
aws
training and
certification

AWS Certified Solutions Architect - Associate

Week 5 Content Review

September 2023 Accelerator

aws training and certification

Week 5 Training Summary

aws training and certification

Week 5 Digital Training Curriculum

Core Trainings

Course
Designing Event-Driven Architectures
Architecting Serverless Applications
Introduction to Simple Workflow Service
Introduction to Amazon EC2 Systems Manager
Introduction to AWS Fargate
Introduction to Amazon Elastic Container Registry

Optional Hands-On

AWS Builder Labs

Lab
Building Serverless Applications with an Event Driven Architecture

aws training and certification

About the Exam

aws training and certification

AWS Certified Solutions Architect - Associate

About the Exam

- 130 minutes
- 65 Questions
  - *50 questions count to your score*
  - Scored 100 to 1000 (720+ pass)
- $150/voucher
- Multiple Response & Individual response questions
- In-Person & Remote proctoring available

AWS Certified Solutions Architect - Associate

Key Exam Topics

Domains Covered:	% of Exam
Domain 1: Design Secure Architectures	30%
Domain 2: Design Resilient Architectures	26%
Domain 3: Design High-Performing Architectures	24%
Domain 4: Design Cost-Optimized Architectures	20%
Total:	**100%**

AWS Certified Solutions Architect - Associate

Helpful Resources

Training

- AWS Partner Accreditation: Technical
- AWS Solutions Architect – Accelerator Learning plan

White Papers

- Overview of Amazon Web Services
- AWS Well-Architected Framework
- Management and Governance Lens
- AWS Global Infrastructure
- Shared Responsibility Model
- How AWS Pricing Works
- AWS Architecture Center
- Secure Content Delivery with Amazon CloudFront
- IPv6 on AWS
- Overview of Deployment options on AWS
- Organizing your AWS Environment using multiple accounts

Exam Preparation

- Twitch Power Hours
- Sample Questions
- Schedule an Exam

Looking for more ***Practice Exams***?

*Check out our **Skill Builder Subscription** (information on the next slide)*

aws training and certification

OPTIONAL AWS Skill Builder Subscription

The Skill Builder subscription provides access to official AWS Certification practice exams, self-paced digital training content including open-ended challenges, self-paced labs, and game-based learning. ***Please note, the Skill Builder subscription is not required for this Accelerator program.***

Free digital training

LINK HERE

Special features include:

- 500+ digital courses
- Learning plans
- 10 Practice Question Sets
- *AWS Cloud Quest*

Individual subscription

LINK HERE

Everything in free digital training, plus:

- AWS Cloud Quest (3 additional roles)
- AWS Certification Official Practice Exams
- Exam prep courses
- 100+ AWS Builder Labs
- AWS Jam Journey (lab-based challenges)

Access ***65*** Solutions Architect - Associate Practice Exam Questions with feedback on your answer choices

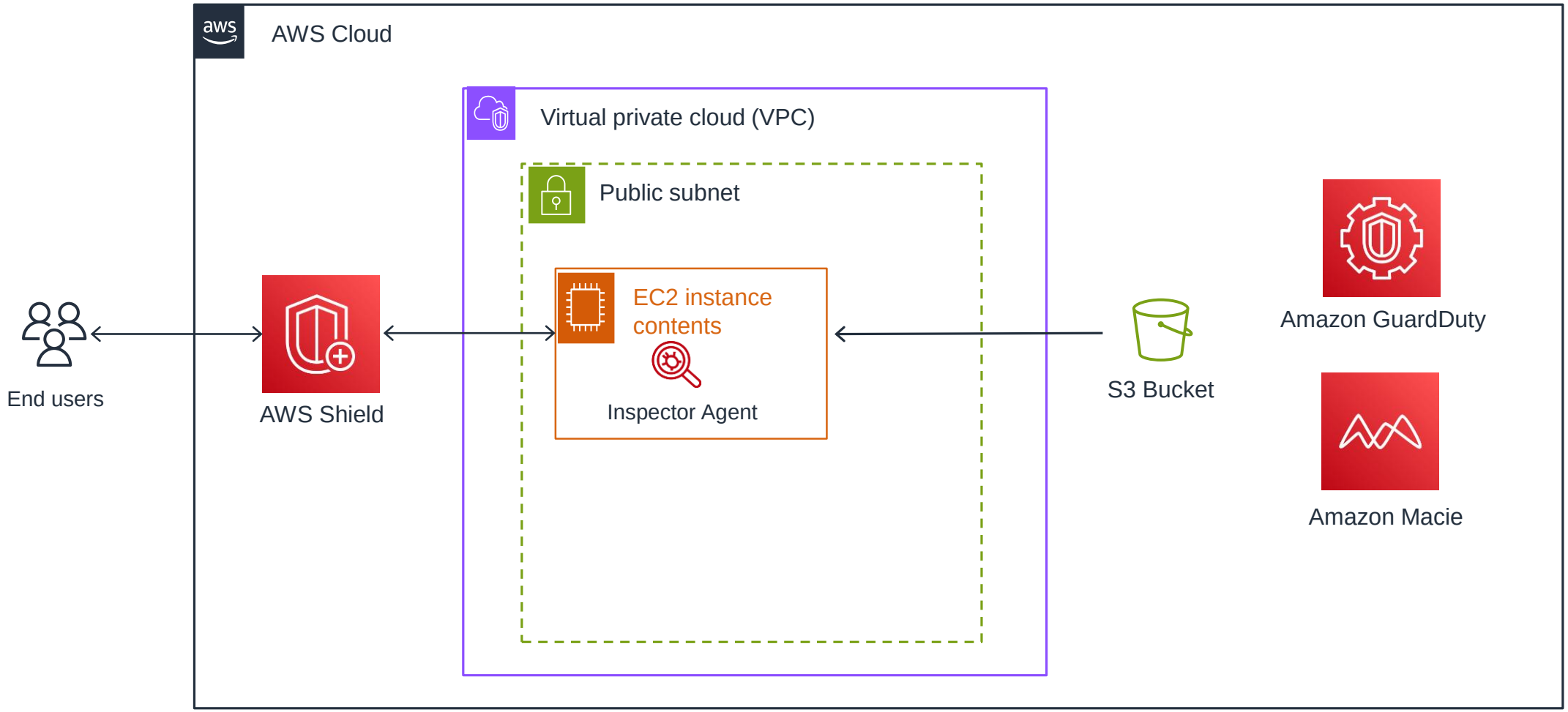
Individual subscriptions are priced at $29 USD per month (*Flexibility to cancel anytime*) or $299 USD per year.

