



AWS Certified Solution Architect Associate

TELCOMA



AWS Certifications

AWS Certifications



Architecting



AWS Certified
Solutions Architect

Associate



AWS Certified
Solutions Architect

Professional



Developing



AWS Certified
Developer

Associate



AWS Certified
DevOps Engineer

Professional



Operations



AWS Certified
SysOps Administrator

Associate

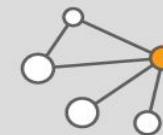


AWS Certified
DevOps Engineer

Professional

Specialty Certifications

Requires one current Associate or Professional Certification



AWS Certified
Advanced Networking

Specialty



AWS Certified
Big Data

Specialty



AWS Certified Solution Architect

Associate

Domain	% of Examination
1.0 Designing highly available, cost efficient, fault tolerant, scalable systems	60%
2.0 Implementation/Deployment	10%
3.0 Data Security	20%
4.0 Troubleshooting	10%
TOTAL	100%

About exam

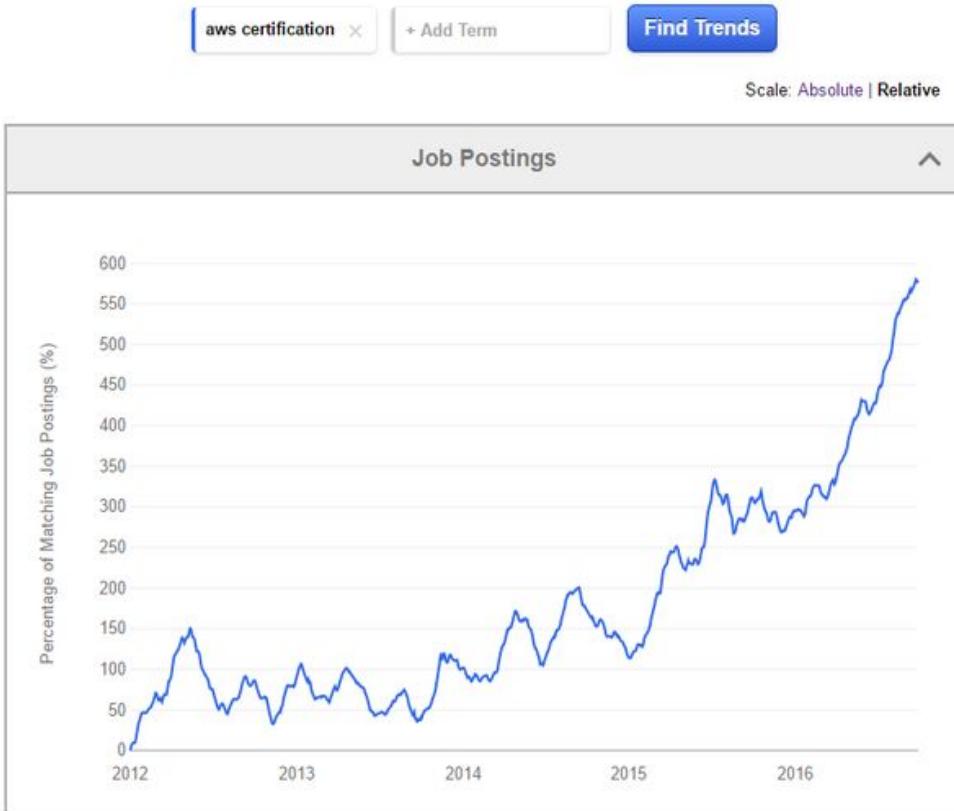
- Total duration : 80 mins
- Total questions : 60 (this can change)
- Type of questions : multiple choice
- Passing marks : based on bell curve (it moves around)
- Aim : to get min 65%
- Validity : 2 years
- Type of questions : scenario based

Why AWS Certification?

Certification	U.S. & Canada			Latin America			EMEA			Asia-Pacific			Total		
	Mean	Median	Count	Mean	Median	Count	Mean	Median	Count	Mean	Median	Count	Mean	Median	Count
Certified in Risk Systems and Control (CRISC)	\$127,507	\$122,900	159	\$61,730	\$46,651	10	\$82,959	\$82,000	65	\$79,546	\$68,000	33	\$108,271	\$109,000	267
Certified Information Security Manager (CISM)	\$122,448	\$120,000	276	\$49,453	\$41,850	33	\$71,534	\$68,500	252	\$86,285	\$70,000	124	\$93,655	\$90,025	685
AWS Certified Solutions Architect – Associate	\$119,085	\$118,350	304	\$58,425	\$36,400	17	\$62,169	\$60,000	202	\$57,346	\$39,618	202	\$84,603	\$80,000	725
Certified Information Systems Security Professional (CISSP)	\$118,179	\$115,000	304	\$43,428	\$47,000	9	\$77,208	\$74,500	116	\$94,334	\$85,110	69	\$103,981	\$100,000	498
Certified Information Systems Auditor (CISA)	\$110,634	\$106,059	588	\$45,886	\$38,000	71	\$66,897	\$64,750	416	\$73,071	\$62,750	262	\$86,226	\$83,000	1337
PMP®: Project Management Professional	\$105,324	\$100,000	293	\$46,783	\$39,500	18	\$53,521	\$52,000	50	\$77,217	\$59,700	73	\$92,200	\$84,344	434
Citrix Certified Professional – Virtualization (CCP-V)	\$102,353	\$97,000	153	\$31,213	\$31,700	30	\$65,850	\$61,875	182	\$50,091	\$29,230	83	\$73,077	\$70,000	448
Citrix Certified Associate – Networking (CCA-N)	\$98,583	\$92,000	163	\$30,691	\$25,750	28	\$58,080	\$52,850	128	\$58,062	\$41,834	56	\$73,637	\$69,000	375
VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV)	\$96,309	\$90,000	159	\$42,180	\$36,000	15	\$57,332	\$53,300	139	\$48,938	\$37,475	83	\$70,649	\$68,000	396
Citrix Certified Associate – Virtualization (CCA-V)	\$96,231	\$92,000	241	\$30,193	\$30,000	41	\$58,190	\$55,000	244	\$41,602	\$24,300	158	\$66,084	\$62,975	684
MCSE: Server Infrastructure	\$94,921	\$92,000	329	\$30,927	\$24,328	28	\$54,305	\$50,775	250	\$61,939	\$35,500	116	\$73,107	\$70,000	723
ITIL® v3 Foundation	\$93,638	\$88,000	891	\$34,187	\$28,160	132	\$56,601	\$52,000	664	\$55,945	\$40,000	434	\$70,630	\$65,800	2121
CompTIA Project+	\$92,593	\$88,000	205	\$33,821	\$43,000	3	\$48,275	\$50,000	27	\$67,063	\$55,500	16	\$85,496	\$81,555	251
CCNP Routing and Switching	\$90,945	\$89,550	193	\$30,968	\$24,578	70	\$37,114	\$28,500	275	\$26,422	\$14,962	193	\$47,915	\$35,000	731
MCSA: SQL Server	\$90,303	\$83,750	188	\$32,103	\$23,157	27	\$48,632	\$45,000	125	\$48,553	\$30,000	57	\$67,230	\$60,000	397
MCSA: Windows Server	\$89,941	\$84,000	628	\$31,505	\$24,828	70	\$50,042	\$45,500	591	\$41,031	\$21,231	290	\$63,434	\$60,000	1579
CompTIA Security+	\$87,666	\$83,000	678	\$32,314	\$23,750	18	\$53,490	\$46,944	101	\$60,210	\$53,500	35	\$81,165	\$78,000	832
CCNA Security	\$84,652	\$80,000	185	\$29,210	\$24,000	41	\$38,193	\$28,440	164	\$29,783	\$16,057	79	\$54,317	\$48,000	469
CCNA Routing and Switching	\$80,873	\$75,000	799	\$24,463	\$18,197	270	\$32,873	\$25,000	825	\$22,700	\$12,000	612	\$44,787	\$34,000	2506
CompTIA Network+	\$79,435	\$75,000	760	\$29,280	\$24,775	27	\$44,747	\$38,498	140	\$41,370	\$27,000	28	\$71,816	\$68,000	955

Source: Global Knowledge

Why AWS Certification





AWS SERVICES

What is AWS?

Amazon Web Services (AWS), a subsidiary of Amazon.com, offering
cloud-computing services

Cloud Computing or simply **Cloud** means, 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

Cloud Computing provides on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services)

AWS Global infrastructure

- AWS locations : regions and availability zones
- 43 availability zones
- 16 regions
- 11 Availability zones and 4 regions - plan to launch
- Placement of data and resources in multiple locations.
- Regions are isolated to each other.

Accessing platform

To access AWS cloud services , you can use

- AWS management console
- AWS command line interface
- AWS software development kits

AWS management console

- It is a web application for managing AWS cloud services. It provides an interactive user interface. Each service has its own console which can be accessed by AWS management console.
- It also provides information about account and billing.

AWS command line interface

- It is a unified tool used to manage AWS cloud services.
- With just one tool to download and configure , you can control multiple services from the command line and automate them using scripts.

AWS software development kits

- It provides an application programming interface that interacts with web services that fundamentally make up the AWS platform.
- SDKs provide support for many different programming languages.
- SDKs can take the complexity out of coding by providing programmatic access for many of the services.



Sign in to AWS management console

Getting Started

To create an AWS account

1. Open <https://aws.amazon.com/>, and then choose **Create an AWS Account**.
2. Follow the online instructions.
3. Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

AWS SERVICES

Services | Resource Groups

History	Compute	Developer Tools	Analytics	Application Services
Console Home	EC2	CodeStar	Athena	Step Functions
Billing	EC2 Container Service	CodeCommit	EMR	SWF
IAM	Lightsail	CodeBuild	CloudSearch	API Gateway
EC2	Elastic Beanstalk	CodeDeploy	Elasticsearch Service	Elastic Transcoder
DynamoDB	Lambda	CodePipeline	Kinesis	
	Batch	X-Ray	Data Pipeline	
			QuickSight	
	Storage	Management Tools	Artificial Intelligence	Messaging
	S3	CloudWatch	Lex	Simple Queue Service
	EFS	CloudFormation	Polly	Simple Notification Service
	Glacier	CloudTrail	Rekognition	SES
	Storage Gateway	Config	Machine Learning	
	Database	OpsWorks		
	RDS	Service Catalog		Business Productivity
	DynamoDB	Trusted Advisor		WorkDocs
	ElastiCache	Managed Services		WorkMail
	Redshift			Amazon Chime
	Networking & Content Delivery	Security, Identity & Compliance	Internet Of Things	Desktop & App Streaming
	VPC	IAM	AWS IoT	WorkSpaces
	CloudFront	Inspector		AppStream 2.0
	Direct Connect	Certificate Manager	Contact Center	
	Route 53	Directory Service	Amazon Connect	
	Migration	WAF & Shield	Game Development	
	Application Discovery Service	Compliance Reports	Amazon GameLift	
	DMS		Mobile Services	
	Server Migration		Mobile Hub	
	Snowball		Cognito	
			Device Farm	
			Mobile Analytics	
			Pinpoint	



Compute

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Compute



Compute

EC2

EC2 Container Service

Lightsail

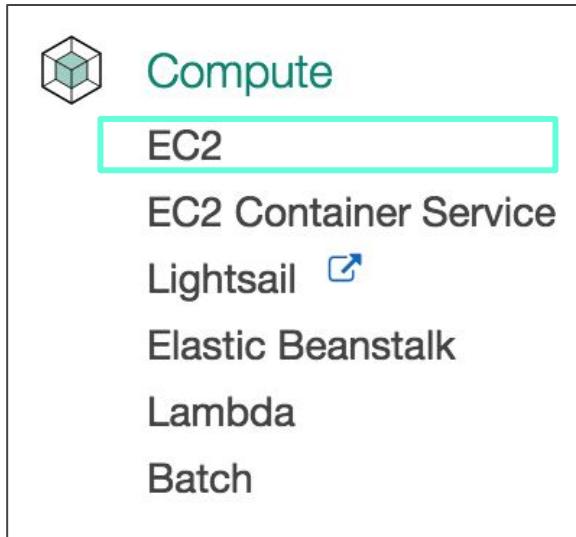
Elastic Beanstalk

Lambda

Batch

- AWS Compute is model which enables on-demand access to a pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services)
- AWS offers multiple compute products allowing you to deploy, run, and scale your applications as virtual servers, containers, or code.

EC2



- Amazon **Elastic Compute Cloud** (Amazon EC2) is a web service that provides secure, resizable server instances (called Amazon EC2 instances)
- Instance types comprise varying combinations of CPU, memory, storage, and networking capacity according to the needs of your applications.

EC2 Container Service



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

- Using containers, everything required to make a piece of software run is packaged into isolated containers.
- Docker is an open-source project that automates the deployment of applications inside software containers.
- ECS allows you to easily run applications on a managed cluster of Amazon EC2 instances

Lightsail



Compute

EC2

EC2 Container Service

Lightsail 

Elastic Beanstalk

Lambda

Batch

- Amazon Lightsail is designed to be the easiest way to launch and manage a **Virtual Private Server** with AWS.
- Lightsail is a lightweight , simplified product offering dramatically simplified console. Lightsail instances are just like regular EC2 instances.

Elastic Beanstalk



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

- AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, & Docker.
- You can simply upload your code, and AWS Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto scaling to application health monitoring.

Lambda



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

- Lambda, you can run code for virtually any type of application or backend service.
- Code can be setup to automatically trigger from other AWS services, or can be called directly from any web or mobile app
- Eg. You can write a image resizing code for Lambda and when you upload image to AWS, it would be automatically resized.

Batch



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

- AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.
- AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted.



Storage

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Storage



Storage

S3

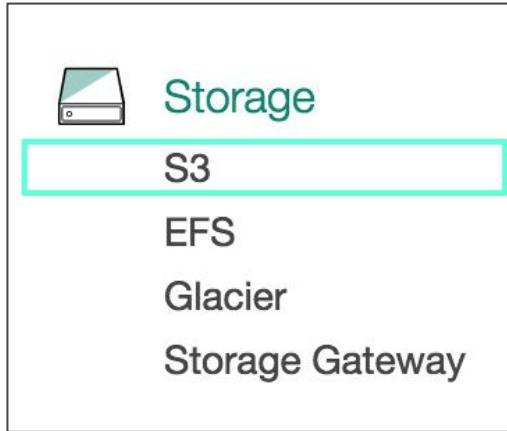
EFS

Glacier

Storage Gateway

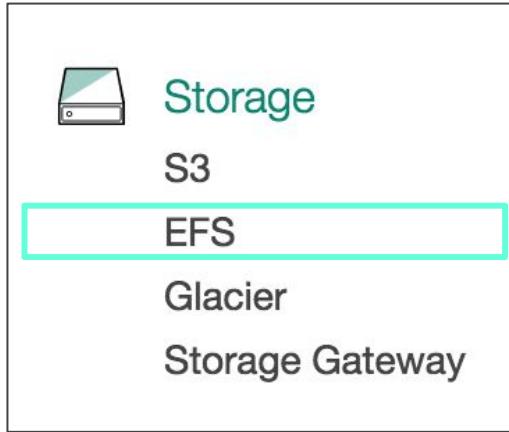
- A critical component of cloud computing is cloud storage that holds the information used by applications.
- AWS offers a complete range of cloud storage services to support both application and archival compliance requirements.

S3 Simple Storage Service



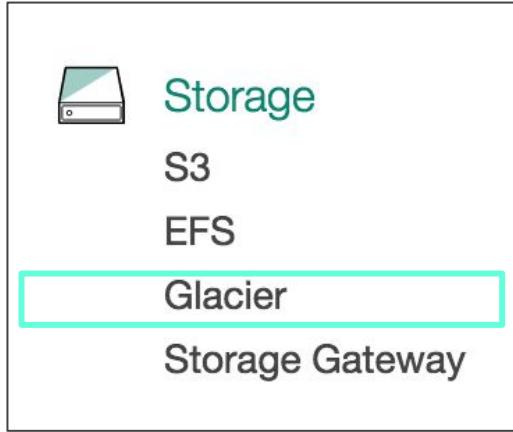
- Internet storage
- Any amount of data can be stored and retrieved at any time.
- AWS management console-a simple and intuitive web interface is used for this purpose.

EFS Elastic File System



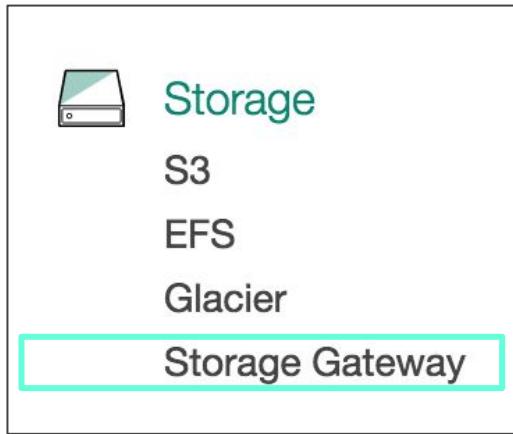
- Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud.
- Multiple EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to provide a common data source for workloads and applications running on more than one EC2 instance

Glacier



- Amazon Glacier is a secure, durable, and extremely low-cost storage service for data archiving and long-term backup.
- Store large or small amounts of data for as little as \$0.004 per gigabyte per month.
- To keep costs, Amazon Glacier provides three options for access to archives, from a few minutes to several hours

Storage Gateway



- AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use storage in the AWS Cloud.
- Applications connect to the service through a gateway appliance using standard storage protocols, such as NFS and iSCSI.



Database

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Database



Database

RDS

DynamoDB

ElastiCache

Redshift

AWS provides fully-managed relational and NoSQL database services, as well as in-memory caching as a service and a petabyte-scale data-warehouse solution.

The following are the **key database service**

Amazon RDS: Provides managed relational databases.

Amazon Redshift: A fast, fully-managed, petabyte-scale data warehouse.

Amazon DynamoDB: Provides managed NoSQL databases.

Amazon ElastiCache: An in-memory caching service.

RDS Relational Database Service



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud.
- Amazon RDS provides six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.

DynamoDB



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale.
- It is a fully managed database
- Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, Internet of Things (IoT), and many other applications.

ElastiCache



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud.
- The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases.
- Amazon ElastiCache supports two open-source in-memory caching engines i.e **Redis** and **Memcached**

Redshift



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools.
- It allows you to run complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution.



Networking & Content Delivery

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Networking & Content Delivery



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Networking products include virtual private cloud network, dedicated connection to the AWS and registering a domain name.
- Content Delivery Network like CloudFront reduces network latency and increases throughput thus improving the performance of your website by pushing content closer to your users.

VPC



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon Virtual Private Cloud (Amazon VPC) provides a logically isolated section of the Amazon Web Services (AWS) cloud where AWS resources can be launched in a virtual network
- There is a complete control over the virtual networking environment.
- Both IPv4 and IPv6 can be used in VPC for secure and easy access to resources and applications.

CloudFront



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon CloudFront is a global content delivery network (CDN) service that accelerates delivery of your websites, APIs, video content, or other web assets.
- It integrates with other AWS products to give developers an easy way to accelerate content to end users.
- It also works seamlessly with any non-AWS origin server that stores the original, definitive versions of your files.

Direct Connect



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- AWS Direct Connect makes it easy to establish a dedicated network connection to AWS.
- It helps to establish a dedicated network connection between the network and one of the AWS Direct Connect locations.
- Private connectivity can be established between AWS and data centre, office or co-location environment by using AWS Direct Connect.

Route 53



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.
- It provides an extremely reliable and cost effective way to route end users to Internet applications.
- It is fully compliant with IPv6 as well.



Migration

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Migration



Migration

Application Discovery Service
DMS
Server Migration
Snowball

- Migration is an agentless service which makes it easier and faster to migrate data via networks.
- Amazon offers a suite of tools to help you to move data via networks, roads and technology partners.

Application Discovery Service



Migration

Application Discovery Service

DMS

Server Migration

Snowball

- It provides multiple ways to set up and run Amazon cloud directory, amazon cognito & microsoft AD with other AWS services.
- AWS Application Discovery Service automatically collects configuration and usage data from servers, storage, and networking equipment to develop a list of applications, how they perform and how they are independent.

DMS



Migration

Application Discovery Service

DMS

Server Migration

Snowball

- AWS Database Migration Service helps to migrate databases to AWS easily and securely.
- The service supports homogenous migrations as well as heterogeneous migrations between different database platforms.
- It can also be used for continuous data replication with high availability.

Server Migration



Migration

Application Discovery Service

DMS

Server Migration

Snowball

- AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster to migrate thousands of on-premises workloads to AWS.
- It allows you to automate, schedule, and track incremental replications of live server volumes, making it easier to coordinate large-scale server migrations.

Snowball



Migration

Application Discovery Service

DMS

Server Migration

Snowball

- AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS.
- Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet.



Developer Tools

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Developer Tools



Developer Tools

CodeStar

CodeCommit

CodeBuild

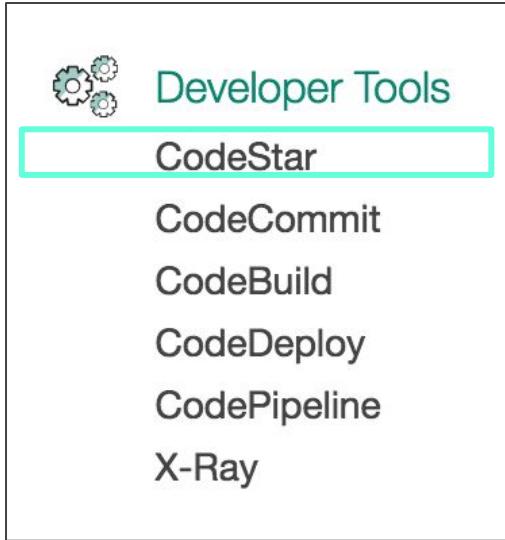
CodeDeploy

CodePipeline

X-Ray

- The AWS Developer Tools is a set of services designed to enable developers and IT operations professionals practicing DevOps to rapidly and safely deliver software.
- These services help to securely store and version control application's source code and automatically build, test, and deploy application to AWS or on-premises environment.

CodeStar



- It is a cloud based service for creating, managing and working with software development projects on AWS.
- An AWS code star project creates and integrates AWS services for your project development toolchain.

CodeCommit



- AWS CodeCommit is a fully managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories.
- It eliminates the need to operate the source control system or worry about scaling its infrastructure.
- It is used to securely store anything from source code to binaries, and it works seamlessly with the existing Git tools.

CodeBuild



Developer Tools

CodeStar

CodeCommit

CodeBuild

CodeDeploy

CodePipeline

X-Ray

- AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy.
- With CodeBuild, there is no need to provision, manage, and scale the build servers.
- It scales continuously and processes multiple builds concurrently.

CodeDeploy



Developer Tools

CodeStar

CodeCommit

CodeBuild

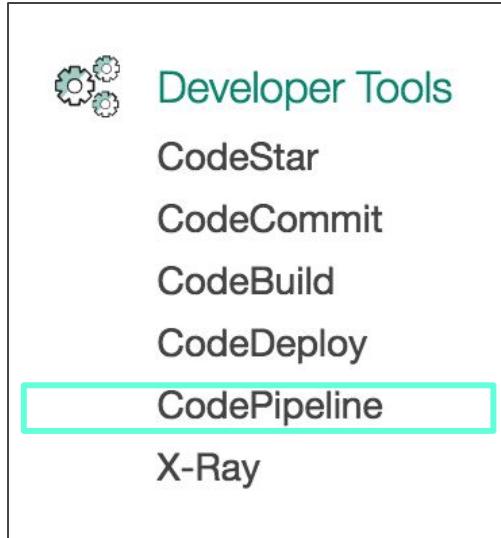
CodeDeploy

CodePipeline

X-Ray

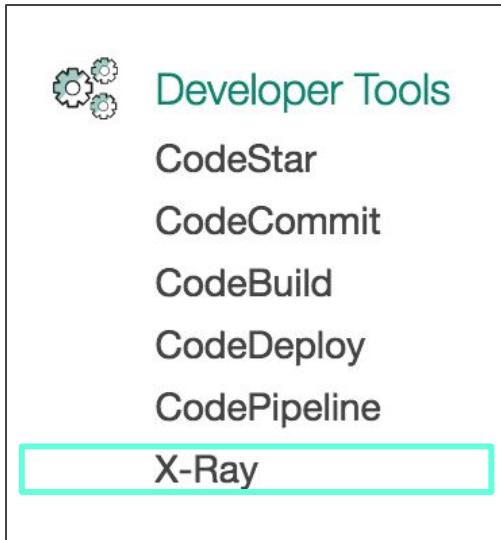
- AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and instances running on premises.
- It can be used to automate software deployments, eliminating the need for error-prone manual operations.

CodePipeline



- AWS CodePipeline is a continuous integration and continuous delivery service for fast and reliable application and infrastructure updates.
- It builds, tests, and deploys the code every time there is a code change, based on the release process models.
- This enables rapid and reliable delivery of features and updates.

X-Ray



- AWS X-Ray helps developers analyze and debug distributed applications in production or under development, such as those built using a microservices architecture.
- It provides an end-to-end view of requests as they travel through the application, and shows a map of application's underlying components.
- It can be used to analyze both applications in development and in production.



Management Tools

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Management Tools



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS provides a broad set of services that help IT administrators, systems administrators, and developers more easily manage and monitor their hybrid infrastructure resources.
- Infrastructure logs and metrics can be monitored using real-time dashboards and alarms.

CloudWatch



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications that run on AWS.
- It can be used to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in the AWS resources.

CloudFormation



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- It is a service that helps you to model and setup your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS.
- We can create a template that describes all the AWS resources that you want (EC2 instances or RDS DB instances) & cloud formation will take care of provisioning and configuring those resources.

CloudTrail



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS CloudTrail is a web service that records AWS API calls for user's account and delivers log files to user.
- The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

Config



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS Config is a fully managed service that provides an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.
- The Config Rules feature helps to create rules that automatically check the configuration of AWS resources recorded by AWS Config.

OpsWorks



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS OpsWorks is a configuration management service that uses Chef, an automation platform that treats server configurations as code.
- OpsWorks uses Chef to automate how servers are configured, deployed, and managed across the EC2 instances or on-premises compute environments.
- OpsWorks has two offerings, AWS OpsWorks for Chef Automate and AWS OpsWorks Stacks.

Service Catalog



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS.
- These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures
- It allows users to centrally manage commonly deployed IT services and helps to achieve consistent governance and meet the compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

Trusted Advisor



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS Trusted Advisor is an online resource that helps to reduce cost, increase performance, and improve security by optimizing the AWS environment.
- It provides real-time guidance to help provision user's resources following AWS best practices.

Managed Services



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS Managed Services provides ongoing management of the AWS infrastructure so the user can focus on the applications.
- It automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support the infrastructure.



Security, Identity & Compliance

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- Cloud security at AWS is the highest priority.
- An AWS customer will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.
- The AWS cloud provides a platform to scale and innovate, while still maintaining a secure environment.

IAM



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- AWS Identity and Access Management (IAM) enables user to securely control access to AWS services and resources for the users.
- It is used to create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Inspector



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
- It produces a detailed list of security findings prioritized by level of severity.

Certificate Manager



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- AWS Certificate Manager is a service that provides easy provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services.
- It is used to request a certificate, deploy it on AWS resources such as Elastic Load Balancing load balancers or Amazon CloudFront distributions, and to handle certificate renewals.

Directory Service



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as AWS Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.
- User can use standard Active Directory administration tools and take advantage of built-in Active Directory features such as Group Policy, trusts, and single sign-on.

WAF and Shield



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.
- AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS.

Compliance Reports



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- Compliance Reports enable customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud.
- AWS compliance enablers build on traditional programs, helping you to establish and operate in an AWS security control environment.



Analytics

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Analytics



Analytics

Athena

EMR

CloudSearch

Elasticsearch Service

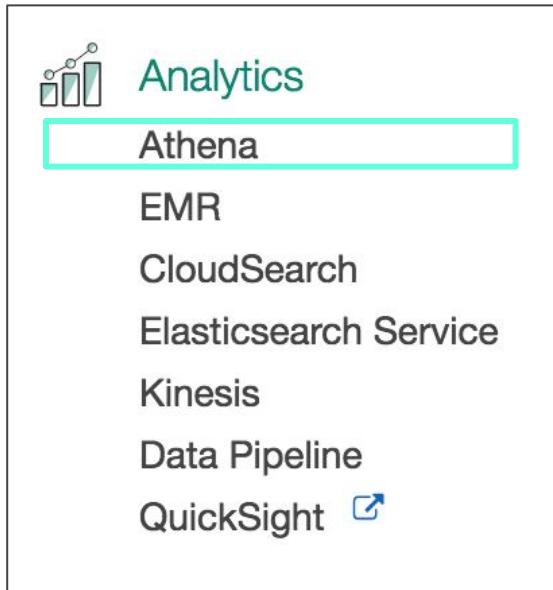
Kinesis

Data Pipeline

QuickSight 

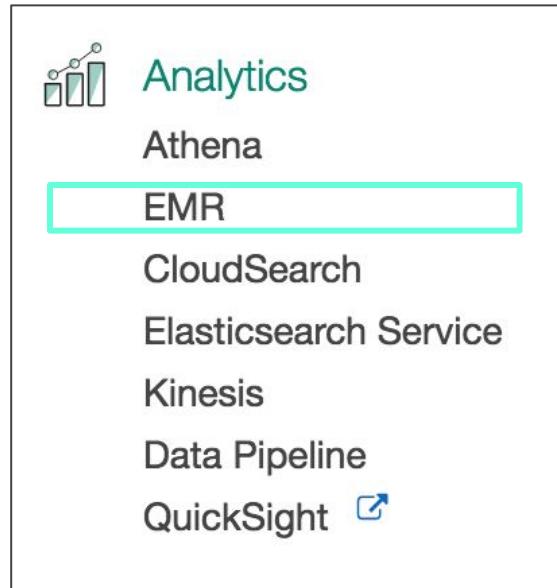
- Extracting insights and actionable information from data requires a broad array of technology that can work with data efficiently, scalably , and cost-effectively.
- These services are powerful, flexible, and yet simple to use, enabling organizations to put their raw data to work quickly and easily.

Athena



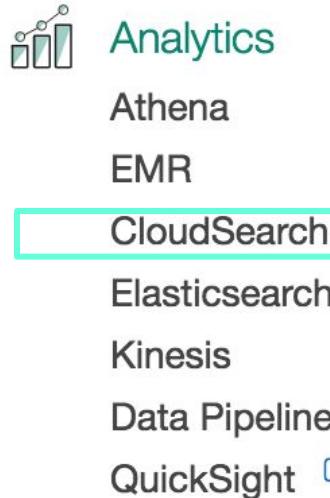
- Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.
- With Athena, there's no need for complex extract, transform, and load (ETL) jobs to prepare data for analysis.
- This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

EMR



- Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost effective to process vast amounts of data across dynamically scalable EC2 instances.
- It securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

Cloud Search



- Amazon CloudSearch is a managed service in the AWS Cloud that makes it simple and cost effective to set up, manage, and scale a search solution for the website or application.
- It supports 34 languages and popular search features such as highlighting, autocomplete, and geospatial search.

Elasticsearch Service



Analytics

Athena

EMR

CloudSearch

Elasticsearch Service

Kinesis

Data Pipeline

QuickSight

- Amazon Elasticsearch Service makes it easy to deploy, operate, and scale Elasticsearch for log analytics, full text search, application monitoring, and more.
- It is a fully managed service that delivers Elasticsearch's easy-to-use APIs and real-time capabilities along with the availability, scalability, and security required by production workloads.

Kinesis



Analytics

Athena

EMR

CloudSearch

Elasticsearch Service

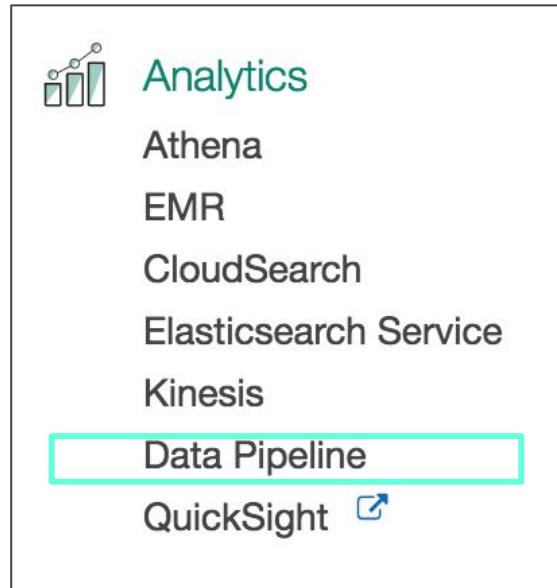
Kinesis

Data Pipeline

QuickSight

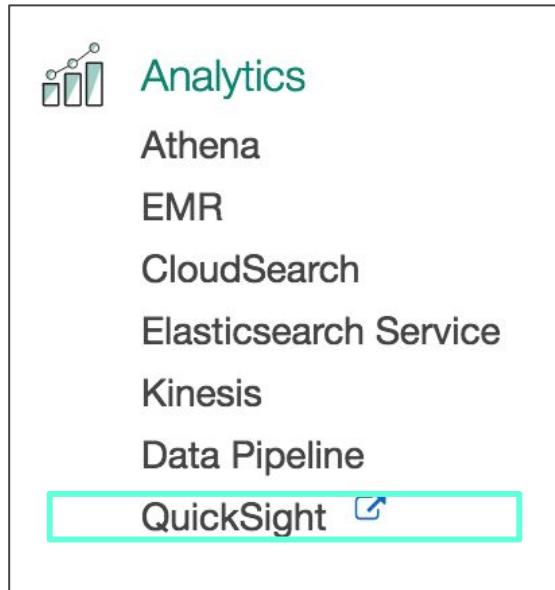
- Amazon Kinesis is a platform for streaming data on AWS, offering powerful services to make it easy to load and analyze streaming data
- It also provides the ability to build custom streaming data applications for specialized needs.
- It currently offers three services: Amazon Kinesis Firehose, Amazon Kinesis Analytics, and Amazon Kinesis Streams.

Data Pipeline



- AWS Data Pipeline is a web service that helps to reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals.
- It is used to regularly access data where it's stored, transform and process it at scale, and efficiently transfer the results to AWS services such as Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon EMR.

QuickSight



- Amazon QuickSight is a fast, cloud-powered business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get business insights from data.
- Using our cloud-based service one can easily connect to data, perform advanced analysis, and create stunning visualizations and rich dashboards that can be accessed from any browser or mobile device.



Artificial Intelligence

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Artificial Intelligence



Artificial Intelligence

Lex

Polly

Rekognition

Machine Learning

- It is basically dedicated to solving cognitive problems commonly associated with human intelligence such as learning, problem solving and pattern recognition.
- Amazon AI services bring natural language understanding (NLU), automatic speech recognition (ASR), visual search and image recognition, text-to-speech (TTS), and machine learning (ML) technologies within the reach of every developer.

Lex



Artificial Intelligence

Lex

Polly

Rekognition

Machine Learning

- Amazon Lex is a service for building conversational interfaces into any application using voice and text.
- Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to build applications with highly engaging user experiences and lifelike conversational interactions.

Polly



Artificial Intelligence

Lex

Polly

Rekognition

Machine Learning

- Amazon Polly is a service that turns text into lifelike speech.
- It is an Amazon artificial intelligence (AI) service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice.
- It includes 47 lifelike voices spread across 24 languages.

Rekognition



Artificial Intelligence

Lex

Polly

Rekognition

Machine Learning

- Amazon Rekognition is a service that makes it easy to add image analysis to the applications.
- It is based on the same proven, highly scalable, deep learning technology developed by Amazon's computer vision scientists to analyze billions of images daily for Prime Photos.

Machine Learning



Artificial Intelligence

Lex

Polly

Rekognition

Machine Learning

- Amazon Machine Learning (Amazon ML) is a service that makes it easy for developers of all skill levels to use machine learning technology.
- It provides visualization tools and wizards.
- It is based on the same proven, highly scalable, ML technology used for years by Amazon's internal data scientist community.



Internet of Things

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

AWS IoT

Contact Center

Amazon Connect

Game Development

Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Internet of Things

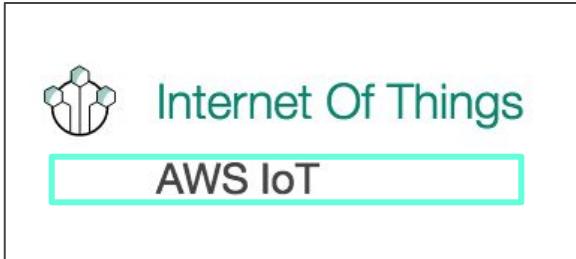


Internet Of Things

AWS IoT

- IOT is the inter-networking of physical devices, vehicles , buildings and other embedded devices and network connectivity which enables devices to collect and exchange data.
- IOT also referred to as IOE consists of web enabled devices that collect, send and act on data they require from their surrounding environment using embedded sensors , processors and communication hardware.

AWS IoT



- AWS IoT is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices.
- AWS IoT can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely.



Contact Center

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

AWS IoT

Contact Center

Amazon Connect

Game Development

Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Contact Center



Contact Center

Amazon Connect

- Contact center makes it easy for any business to deliver better customer service at lower cost.

Amazon Connect



- Amazon Connect is a self-service, cloud-based contact center service.
- The self-service graphical interface in Amazon Connect makes it easy for non-technical users to design contact flows, manage agents, and track performance metrics – no specialized skills required.



Game Development

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Game Development



Game Development
Amazon GameLift

- Amazon Web Services offers a comprehensive suite of products and services for video game developers across every major platform: mobile, console, PC and online.
- From AAA console and PC games, to educational and serious games, AWS provides the back end servers and hosting services for the game studio.

Amazon Game Lift



Game Development

Amazon GameLift

- Amazon Game Lift is a managed service for deploying, operating, and scaling dedicated game servers for session-based multiplayer games.
- It makes it easy to manage server infrastructure, scale capacity to lower latency and cost, match players into available game sessions, and defend from distributed denial-of-service (DDoS) attacks.



Mobile Services

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Mobile Services



Mobile Services

Mobile Hub

Cognito

Device Farm

Mobile Analytics

Pinpoint

- AWS provides a range of services to help you develop mobile apps that can scale to hundreds of millions of users, and reach global audiences.
- With AWS users can get started quickly, ensure high quality by testing on real devices in the cloud, and measure and improve user engagement.

Mobile Hub



Mobile Services

Mobile Hub

Cognito

Device Farm

Mobile Analytics

Pinpoint

- AWS Mobile Hub provides an integrated console experience that you can use to quickly create and configure powerful mobile app backend features and integrate them into your mobile app.
- Features include:
 - App Analytics, App Content Delivery, Cloud Logic
 - NoSQL Database , Push Notifications, User Data Storage
 - User Sign-in , Connectors , Conversational Bots
 - User Engagement

Cognito



Mobile Services

Mobile Hub

Cognito

Device Farm

Mobile Analytics

Pinpoint

- Amazon Cognito is a mobile service that easily add user sign-up and sign-in to mobile and web apps.
- It is used to create great app experiences instead of worrying about building, securing, and scaling a solution to handle user management, authentication, and sync across devices.

Device Farm



Mobile Services

Mobile Hub

Cognito

Device Farm

Mobile Analytics

Pinpoint

- AWS Device Farm is an app testing service that helps to test and interact with Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.
- View video, screenshots, logs, and performance data to pinpoint and fix issues before shipping the app.

Mobile Analytics



Mobile Services

Mobile Hub

Cognito

Device Farm

Mobile Analytics

Pinpoint

- Mobile Analytics is used to measure app usage and app revenue.
- By tracking key trends such as new versus returning users, app revenue, user retention, and custom in-app behavior events, user can make data-driven decisions to increase engagement and monetization for the app.

Pinpoint



Mobile Services

Mobile Hub

Cognito

Device Farm

Mobile Analytics

Pinpoint

- Amazon Pinpoint makes it easy to run targeted campaigns to drive user engagement in mobile apps.
- It helps to understand user behavior, define which users to target, determine which messages to send, schedule the best time to deliver the messages, and then track the results of the campaign.



Application Services

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Application Services



Application Services

Step Functions

SWF

API Gateway

Elastic Transcoder

- AWS provides a variety of managed services to use with your applications.

Step Functions



Application Services

Step Functions

SWF

API Gateway

Elastic Transcoder

- AWS Step Functions makes it easy to coordinate the components of distributed applications and microservices using visual workflows.
- It provides a graphical console to arrange and visualize the components of the application as a series of steps.

SWF



Application Services

Step Functions

SWF

API Gateway

Elastic Transcoder

- Amazon Simple Workflow (Amazon SWF) helps developers build, run, and scale background jobs that have parallel or sequential steps.
- It is a fully-managed state tracker and task coordinator in the cloud.

API Gateway



Application Services

Step Functions

SWF

API Gateway

Elastic Transcoder

- Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.
- It handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.

Elastic Transcoder



Application Services

Step Functions

SWF

API Gateway

Elastic Transcoder

- Amazon Elastic Transcoder is media transcoding in the cloud.
- It is designed to be a highly scalable, easy-to-use, and cost-effective way for developers and businesses to convert (or transcode) media files from their source format into versions that will play back on devices like smartphones, tablets, and PCs.



Messaging

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Messaging



Messaging

Simple Queue Service

Simple Notification Service

SES

- AWS manages the ongoing operations and underlying infrastructure needed to reliably run and scale message queues.
- User can eliminate the complexity and administrative overhead associated with managing dedicated message-oriented middleware (MoM) and associated infrastructure.

Simple Queue Service



Messaging

Simple Queue Service

Simple Notification Service

SES

- Amazon Simple Queue Service (Amazon SQS) is a fast, reliable, scalable, fully managed message queuing service.
- It makes it simple and cost-effective to decouple the components of a cloud application.
- It includes standard queues with high throughput, and FIFO queues.

Simple Notification Service



Messaging

Simple Queue Service

Simple Notification Service

SES

- Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push notification service that lets you send individual messages or to fan-out messages to large numbers of recipients.
- Amazon SNS makes it simple and cost effective to send push notifications to mobile device users, email recipients or even send messages to other distributed services.

SES



Messaging

Simple Queue Service

Simple Notification Service

SES

- Amazon Simple Email Service (Amazon SES) is a cost-effective email service built on the reliable and scalable infrastructure that Amazon.com developed to serve its own customer base.
- It is used to receive messages and deliver them to an Amazon S3 bucket, call the custom code via an AWS Lambda function, or publish notifications to Amazon SNS.



Business Productivity

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Business Productivity



Business Productivity

WorkDocs

WorkMail

Amazon Chime 

- Time to market is critical in today's competitive environment.
- Amazon Web Services can help take user into the future of business with a breadth of services designed to help build the applications needed to remain ahead of the curve.

WorkDocs



Business Productivity

WorkDocs

WorkMail

Amazon Chime 

- Amazon WorkDocs is a fully managed, secure enterprise storage and sharing service with strong administrative controls and feedback capabilities that improve user productivity.
- It offers IT administrators the option of integrating with existing corporate directories, flexible sharing policies and control of the location where data is stored.

WorkMail



Business Productivity

WorkDocs

WorkMail

Amazon Chime 

- Amazon WorkMail is a secure, managed business email and calendar service with support for existing desktop and mobile email client applications.
- It gives users the ability to seamlessly access their email, contacts, and calendars using the client application of their choice, including Microsoft Outlook, native iOS and Android email applications, any client application supporting the IMAP protocol, or directly through a web browser.

Amazon Chime



Business Productivity

WorkDocs

WorkMail

Amazon Chime 

- Amazon Chime is a communications service that transforms online meetings with a secure, easy-to-use application that you can trust.
- It works seamlessly across the devices so that user can stay connected.



Desktop & App Streaming

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Desktop & App Streaming



Desktop & App Streaming

WorkSpaces

AppStream 2.0

- AWS offers two managed end user computing services running on the AWS cloud - Amazon WorkSpaces and Amazon AppStream 2.0.
- With these services, you can move your desktops and applications to AWS, and get enhanced security, low cost pay-as-you-go pricing, on-demand scaling, and global availability.

Workspaces



Desktop & App Streaming

WorkSpaces

AppStream 2.0

- Amazon WorkSpaces is a fully managed, secure desktop computing service that runs on the AWS Cloud.
- It eliminates the need to procure and deploy hardware or install complex software.

AppStream 2.0



Desktop & App Streaming

WorkSpaces

AppStream 2.0

- AppStream 2.0 is a fully managed, secure, application streaming service that helps to stream desktop applications from AWS to any device running a web browser, without rewriting them.
- It provides instant-on access to the applications needed, and a responsive, fluid user experience on the device of choice.



SERVICES REQUIRED FOR AWS EXAM

AWS CONSOLE

Services ▾ | Resource Groups ▾

- History
- Console Home
- Billing
- IAM
- EC2
- DynamoDB

- Compute**
 - EC2
 - EC2 Container Service
 - Lightsail
 - Elastic Beanstalk
 - Lambda
 - Batch
- Storage**
 - S3
 - EFS
 - Glacier
 - Storage Gateway
- Database**
 - RDS
 - DynamoDB
 - ElastiCache
 - Redshift
- Networking & Content Delivery**
 - VPC
 - CloudFront
 - Direct Connect
 - Route 53
- Migration**
 - Application Discovery Service
 - DMS
 - Server Migration
 - Snowball

- Developer Tools**
 - CodeStar
 - CodeCommit
 - CodeBuild
 - CodeDeploy
 - CodePipeline
 - X-Ray
- Management Tools**
 - CloudWatch
 - CloudFormation
 - CloudTrail
 - Config
 - OpsWorks
 - Service Catalog
 - Trusted Advisor
 - Managed Services
- Security, Identity & Compliance**
 - IAM
 - Inspector
 - Certificate Manager
 - Directory Service
 - WAF & Shield
 - Compliance Reports

- Analytics**
 - Athena
 - EMR
 - CloudSearch
 - Elasticsearch Service
 - Kinesis
 - Data Pipeline
 - QuickSight
- Artificial Intelligence**
 - Lex
 - Polly
 - Rekognition
 - Machine Learning
- Internet Of Things**
 - AWS IoT
- Contact Center**
 - Amazon Connect
- Game Development**
 - Amazon GameLift
- Mobile Services**
 - Mobile Hub
 - Cognito
 - Device Farm
 - Mobile Analytics
 - Pinpoint

- Application Services**
 - Step Functions
 - SWF
 - API Gateway
 - Elastic Transcoder
- Messaging**
 - Simple Queue Service
 - Simple Notification Service
 - SES
- Business Productivity**
 - WorkDocs
 - WorkMail
 - Amazon Chime
- Desktop & App Streaming**
 - WorkSpaces
 - AppStream 2.0



Compute

AWS CONSOLE

Services ▾ | Resource Groups ▾

- History
- Console Home
- Billing
- IAM
- EC2
 - Compute
 - EC2
 - EC2 Container Service
 - Lightsail
 - Elastic Beanstalk
 - Lambda
 - Batch
 - Storage
 - S3
 - EFS
 - Glacier
 - Storage Gateway
 - Database
 - RDS
 - DynamoDB
 - ElastiCache
 - Redshift
 - Networking & Content Delivery
 - VPC
 - CloudFront
 - Direct Connect
 - Route 53
 - Migration
 - Application Discovery Service
 - DMS
 - Server Migration
 - Snowball
- Developer Tools
 - CodeStar
 - CodeCommit
 - CodeBuild
 - CodeDeploy
 - CodePipeline
 - X-Ray
- Analytics
 - Athena
 - EMR
 - CloudSearch
 - Elasticsearch Service
 - Kinesis
 - Data Pipeline
 - QuickSight
- Application Services
 - Step Functions
 - SWF
 - API Gateway
 - Elastic Transcoder
- Messaging
 - Simple Queue Service
 - Simple Notification Service
 - SES
- Business Productivity
 - WorkDocs
 - WorkMail
 - Amazon Chime
- Internet Of Things
 - AWS IoT
- Contact Center
 - Amazon Connect
- Game Development
 - Amazon GameLift
- Mobile Services
 - Mobile Hub
 - Cognito
 - Device Farm
 - Mobile Analytics
 - Pinpoint

Compute



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

- Amount of computational power required to fulfill your workload.
- Building and running your business starts with compute, whether you are building mobile apps, or running massive clusters
- AWS offers multiple compute products allowing you to deploy, run, and scale your applications as virtual servers, containers, or code.

