWS best practices

Generates a report that summarizes your workload review

View the results of workload reviews across your organization in a single dashboard

Outcomes

THANK YOU