aws training and certification

Week 5 Homework Assignment

aws training and certification

Week 4 Homework – Solution Key



Week 4 Homework (Bonus) – Solution Key

JSON

IAM policy

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::EXAMPLE-BUCKET/share/dev/*"
      }
   ]
}
```

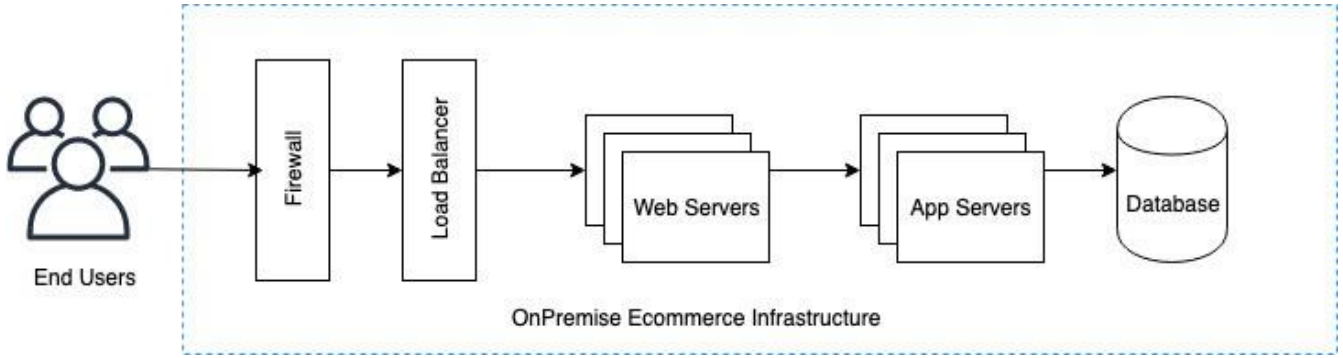
IAM Group (Dev)

aws training and certification

Week 5 Homework – Let's go Serverless!

Solution Requirements:

1. **Decompose an application into a serverless solution.**
2. **Adjust for an event-driven architecture.**
3. **Our Solution Example will be a Shopping Cart in an e-commerce store**



<u>Your Task:</u>

Design an architecture diagram meeting these requirements.

Week 5 Homework – Bonus Points!

<u>Your Task:</u>

- **Add Monitoring solution to your application**
- **Make it multi-region**
- **Have FUN and get CREATIVE – what else could you add to this app?**

Week 5 Homework – Show and Tell!

Share us your architecture, answers, and explanation on LinkedIn!

#AWSpartners

#AWSaccelerator

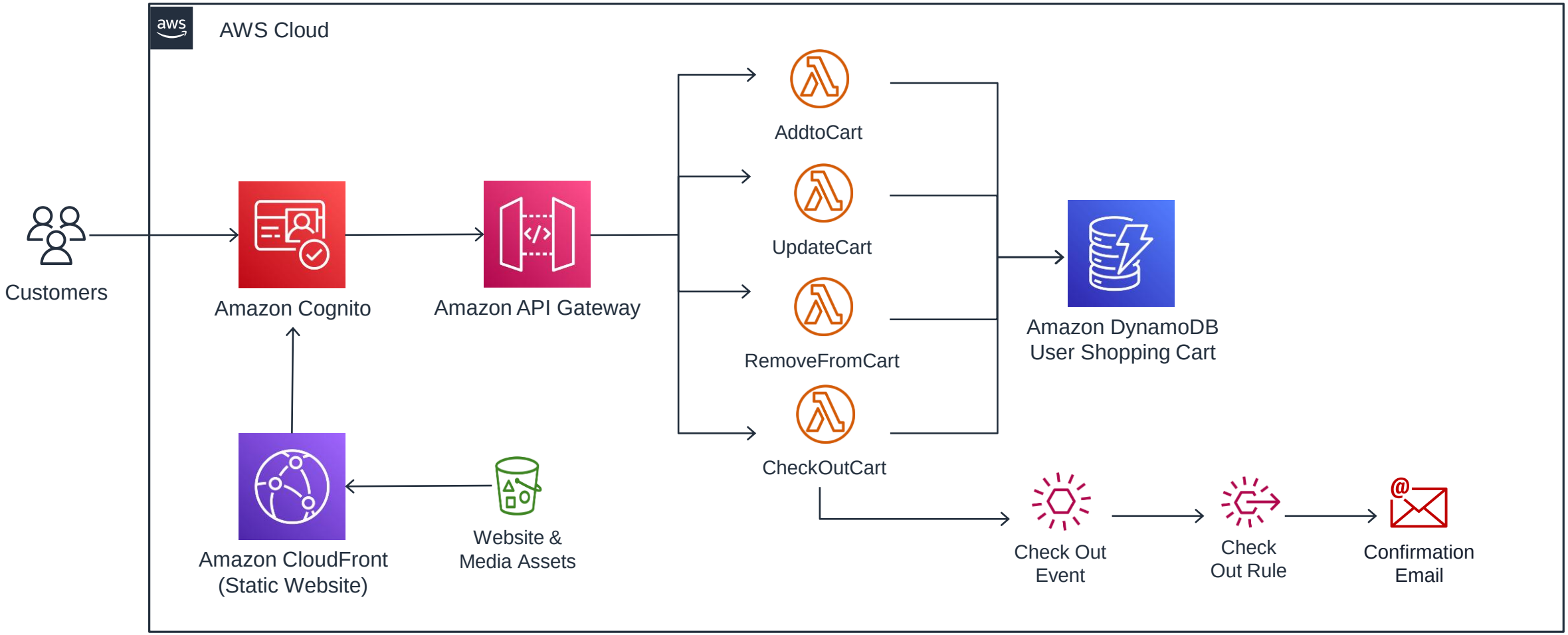
Tag us so we don't miss it!

Kevin, Sam, Brady

Please do not share confidential or proprietary information on social media.

aws training and certification

Week 5 Homework – Solution Key



Everything Left!

aws training and certification

Decoupling and Messaging

aws training and certification

Amazon Simple Queue Service (SQS)

A fully managed message queue for microservices, distributed systems, and serverless applications

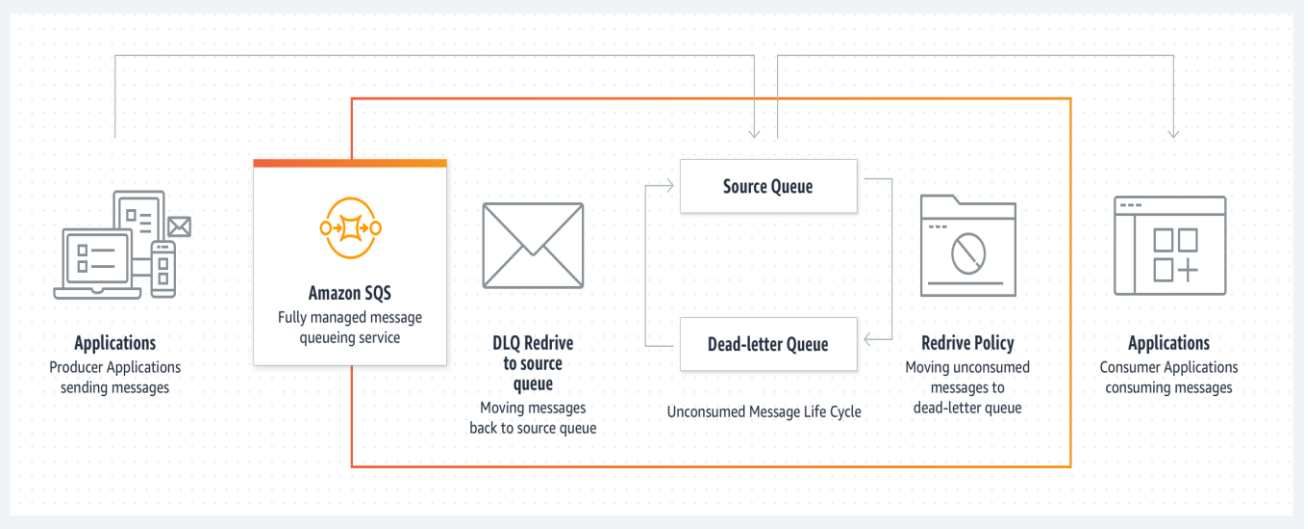
Purpose

A fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless apps. Using SQS you can send, store, and receive messages between software components at any volume.

Use Cases

SQS has an ever increasing number of applications. Some include:

- Buffer and Batch Operations
- Reliable message delivery (at any scale)
- Request Offloading



aws training and certification

Amazon SQS Queue Types

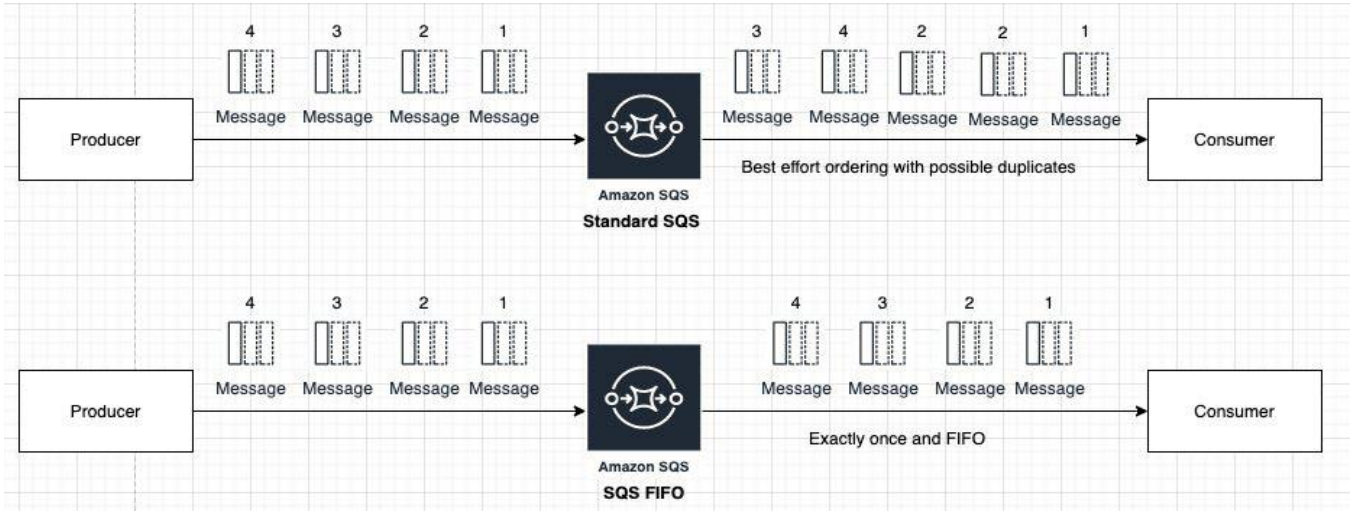
Standard vs. FIFO – What's the difference and why should I care?

Overview

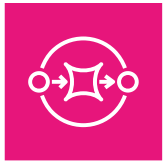
Amazon SQS provides two types of queue services – Standard and First In – First Out (FIFO).

Important Differences

- SQS Standard Queues can support unlimited throughput by adding as many concurrent producers as is needed,
- FIFO Queues can support up to 300 TPS without batching, and up to 3,000 TPS with batching
- BOTH are used for decoupling applications and as messaging agents between applications or services.



Amazon Simple Queue Service (SQS)



Amazon SQS offers two queue types for different application requirements:

Standard Queues

- You can use standard message queues in many scenarios, as long as your application can process messages that arrive more than once and out of order
- Unlimited Throughput: Standard queues support a nearly unlimited number of transactions per second (TPS) per API action.
- At-Least-Once Delivery: A message is delivered at least once, but occasionally more than one copy of a message is delivered.
- Best-Effort Ordering: Occasionally, messages might be delivered in an order different from which they were sent.