Compute

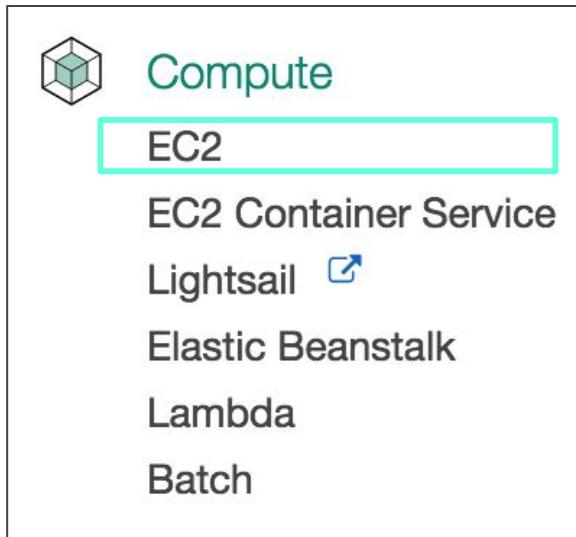
AWS provide a variety of compute and networking services.

Organizations use these services to develop and run their workloads according to business need.

AWS provide services such as storage, database and application services.

Example: Amazon Elastic Compute cloud (Amazon EC2), AWS Lambda, AWS Elastic Beanstalk, Amazon Virtual private cloud (Amazon VPC) etc.

EC2



EC2 Deployment Unit - Virtual Machines

Run any application. Control and manage server or cluster level functions such as scaling and deployment.

You provision, scale, and manage server capacity. EC2 offers a wide selection of instance configurations optimized for every use case

Amazon EC2

- Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud.
- Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
- You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage.
- Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

Amazon EC2

- Amazon Elastic Compute Cloud (EC2) allows users to rent virtual computers on which to run their own computer applications.
- EC2 encourages scalable deployment of applications by providing a web service through which a user can boot an **Amazon Machine Image (AMI)** to configure a **virtual machine**, which Amazon calls an "**instance**", containing any software desired.
- A user can create, launch, and terminate server-instances as needed, paying by the hour for active servers – hence the term "elastic".

Instance

- An instance type essentially determines the hardware of the host computer used for your instance.
- Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications.
- Each instance type offers different compute and memory capabilities.
- Select an instance type based on the amount of memory and computing power that you need for the application or software that you plan to run on the instance.

Concepts to launch instances on AWS

- Amount of virtual hardware dedicated to the instances.
- Software loaded on the instance.

Two dimensions of new instance are controlled by:

- Instance type
- AMI (Amazon machine images)

Instance types

- T2 instances
- Compute optimized instances
- Memory optimized instances
- Storage optimized instances
- Accelerated computing instances
- T1 micro instances
- Resizing instances

Instance types

- T2 instances - T2 , M4 , M3
- Compute optimized instances - C3 , C4
- Memory optimized instances - R3, R4 , X1
- Storage optimized instances - D2, D3, I3
- Accelerated computing instances- F1 , P2 , G2, CG1
- T1 micro instances - t1. micro
- Resizing instances

Instance types

Family	Speciality	Use case
D2	Dense Storage	Fileservers/Data Warehousing/Hadoop
R4	Memory Optimized	Memory Intensive Apps/DBs
M4	General Purpose	Application Servers
C4	Compute Optimized	CPU Intensive Apps/DBs
G2	Graphics Intensive	Video Encoding/ 3D Application Streaming
I2	High Speed Storage	NoSQL DBs, Data Warehousing etc
F1	Field Programmable Gate Array	Hardware acceleration for your code.
T2	Lowest Cost, General Purpose	Web Servers/Small DBs
P2	Graphics/General Purpose GPU	Machine Learning, Bit Coin Mining etc
X1	Memory Optimized	SAP HANA/Apache Spark etc

To choose Instance type

- Specify network performance - low , moderate and high, - for workloads requiring greater network performance many instances support **enhanced networking**.
- It results in more PPS (packets per second), lower latency and less jitter.

Securely using an Instance

- Addressing an instance : name in description tab of console or via CLI or API.
- Public IP
- Elastic IP
- Initial access : EC2 uses public key cryptography- keys together form keypair.
- Virtual firewall protection- allows you to control traffic based on port, protocol, source & destination.

Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance.

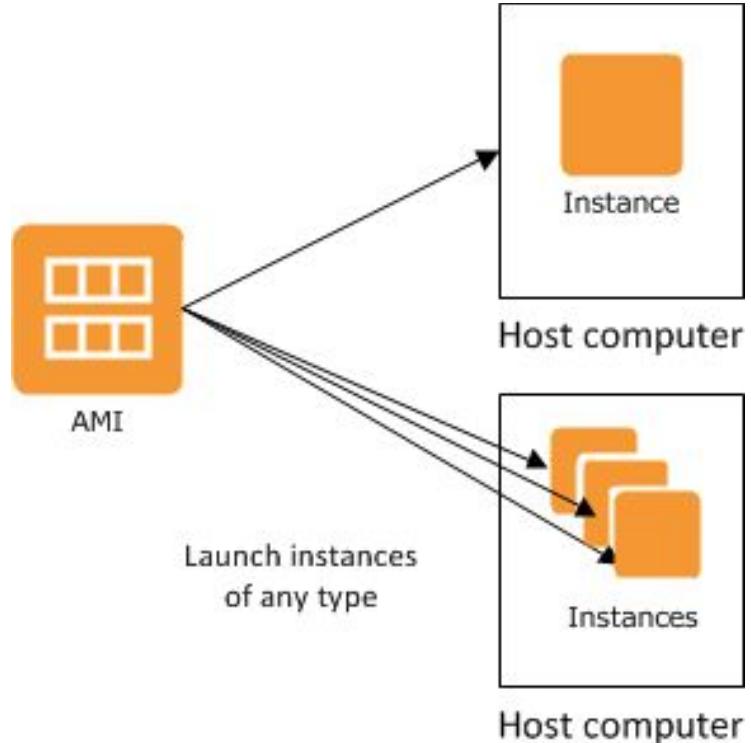
Like all virtual appliances, the main component of an AMI is a read-only filesystem image that includes an operating system (e.g., Linux, Unix, or Windows) and any additional software required to deliver a service or a portion of it

Sources of AMI

- Published by AWS
- AWS marketplace
- Generated from existing instances
- Uploaded virtual servers

AMI & Instance

- From an AMI, you launch an instance, which is a copy of the AMI running as a virtual server in the cloud.
- You can launch multiple instances of an AMI, as shown in the following figure.



AMI - Operating Systems

EC2 service offers around 60,000 AMI's. The prominent being

- Amazon Linux AMI based on Red Hat Enterprise Linux
- Linux (Redhat/SUSE/Ubuntu Enterprise)
- Windows Server 2016, Windows Server 2012, Windows Server 2008

Features of EC2

- **Instances** - virtual computing environments.
- **Amazon Machine Images**- AMIs preconfigured templates for instances.
- **Instance types** - various configurations of CPU, memory, storage & networking capacity.
- **Key pairs** - secure login information for instances.
- **Instance store volumes** - volumes for temporary data that is deleted when you stop or terminate your instance.
- **EBS volumes** - persistent storage volume for your data.
- **Regions & availability zones** - multiple physical locations of your resources.

Features of EC2

- **Security groups** - a firewall that enables you to specify the protocols , ports and source IP addresses.
- **Elastic IP addresses** - static IPV4 addresses for dynamic cloud computing.
- **Metadata** - also known as tags that you can create and assign to your EC2 instances.
- **Virtual private cloud** - virtual networks you can create that are logically isolated from rest of AWS cloud.
- **EBS optimized instances**.

Amazon Elastic Block Store

- Provides persistent block level storage volumes for use with Amazon EC2 instances.
- EBS volume is automatically replicated within availability zone.
- Multiple EBS volumes can be attached to a single instance at a time.
- EBS volume types vary in hardware, performance and cost.
- Types of Amazon EBS volumes - Magnetic volumes (HDD) , general purpose SSD, and provisioned IOPS SSD.

EBS optimized instances

- It enables EC2 instances to fully use the IOPS provisioned on an EBS volume.
- It delivers dedicated throughput between Amazon EC2 & EBS between 500 - 4000 mbps.
- The dedicated throughput minimizes contention between EBS I/O and other traffic from your EC2 instance, providing the best performance for your EBS volumes.
- Designed for use with both standard and provisioned IOPS Amazon EBS volumes.

Multiple locations

- It provides the ability to place instances in multiple locations.
- By launching instances in separate availability zones , we can protect applications from failure of single location.
- The Amazon EC2 service level agreement commitment is 99.95% availability for each Amazon EC2 region.

Elastic IP addresses

- These are static IP addresses designed for dynamic cloud computing.
- An Elastic IP address is associated with your account not a particular instance.
- Elastic IP addresses allow you to mask instance or availability zone failures by programmatically remapping your public IP addresses to any instance in your account.

Amazon Virtual private cloud

- It lets you provision a logically isolated section of AWS cloud where you can launch AWS resources in a virtual network that you define.
- You can have complete control over virtual networking environment.
- You can create a hardware virtual private network connection between corporate datacenter and VPC.

Amazon Cloud watch

- It is a web service that provides monitoring for AWS cloud resources and applications starting with Amazon EC2.
- It provides you with visibility into resource utilization, operational performance and overall demand patterns.
- You can get statistics, view graphs and set alarms for your metric data.
- To use cloud watch, you can simply select the instance that you'd like to monitor.

Auto scaling

- It allows you to automatically scale your Amazon EC2 capacity up or down according to the conditions defined.
- With auto scaling , we can ensure that the number of Amazon EC2 instances you're using scales up during demand spikes to maintain performance.
- It scales down automatically to minimize costs.

High performance computing (HPC) clusters

- These are required for customers with complex computational workloads such as tightly coupled parallel processes,
- Used for applications sensitive to network performance , can achieve high compute and network performance.
- Cluster instances also provide significantly increased throughput making them well suited for customer applications that need to perform network - intensive operations.

Accelerated compute instances

- It is a family of instances which use hardware accelerators , co-processors to perform some functions such as floating point number calculation and graphic processing.
- It can perform calculations more efficiently than is possible in software running on CPUs.

GPU compute & Graphic instances

- It is used for customers requiring massive floating point processing.
- It can perform 40 thousand parallel processing cores
- Ideally suited for machine learning.
- Used in high performance databases, computational fluid dynamics , computational finance , seismic analysis , molecular modeling , genomics and rendering workloads.
- GPU graphic instances are for customers that require high graphics .

System manager

- It is a management service that helps you automatically collect software inventory, apply OS patches, create system images and configure operating systems.
- It helps to define and track system configurations.
- It maintains software compliance of EC2 and on premises configurations .

EC2 - Common Use Cases

- Big data (e.g. Hadoop, Spark)
- Database software (e.g., Aurora, DynamoDB)
- Enterprise applications (e.g., SAP, Oracle, Sharepoint)
- Migrations from on-premises environments, including BYOL
- Open-source cluster management

Benefits of EC2

1. Elastic Web-Scale Computing
2. Completely Controlled
3. Flexible Cloud Hosting Services
4. Designed for use with other Amazon Web Services
5. Reliable
6. Secure
7. Inexpensive
8. Easy to Start

EC2 pricing

Amazon EC2 is free to use. There are four ways to pay for Amazon EC2 instances :

- On demand instances
- Reserved instances
- Spot instances
- Dedicated hosts

ECS - EC2 Container Service



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

ECS Deployment Unit - Containers

It is container management service that supports Docker containers.

- You provision and scale the server capacity and manage the utilization and availability.
- AWS manages the fault tolerance of the application.
- AWS manages cluster state and container deployment.

EC2 container service

- It is highly scalable and highly managed container service.
- It supports docker containers that allows you to run applications on a managed cluster of EC2 instances.
- With API calls , you can launch and stop dockor enabled applications , query the complete state of your cluster and access many familiar features like security groups, elastic load balancing, EBS volumes and IAM roles.
- There is no additional charge for Amazon EC2 container service , you pay for AWS resources (EC2 instances or EBS volumes).

ECS - Common Use Cases

- Web applications
- Microservices
- Batch jobs
- Docker workloads

Lightsail



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

Light Sail Deployment Unit - Virtual Private Servers (Instance)

It is the easiest way to launch and manage a virtual private server with AWS.

- You follow instance creation experience to spin up a preconfigured virtual server in seconds. You don't have to worry about security groups or other settings.
- You control the server, OS, and other software through the intuitive Lightsail console.

Lightsail

- With a couple of clicks you can choose a configuration from a menu and launch a virtual machine pre- configured with SSD based storage, DNS management and a static IP address.
- You can launch your favourite operating system , developer stack or application at a flat pricing rate.

Lightsail - Common Use Cases

- Simple Web Applications
- WordPress Blogs and Websites
- Ecommerce Websites
- Single - server Business Software

Elastic Beanstalk

Elastic Beanstalk Deployment Unit- beanstalk



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

It is an easy to use service for deploying and scaling web applications and services.

- You can simply upload your code and it automatically handles the deployment from capacity provisioning, load balancing, auto scaling to health monitoring.
- You retain full control over AWS resources powering your application and can access the underlying resources at any time.

Elastic Beanstalk

- Quickly deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications.
- Reduces management complexity.
- Simply upload application , it automatically handles the details of capacity provisioning, load balancing , scaling and application health monitoring .
- It automatically launches an environment , creates and configures AWS resources need to run your code.

Elastic Beanstalk

Elements of application that we can control using Elastic Beanstalk

- Select operating system as per requirements.
- Improve application by running in more than one availability zone.
- Enhance application security by enabling HTTPS on load balancing.
- Access built in cloud watch.
- Access log files without logging in application servers.
- Adjust application server settings
- Getting notifications on health checks and other important events.

Elastic Beanstalk - Common Use Cases

- Fast and simple to begin
- Developer productivity
- Impossible to outgrow
- Complete resource control

Lambda



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

Lambda Deployment Unit - Code

Run event-initiated, stateless applications that need quick response times

- AWS provisions and scales the server capacity and manages the utilization.
- AWS manages the availability and fault tolerance of the application.

Lambda - Common Use Cases

- It is a compute service that lets you run code without provisioning or managing servers.
- It executes your code only when needed and scales automatically.
- With this, you can run code for virtually any type of application or back-end service , with zero administration.
- AWS lambda manages the complete fleet that offers a balance of memory , CPU, network & other resources.

Batch



Compute

EC2

EC2 Container Service

Lightsail

Elastic Beanstalk

Lambda

Batch

Batch Deployment Unit - job

It enables developers, scientists and engineers to execute a series of jobs automatically in the cloud.

- AWS provisions and scales the server capacity and manages the utilization.
- AWS manages the availability and fault tolerance of the application.

Batch

- It enables developers , scientists and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.
- With AWS batch, there is no need to install and manage batch computing software or server clusters that you use to run your jobs , allowing you to focus analysing results & solving problems.
- AWS batch plans, schedules and executes your batch computing workloads across full range of AWS compute services and features such as Amazon EC2 & spot instances.

Batch - Common Use Cases

- It can shift the time of job processing to periods when greater or less expensive capacity is available.
- It avoids idling compute resources with frequent manual intervention and supervision.
- It increases efficiency by driving higher utilization of compute resources.
- Execution of multiple jobs in parallel.



Storage

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Storage



Storage

S3

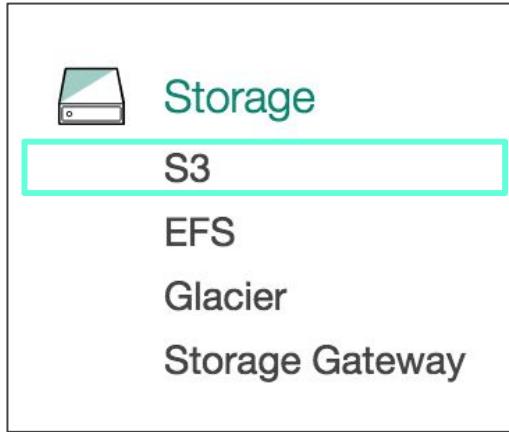
EFS

Glacier

Storage Gateway

- A critical component of cloud computing is cloud storage that holds the information used by applications.
- AWS offers a complete range of cloud storage services to support both application and archival compliance requirements.

Storage



S3 (Simple Storage Service)-

- Internet storage
- Any amount of data can be stored and retrieved at any time.
- AWS management console-a simple and intuitive web interface is used for this purpose.

Amazon S3 Basics

- In Amazon S3, data is stored as objects within buckets.
- The file can be uploaded in order to store object to a bucket.
- Permissions can be set on the object as well as any metadata in order to upload a file.
- Buckets acts as containers for objects and one can have one or more buckets.
- One can control access, view access logs and its objects, and choose the geographical region where S3 will store each bucket and their contents.
- Click on Get started button to begin.

Amazon S3 storage

Storage is of two types:

Block storage and file storage

Block storage : raw storage device level, manages data as a set of numbered , fixed size blocks.

File storage : higher level - operating system level and manages data as a named hierarchy of files and folders.

Object storage

- In Amazon S3 , instead of managing data as blocks or files using SCSI, CIFS or NFS protocols , data is managed as **objects** using an API built on standard HTTP levels.
- Each Amazon S3 object contains both data and metadata.
- Objects reside in containers called buckets.
- Identification of each object by a unique user specified key (file-name).
- 1 object = 0 byte - 5TB
- 1 bucket = unlimited number of objects.

Amazon S3 operations

- S3 API is intentionally simple .
- It has list of common operations :

create/ delete a bucket

Write an object

Read an object

Delete an object

List keys in a bucket

Object life cycle management

- Data - natural lifecycle : “hot” - frequently accessed data,
“Warm”- less frequently accessed data
“ cold” - long term backup and archive

Using Amazon S3 lifecycle configuration rules, can reduce storage costs by automatically transitioning data from one storage class to another or eventually deleting data after a period of time.

Amazon S3 key features

- Simplicity
- Durability
- Scalability
- Security
- Broad integration with other AWS services.
- Cloud data migration options
- Enterprise- class storage management

Sign up for Amazon S3

- AWS account is needed to use Amazon S3.
- To sign up for Amazon S3
 - Go to <https://aws.amazon.com/s3/> and choose Get started with Amazon S3.
 - Follow the on screen instructions
- Create a bucket
- Add an object to a bucket
- View an object
- Delete an object

Sign up for Amazon S3

Follow practical exercises

- Ex 2.1 : to create S3 bucket
- Ex 2.2 : to add and make an object public
- Ex 2.3 : to enable version of an object
- Ex 2.4 : to enable life cycle management
- Ex 2.5 : to enable static web hosting on a bucket
- Ex 2.6 : to enable web hosting.

Amazon S3 storage management

- It allow customers to take a data driven approach to storage optimization, compliance and management efficiency.
- These features work together to help improve workload performance, streamline business process workflows .
- It enable more intelligent storage tiering to optimize storage costs and performance.

Storage management

- **S3 object tagging** : you can manage and control access for Amazon S3 objects. S3 object tags are key value pairs applied to S3 objects which can be created, updated or deleted at any time during the lifetime of an object.
- **S3 inventory** : speed up business workflows and big data jobs . it supports CSV format.
- **S3 analytics - storage class analysis** : you can monitor the access frequency of the objects within S3 bucket in order to transition less frequently accessed storage to help you transition the right objects to S3 standard-IA.

Storage management

- **S3 analytics - storage class analytics** : with this, you can monitor the access frequency of the objects within S3 bucket in order to transition less frequently accessed storage to a lower cost storage class.
- **S3 cloudwatch metrics** : it helps to improve end user experience by providing end user monitoring and alarming on a host of different metrics. 1 min metrics are available at bucket level.
- **Data lifecycle management** : assigns and change cost performance as data evolves.
- **Cross region replication** : it replicates every object uploaded to your source bucket to a destination bucket in AWS region.

Data durability and reliability

- It provides highly durable storage infrastructure designed for mission - critical and primary data storage.'

Standard is :

- Backed with the Amazon S3 service level agreement for availability.
- Designed for 99.99999% durability and 99.99999% availability of objects over a given period.
- Designed to sustain concurrent loss of data.

Data durability and reliability

Standard - infrequent access is :

- Backed with the Amazon S3 service level agreement for availability.
- Designed for 99.99999% durability and 99.99999% availability of objects over a given period.
- Designed to sustain concurrent loss of data.

Amazon Glacier is :

- Designed for 99.99999% durability of objects over a given period.
- Designed to sustain concurrent loss of data.

Transferring large amounts of data

Amazon has a set of tools that makes migrating data into cloud faster , including ways to optimize or replace your network , and ways to integrate existing workflows with S3.

[S3 transfer acceleration](#) : it is designed to maximize transfer speeds to Amazon S3 buckets over long distances. It works by carrying HTTP and HTTPS traffic over a highly optimized network bridge that runs between AWS edge location nearest clients and S3 bucket.

[AWS snowball](#), [snowball edge](#) and [snowmobile](#) : used for large scale data transfers including high network costs, long transfer times & security concerns.

Transferring large amounts of data

AWS storage gateway : data or storage systems that exist on - premises can be easily linked to Amazon S3 using AWS storage gateway.

3rd party partner integration : a number of ISV partners are integrated with Amazon S3 for simplified data transfers and retrievals.

Security and Access management

Data stored in Amazon S3 is secure by default, only bucket and object owners have access to S3 resources they create. It supports multiple access control mechanisms as well as encryption for both secure transit and secure storage at rest.

Flexible access control mechanisms : it provides four different access control mechanisms : **AWS IAM (identity and access management) policies , ACLs (Access control lists) , bucket policies and query string authentication .**

Security and Access management

VPC endpoints : they are easy to configure and provide reliable connectivity to Amazon S3 without requiring an internet gateway or a NAT (network address translation) instance. With these endpoints , the data between an Amazon VPC and Amazon S3 is transferred within Amazon network , helping protect your instances from internet traffic.

Encryption : when Amazon S3 SSE encrypts data at rest, it uses Advanced encryption standard (AES) 256 bit encryption keys . for server side encryption keys are:

- SSE-S3, SSE- C, SSE- KMS

Security and Access management

[Audit logs](#) : it also supports logging of requests made against your S3 resources. These server access logs capture all requests made against a bucket or the objects in it and can be used for auditing purposes.

[Versioning](#) : it provides further protection with versioning capability. You can use versioning to preserve, retrieve and restore every version of every object in s3 bucket.

Security and Access management

Multifactor authentication delete : this is an additional security. It requires the use of MFA device to delete objects stored in S3 bucket.

Time limited access to objects : it supports query string authentication which allows you to provide a URL that is valid only for a length of time that you define. This time limited URL can be useful for scenarios such as software downloads or other applications where you want to restrict the length of time users have access to an object.

Elastic Block Store (EBS)

- Amazon EBS provides block level storage volumes for use with EC2 instances.
- EBS volumes are highly available and reliable storage volumes.
- These can be attached to any running instance that is in the same availability zone.

Elastic Block Store (EBS)

- EBS volumes can be launched as encrypted volumes for simplified data encryption.
- There is no need to build, manage, and secure key management infrastructure.
- When an encrypted EBS is created and attached to a supported instance type, data stored at rest on the volume, disk I/O and snapshots created from the volume are all encrypted.

Elastic Block Store (EBS)

- AWS key Management Service (AWS KMS) master keys are used by EBS to create encrypted volumes and any snapshots from encrypted volumes.
- A default master key is created automatically when an encrypted EBS volume is created for the first time.
- This key is used unless Customer Master Key (CMK) is selected that has been created separately using AWS key Management service.

Features of EBS

- One can Create EBS General Purpose SSD (gp2), Provisioned IOPS SSD (io1), Throughput Optimized HDD (st1), and Cold HDD (sc1) volumes up to 16 TiB in size.
- With General Purpose SSD (gp2) volumes, the base performance of 3 IOPS/GiB, with the ability to burst to 3,000 IOPS for extended periods of time has been expected.
- Volume performance monitoring.

Benefits of EBS volumes

- Data availability
- Data persistence
- Data encryption
- Snapshots
- Flexibility

EBS volume types

- Solid-state Drives (SSD)
- Hard disk Drives (HDD)

Creating an EBS volume

- Open console
- Select the region from the navigator bar
- Choose VOLUMES under ELASTIC BLOCK STORE in the navigation bar
- Above the upper pane, choose Create Volume.
- In the Create Volume dialog box, for Volume Type, choose General Purpose SSD (GP2), Provisioned IOPS SSD (IO1), Throughput Optimized HDD (ST1), Cold HDD (SC1), or Magnetic.
- For Size, enter the size of the volume, in GiB.



Attaching an EBS volume to instance

- Open console
- Choose volumes in the navigation bar
- Select a volume and choose Actions, Attach Volume
- In the Attach Volume dialog box, start typing the name or ID of the instance to attach the volume to for Instance, and select it from the list of suggestion options
- You can keep the suggested device name, or enter a different supported device name.
- Choose Attach.
- Connect to your instance and make the volume available.

Amazon EBS-Optimized Instances

- An Amazon EBS-optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O.
- This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.
- EBS-optimized instances deliver dedicated bandwidth to Amazon EBS, with options between 500 Mbps and 12,000 Mbps, depending on the instance type you use.

Amazon EBS-Optimized Instances

- When attached to an EBS-optimized instance, General Purpose SSD (gp2) volumes are designed to deliver within 10% of their baseline and burst performance 99% of the time in a given year.
- Provisioned IOPS SSD (io1) volumes are designed to deliver within 10% of their provisioned performance 99.9% of the time in a given year.

Amazon EBS-Optimized Instances

- Enabling EBS Optimization at Launch
 - Open the Amazon EC2 [console](#).
 - Click [Launch Instance](#). In [Step 1: Choose an Amazon Machine Image \(AMI\)](#), select an AMI.
 - In [Step 2: Choose an Instance Type](#), select an instance type that is listed as supporting EBS optimization.
 - In [Step 3: Configure Instance Details](#), complete the fields that you need and select [Launch as EBS-optimized instance](#).
 - Follow the directions to complete the wizard and launch your instance.

Amazon EBS-Optimized Instances

- Modifying EBS Optimization for a Running Instance
 - Open the Amazon EC2 [console](#).
 - In the navigation pane, click [Instances](#), and select the [instance](#).
 - Click [Actions](#), select [Instance State](#), and then click [Stop](#).
 - In the confirmation dialog box, click [Yes, Stop](#).
 - With the instance still selected, click [Actions](#), select [Instance Settings](#), and then click [Change Instance Type](#).
 - Click [Actions](#), select [Instance State](#), and then click [Start](#).

Amazon EBS Encryption

- Amazon EBS encryption offers you a simple encryption solution for your EBS volumes without the need for you to build, maintain, and secure your own key management infrastructure.
- The following types of data are encrypted:
 - Data at rest inside the volume
 - All data moving between the volume and the instance
 - All snapshots created from the volume

Amazon EBS Encryption

- The first time you create an encrypted volume in a region, a default CMK is created for you automatically.
- This key is used for Amazon EBS encryption unless you select a CMK that you created separately using AWS KMS.

Amazon EBS Encryption

- Snapshots that are taken and volumes that are created from encrypted volumes are automatically encrypted.
- You can share an encrypted snapshot with specific accounts if you take the following steps:
 - Use a custom CMK, not your default CMK, to encrypt your volume.
 - Give the specific accounts access to the custom CMK.
 - Create the snapshot.
 - Give the specific accounts access to the snapshot.

Initializing Amazon EBS Volumes

- New EBS volumes receive their maximum performance the moment that they are available and do not require initialization.
- Storage blocks on volumes that were restored from snapshots must be initialized before you can access the block.
- This preliminary action takes time and can cause a significant increase in the latency of an I/O operation the first time each block is accessed.

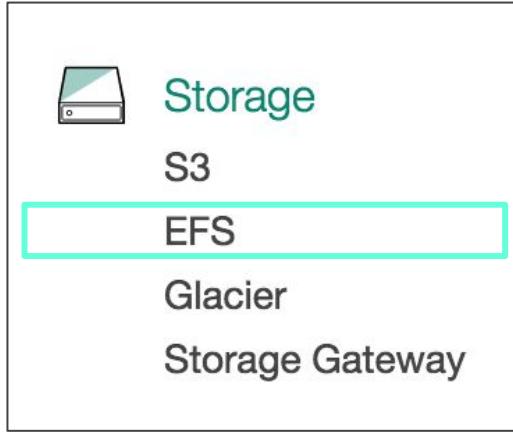
Benchmark EBS Volumes

- Launch an EBS-optimized instance.
- Create new EBS volumes.
- Attach the volumes to your EBS-optimized instance.
- Configure and mount the block device.
- Install a tool to benchmark I/O performance.
- Benchmark the I/O performance of your volumes.
- Delete your volumes and terminate your instance so that you don't continue to incur charges.

Amazon CloudWatch Events for Amazon EBS

- Amazon EBS emits notifications based on Amazon CloudWatch Events for a variety of snapshot and encryption status changes.
- With CloudWatch Events, you can establish rules that trigger programmatic actions in response to a change in snapshot or encryption key state.

Storage



EFS (Elastic File System)

- Provides simple, scalable file storage.
- With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it.

Elastic file systems

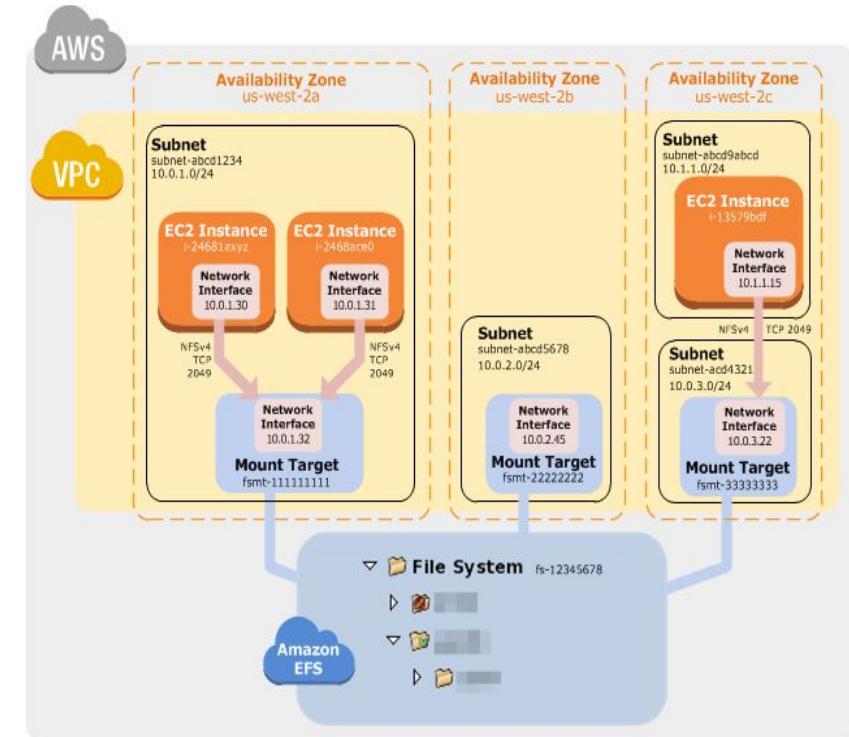
- These are distributed across an unconstrained number of storage servers, enabling file systems to grow elastically to petabyte scale and allowing massively parallel access from Amazon EC2 instances to your data.
- This distributed data storage design means that multi-threaded applications and applications that concurrently access data from multiple instances can drive substantial level of aggregate throughput and IOPS.
- Amazon EFS data is distributed across multiple availability zones providing high level of durability and availability.

Amazon EFS use cases

- Big data and analytics
- Media processing workflows
- Content management and web serving
- Home directories

EFS: How it works?

- The VPC has three Availability Zones, and each has one mount target created in it.
- Creating this setup works as follows :
 - Create your EC2 resources and launch your EC2 instance.
 - Create your EFS file system.
 - Connect to your EC2 instance, and mount the EFS file system.



Security groups

- Both an Amazon EC2 instance and a mount target have associated security groups which act as a virtual firewall that controls the traffic between them.
- The security groups you associate with a mount target must allow inbound access for the TCP protocol on the NFS port from all EC2 instances on which you want to mount the file system.

Managing EFS file systems

- File system management tasks refer to creating and deleting file systems, managing tags, and managing network accessibility of an existing file system.
- Managing network accessibility is about creating and managing mount targets.

Monitoring tools

- Automated monitoring tools
 - Amazon CloudWatch Alarms
 - Amazon CloudWatch Logs
 - Amazon CloudWatch Events
 - AWS CloudTrail Log Monitoring
- Manual monitoring tools
 - The current metered size, number of mount targets, and life cycle state from the EFS console
 - Current alarms and status, graphs of alarms and resources, and service health status from CloudWatch home page.

Authentication for Amazon EFS

- AWS account root user
 - You provide an email address and password that is associated with your AWS account when you sign up for AWS.
 - This is your AWS account root user.
- IAM user
 - Simply an identity within your AWS account that has specific custom permissions.

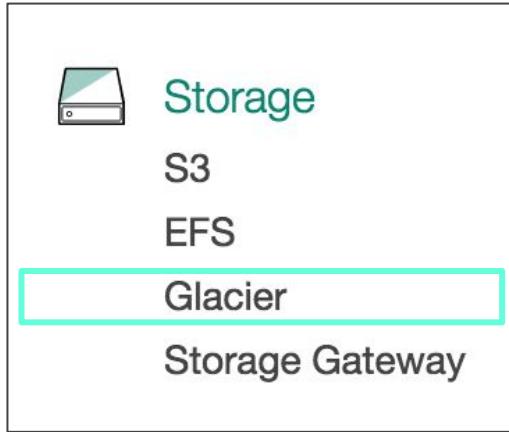
Authentication for Amazon EFS

- IAM role
 - It is another IAM identity that you can create in your account that has specific permissions.
 - An IAM role enables you to obtain temporary access keys that can be used to access AWS services and resources.

Amazon storage

- Amazon EFS provides a file system interface which provides concurrently accessible storage upto thousands of Amazon EC2 instances.
- Amazon EBS can deliver performance for workloads that require low latency access to data from a single EC2 instances.
- Amazon S3 makes data available through an internet API that can be accessed anywhere.

Storage



Glacier-

- A storage service optimized for infrequently used data, or "cold data."
- Provides durable, secure, and flexible storage for data archiving and online backup.
- Can store an unlimited amount of virtually any kind of data, in any format

Amazon Glacier Data Model

- The Amazon Glacier data model core concepts include vaults and archives.
- Amazon Glacier is a REST-based web service. In terms of REST, vaults and archives are the resources.
- Vault: In Amazon Glacier, a vault is a container for storing archives.
- Archive: It can be any data such as a photo, video, or document and is a base unit of storage in Amazon Glacier which has a unique ID and an optional description.

Amazon Glacier Data Model

- Job : Retrieving an archive and vault inventory are asynchronous operations in Amazon Glacier in which you first initiate a job, and then download the job output after Amazon Glacier completes the job.
- Notification Configuration: Amazon Glacier supports a notification mechanism to notify you when a job is complete.

Supported operations in Amazon Glacier

- **Vault Operations** : Amazon Glacier provides operations to create and delete vaults
- **Archive Operations** : Amazon Glacier provides operations for you to upload and delete archives . You cannot update an existing archive; you must delete the existing archive and upload a new archive.
- **Jobs** : Retrieving an archive or vault inventory from Amazon Glacier is an asynchronous operation. It requires you to first initiate a job, wait for the job to complete and then download the job output.

Amazon Glacier Data Model

- Accessing Amazon Glacier
 - Amazon Glacier is a RESTful web service that uses HTTP and HTTPS as a transport and JavaScript Object Notation (JSON) as a message serialization format.
 - When using the REST API directly, you must write the necessary code to sign and authenticate your requests.

Getting Started with Amazon Glacier

- In this, you will create a vault, upload and download an archive, and finally delete the archive and the vault.
- You can do all these operations programmatically.
- Step 1: Before You Begin with Amazon Glacier
- Step 2: Create a Vault in Amazon Glacier

Amazon Glacier features

- **Archives** : data is stored in Amazon Glacier in the form of archives, you can upload a single file as an archive or aggregate multiple files into TAR or ZIP file and upload as one archive. A single archive can be as large as 40 terabytes.
- **Vaults** : these serve as " containers " to store archives. You can view a list of vaults in the AWS management console and use AWS SDKs to perform a variety of vault operations such as create vault, delete vault, lock vault, list vault metadata, retrieve vault inventory , tag vaults for filtering and configure vault notifications.

Amazon Glacier key features

- Data retrieval features
- AWS snowball and direct connect integration
- Vault lock
- Access control
- Tagging support
- Audit logs
- Vault access policies
- Vault inventory
- Integrated lifecycle management with Amazon S3.

Amazon Glacier key features

- **Data retrieval features** : it provides three ways to retrieve your archives to meet varying access time and cost requirements: expedited, standard and bulk retrievals.
- **AWS snowball and direct connect integration** : AWS snowball can accelerate moving large amounts of data directly into and out of AWS using portable storage devices for transport. AWS transfers your data directly onto and off of storage devices using Amazon high speed internal network and by passing the internet. AWS direct connect makes it easy to establish a high bandwidth , dedicated network connection from your premises to AWS.

Amazon Glacier key features

- **Vault lock** : it allows you to easily deploy and enforce compliance controls on individual glacier vaults via a lockable policy and lock the policy from future edits. Once locked, the policy becomes immutable and Glacier will enforce the prescribed controls to help achieve your compliance objectives.
- **Access control** : it uses AWS IAM to help you securely control access to AWS and Glacier data. You can create users in IAM , assign individual security credentials and IAM policies on each Amazon Glacier vault to grant permitted activities to intended users.

Amazon Glacier key features

- **Vault access policies** : these policies allows you to easily manage access to your individual Glacier vaults. You can define an access policy on a vault to grant vault access to users and business groups internal to your organization as well as external business partners.
- **Vault inventory** : it maintains an inventory of all archives in each of your vaults for disaster recovery. It is updated approximately once a day.
- **Tagging support** : it allows you to tag your Glacier vaults for easier resource and cost management. Tags are labels that you can define and associate with your vaults.

Amazon Glacier key features

- **Integrated lifecycle management with Amazon S3** : Amazon Glacier works together with Amazon S3 lifecycle rules to help you to automate archiving of Amazon S3 data and reduce overall storage costs. You can easily set up a rule that stores all your previous Amazon S3 object versions in the lower cost Glacier storage class and deletes them from Glacier storage after 100 days.
- **AWS software development kits (SDKs)** : data upload and retrieval are done using AWS SDKs or Amazon Glacier API. Amazon Glacier is supported by AWS SDKs for java, .net, php, python. The SDKs libraries wrap the underlying Amazon API simplifying programming tasks. API libraries are : low level API & high level API.

Protecting your data

- Data stored in Amazon Glacier is protected by default, only vault owners have access to Amazon glacier resources they create. It encrypts your data at rest by default and supports secure data transit by SSL.
- It also supports access control mechanisms with IAM policies.
- With Amazon Glacier data protection features, you can protect your data from logical and physical failures, guarding against data loss from unintended user accounts, application errors and infrastructure breakdown.

Managing your data

- Uploading an archive to Amazon glacier.
- Downloading an archive from Amazon glacier.
- Deleting an archive in Amazon glacier.

Amazon Glacier Vault Lock

- Amazon Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual Amazon Glacier vaults with a vault lock policy.
- You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits.
- Once locked, the policy can no longer be changed.

Authentication

- You can access AWS as any of the following types of identities:
 - AWS account root user
 - IAM user
 - IAM role

Access control

- Every AWS resource is owned by an AWS account, and permissions to create or access a resource are governed by permissions policies.
- Amazon Glacier Resources and Operations
 - Amazon Glacier supports policies only at the vault level.
 - In an IAM policy, the Resource value that you specify can be a specific vault or a set of vaults in a specific AWS Region.

Access control

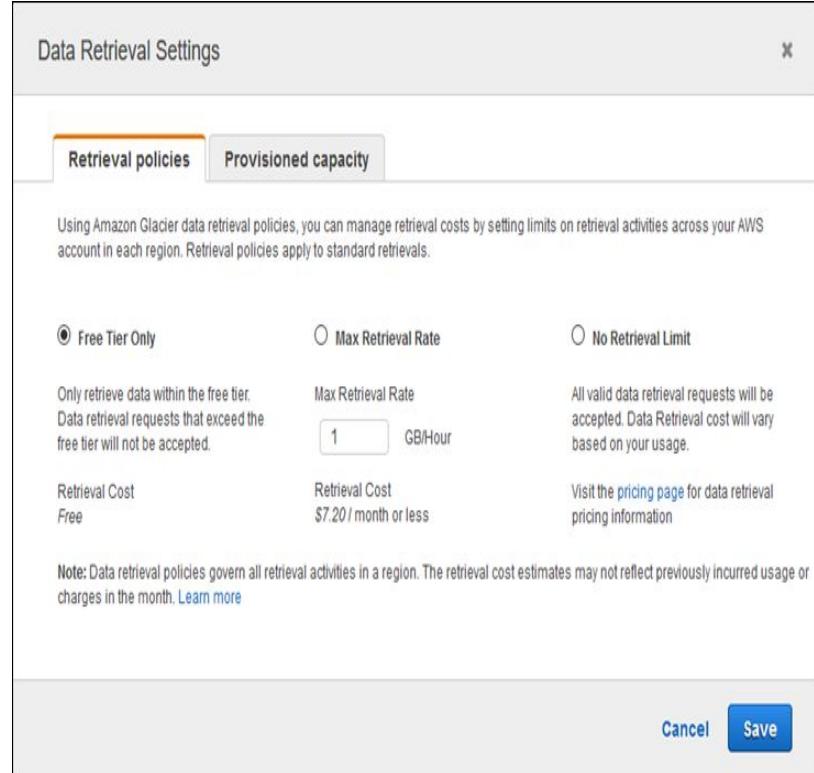
- Understanding Resource Ownership
 - A resource owner is the AWS account that created the resource.
 - The resource owner is the AWS account of the principal entity that authenticates the request that creates the resource.
- Managing Access to Resources
 - Identity-Based Policies (IAM policies)
 - Resource-Based Policies (Amazon Glacier Vault Policies)

Amazon Glacier Data Retrieval Policies

- With Amazon Glacier data retrieval policies, you can easily set data retrieval limits and manage the data retrieval activities across your AWS account in each region.
- Choosing an Amazon Glacier Data Retrieval Policy
- Three types of Amazon Glacier data retrieval policies : free tier only, max retrieval policies and no retrieval limit.

Amazon Glacier Data Retrieval Policies

- Using the Amazon Glacier Console to Set Up a Data Retrieval Policy
 - You can view and update the data retrieval policies in the Amazon Glacier console or by using the Amazon Glacier API.



Vault operations

- Abort Vault Lock (DELETE lock-policy)
- Add Tags To Vault (POST tags add)
- Create Vault (PUT vault)
- Complete Vault Lock (POST lockId)
- Delete Vault (DELETE vault)
- Delete Vault Access Policy (DELETE access-policy)
- Get Vault Notifications (GET notification-configuration)

Archive operations

- Delete Archive (DELETE archive)
 - This operation deletes an archive from a vault.
 - You can delete one archive at a time from a vault.
 - To delete the archive you must provide its archive ID in the delete request.
 - You can get the archive ID by downloading the vault inventory for the vault that contains the archive.

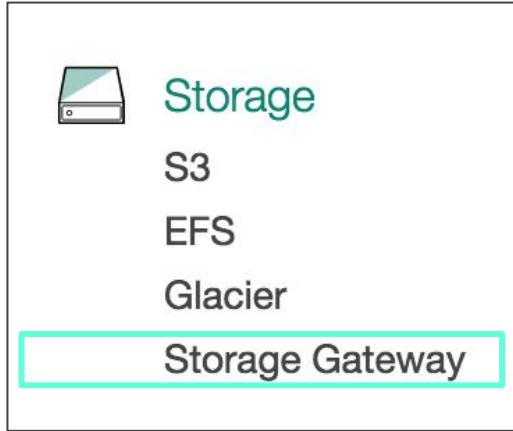
Archive operations

- Upload Archive (POST archive)
 - This operation adds an archive to a vault.
 - For a successful upload, your data is durably persisted. In response, Amazon Glacier returns the archive ID in the `x-amz-archive-id` header of the response.
 - You should save the archive ID returned so that you can access the archive later.



Storage gateway

Storage

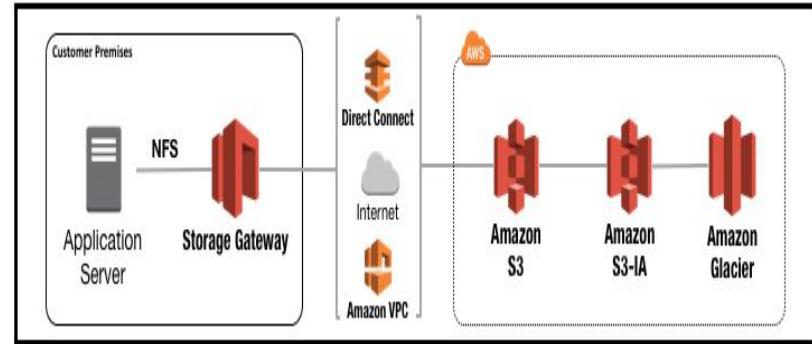


Storage Gateway-

- Connects an on-premises software appliance with cloud-based storage
- Provide seamless integration with data security features between your on-premises IT environment and the Amazon Web Services (AWS) storage infrastructure.
- offers file-based, volume-based and tape-based storage solutions

How AWS Storage Gateway Works

- File Gateway
 - Download a virtual machine image for the file storage gateway and activate it from the AWS Management Console or the storage gateway API to use file gateway storage.
 - Once activated, you configure the S3 bucket(s) that the gateway will expose as file system(s).

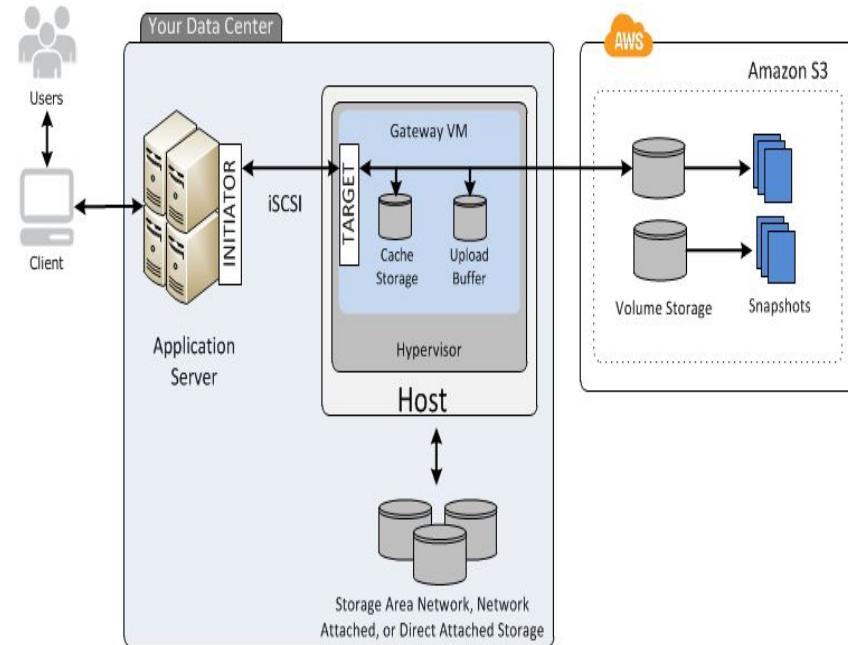


Data retrieval operations

- Volume Gateways
 - Cached Volumes Architecture
 - Cached volumes let you use Amazon S3 as your primary data storage while retaining frequently accessed data locally in your storage gateway.
 - Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data.
 - In the cached volumes solution, AWS Storage Gateway stores all your on-premises application data in a storage volume in Amazon S3.