FIFO Queues

- FIFO queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated
- High Throughput: By default, FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second.
- Exactly-Once Processing: A message is delivered once and remains available until a consumer processes and deletes it. Duplicates aren't introduced into the queue.

Amazon Simple Notification Service (SNS)

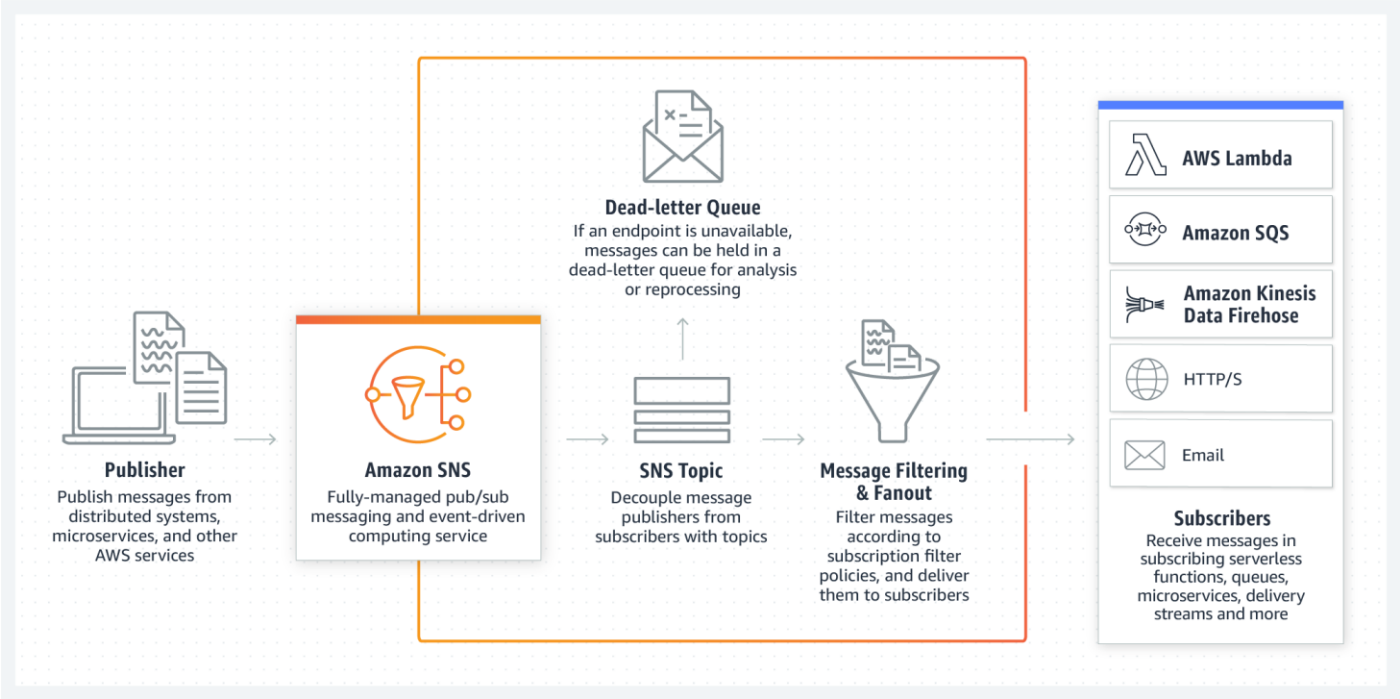
Fully managed pub/sub messaging, SMS, email, and mobile push notifications

Overview

Amazon SNS is a fully managed messaging service for App-to-App (A2A) and app-to-person (A2P) communication.

What's it do?

The A2A pub/sub functionality provides topics for high-throughput, push-based, many-to-many messaging between distributed systems, microservices, and event-driven serverless applications.

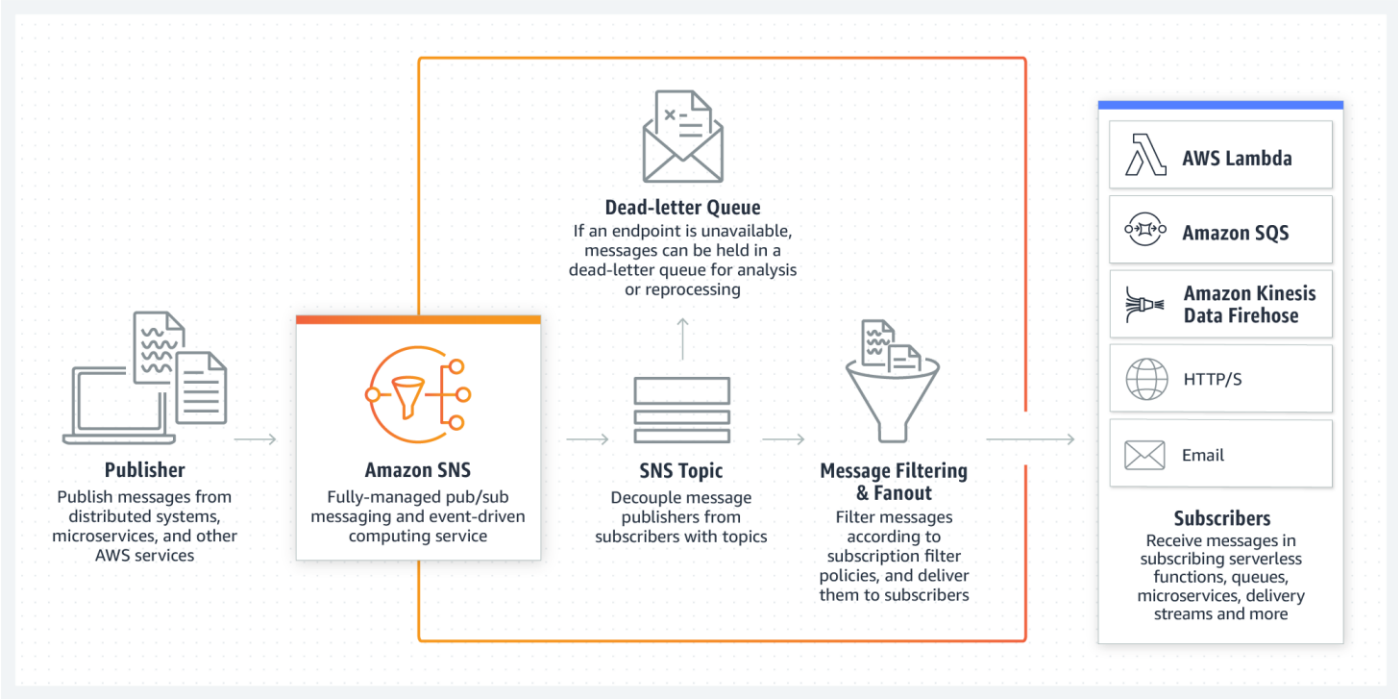


Amazon Simple Notification Service (SNS)

Fully managed pub/sub messaging, SMS, email, and mobile push notifications

Key Benefits of SNS

- Simplify and reduce costs with message filtering and batching
- Ensure accuracy with message ordering and deduplication
- Capture and fan out events from AWS services
- Increase security with message encryption and privacy
- Increase durability with message archiving, delivery retries, and DLQ
- Send A2P notifications via SMS, mobile push, and email



aws training and certification

Common Amazon SNS Scenario – Fanout

The Fanout scenario is when a message published to an SNS topic is replicated and pushed to multiple endpoints, such as Kinesis Data Firehose delivery streams, Amazon SQS queues, HTTP(S) endpoints, and Lambda functions.

This allows for parallel asynchronous processing.

For example, you can develop an application that publishes a message to an SNS topic whenever an order is placed for a product.

- Then, SQS queues that are subscribed to the SNS topic receive identical notifications for the new order.
- An Amazon Elastic Compute Cloud (Amazon EC2) server instance attached to one of the SQS queues can handle the processing or fulfillment of the order.
- And you can attach another Amazon EC2 server instance to a data warehouse for analysis of all orders received.

AWS Lambda

aws training and certification

AWS Lambda

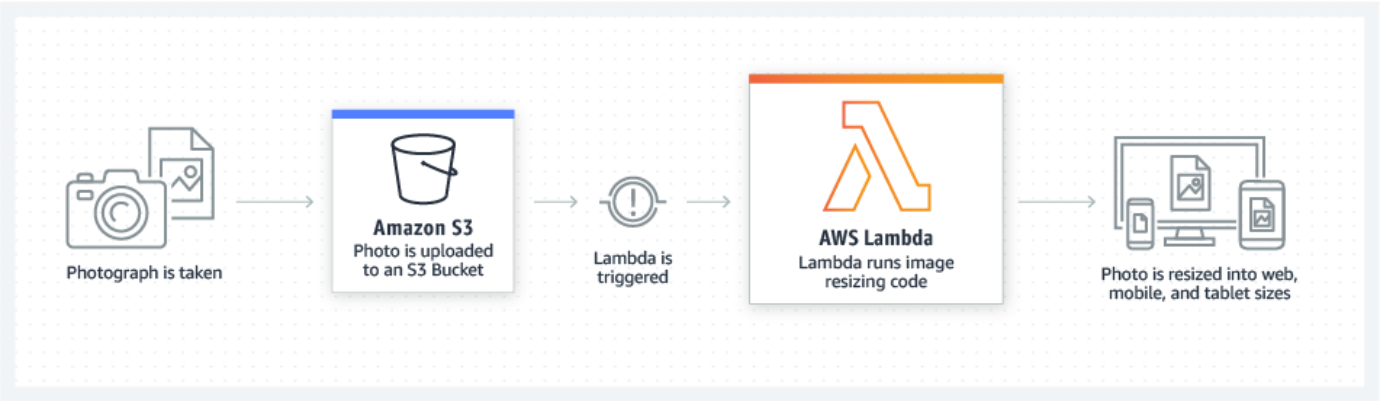
Run code without thinking about servers or clusters!

How does it work?

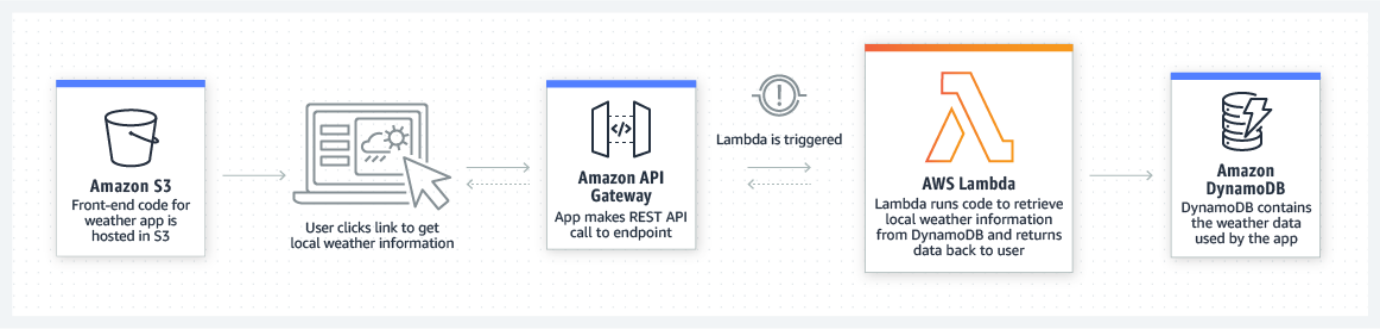
AWS Lambda is a serverless, event-driven compute service that lets you run code for virtually any type of application or backend service without provisioning or managing servers.

You can trigger Lambda from over 200 AWS services and software as a service (SaaS) applications, and only pay for what you use.

File Processing



Web Applications



aws training and certification

AWS Lambda – A closer look

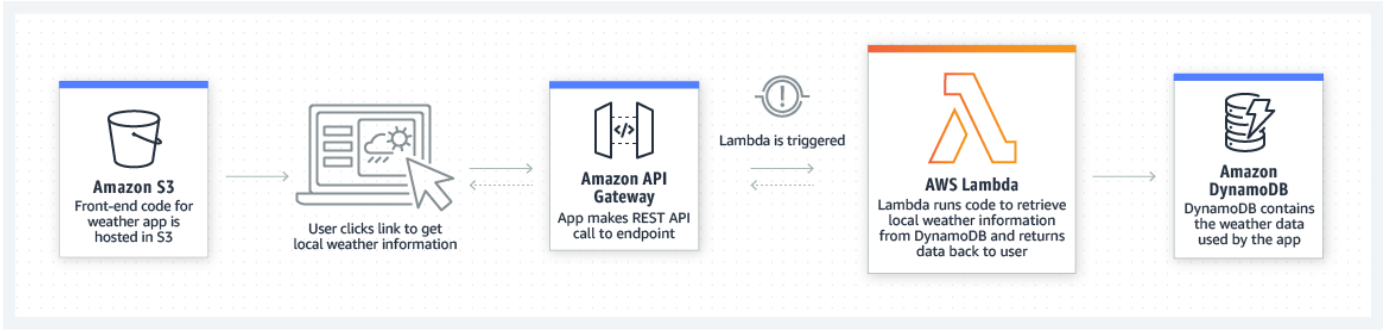
Run code without thinking about servers or clusters!

What does it do?

- Run code without provisioning or managing infrastructure. Simply write and upload code as a .zip file or container image.
- Automatically respond to code execution requests at any scale, from a dozen events per day to hundreds of thousands per second.