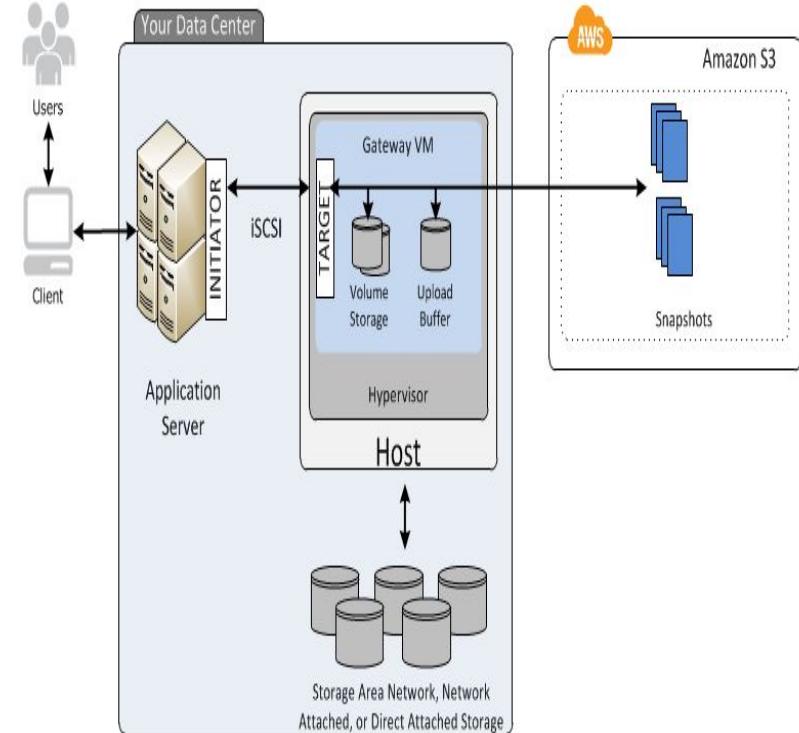
How AWS Storage Gateway Works

- After you've installed the AWS Storage Gateway software appliance—the virtual machine (VM)—on a host in your data center and activated it, you can use the AWS Management Console to provision storage volumes backed by Amazon S3.



Data retrieval operations

- Stored Volumes Architecture
Stored volumes let you store your primary data locally, while asynchronously backing up that data to AWS.

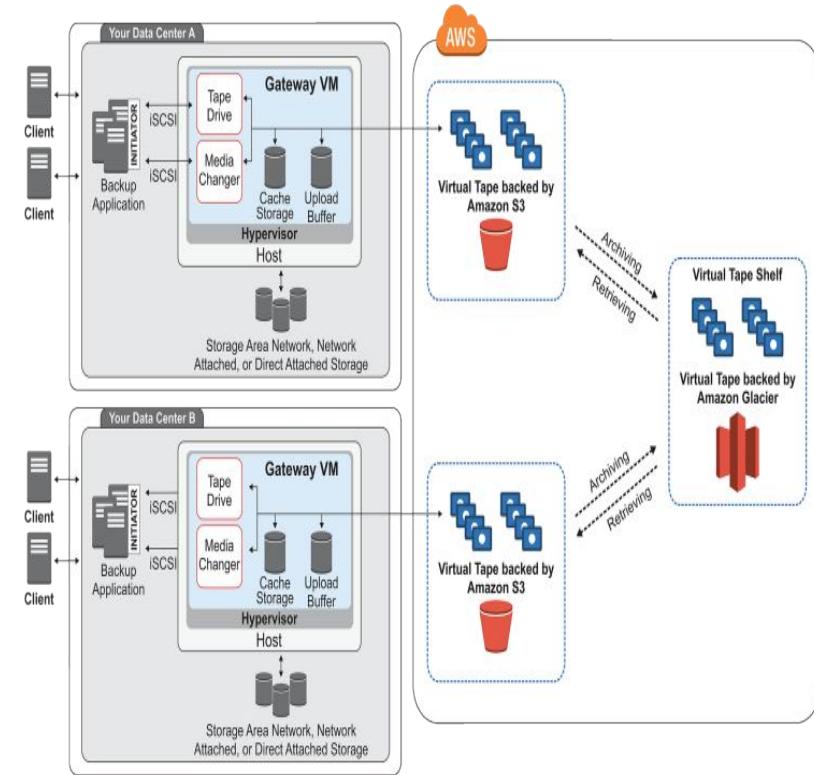


Data retrieval operations

- With stored volumes, you maintain your volume storage on-premises in your data center.
- After you've installed the AWS Storage Gateway software appliance—the virtual machine (VM)—on a host in your data center and activated it, you can create gateway storage volumes and map them to on-premises direct-attached storage (DAS) or storage area network (SAN) disks.

Data retrieval operations

- Tape gateway offers a durable, cost-effective solution to archive your data in the AWS Cloud. The VTL interface it provides lets you leverage your existing tape-based backup application infrastructure to store data on virtual tape cartridges that you create on your tape gateway.



Data retrieval operations

- Each tape gateway is preconfigured with a media changer and tape drives, which are available to your existing client backup applications as iSCSI devices.
- You add tape cartridges as you need to archive your data.
- The diagram identifies the following tape gateway components:
 - Virtual tape
 - Virtual tape library (VTL)
 - Archive
- Allocating Local Disks for the Gateway VM
 - Cache storage
 - Upload buffer

Creating Your Gateway

- To create your gateway, open the AWS Storage Gateway console and choose the AWS Region you want to create your gateway in.
- If you haven't created a gateway in this region, the AWS Storage Gateway page is displayed.



Managing file gateway

- Adding a file share
 - After your file gateway is activated and is running, you can add additional file shares.
 - When you create a file share, file gateway requires access to upload files into your Amazon S3 bucket.
 - To grant this access, file gateway creates an IAM access policy and role on your behalf.
- Deleting a File Share
 - If you no longer need a file share, you can delete it from the AWS Storage Gateway management console.
 - When you delete file share, the gateway is detached from the Amazon S3 bucket the file share maps to but the bucket and its contents are not deleted.

Managing file gateway

- Updating a File Share
 - You can update the default file share settings, the clients allowed to connect to your file share, and the metadata defaults for your file share.
- Refreshing Objects in Your Amazon S3 Bucket
 - As your NFS client performs file system operations, your gateway maintains an inventory of the objects in the Amazon S3 bucket associated with your file share.
 - Your gateway uses this cached inventory to reduce the latency and frequency of S3 requests.

Managing file gateway

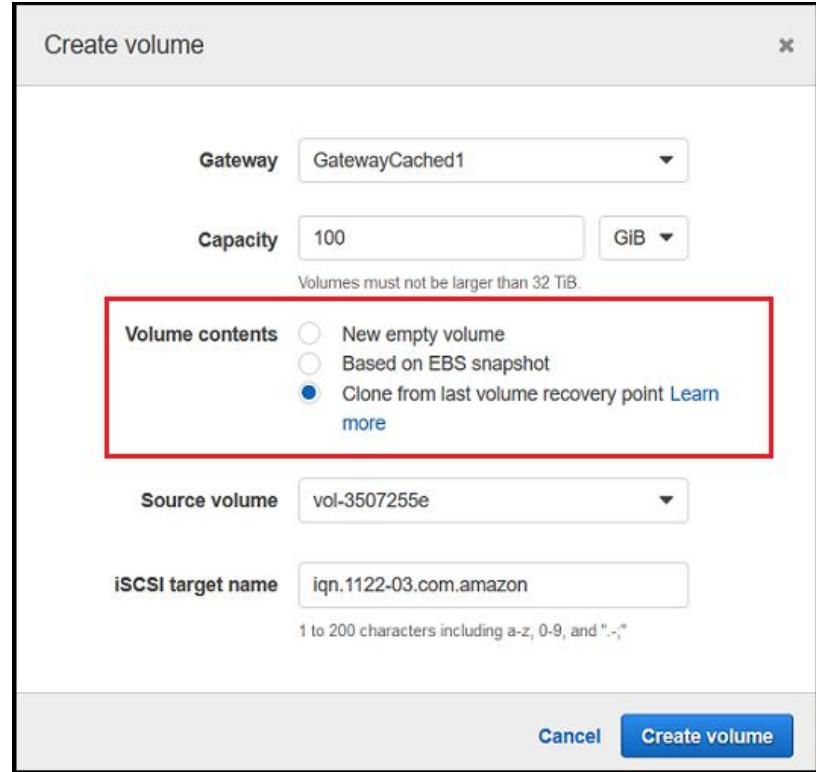
- Understanding File Share Status
 - You can see file share status on the AWS Storage Gateway console.
 - File share status appears in the Status column for each file share in your gateway.
 - A file share that is functioning normally has statusid as AVAILABLE.

Managing volume gateway

- Adding a Volume
 - As your application needs grow, you might need to add more volumes to your gateway.
 - As you add more volumes, you must consider the size of the cache storage and upload buffer you allocated to the gateway.
 - The gateway must have sufficient buffer and cache space for new volumes.

Managing volume gateway

- Cloning a Volume
 - To clone a volume, you choose the Clone from last recovery point option in the Create volume dialog box, then select the volume to use as the source.



Managing volume gateway

- Deleting a Volume
 - You might need to remove a volume as your application needs change
 - Before removing a volume, make sure that there are no applications currently writing to the volume.
- Creating a One-Time Snapshot
 - In addition to scheduled snapshots, Volume gateways allows you to take one-time, ad hoc snapshots.
 - By doing this, you can back up your storage volume immediately without waiting for the next scheduled snapshot.
- Editing a Snapshot Schedule
 - This schedule helps ensure that your gateway can keep up with the rate of incoming write operations on your local storage volumes.

Managing volume gateway

- Deleting a Snapshot
 - You might want to delete a snapshot, if you have taken many snapshots of a storage volume over a period of time and you don't need the older snapshots.
 - Because snapshots are incremental backups, if you delete a snapshot, only the data that is not needed in other snapshots is deleted.
- Understanding Volume Status
 - The status indicates that the volume is functioning normally and that no action is needed on your part.
 - The status also indicates a problem with the volume that might or might not require action on your part.

Managing volume gateway

- Deleting a Snapshot
 - You might want to delete a snapshot, if you have taken many snapshots of a storage volume over a period of time and you don't need the older snapshots.
 - Because snapshots are incremental backups, if you delete a snapshot, only the data that is not needed in other snapshots is deleted.
- Understanding Volume Status
 - The status indicates that the volume is functioning normally and that no action is needed on your part.
 - The status also indicates a problem with the volume that might or might not require action on your part.



Security, Identity & Compliance

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

- The first priority at AWS is cloud security.
- AWS and its partners offer tools and features to help you meet your security objectives around visibility, auditability, controllability, and agility.

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

IAM

- A web service that helps you securely control access to AWS resources for your users.
- Controls who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

Principals

- It is an IAM entity that is allowed to interact with AWS resources.
- It can be permanent or temporary.
- It can represent a human or an application.
- Types of principals : root users, IAM users , rules/ temporary security tokens.

Overview of Identity Management: Users

- Root User
 - When you create an AWS account, you create an account (or "root") identity, which you use to sign in to AWS.
 - You can sign in to the AWS Management Console using this root identity.
 - This combination of your email address and password is also called your root account credentials.

Overview of Identity Management: Users

- IAM User
 - Instead of sharing your root account credentials with others, you can create individual IAM users within your account that correspond to users in your organization.
 - IAM users are not separate accounts; they are users within your account.

Overview of Identity Management: Users

- Roles/ temporary security tokens
 - They are used to grant specific privileges to specific actors for a set duration of time.
 - Actors are authenticated by AWS.

Security Features Outside of IAM

- You use IAM to control access to tasks that are performed using the AWS Management Console, the AWS Command Line Tools, or service APIs using the AWS SDKs.
- Some AWS products have other ways to secure their resources as well.

Security Features Outside of IAM

- These access control methods are not part of IAM.
- IAM helps you control the tasks that are performed by making requests to Amazon Web Services, and it helps you control access to the AWS Management Console.
- IAM does not help you manage security for tasks like signing in to an operating system (Amazon EC2), database (Amazon RDS), desktop (Amazon WorkSpaces) , or collaboration site (Amazon WorkDocs).

Authentication

- IAM authenticates a principal in three ways:
 - **User Name/Password**—A username / password pair will be provided to the human, which is represented by a principal, to verify their identity.
 - **Access Key**—A combination of an access key ID (20 characters) and an access secret key (40 characters) is known as an access key.
 - **Access Key/Session Token**—The temporary security token provides an access key for authentication when a process operates under an assumed role.

Authentication

- An IAM user has neither an access key nor a password when it is created, and either or both can be set up by the IAS administrator.
- This adds an extra layer of security.
- After authenticating a principal, IAM, in order to protect your AWS infrastructure, must then manage the access of that principal.

Authorization

- Policies
 - Each permission defining:
 - Effect—A single word: Allow or Deny.
 - Service—Most AWS Cloud services support granting access through IAM, including IAM itself.
 - Resource—The specific AWS infrastructure is specified by the resource value, for which this permission applies. This is specified as an Amazon Resource Name (ARN).

Authorization

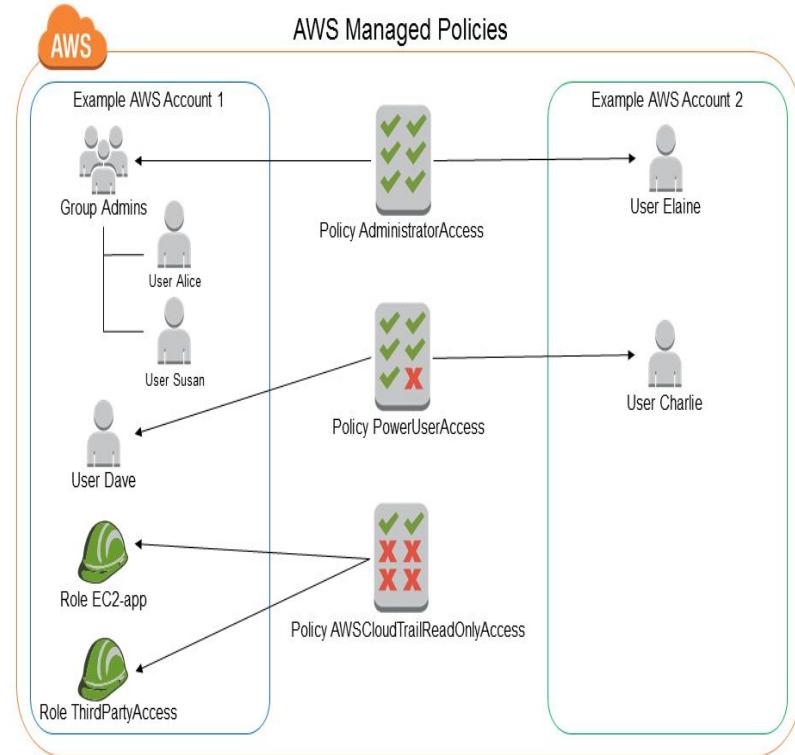
- Action—The subset of actions within a service that the permission allows or denies is specified by the action value.
- Condition—One or more additional restrictions that limit the actions allowed by the permission is defined by the condition value.

Authorization

- Associating Policies with Principals:
 - User Policy
 - Managed Policies
 - Group Policy
 - Managed Policies

Authorization

- Managed Policies—Standalone policies that you can attach to multiple users, groups, and roles in your AWS account.
- The following diagram illustrates AWS managed policies.



Using Multi-Factor Authentication (MFA) in AWS

- For increased security, you configure multi-factor authentication (MFA) to help protect your AWS resources.
- MFA adds extra security because it requires users to enter a unique authentication code from an approved authentication device or SMS text message when they access AWS websites or services.
- Security token-based: This type of MFA requires you to assign an MFA device (hardware or virtual) to the IAM user or the AWS root account.

Rotating Access Keys

- As a security best practice, an administrator, regularly rotate (change) the access keys for IAM users in your account.
- You can also apply a password policy to your account to require that all of your IAM users periodically rotate their passwords.

Changing Permissions for an IAM User

- You can change the permissions for an IAM user in your AWS account by changing its group memberships or by attaching and detaching managed policies.
- A user gets its permissions through one of the following methods:
 - Group membership
 - Direct policy attachment
- You can change permissions associated with a user through one of three techniques:
Add user to the group, copy permissions from existing user, attach policies directly to user.

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

Inspector

- Enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues.
- You can define a collection of AWS resources, create an assessment template and launch a security assessment run of assessment target.

Amazon Inspector Terminology and Concepts

- AWS agent
 - A software agent that you must install on all Amazon EC2 instances that are included in the assessment target, the security of which you want to evaluate with Amazon Inspector.
 - Monitors the behavior of the EC2 instance on which it is installed, including network, file system, and process activity
 - Collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service.

Amazon Inspector Terminology and Concepts

- Assessment run
 - The process of discovering potential security issues through the analysis of your assessment target's configuration and behavior against specified rules packages.
 - During an assessment run, the agent monitors, collects, and analyzes behavioral data (telemetry) within the specified target, such as the use of secure channels, network traffic among running processes, and details of communication with AWS services.

Amazon Inspector Terminology and Concepts

- Assessment target
 - In the context of Amazon Inspector, a collection of AWS resources that work together as a unit to help you accomplish your business goals.
 - Amazon Inspector evaluates the security state of the resources that constitute the assessment target.
 - To create an Amazon Inspector assessment target, you must first tag your EC2 instances with key-value pairs of your choice, and then create a view of these tagged EC2 instances that have common keys or common values.

Amazon Inspector Terminology and Concepts

- Assessment template
 - A configuration that is used during your assessment run, including rules packages against which you want Amazon Inspector to evaluate your assessment target, the duration of the assessment run, Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings.

Amazon Inspector Terminology and Concepts

- **Finding** : A potential security issue discovered during the Amazon Inspector assessment run of the specified target.
- **Rule**: A security check that the agent performs during an assessment run.
- **Rules package** :A collection of rules : A rules package corresponds to a security goal that you might have.
- **Telemetry**: Data such as records of network connections and process creations, collected during an assessment run and passed to the Amazon Inspector service for analysis.

Setting up Amazon Inspector

- To sign up for AWS
 - Open <https://aws.amazon.com/>, and then choose Create an AWS Account.
 - Follow the online instructions.
- Create a Role
 - On the Inspector prerequisites page, choose Select/Create Role.
- Create Assessment Targets with EC2 instance Tags
 - Amazon Inspector evaluates whether your assessment targets have potential security issues.
- Install the AWS Agent

AWS Agents

- To assess the security of the EC2 instances that make up your Amazon Inspector assessment targets, you must install the AWS agent on each instance.
- The agent monitors the behavior (including network, file system, and process activity) of the EC2 instance on which it is installed, collects behavior and configuration data (telemetry), and then passes the data to the Amazon Inspector service.

AWS Agents

- Once authenticated, the agent sends heartbeat messages to the service and receives instructions from the service as responses to the heartbeat messages.
- If an assessment has been scheduled, the agent receives the instructions for that assessment.
- During an assessment, the agent gathers telemetry data from the system to send back to Amazon Inspector over a TLS-protected channel.

AWS Agents

- Telemetry Data Lifecycle
 - The telemetry data stored in S3 is retained only to allow for assistance with support requests and is not used or aggregated by Amazon for any other purpose.
 - After 30 days, telemetry data is permanently deleted per a standard Amazon Inspector-dedicated S3 bucket lifecycle policy.

Amazon Inspector Assessment Targets

- You can use Amazon Inspector to evaluate whether your AWS assessment targets have potential security issues that you need to address.
- To create an assessment target for Amazon Inspector to assess, you start by tagging the EC2 instances that you want to include in your target.
- Every AWS tag consists of a key and value pair of your choice.

Amazon Inspector Assessment Templates

- An assessment template allows you to specify a configuration for your assessment runs, including the following:
 - Rules packages that Amazon Inspector uses to evaluate your assessment target
 - Duration of the assessment run
- Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings.

Assessment Runs

- After you create an assessment template, you can use it to start assessment runs.
- You can start multiple assessment runs using the same template as long as you stay within the assessment runs limit per AWS account.
- If you use the Amazon Inspector console, you must start the first run of your new assessment template from the [Assessment templates](#) page.
- After you start the run, you can use the [Assessment runs](#) page to monitor the run's progress.

Amazon Inspector Findings

- Findings are potential security issues discovered during the Amazon Inspector's assessment of the selected assessment target.
- Findings contain both a detailed description of the security issues and recommendations for resolving them.
- Once Amazon Inspector generates the findings, you can track them by assigning Amazon Inspector-specific attributes to them.

Assessment Reports

- An assessment report is a document that details what is tested in the assessment run, and the results of the assessment.
- The results of your assessment are formatted into standard reports, which can be generated to share results within your team for remediation actions, to enrich compliance audit data, or to store for future reference.

Amazon Inspector Rules Packages and Rules

- In Amazon Inspector, rules are grouped together into distinct **rules packages** either by category, severity, or pricing.
- **High**, **Medium**, and **Low** levels all indicate a security issue that can result in compromised information confidentiality, integrity, and availability within your assessment target.
- The **Informational** level simply highlights a security configuration detail of your assessment target.

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

Certificate Manager

- Handles the complexity of creating and managing SSL/TLS certificates for your AWS based websites and applications.
- You use certificates provided by ACM (ACM Certificates) or certificates that you import into ACM.

Concepts

- Certificate Authority
- Domain Name System
- Domain Name
- Encryption and decryption
- Public key infrastructure
- Root certificate
- Secure sockets layer
- Secure HTTPS
- SSL server certificates
- Symmetric key cryptography
- trust

ACM Certificate Characteristics

- Domain Validation (DV)
- Validity Period
- Managed Renewal and Deployment
- Browser and Application Trust
- Multiple domain names
- Wildcard names
- Algorithms

Services Integrated with AWS Certificate Manager

- Elastic Load Balancing
- Amazon CloudFront
- AWS Elastic Beanstalk
- Amazon API gateway
- AWS cloud formation

Importing Certificates into AWS Certificate Manager

- In addition to requesting SSL/TLS certificates provided by AWS Certificate Manager (ACM), you can import certificates that you obtained outside of AWS.
- You might do this because you already obtained a certificate from a third-party issuer, or because the certificates provided by ACM do not meet your requirements.

Tagging AWS Certificate Manager Certificates

- A tag is a label that you can assign to an ACM Certificate.
- You can create custom tags that suit your needs.
- Tag Restrictions
 - The maximum number of tags per ACM Certificate is 50.
 - The maximum length of a tag key is 127 characters.
 - The maximum length of a tag value is 255 characters.
 - Tag keys and values are case sensitive.

Authentication

- Access to ACM requires credentials that AWS can use to authenticate your requests.
- You can access AWS as any of the following types of identities:
 - AWS account root user
 - IAM user
 - IAM role

Access Control

- You can have valid credentials to authenticate your requests, but unless you have permissions you cannot create or access ACM resources.
- Every AWS resource belongs to an AWS account, and permissions to create or access the resources are defined in permissions policies in that account.
- In ACM, the primary resource is a certificate. Certificates have unique Amazon Resource Names (ARNs) associated with them.

Access Control

- IAM offers the following types of identity-based policies:
 - AWS-managed policies
 - Policies that are created and managed by AWS.
 - These are standalone policies that you can attach to multiple users, groups, and roles in your AWS account.
 - Customer-managed policies
 - Policies that you create and manage in your AWS account and which you can attach to multiple users, groups, and roles.
 - Inline policies
 - Policies that you create and manage and which you embed directly into a single user, group, or role.

ACM Private Key Security

- When you request a certificate, AWS Certificate Manager (ACM) generates a public/private key pair.
- The process works like this:
 - Creation of an AWS-managed customer master key (CMK) in AWS KMS with the alias aws/acm.
 - Encryption of the certificate's private key using CMK
 - Sending of the certificate and the encrypted private key to the load balancer or distribution.
 - Decryption of the private key by the load balancer or distribution.
 - Disassociation of certificate from the load balancer or distribution.

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

Directory Service

- Provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory with other AWS services.
- You can choose the directory service with the features you need at a cost that fits your budget.

Which to Choose?

- [Amazon Cloud Directory](#) is a cloud-native directory that can store hundreds of millions of application-specific objects with multiple relationships and schemas.
- [Amazon Cognito](#) is a user directory that adds sign-up and sign-in to your mobile app or web application using Amazon Cognito User Pools.
- [AWS Directory Service for Microsoft Active Directory \(Enterprise Edition\)](#) is a managed Microsoft Active Directory hosted on the AWS cloud.

Which to Choose?

- **AD Connector** is a proxy service for connecting your on-premises Microsoft Active Directory to the AWS cloud without requiring complex directory synchronization or the cost and complexity of hosting a federation infrastructure.
- **Simple AD** is a Microsoft Active Directory-compatible directory from AWS Directory Service.

Amazon Cloud Directory

- Amazon Cloud Directory is a highly available multi-tenant directory-based store in AWS.
- It is a directory-based data store that can create various types of objects in a schema-oriented fashion.
- These directories scale automatically to hundreds of millions of objects as needed for applications.

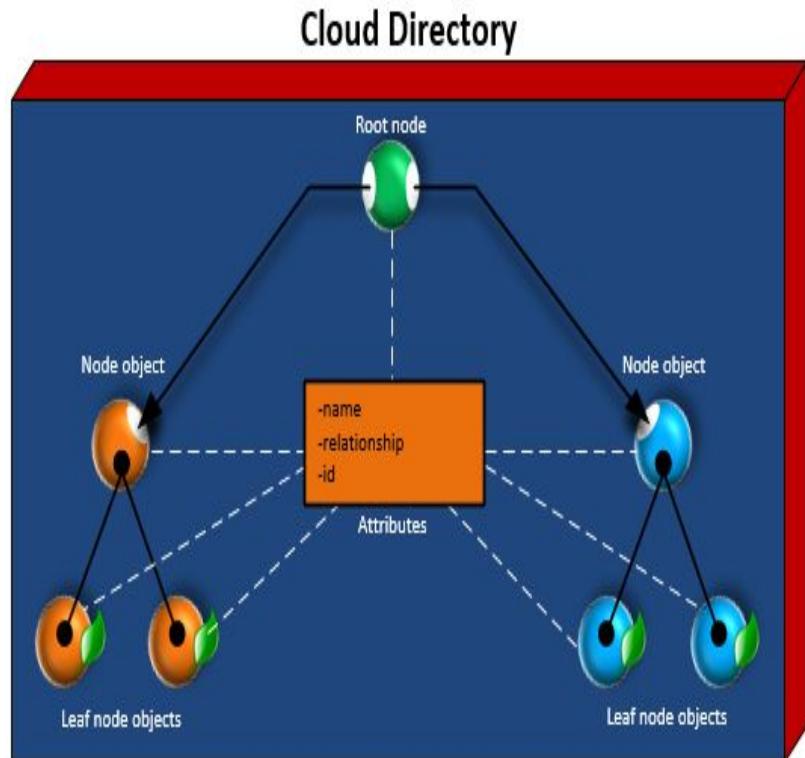
Amazon Cloud Directory

- Amazon Cloud Directory is a highly available multi-tenant directory-based store in AWS.
- It is a directory-based data store that can create various types of objects in a schema-oriented fashion.
- These directories scale automatically to hundreds of millions of objects as needed for applications.

Amazon Cloud Directory

- Directory Structure

- Data in a directory is structured hierarchically in a tree pattern consisting of nodes, leaf nodes, and links between the nodes, as shown in the figure.



Amazon Cloud Directory

- **Root Node** : The root is the top node in a directory that is used to organize the parent and child nodes in the hierarchy.
- **Node** : A node represents an object that can have child objects.
- **Leaf node** : A leaf node represents an object with no children that may or may not be directly connected to a parent node.
- **Node link** : The connection between one node and another.

Microsoft Active Directory

- It is created as a highly available pair of domain controllers connected to your virtual private cloud (VPC).
- With Microsoft AD, you can run directory-aware workloads in the AWS Cloud, including Microsoft SharePoint and custom .NET and SQL Server-based applications.

Microsoft Active Directory

- Securely connect to Amazon EC2 Linux and Windows instances.
- Simplify the deployment and management of cloud-based Linux and Microsoft Windows workloads.
- You can use Microsoft AD to enable multi-factor authentication by integrating with your existing RADIUS-based MFA infrastructure to provide an additional layer of security when users access AWS applications.

Active Directory Connector

- AD Connector is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud.
- AD Connector comes in two sizes, small and large.
- A small AD Connector is designed for smaller organizations of up to 500 users.
- A large AD Connector can support larger organizations of up to 5,000 users.

Simple Active Directory

- Simple AD is a standalone managed directory.
- It is available in two sizes, small and large.
- A small Simple AD supports up to 500 users (approximately 2,000 objects including users, groups, and computers).
- A large Simple AD supports up to 5,000 users (approximately 20,000 objects, including users, groups, and computers).

Managing Your Directory

- You use the AWS Directory Service management console to perform certain directory-related actions, such as changing directory information or deleting an existing directory.
- After a directory is created, most administrative functions are performed with directory management tools, such as the Active Directory Administration Tools.

Managing Your Directory

- Get Notified of Directory Status Updates Using Amazon SNS
 - Using SNS, you can receive email or text (SMS) messages when the status of your directory changes.
 - You get notified if your directory goes from an Active status to an Impaired or Inoperable status.
 - You also receive a notification when the directory returns to an Active status.

Managing Your Directory

- **Snapshots**
 - The snapshots can be used to perform a point-in-time restore for your directory.
 - A snapshot can be used to restore your directory to what it was at the point in time that the snapshot was taken.
 - Restoring a directory from a snapshot is equivalent to moving the directory back in time.
 - You can also delete the snapshot whenever required.

Add Users and Groups

- You can create users and groups with the Active Directory Users and Computers tool.
- Users represent individual people or entities that have access to your directory.
- Groups are very useful for giving or denying privileges to groups of users, rather than having to apply those privileges to each individual user.

Grant Users and Groups Access to AWS Resources

- AWS Directory Service provides the ability to give your directory users and groups access to AWS services and resources, such as:
 - Editing the Trust Relationship for an Existing Role
 - Creating a New Role
 - You must create a new IAM role using the IAM console.

Grant Users and Groups Access to AWS Resources

- Assigning Users or Groups to an Existing Role
 - You can assign an existing IAM role to an AWS Directory Service user or group.
 - The role must have a trust relationship with AWS Directory Service.
- Viewing Users and Groups Assigned to a Role
- Removing a User or Group from a Role

Add an Instance to Your Directory

- You can seamlessly join an EC2 instance to your directory domain when the instance is launched using the Amazon EC2 Systems Manager.
- If you need to manually join an EC2 instance to your domain, you must launch the instance in the proper region and security group or subnet, then join the instance to the domain.

Authentication and Access Control

- You can have valid credentials to authenticate your requests, but unless you have permissions you cannot create or access AWS Directory Service resources.
- Every AWS resource is owned by an AWS account, and permissions to create or access the resources are governed by permissions policies.
- An account administrator can attach permissions policies to IAM identities, and some services also support attaching permissions policies to resources.



WAF & SHIELD

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

WAF & Shield

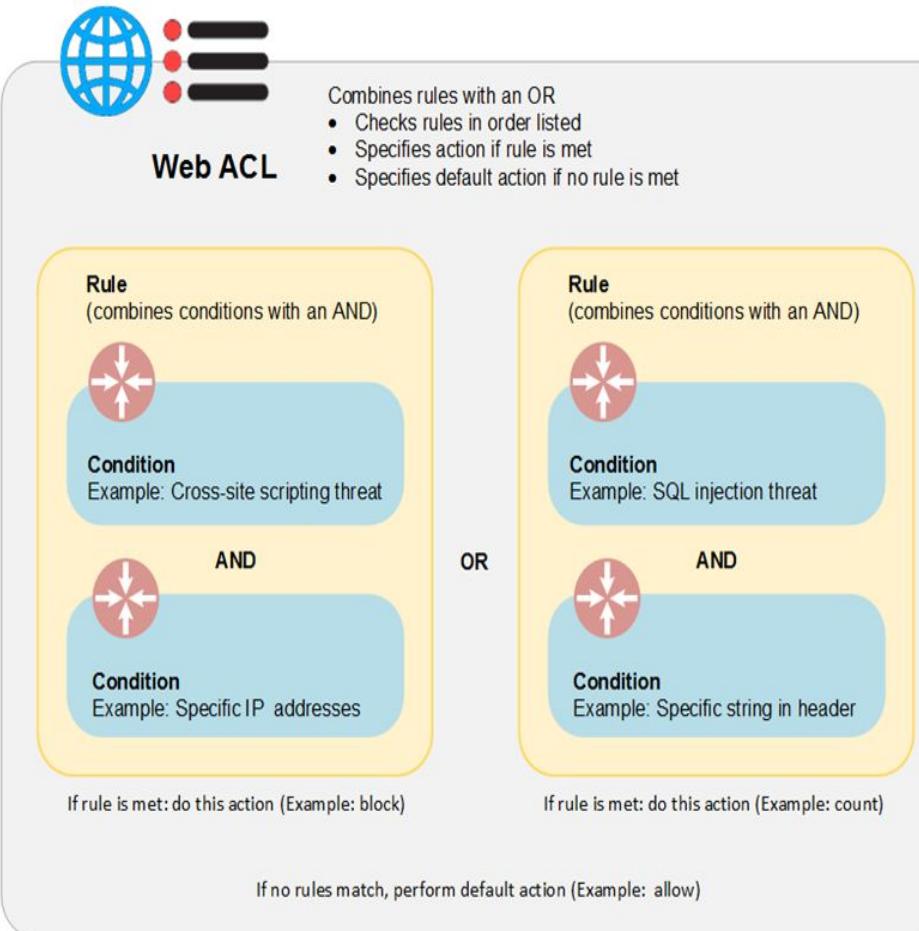
- AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests.
- AWS also provides AWS Shield Standard and AWS Shield Advanced to help minimize the effects of a distributed denial of service (DDoS) attack.

AWS WAF

- You use AWS WAF to control how Amazon CloudFront or an Application Load Balancer responds to web requests.
- You start by creating conditions, rules, and web access control lists (web ACLs).
- Conditions define the basic characteristics that you want AWS WAF to watch for in web requests.

AWS WAF

- The following illustration shows how AWS WAF checks the rules and performs the actions based on those rules.



AWS WAF with Amazon CloudFront Features

- When you create a web ACL, you can specify one or more CloudFront distributions that you want AWS WAF to inspect.
- AWS WAF starts to allow, block, or count web requests for those distributions based on the conditions that you identify in the web ACL.
- CloudFront provides some features that enhance the AWS WAF functionality.

AWS WAF with Amazon CloudFront Features

- Using AWS WAF with CloudFront Custom Error Pages
 - When AWS WAF blocks a web request based on the conditions that you specify, it returns HTTP status code 403 (Forbidden) to CloudFront.
 - CloudFront returns that status code to the viewer.
 - The viewer then displays a brief and sparsely formatted default message.
- Using AWS WAF with CloudFront Geo Restriction
 - If you want to block web requests from specific countries and also block requests based on other conditions, you can use CloudFront geo restriction in conjunction with AWS WAF.

AWS WAF with Amazon CloudFront Features

- Choosing the HTTP Methods That CloudFront Responds To
 - GET, HEAD
 - You can use CloudFront only to get objects from your origin or to get object headers.
 - GET, HEAD, OPTIONS
 - You can use CloudFront only to get objects from your origin, get object headers, or retrieve a list of the options that your origin server supports.

Authentication and Access Control for AWS WAF

- AWS WAF integrates with AWS Identity and Access Management (IAM), a service that lets your organization do the following:
 - Create users and groups under your organization's AWS account
 - Share your AWS account resources with users in the account
 - Assign unique security credentials to each user
 - Control user access to services and resources
- In AWS WAF, the resources are [web ACLs](#) and [rules](#).

Authentication and Access Control for AWS WAF

- For each AWS WAF resource, the service defines a set of API operations.
- To grant permissions for these API operations, AWS WAF defines a set of actions that you can specify in a policy.
- When you grant permissions, you can use the IAM policy language to specify the conditions when a policy should take effect.

AWS Shield

- A DDoS attack can prevent legitimate users from accessing a service and can cause the system to crash due to the overwhelming traffic volume.
- This DDoS protection, known as AWS Shield Standard, is included with AWS WAF.
- AWS Shield Advanced provides expanded DDoS attack protection
- AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks, but also for application layer (layer 7) attacks.

AWS Shield

- Types of DDoS Attacks
 - User Datagram Protocol (UDP) reflection attacks
 - SYN flood
 - DNS query flood
 - HTTP flood/cache-busting (layer 7) attacks
- For layer 7 DDoS attacks, AWS attempts to detect and notify AWS Shield Advanced customers through CloudWatch alarms, but does not apply mitigations proactively.

Monitoring AWS WAF and AWS Shield Advanced

- Monitoring is an important part of maintaining the reliability, availability, and performance of AWS WAF and for identifying possible DDoS attacks using AWS Shield.
- As you start, you should create a monitoring plan.
- The next step is to establish a baseline for normal performance in your environment.

Monitoring AWS WAF and AWS Shield Advanced

- Automated Monitoring Tools
 - Amazon CloudWatch Alarms
 - Amazon CloudWatch Logs
 - Amazon CloudWatch Events
 - AWS CloudTrail Log Monitoring
- Manual Monitoring Tools
 - This involves manually monitoring those items that the CloudWatch alarms don't cover.

Monitoring with Amazon CloudWatch

- You can monitor web requests and web ACLs and rules using CloudWatch, which collects and processes raw data from AWS WAF into readable, near real-time metrics.
- You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state.
- A notification is sent to an Amazon SNS topic or Auto Scaling policy.
- Alarms invoke actions for sustained state changes only.

Responding to DDoS Attacks

- Layer 3 and layer 4 attacks are addressed automatically by AWS.
- However, if DDoS alarms in CloudWatch indicate a possible layer 7 attack, you have two options:
 - Investigate and mitigate the attack on your own
 - If you are an AWS Shield Advanced customer, you also have the option of contacting the AWS Support Center



Compliance reports

Security, Identity & Compliance



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

Compliance Reports

- Enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud
- AWS compliance enablers build on traditional programs, helping you to establish and operate in an AWS security control environment.

Overview of Compliance in AWS

- When customers move their production workloads to the AWS cloud, the IT environment is managed by both the parties.
- The environment can be set by the customers in a secure and controlled manner.
- An adequate governance can be maintained by the customers over their entire IT control environment.

Strong Compliance Governance

- Regardless of how their IT is deployed, it is still the responsibility of the customer to maintain adequate governance over the entire IT control environment.
- The customers can apply different types of controls and various verification methods by deploying to the AWS Cloud.

Evaluating and Integrating AWS Controls

- A wide range of information regarding its IT control environment is provided by AWS via white papers, reports, certifications, and other third-party attestations.
- Internal and/or external auditors validate the design and operating effectiveness of controls and control objectives.

Risk Management

- A strategic business plan has developed by AWS that includes risk identification and the implementation of controls to mitigate or manage risks.
- An information security framework and policies have been established by the AWS compliance and security teams based on the [Control Objectives for Information and Related Technology \(COBIT\)](#) framework.

Risk Management

- Any public-facing endpoint IP addresses are regularly scanned by the AWS security team for vulnerabilities, and these scans do not include customer instances.
- Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.
- Customers can request permission to conduct their own vulnerability scans on their own environments.

Control Environment

- A comprehensive control environment, consists of policies, processes, and control activities, for the secure delivery of AWS service offerings, has been managed by AWS.
- To establish and maintain an environment that supports the operating effectiveness of AWS control framework, the collective control environment includes people, processes, and technology.

Information Security

- To protect the confidentiality, integrity, and availability of customer's systems and data, a formal information security program is used by AWS.
- Several security white papers have been published by AWS that are available on the main AWS website.
- These white papers are recommended for reading before you should take the AWS Solutions Architect Associate exam.

AWS CloudHSM

- A hardware security module (HSM) is a hardware appliance that provides secure key storage and cryptographic operations within a tamper-resistant hardware module.
- It helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated HSM appliances within the AWS cloud.

AWS Key Management Service

- AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.
- It is integrated with other AWS services to make it simple to encrypt your data with encryption keys that you manage.
- It is also integrated with AWS CloudTrail to provide you with key usage logs to help meet your auditing, regulatory and compliance needs.

AWS Key Management Service

- The following management actions can be performed on master keys by using AWS KMS:
 - Create, describe, and list master keys
 - Enable and disable master keys
 - Set and retrieve master key usage policies (access control)
 - Create, delete, list, and update aliases, which are friendly names that point to your master keys
 - Delete master keys to complete the key lifecycle

AWS Key Management Service

- The following cryptographic functions can be performed using master keys:
 - Encrypt, decrypt, and re-encrypt data
 - Generate data encryption keys that you can export from the service in plaintext or encrypted under a master key that doesn't leave the service
 - Generate random numbers suitable for cryptographic applications

AWS Organizations

- AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an **organization** that you create and centrally manage.
- AWS Organizations includes all the functionality of Consolidated Billing.
- You can use your organization to create accounts and invite existing accounts to join your organization.

AWS Organizations

- Features
 - Centralized management of all of your AWS accounts
 - Consolidated billing for all member accounts
 - Hierarchical grouping of your accounts to meet your budgetary, security, or compliance needs
 - Control over the AWS services and actions that each account can access
 - Integration and support for AWS Identity and Access Management (IAM)
 - Data replication that is "eventually consistent"



Start database



Messaging

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Messaging



Messaging

Simple Queue Service

Simple Notification Service

SES

- AWS manages the ongoing operations and underlying infrastructure needed to reliably run and scale your message queues.
- You eliminate the complexity and administrative overhead associated with managing dedicated message-oriented middleware (MoM) and associated infrastructure.

Messaging



Messaging

Simple Queue Service

Simple Notification Service

SES

Simple Queue Service:

- Offers a reliable, highly-scalable hosted queue for storing messages as they travel between applications or microservices.
- It moves data between distributed application components and helps you decouple these components.

Amazon SQS

- Amazon SQS provides familiar middleware constructs such as dead-letter queues and poison-pill management.
- It also provides a generic web services API.
- Use Amazon SQS when you need each unique message to be consumed only once and for cases such as the following:
 - Decoupling the components of an application
 - Configuring individual message delay
 - Dynamically increasing concurrency or throughput at read time
 - Scaling transparently

Amazon SQS

- Main Features of Amazon SQS
 - Redundant infrastructure
 - Multiple producers and consumers
 - Configurable settings per queue
 - Variable message size
 - Access control
 - Delay queues
 - PCI compliance
 - HIPAA compliance

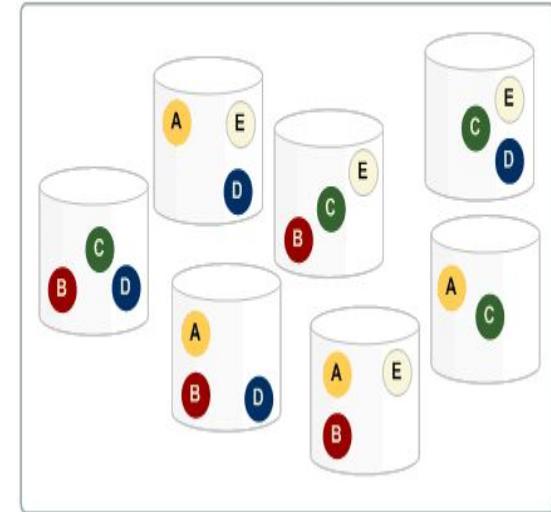
Basic Architecture of Amazon SQS

- There are three main actors in the overall system:
 - The components of your distributed system
 - Queues
 - Messages in the queues

Your Distributed System's Components



Your Queue (Distributed on SQS Servers)

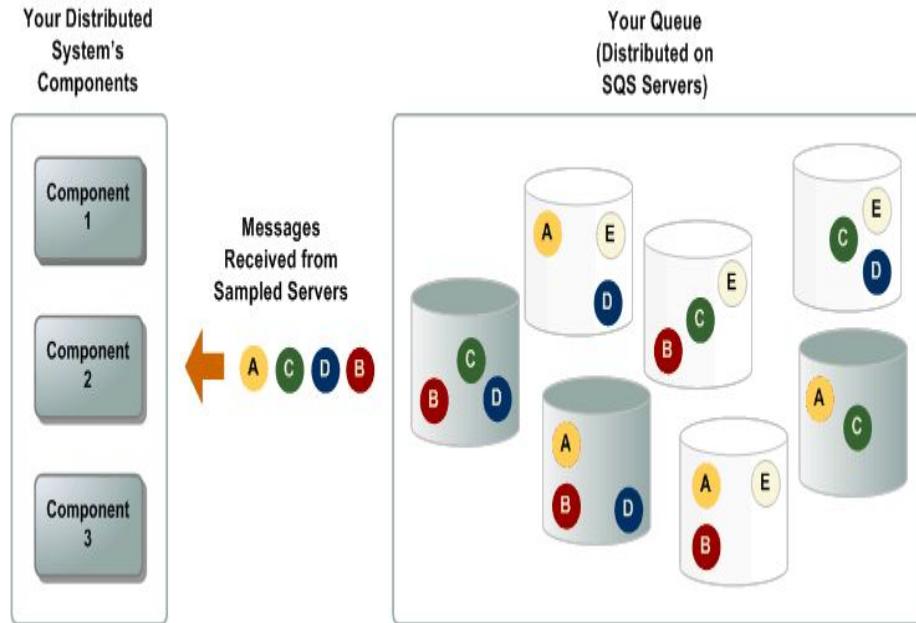


Amazon SQS Queues

- Basic Prerequisites
- Standard Queues : Amazon SQS stores copies of your messages on multiple servers for redundancy and high availability. On rare occasions, one of the servers that stores a copy of a message might be unavailable when you receive or delete a message. When you consume messages from the queue using short polling, Amazon SQS samples a subset of the servers and returns messages from just these servers.

Amazon SQS Queues

- The following figure shows the short-polling behavior of messages returned after one of your system components makes a receive request.



Amazon SQS Queues

- **FIFO (First-In-First-Out) Queues**
 - FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated.
 - The most important features of this queue type are FIFO (First-In-First-Out) delivery and exactly-once processing.
 - If multiple messages are sent in succession to a FIFO queue, each with a distinct message deduplication ID, Amazon SQS stores the messages and acknowledges the transmission.

Amazon SQS Queues

- When receiving messages from a FIFO queue with multiple message group IDs, Amazon SQS first attempts to return as many messages with the same message group ID as possible.
- FIFO queues allow the producer or consumer to attempt multiple retries.
- The Amazon SQS Buffered Asynchronous Client doesn't currently support FIFO queues.

Amazon SQS Queues

- Queue and Message Identifiers
 - Queue Name and URL
 - When you create a new queue, you must specify a queue name that is unique within the scope of all your queues.
 - Message ID
 - Each message receives a system-assigned **message ID** that Amazon SQS returns to you in the **SendMessage** response.
 - This identifier is useful for identifying messages.

Amazon SQS Queues

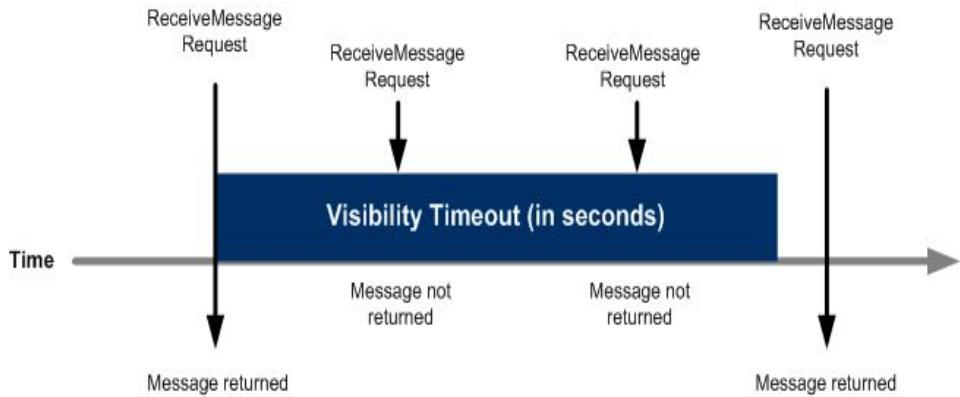
- Receipt Handle
 - Every time you receive a message from a queue, you receive a receipt handle for that message.
 - This handle is associated with the action of receiving the message, not with the message itself.
- Message Deduplication ID
 - If a message with a particular message deduplication ID is sent successfully, any messages sent with the same message deduplication ID are accepted successfully.
- Message Group ID
 - Messages that belong to the same message group are always processed one by one, in a strict order relative to the message group.

Amazon SQS Queues

- Sequence Number
 - The large, non-consecutive number that Amazon SQS assigns to each message.
- Resources Required to Process Messages
 - To help you estimate the resources you need to process queued messages, Amazon SQS can determine the approximate number of delayed, visible, and not visible messages in a queue.
- Visibility Timeout
 - To prevent other consumers from processing the message again, Amazon SQS sets a **visibility timeout**, a period of time during which Amazon SQS prevents other consuming components from receiving and processing the message.

Amazon SQS Queues

- **Inflight Messages**
 - A message is considered to be in flight after it's received from a queue by a consumer, but not yet deleted from the queue.
 - The following figure illustrates the visibility timeout.

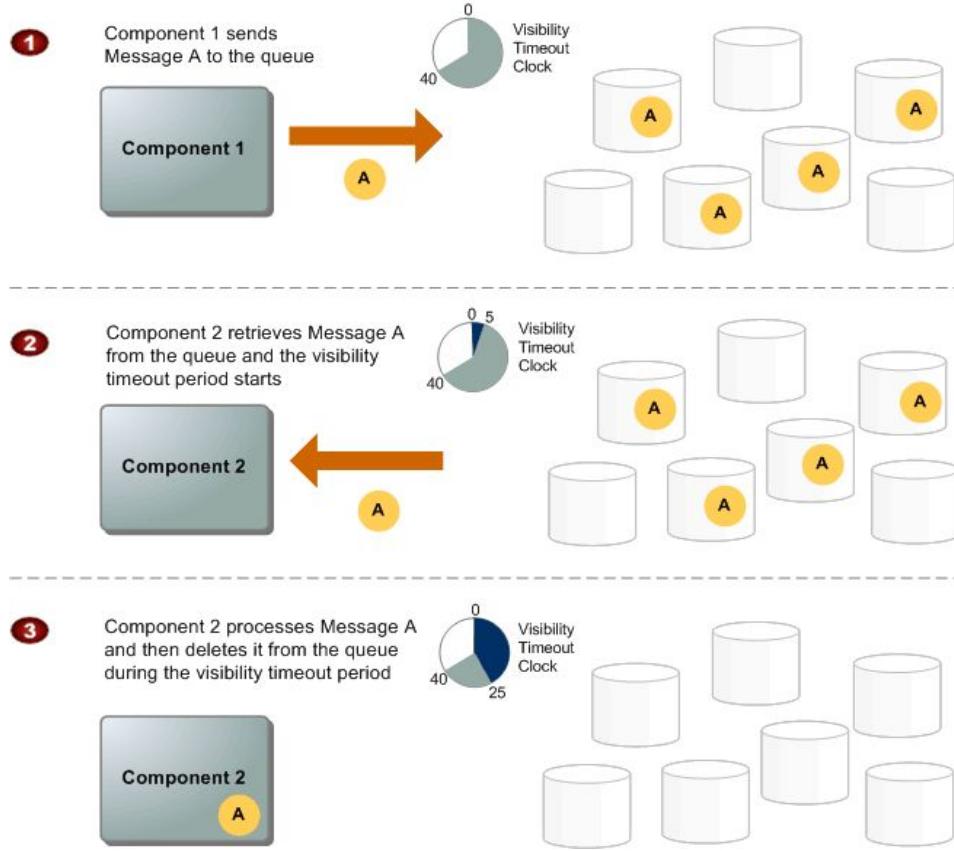


Amazon SQS Queues

- Configuring the Visibility Timeout
 - The visibility timeout clock starts ticking once Amazon SQS returns the message.
 - During that time, the component processes and deletes the message.
 - Each queue starts with a default setting of 30 seconds for the visibility timeout.
- Changing a Message's Visibility Timeout
 - You can shorten or extend a message's visibility by specifying a new timeout value using the [ChangeMessageVisibility](#) action.

Amazon SQS Queues

- Message Lifecycle
 - The following diagram describes the lifecycle of an Amazon SQS message, from creation to deletion.



Amazon SQS Queues

- Component 1 sends Message A to a queue, and the message is distributed across the Amazon SQS servers redundantly.
- When Component 2 is ready to process a message, it consumes messages from the queue, and Message A is returned.
- While Message A is being processed, it remains in the queue and isn't returned to subsequent receive requests for the duration of the visibility timeout. Component 2 deletes Message A from the queue to prevent the message from being received and processed again once the visibility timeout expires.

Amazon SQS Queues

- [Amazon SQS Dead-Letter Queues](#)
 - A dead-letter queue is a queue that other (source) queues can target for messages that can't be processed (consumed) successfully.
 - Messages that can't be processed in a timely manner are delivered to a dead-letter queue.
 - Setting up a dead-letter queue allows you to do the following:
 - Configure an alarm for any messages delivered to a dead-letter queue.
 - Examine logs for exceptions that might have caused messages to be delivered to a dead-letter queue.

Amazon SQS Queues

- Analyze the contents of messages delivered to a dead-letter queue to diagnose software or the producer's or consumer's hardware issues.
- Determine whether you have given your consumer sufficient time to process messages.
- Use of a Dead-Letter Queue
 - Dead-letter queues can help you troubleshoot incorrect message transmission operations with standard queues.
 - To decrease the number of messages and to reduce the possibility of exposing your system to poison-pill messages

Amazon SQS Queues

- Amazon SQS Message Attributes
 - Message attributes allow you to provide structured metadata items about the message.
 - Each message attribute consists of the name, type and value.
- Amazon SQS Long Polling
 - Long polling helps reduce your cost of using Amazon SQS by reducing the number of empty responses and eliminating false empty responses.
- The Differences Between Short and Long Polling
 - Amazon SQS uses short polling by default, querying only a subset of the servers to determine whether any messages are available for inclusion in the response.

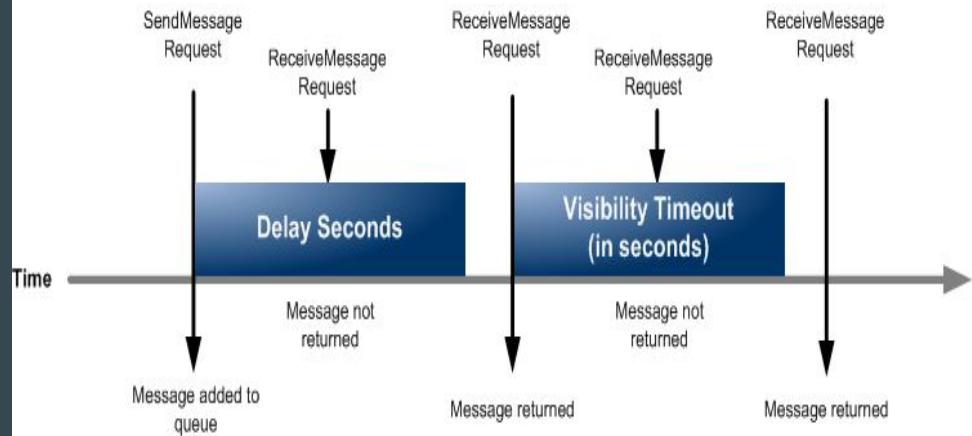
Amazon SQS Queues

- Amazon SQS Delay Queues

- Delay queues let you postpone the delivery of new messages in a queue for the specified number of seconds.
- Any message that you send to that queue is invisible to consumers for the duration of the delay period.
- Delay queues are similar to visibility timeouts because both features make messages unavailable to consumers for a specific period of time.

Amazon SQS Queues

- The following figure illustrates the relationship between delay queues and visibility timeouts.



Amazon SQS Queues

- Amazon SQS Message Timers
 - Amazon SQS message timers allow you to specify an initial invisibility period for a message that you add to a queue.
 - To set a delay period that applies to all messages in a queue, use delay queues.
 - A message timer setting for an individual message overrides any **Delay Seconds** value that applies to the entire delay queue.

Using JMS with Amazon SQS

- The Amazon SQS Java Messaging Library is a JMS interface for Amazon SQS that lets you take advantage of Amazon SQS in applications that already use JMS.
- The interface lets you use Amazon SQS as the JMS provider with minimal code changes.
- Together with the AWS SDK for Java, the Amazon SQS Java Messaging Library lets you create JMS connections and sessions, as well as producers and consumers that send and receive messages to and from Amazon SQS queues.

Monitoring Amazon SQS using CloudWatch

- Amazon SQS and Amazon CloudWatch are integrated so you can use CloudWatch to view and analyze metrics for your Amazon SQS queues.
- CloudWatch metrics for your Amazon SQS queues are automatically collected and pushed to CloudWatch every five minutes.
- These metrics are gathered on all queues that meet the CloudWatch guidelines for being active.

Authentication and Access Control

- Amazon SQS has its own resource-based permissions system that uses policies written in the same language used for AWS Identity and Access Management (IAM) policies.
- In addition to creating IAM users with their own security credentials, IAM also allows you to grant temporary security credentials to any user, allowing the user to access your AWS services and resources.

Protecting Data Using Server-Side Encryption (SSE) and AWS KMS

- SSE lets you transmit sensitive data in encrypted queues.
- SSE protects the contents of messages in Amazon SQS queues using keys managed in the AWS Key Management Service (AWS KMS).
- The messages are stored in encrypted form and Amazon SQS decrypts messages only when they are sent to an authorized consumer.

Protecting Data Using Server-Side Encryption (SSE) and AWS KMS

- Encrypting a message makes its contents unavailable to unauthorized or anonymous users.
- The **data encryption key (DEK)** is used which is responsible for encrypting the contents of Amazon SQS messages.
- The length of time, in seconds, for which Amazon SQS can reuse a data key to encrypt or decrypt messages before calling AWS KMS again is called **data key reuse period**.

Amazon SQS Compliance

- PCI DSS
 - Amazon SQS supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as compliant with [Payment Card Industry \(PCI\) Data Security Standard \(DSS\)](#).
- HIPAA
 - AWS has expanded its HIPAA compliance program to include Amazon SQS as a HIPAA Eligible Service.

Messaging



Messaging

Simple Queue Service

Simple Notification Service

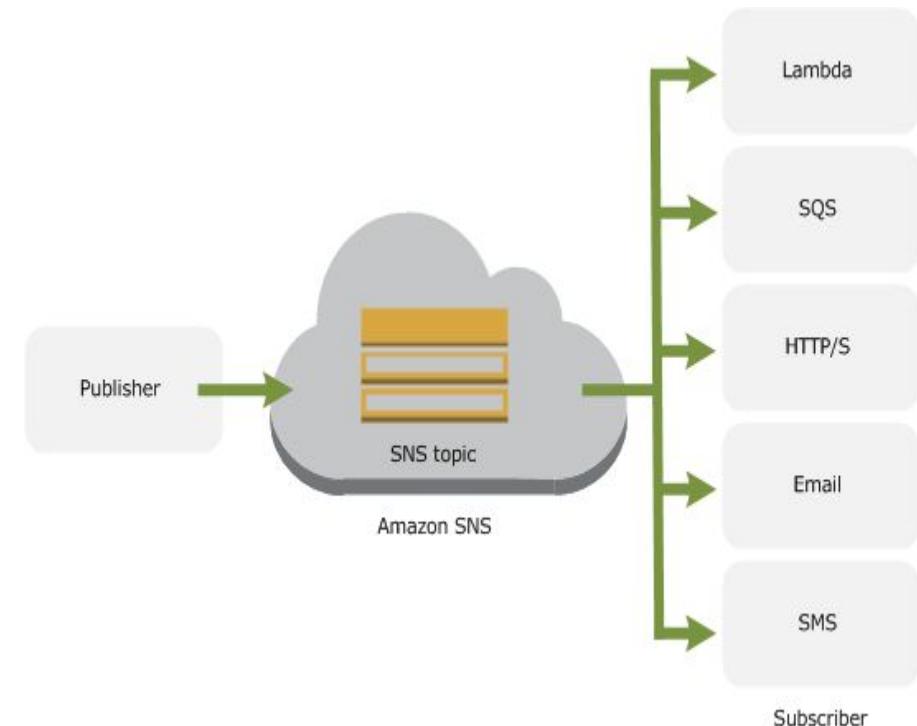
SES

Simple Notification Service

- A web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.
- You (as the owner) create a topic and control access to it by defining policies.

Amazon SNS

- In Amazon SNS, there are two types of clients—publishers and subscribers—also referred to as producers and consumers.
- Publishers communicate asynchronously with subscribers by producing and sending a message to a topic, which is a logical access point and communication channel.



Amazon SNS

- Subscribers (i.e., web servers, email addresses, Amazon SQS queues, AWS Lambda functions) consume or receive the message or notification over one of the supported protocols (i.e., Amazon SQS, HTTP/S, email, SMS, Lambda) when they are subscribed to the topic.
- A publisher sends messages to topics that they have created or to topics they have permission to publish to.
- Subscribers receive all messages published to the topics to which they subscribe, and all subscribers to a topic receive the same messages.

Key Concepts

- **Permission**
 - A permission is the concept of allowing or disallowing some kind of access to a particular resource.
- **Statement**
 - A statement is the formal description of a single permission, written in the access policy language.
- **Policy**
 - A policy is a document (written in the access policy language) that acts as a container for one or more statements.
- **Issuer**
 - The issuer is the person who writes a policy to grant permissions for a resource.

Key Concepts

- Principal
 - The principal is the person or persons who receive the permission in the policy.
- Action
 - The action is the activity the principal has permission to perform.
- Resource
 - The resource is the object the principal is requesting access to.
- Conditions and Keys
 - The conditions are any restrictions or details about the permission.
 - A key is the specific characteristic that is the basis for access restriction.

Key Concepts

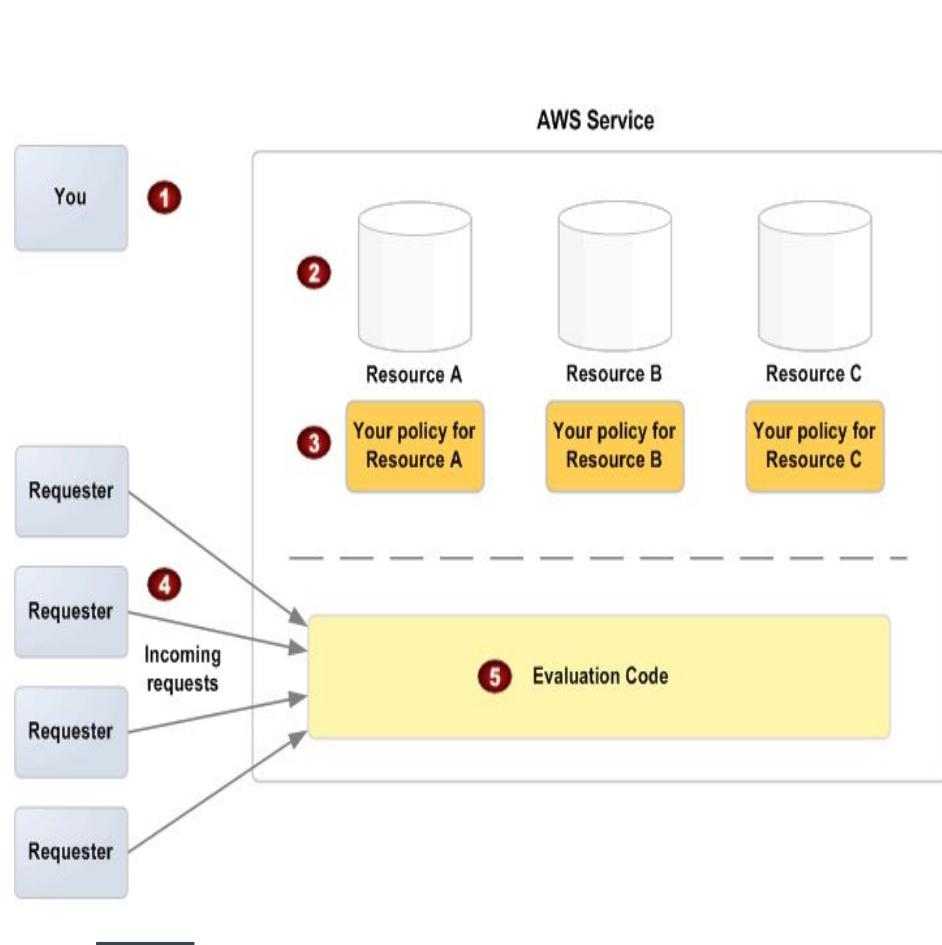
- Requester
 - The requester is the person who sends a request to an AWS service and asks for access to a particular resource.
- Evaluation
 - Evaluation is the process the AWS service uses to determine if an incoming request should be denied or allowed based on the applicable policies.
- Effect
 - The effect is the result that you want a policy statement to return at evaluation time.

Key Concepts

- Default Deny
 - A default deny is the default result from a policy in the absence of an allow or explicit deny.
- Allow
 - An allow results from a statement that has effect=allow, assuming any stated conditions are met.
- Explicit Deny
 - An explicit deny results from a statement that has effect=deny, assuming any stated conditions are met.

Architectural Overview

- The following figure shows the main components that interact to provide access control for your resources.

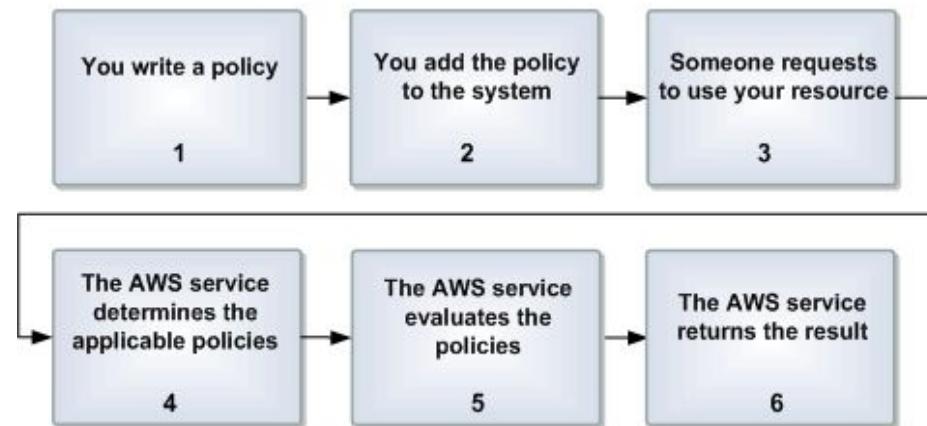


Architectural Overview

- 1 You, the resource owner.
- 2 Your resources
- 3 Your policies.
- 4 Requesters and their incoming requests to the AWS service.
- 5 The access policy language evaluation code.

Using the Access Policy Language

- The following figure shows the general process of how access control works with the access policy language.

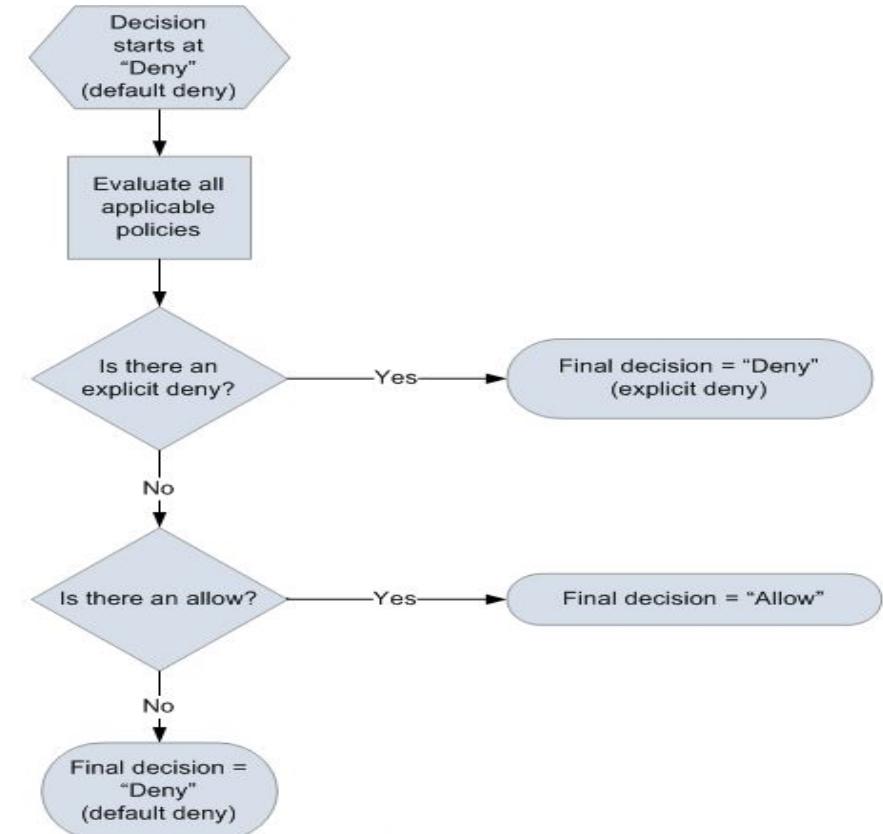


Architectural Overview

- 1 You write a policy for your resource.
- 2 You upload your policy to AWS.
- 3 Someone sends a request to use your resource.
- 4 The AWS service determines which policies are applicable to the request.
- 5 The AWS service evaluates the policies.
- 6 The AWS service either denies the request or continues to process it.

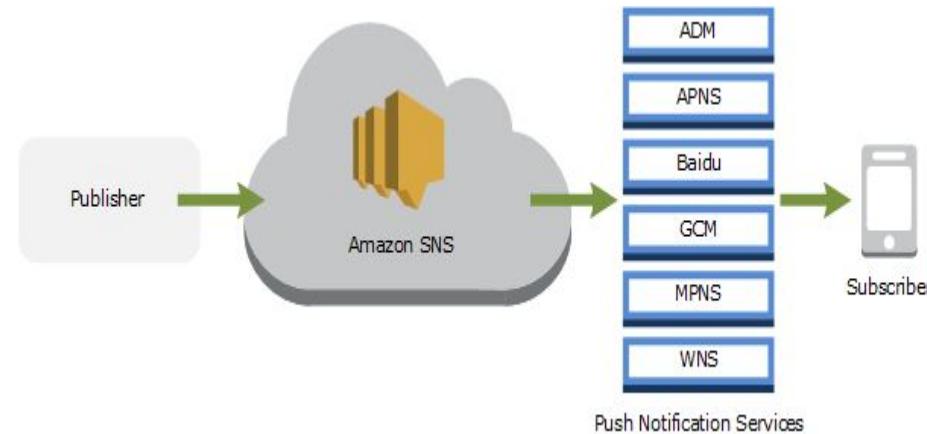
Evaluation Logic

- The evaluation logic follows several basic rules:
 - By default, all requests to use your resource coming from anyone but you are denied
 - An allow overrides any default denies
 - An explicit deny overrides any allows
 - The order in which the policies are evaluated is not important.



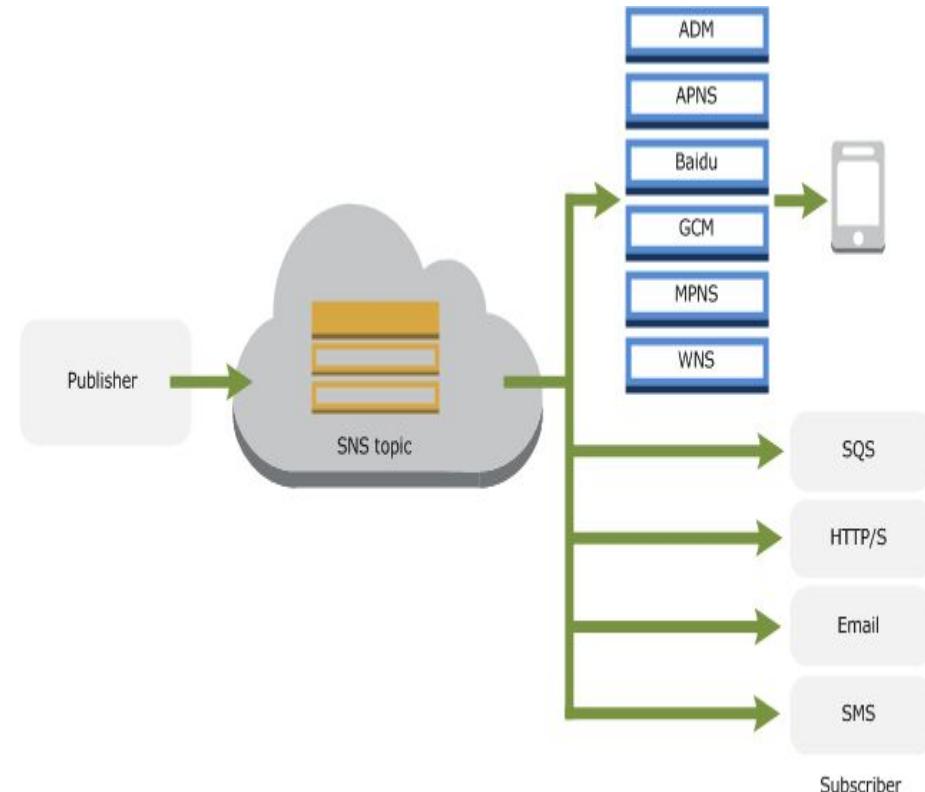
Amazon SNS Mobile Push

- You send push notification messages to both mobile devices and desktops.
- The following figure shows an overview of how Amazon SNS is used to send a direct push notification message to a mobile endpoint.



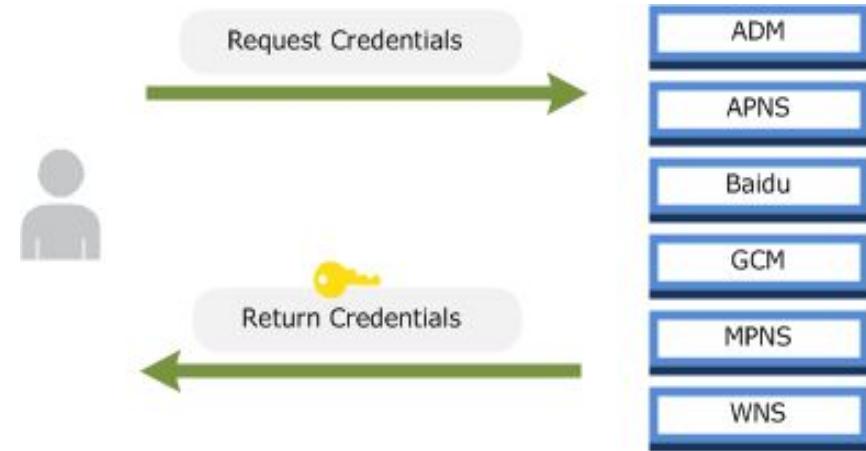
Amazon SNS Mobile Push

- The following figure shows a mobile endpoint as a subscriber to an Amazon SNS topic.
- The mobile endpoint communicates using push notification services where the other endpoints do not.



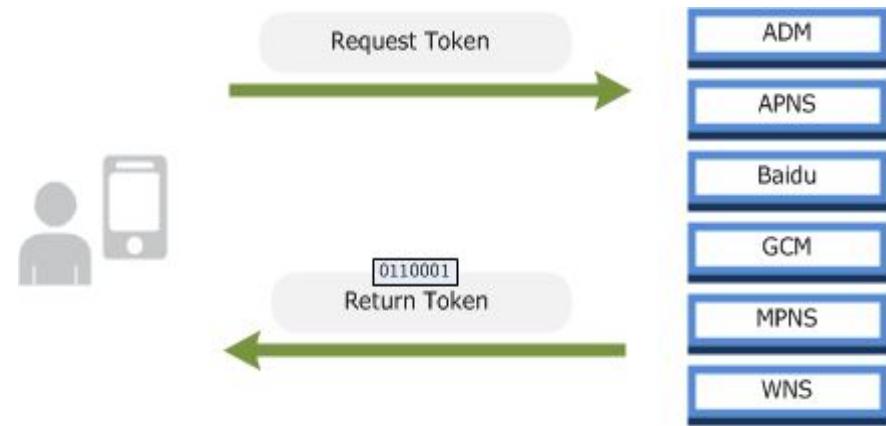
Amazon SNS Mobile Push

- Amazon SNS Mobile Push High-Level Steps
 - Step 1: Request Credentials from Mobile Platforms



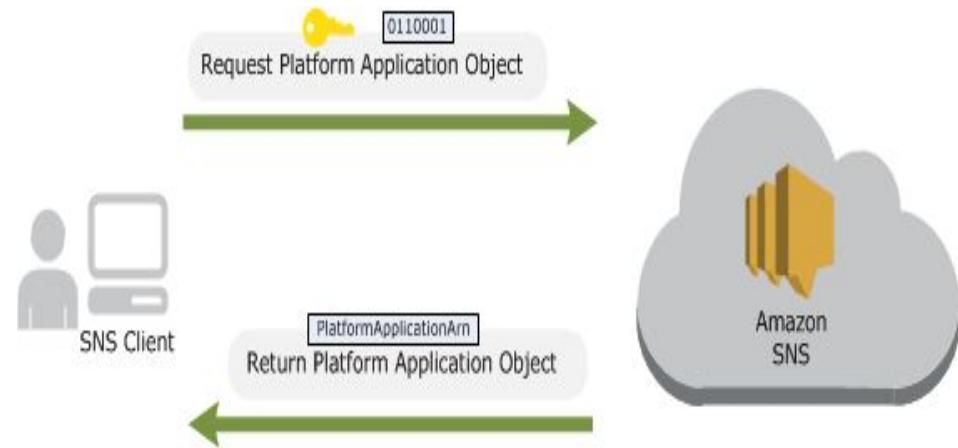
Amazon SNS Mobile Push

- Step 2: Request Token from Mobile Platforms



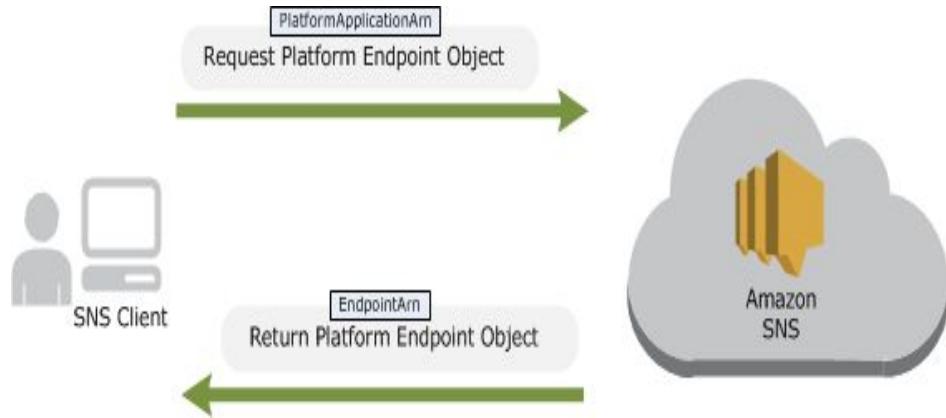
Amazon SNS Mobile Push

- Step 3: Create Platform Application Object



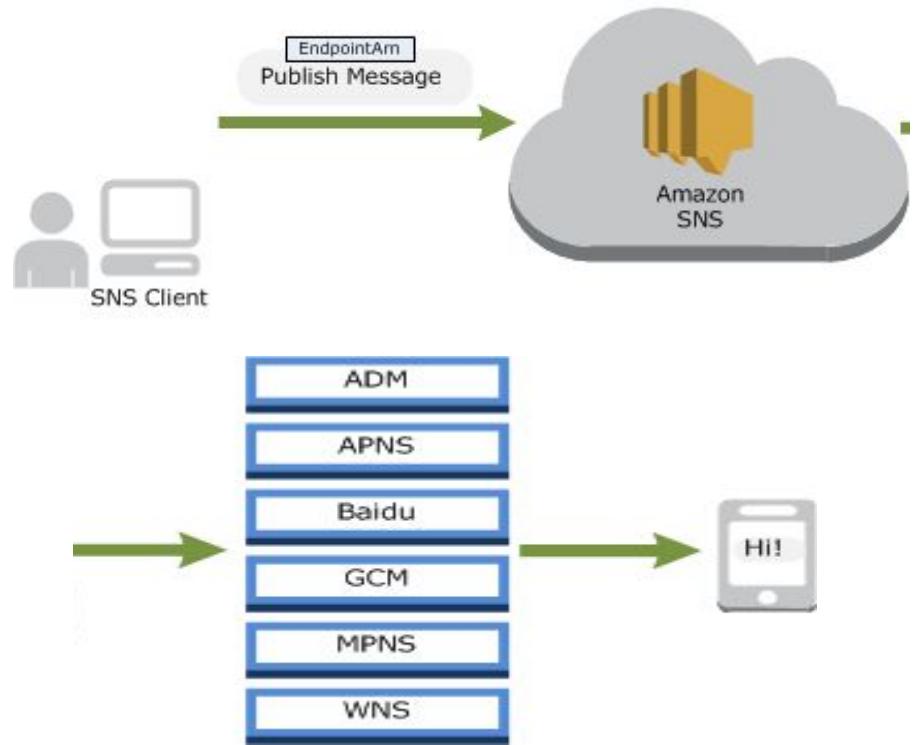
Amazon SNS Mobile Push

- Step 4: Create Platform Endpoint Object



Amazon SNS Mobile Push

- Step 5: Publish Message to Mobile Endpoint



Sending Amazon SNS Messages to Amazon SQS Queues

- Amazon SNS works closely with Amazon Simple Queue Service.
- Amazon SNS allows applications to send time-critical messages to multiple subscribers through a “push” mechanism, eliminating the need to periodically check or “poll” for updates.
- Amazon SQS is a message queue service used by distributed applications to exchange messages through a polling model, and can be used to decouple sending and receiving components—without requiring each component to be concurrently available.

Sending SMS Messages with Amazon SNS

- You can use Amazon SNS to send text messages, or SMS messages, to SMS-enabled devices.
- You can send a message directly to a phone number, or you can send a message to multiple phone numbers at once by subscribing those phone numbers to a topic and sending your message to the topic.
- You can set SMS preferences for your AWS account to tailor your SMS deliveries for your use cases and budget.

Sending SMS Messages with Amazon SNS

- Monitoring SMS Activity
 - By monitoring your SMS activity, you can keep track of destination phone numbers, successful or failed deliveries, reasons for failure, costs, and other information.
- Managing Phone Numbers and SMS Subscriptions
 - Amazon SNS provides several options for managing who receives SMS messages from your account.
 - With a limited frequency, you can opt in phone numbers that have opted out of receiving SMS messages from your account.

Sending SMS Messages with Amazon SNS

- Reserving a Dedicated Short Code for SMS Messaging
 - To send SMS messages using a persistent short code, you can reserve a dedicated short code that is assigned to your account and available exclusively to you.
 - A short code is a 5 or 6 digit number that you can use to send SMS messages to certain destinations.
 - Short codes are often used for application-to-person (A2P) messaging, two-factor authentication (2FA), and marketing.

Sending Amazon SNS Messages to HTTP/HTTPS Endpoints

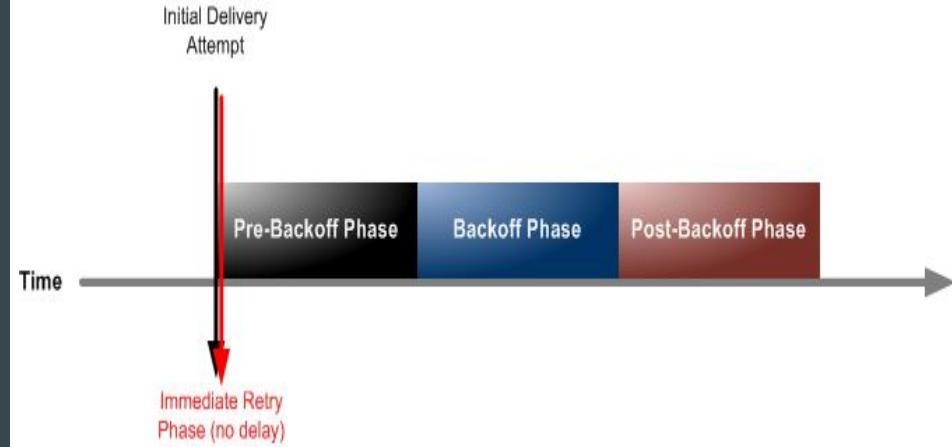
- You can use Amazon SNS to send notification messages to one or more HTTP or HTTPS endpoints.
- If you use HTTPS, then you can take advantage of the support in Amazon SNS for Server Name Indication (SNI) and Basic and Digest Access Authentication.

Sending Amazon SNS Messages to HTTP/HTTPS Endpoints

- Setting Amazon SNS Delivery Retry Policies for HTTP/HTTPS Endpoints
 - A successful Amazon SNS delivery to an HTTP/HTTPS endpoint sometimes requires more than one attempt.
 - If an initial delivery attempt doesn't result in a successful response from the subscriber, Amazon SNS attempts to deliver the message again.

Sending Amazon SNS Messages to HTTP/HTTPS Endpoints

- You can use delivery policies to control not only the total number of retries, but also the time delay between each retry.
- The maximum lifetime of a message in the system is one hour.
- This one hour limit cannot be extended by a delivery policy.

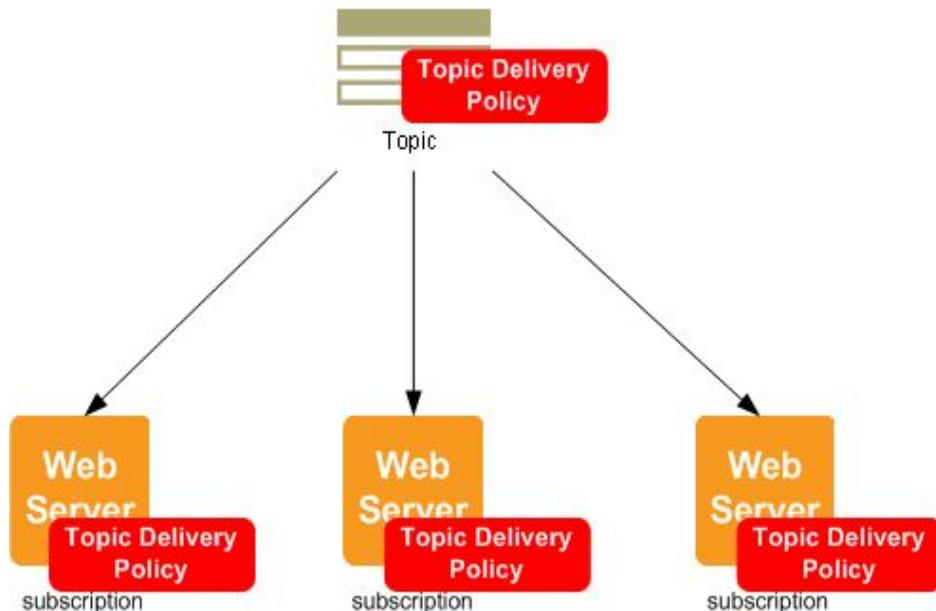


Sending Amazon SNS Messages to HTTP/HTTPS Endpoints

- Immediate Retry Phase
- Pre-Backoff Phase
- Backoff Phase
- Post-Backoff Phase

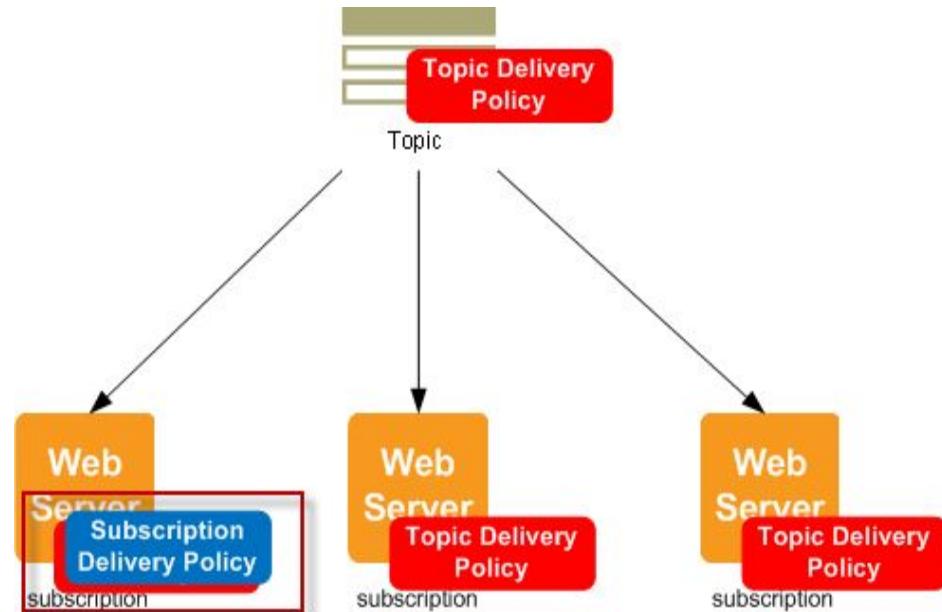
Applying Delivery Policies to Topics and Subscriptions

- The following diagram illustrates a topic with a delivery policy that applies to all three subscriptions associated with that topic.



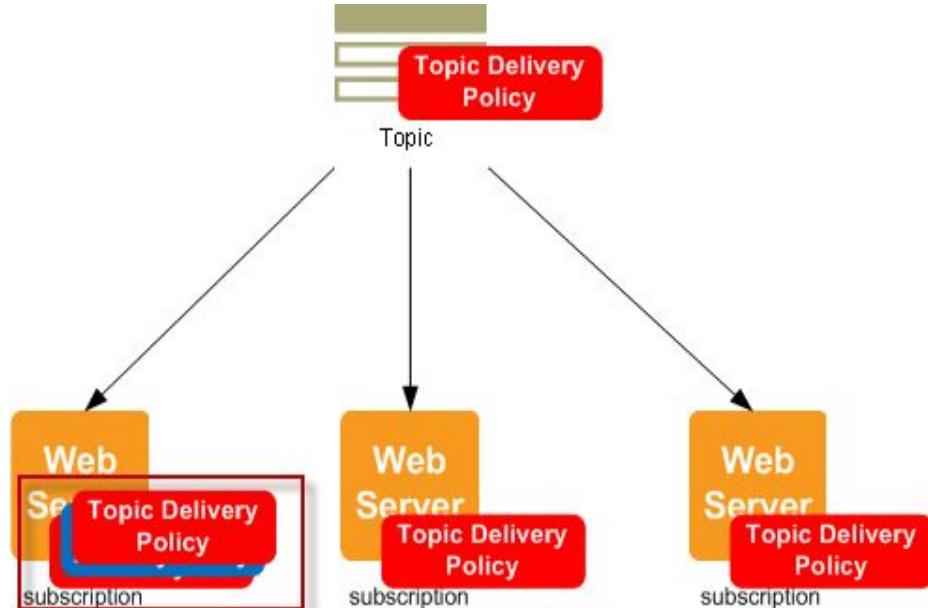
Applying Delivery Policies to Topics and Subscriptions

- In the following diagram, one subscription has a subscription-level delivery policy whereas the two other subscriptions do not.



Applying Delivery Policies to Topics and Subscriptions

- The following diagram shows a topic-level delivery policy that applies to all subscriptions, even the subscription that has its own subscription delivery policy because subscription-level policies have been specifically ignored.



Invoking Lambda functions

- Amazon SNS and AWS Lambda are integrated so you can invoke Lambda functions with Amazon SNS notifications.
- When a message is published to an SNS topic that has a Lambda function subscribed to it, the Lambda function is invoked with the payload of the published message.

Using Amazon SNS Message Attributes

- Amazon SNS provides support for delivery of message attributes to Amazon SQS endpoints.
- Message attributes allow you to provide structured metadata items about the message.
- You can also use message attributes to help structure the push notification message for mobile endpoints.
- Each message attribute consists of name, type and value.

Monitoring Amazon SNS with CloudWatch

- Amazon SNS and CloudWatch are integrated so you can collect, view, and analyze metrics for every active Amazon SNS notifications.
- Once you have configured CloudWatch for Amazon SNS, you can gain better insight into the performance of your Amazon SNS topics, push notifications, and SMS deliveries.

Logging Amazon Simple Notification Service API Calls By Using AWS CloudTrail

- Amazon SNS is integrated with CloudTrail, a service that captures API calls made by or on behalf of Amazon SNS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify.
- Using the information collected by CloudTrail, you can determine what request was made to Amazon SNS, the source IP address from which the request was made, who made the request, when it was made, and so on.

Logging Amazon Simple Notification Service API Calls By Using AWS CloudTrail

- When CloudTrail logging is enabled in your AWS account, API calls made to Amazon SNS actions are tracked in log files.
- Amazon SNS records are written together with other AWS service records in a log file.
- CloudTrail determines when to create and write to a new file based on a time period and file size.

Messaging



Messaging

Simple Queue Service

Simple Notification Service

SES

Simple Email Service-

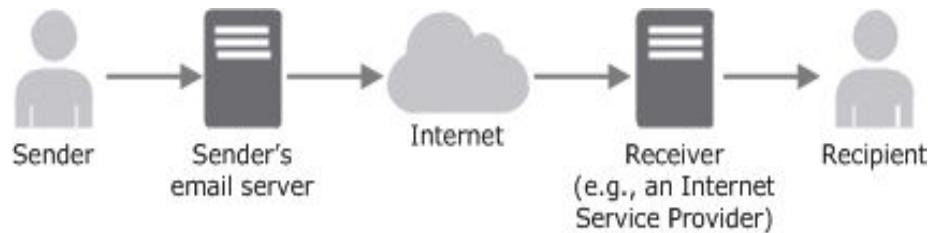
- enables you to benefit from the years of experience and sophisticated email infrastructure.
- Amazon.com has built to serve its own large-scale customer base.

Sending Email with Amazon SES

- When you send an email, you are sending it through some type of outbound email server.
- That email server might be provided by your Internet service provider (ISP), your company's IT department, or you might have set it up yourself.
- The email server accepts your email content, formats it to comply with email standards, and then sends the email out over the Internet.
- The email may pass through other servers until it eventually reaches a receiver

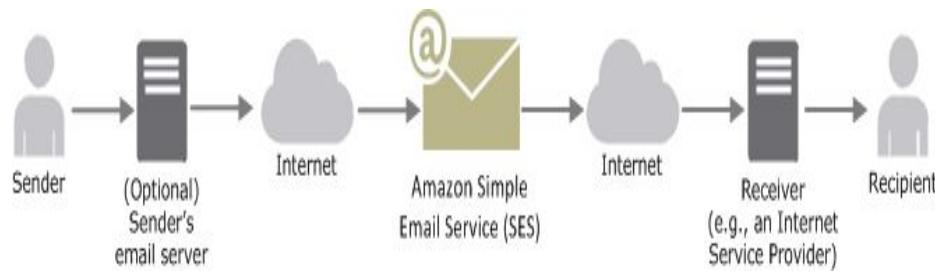
Sending Email with Amazon SES

- The receiver then delivers the email to the recipient.
- The following diagram illustrates the basic email-sending process.



Sending Email with Amazon SES

- The following diagram shows where Amazon SES fits into the email sending process.



Amazon SES and Deliverability

- You want your recipients to read your emails, find them valuable, and not label them as spam.
- In other words, you want to maximize email deliverability—the percentage of your emails that arrive in your recipients' inboxes.
- To maximize email deliverability, you need to understand email delivery issues, proactively take steps to prevent them, stay informed of the status of the emails that you send, and then improve your email-sending program, if necessary, to further increase the likelihood of successful deliveries.

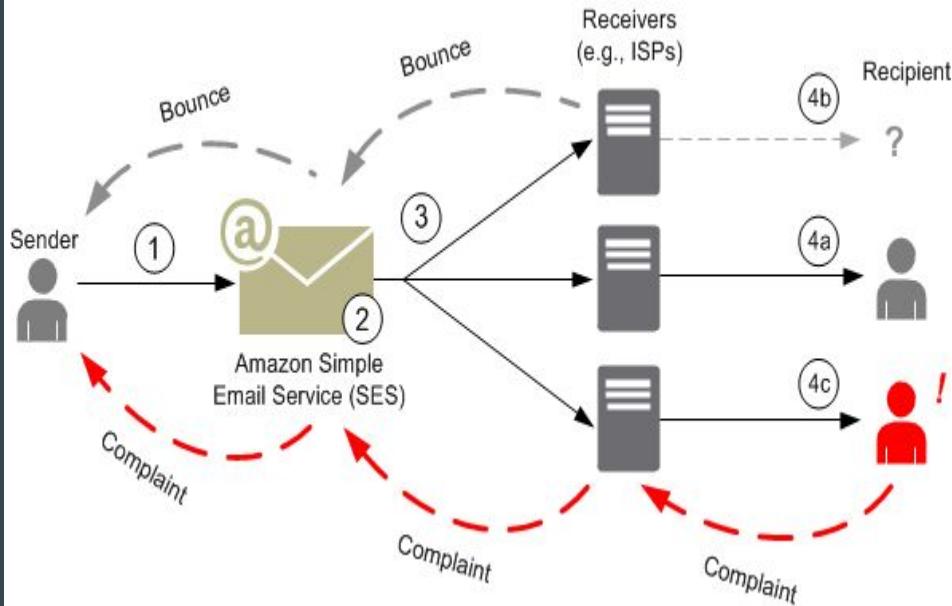
Sending Email with Amazon SES

- The following sections review the concepts behind these steps and how Amazon SES helps you through the process.