- Optimize code execution time and performance with the right function memory size. Respond to high demand in double-digit milliseconds with Provisioned Concurrency.

File Processing

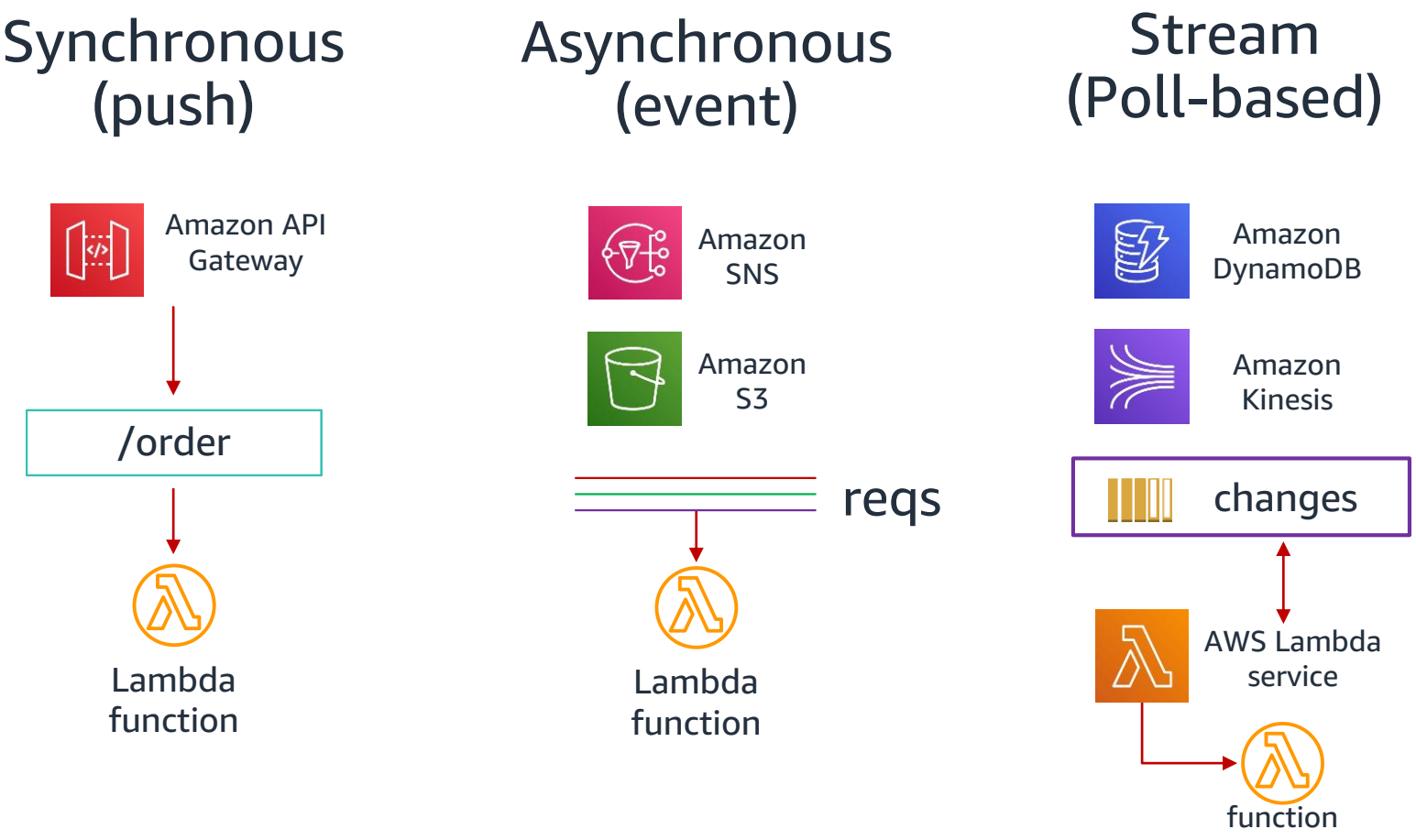
Web Applications



AWS Lambda – Example Pattern

You can use Amazon Simple Storage Service (Amazon S3) to trigger AWS Lambda data processing in real time after an upload, or connect to an existing Amazon EFS file system to enable massively parallel shared access for large-scale file processing.

Lambda Execution Models

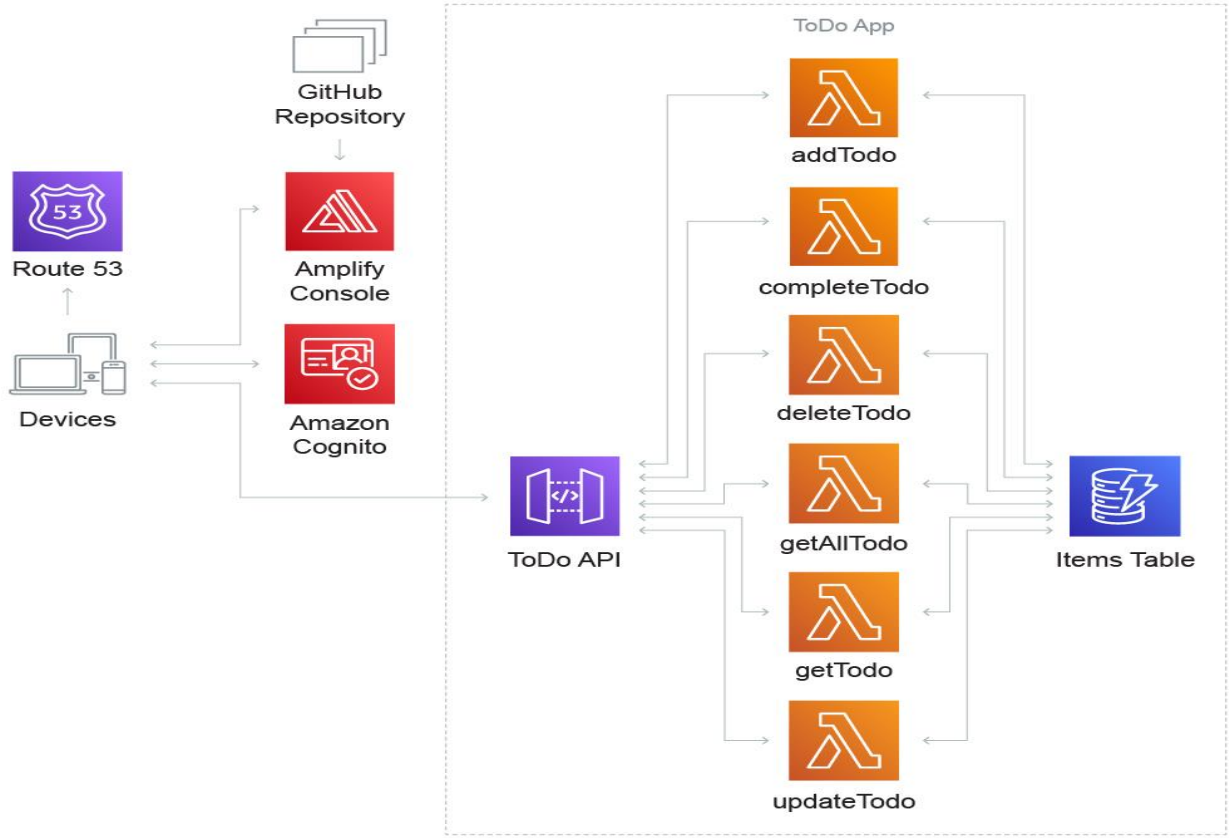


Example Serverless Pattern with AWS Services

Here's an example of a simple "to-do list" web app that enables a registered user to create, update, view, and delete items.

An event-driven web application may use:

- AWS Lambda and Amazon API Gateway for its business logic
- Amazon DynamoDB as its database
- AWS Amplify to host all static content.



AWS Lambda – Memory Considerations

Memory is the principal lever available to Lambda developers for controlling the performance of a function.

- The amount of memory also determines the amount of virtual CPU available to a function. Adding more memory proportionally increases the amount of CPU, increasing the overall computational power available.
- If a function is CPU-, network- or memory-bound, then changing the memory setting can dramatically improve its performance.
- For example, 1000 invocations of a function that computes prime numbers may have the following average durations at different memory levels:

Memory	Duration	Cost
128 MB	11.722 s	$0.024628
256 MB	6.678 s	$0.028035
512 MB	3.194 s	$0.026830
1024 MB	1.465 s	$0.024638

AWS Lambda – Function Timeouts

Lambda functions can time out for a variety of reasons.

Best practices for preventing Lambda function timeouts

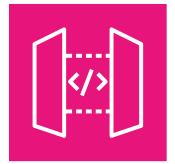
- Verify that your Lambda function has enough system resources
  - The amount of **network bandwidth and CPU allocated** to a Lambda function invocation is determined by the function's memory configuration.

- Verify that your Lambda function is configured to work within the maximum timeout settings of any integrated AWS services
  - Even though a Lambda function's **maximum invocation timeout limit is 15 minutes**, other AWS services may have different timeout limits.

- (Optional) Configure **provisioned concurrency** for your Lambda function
  - Provisioned concurrency initializes a requested number of runtime environments so that they're prepared to respond immediately to your function's invocations.

- See other best practices here

Amazon API Gateway



Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale.

Use API Gateway to create **REST APIs**

- An API Gateway REST API is made up of resources and methods. A resource is a logical entity that an app can access through a resource path. A method corresponds to a REST API request that is submitted by the user of your API and the response returned to the user.

Use API Gateway to create **HTTP APIs**

- HTTP APIs enable you to create RESTful APIs with lower latency and lower cost than REST APIs.
- You can use HTTP APIs to send requests to AWS Lambda functions or to any publicly routable HTTP endpoint.

Use API Gateway to create **WebSocket APIs**

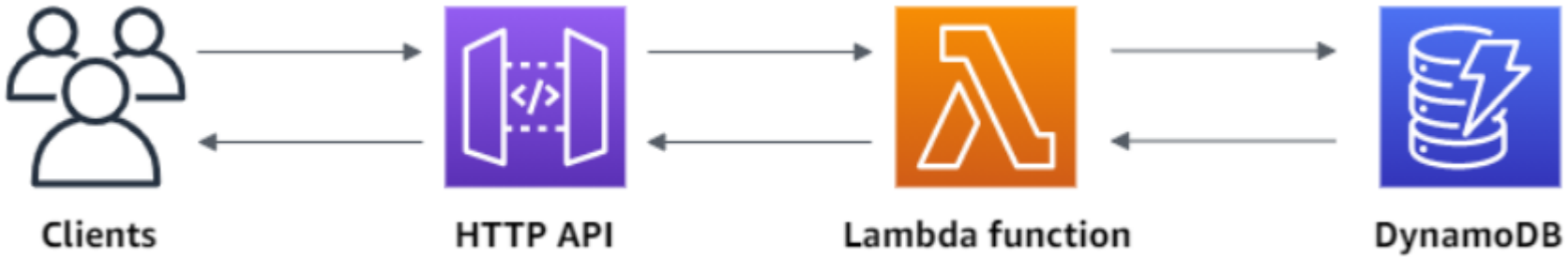
- In a WebSocket API, the client and the server can both send messages to each other at any time. Backend servers can easily push data to connected users and devices, avoiding the need to implement complex polling mechanisms.

Amazon API Gateway - Example

Example CRUD API with AWS Lambda and Amazon DynamoDB

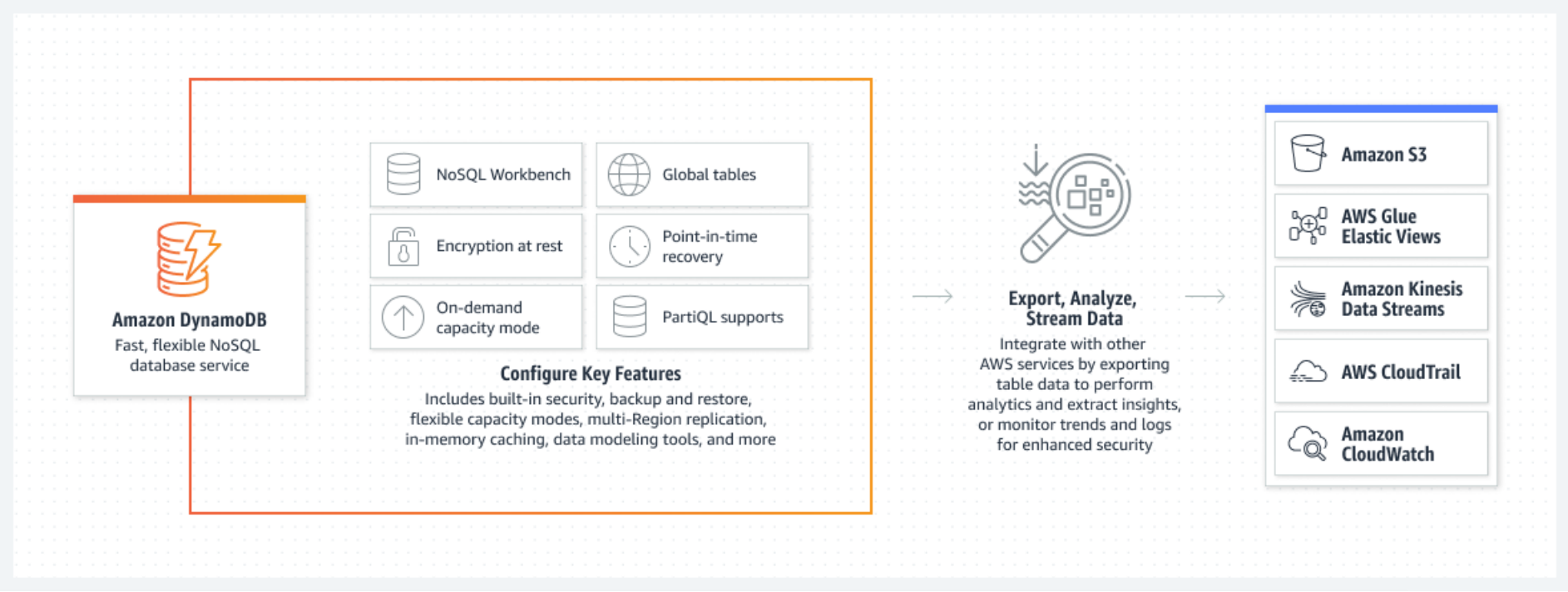
Let’s assume we have a serverless API that creates, reads, updates, and deletes items from a DynamoDB table.

1. When you invoke your **HTTP API**, API Gateway routes the request to your Lambda function.
2. The Lambda function interacts with DynamoDB, and returns a response to API Gateway.
3. API Gateway then returns a response to you.



Amazon DynamoDB

Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale.

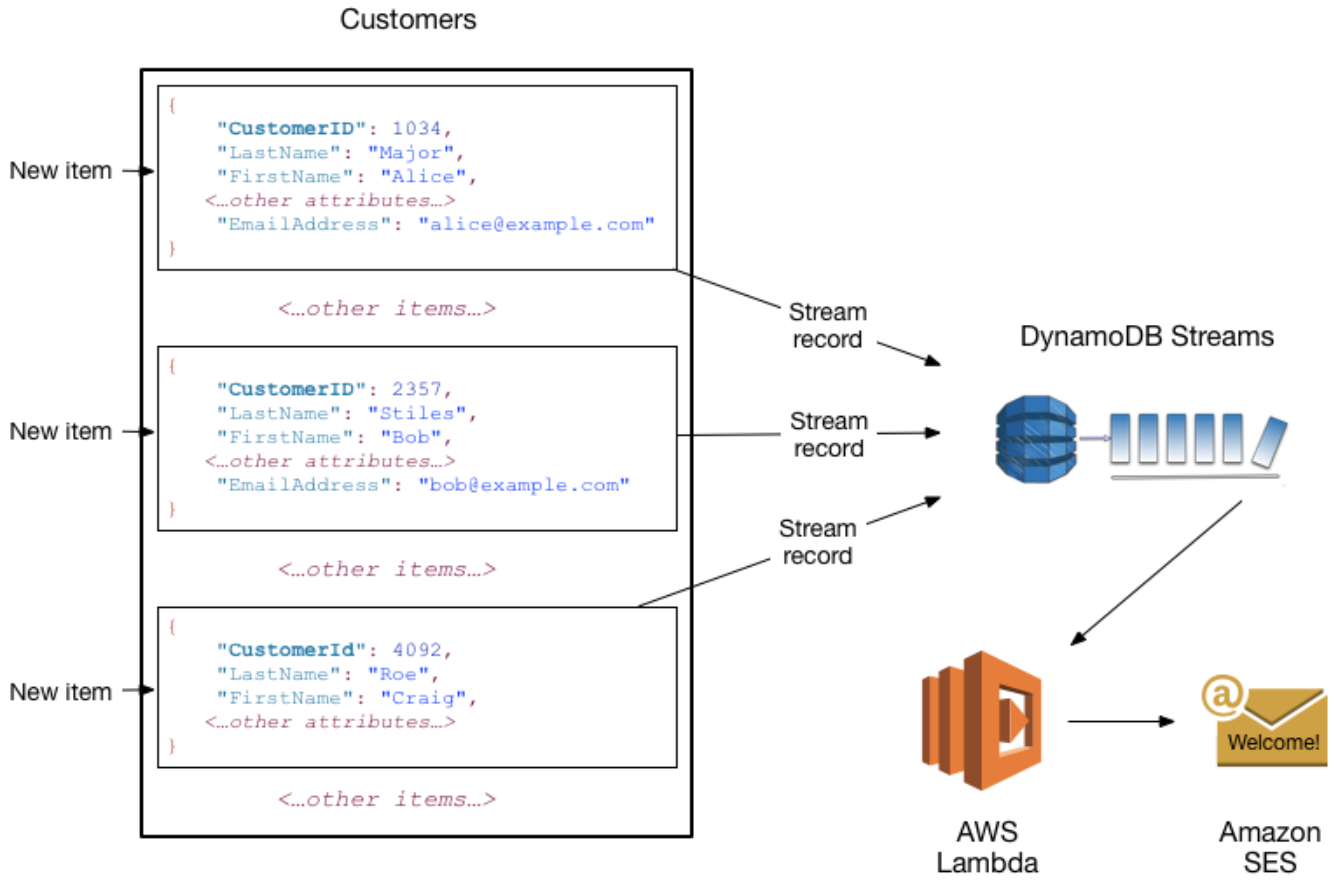


Amazon DynamoDB Streams

Amazon DynamoDB supports streaming of item-level change data capture records in near-real time. You can build applications that consume these streams and take action based on the contents.

DynamoDB Streams

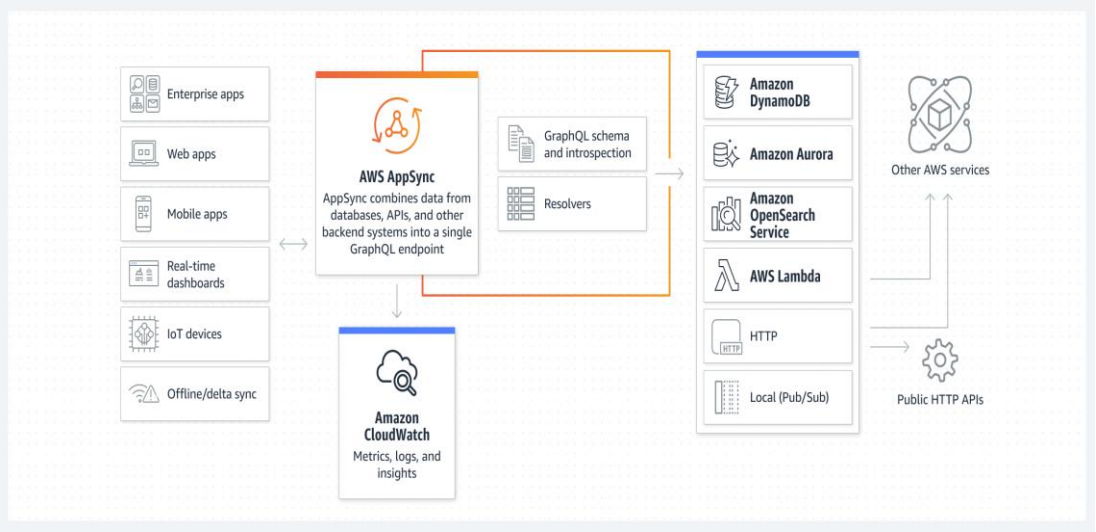
- DynamoDB Streams is an optional feature that captures data modification events in DynamoDB tables.
- You can use DynamoDB Streams together with AWS Lambda to create a trigger—code that runs automatically whenever an event of interest appears in a stream.



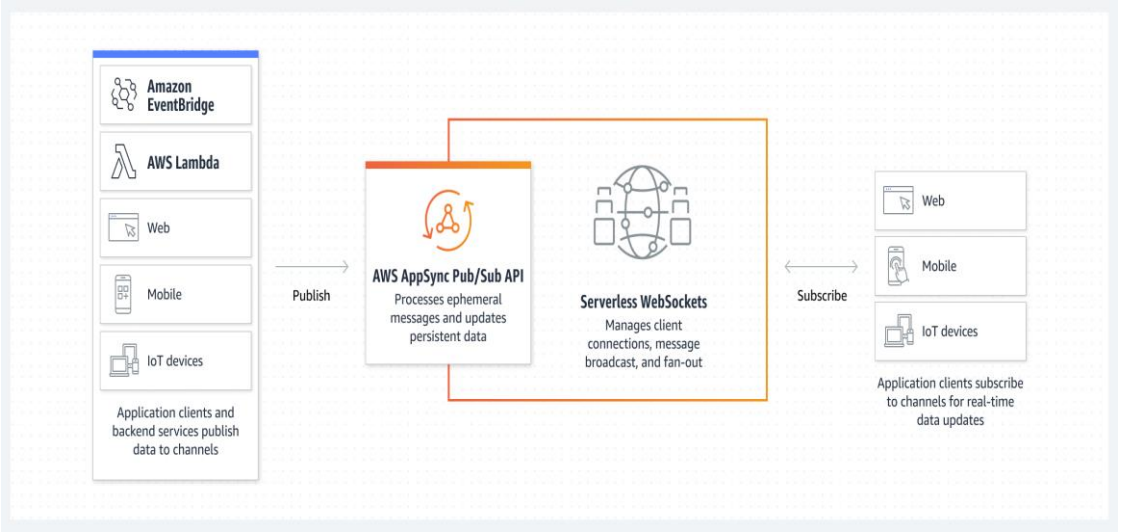
AWS AppSync

AWS AppSync creates serverless **GraphQL** and **Pub/Sub APIs** that simplify application development through a single endpoint to securely query, update, or publish data.

GraphQL APIs



Pub/Sub APIs

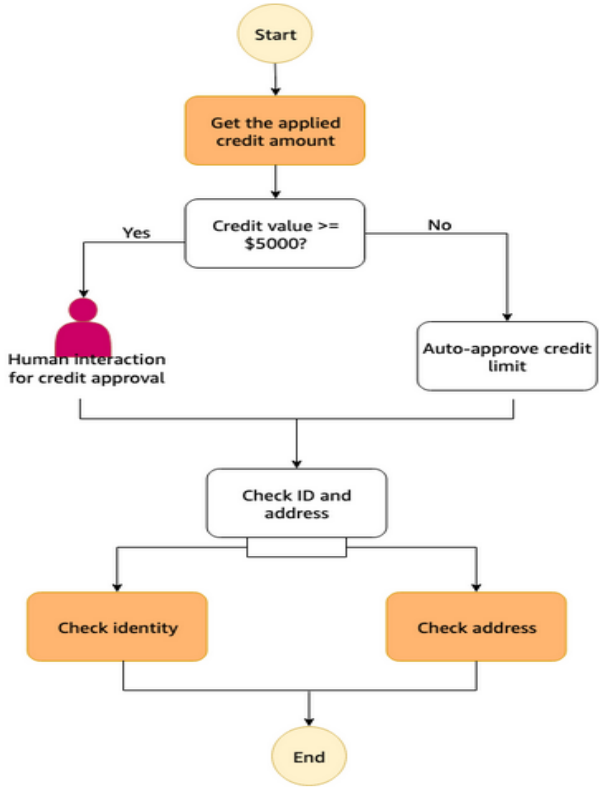


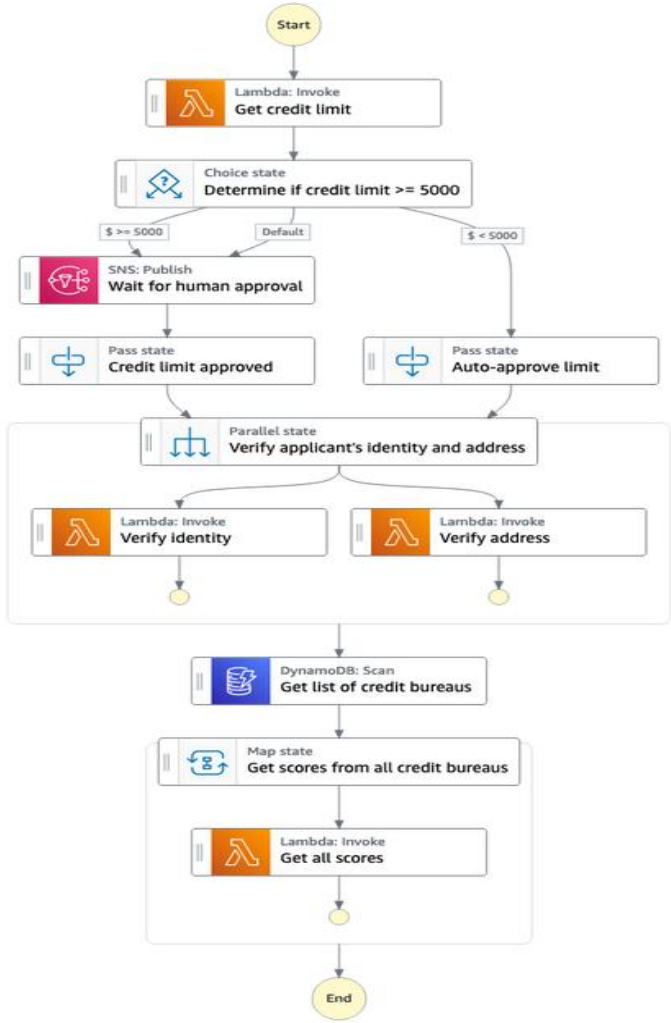
AWS Step Functions

AWS Step Functions is a fully managed service that makes it easier to coordinate the components of distributed applications and microservices using visual workflows.

The following images represent a credit card application workflow and how it appears when orchestrated using Step Functions.

Each step in the flowchart is represented with a state in the Step Functions workflow.





Amazon Cognito

aws training and certification

Amazon Cognito

Simple and Secure User Sign-Up, Sign-In, and Access Control

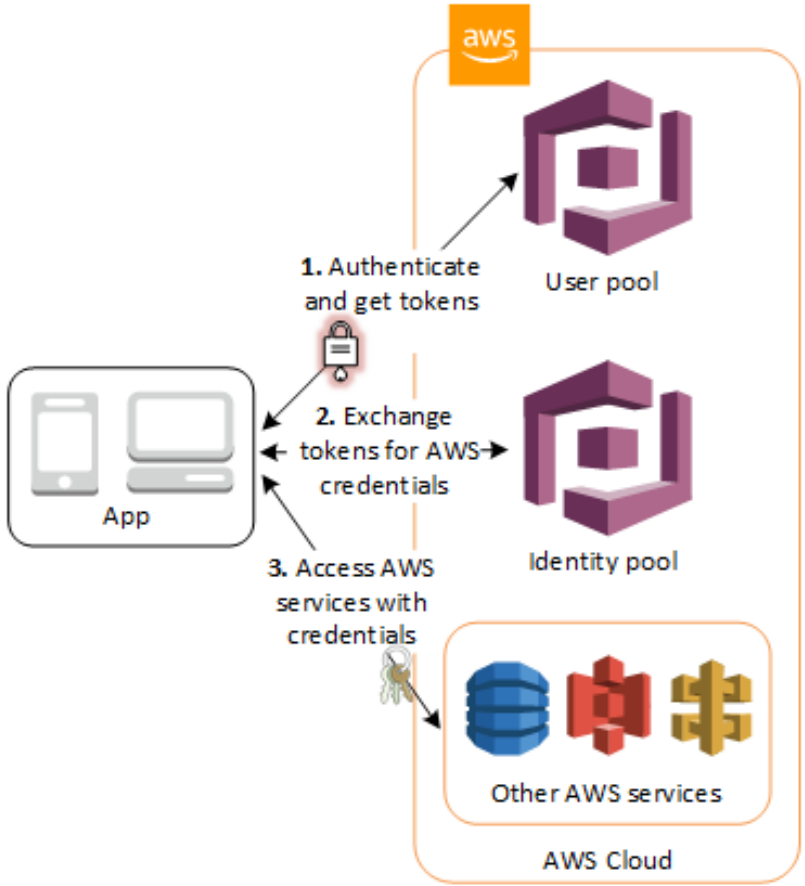
Overview

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, Google or Apple.

When would it be used?

You can enable your users to authenticate with a user pool. Your app users can sign in either directly through a user pool, or federate through a third-party identity provider (IdP).

The user pool manages the overhead of handling the tokens that are returned from social sign-in through Facebook, Google, Amazon, and Apple, and from OpenID Connect (OIDC) and SAML IdPs. After a successful authentication, your web or mobile app will receive user pool tokens from Amazon Cognito.



aws training and certification

Containers on AWS

aws training and certification

Containers

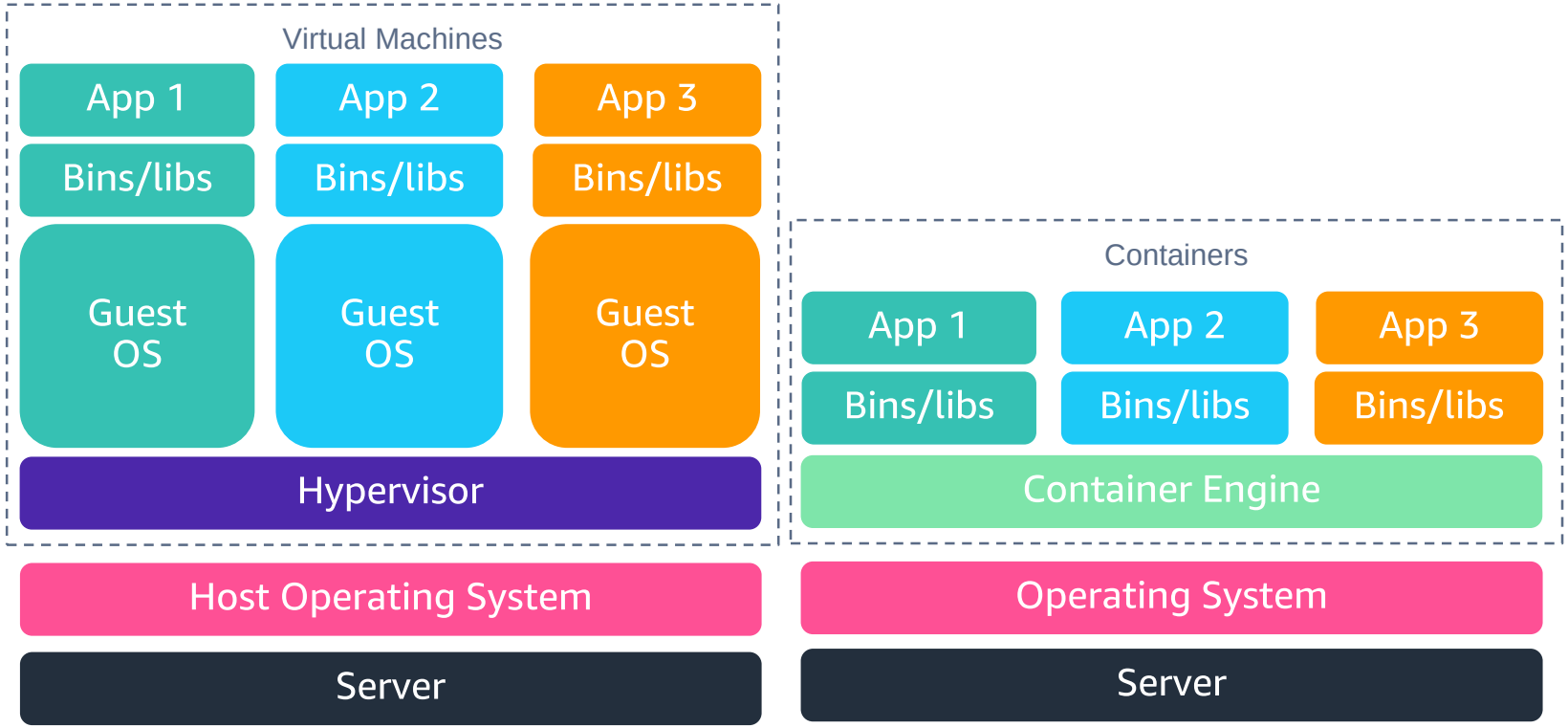