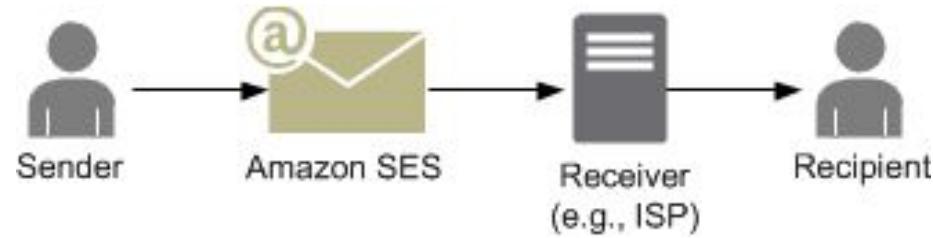
Sending Email with Amazon SES

- Amazon SES Email-Sending Process
 - The following figure is a high-level overview of the sending process.



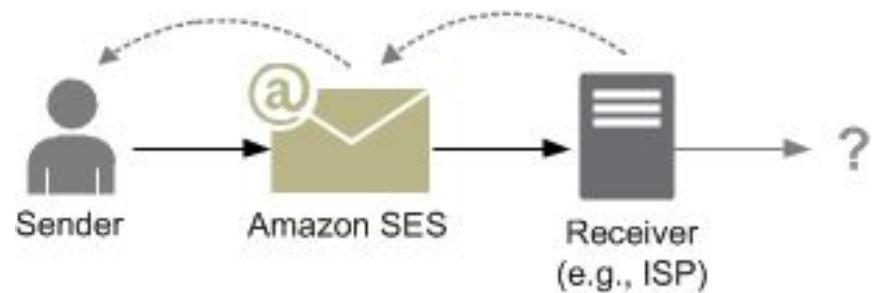
Sending Email with Amazon SES

- If the sender's request to Amazon SES succeeds, then Amazon SES sends the email and one of the following outcomes occurs:
 - Successful delivery and the recipient does not object to the email



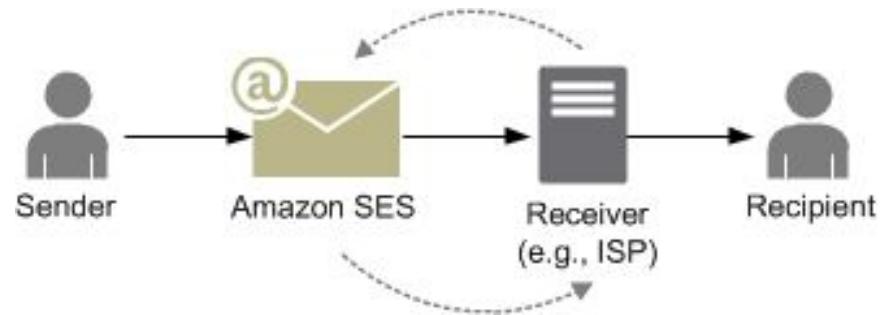
Sending Email with Amazon SES

- Hard bounce



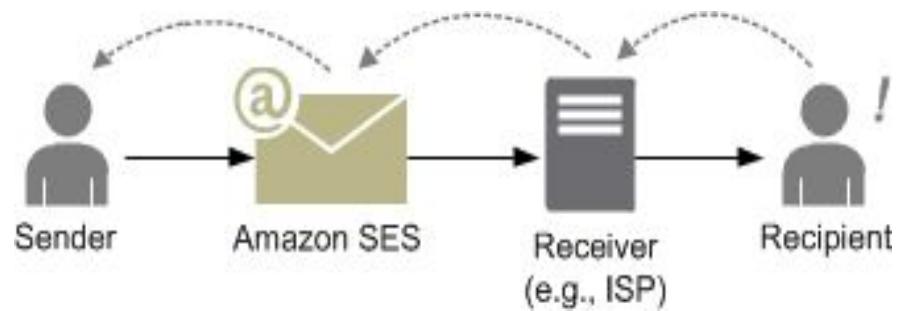
Sending Email with Amazon SES

- Soft bounce



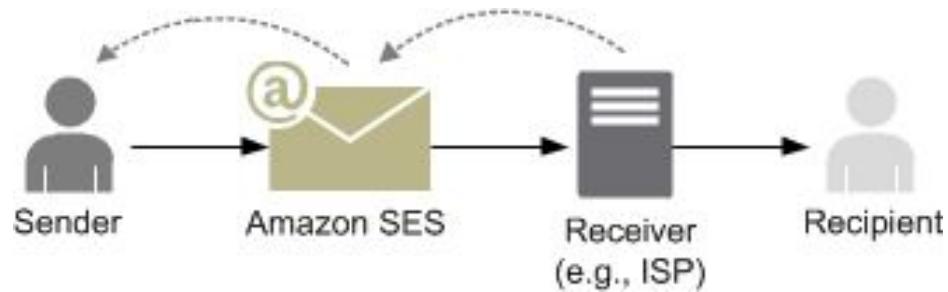
Sending Email with Amazon SES

- Complaint



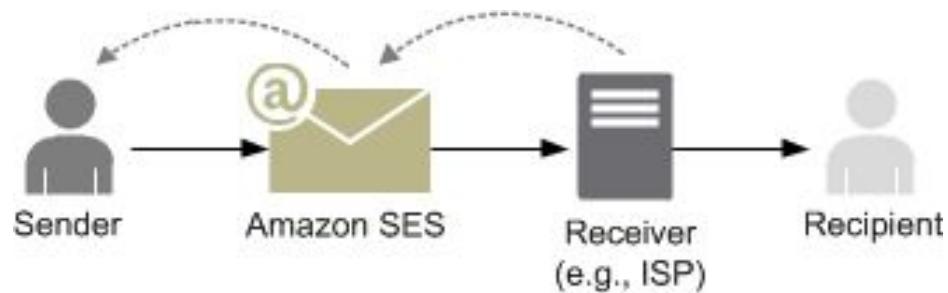
Sending Email with Amazon SES

- Auto response



Sending Email with Amazon SES

- Auto response



Email Format and Amazon SES

- An email consists of a header, a body, and an envelope.
- There is one header per email message.
- When you read an email in an email client, the email client typically displays the values of the following header fields:
 - To—The email addresses of the message's recipients.
 - CC—The email addresses of the message's carbon copy recipients.
 - From—The email address from which the email is sent.
 - Subject—A summary of the message topic.
 - Date—The time and date the email is sent.
- The email body contains the text of the message. The body can be sent in HTML, plain text, or both HTML and plain text formats.

Setting up Email with Amazon SES

- To set up email with Amazon SES, you need to perform the following tasks:
 - Before you can access Amazon SES or other AWS services, you need to set up an AWS account.
 - Before you send email through Amazon SES, you need to verify that you own the "From" address.
 - If your account is still in the Amazon SES sandbox, you also need to verify your "To" addresses.

Using a Custom MAIL FROM Domain with Amazon SES

- When an email is sent, it has two addresses that indicate its source:
 - A "From" address provided by the email header.
 - A MAIL FROM address that the sending mail server specifies to the receiving mail server to indicate the source of the message.
- By default, messages that you send through Amazon SES use amazonses.com as the MAIL FROM domain.
- Sender Policy Framework (SPF) authentication successfully validates these messages because the default MAIL FROM domain matches the sending mail server, Amazon SES.
- You might want to set the MAIL FROM domain to a domain that you own to enable your emails to authenticate with [Domain-based Message Authentication](#).

Using a Custom MAIL FROM Domain with Amazon SES

- There are two ways to achieve DMARC validation:
 - Using SPF
 - Using DKIM
- Setting up SPF Records for Amazon SES
 - When you use Amazon SES, your decision about whether to publish an SPF record depends on whether you only require your email to pass an SPF check by the receiving mail server, or if you want your email to comply with the additional requirements needed to pass DMARC authentication based on SPF.

Using a Custom MAIL FROM Domain with Amazon SES

- Moving Out of the Amazon SES Sandbox
 - To help protect our customers from fraud and abuse and to help you establish your trustworthiness to ISPs and email recipients, we do not immediately grant unlimited Amazon SES usage to new users.
 - New users are initially placed in the Amazon SES sandbox.
 - In the sandbox, you have full access to all Amazon SES email-sending methods and features so that you can test and evaluate the service.

Authenticating Your Email in Amazon SES

- Amazon SES uses the Simple Mail Transfer Protocol (SMTP) to send email.
- Because SMTP does not provide any authentication by itself, spammers can send email messages that claim to originate from someone else, while hiding their true origin.
- Most ISPs that forward email traffic take measures to evaluate whether email is legitimate.
- One such measure that ISPs take is to determine whether an email is authenticated.
- Authentication requires senders to verify that they are the owner of the account that they are sending from.

Complying with DMARC Using Amazon SES

- DMARC is an email authentication protocol that uses Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to detect email spoofing.
- An email can comply with DMARC through SPF or through DKIM.
- For maximum deliverability, it is a best practice to set up your email-sending to comply with both methods.

Managing Your Amazon SES Sending Limits

- Amazon SES account has a set of sending limits to regulate the number of email messages that you can send and the rate at which you can send them.
- Sending limits benefit all Amazon SES customers because they help to maintain the trusted relationship between Amazon SES and ISPs.
- Sending limits help you to gradually ramp up your sending activity and decrease the likelihood that ISPs will block your emails because of sudden, unexpected spikes in your email sending volume or rate.

Sending Authorization

- Amazon SES enables you to authorize other users to send emails from your identities on your behalf.
- This feature, called [sending authorization](#).
- It lets you to maintain control over your identities so that you can change or revoke the permissions at any time.
- If you want to authorize someone to send emails on your behalf, then you are an [identity owner](#).
- If you have been authorized to send emails on behalf of someone else, then you are a [delegate sender](#).

Identity Owner Tasks

- Verifying an Identity for Amazon SES Sending Authorization
- Setting Up Identity Owner Notifications for Amazon SES Sending Authorization
- Getting Information from the Delegate Sender for Amazon SES Sending Authorization
- Creating a Policy for Amazon SES Sending Authorization
- Providing the Delegate Sender with the Identity Information for Amazon SES Sending Authorization
- Managing Your Policies for Amazon SES Sending Authorization

Delegate Sender Tasks

- Providing Information to the Identity Owner for Amazon SES Sending Authorization
- Using Delegate Sender Notifications for Amazon SES Sending Authorization
- Sending Emails for the Identity Owner for Amazon SES Sending Authorization

Using Dedicated IP Addresses with SES

- SES sends your email from IP addresses (IPs) that you share with other Amazon SES customers.
- When you choose whether to use dedicated IPs, shared IPs, or a mix, consider the following trade-offs.
 - Cost
 - Email Volume
 - Sending Pattern
 - Reputation Isolation
 - Knowledge of the IP Addresses
 - Engaging Amazon SES

Using Dedicated IP Addresses with SES

- How to Warm up Dedicated IPs
 - When determining whether to accept or reject an email, ISPs consider the reputation of the IP that sent it.
 - One of the factors that contributes to the reputation of an IP is whether the IP has a considerable history of sending high-quality emails.
 - You should therefore gradually increase your sending through a new dedicated IP before you use it to its full capacity.
 - This process is called warming up the IP.

Testing Amazon SES Email Sending

- Amazon SES provides a mailbox simulator that you can use to test how your application handles various email sending scenarios without affecting your sending quota or your bounce and complaint metrics.
- Each email address represents a specific scenario.
- The mailbox simulator provides typical bounce, complaint, and OOTO responses. In the bounce scenario, multiple bounces from the same sending request are gathered into a single response.

Amazon SES and Security Protocols

- The security protocol that you use to connect to Amazon SES depends on whether you are using the Amazon SES API or the Amazon SES SMTP interface.
- If you are using the Amazon SES API, then all communications are encrypted by TLS through the Amazon SES HTTPS endpoint.
- If you are accessing Amazon SES through the SMTP interface, you are required to encrypt your connection using **Transport Layer Security (TLS)**.
- Amazon SES supports two mechanisms for establishing a TLS-encrypted connection: **STARTTLS** and **TLS Wrapper**.
- The method of sending messages over a TLS-protected connection is called **opportunistic TLS**.

Receiving Email with Amazon SES

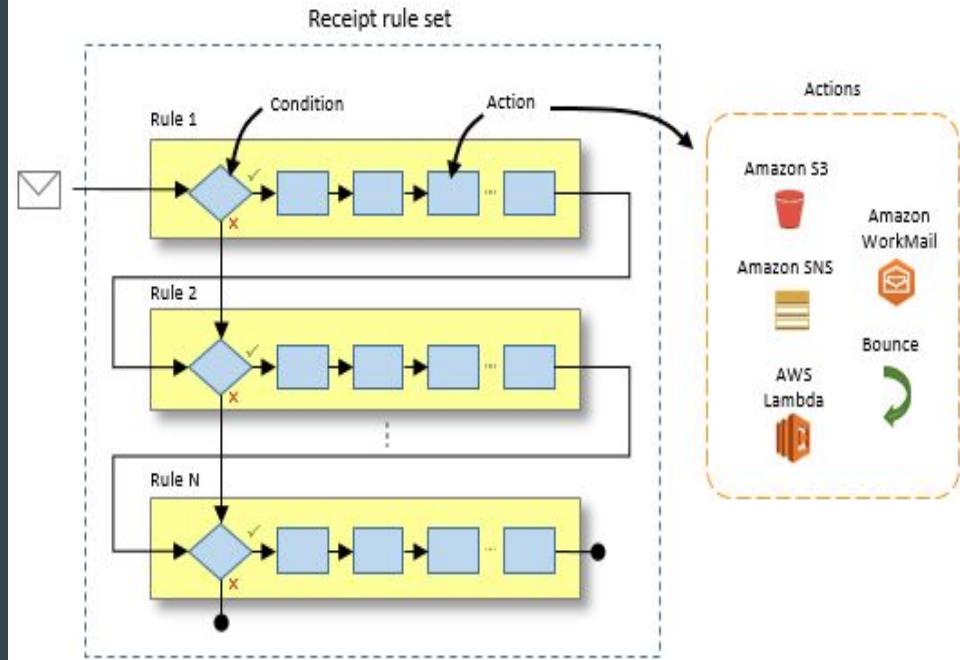
- Amazon SES is a mail server that can both send and receive mail on behalf of your domain.
- When you use Amazon SES to receive your mail, Amazon SES handles underlying mail-receiving operations, such as:
 - communicating with other mail servers
 - scanning for spam and viruses
 - rejecting mail from untrusted sources
 - accepting mail for recipients in your domain

Receiving Email with Amazon SES

- Amazon SES Email-Receiving Concepts
 - Recipient-Based Control
 - The primary way to control your incoming mail is to specify how mail is handled based on its recipient.
 - You set up **receipt rules** to specify how to handle the mail when a condition is satisfied, which consists of a condition and an ordered list of actions.
 - The actions available are S3, SNS, lambda, bounce, stop, add header, work mail action.

Receiving Email with Amazon SES

- Receipt rules are grouped together into **receipt rule sets**.
- The following figure shows how receipt rules, receipt rule sets, and actions relate to each other.



Receiving Email with Amazon SES

- IP Address-Based Control
 - You can control your mail flow on a broader level by setting up [IP address filters](#).
 - Your IP address filters can include [block lists](#) and [allow lists](#).
 - These filters are useful for blocking spam.
- Email-Receiving Process
 - Amazon SES first looks at the IP address of the sender.
 - Examines your active receipt rule set.
 - Amazon SES rejects the mail if there aren't any matches.
Otherwise, accepts the mail.
 - After accepting the mail, SES evaluates your active receipt rule set.

Controlling Access to Amazon SES

- You can use IAM with Amazon SES to specify which Amazon SES API actions an IAM user, group, or role can perform.
- You can also control which email addresses the user can use for the "From", recipient, and "Return-Path" addresses of emails.
- To use IAM, you define an IAM policy, which is a document that explicitly defines permissions, and attach the policy to a user.
- There are three reasons you might use IAM with Amazon SES:
 - To restrict the email-sending action.
 - To restrict the "From", recipient, and "Return-Path" addresses of the emails that the user sends.
 - To control general aspects of API usage.

Logging Amazon SES API Calls By Using AWS CloudTrail

- Amazon SES is integrated with CloudTrail, a service that
 - Captures API calls made by or on behalf of Amazon SES in your AWS account.
 - Delivers the log files to an Amazon S3 bucket that you specify.
- When CloudTrail logging is enabled in your AWS account, API calls made to a subset of Amazon SES actions are tracked in log files.
- Amazon SES records are written together with other AWS service records in a log file.
- CloudTrail determines when to create and write to a new file based on a time period and file size.

Regions and Amazon SES

- When you use Amazon SES, you connect to a URL that provides an endpoint for the Amazon SES API or SMTP interface.
- Amazon SES has endpoints in multiple AWS regions.
- To reduce network latency, it's a good idea to choose an endpoint closest to your application.

Regions and Amazon SES

- Email sending end points

Region Name	API (HTTPS) endpoints	SMTP endpoint
US East (N. Virginia)	email.us-east-1.amazonaws.com	email-smtp.us-east-1.amazonaws.com
US West (Oregon)	email.us-west-2.amazonaws.com	email-smtp.us-west-2.amazonaws.com
EU (Ireland)	email.eu-west-1.amazonaws.com	email-smtp.eu-west-1.amazonaws.com

Regions and Amazon SES

- Email receiving end points

Region Name	API (HTTPS) endpoints
US East (N. Virginia)	inbound-smtp.us-east-1.amazonaws.com
US West (Oregon)	inbound-smtp.us-west-2.amazonaws.com
EU (Ireland)	inbound-smtp.eu-west-1.amazonaws.com

Regions and Amazon SES

- Before you send email using Amazon SES, you must verify that you own your email address or domain with Amazon SES.
- Verification status for each region is separate.
- You must perform the [Easy DKIM](#) setup procedure for each region in which you want to use [Easy DKIM](#).
- Although each region has a separate suppression list, if you remove an address from the suppression list of one region, the address is removed from the suppression list of all regions.

Regions and Amazon SES

- You can use the same set of SMTP credentials in all regions.
- You can use the same custom MAIL FROM domain for verified identities in different AWS regions.
- The delegate sender must send the emails from the AWS region in which the identity owner's identity is verified.
- When you receive email with Amazon SES, all of the resources that you use must be in the same region as the Amazon SES endpoint.

Metrics That Define Your Success

- Bounce Rate
 - A **bounce** occurs when an email cannot be delivered to the intended recipient.
 - There are two types of bounces: **hard bounces** and **soft bounces**.
- Complaints
 - A **complaint** occurs when an email recipient clicks the "Mark as Spam" button in their web-based email client.
 - If you accumulate a large number of these complaints, the ISP assumes that you are sending spam.
 - This has a negative impact on your deliverability rate and sender reputation.
 - Some ISPs will notify you when a complaint is reported; is called a **feedback loop**.

Metrics That Define Your Success

- Message Quality
 - Email receivers use content filters to detect certain attributes in your messages to identify whether your message is legitimate.
 - These content filters automatically review the content of your messages to identify common traits of unwanted or malicious messages.
 - Amazon SES uses content filtering technologies to help detect and block messages that contain malware before they are sent.

Amazon Pinpoint

- Amazon Pinpoint is an AWS service that you can use to improve user engagement.
- Use Amazon Pinpoint to create campaigns that reach audience segments with tailored messages.
- It supports multiple messaging channels.
- With Amazon Pinpoint, you can do the following:
 - Define audience segments
 - Engage your audience with messaging campaigns
 - Analyze user behavior

Amazon Pinpoint Segments

- A user segment represents a subset of your audience based on shared characteristics, such as how recently the users have used your application or which device platform they use.
- A segment designates who receives the messages delivered by a campaign.
- You can add segments to Amazon Pinpoint in either of the following ways:
 - Building segments by choosing selection criteria that is based on data that your application reports to Amazon Pinpoint.
 - Importing segments that you defined outside of Amazon Pinpoint.

Amazon Pinpoint Campaigns

- A campaign is a messaging initiative that engages a specific audience segment.
- It sends tailored messages according to a schedule that you define.
- Your campaign can send a message to all users in a segment, or you can allocate a holdout, which is a percentage of users who receive no messages.
- The segment can be one that you created on the [Segments](#) page or one that you define while you create the campaign.
- You can set the campaign's schedule to send the message once or at a recurring frequency.

Direct Messages with Amazon Pinpoint

- With Amazon Pinpoint, you can send a **direct message**, which is a one time message that you send to a limited audience without creating a campaign.
- Sending a direct message is useful if, before creating a campaign, you want to test how your message appears to recipients.
- You can send the message to up to 15 recipients.
- Amazon Pinpoint delivers a message immediately, and you cannot schedule the delivery.
- To engage a user segment, and to schedule the message delivery, **create a campaign** instead of sending a direct message.



Desktop & App Streaming

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Desktop & App Streaming



Desktop & App Streaming

WorkSpaces

AppStream 2.0

- AWS offers two managed end user computing services running on the AWS cloud - Amazon WorkSpaces and Amazon AppStream 2.0.
- With these services, you can move your desktops and applications to AWS, and get enhanced security, low cost pay-as-you-go pricing, on-demand scaling, and global availability.

Desktop & App Streaming



Desktop & App Streaming

WorkSpaces

AppStream 2.0

- Enables you to provision cloud-based virtual desktops for your users, known as WorkSpaces.
- Eliminates the need to procure and deploy hardware or install complex software.

Amazon WorkSpaces

- Features
 - Select from a range of hardware configurations, software configurations, and AWS regions.
 - Connect to your WorkSpace and pick up from right where you left off.
 - Amazon WorkSpaces provides the flexibility of either monthly or hourly billing for WorkSpaces.
 - Deploy and manage applications for your WorkSpaces using Amazon WorkSpaces Application Manager.

Amazon WorkSpaces

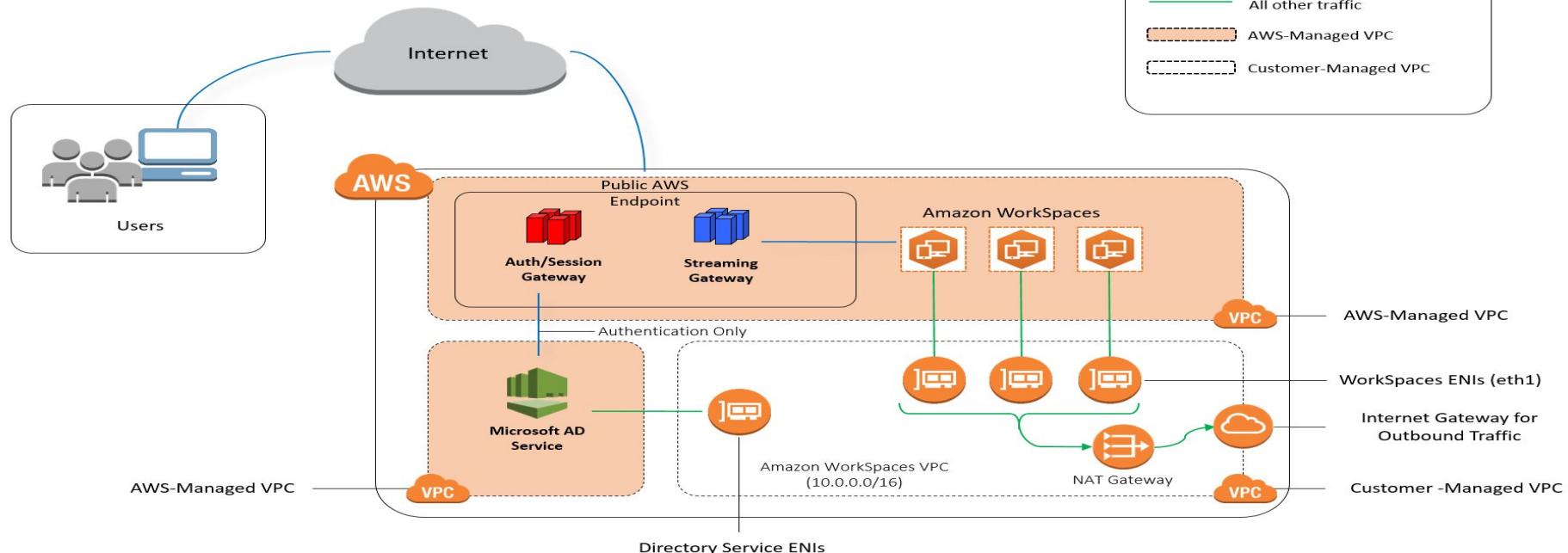
- Use the same tools to manage WorkSpaces that you use to manage on-premises desktops.
- Use multi-factor authentication (MFA) for additional security.
- Use AWS Key Management Service (AWS KMS) to encrypt data at rest, disk I/O, and volume snapshots.

Amazon WorkSpaces

- Architecture
 - Each WorkSpace is associated with the virtual private cloud (VPC), and a directory.
 - Directories are managed through the AWS Directory Service.
 - Amazon WorkSpaces uses a directory, either AWS Directory Service or Microsoft AD, to authenticate users.
 - Users access their WorkSpaces using a client application from a supported device or a web browser and log in using their directory credentials.

Amazon WorkSpaces

Amazon WorkSpaces Architectural Diagram



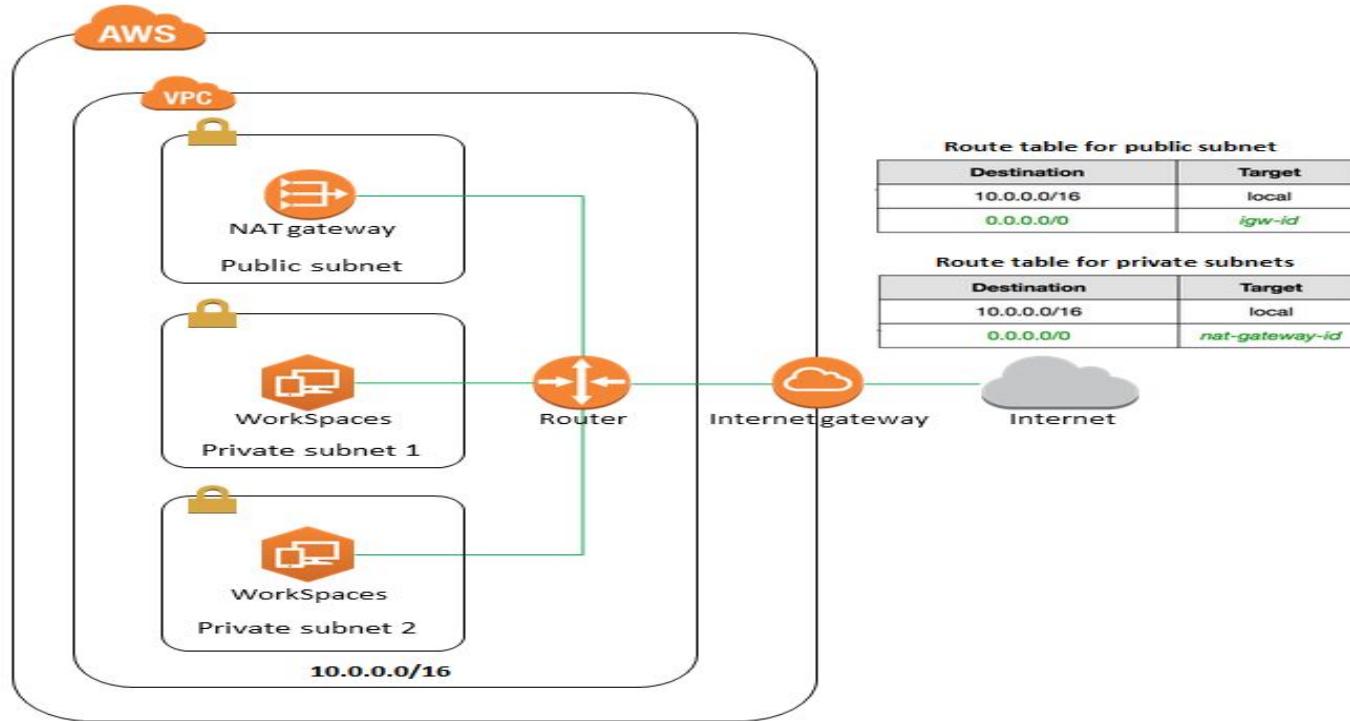
Amazon WorkSpaces

- The following devices are supported:
 - Windows computers
 - Mac computers
 - Chromebooks
 - iPads
 - Android tablets
 - Fire tablets
 - Zero client devices

Configure a VPC for Amazon WorkSpaces

- Amazon WorkSpaces launches your WorkSpaces in a virtual private cloud (VPC).
- Configure your directory to launch your WorkSpaces in the private subnets.
- To provide Internet Access to WorkSpaces in a private subnet, configure a NAT gateway in the public subnet.

Configure a VPC for Amazon WorkSpaces



Port Requirements for Amazon WorkSpaces

- To connect to your WorkSpaces, the network that your Amazon WorkSpaces clients are connected to must have certain ports open to the IP address ranges for the various AWS services.
- These address ranges vary by AWS region.
- These same ports must also be open on any firewall running on the client.

Port Requirements for Amazon WorkSpaces

- Ports for Client Applications
 - Port 443 (TCP)
 - Port 4172 (UDP and TCP)
- Ports for Web Access
 - Port 53 (UDP)
 - Port 80 (UDP and TCP)
 - Port 443 (UDP and TCP)

Manage Directories for Amazon WorkSpaces

- Amazon WorkSpaces uses a directory to store and manage information for your WorkSpaces and users.
- You can use one of the following options:
 - AD Connector
 - Microsoft AD
 - Simple AD
 - Cross trust

Launch a Virtual Desktop Using Amazon WorkSpaces

- With Amazon WorkSpaces, you can provision cloud-based virtual desktops for your users, known as **WorkSpaces**, in the AWS cloud.
- Amazon WorkSpaces uses a directory to store and manage information for your WorkSpaces and users.
- AWS Directory Service creates two directory servers, one in each of the private subnets of your VPC.

Administer Your WorkSpaces

- Each WorkSpace is assigned to a single user and cannot be shared by multiple users.
- Whenever you launch a WorkSpace, you must assign it to a user that does not already have a WorkSpace.
- The [running mode](#) of a WorkSpaces determines its immediate availability and how you pay for it.
- You can choose between the following running modes when you create the workspace:
 - AlwaysOn
 - AutoStop

Administer Your WorkSpaces

- You can organize and manage your WorkSpaces by assigning your own metadata to each WorkSpace in the form of **tags**.
- You specify a **key** and a **value** for each tag.
- You can apply tags to a WorkSpace when you launch it or apply them to the WorkSpace later on.
- Each tag automatically applies to all WAM applications and WAM related service charges for the WorkSpace.

Administer Your WorkSpaces

- When you launch a WorkSpace, you have the option to encrypt the root volume (C: drive) and the user volume (D: drive) using customer master keys.
- This ensures that the data stored at rest, disk I/O to the volume, and snapshots created from the volumes are all encrypted.
- Reboot a WorkSpace
 - Rebooting a WorkSpace performs a shutdown and restart of the WorkSpace.
 - The user data, operating system, and system settings are not affected.

Administer Your WorkSpaces

- Rebuild a WorkSpace
 - Rebuilding a WorkSpace causes the following to occur:
 - The system is restored to the most recent image of the bundle that the WorkSpace is created from.
 - The data drive (D drive) is recreated from the last automatic snapshot taken of the data drive.
- Delete a WorkSpace
 - When you are finished with a WorkSpace, you can delete it.
 - You can also delete related resources.

WorkSpace Bundles and Images

- A [WorkSpace bundle](#) specifies the hardware and software for your WorkSpace.
- When you launch a WorkSpace, you select the bundle that meets your needs.
- You can create an image from a WorkSpace that you've customized, create a custom WorkSpace bundle from the image, and launch WorkSpaces from your custom bundle.
- By creating a custom bundle, you can ensure that the WorkSpaces for your users have everything that they need already installed.

Monitoring Amazon WorkSpaces

- Amazon WorkSpaces and Amazon CloudWatch are integrated, so you can gather and analyze performance metrics.
- You can monitor these metrics.
- CloudWatch also allows you to set alarms when you reach a specified threshold for a metric.
- To get CloudWatch metrics, enable access on port 443 on the [AMAZON](#) subset in the [us-east-1](#) region.

Monitoring Amazon WorkSpaces

- Dimensions for Amazon WorkSpaces Metrics

Dimension	Description
Directory Id	Limits the data you receive to the WorkSpaces in the specified directory. The Directory Id value is in the form of d-XXXXXXXXXXXX.
WorkspaceId	Limits the data you receive to the specified WorkSpace. The WorkspaceId value is in the form ws-XXXXXXXXXXXX.

Desktop & App Streaming



Desktop & App Streaming

WorkSpaces

AppStream 2.0

- a fully managed, secure, application streaming service that allows you to stream desktop applications from AWS to any device running a web browser, without rewriting them.
- You can easily add your existing desktop applications to AWS and instantly start streaming them to an HTML5 compatible browser.

Amazon AppStream 2.0

- AppStream 2.0 provides users instant-on access to the applications they need, and a responsive, fluid user experience on the device of their choice.
- You can maintain a single version of each of your apps, which makes application management easier.
- Features
 - Run desktop applications on any device
 - Instant-on access
 - Secure applications and data
 - Easily integrate with your IT environment
 - Fully managed service
 - Consistent, scalable performance

Amazon AppStream 2.0

- Key Concepts
 - Stack
 - Set up an AppStream 2.0 stack to start streaming apps to user browsers.
 - An AppStream 2.0 stack consists of a fleet of streaming instances, user access policies, and storage configurations.
 - Fleet
 - The fleet in an AppStream 2.0 stack consists of streaming instances that can scale automatically based on demand.

Amazon AppStream 2.0

- Image
 - An AppStream 2.0 image contains applications to be streamed to users accessing an AppStream 2.0 stack.
- Image builder
 - Install your apps and create an image by using an AppStream 2.0 image builder.

Getting Started with Amazon AppStream 2.0

- To stream your applications, Amazon AppStream 2.0 requires an environment consisting of a stack and at least one application image.
- Before you can stream your applications, you need to create a stack.
- You create a new stack from the sample stack template to simplify the creation.
- After you create a stack, each user needs an active URL for access.

Using an AppStream 2.0 Image Builder

- Before you can stream your applications, Amazon AppStream 2.0 requires at least one image that you create using an image builder.
- After that connect to the image builder that you created and launched, then install the applications to be included in the image.
- After that you can add applications (.exe), batch scripts (.bat), and application shortcuts (.lnk) to the image.

Persistent Storage with AppStream 2.0 Home Folders

- AppStream 2.0 offers persistent storage support for your end users with Home Folders.
- When this option is enabled for an AppStream 2.0 stack, end users of the stack are presented with a persistent storage folder in their AppStream 2.0 sessions.
- Data stored by the user in this folder is automatically backed up to an Amazon S3 bucket in your AWS account and is made available in subsequent sessions for that user.

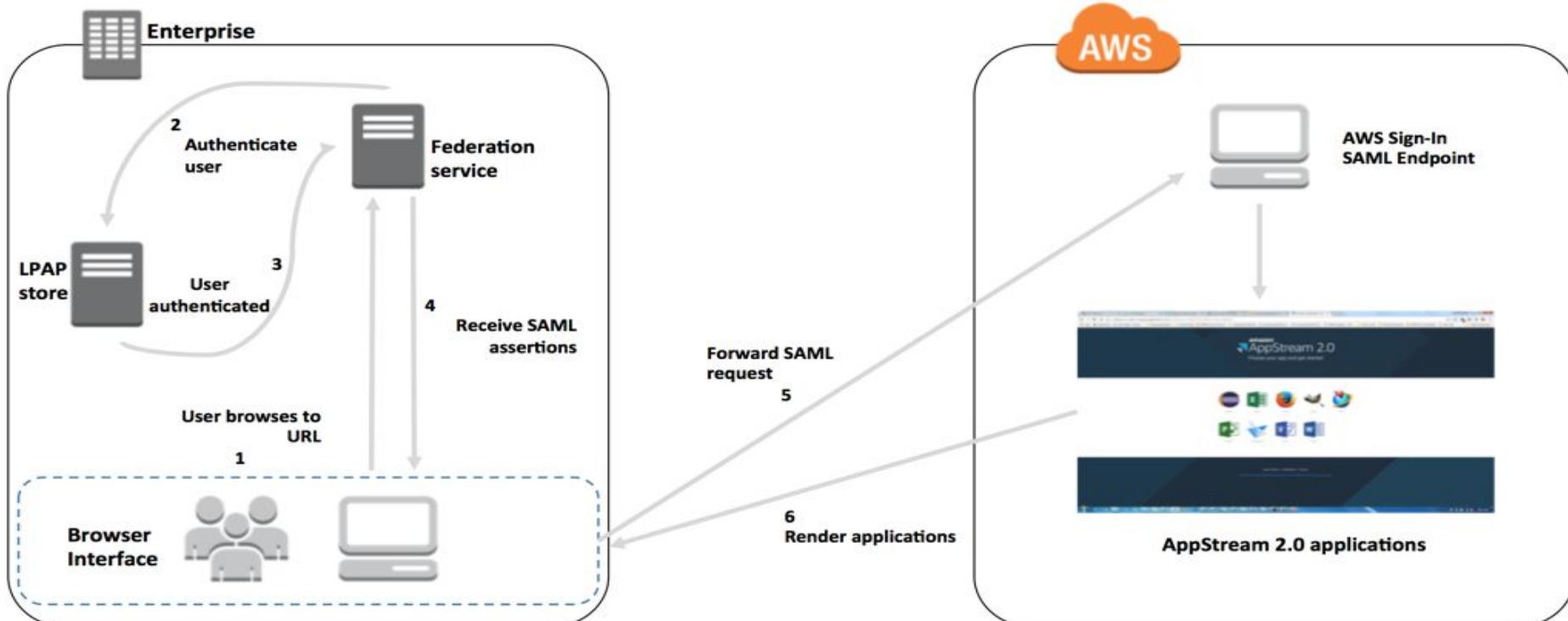
Network Settings for Fleet and Image Builder Instances

- When creating an AppStream 2.0 fleet or image builder, you can provide Amazon VPC subnets.
- AppStream 2.0 sets up elastic network interfaces (ENI) to the subnets provided.
- This is so that AppStream 2.0 instances have access to your network resources or have access to public Internet through your VPC.
- Security groups that belong to your VPC allow you to control the network traffic between AppStream 2.0 streaming instances and VPC resources.

Enabling Single Sign-on Access to AppStream 2.0 Using SAML 2.0

- Amazon AppStream 2.0 supports identity federation to AppStream 2.0 stacks through Security Assertion Markup Language 2.0 (SAML 2.0).
- This feature offers your users the convenience of one-click access to their AppStream 2.0 applications using their existing identity credentials.
- You also have the security benefit of identity authentication by your identity provider. You can control which users have access to a particular AppStream 2.0 stack, using your existing identity provider.

Example Authentication Workflow



Controlling Access to Amazon AppStream 2.0

- IAM users don't have permission to create or modify AppStream 2.0 resources, use Fleet Auto Scaling, or perform tasks using the AppStream 2.0 API.
- To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant permissions on specific resources and API actions, and then attach those policies to the IAM users or groups that require those permissions.

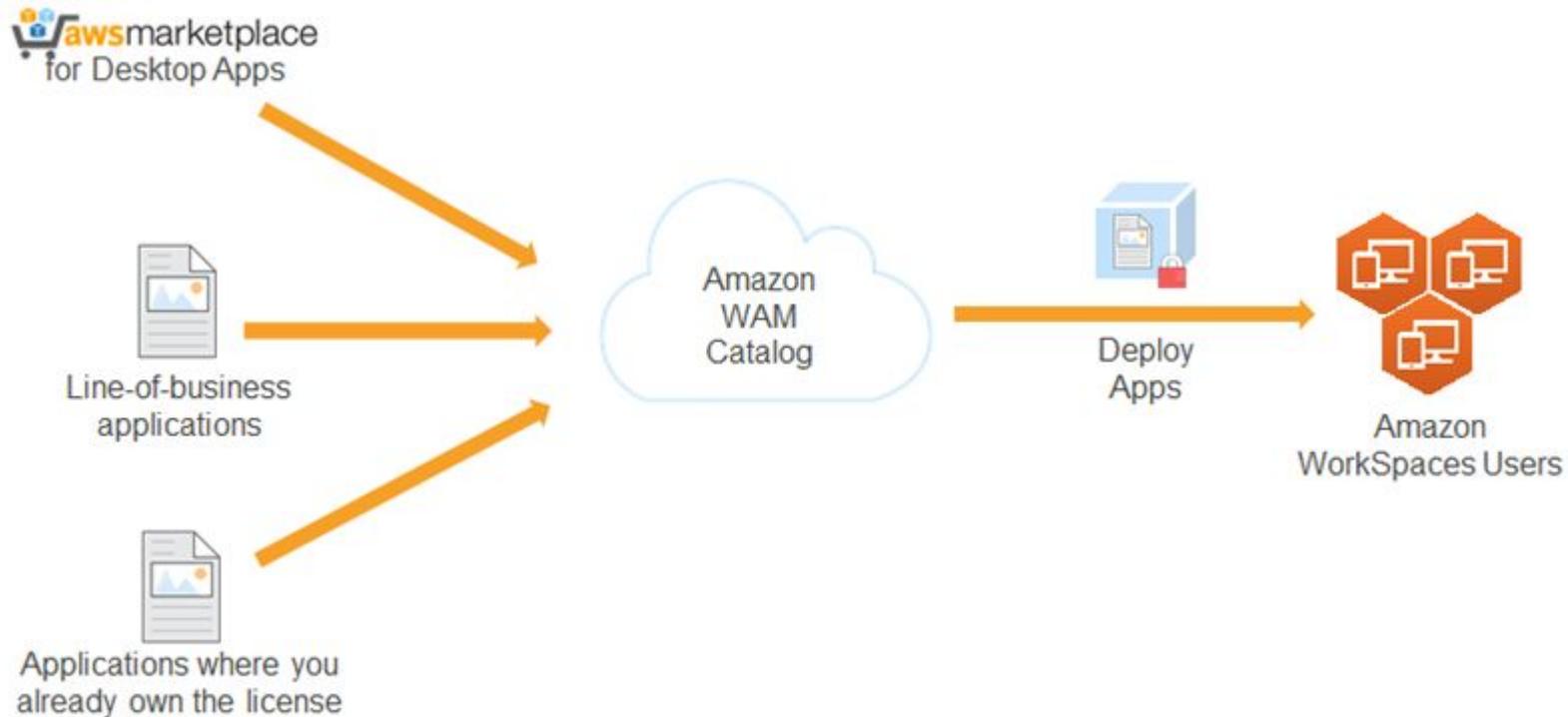
Controlling Access to Amazon AppStream 2.0

- While creating AppStream 2.0 resources, AppStream 2.0 makes API calls to other AWS services on behalf of the user.
- This authentication is accomplished by the service assuming specific IAM roles available in the user's account.
- These IAM roles are created by the service when the user gets started with the service in an AWS region.

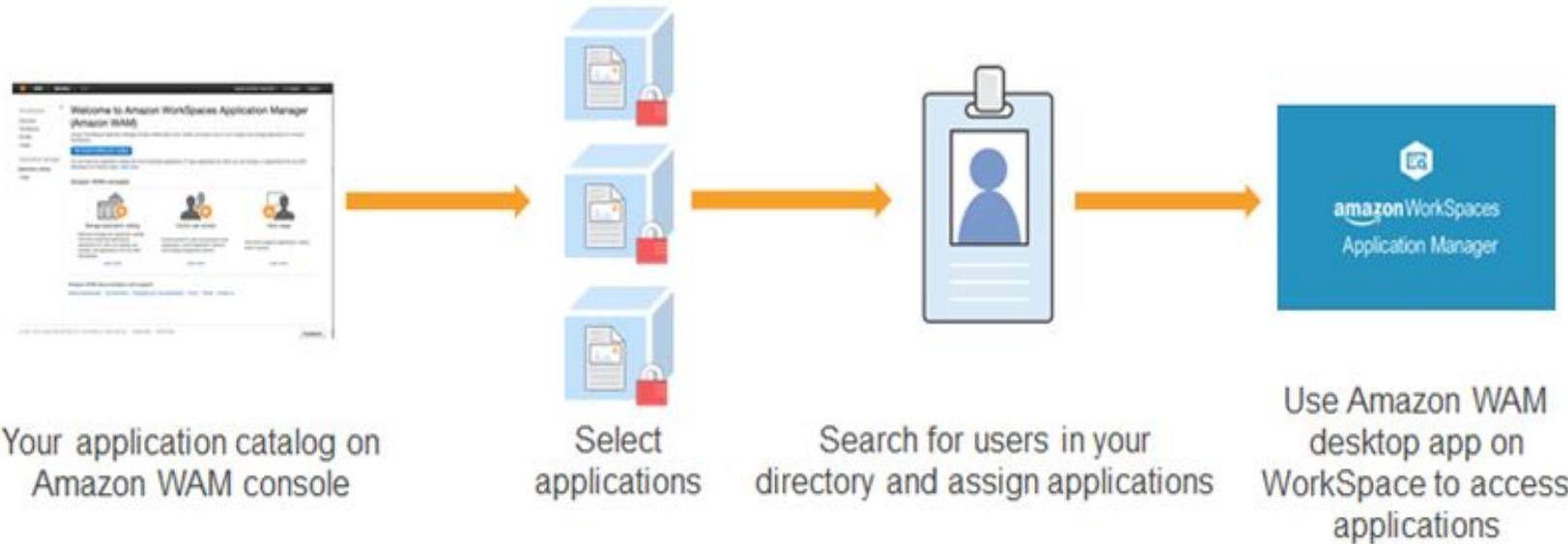
Amazon WorkSpaces Application Manager

- Amazon WAM offers a fast, flexible, and secure way for you to deploy and manage applications for Amazon WorkSpaces.
- It accelerates software deployment, updates, patching, and retirement by packaging Microsoft Windows desktop applications into virtual containers that run as though they are installed natively.
- You can deploy subscriptions to your Amazon WorkSpaces users from the AWS Marketplace, your line-of-business applications, or applications where you already own the licenses.

Process to Deploy Applications



Process to Assign an Application to User



Managing Your Amazon WAM Applications

- You can use Amazon WorkSpaces Application Manager (Amazon WAM) to deploy applications to the WorkSpaces that you created for your users.
- First, you add applications to your application catalog.
- Then you assign applications to the users.
- After you assign applications to users, they can connect to their WorkSpaces and install and use the applications.

Packaging and Validating Your Applications

- To create Amazon WAM applications of your own making, you must create the application package, and validate that the package installs and works correctly.
- This is accomplished using two special EC2 instances.
- You should launch an entirely new packaging instance for each application package that is created.

Controlling Access to Amazon WAM Resources

- Amazon WAM must have permission to perform certain actions on your behalf.
- You can grant this access using IAM roles.
- By default, IAM users don't have permission to access Amazon WAM resources.
- To allow an IAM user to perform actions on Amazon WAM resources, you must create a policy that grants the user permission to access Amazon WAM.
- This IAM role allows the Amazon WAM packaging instance to access your application package catalog.



Amazon Web Services (AWS)



Amazon Web Services (AWS)

AWS:

Amazon Web Services (AWS) is a subsidiary of Amazon.com, providing **on-demand** cloud computing services.

It offer services such as compute, storage, database, content delivery and management tools etc.

These services are used by organization to scale and grow their business.

A key features on which AWS works are **AWS global Infrastructure** and **AWS security and compliance**.

AWS:

1. AWS Global Infrastructure:

AWS expand its global infrastructure to provide services to large number of enterprises.

AWS emphasis on lowering the latency (delay) and increasing throughput of infrastructure.

It provide highly available infrastructure having multiple location worldwide.

Locations are consist of **Regions** and **Availability Zones**

AWS:

- Regions:

Regions are the separate geographical area.

Each region is completely separated from other region

Isolation is done to provide highly fault tolerance and stable network.

Region are consist of multiple availability zones.