Lightweight, standardized packaging for application code, config, and dependencies

Why

Portable method to package and deploy applications to run and scale anywhere. Suitable for deploying microservices, running batch jobs, for ML applications, and migrating applications to the cloud.

How it Works

Container images contain all the code, runtime, system libraries, dependencies, and configuration required for the application to run. Abstraction at the application layer allows containers to share the OS resources. Container engines "run" the images.



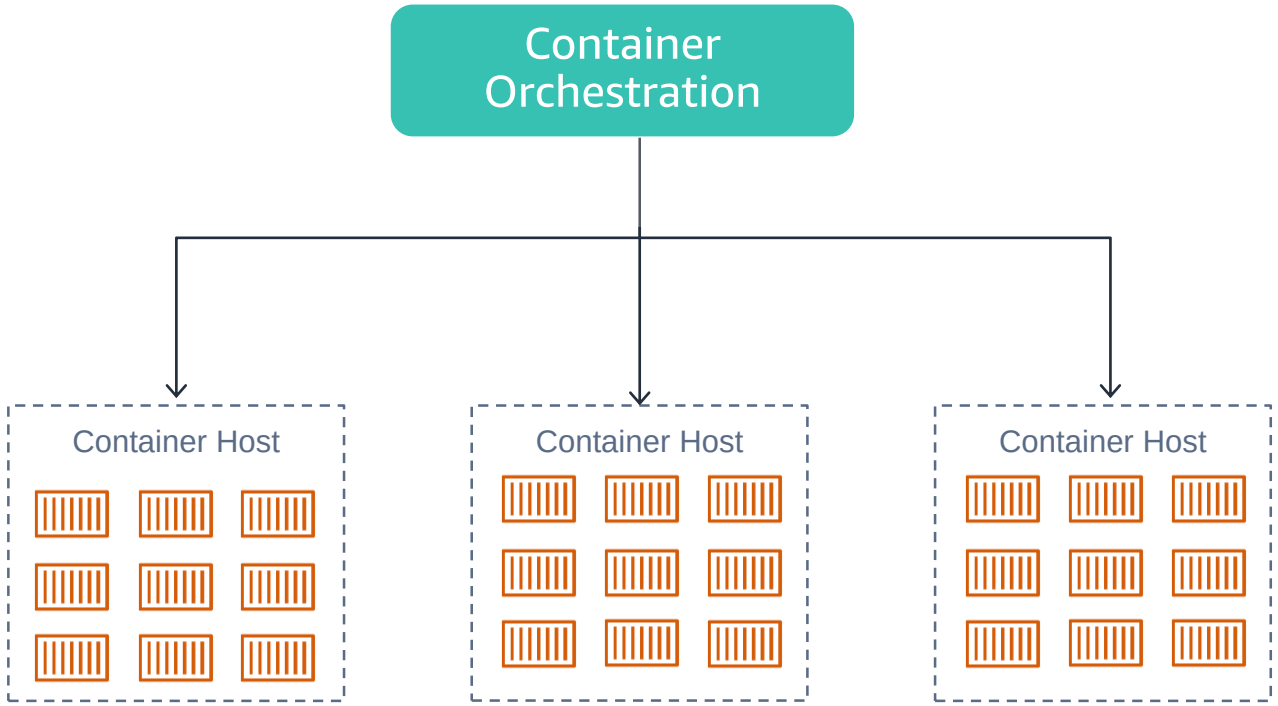
aws training and certification

Container Orchestration

Automates scheduling, development, networking, scaling, health monitoring, and management of containers.

What it is

Container orchestration automates the scheduling, development, networking, scaling, health monitoring, and management of your containers. Orchestration keeps containers running in the required state, and helps maintain your service-level agreements (SLAs).



Amazon Elastic Container Service

Highly secure, reliable, and scalable way to run containers

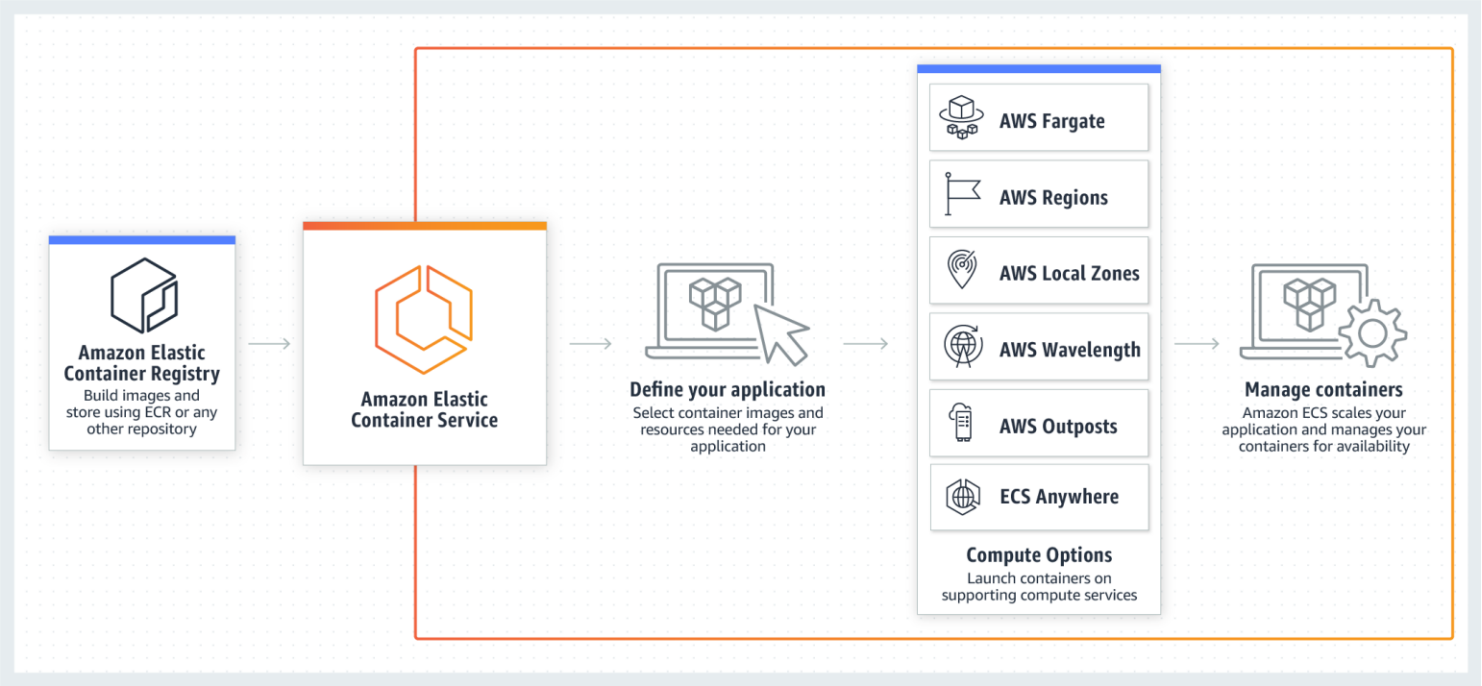
Fully managed container orchestration service that helps you easily deploy, manage, and scale containerized applications

Manage

Amazon ECS enables you to launch and stop your container-based applications by using simple API calls

Offload

With Amazon ECS, you don't have to operate your own cluster management and configuration management systems or worry about scaling your management infrastructure



aws training and certification

Amazon Elastic Kubernetes Service

The most trusted way to start, run, and scale Kubernetes

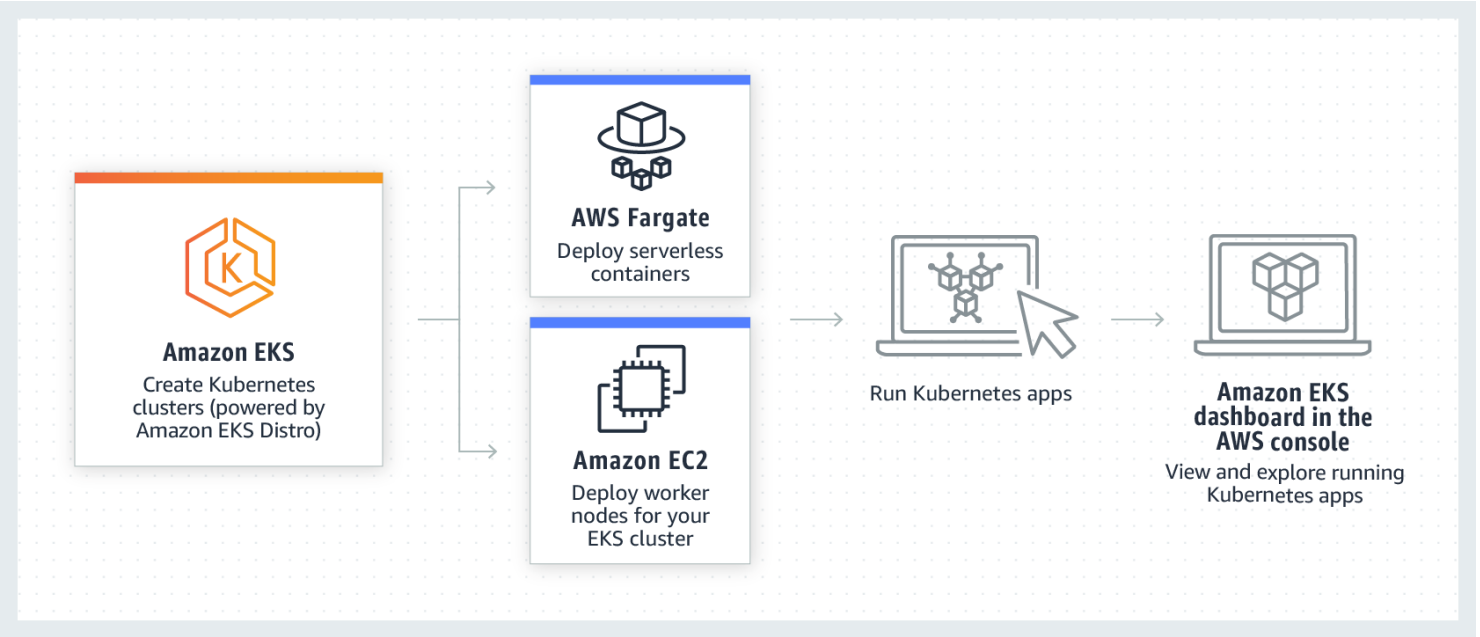
Gives you the flexibility to start, run, and scale Kubernetes applications in the AWS Cloud or on-premises. Runs upstream Kubernetes and is certified Kubernetes conformant

Availability

EKS runs the Kubernetes control plane across multiple Availability Zones, automatically detects and replaces unhealthy control plane nodes, and provides on-demand, zero downtime upgrades and patching

Scalability

With EKS managed node groups, you don't need to separately provision compute capacity to scale your Kubernetes applications



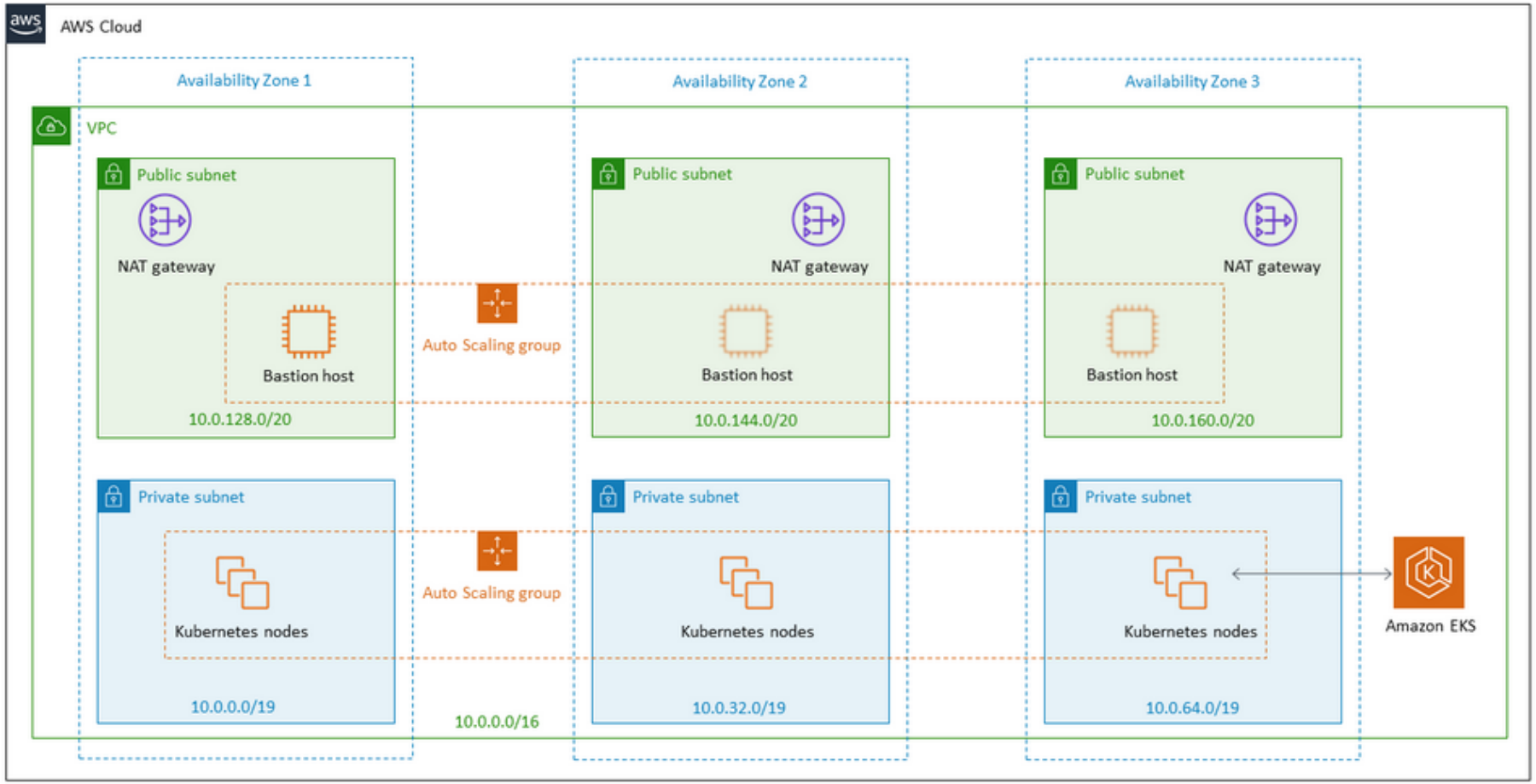
aws training and certification

Amazon EKS Example

EKS with a highly available architecture that spans three Availability Zones

Functionality

Amazon EKS is integrated with multiple AWS services to provide scalability and security for your applications. These services include Elastic Load Balancing for load distribution, IAM for authentication, Amazon Virtual Private Cloud (Amazon VPC) for isolation, and AWS CloudTrail for logging.



AWS Fargate

Serverless compute for containers

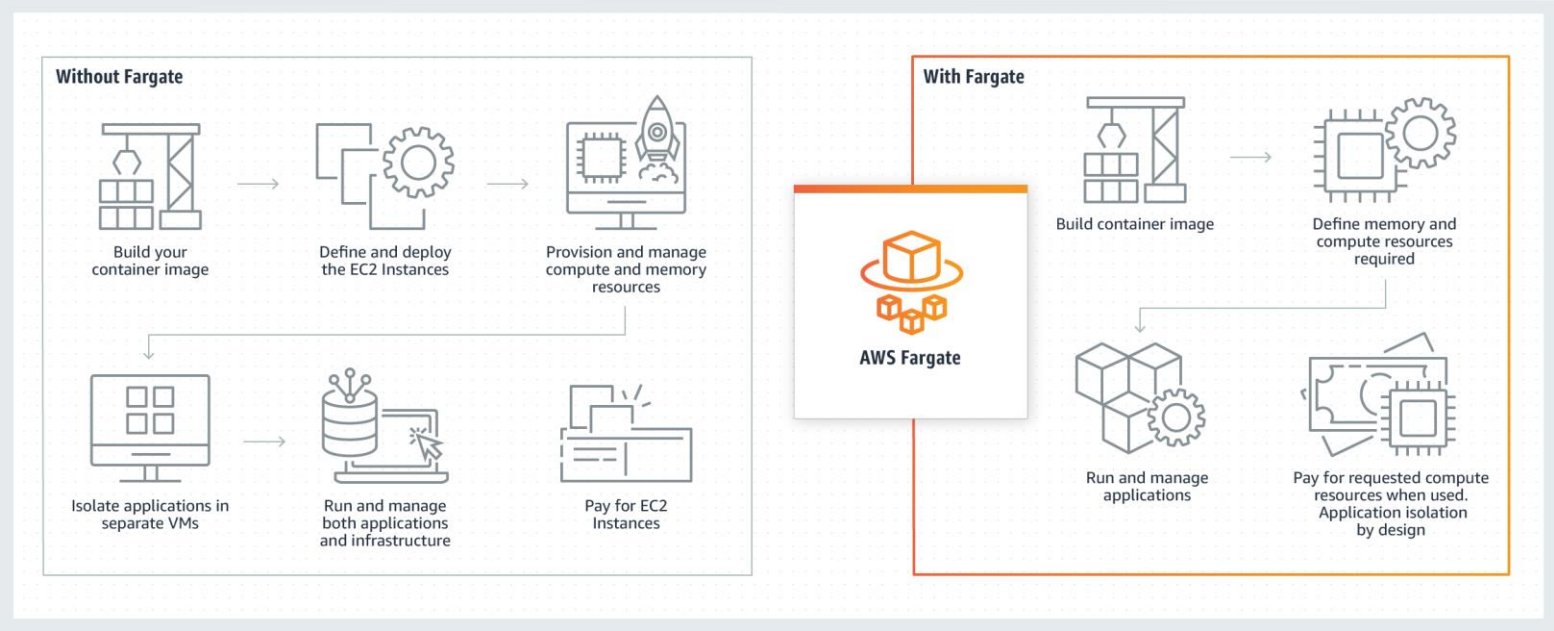
Serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers

Scale Containers

Use Fargate with Amazon ECS or Amazon EKS to easily run and scale your containerized data processing workloads.

Build Microservices

Fargate removes the need to own, run, and manage the lifecycle of a compute infrastructure



aws training and certification

Additional AWS Security Services