AWS:

- Availability Zone:

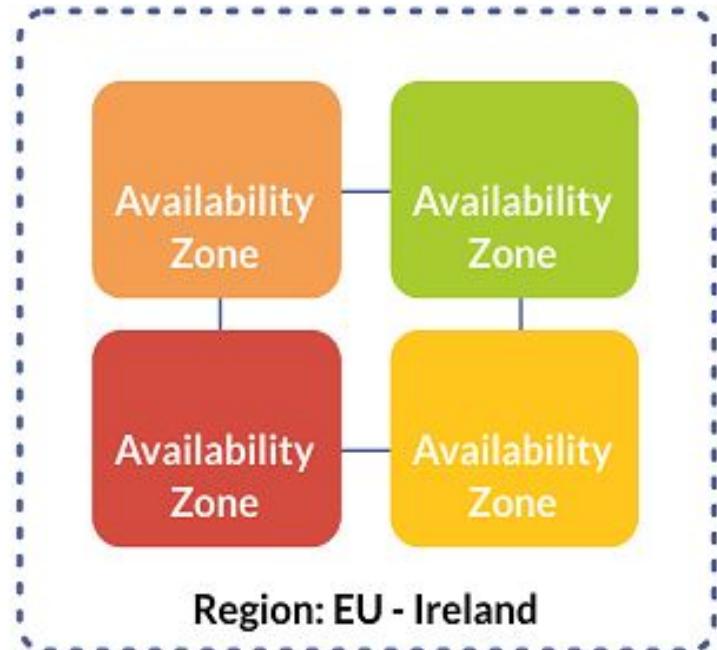
Each region consist of multiple isolated location known as Availability Zones.

Availability Zones in a particular region are connected through a low-latency link.

Availability Zones between different region are completely isolated and are located in lower-risk flood plain.

Availability Zones consist data centers equipped with redundant power, networking and connectivity and are housed in separate facilities.

AWS:



AWS:

2. Security and Compliance:

Security - most important aspect for Amazon Web Services.

In AWS, Security is given first priority to gain trust and confidence of their customers using their services.

AWS provide various tools and add various features dealing with the security of data and resources.

AWS design an infrastructure that is monitored and protected by maintaining data privacy and segregation while providing higher availability of resources.

AWS:

2. **Security and Compliance:**

Compliance help organizations to establish and operate in an AWS security control environment.

Certification and standards that AWS complies for security purpose:

- Payment Card Industry Security Standard (PCI DSS) Level 1
- Service Organization Controls (SOC) 1/ International Standard on Assurance Engagement (ISAE) 3402, SOC2 and SOC 3
- International organization for standardization (ISO) 9001, ISO 27001, ISO 27018



Accessing AWS Platform

Accessing AWS Platform

How to access the AWS Platform?

AWS Platform provide services which is used to fulfill the business requirement.

Aws Platform can be accessed in three ways:

- AWS Management Console
- AWS Command Line Interface (CLI)
- AWS Software Development Tool (SDK)

Accessing AWS Platform

AWS Management Console

AWS Management Console is a web application where user interact with AWS cloud services.

Used for managing AWS cloud services and performing various tasks.

Each service will have their own console.

AWS Management console provide information about the account and billing.

Accessing AWS Platform

Features of AWS Management Console

- Managing AWS account
- Navigate various services in AWS console
- Pin important services
- Viewing collection of resources in “Resource Group”
- Tag Editor
- About AWS

Accessing AWS Platform

AWS Command Line Interface (CLI)

AWS Command Line Interface (CLI) is a unified tool which is used to manage AWS Services.

This manage the multiple services through command lines and automate through the script.

aws-shell is a command-line shell program that provides convenience and productivity features to help both new and advanced users of the AWS Command Line Interface.

Accessing AWS Platform

AWS Software Development kit (SDK)

AWS Software Development kit (SDK) provide an Application programming interface (API).

It interact with the web services that make the AWS platform.

It also provide support to many different programming language.



Compute

Compute:

AWS provide a variety of compute and networking services.

Organizations use these services to develop and run their workloads according to business need.

AWS provide services such as storage, database and application services.

Example: Amazon Elastic Compute cloud (Amazon EC2), AWS Lambda, AWS Elastic Beanstalk, Amazon Virtual private cloud (Amazon VPC) etc.

Compute:

1. Amazon Elastic Compute Cloud (Amazon EC2):

Amazon EC2 is a kind of [web service](#) which is used for scalable computing capacity in AWS cloud.

It allow organizations to launch as many or as few virtual servers according to their need, configure security and networking, and manage storage.

Organization can select variety of Operating System and resource configuration such as memory, CPU, storage etc.

Organization use these resources to build and deploy their mobile application and websites etc.

Compute:

2. AWS Lambda:

AWS Lambda is a serverless compute service with zero administration.

It is used by back-end developers to quickly build an application by running codes without provisioning and managing any servers.

Developers just upload their codes and Lambda takes care of everything required to run and scale their codes with high availability.

Developers pay only for the compute time they consume - there is no charge when their code is not running.

Compute:

3. AWS Elastic Beanstalk:

AWS Elastic Beanstalk is used to quickly deploy and manage application in AWS Cloud.

Developers upload their applications and Elastic Beanstalk handles all the details such as capacity provisioning, load balancing and monitoring etc.

It support application developed in java, .NET, PHP, Python, Ruby, Node.js etc

Compute:

4. Amazon Virtual Private Cloud (VPC):

Amazon Virtual Private Cloud provision a logically isolated section of AWS cloud.

Organizations can launch AWS resources in a virtual network topology.

It provides organizations with complete control over the virtual networking environment.

Organization can make selection of their own IP address range, creation of subnets and configuration of route tables and network gateways.

Organizations use Amazon VPN to expand their data centers using hardware and software VPN connections.

Compute:

5. AWS Direct Connect:

AWS Direct connect provides a dedicated network connection over AWS cloud.

It allow their customers to establish a direct connection between their office or data centers and AWS Direct connect location.

It reduce the bandwidth cost by providing more consistent network which is compatible with all AWS services.

Compute:

6. Amazon Route 53:

Amazon Route 53 is a part of AWS which provide highly scalable and available Domain Name Server (DNS).

It provide a reliable and cost effective way to translate domain name of any website and application into its IP address.

Developer define the route to end users over internet to their application or web pages by defining domain names such as amazon.com and their associated IP address.

It perform these functions such as registering domain names, routing internet traffic to particular websites or application and checking the health of resources (web server).

Compute:

AWS offer compute and networking services like

Auto Scaling:

It is a method in which Amazon EC2 scale its capacity up and down automatically according to condition defined about the workload.

Elastic Load Balancing:

It is used to divide the incoming application traffic in multiple Amazon EC2 instances to increase the fault tolerance capacity of network.



Storage

Storage:

AWS Storage Services are used to meet the demand of storage space required by various organizations.

AWS Storage services include Amazon Simple Storage Service (Amazon S3), Amazon CloudFront or Amazon Elastic Block store (EBS) etc.

Storage:

1. Amazon Simple Storage Secure (Amazon S3):

Amazon S3 is a object storage with simple web service interface.

It is used to store large amount of data and retrieve from anywhere on the web using http protocol.

It can store any type of data like html page, source codes, image file or encrypted data etc.

User can store backup and recovery, disaster recovery data, cloud applications etc.

Storage:

Features of Amazon S3:

1. Simple
2. Durable & scalable
3. Secure
4. Low cost
5. Simple data transfer
6. Easy to manage

Storage:

2. Amazon Glacier:

Amazon Glacier is a online storage service having low cost.

It is used to store long term backups and archive files at very low cost of \$0.004 per gigabyte per month.

It is best option for storing data having less access or data which is not accessed regularly.

AWS provide the large retrieval time which varies from several minutes to several hours.

Storage:

Features of Amazon Glacier:

1. Low cost
2. Secure
3. Durable
4. Simple
5. Flexible
6. Integrated

Storage

3. Amazon Elastic Block store (Amazon EBS):

Amazon EBS is a type of persistent block level storage device.

It is used with Amazon EC2 instances.

Each Amazon EBS volume replicates itself within its Availability Zone which provides protection against component failure.

It provides high availability and durability of Amazon EBS network.

It provides disk storage space to run wide variety of workloads.

Storage:

4. Amazon CloudFront:

Amazon CloudFront is a global content delivery network (CDN) service.

CloudFront of AWS is a world's largest cloud service provider.

It give developers an easy way to distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.

It provide globally-distributed network of proxy server with cache content of websites, videos contents, APIs or other web assets more locally to consumer which improve the access speed of downloading the content.

Storage:

5. Amazon Storage Gateway:

Amazon Storage Gateway provides a hybrid cloud storage service.

It enables on-premises software applications to seamlessly use storage in AWS cloud.

The applications connect to the Amazon Storage Gateway using standard storage protocols, such as NFS and iSCSI.

The gateway connects to AWS storage services such as Amazon S3, Amazon Glacier and Amazon EBS, providing storage for files, volumes, and virtual tapes in AWS.



Database

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Database:



Database

RDS

DynamoDB

ElastiCache

Redshift

Provides

- fully-managed relational and NoSQL database services
- in-memory caching as a service
- a petabyte-scale data-warehouse solution.

RDS Relational Database Service



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon Relational Database Service (Amazon RDS) is a web service
- manage relational databases in the cloud.
- Amazon RDS provides six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.

Amazon RDS

Amazon Relational Database service (RDS) is a web service used to manage relational database in the AWS cloud.

It provide a cost-effective service that allow organization to launch secure and highly available production ready database in few minute.

Amazon RDS manages time-consuming administration such as backup, software patching, automatic failure detection and recovery.

Organizations can add security to their database packages by using AWS IAM to define users and permissions.

Amazon RDS components

- DB instances
- Regions and Availability Zones
- Security Groups
- DB Parameter Groups
- DB Option Groups

Amazon RDS components

DB instances :

DB instance - Basic Building block of Amazon RDS.

A DB instance is an isolated database environment in the cloud.

It contain multiple user-created databases and can be access by using same tools and application.

DB instance is created and modified by using the AWS Command Line Interface, Amazon RDS API or AWS Management Console.

Amazon RDS components

DB instances :

DB Engine - Each DB instance runs a DB engine.

It support DB engines such as MySQL, MariaDB, PostgreSQL, Oracle and Microsoft SQL server.

Each DB engine has its own supported features and set of parameters (DP Parameters Groups) for controlling and managing databases.

Amazon RDS components

DB instances :

[DB Engine](#) - MySQL

MySQL is one of the most popular open source databases in the world.

it is used to power a wide range of applications, from small personal blogs to some of the largest websites in the world.

Amazon RDS for MySQL currently supports MySQL 5.7, 5.6, 5.5, and 5.1.

Amazon RDS components

DB instances :

[DB Engine](#) - PostgreSQL

PostgreSQL is a widely used open source database engine with a very rich set of features and advanced functionality.

Amazon RDS supports DB Instances running several versions of PostgreSQL.

Amazon RDS supports multiple releases of PostgreSQL, including 9.5. x, 9.4. x, and 9.3. x.

Amazon RDS components

DB instances :

DB Engine - MariaDB

Amazon RDS recently added support for DB Instances running MariaDB.

MariaDB is a popular open source database engine built by the creators of MySQL and enhanced with enterprise tools and functionality.

MariaDB adds features that enhance the performance, availability, and scalability of MySQL.

Amazon RDS components

DB instances :

[DB Engine](#) - Oracle

Oracle is the one of the most popular relational databases used in the enterprise and is fully supported by Amazon RDS.

Amazon RDS supports DB instances running several editions of Oracle 11g and oracle 12c

Amazon RDS support three different editions of the popular database engine: Standard edition one, Standard edition and Enterprise edition.

Amazon RDS components

DB instances :

DB Engine - Oracle

Edition	Performance	Multi-AZ	Encryption
Standard one	++++	Yes	KMS
Standard	++++++	Yes	KMS
Enterprise	++++++	Yes	KMS & TDE

Amazon RDS components

DB instances :

DB Engine - Microsoft SQL Server

Microsoft SQL server is another very popular relational database used in the enterprise.

Amazon RDS allows Database Administrators (DBAs) to connect to their SQL Server DB instance in the cloud using native tools like SQL server management studio.

Amazon RDS support several version of Microsoft SQL server such as SQL server 2008 R2, SQL server 2012, SQL server 2014.

Amazon RDS components

DB instances :

DB Engine - Microsoft SQL Server

Edition	Performance	Multi-AZ	Encryption
Express	+	No	KMS
Web	****	No	KMS
Standard	****	Yes	KMS
Enterprise	*****	Yes	KMS & TDE

Amazon RDS components

DB instances

DB instance class - determine the computation and storage capacity of DB instance.

Each DB instance have 5GB to 6TB of associated storage capacity.

DB instance storage comes in 3 types: Magnetic, General Purpose (SSD) and provisioned IOPS (SSD).

DB instance can be run on virtual private cloud using the Amazon VPC service.

Amazon RDS components

Regions and Availability Zones

Region - is a location of highly available data centers

Availability Zones (AZs) - are multiple-distinct location in every region.

Amazon RDS components

Security Groups

Security Groups control access to the DB instances.

It specify rules to access the instances by configuring specific range of IP addresses, ports or EC2 security group.

Amazon RDS use 3 types of security group:

- DB security groups
- VPC security groups
- EC2 security groups

Amazon RDS components

DB Parameter Groups

DB Parameter Groups are used to configure DB engine.

It contain engine configuration values which is applied to one or more DB instances of same instance type.

If parameters are not defined by user while creating DB instance, Amazon RDS applies a default DB parameter group.

Amazon RDS components

DB Option Groups

DB engine use DB Option Group to offer additional features to manage databases and to add security.

Amazon RDS use Option Group to enable and configure features.

Amazon RDS interfaces

These interfaces are used to interact with Amazon RDS

- Amazon RDS Console
- Command Line Interface
- Programmatic Interface

Amazon RDS interfaces

Amazon RDS Console

Simple Web-based User Interface.

Console window is used to perform all task, no programming is required.

To access Amazon RDS Console:

Sign in to AWS Management console and Open the Amazon RDS Console at <https://console.aws.amazon.com/rds/>

Amazon RDS interfaces

Command Line Interface

AWS CLI is an open source tool built on top of AWS SDK.

It provides command for interacting with AWS services.

It give access to the functionality that are available in Amazon RDS API.

Amazon RDS interfaces

Programmatic Interface

Following are the resources used to access Amazon RDS programmatically.

AWS-SDK :- It includes sample codes, libraries, tools documentations and templates.

Amazon RDS API :- provides an application programming interface (API) which is used to automate many of the tasks for managing DB instances and other objects on Amazon RDS.



Amazon DynamoDB

DynamoDB



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon DynamoDB is a fully managed NoSQL database service.
- It provides fast and flexible database services.
- Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, Internet of Things (IoT), and many other applications.

Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service..

It provides fast and predictable performance with seamless scalability.

It also reduce the administrative burdens of operating and scaling a distributed database, such as hardware provisioning, setup and configuration, replication, software patching or cluster scaling.

DynamoDB is used to create database tables that can store and retrieve any amount of data, and serve any level of request traffic.

Amazon DynamoDB

DynamoDB allows to delete expired items from tables automatically to reduce storage usage and the cost of storing data that is no longer in use.

Data is stored on solid state disks (SSDs) and automatically replicated across multiple Availability Zones in an AWS region for providing built-in high availability and data durability.

Amazon DynamoDB components

- Tables
- Items
- Attributes
- Primary Keys
- Secondary Indexes

Amazon DynamoDB components

- Tables :

DynamoDB stores data in **tables**.

A **table** is a collection of **data**.

For example:

You could create a table named “Relations”, where you could store information about friends, family, or anyone else of interest.

You could also have a “Vehicles” table to store information about vehicles that people drive.

Amazon DynamoDB components

- Items :

An **item** is a group of attributes that is uniquely identifiable among all of the other items.

Each **table** contains **multiple items**.

Items are similar to rows, records or tuples in relational database Systems.

In DynamoDB, there is no limit to the number of items you want to store in a table.

Amazon DynamoDB components

- Attributes:

An **attribute** is a fundamental data element that does not need to be divided any further.

Each **item** is composed of **one or more attributes**.

Attributes in DynamoDB are similar in many ways to fields or columns.

For example: a Department item contain attributes such as DepartmentID, Name, Manager, and so on.

Amazon DynamoDB components

- Primary Key:

A primary key in DynamoDB uniquely identifies each item in the table, so that no two items can have the same key.

When item is added, updated or deleted from the table, the primary key attribute values must be specify with that item.

The key values are required very important to add while creating database in DynamoDB.

DynamoDB consist of two type of primary keys: Partition keys & Partition key and Sort key

Amazon DynamoDB components

- Primary Key, Partition key:

A simple primary key, composed of one attribute known as the partition key.

This partition key values that are input or output to an internal hash function are used to determine the partition where the item is stored.

With a simple primary key, no two items in a table can have the same partition key value.

Amazon DynamoDB components

- Primary Key: Partition key and Sort key

A composite primary key, composed of two attributes: Partition key and Sort key.

Partition key value is used to determine the partition where the item is stored using hash function.

Sort key value store all items in sorted order which have same partition key.

Amazon DynamoDB components

- Primary Key:

The Partition key of an item is also known as its Hash Attribute.
(because of the service's use of an internal hash function to evenly distribute data items across partitions, based on their partition key values.)

The Sort key of an item is also known as its Range Attribute.
(Because of the way DynamoDB stores items with the same partition key physically close together, in sorted order by the sort key value.)

Amazon DynamoDB components

- Secondary Indexes:

A Secondary index is used to query the data in the table using an alternate key (in place of primary key).

DynamoDB supports two kinds of indexes:

- Global secondary index – an index with a partition key and sort key that can be different from those on the table.
- Local secondary index – an index that has the same partition key as the table, but a different sort key.

Amazon DynamoDB

Amazon DynamoDB is set up in two ways:

1. Setting up DynamoDB Local (Downloadable version)
2. Setting up DynamoDB (Web Service)

Amazon DynamoDB

1. Setting up DynamoDB Local (Downloadable version):

The downloadable version of DynamoDB is used to write applications without accessing the actual Amazon DynamoDB web service.

In this, the database is self-contained on local computer.

This local version of DynamoDB help to save on provisioned throughput, data storage, and data transfer fees.

User doesn't need an Internet connection while developing application.

Amazon DynamoDB

1. Setting up DynamoDB Local (Downloadable version):

The downloadable version of DynamoDB is provided as an executable jar file. It will run on Windows, Linux, Mac OS X, and other platforms that support Java.

DynamoDB requires the Java Runtime Environment (JRE) version 6.x or newer on computer; it will not run on older JRE versions

DynamoDB is also available on Maven or as part of the AWS Toolkit for Eclipse

Amazon DynamoDB

2. Setting up DynamoDB (Web Service):

To use the DynamoDB web service follow these steps:

1. Sign Up for AWS
2. Get Your AWS Access Key ID and Secret Key (used to access DynamoDB programmatically).

Amazon DynamoDB

Amazon DynamoDB can be accessed by using the following method:

1. Using Console
2. Using CLI
3. Using API

Amazon DynamoDB

1. Using Console:

To access the DynamoDB AWS Management Console

<https://console.aws.amazon.com/dynamodb/home>

Console is used to access DynamoDB different features.

- Overview – Shows Stream and Table details. Manage Streams and Time To Live (TTL).
- Items – Manage items and perform queries and scans.
- Metrics – Monitor your CloudWatch metrics.

Amazon DynamoDB

1. Using Console:

- [Alarms](#) – Manage CloudWatch alarms.
- [Capacity](#) – Modify your table's provisioned capacity.
- [Indexes](#) – Manage Global Secondary Indexes (GSIs).
- [Triggers](#) – Manage triggers to connect DynamoDB streams to Lambda functions.

Amazon DynamoDB

1. Using Console:

- **Access control** – Setup fine-grained access control with Web Identity Federation.
- **Tags** – Apply tags to your resources to help organize and identify them.

Amazon DynamoDB

2. Using CLI:

DynamoDB AWS Command Line Interface (AWS CLI) is used to control multiple AWS services from the command line and automate them through scripts.

User can use the AWS CLI for ad hoc operations, such as creating a table and embed DynamoDB operations within utility scripts.

Before setting up the AWS CLI on computer, firstly get AWS Access Key ID and Secret Key (User IAM).

Amazon DynamoDB

2. Using CLI:

The AWS CLI is available at <http://aws.amazon.com/cli>, and will run on Windows, Mac, or Linux.

After downloading the AWS CLI, then install and configure it:

Amazon DynamoDB

3. Using API:

User can write application code using the AWS SDKs.

The AWS SDKs provide broad support for DynamoDB in java, javascript in the browser, .NET, node.js, PHP, Python, Ruby, C++, Go, Android and iOS

ElastiCache



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon ElastiCache is a web service used to manage in-memory cache in the cloud.
- High performance, cost effective and scalable service.
- Amazon ElastiCache supports two open-source in-memory caching engines i.e **Redis** and **Memcached**

Amazon ElastiCache

ElastiCache is a [web service](#) that is used to set up, manage and scale a distributed in-memory cache environment in the cloud in easy way.

It provides a high-performance, scalable and cost-effective caching solution.

It also remove complexity associated with deploying and managing a distributed cache environment.

User can quickly deploy their cache environment, without provisioning hardware or installing software.

Amazon ElastiCache

Memcached or Redis protocol-compliant cache engine software are used to cache memory in ElastiCache.

ElastiCache automatically perform software upgrades and patch management.

To enhanced security, ElastiCache can be run in the Amazon Virtual Private Cloud (Amazon VPC) environment.

Amazon ElastiCache

Cache Engine: [Memcached](#)

Memcached provides a very simple interface that allows the user to write and read objects into in-memory key/ value data stores.

With Amazon ElastiCache, user can elastically grow and shrink a cluster of Memcached nodes to meet their demands.

User can partition their cluster into shards and support parallelized operations for very high performance throughput.

Memcached deals with objects as blobs that can be retrieved using a unique key.

Amazon ElastiCache

Cache Engine: [Redis](#)

In late 2013, Amazon ElastiCache added support to deploy Redis clusters.

This service supports the deployment of Redis version 2.8.24, and also a number of older versions.

Beyond the object support provided in Memcached, Redis supports a rich set of data types like strings, lists, and sets.

Unlike Memcached, Redis supports the ability to persist the in-memory data onto disk.

Amazon ElastiCache

Cache Engine: [Redis](#)

This allow users to create snapshots that back up their data and then recover or replicate from the backups.

Redis clusters also can support up to five read replicas to offload read requests.

Redis also has advanced features that make it easy to sort and rank data.

Some common use cases include building a leaderboard for a mobile application or serving as a high-speed message broker in a distributed system.

Amazon ElastiCache

ElastiCache has multiple features to enhance reliability for critical production deployments:

- Automatic detection and recovery from cache node failures.
- Multi-AZ with Automatic Failover that support replication
- Flexible Availability Zone placement of nodes and clusters.
- Integration with other AWS services such as Amazon EC2, Amazon CloudWatch, AWS CloudTrail, and Amazon SNS to provide a secure, high-performance, managed in-memory caching solution.

Redshift



Database

RDS

DynamoDB

ElastiCache

Redshift

- Amazon Redshift is a fast, fully managed, petabyte scale data warehouse service that makes it simple and cost-effective
- It analyzes all the data using standard SQL and existing Business Intelligence (BI) tools.
- Use **Nodes** and **Clusters** to organize data.

Amazon Redshift

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud.

Nodes represents the collection of computing resources in data warehouse of Amazon Redshift.

These Nodes are organized into a group called a Cluster.

Each cluster runs an Amazon Redshift engine and contains one or more databases.

Amazon Redshift

Clusters and Nodes:

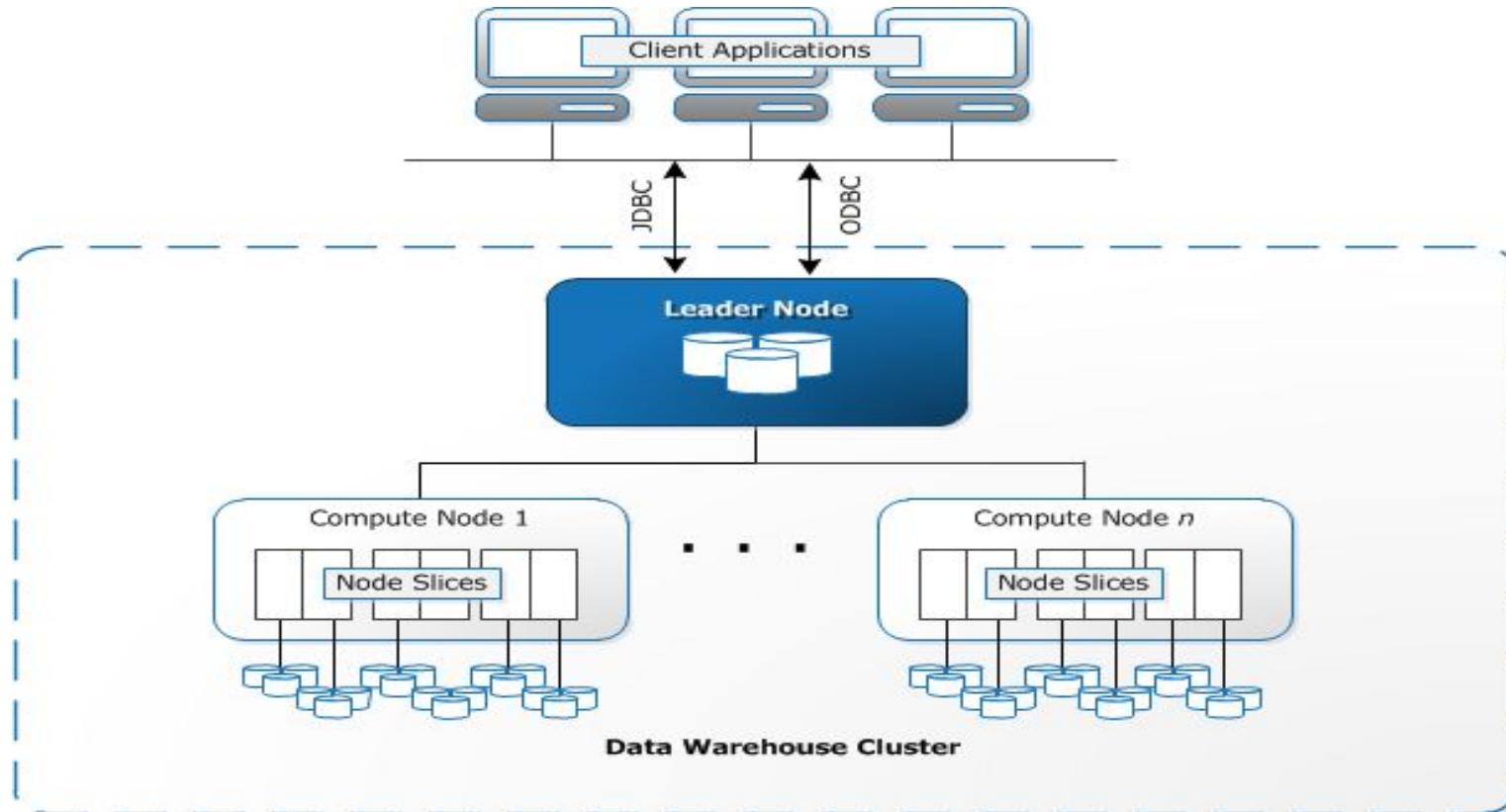
The key component of an Amazon Redshift data warehouse is a **cluster**.

Each cluster is composed of a one leader node and one or more compute nodes.

Amazon Redshift currently has support for six different node types and each has a different mix of CPU, memory, and storage.

The six node types are grouped into two categories: **Dense Compute** and **Dense Storage**.

Amazon Redshift



Amazon Redshift

Clusters and Nodes:

The disk storage for a compute node is divided into a number of slices.

The number of slices per node depends on the node size of the cluster and typically varies between 2 and 16.

The nodes all participate in parallel query execution, working on data that is distributed as evenly as possible across the slices.

Amazon Redshift

Amazon Redshift Management:

The Amazon Redshift service manages all the work such as 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.



Amazon Redshift

Amazon Redshift

Amazon Redshift Management:

1. Managing Clusters
2. Access and security to cluster
3. Monitoring Clusters
4. Databases

Amazon Redshift

1. Managing Clusters:

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 depends on the size of data, the number of queries execute and the query execution performance.

- Creating and managing cluster
- Reserving Compute nodes
- Creating Clusters Snapshots

Amazon Redshift

2. Access and Security to cluster:

Access and security in Amazon Redshift clusters have many features.

These features help user to control access to their cluster, define connectivity rules and encrypt data and connections.

- AWS account and IAM credentials
- Security Groups
- Encryption
- SSL Connection

Amazon Redshift

3. Monitoring Clusters:

There are many features related to monitoring cluster in Amazon Redshift such as:

- Database Audit logging
- Events and Notifications
- Performances

Amazon Redshift

4. Databases:

Amazon Redshift creates one database when user provision a cluster.

User use this database to load data and run queries.

More databases can be created by running a [SQL command](#).

[Super user](#) : When a cluster is provision user specify a [master user](#) who has access to all of the databases that are created within the cluster.

Master user can create additional super users and users.

Amazon Redshift

4. Databases:

Amazon Redshift uses parameter groups to define the behavior of all databases in a cluster, such as date presentation style and floating-point precision.



Networking & Content Delivery

AWS CONSOLE

Services ▾ | Resource Groups ▾

History

Console Home

Billing

IAM

EC2

DynamoDB

Compute

- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Database

- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery

- VPC
- CloudFront
- Direct Connect
- Route 53

Migration

- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools

- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance

- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Compliance Reports

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence

- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things

- AWS IoT

Contact Center

- Amazon Connect

Game Development

- Amazon GameLift

Mobile Services

- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services

- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging

- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity

- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Networking & Content Delivery



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- AWS networking products enable user to isolate cloud infrastructure, scaling request handling capacity, and connecting physical network to private virtual network.
- AWS networking products work together to meet the needs of particular application.
- For example, Elastic Load Balancing works with Amazon VPC to provide robust networking and security features.

VPC (Virtual Private cloud)



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon VPC is a web service used to launch AWS resources in Virtual Private network.
- Highly secure network formation
- Users can configure their own VPC and selects its IP address range, create subnets, and configure route tables, network gateways, and security settings.

Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) is used to launch Amazon Web Services (AWS) resources into a virtual network.

This virtual network closely resembles a traditional network that operate in data center

Amazon VPC have the benefits of using the scalable infrastructure of AWS.

Amazon VPC Components

- Route tables
- DHCP option sets
- Security groups
- Network Access Control List

Amazon VPC Components

Route Tables

A route table is a logical construct which contains a set of rules (**called routes**) that are applied to the subnet.

Route Tables used to determine where network traffic is directed.

Each route table contains a default route called the **local route**.

It enables communication within the Amazon VPC, and this route cannot be modified or removed.

Amazon VPC Components

Route Tables

- VPC has an implicit router.
- VPC automatically comes with a main route table that can be modified.
- User can create additional custom route table.
- Each subnet must be associated with a route table, which controls the routing for the subnet.
- Each route in a table specifies a destination CIDR and a target.

Amazon VPC Components

DHCP Options Sets

Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/ IP network.

The options field of a DHCP message contains the configuration parameters.

Some of those parameters are the domain name, domain name server, and the netbios-node-type.

Amazon VPC Components

DHCP Options Sets

AWS automatically creates and associates a DHCP option set for user Amazon VPC upon creation and sets two options :

- domain-name-servers (defaulted to AmazonProvidedDNS)
- domain-name (defaulted to the domain name for your region)

To assign your own domain name to the instances, create a custom DHCP option set and assign it to your Amazon VPC.

Amazon VPC Components

DHCP Options Sets

You can configure the following values within a DHCP option set:

- domain-name-servers
- domain-name
- ntp-server
- netbios-name-servers
- netbios-node-type



VPC Components

Amazon VPC Components

Security Groups

A security group is a virtual stateful firewall that controls inbound and outbound network traffic to AWS resources and Amazon EC2 instances.

All Amazon EC2 instances are launched into a security group.

If a security group is not specified at launch, then the instance will be launched into the default security group for the Amazon VPC.

Amazon VPC Components

Security Groups rule

Inbound			
Source	Protocol	Port Range	Comments
Sg-xxxxxxxx	All	All	Allow inbound traffic from instances within the same security group.

Amazon VPC Components

Security Groups rule

Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0 /0	All	All	Allow all outbound call.

Amazon VPC Components

For Example Security Groups rule for Web server

Inbound			
Destination	Protocol	Port Range	Comments
0.0.0.0 /0	TCP	80	Allow all inbound traffic from the internet to port 80.
Your network's shell	TCP	22	Allow Secure (SSH) traffic from your company network
Public IP range			

Amazon VPC Components

For Example Security Groups rule for Web server:

Inbound			
Destination	Protocol	Port Range	Comments
Your network's Public IP range	TCP	3389	Allow Remote Desktop Protocol (RDP) traffic from your company network.

Amazon VPC Components

For Example Security Groups rule for Web server:

Outbound			
Destination	Protocol	Port Range	Comments
The ID of the Security group for your MySQL database servers	TCP	3306	Allow outbound MySQL access to instances in the specified security group.

Amazon VPC Components

For Example Security Groups rule for Web server:

Outbound			
Destination	Protocol	Port Range	Comments
The ID of the Security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL server access to instances in the specified security group

Amazon VPC Components

Security Group

- User can create up to 500 security groups for each Amazon VPC
- User can add up to 50 inbound and 50 outbound rules to each security group.
- User can specify allow rules, but not deny rules. (this is an important difference between security group and ACL's)
- User can specify separate rules for inbound and outbound traffic.

Amazon VPC Components

Security Group

- By default, no inbound traffic is allowed until user add inbound rules to the security group.
- By default, new security group have an outbound rule that allow all outbound traffic.
- Security groups are stateful.
- Instances associated with the same security group can't talk to each other unless u add rules allowing it.

Amazon VPC Components

Network Access Control Lists (ACLs)

A network ACL is a numbered list of rules that AWS evaluates in order.

It starts with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL.

Amazon VPC are created with a modifiable default network ACL.

Amazon VPC Components

Comparison between Security group and Network ACL

Security Group	Network ACL
<ol style="list-style-type: none">1. Operates at the instance level (First Layer of defence).2. Supports allow rules only.3. Stateful: Return traffic is automatically allowed, regardless of any rules.	<ol style="list-style-type: none">1. Operates at the subnet level (Second layer of defence).2. Supports Allow rules and deny rules.3. Stateless: Return traffic must be explicitly allowed by rules.

Amazon VPC Components

Comparison between Security group and Network ACL

Security Group	Network ACL
4. AWS evaluates all rules before number deciding whether to allow traffic.	4. AWS processes rules in order when deciding whether to allow traffic.
5. Applied selectively to individual Instances.	5. Automatically applied to all instances in the associated subnet, this is a backup layer of defence.

Amazon VPC Components

Additional components

- Internet Gateway (IGWs)
- Elastic IP (EIP) addresses
- Elastic Network Interfaces (ENIs)
- Endpoints
- Peering
- Network address translation (NAT)
- Virtual Private Gateway (VPGs), Customer Gateway (CGWs), Virtual Private network (VPNs)

Amazon VPC Components

Internet Gateway

Internet Gateway is a horizontally scaled, redundant and highly available Amazon VPC component.

It allow communication between instances in Amazon VPC and Internet.

It provide a target in Amazon VPC route tables for Internet-routable traffic.

It perform NAT (network address translation) for instances that have been assigned public IP address.

Amazon VPC Components

Internet Gateway

To create a public subnet with internet access:

- Attach an IGW to your Amazon VPC
- Create a subnet route table rule to send all nonlocal traffic (0.0.0.0/0) to the IGW.
- Configure your network ACLs and security group rules to allow relevant traffic to flow to and from your instance.

Amazon VPC Components

Elastic IP addresses (EIPs)

AWS maintains a pool of IP addresses in each region and makes them available for user to associate to resources within amazon VPC.

An Elastic IP addresses (EIP) is a static, public IP address in the pool for the region that user can allocate to their account (pull from the pool) and release (return to the pool).

Amazon VPC Components

Elastic IP addresses (EIPs)

- User must first allocate an EIP for use within a VPC and then assign it to an instance.
- EIPs are specific to a region.
- There is one-to-one relationship between network interfaces and EIPs.
- EIPs remain associated with user AWS account until user explicitly release them.

Amazon VPC Components

Elastic Network Interfaces (ENIs)

An **Elastic Network Interface** (ENI) is a virtual network interface that user can attach to an instance in an Amazon VPC.

ENI have one public IP address and multiple private IP addresses.

One address acts as a primary address from the multiple private IP addresses.

ENI are only available within an Amazon VPC, and they are associated with a subnet upon creation.

Amazon VPC Components

Endpoints

An Amazon VPC [endpoint](#) enables the users to create private connection between user's amazon VPC and other AWS services without requiring access over internet or through a NAT instance, VPN connection or AWS Direct connect.

Amazon VPC endpoints currently support communication with amazon S3, and other services are expected to be added in future.



VPC Components

Amazon VPC Components

Peering

An Amazon VPC **peering** connection is a networking connection between two Amazon VPCs that enables instances in either Amazon VPC to communicate with each other as if they are within the same network.

A peering connection is neither a gateway nor an Amazon VPN connection and does not introduce a single point of failure for communication.

Peering connections are created through a request/ accept protocol.

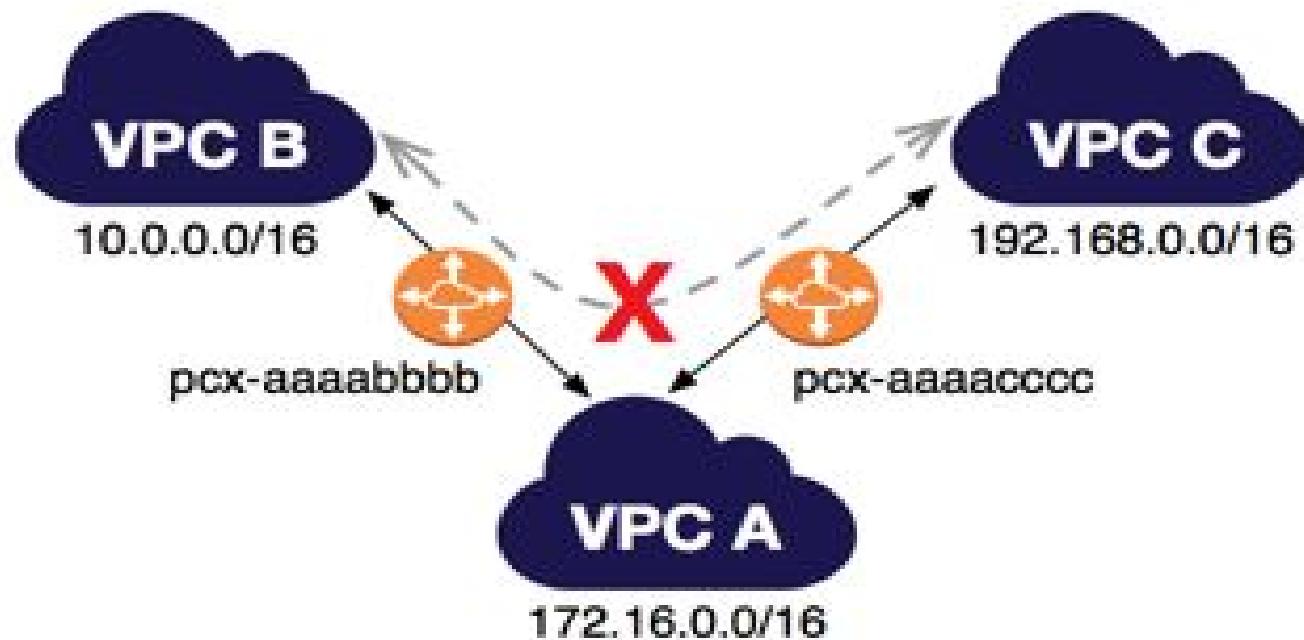
Amazon VPC Components

Peering

An Amazon VPC may have multiple peering connections, it means two Amazon VPCs cannot have two peering agreements between them.

Peering connections do not support transitive routing.

Amazon VPC Components: Peering



Amazon VPC Components

Peering

- User cannot create a peering connection between Amazon VPCs that have matching or overlapping CIDR blocks.
- User cannot create a peering connection between Amazon VPCs in different regions.
- Amazon VPC peering connections do not support transitive routing.
- User cannot have more than one peering connection between the same two Amazon VPCs at the same time.

Amazon VPC Components

Network Address Translation (NAT)

By default, any instance that is launched into a private subnet in an Amazon VPC is not able to communicate with the Internet through the IGW.

This is a problematic issue: if the instances within private subnets need direct access to the Internet from the Amazon VPC in order to apply security updates, download patches, or update application software.

AWS provides **NAT instances** and **NAT gateways** to allow instances deployed in private subnets to gain Internet access.

Amazon VPC Components

NAT Gateway

A NAT gateway is an Amazon managed resource

It is designed to operate just like a NAT instance, but it is simpler to manage and highly available within an Availability Zone.

Amazon VPC Components

NAT Gateway

To allow instances within a private subnet to access Internet resources through the IGW via a NAT gateway, user must do the following:

- Configure the route table associated with the private subnet to direct Internet-bound traffic to the NAT gateway (for example, nat-1a2b3c4d).
- Allocate an EIP and associate it with the NAT gateway.

Amazon VPC Components

Virtual Private Gateway (VPGs), Customer Gateway (CGWs), Virtual Private network (VPNs)

User can connect an existing data center to Amazon VPC using either hardware or software VPN connections, which will make Amazon VPC an extension of the data center.

Amazon VPC offers two ways to connect a corporate network to a VPC: VPG and CGW.

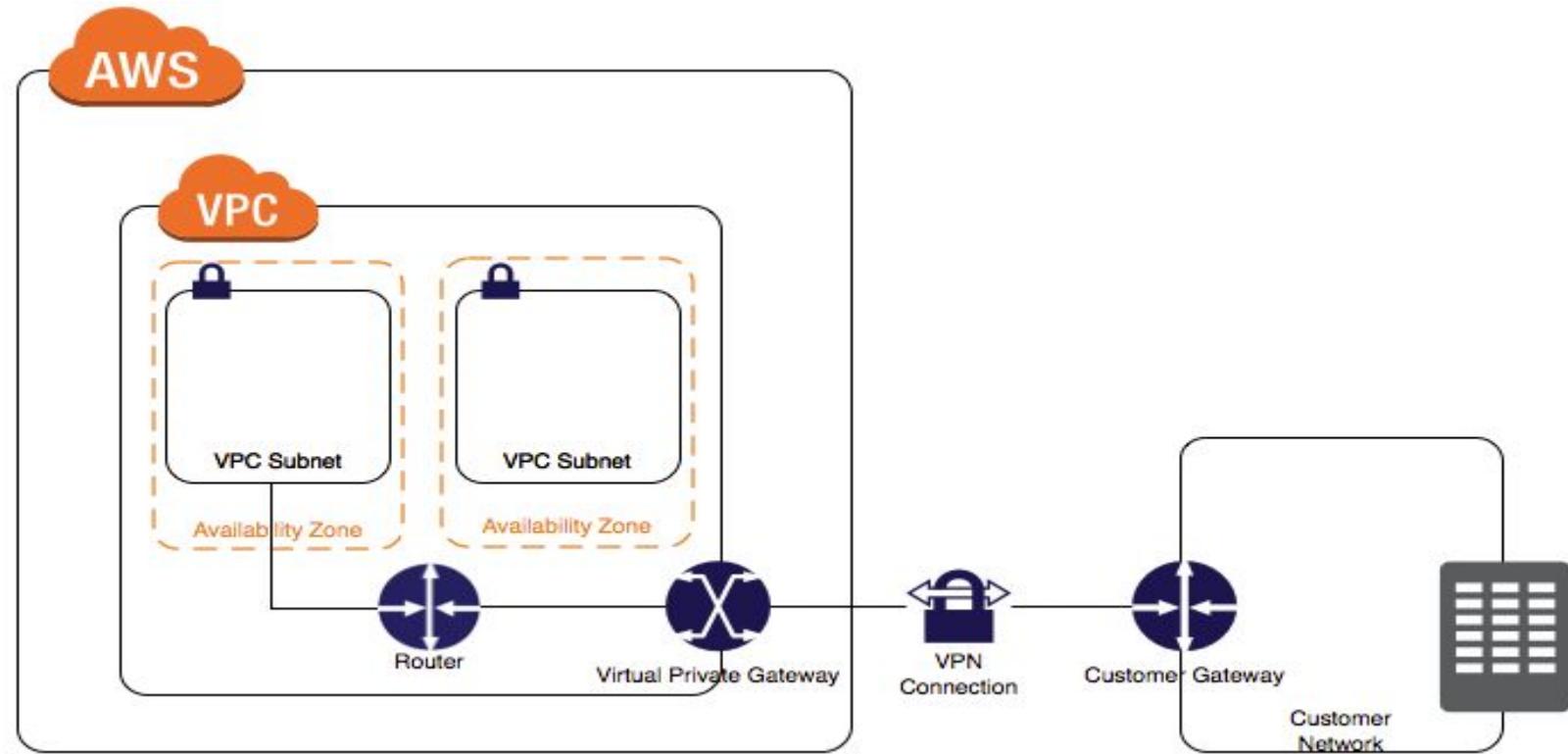
Amazon VPC Components

Virtual Private Gateway (VPGs), Customer Gateway (CGWs), Virtual Private network (VPNs)

A **virtual private gateway** (VPG) is the virtual private network (VPN) concentrator on the AWS side of the VPN connection between the two networks.

A **customer gateway** (CGW) represents a physical device or a software application on the customer's side of the VPN connection.

Amazon VPC Components



Amazon VPC Components

Virtual Private Gateway (VPGs), Customer Gateway (CGWs), Virtual Private network (VPNs)

- The VPG is the AWS end of the VPN tunnel.
- The CGW is a hardware or software application on the customer's side of the VPN tunnel.
- User must initiate the VPN tunnel from the CGW to the VPG.
- VPGs support both dynamic routing with BGP and static routing.
- The VPN connection consists of two tunnels for higher availability to the VPC.

Amazon VPC concepts

- VPCs and Subnets
- Supported Platforms
- Default and Non default VPCs
- Accessing the Internet
- Accessing a corporate or Home network

Amazon VPC concepts

- VPCs and Subnets:

A **Virtual Private Cloud** (VPC) is a virtual network dedicated to the AWS account.

It is logically isolated from other virtual networks in the AWS cloud.

Users can configure their own VPC and selects its IP address range, create subnets, and configure route tables, network gateways, and security settings.

Amazon VPC concepts

- VPCs and Subnets:

A **subnet** is a range of IP addresses in the VPC.

Selected AWS resources are launched into subnet.

User use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.

Amazon VPC concepts

- Supported Platforms:

The original release of Amazon EC2 supported a single, flat network that's shared with other customers called the EC2-Classic platform.

Older AWS accounts still support this platform, and can launch instances into either EC2-Classic or a VPC.

Accounts created after 2013-12-04 support EC2-VPC only.

Amazon VPC concepts

- Supported Platforms:

Benefits of launching instances into a VPC instead of EC2-Classic:

- Assign static private IPv4 addresses to the instances that persist across starts and stops.
- Optionally associate an IPv6 CIDR block to VPC and assign IPv6 addresses to instances.

Amazon VPC concepts

- Supported Platforms:
 - Change security group membership for instances while they're running.
 - Control the outbound traffic from instances (egress filtering) in addition to controlling the inbound traffic to them (ingress filtering).

Amazon VPC concepts

- Default and non default VPCs:

When AWS account supports the EC2-VPC platform only, then it comes with a default VPC

It has a default subnet in each Availability Zone.

A default VPC has the benefits of the advanced features provided by EC2-VPC.

Amazon VPC concepts

- Default and non default VPCs:

When user create its own VPC and configure it according to their needs.

This is known as a non default VPC.

Subnets that are created in non default VPC and additional subnets that are created in default VPC are called non default subnets.

Amazon VPC concepts

- Accessing the Internet:

User can control how the instances that are launched into a VPC access resources outside the VPC.

The default VPC includes an Internet gateway, and each default subnet is a public subnet.

Each instance that is launched into a default subnet has a private IPv4 address and a public IPv4 address.

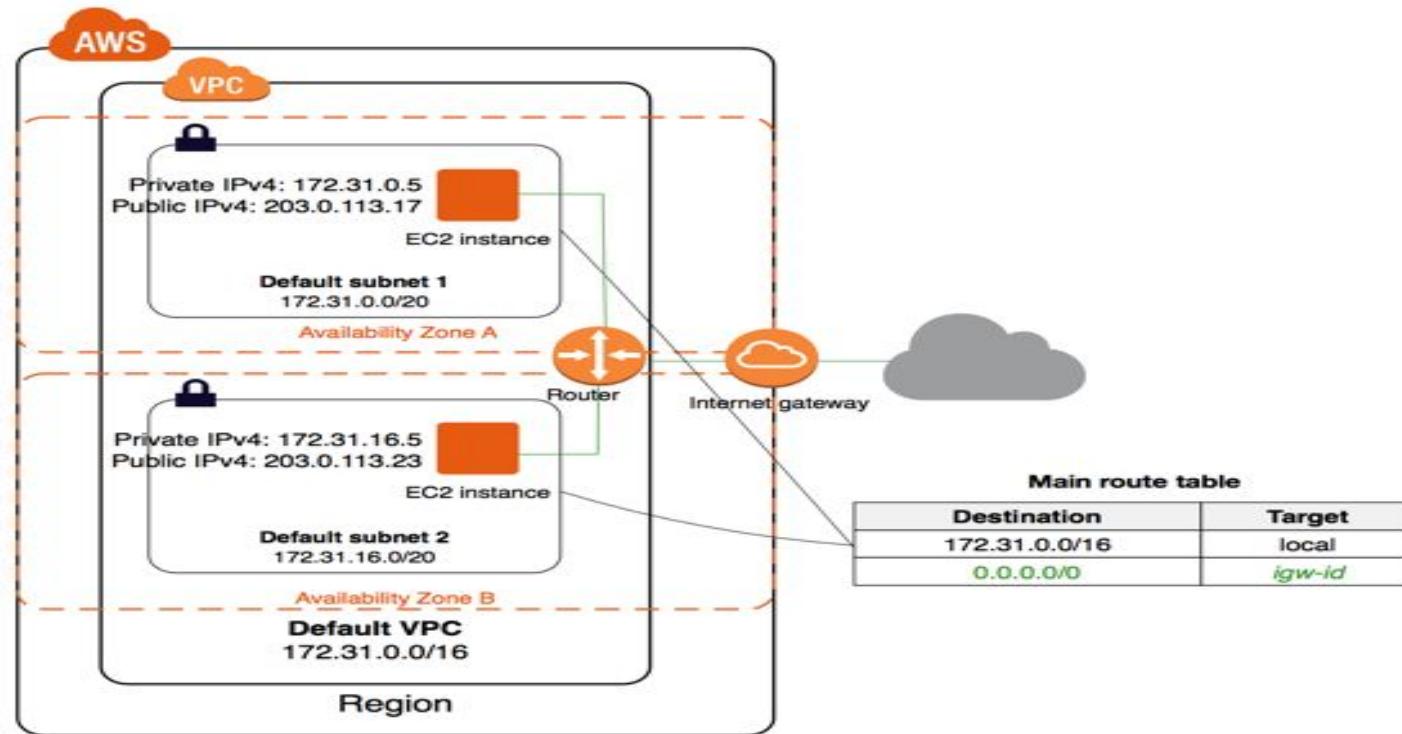
Amazon VPC concepts

- Accessing the Internet:

These instances can communicate with the Internet through the Internet gateway.

An Internet gateway enables the instances to connect to the Internet through the Amazon EC2 network edge.

Amazon VPC: Accessing the Internet



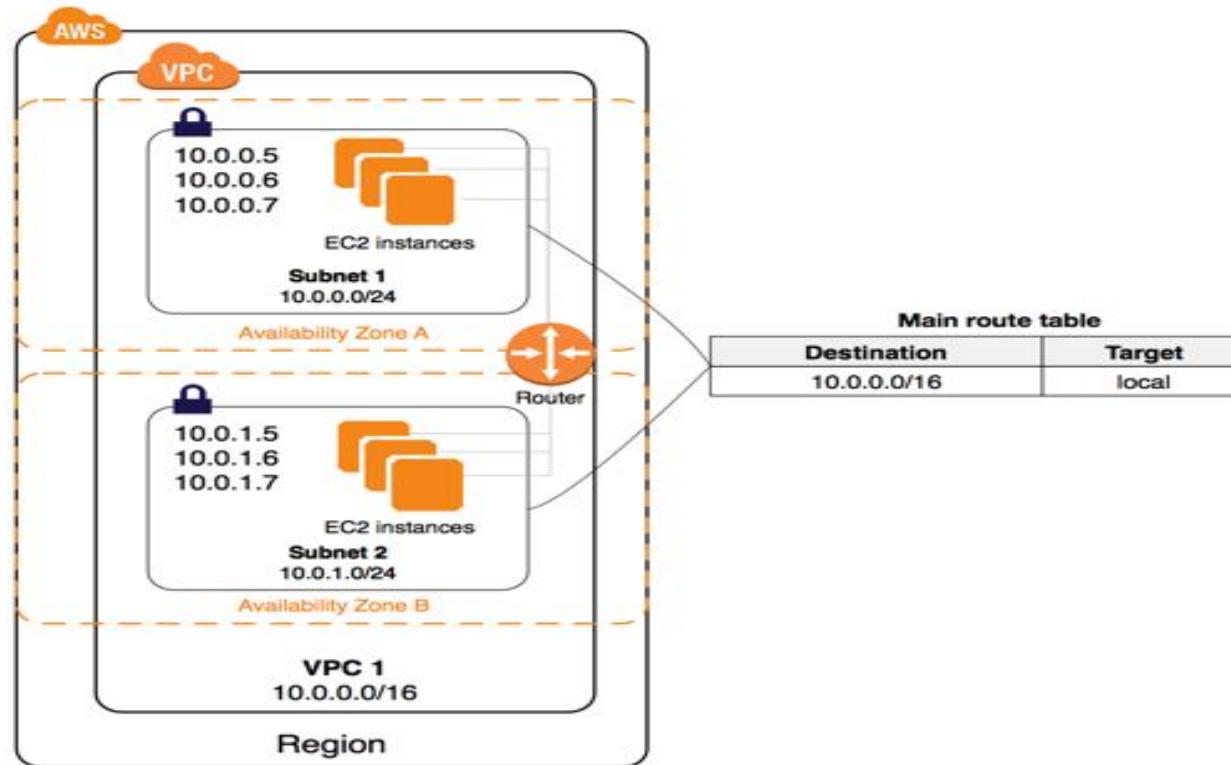
Amazon VPC concepts

- Accessing the Internet:

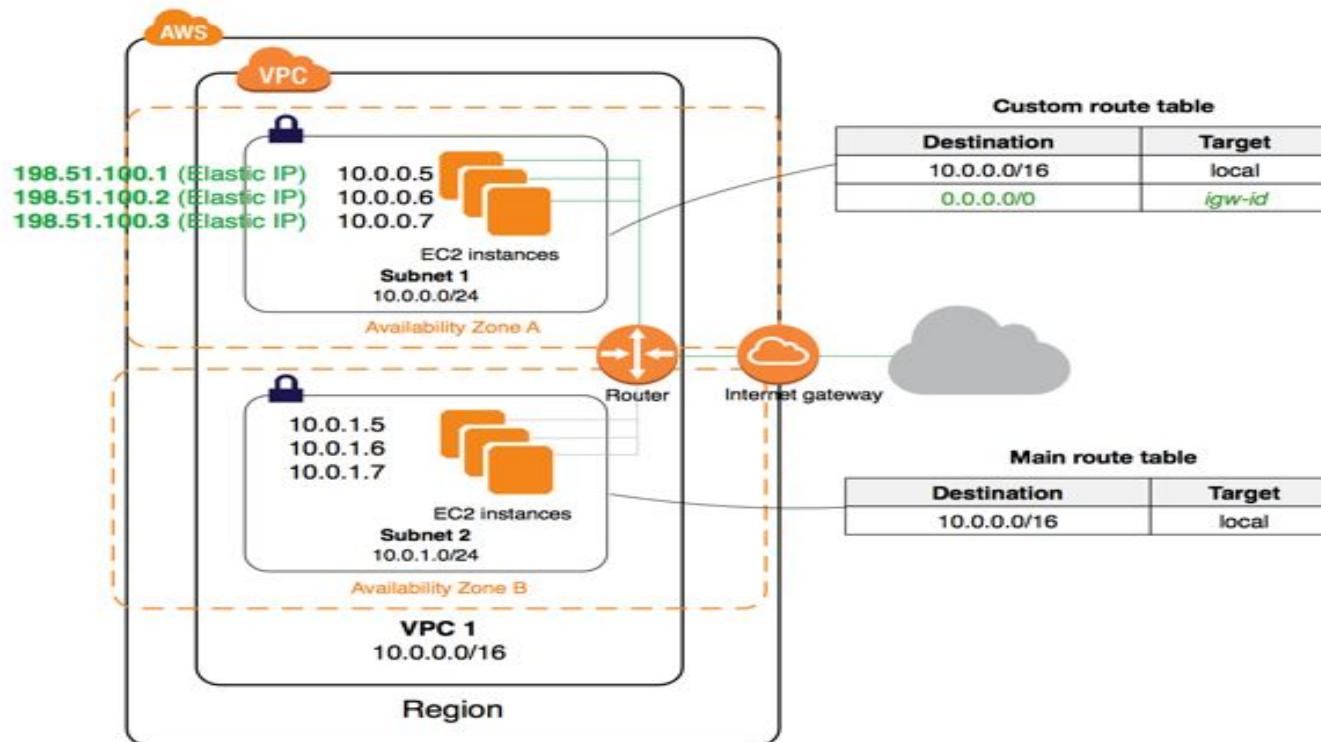
By default, each instance that launch into a non default subnet has a private IPv4 address, but no public IPv4 address.

Public IPv4 address is added by the user during launch of an instance.

Amazon VPC: Accessing the Internet



Amazon VPC: Accessing the Internet



Amazon VPC concepts

- Accessing the Internet:

Network address translation (NAT) device can be used to allow an instance in VPC to initiate outbound connections to the Internet while preventing unsolicited inbound connections.

NAT maps multiple private IPv4 addresses to a single public IPv4 address.

A NAT device has an Elastic IP address and is connected to the Internet through an Internet gateway.

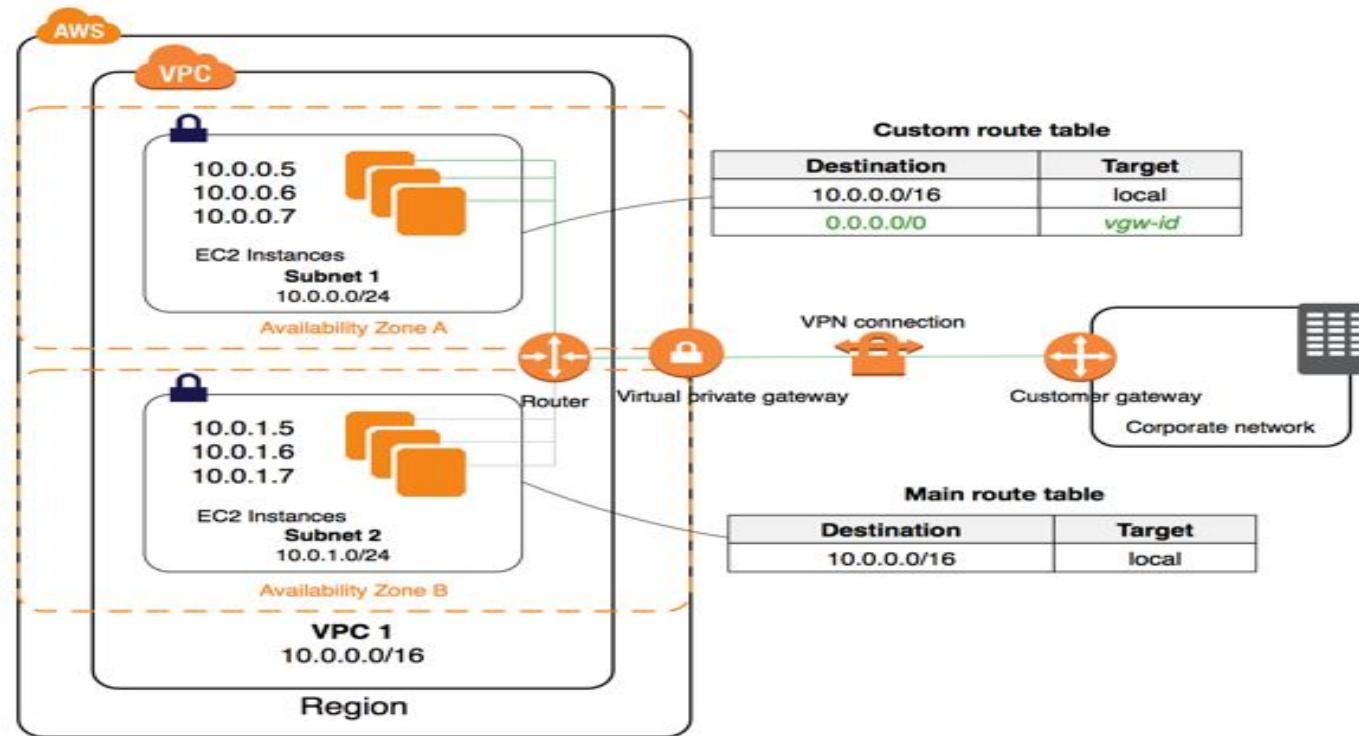
Amazon VPC concepts

- Accessing a corporate or Home network:

Amazon VPC can be connected to the corporate data center by using an IPsec hardware VPN connection.

A VPN connection consists of a virtual private gateway attached to VPC and a customer gateway located in data center.

Amazon VPC: Accessing a corporate network





Amazon VPC

Amazon VPC

Amazon VPC can be used with these following AWS services:

1. AWS EC2
2. Auto Scaling
3. AWS OpsWorks
4. Amazon RDS
5. Amazon Route 53
6. Amazon WorkSpaces
7. Amazon Redshift

Amazon VPC

AWS configuration :

AWS Config provides a detailed view of the configuration of AWS resources in AWS account.

This includes how the resources are related to one another and how they were configured in the past.

Amazon VPC

With AWS Config, user can config the following:

- Evaluate the AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
- Retrieve configurations of one or more resources that exist in your account.
- Retrieve historical configurations of one or more resources.

Amazon VPC

With AWS Config, user can config the following:

- Receive a notification whenever a resource is created, modified, or deleted.
- View relationships between resources. For example, you might want to find all resources that use a particular security group.

Amazon VPC

Accessing Amazon VPC:

Amazon VPC provides a web-based user interface, the Amazon VPC console.

1. Signed up for an AWS account
2. Then access the Amazon VPC console by signing into the AWS Management Console.
3. select **VPC** from the console home page.

Amazon VPC

AWS Command Line Interface (CLI) :

Amazon VPC can be accessed using AWS CLI.

Provides commands for a broad set of AWS products and is supported on Windows, Mac, and Linux/UNIX.

AWS Tools for Windows PowerShell

Provides commands for a broad set of AWS products for those who script in the PowerShell environment.

Amazon VPC

Accessing Amazon VPC:

To build applications using language-specific APIs , AWS provides libraries, sample code, tutorials, and other resources for software developers.

These libraries provide basic functions that automatically take care of tasks such as cryptographically signing your requests, retrying requests, and handling error responses etc.

Amazon VPC

Amazon VPC Limits:

There are limits to the number of Amazon VPC components that can be provisioned.

To increase a limit that applies per resource, increase the limit for all resources in the region.

For example: the limit for security groups per VPC applies to all VPCs in the region.

Amazon VPC

The following list show the limits for Amazon VPC resources per region for AWS account.

AWS Resource	Default Limit
1. VPCs per region	5
2. Subnet per VPC	200
3. Elastic IP addresses per region	5
4. Customer gateways per region	50
5. Internet gateway per region	5
6. NAT gateway per availability zone	5

Amazon VPC

AWS Resource	Default Limit
7. Virtual private gateways per region	5
8. Network ACLs per VPC	200
9. Network interfaces per region	350
10. Route Table per VPC	200
11. Security groups per VPC per region	500
12. Security groups per network interfaces	5
13. Active VPC peering connection per VPC	50
14. VPC endpoints per region	20
15. VPN connection per region	50



Amazon Cloudfront

CloudFront



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon CloudFront is a web service.
- Quickly distribute user content over worldwide network of data centers.
- Increasing network performance by reducing latency (time delays).
- CloudFront is compliance with **HIPAA** and **PCI DSS**

Amazon CloudFront

Amazon CloudFront is a web service that speeds up distribution of static and dynamic web content, such as .html, .css, .php, and image files, to end users.

CloudFront delivers user content through a worldwide network of data centers called [edge locations](#).

When a user requests content that is serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Amazon CloudFront

If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

If the content is not in that edge location, CloudFront retrieves it from an Amazon S3 bucket or an HTTP server (for example, a web server).

Amazon CloudFront

Amazon CloudFront Content delivering:

1. Configuring CloudFront to deliver Content.
2. How cloudFront deliver content to user?

Amazon CloudFront

- Configuring CloudFront to deliver Content:
 1. Firstly, configure your **origin servers**, from which CloudFront gets your files for distribution from CloudFront edge locations all over the world.
An origin server stores the original, definitive version of user's objects.
If user serving content over HTTP, then origin server is either an Amazon S3 bucket or an HTTP server, such as a web server.
HTTP server can run on an Amazon Elastic Compute Cloud (Amazon EC2) instance or on a server that you manage
These servers are also known as **custom origins**.

Amazon CloudFront

2. Then upload your files to your **origin servers**.

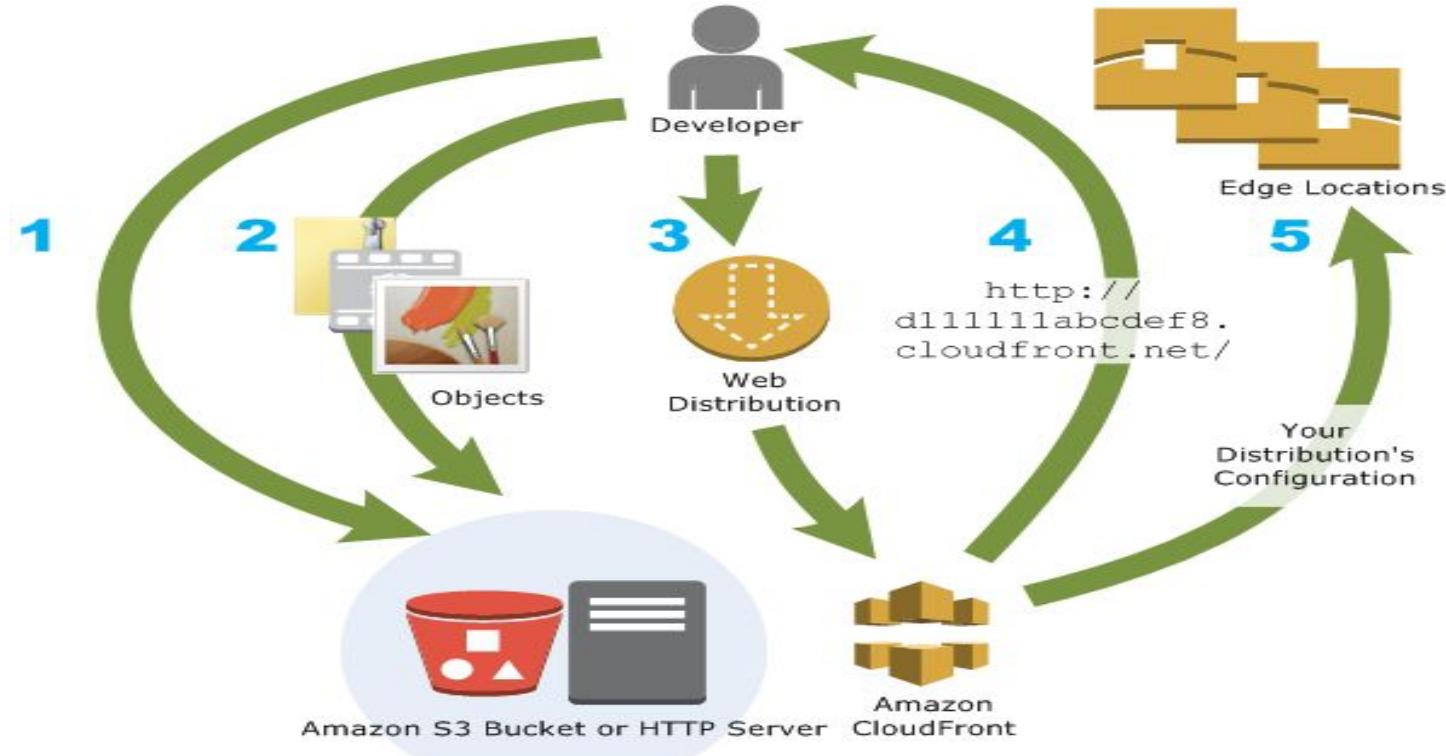
Your files, also known as **objects**, which include web pages, images, and media files, that can be served over HTTP or a supported version of Adobe RTMP, the protocol used by Adobe Flash Media Server.

3. Then create a CloudFront **distribution**, which tells CloudFront which origin servers to get your files from when users request the files through your web site or application.

Amazon CloudFront

4. CloudFront assigns a **domain name** to your new distribution and displays it in the CloudFront console or returns it in the response to a programmatic request, for example, an API request.
5. CloudFront sends your distribution's configuration (but not your content) to all of its **edge locations**—collections of servers in geographically dispersed data centers where CloudFront caches copies of your objects.

Amazon CloudFront



Amazon CloudFront

- How cloudFront deliver content to user?

After configuring CloudFront to deliver your content, what happens when users request your objects:

1. A user accesses your website or application and requests one or more objects, such as an image file and an HTML file.
2. DNS routes the request to the CloudFront edge location that can best serve the user's request, typically the nearest CloudFront edge location in terms of latency, and routes the request to that edge location.

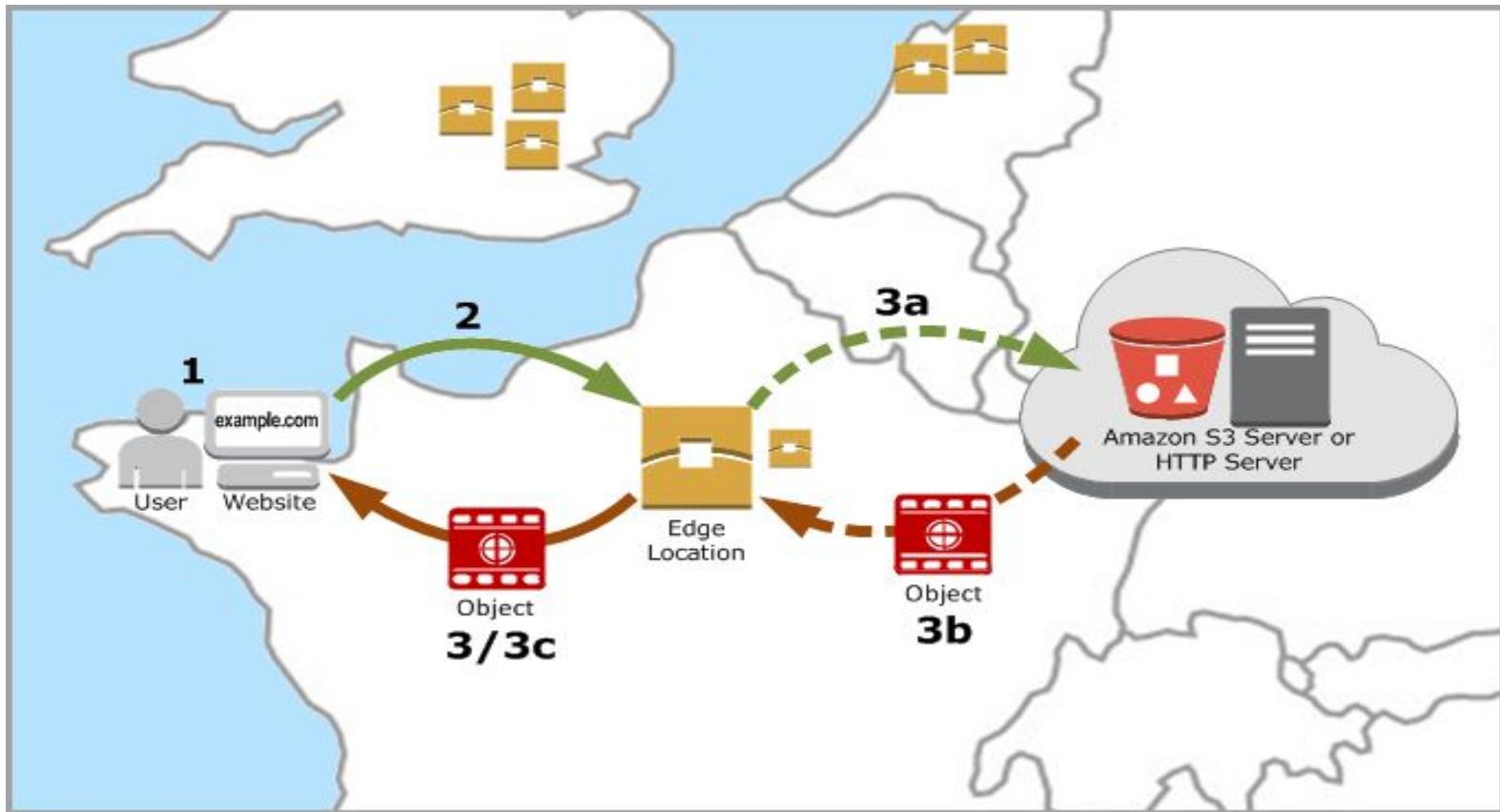
Amazon CloudFront

3. In the edge location, CloudFront checks its cache for the requested files. If the files are in the cache, CloudFront returns them to the user. If the files are *not* in the cache, it does the following:
 - a. CloudFront compares the request with the specifications in your distribution and forwards the request for the files to the applicable origin server for the corresponding file type—for example, to your Amazon S3 bucket for image files and to your HTTP server for the HTML files.

Amazon CloudFront

- b. The origin servers send the files back to the CloudFront edge location.
- c. As soon as the first byte arrives from the origin, CloudFront begins to forward the files to the user. CloudFront also adds the files to the cache in the edge location for the next time someone requests those files.

Amazon CloudFront





Amazon Cloudfront

Amazon CloudFront

CloudFront Regional Edge Caches bring more of the user content closer to the viewers.

It also stores not so popular content at a CloudFront edge location.

This helps to improve performance for viewers, while lowering the operational burden and cost of scaling origin resources.

This feature helps with all types of content, particularly content that tends to become less popular over time.

Amazon CloudFront

Features of CloudFront Regional Edge:

- There is no need to make any changes to CloudFront distributions. Regional edge caches are enabled by default for all CloudFront distributions.
- There is no additional cost for using this feature.
- Regional Edge Caches have feature parity with edge locations. For example, a cache invalidation request removes an object from both edge caches and Regional Edge Caches before it expires.

Amazon CloudFront

- Regional Edge Caches are available for custom origins. Amazon S3 origins are not supported.
- Dynamic content as determined at request time (cache-behavior configured to forward all headers) does not flow through the Regional Edge Caches, but goes directly to the origin.
- User can measure the performance improvements from this feature by using cache-hit ratio metrics available on the console.

Amazon CloudFront

Amazon Web Services (AWS) publishes its current IP address ranges in [JSON](#) format.

To view the current ranges, download the .json file.

To maintain history, save successive versions of the .json file.

Amazon CloudFront

Amazon CloudFront is Compliance with

- PCI DSS
- HIPAA

Amazon CloudFront

- PCI DSS:

The [Payment Card Industry Data Security Standard](#) (PCI DSS) is a proprietary information security standard

It is administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

CloudFront supports the processing, storage, and transmission of credit card data by a merchant or service provider and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS).

Amazon CloudFront

- HIPAA:

A large and growing number of healthcare providers, payers and IT professionals are using AWS's utility-based cloud services to process, store, and transmit **PHI (Protected health information)**.

AWS enables covered entities and their business associates subject to the U.S. **Health Insurance Portability and Accountability Act** (HIPAA).

It is used to leverage the secure AWS environment to process, maintain, and store protected health information.



AWS Direct connect

Direct Connect



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon Direct Connect links the user internal network with AWS Direct Connect location.
- Use fiber optical cable of 1 gigabit and 10 gigabit

AWS Direct Connect

AWS Direct Connect links the user internal network to an AWS Direct Connect location over a standard 1-gigabit or 10-gigabit Ethernet fiber-optic cable.

One end of the cable is connected to user's router, the other to an AWS Direct Connect router.

With this connection in place, user's can create [virtual interfaces](#) directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing Internet service providers in network path.

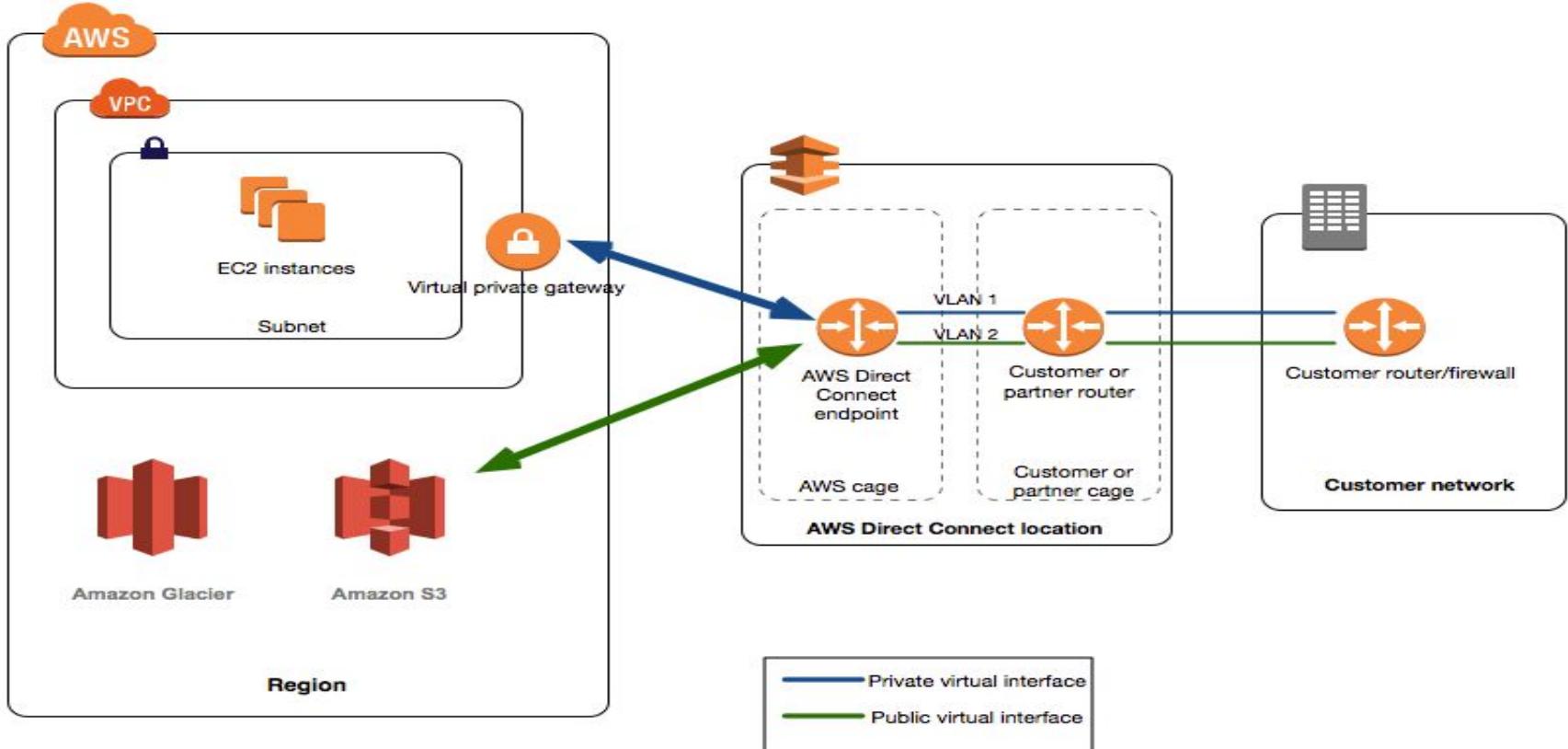
AWS Direct Connect

An AWS Direct Connect location provides access to AWS in the region with which it is associated.

User can provision a single connection to any AWS Direct Connect location in North America and use it to access public AWS services in all North America regions and AWS GovCloud (US).

Following diagram shows how AWS Direct Connect interfaces with user's network.

AWS Direct Connect



AWS Direct Connect

Key Components of AWS Direct Connect are:

- Connection
- Virtual interface

AWS Direct Connect

- Connection:

Creating a **connection** in an AWS Direct Connect location to establish a network connection between user's premises to an AWS region.

To create connection, study following information:

1. AWS Direct Connect location
2. Port speed

AWS Direct Connect

- Connection:
 1. AWS Direct Connect location

AWS Partner Network (APN) help to establish network circuits between an AWS Direct Connect location and user's data center, office, or colocation environment.

It is used to provide colocation space within the same facility as the AWS Direct Connect location.

AWS Direct Connect

- Connection:

2. Port speed:

AWS Direct Connect supports two port speeds:

1 Gbps: 1000BASE-LX (1310nm) over single-mode fiber

10 Gbps: 10GBASE-LR (1310nm) over single-mode fiber

User cannot change the port speed after created the connection request. If he/she need to change the port speed, then create and configure a new connection.

AWS Direct Connect

- Virtual Interface:

Create a [virtual interface](#) to enable access to AWS services.

A public virtual interface enables access to public-facing services, such as Amazon S3.

A private virtual interface enables access to user's VPC.

User can configure multiple virtual interfaces on a single AWS Direct Connect connection.



AWS Direct connect

AWS Direct Connect

Network Requirements for AWS Direct Connect:

To use AWS Direct Connect in an AWS Direct Connect location, user's network must meet one of the following conditions:

- User network must be collocated with an existing AWS Direct Connect location.
- User must be working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN)

AWS Direct Connect

AWS Direct Connect supports both the IPv4 and IPv6 communication protocols.

AWS Direct Connect supports a maximum transmission unit (MTU) of up to 1522 bytes at the physical connection layer .

(14 bytes ethernet header + 4 bytes VLAN tag + 1500 bytes IP datagram + 4 bytes FCS).

AWS Direct Connect

Following list shows the limits of Amazon Direct Connect:

Component	Limit
1. Virtual interfaces per AWS Direct Connect connection	50
2. Active AWS Direct Connect connections per region per account	10
3. Routes per Border Gateway Protocol (BGP) session on a private virtual interface	100

AWS Direct Connect

Component	Limit
4. Routes per Border Gateway Protocol (BGP) session on a public virtual interface	1000
5. Number of connections per link aggregation group (LAG)	4
6. Number of link aggregation groups (LAGs) per region	10



AWS Route 53

Route 53



Networking & Content Delivery

VPC

CloudFront

Direct Connect

Route 53

- Amazon Route 53 provide highly available and scalable Domain Name system (DNS)
- Translate domain names of websites or web applications into associated ip addresses.
- Reliable and cost effective service.

Amazon Route 53

Amazon Route 53 is a part of AWS which provide highly scalable and available Domain Name Server (DNS).

It provide a reliable and cost effective way to translate domain name of any website and application into its IP address.

Developer define the route to end users over internet to their application or web pages by defining domain names such as amazon.com and their associated IP address.

Amazon Route 53

It performs these functions such as

- Registering domain names
- Routing internet traffic to particular websites or applications
- Checking the health of resources (web server).

Amazon Route 53 concepts

Domain Registration concepts include:

- Domain Name
- Domain Registrar
- Domain Registry
- Domain Reseller
- Top-level Domain

Amazon Route 53 concepts

- Domain Name:

Domain Name is the name that a user types in the address bar of a web browser to access a website or a web application such as example.com.

To make your website or web application available on the Internet, you must register a domain name first.

Amazon Route 53 concepts

- Domain Registrar:

Domain Registrar is a company that is accredited by ICANN to process domain registrations for specific top-level domains (TLDs).

For example, Amazon Registrar, Inc. is a domain registrar for .com, .net, and .org domains.

Our registrar associate, Gandi, is a domain registrar for hundreds of TLDs, such as .apartments, .boutique, and .camera

Amazon Route 53 concepts

- Domain Registry:

Domain Registry is a company that owns the right to sell domains that have a specific TLDs.

A domain registry defines the rules for registering a domain and maintains the authoritative database for all of the domain names.

The registry's database contains information such as contact information and the name servers for each domain.

For example, VeriSign is the registry that owns the right to sell domains that have a .com TLD.

Amazon Route 53 concepts

- Domain Reseller:

Domain Reseller is a company that sells domain names for registrars such as Amazon Registrar.

Amazon Route 53 is a domain reseller for Amazon Registrar and for our registrar associate, Gandi.

Amazon Route 53 concepts

- Top-level Domain:

Top-level Domain refers to .com, .org, or .edu. There are two types of top-level domains:

1. Generic top-level domains
2. Geographic top-level domains

Amazon Route 53 concepts

Health Checking concepts include:

- DNS Failover
- Endpoints
- Health Check

Amazon Route 53 concepts

- DNS Failover:

DNS Failover is a method for routing traffic away from unhealthy resources and to healthy resources.

Amazon Route 53 perform health checks to check the health of user's resources and configure resource record sets in hosted zone to route traffic only to healthy resources.

Amazon Route 53 concepts

- Endpoints:

User specify the [endpoint](#) by IPv4 address (192.0.2.243), by IPv6 address (2001:odb8:85a3:0000:0000:abcd:0001:2345), or by domain name (example.com) of resources (such as web server or an email server) which are configured for health check.

User's can create health checks that monitor the status of other health checks or that monitor the alarm state of a CloudWatch alarm.

Amazon Route 53 concepts

- Health Check:

An Amazon Route 53 [health check](#) component performs these functions:

- Monitor whether a specified endpoint, such as a web server, is healthy
- Optionally, get notified when an endpoint becomes unhealthy
- Optionally, configure DNS failover, which allows you to reroute Internet traffic from an unhealthy resource to a healthy resource



AWS Route 53

Amazon Route 53

Domain Name System (DNS) concepts include:

- alias resource record set
- authoritative name server
- resource record set (DNS record)
- reusable delegation set
- subdomain
- time to live (TTL)

Amazon Route 53

- IP address
- name servers
- private DNS
- DNS query
- DNS resolver or recursive name server
- Domain Name System (DNS)
- hosted zone

Amazon Route 53

- Alias Resource set:

It is a type of resource record set that is created by user with Amazon Route 53 to route traffic to AWS resources such as Amazon CloudFront distributions and Amazon S3 buckets.

- Authoritative name server:

It is a name server that has definitive information about one part of the Domain Name System (DNS) and that responds to requests from a DNS resolver by returning the applicable information.

Amazon Route 53

- DNS query:

It a request that is submitted by a device, such as a computer or a smartphone, to the Domain Name System (DNS) for a resource that is associated with a domain name.

- DNS Resolver:

A DNS resolver is also known as a recursive name server because it sends requests to a sequence of authoritative DNS name servers until it gets the response (typically an IP address) that it returns to a user's device, for example, a web browser on a laptop computer.

Amazon Route 53

- Domain Name System (DNS):

DNS is a worldwide network of servers that help computers, smart phones, tablets, and other IP-enabled devices to communicate with one another.

- Hosted zone:

Hosted zone is a container for resource record sets, which include information about how user want to route traffic for a domain (such as example.com) and all of its subdomains (such as www.example.com, retail.example.com).

Amazon Route 53

- IP address:

IP address is a number that is assigned to a device on the Internet that allows the device to communicate with other devices on the Internet. IP addresses are in one of the following formats:

Internet Protocol version 4 (IPv4) format, such as 192.0.2.44

Internet Protocol version 6 (IPv6) format, such as
2001:odb8:85a3:0000:0000:abcd:0001:2345

Amazon Route 53

- Name servers:

Name Servers are the Servers in the DNS that help to translate domain names into the IP addresses that computers use to communicate with one another.

Name servers are either recursive name servers (also known as DNS resolver) or authoritative name servers.

Amazon Route 53

- Private DNS:

It is a local version of the DNS that lets the user to route traffic for a domain and its subdomains to Amazon EC2 instances within one or more Amazon VPCs.

- Resource Record set (DNS Record):

An object in a hosted zone that is used to define how to route traffic for the domain or a subdomain.

Amazon Route 53

- Reusable Delegation set:

It is a set of four authoritative name servers that is used with more than one hosted zone.

- Subdomain:

It is a domain name that has one or more labels prepended to the registered domain name.

Amazon Route 53

- Time to live (TTL):

TTL indicate the amount of time, in seconds, that user wants a DNS resolver to cache (store) the values for a resource record set before submitting another request to Amazon Route 53 to get the current values for that resource record set.

If the DNS resolver receives another request for the same domain before the TTL expires, the resolver returns the cached value.

Amazon Route 53

Registering Domain Names:

To create a website or a web application,

Start with by registering the name of website, known as a domain name.

Domain name is the name, such as example.com, that users enter in a browser to display their websites.

Amazon Route 53

How to register a domain name with Amazon Route 53?

1. Choose a domain name and confirm that it's available, meaning that no one else has registered with the same domain name.
2. Then Register the domain name with Amazon Route 53. When user register a domain, user must provide names and contact information for the domain owner and other contacts.

Amazon Route 53

4. When domain get registered with Amazon Route 53, the service automatically makes itself the DNS service for the domain by doing the following:
 - Creates a hosted zone that has the same name as that of domain.
 - Assigns a set of four name servers to the hosted zone. (these name servers tell the browser where to find your resources as per www.example.com, such as a web server or an [Amazon S3 bucket](#)).

Amazon Route 53

5. At the end of the registration process, AWS send user's information to the **registrar** for the domain.
6. The registrar sends user information to the **registry** for the domain.
7. The registry stores the information about user's entered domain in their own database and also stores some of the information in the public WHOIS database.

Amazon Route 53

Routing Internet traffic to particular web application or websites:

All computers on the Internet, from smartphone or laptop to the servers that serve content various websites, communicate with one another by using numbers. These numbers, known as **IP addresses** (IPv4 or IPv6).

A DNS service such as Amazon Route 53 helps to make connection between domain names of the websites and IP addresses.

Amazon Route 53

Configuring Amazon Route 53 to route internet traffic for various domain:

To route traffic to user resources, user must create **resource record sets**, also known as **records**, in hosted zone.

Each record includes information about how user want to route traffic for their domain, such as the following:

- Name
- Type
- Value

Amazon Route 53

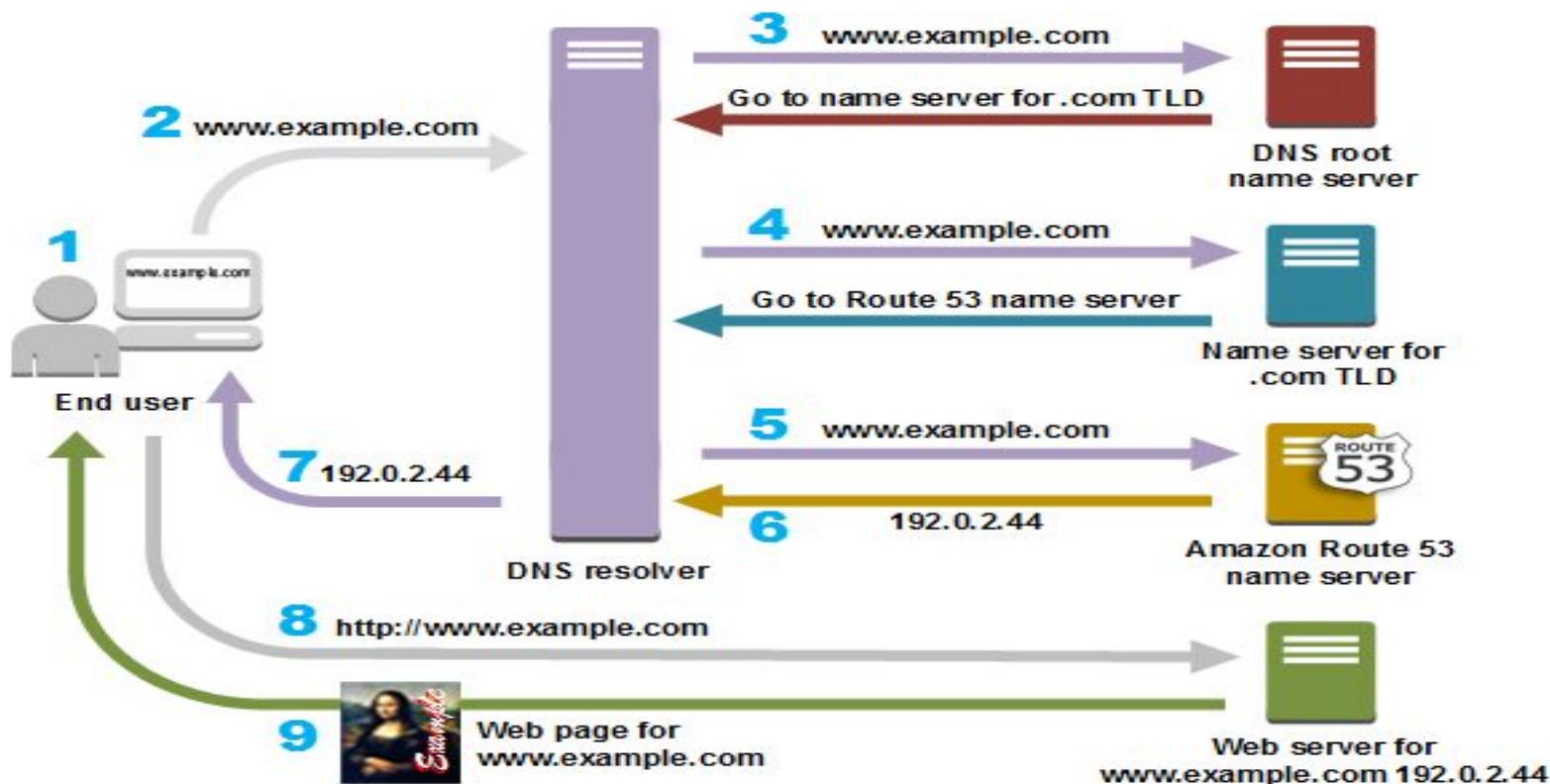
How Amazon Route 53 route traffic for particular Domain?

After configuring Amazon Route 53 to route internet traffic to particular resources such as web server or amazon S3 bucket.

Then

What happens in just a few milliseconds when someone requests content for www.example.com let see:

Amazon Route 53





AWS Route 53

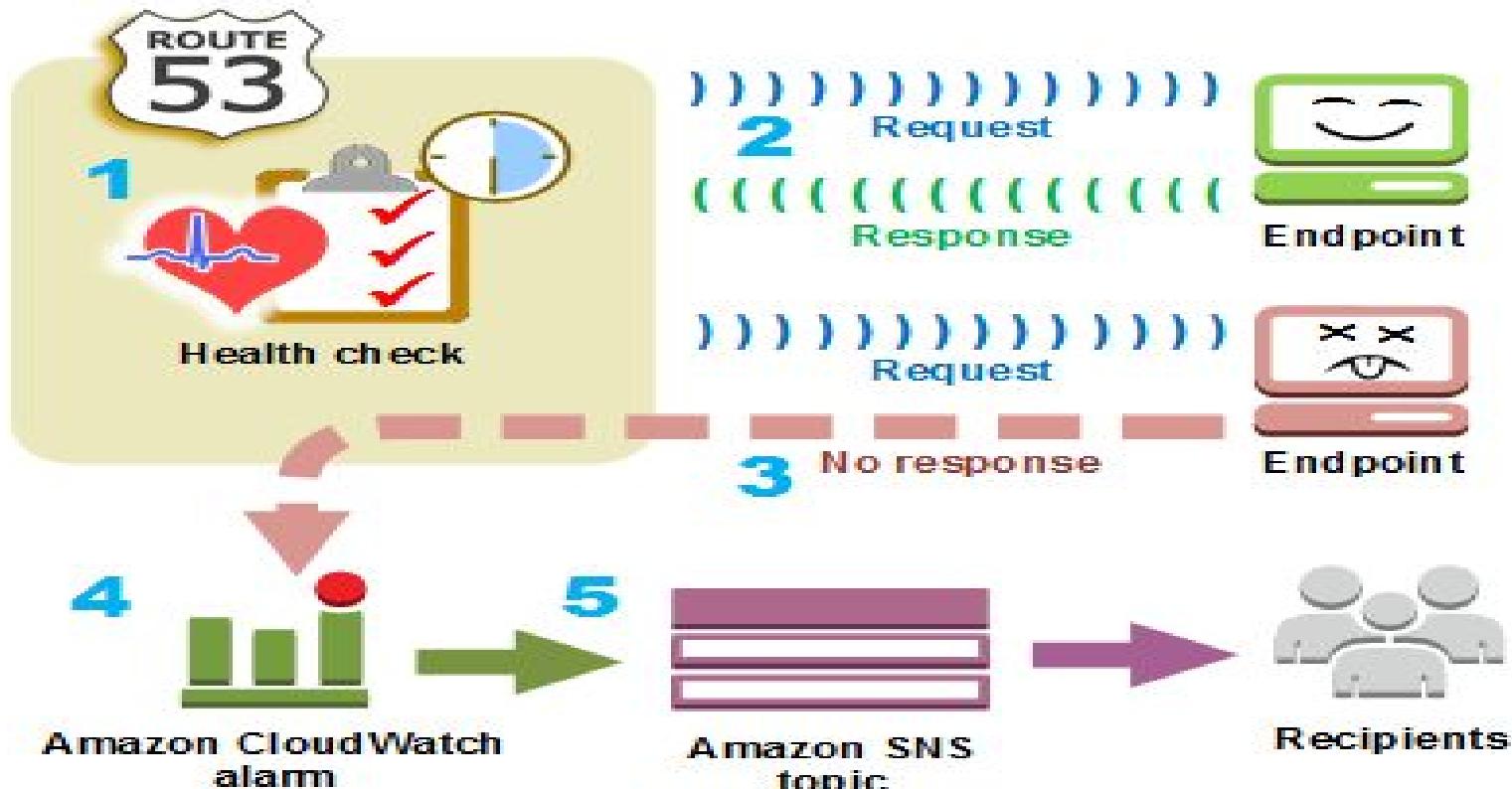
Amazon Route 53

Amazon Route 53 health checks monitor the health of user's resources such as web servers and email servers.