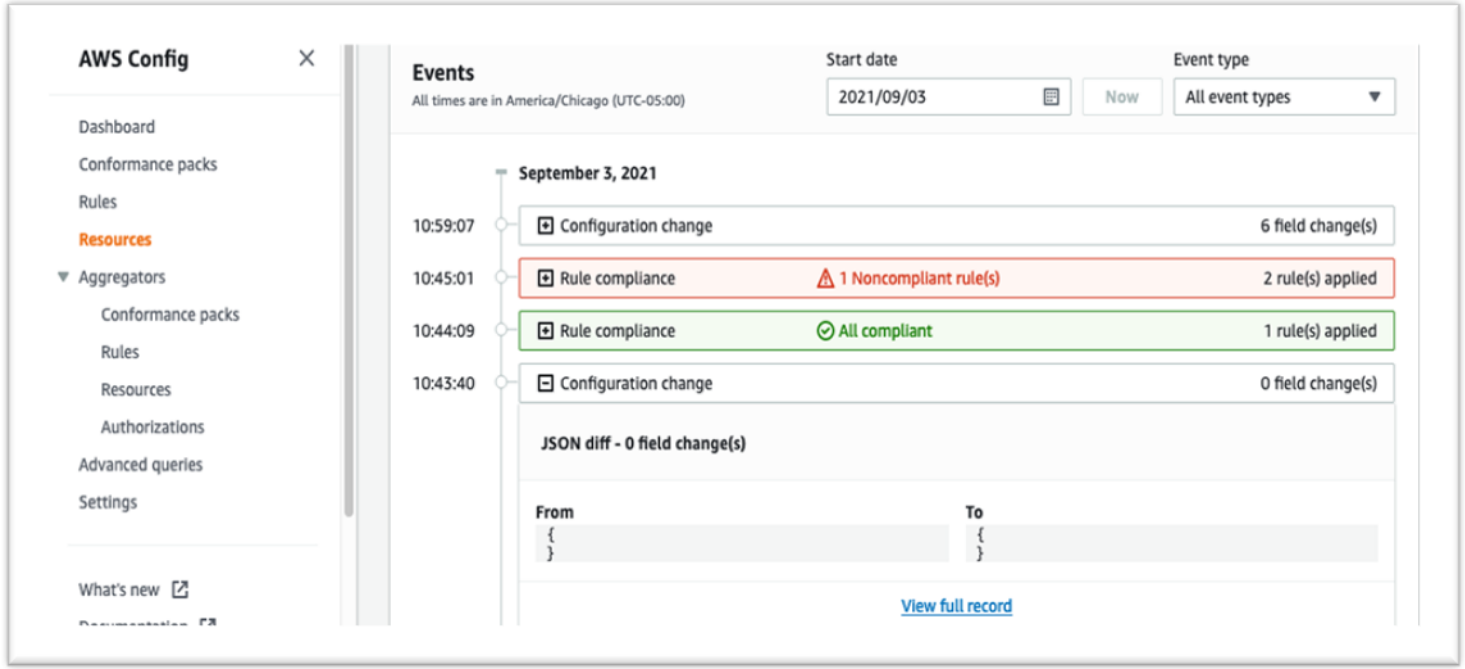
aws training and certification

AWS Config – Compliance management

AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources on AWS, on premises, and on other clouds.

AWS Config can help address questions like:

- Are my resources properly configured?
- Do my resources comply with regulatory requirements?
- How do I ensure continuous compliance?
- How can I get notified in near real-time if resource(s) go out of compliance?

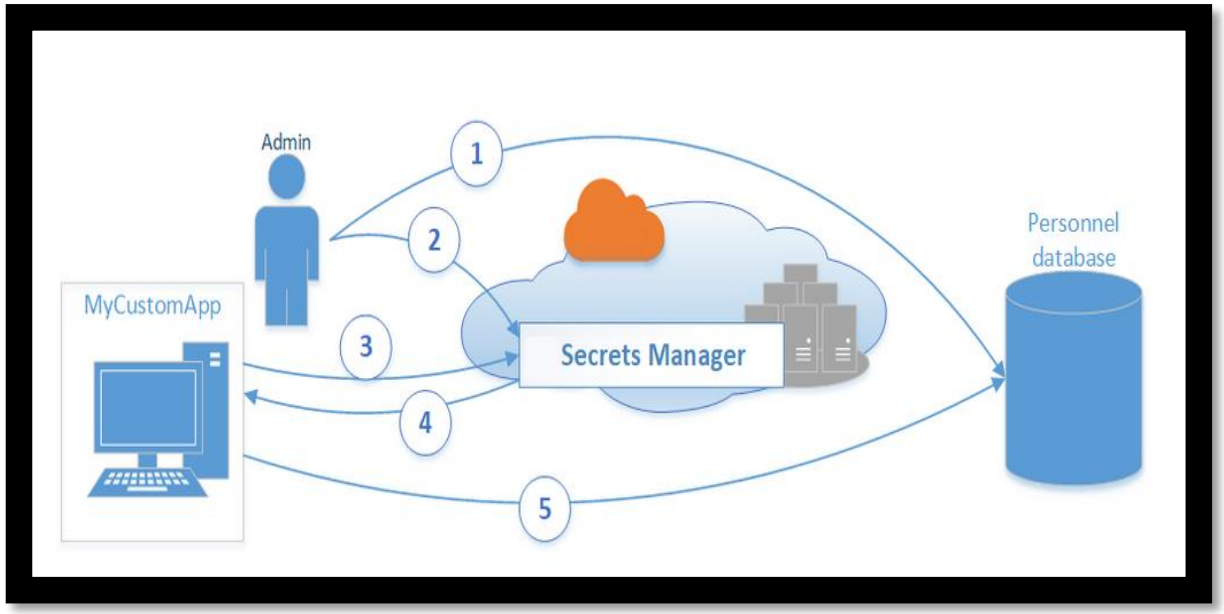


AWS Secrets Manager

AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their lifecycles.

Key Features

- You can configure Secrets Manager to automatically rotate your secrets without user intervention and on a specified schedule.
- Secrets Manager encrypts the protected text of a secret by using AWS Key Management Service (AWS KMS).
- Secrets Manager helps you improve your security posture by removing hard-coded credentials from your application source code, and by not storing credentials within the application, in any way.



AWS Certificate Manager (ACM)

Provision and manage SSL/TLS certificates with AWS services and connected resources

Key Concepts

Protect and secure your website

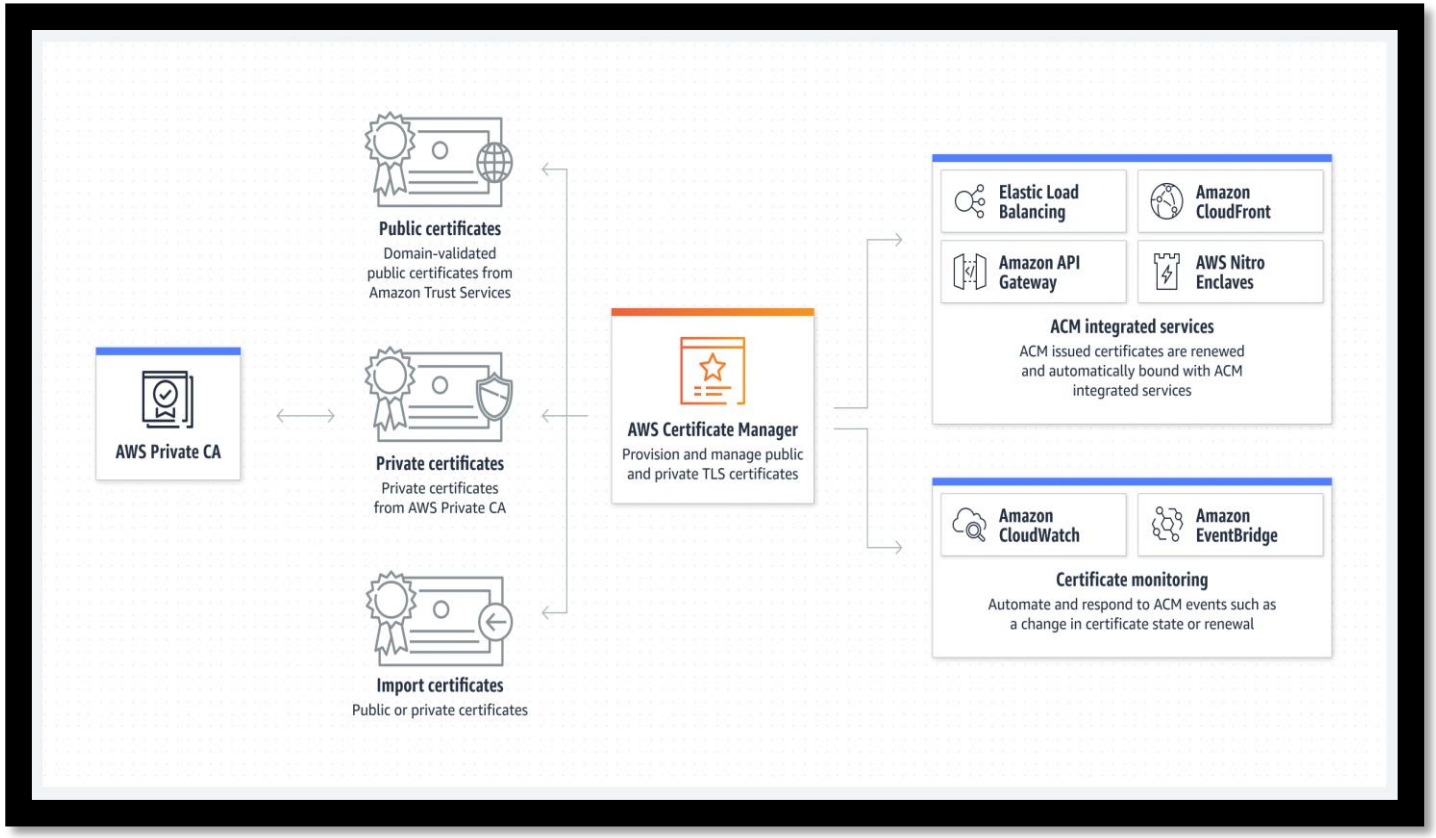
- Provision and manage certificates so you can securely stop traffic to your website or application.

Protect your internal resources

- Secure communication between connected resources on private networks, such as servers, mobile and IoT devices, and applications.

Improve uptime

- Maintain SSL/TLS certificates, including certificate renewals, with automated certificate management.

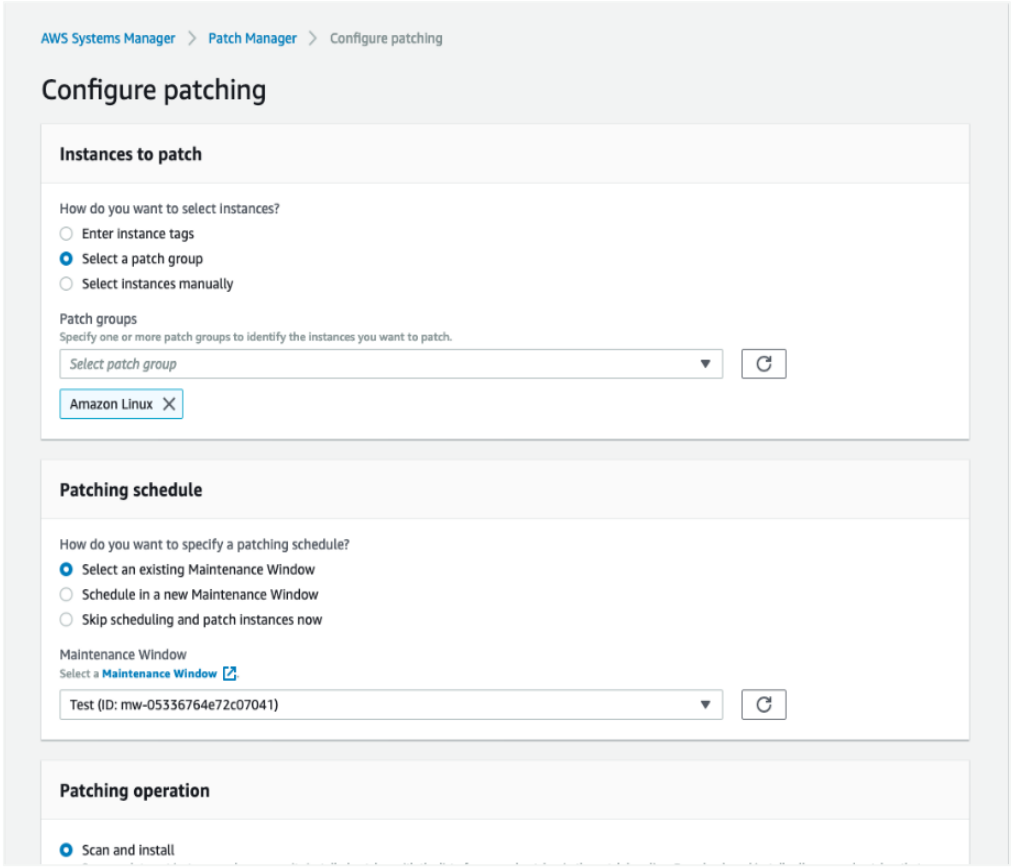


AWS Systems Manager Patch Manager

Systems Manager Patch Manager

Automate the process of patching your instances

- Automate patching by defining rules for auto approval
- Scan and install patches on a regular basis by scheduling maintenance windows
- View aggregate patch compliance using Explorer

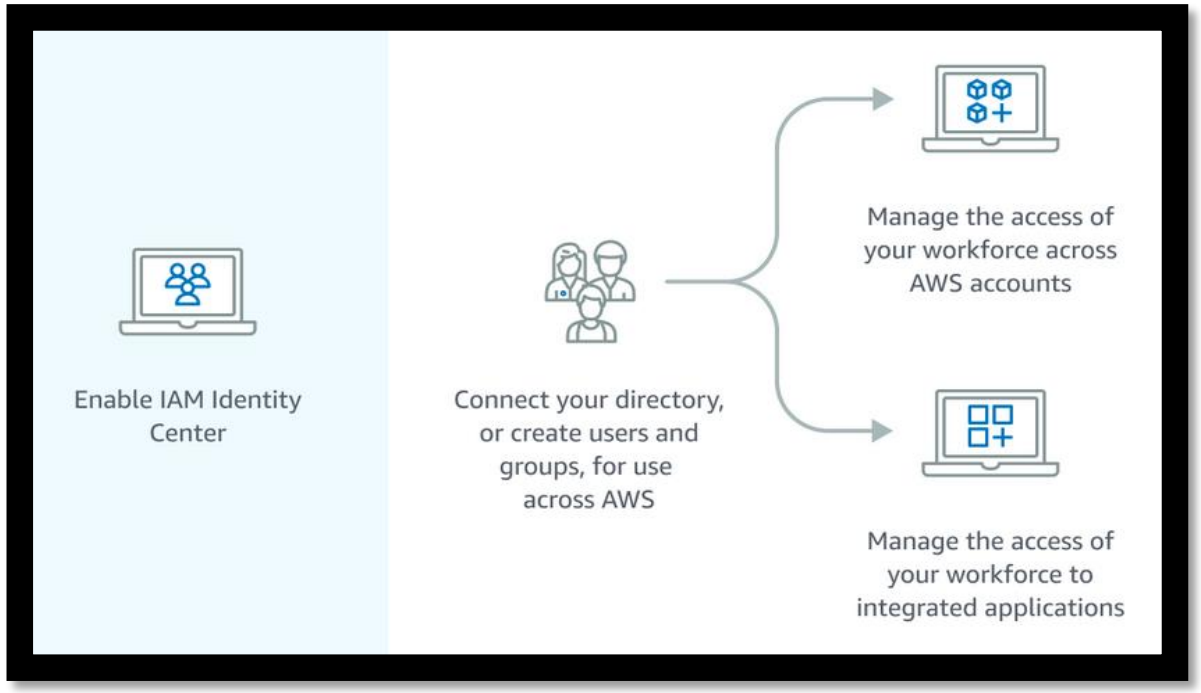


AWS IAM Identity Center (formerly AWS SSO)

AWS IAM Identity Center (successor to AWS Single Sign-On) helps you securely create or connect your workforce identities and manage their access centrally across AWS accounts and applications.

Key Concepts

- Active Directory should be used if you want to continue managing users in either your AWS Managed Microsoft AD directory using AWS Directory Service or your self-managed directory in Active Directory (AD).
- External identity provider should be used if you want to manage users in an external identity provider (IdP) such as Okta or Azure Active Directory.



AWS Directory Service

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, activates your directory-aware workloads and AWS resources to use managed AD on AWS.

If you need Active Directory or LDAP for your applications in the cloud:

Use **AWS Directory Service for Microsoft Active Directory** if you need an actual Microsoft Active Directory in the AWS Cloud that supports Active Directory–aware workloads, or AWS applications and services such as Amazon WorkSpaces and Amazon QuickSight

Use **AD Connector** if you only need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials.

Use **Simple AD** if you need a low-scale, low-cost directory with basic Active Directory compatibility that supports Samba 4–compatible applications, or you need LDAP compatibility for LDAP-aware applications.

Or if you develop high-scale SaaS applications and need a scalable directory to manage and authenticate your subscribers and that works with social media identities.

Use **Amazon Cognito**

aws training and certification

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) helps you securely share the AWS resources that you create in one AWS account with other AWS accounts.

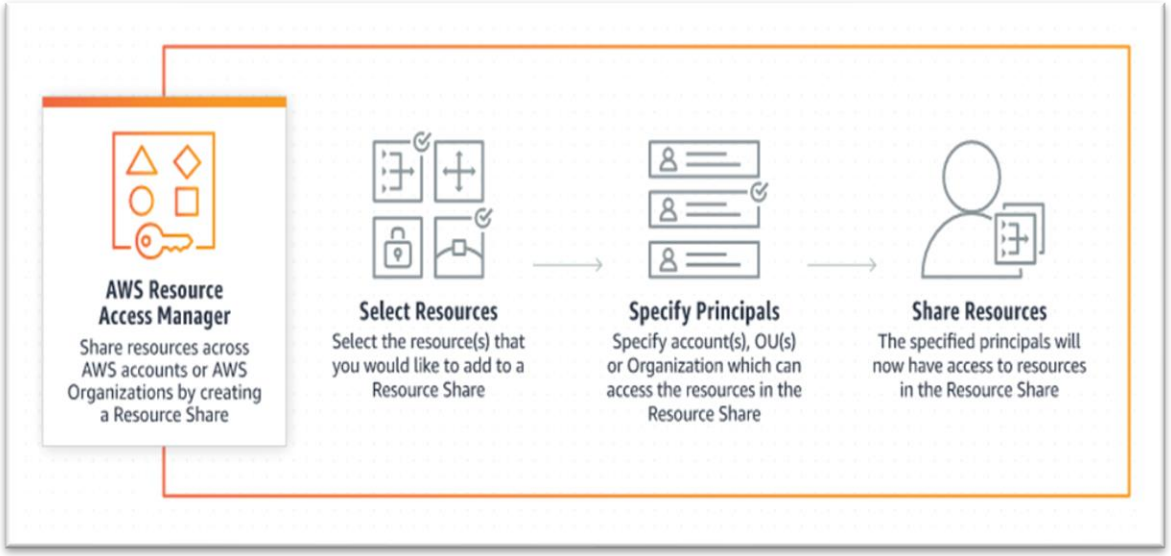
Example Use Cases

Share resources in multi-account environments

- Share foundational infrastructure like Amazon VPC subnets across accounts, allowing multiple accounts to deploy application resources to the same subnet

Centrally govern access to resources

- Centrally manage resources like private certificate authorities allowing certificate issuance across multiple accounts to manage cost and reduce operational overhead

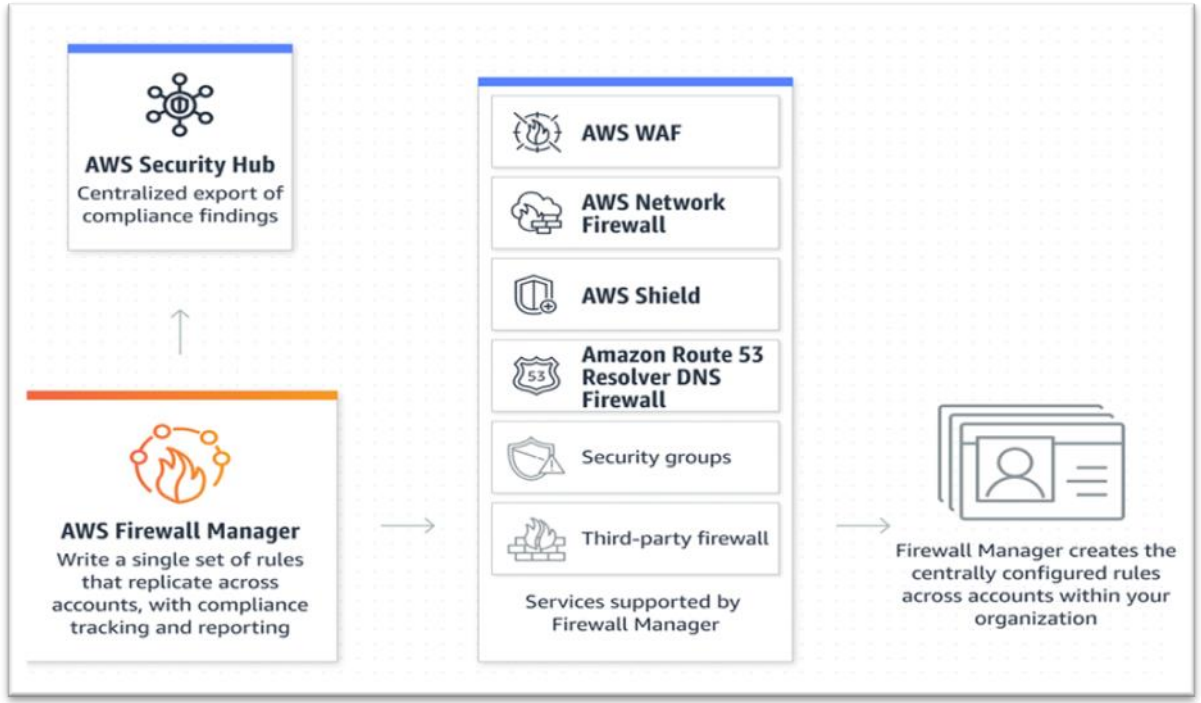


AWS Firewall Manager

AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations.

Key Takeaways

- AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections, including:
  - AWS WAF
  - AWS Shield Advanced
  - Amazon VPC security groups
  - AWS Network Firewall
  - Amazon Route 53 Resolver DNS Firewall



AWS Trusted Advisor and AWS Audit Manager

AWS Trusted Advisor Key Takeaways

- Trusted Advisor inspects your AWS environment and makes recommendations for saving money, improving system performance, or closing security gaps.
- With a Basic or Developer Support plan, Trusted Advisor provides access to all checks in the Service Limits category and six checks in the Security category (listed below):
  - Amazon EBS Public Snapshots
  - Amazon RDS Public Snapshots
  - Amazon S3 Bucket Permissions
  - IAM Use
  - MFA on Root Account
  - Security Groups – Specific Ports Unrestricted

AWS Audit Manager Key Takeaways

- AWS Audit Manager helps you continually audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.
- AWS Audit Manager integrates with multiple AWS services to automatically collect evidence that you can include in your assessment reports. Services that integrate with Audit Manager include:
  - AWS Security Hub
  - AWS CloudTrail
  - AWS Config
  - AWS License Manager
  - AWS Control Tower
  - AWS Artifact

AWS CloudHSM

AWS CloudHSM provides cloud-based hardware security modules (HSMs) for generating and using your own encryption keys in the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs and integrate with your applications using industry-standard APIs.

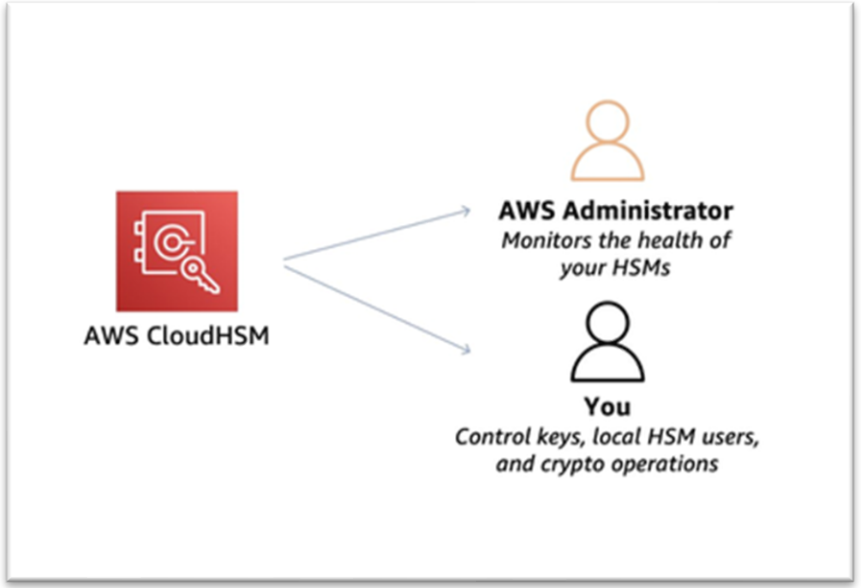
Important Concepts

When Do I Use It?

- Use AWS CloudHSM when you need to manage the HSMs that generate and store your encryption keys.

When Do I Use Something Else?

- If you need to secure your encryption keys in a service backed by FIPS-validated HSMs, but you do not need to manage the HSM, try AWS Key Management Service.



Thank you!

aws training and certification