User's can optionally configure Amazon CloudWatch alarms for their health checks, so that they receive notification when a resource becomes unavailable.

Here's shown that how health checking works if user want to be notified when a resource becomes unavailable:

Amazon Route 53



Amazon Route 53

To create a health check then specify values that define how to check health, as following:

- Specify the IP address or domain name of the endpoint, such as a web server, that user want Amazon Route 53 to monitor.
- Specify the protocol that user want Amazon Route 53 to use to perform the check: HTTP, HTTPS, or TCP.
- Specify How often user want that Amazon Route 53 to send a request to the endpoint. This is the **request interval**.

Amazon Route 53

- Specify How many consecutive times the endpoint must fail to respond to requests before Amazon Route 53 considers it unhealthy. This is the **failure threshold**.
- Specify how user want to be notified when Amazon Route 53 detects that the endpoint is unhealthy. When user configure notification, Amazon Route 53 automatically sets a CloudWatch alarm. (CloudWatch uses Amazon SNS to notify users that an endpoint is unhealthy.) (optional)

Amazon Route 53

1. Amazon Route 53 starts to send requests to the endpoint at the interval that user specified in the health check.
2. If the endpoint responds to the requests, Amazon Route 53 considers the endpoint to be healthy and takes no action.
3. If the endpoint doesn't respond to a request, Amazon Route 53 starts to count the number of consecutive requests that the endpoint doesn't respond to:

Amazon Route 53

- If the count reaches the value that user specified for the failure threshold, Amazon Route 53 considers the endpoint unhealthy.
 - If the endpoint starts to respond again before the count reaches the failure threshold, Amazon Route 53 resets the count to 0, and CloudWatch doesn't show notification.
4. If Amazon Route 53 considers the endpoint unhealthy and if user configured notification for the health check, Amazon Route 53 notifies CloudWatch

Amazon Route 53

Amazon Route 53 can be accessed by using following interfaces:

- AWS Management Console
- AWS SDKs
- Amazon Route 53 API
- AWS CLI
- AWS tools for Windows Powershell

Amazon Route 53

Amazon Route 53 integrates with AWS Identity and Access Management (IAM) to provide following services:

- Creating users and groups under the organization's AWS account
- Easily sharing of AWS account resources among the users in the account
- Assigning unique security credentials to each user
- Granularly control user access to services and resources

Amazon Route 53

IAM and Amazon route 53 use two features to provide securities to user AWS resources:

- Authentication
- Access Control

Amazon Route 53

Authentication:

AWS IAM authenticate the AWS user who is performing various operation on Amazon Route 53 resources, such as registering a domain or updating a resource record set etc.

After authenticating the user's identity.

Access Control:

IAM controls access to AWS by verifying that user have permissions to perform operations and to access resources.



Management Tools

AWS CONSOLE

Services ▾ | Resource Groups ▾

- History
- Console Home
- Billing
- IAM
- EC2
 - DynamoDB
- Compute
 - EC2
 - EC2 Container Service
 - Lightsail ↗
 - Elastic Beanstalk
 - Lambda
 - Batch
- Storage
 - S3
 - EFS
 - Glacier
 - Storage Gateway
- Database
 - RDS
 - DynamoDB
 - ElastiCache
 - Redshift
- Networking & Content Delivery
 - VPC
 - CloudFront
 - Direct Connect
 - Route 53
- Migration
 - Application Discovery Service
 - DMS
 - Server Migration
 - Snowball
- Developer Tools
 - CodeStar
 - CodeCommit
 - CodeBuild
 - CodeDeploy
 - CodePipeline
 - X-Ray
- Management Tools
 - CloudWatch
 - CloudFormation
 - CloudTrail
 - Config
 - OpsWorks
 - Service Catalog
 - Trusted Advisor
 - Managed Services
- Security, Identity & Compliance
 - IAM
 - Inspector
 - Certificate Manager
 - Directory Service
 - WAF & Shield
 - Compliance Reports
- Analytics
 - Athena
 - EMR
 - CloudSearch
 - Elasticsearch Service
 - Kinesis
 - Data Pipeline
 - QuickSight ↗
- Application Services
 - Step Functions
 - SWF
 - API Gateway
 - Elastic Transcoder
- Messaging
 - Simple Queue Service
 - Simple Notification Service
 - SES
- Artificial Intelligence
 - Lex
 - Polly
 - Rekognition
 - Machine Learning
- Business Productivity
 - WorkDocs
 - WorkMail
 - Amazon Chime ↗
- Internet Of Things
 - AWS IoT
- Contact Center
 - Amazon Connect
- Game Development
 - Amazon GameLift
- Mobile Services
 - Mobile Hub
 - Cognito
 - Device Farm
 - Mobile Analytics
 - Pinpoint

Management Tools



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS provides fully managed services to automatically provision, configure and manage the AWS and on-premises resources.
- AWS provides a broad set of services to monitor infrastructure logs and metrics using real-time dashboards and alarms.

CloudWatch



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- Amazon CloudWatch monitors the AWS resources and services.
- It collects and tracks metrics of the resources and applications.
- CloudWatch sends notifications to users about changes occurring in resources.

Amazon CloudWatch

- Amazon CloudWatch monitors Amazon Web Services (AWS) resources and the applications that are running on AWS in real time.
- CloudWatch is used to collect and track metrics of resources and applications.
- CloudWatch alarms send notifications or automatically make changes to the resources that are monitoring based on defined rules.

Accessing Amazon CloudWatch

Methods to access Amazon CloudWatch are:

- Amazon CloudWatch console
- AWS CLI
- CloudWatch API
- AWS SDKs

Amazon CloudWatch related Services

AWS services related to Amazon CloudWatch are:

- Amazon SNS
- Auto Scaling
- AWS CloudTrail
- AWS Identity and Access Management

Amazon CloudWatch related Services

- Amazon SNS:

Amazon **Simple Notification Service** (Amazon SNS) coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

- Auto Scaling:

It is used to automatically launch or terminate Amazon EC2 instances based on user-defined policies, health status checks, and schedules.

Amazon CloudWatch related Services

- AWS CloudTrail:
It is used to monitor the calls made to the Amazon CloudWatch API for a particular account, including calls made by the AWS Management Console, AWS CLI, and other services.
- AWS Identity and Access Management (IAM):
It is a web service that helps the users to securely control access to AWS resources.

Amazon CloudWatch

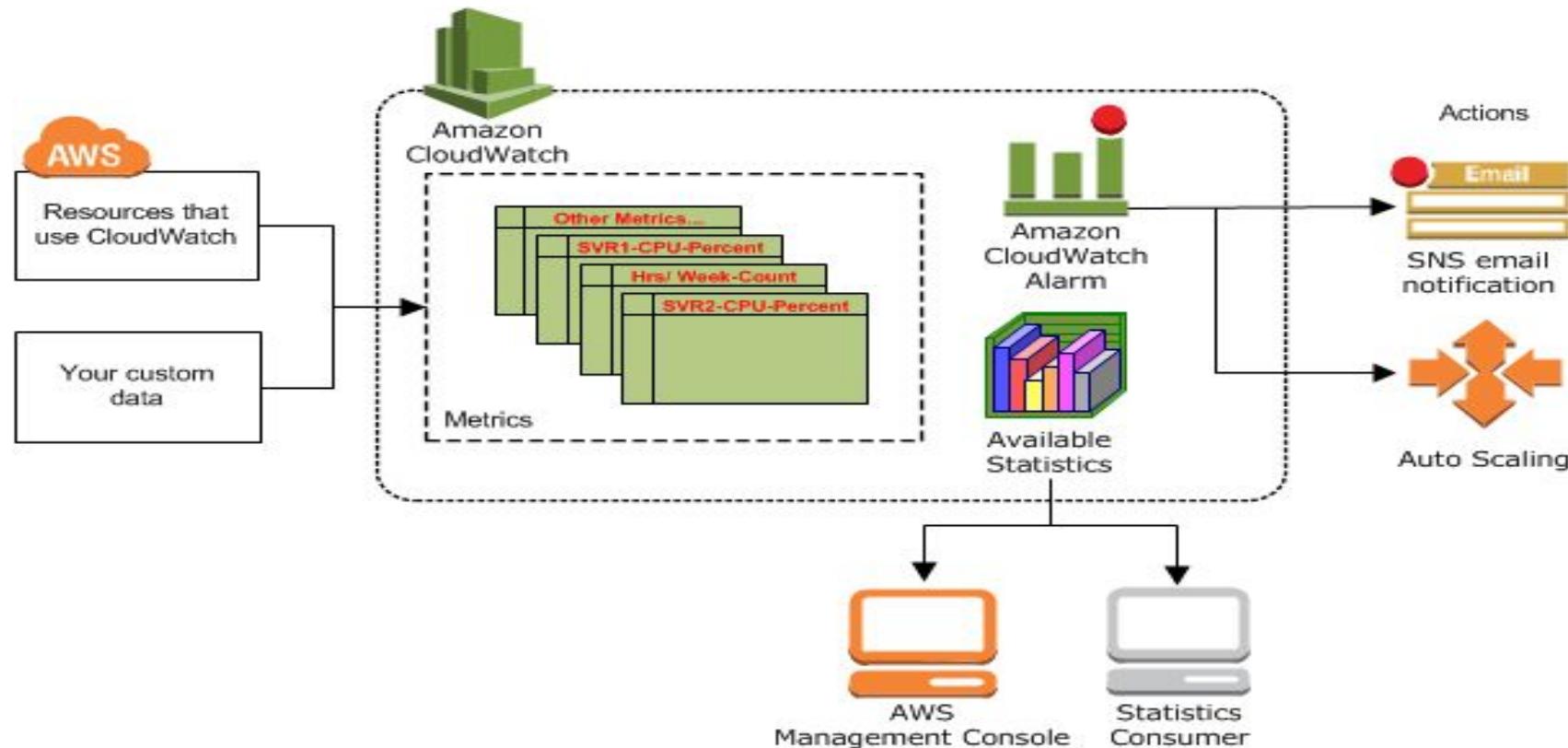
How Amazon CloudWatch Work?

Amazon CloudWatch is basically a metrics repository.

An AWS product—such as Amazon EC2—puts metrics into the repository, and user's retrieve statistics based on those metrics.

If user put their own custom metrics into the repository, then they can retrieve statistics on these metrics as well.

Amazon CloudWatch



Amazon CloudWatch

- Metrics are used to calculate statistics and then present the data graphically in the CloudWatch console.
- User's can configure alarm actions to stop, start, or terminate an Amazon EC2 instance when certain criteria are met.

Amazon CloudWatch Concept

The Amazon CloudWatch Concepts are:

- Namespace
- Metrics
- Dimensions
- Statistics
- Percentiles
- Alarms

Amazon CloudWatch Concept

- Namespace:

The namespace is the **container** for CloudWatch metrics.

Metrics in different namespaces are isolated from each other to increase fault tolerance.

There is no default namespace it means user must specify a namespace for each data point that publish to CloudWatch.

Amazon CloudWatch Concept

- Metrics:

Metrics are the **fundamental concept** in CloudWatch.

It represents a time-ordered set of data points that are published to CloudWatch.

Metrics exist only in the region in which they are created.

Metrics cannot be deleted, but they automatically expire after 15 months if no new data is published to them.

Amazon CloudWatch Concept

- Metrics:

Metrics are uniquely defined by a name, a namespace, and one or more dimensions.

Each data point has a timestamp, and a unit of measure.

Timestamp: Each metric data point must be marked with a time stamp. The time stamp can be up to two weeks in the past and up to two hours into the future.

Amazon CloudWatch Concept

- Dimensions:

A dimension is a **name/value pair** that uniquely identifies a metric.

User's can assign up to ten dimensions to a metric.

Every metric has specific characteristics that describe it.

AWS services that send data to CloudWatch attach dimensions to each metric. It is used to filter the results that CloudWatch returns.

Amazon CloudWatch Concept

- Statistics:

Statistics are **metric data aggregations** over specified periods of time.

Aggregations are made using the namespace, metric name, dimensions, and the data point unit of measure, within the time period that user's specify.

Amazon CloudWatch Concept

Statistics	Description
Minimum	The lowest value observed during the specified period
Maximum	The highest value observed during the specified period
Sum	All values submitted for the matching metric added together.
Average	The value of Sum / SampleCount during the specified period.
Samplecount	The count (number) of data points used for the statistical calculation.
pNN.NN	The value of the specified percentile.

Amazon CloudWatch Concept

- Statistics:

Units: Each statistic has a unit of measure. Example of units include Bytes, Seconds, Count, and Percent.

Periods: A period is the length of time associated with a specific Amazon CloudWatch statistic.

Aggregation: Amazon CloudWatch aggregates statistics according to the period length that is specified by user's while retrieving statistics. For large data sets, user's can insert a pre-aggregated data set called a **statistic set**.

Amazon CloudWatch Concept

- Percentiles:

A percentile indicates the **relative standing** of a value in a data set.

For example, the 95th percentile means that 95 percent of the data is below this value and 5 percent of the data is above this value.

Percentiles help to get a better understanding of the distribution of your metric data.

Amazon CloudWatch Concept

- Percentiles:

CloudWatch needs raw data points to calculate percentiles.

To retrieve percentile statistics for particular data then one of the following conditions must be true:

- The Sample Count of the statistic set is 1
- The Min and the Max of the statistic set are equal

Amazon CloudWatch Concept

- Alarms:

An alarm watches a single metric over a specified time period.

It performs one or more specified actions, based on the value of the metric relative to a threshold over time.

User's can use an alarm to automatically initiate actions on their behalf

The action is a notification sent to an Amazon SNS or an Auto Scaling policy.

Amazon CloudWatch Set up

To use Amazon CloudWatch user's must need an AWS account.

The AWS account allows users to use services (for example, Amazon EC2) to generate metrics that can be viewed in the CloudWatch console, a point-and-click web-based interface.

Steps to set up the Amazon CloudWatch service:

- Sign up for an AWS account
- Sign in to the Amazon CloudWatch console

Amazon CloudWatch Set up

To sign up for an AWS account

1. Open <https://aws.amazon.com/>, and then choose Create an AWS Account.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Amazon CloudWatch Set up

To sign in to the Amazon CloudWatch console

1. Open the CloudWatch console at
<https://console.aws.amazon.com/cloudwatch/>.
2. If necessary, use the navigation bar to change the region to the region where you have your AWS resources.
3. Even if this is the first time you are using the CloudWatch console, Your Metrics could already report metrics, because you have used a AWS product that automatically pushes metrics to Amazon CloudWatch for free.

Amazon CloudWatch Set up

4. If you do not have any alarms, the Your Alarms section will have a Create [Alarm button](#).

You can use the AWS CLI or the Amazon CloudWatch CLI to perform CloudWatch commands.



Amazon Cloudformation

CloudFormation



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS CloudFormation set up the AWS resources as per user's requirements.
- It automatically provision and configure the selected resources.
- It enables users to use a template file to create and delete a collection of resources together as a single unit (a stack).

AWS CloudFormation

- AWS CloudFormation is a service that helps to model and set up Amazon Web Services resources.
- It help users by reducing their time that spend on managing AWS resources and provide more time to focus on their applications that run in AWS.

AWS CloudFormation Features

The features of AWS CloudFormation are:

- Simplify Infrastructure Management
- Quickly replicate the users infrastructure
- Easily control and track changes to users infrastructure

AWS CloudFormation Concept

Concept of AWS CloudFormation are:

- Templates
- Stacks
- Change Sets

AWS CloudFormation Concept

Templates:

An AWS CloudFormation template is a [JSON](#) or [YAML](#) formatted text file.

Save these files with any extension, such as [.json](#), [.yaml](#), [.template](#), or [.txt](#).

AWS CloudFormation Concept

Stacks:

Using AWS CloudFormation, resources can be managed as a **single unit** called a stack.

Users can create, update, and delete a collection of resources by creating, updating, and deleting stacks.

AWS CloudFormation Concept

Change Sets:

Change set is generated as a [summary of the proposed changes](#), which is made by users to their resources.

Change sets allow users to see how the changes might impact their running resources, especially for critical resources, before implementing them.

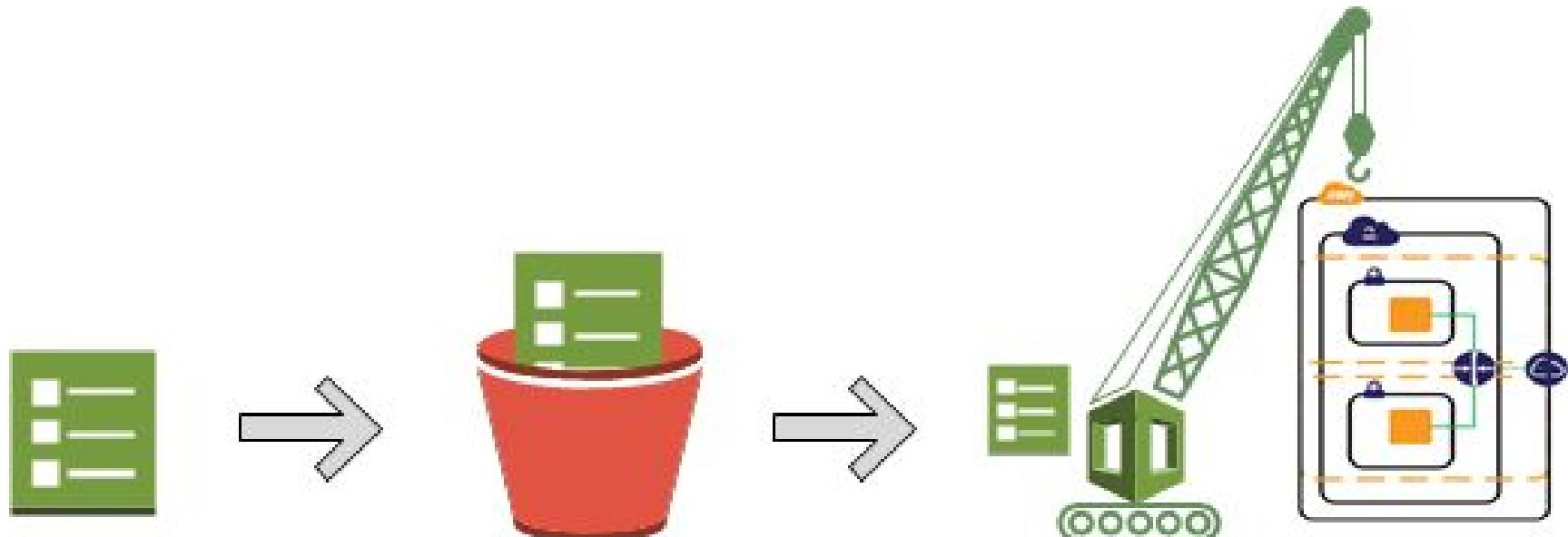
AWS CloudFormation Working

When users create a stack, AWS CloudFormation makes underlying service calls to AWS to provision and configure these resources.

AWS CloudFormation can perform only actions that are defined by users.

Users use AWS Identity and Access Management (IAM) to manage permissions.

AWS CloudFormation:



1 Create or use an existing template

2 Save locally or in S3 bucket

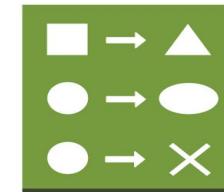
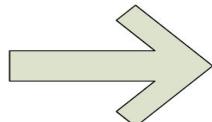
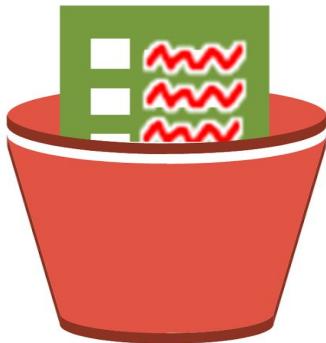
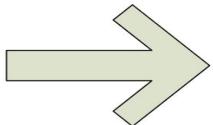
3 Use AWS CloudFormation to create a stack based on your template. It constructs and configures your stack resources.

AWS CloudFormation Working

Updating a Stack with change set:

- When there is need to update the stack's resources, then modify the stack's template.
- There is no need to create a new stack and delete the old one.

AWS CloudFormation Working

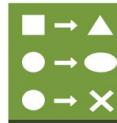
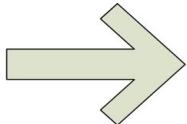
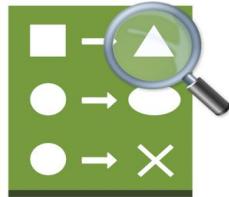
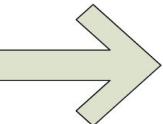


1 Edit template.

2 Save locally or
in S3 bucket.

3 Use AWS CloudFormation to
generate a change set based
on your modified template
and input parameter values.

AWS CloudFormation Working



4 View the change set, which describes the actions AWS CloudFormation performs if you execute it.

5 Execute the change set to update your stack. AWS CloudFormation performs all the changes described in the change set.

AWS CloudFormation Working

Deleting a Stack:

- When user delete a stack, AWS CloudFormation deletes the stack as well as the associated resources with that stack.
- Stacks can be deleted using the AWS CloudFormation console, API, or AWS CLI.



AWS Cloudtrail

CloudTrail



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS CloudTrail monitor the AWS deployments in the cloud by getting a history of AWS API calls for particular user account.
- CloudTrail integrates into applications using the API, automate trail creation for the organization, check the status of the trails, and control how administrators turn CloudTrail logging on and off.

AWS CloudTrail

- AWS CloudTrail is used to get a history of AWS API calls and related events for your account.
- This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.

AWS CloudTrail Working

- AWS CloudTrail captures AWS API calls and related events made by or on behalf of an AWS account.
- Then delivers these log files to an Amazon S3 bucket as user specify.
- A [trail](#) is a configuration that enables logging of AWS API calls and related events in your account.

AWS CloudTrail Working

Users can create two types of trails:

- A trail that applies to all regions
- A trail that applies to one region

For both types of trails, user can specify an S3 bucket from any region

AWS CloudTrail Workflow

- Create a trail
- Create and subscribe to an Amazon SNS
- View your log files
- Manage user permissions
- Monitor events with CloudWatch Logs
- Log management and data events
- Enable log encryption
- Enable log file integrity
- Share log files with other AWS accounts
- Aggregate logs from multiple accounts
- Work with partner solutions

AWS CloudTrail Workflow

Create a trail:

A trail enables CloudTrail to deliver log files to users Amazon S3 bucket.

By default, When users create a trail in the console, the trail applies to all regions.

The trail logs events from all regions in the AWS partition and delivers the log files to the S3 bucket that users specify.

AWS CloudTrail Workflow

Create and subscribe to an Amazon SNS:

Subscribe to a topic to receive notifications about log file delivery to your bucket.

Amazon SNS can notify user in multiple ways, including programmatically with Amazon Simple Queue Service.

AWS CloudTrail Workflow

View your log files:

Use Amazon S3 to retrieve log files.

After setting up CloudTrail to capture the log files that user wants, then user can able to find the log files and interpret the information they contain.

CloudTrail delivers the log files to an Amazon S3 bucket that is specified by the user when the trail is created.

AWS CloudTrail Workflow

Manage user permission:

User can use AWS Identity and Access Management (IAM) to manage the permissions to create, configure, or delete trails; start and stop logging; and access buckets that have log files.

AWS CloudTrail Workflow

Monitor events with CloudWatch Logs:

User can configure their own trail to send events to CloudWatch Logs.

User can then use CloudWatch Logs to monitor account for specific API calls and events.

If user configure a trail that applies to all regions to send events to a CloudWatch Logs log group, CloudTrail sends events from all regions to a single log group.

AWS CloudTrail Workflow

Enable log encryption:

Log file encryption provides an extra layer of security for the log files.

By default, the log files delivered by CloudTrail to the bucket are encrypted by [Amazon server-side encryption with Amazon S3-managed encryption keys \(SSE-S3\)](#).

To provide a security layer that is directly manageable, user can instead use [server-side encryption with AWS KMS-managed keys \(SSE-KMS\)](#) for user's CloudTrail log files.

AWS CloudTrail Workflow:

Enable log encryption:

To use SSE-KMS with CloudTrail, first create and manage a [KMS key](#), also known as a [customer master key](#) (CMK).

User attach a policy to the key that determines which users can use the key for encrypting and decrypting CloudTrail log files.

The decryption is seamless through S3.

AWS CloudTrail Workflow

Enable log file integrity

Log file integrity validation helps user to verify that log files have remained unchanged since CloudTrail delivered them.

This feature is built using industry standard algorithms: [SHA-256 for hashing](#) and [SHA-256 with RSA for digital signing](#).

AWS CloudTrail WorkFlow

Share log files with other AWS account:

Users can share their log files between accounts.

To share log files between multiple AWS accounts, the following general steps must be performed.

- Create an IAM role for each account that you want to share log files with.
- For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.

AWS CloudTrail Workflow

Share log files with other AWS account:

- Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files.

AWS CloudTrail Workflow

Aggregate logs from multiple accounts

Users can aggregate log files from multiple accounts to a single bucket.

For example, user have four AWS accounts with account ID's 111111111111, 222222222222, 333333333333, and 444444444444.

he/she wants to configure CloudTrail to deliver log files from all four of these accounts to a bucket belonging to account 111111111111.

AWS CloudTrail Workflow

Work with partner solutions

Analyzing the CloudTrail output with one of the partner solutions that is integrated with CloudTrail.

These solutions offer a broad set of capabilities, such as change tracking, troubleshooting, and security analysis.

AWS CloudTrail Concept

What is Trail?

A trail is a configuration that enables logging of the AWS API activity and related events in user's account.

CloudTrail delivers the logs to an Amazon S3 bucket that user specify, and optionally to a CloudWatch Logs log group.

Users can also specify an Amazon SNS topic that receives notifications of log file deliveries.

AWS CloudTrail Concept

Management of CloudTrail:

- CloudTrail Console
- CloudTrail CLI
- CloudTrail APIs
- AWS SDKs



AWS Cloudtrail

AWS CloudTrail Concept

Controlling Access to the CloudTrail:

AWS IAM is a web service that enables AWS customers to manage users and user permissions.

Users can use IAM to control the access to CloudTrail.

By creating individual IAM users for people accessing a single account,

AWS CloudTrail Concept

Log Management and Data Event:

When users create a trail, then user's account trail logs read-only and write-only management events.

Users can update their trail to specify whether they want their trail to log data events.

AWS CloudTrail Concept

Performing monitoring with CloudTrail: [CloudWatch Logs](#) and [CloudTrail](#)

Amazon CloudWatch is a web service that collects and tracks metrics to monitor AWS resources and the applications that run on AWS.

Amazon CloudWatch Logs is a feature of CloudWatch that users can use specifically to monitor log data.

AWS CloudTrail Concept

How does cloudTrail behave Regionally and Globally?

A trail can be applied to all regions or a single region.

Best option is, create a trail that applies to all regions in the AWS partition in which you are working.

This is the default setting when user create a trail in the CloudTrail console.

AWS CloudTrail Concept

Advantage of applying cloudTrail to all region:

- The configuration settings for the trail apply consistently across all regions.
- User can receive log files from all regions in a single S3 bucket and optionally in a CloudWatch Logs log group.
- User can manage trail configuration for all regions from one location.
- User can immediately receive events from a new region, when a new region launches

AWS CloudTrail Concept

What happen when trail is applied to all regions?

When user apply a trail to all regions, CloudTrail uses the trail that is created in a particular region to create trails with identical configuration in all other regions in user's account.

This has the following effects:

- CloudTrail delivers log files for API activity from all regions to the single Amazon S3 bucket that is specified by user, and optionally to a CloudWatch Logs log group.

AWS CloudTrail Concept

What happen when trail is applied to all regions?

- If user configured an Amazon SNS topic for the trail, SNS notifications about log file deliveries in all regions are sent to that single SNS topic.
- Global service events will be delivered from a single region to the specified S3 bucket and to CloudWatch Logs log group
- If user enabled log file integrity validation, log file integrity validation is enabled in all regions for the trail.

AWS CloudTrail Concept

Multiple trail per regions:

If user in AWS have different but related user groups such as developers, security personnel, and IT auditors etc.

Then user can create multiple trail per region. This allows each group to receive its own copy of the log files.

CloudTrail supports five trail per region.

A trail that applies to all regions counts as one trail in every region.

AWS CloudTrail Concept

AWS security Token Service (AWS STS) and CloudTrail:

AWS STS is a service that has a **global endpoint** and that also supports region-specific endpoints.

An **endpoint** is a URL that is the entry point for web service requests.

For example, <https://cloudtrail.us-west-2.amazonaws.com> is the US West (Oregon) regional entry point for the AWS CloudTrail service.

Regional endpoints help reduce latency in user applications.

When user use an AWS STS region-specific endpoint, the trail in that region delivers only the AWS STS events that occur in that region.

AWS CloudTrail Concept

Global Service Events:

For global services such as IAM, AWS STS, and Amazon CloudFront, events are delivered to any trail that includes global services.

To avoid receiving duplicate global service events, remember the following:

- Global service events are delivered to trails that have the [Apply trail to all regions](#) option enabled. (Events are delivered from a single region to the bucket for the trail.)

AWS CloudTrail Concept

Global Service Events:

- If user have a single region trail, he/she should include global services.
- If user have multiple single region trails, he/she should enable global services in only one of the trails.

When user create or update a trail with the AWS CLI, AWS SDKs, or CloudTrail API, he/she can include or exclude global service events for trails.

AWS CloudTrail Concept

How does CloudTrail relates to other AWS monitoring services?

CloudTrail adds another dimension to the monitoring capabilities already offered by AWS; it does not change or replace logging features user already using such as Amazon S3 or Amazon CloudFront subscriptions.

Amazon CloudWatch focuses on performance monitoring and system health; CloudTrail focuses on API activity.

AWS CloudTrail Supported Services

Cloudtrail support the following services:

- Additional Software and services:

AWS Marketplace: is an online store where user can buy or sell software that runs on AWS.

- Analytics:

Amazon Athena: is an interactive query service that makes it easy to analyze data directly in Amazon S3 using standard SQL.

AWS CloudTrail Supported Services

- **Analytics:**

- Amazon CloudSearch

- Amazon EMR

- AWS Data Pipeline

AWS CloudTrail Supported Services

- **Analytics:**

- Amazon Kinesis Firehose

- Amazon Kinesis Streams

- Amazon Quick Sight

AWS CloudTrail Supported Services

- Application Services:

- Amazon API Gateway

- Amazon Elastic Transcoder

- Amazon Elasticsearch Service

AWS CloudTrail Supported Services

- Application Services:

Amazon Simple Workflow Service

AWS Step Functions

AWS CloudTrail Supported Services

- Artificial Intelligence:

Amazon Machine Learning: makes it easy for developers to build smart applications, including applications for fraud detection, demand forecasting, targeted marketing, and click prediction.

Amazon Polly: is a service that converts text into lifelike speech. Amazon Polly is used to develop applications that increase engagement and accessibility.

AWS CloudTrail Supported Services

- Business Productivity:

Amazon WorkDocs: is a fully managed enterprise storage and sharing service. Users files are stored in the cloud safely and securely.

- Game Development:

Amazon Game Lift is a fully managed service for deploying, operating, and scaling session-based multiplayer game servers in the cloud.

AWS CloudTrail Supported Services

- Compute:

Application Auto Scaling: can automatically scale the AWS resources.

Auto Scaling: is a web service that enables the user to automatically launch or terminate Amazon Elastic Compute Cloud (Amazon EC2) instances based on user-defined policies, health status checks, and schedules.

Amazon EC2 Container Registry (Amazon ECR): is a secure and scalable managed AWS Docker registry service.

AWS CloudTrail Supported Services

- Compute:

Amazon EC2 Container Service (Amazon ECS): is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster of Amazon EC2 instances.

Elastic Beanstalk: is used to quickly deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications.

Amazon EC2 (Amazon EC2) provides resizable computing capacity in the AWS cloud.

AWS CloudTrail Supported Services

- Compute:

Elastic Load Balancing: is used to automatically distribute user's incoming application traffic across multiple Amazon EC2 instances.

AWS Lambda: is a zero-administration compute platform that runs their code in the AWS Cloud, providing the high availability, security, performance, and scalability of AWS infrastructure.

Amazon Lightsail helps developers quickly get started with virtual private servers.

AWS CloudTrail Supported Services

- Database:

Amazon DynamoDB: is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.

Amazon ElastiCache: is a web service that makes it easy to set up, manage, and scale distributed in-memory cache environments in the cloud.

AWS CloudTrail Supported Services

- Database:

Amazon Redshift: is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all data by using the existing business intelligence tools.

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

AWS CloudTrail Supported Services

- Desktop and app streaming:

Amazon WorkSpaces offers an easy way to provide a cloud-based desktop experience to your end-users.

- Internet of Things:

AWS IoT provides secure, bidirectional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud.

AWS CloudTrail Supported Services

- **Developer tools:**

AWS CodeBuild: is a fully managed build service in the cloud. AWS CodeBuild compiles your source code, runs unit tests, and produces artifacts that are ready to deploy.

AWS CodeCommit: is a version control service hosted by AWS that is used to privately store and manage assets (such as documents, source code, and binary files) in the cloud.

AWS CloudTrail Supported Services

- Developer tools:

AWS CodeDeploy: is a deployment service that enables developers to automate the deployment of applications to Amazon EC2 instances, and to update the applications as required.

AWS CodePipeline: is a continuous delivery and automation service hosted by Amazon Web Services that enables you to model, configure, and automate the steps required to release the software.

AWS CloudTrail Supported Services

- Management Tools:

AWS Application Discovery Service: helps to plan application migration projects by automatically identifying servers, virtual machines (VMs), software, and software dependencies running in user on-premises data centers.

AWS CloudFormation is used to create and provision AWS infrastructure deployments predictably and repeatedly.

AWS CloudTrail: is used to get a history of AWS API calls and related events for your account.

AWS CloudTrail Supported Services

- Management Tools:

Amazon CloudWatch: monitors the user's AWS resources and the applications that run on AWS.

Amazon CloudWatch Events: delivers a timely stream of system events that describe changes in AWS resources to AWS Lambda functions, streams in Amazon Kinesis Streams, Amazon SNS topics, or built-in targets.

Amazon CloudWatch Logs: monitors, stores, and accesses their log files from Amazon EC2 instances, AWS CloudTrail, and other sources.

AWS CloudTrail Supported Services

- Management Tools:

AWS Config: provides a detailed view of the resources associated with user's AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.

AWS Managed Services: provides ongoing management of AWS infrastructure so user can focus on their applications. AWS Managed Services helps to reduce the operational overhead and risk.

AWS CloudTrail Supported Services

- Management Tools:

AWS OpsWorks: provides a simple and flexible way to create and manage stacks and applications.

AWS OpsWorks for Chef Automate: is used to run a Chef Automate server in AWS. it is used to provision a Chef server within minutes, and let AWS OpsWorks Stacks to handle its operations, backups, restorations, and software upgrades.

AWS CloudTrail Supported Services

- Management Tools:

AWS Service Catalog: allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

AWS CloudTrail Supported Services

- **Messaging:**

Amazon Simple Email Service: is an outbound-only email-sending service that provides an easy, cost-effective way for you to send email.

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

Amazon Simple Queue Service (Amazon SQS): offers reliable and scalable hosted queues for storing messages as they travel between computers.

AWS CloudTrail Supported Services

- Migration:

AWS Database Migration Service (AWS DMS): can migrate the user data to and from most widely used commercial and open-source databases such as Oracle, PostgreSQL, Microsoft SQL Server, Amazon Aurora, MariaDB, and MySQL.

AWS Server Migration Service (AWS SMS): automates the migration of on-premises VMware virtual machines to the AWS Cloud and Amazon EC2.

AWS CloudTrail Supported Services

- Mobile Services:

Amazon Cognito: is a service that is used to create unique identities for users, authenticate these identities with identity providers, and save mobile user data in the AWS Cloud.

AWS Device Farm: is an app testing service that is used to test the Android and Fire OS apps on real, physical phones and tablets that are hosted by AWS.

AWS CloudTrail Supported Services

- **Networking and Content Delivery:**

Amazon CloudFront: speeds up distribution of user's static and dynamic web content to end users.

AWS Direct Connect: is used to establish a direct connection from user's premises to AWS. This may reduce user's network costs and increase bandwidth throughput.

Amazon Route 53: is a Domain Name System (DNS) and domain name registration web service.

AWS CloudTrail Supported Services

- **Networking and Content Delivery:**

Amazon Virtual Private Cloud (Amazon VPC): is used to launch AWS resources into a virtual network that is defined by user.

AWS CloudTrail Supported Services

- Security, Identity and compliance:

AWS Security Manager: handles the complexity of provisioning, deploying, and managing certificates provided by ACM (ACM Certificates) for AWS-based user's websites and applications.

Amazon Cloud Directory is a highly scalable, high performance, multi tenant directory service in the cloud.

AWS CloudHSM: provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud.

AWS CloudTrail Supported Services

- Security, Identity and compliance:

AWS Directory Service: is a managed service that makes it easy for the user to connect their existing on-premises Microsoft Active Directory and deploy and manage Windows workloads in the AWS cloud.

AWS Identity and Access Management (IAM): is a web service that enables AWS customers to manage users and user permissions.

Amazon Inspector: is used to analyze the behavior of user's AWS resources and helps them to identify potential security issues.

AWS CloudTrail Supported Services

- Security, Identity and compliance:

AWS Key Management Service: is a managed service used to create and control the encryption keys to encrypt the data.

AWS Security Token Service (AWS STS): is used to grant a trusted user temporary, limited access to the user's AWS resources.

AWS WAF: is a web application firewall that monitors the HTTP and HTTPS requests that are forwarded to Amazon CloudFront and lets users to control access to their content.

AWS CloudTrail Supported Services

- Storage:

Amazon Elastic Block Store (Amazon EBS): allows the user to create persistent storage volumes and attach them to Amazon EC2 instances.

Amazon Elastic File System (Amazon EFS): is a file storage service for Amazon Elastic Compute Cloud (Amazon EC2) instances.

Amazon Glacier: is a storage service optimized for data archiving and backup of infrequently used data. The service is durable, extremely low-cost, and includes security features.

AWS CloudTrail Supported Services

- Storage:

Amazon Simple Storage Service (Amazon S3): is used to store and retrieve any amount of data at any time, from anywhere on the web. CloudTrail logs are used together with Amazon S3 server access logs.

AWS Storage Gateway: is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between user's on-premises IT environment and the AWS storage infrastructure in the cloud.

AWS CloudTrail Supported Services

- **Support:**

AWS Personal Health Dashboard: provides ongoing visibility into the state of user AWS resources, services, and accounts.

AWS Support: offers a range of plans that provide access to tools and expertise that support the success and operational health of AWS solutions. All support plans provide 24x7 access to customer service, AWS documentation, whitepapers, and support forums.



AWS Config

Config



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS Config provides a detailed view of the resources associated with your AWS account, including
 - how they are configured,
 - how they are related to one another, and
 - how the configurations and their relationships have changed over time.

AWS Config

- AWS Config provides a detailed view of the configuration of AWS resources in the AWS account.
- This includes how the resources are related to one another and how they were configured in the past so that user can see how the configurations and relationships change over time.

AWS Config Functions

- Evaluate the user AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with user AWS account.
- Retrieve configurations of one or more resources that exist in user account.

AWS Config Usage

AWS Config is used to oversee the application resources in following scenarios:

- Resource Administration
- Auditing and Compliance
- Managing and troubleshooting configuration changes
- Security Analysis



AWS opsWorks

OpsWorks



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS OpsWorks provides a simple and flexible way to create and manage stacks and applications.
- With AWS OpsWorks, user can provision AWS resources, manage their configuration, deploy applications to those resources, and monitor their health.

AWS OpsWorks

- AWS OpsWorks is a configuration management service that helps user configure and operate applications in a cloud enterprise by using Chef.
- AWS OpsWorks Stacks and AWS OpsWorks for Chef Automate let the user use Chef cookbooks and solutions for configuration management.

AWS OpsWorks Services

AWS OpsWorks for Chef Automate:

AWS OpsWorks for Chef Automate is used to create AWS-managed Chef servers that include Chef Automate premium features, and the Chef DK (Development Kit) and other Chef tooling to manage them.

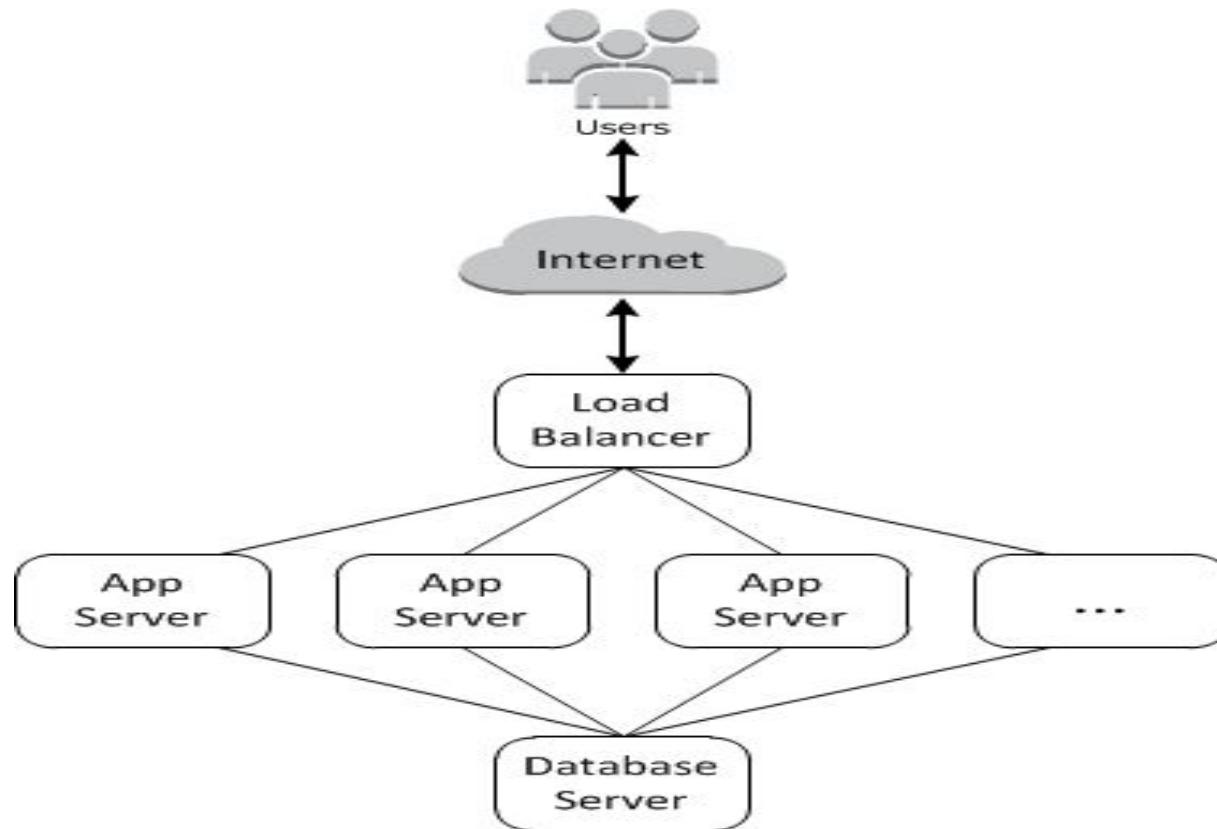
AWS OpsWorks Services

AWS OpsWorks Stacks

Cloud-based computing usually involves groups of AWS resources, such as EC2 instances and Amazon RDS instances.

For example, a web application typically requires application servers, database servers, load balancers, and other resources. This group of instances is typically called a stack.

AWS OpsWorks Services





AWS Service Catalog

Service Catalog



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

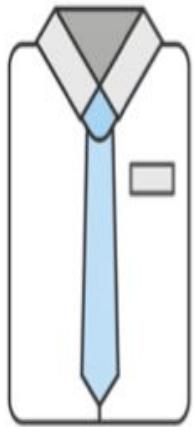
Managed Services

- AWS Service Catalog allows IT administrators to create, manage, and distribute portfolios of approved products to end users.
- Users can access these products which they need through their personalized portal.

AWS Service Catalog

- AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS.
- These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

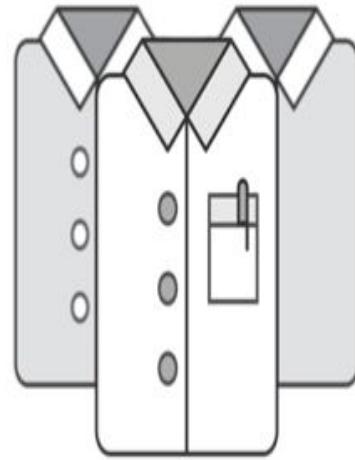
AWS Service Catalog



Control
Standardization
Governance



Agility
Self-service
Time to market



Administrator

End Users

AWS Service Catalog

AWS Service Catalog provides the following benefits:

- Promote standardization
- Self-service discovery and launch
- Fine-grain access controls of configuration and provisioning
- Extensibility and version control

AWS Service Catalog Component

- AWS Service Catalog users
- Portfolio
- Product
- Provisioned Product
- AWS CloudFormation Stack
- Versioning
- Permissions
- Constraints

AWS Service Catalog Component

AWS Service Catalog users:

AWS Service Catalog users are of following types, depending on the level of permissions that they have:

Catalog administrators (administrators) – Manage a catalog of products (applications and services), organizing them into portfolios and granting access to end users.

End users – Receive AWS credentials from their IT department or manager and use the AWS Management Console to launch products to which they have been granted access.

AWS Service Catalog Component

Portfolio:

A portfolio is a collection of products, together with configuration information.

Portfolios help manage who can use specific products and how they can use them.

When user add a new version of a product to a portfolio, that version is automatically available to all current users.

AWS Service Catalog Components

Product:

A product is an IT service that user want to make available for deployment on AWS.

A product can comprise one or more AWS resource, such as EC2 instances, storage volumes, databases, monitoring configurations, and networking components, or packaged AWS Marketplace products.

A product can be a single compute instance running AWS Linux, a fully configured multi-tier web application running in its own environment, or anything in between.

AWS Service Catalog Components

Provisioned Product:

When an end user launches a product, an instance of the product is created and is using resources.

Most commonly, a provisioned product is an AWS CloudFormation stack.

AWS Service Catalog Components

AWS CloudFormation Stack:

AWS CloudFormation stacks is used to manage the lifecycle of user's product by allowing them to provision, tag, update, and terminate their product instance as a single unit.

An AWS CloudFormation stack includes an AWS CloudFormation template, written in either JSON or YAML format, and its associated collection of resources.

A provisioned product in AWS Service Catalog is most commonly a stack.

AWS Service Catalog Components

Versioning:

AWS Service Catalog allows user to manage multiple versions of the products in their catalog.

This allows user to add new versions of templates and associated resources based on software updates or configuration changes.

Users can update running instances of the product to the new version quickly and easily.

AWS Service Catalog Components

Permissions:

Granting a user access to a portfolio enables that user to browse the portfolio and launch the products in it.

User apply AWS IAM permissions to control who can view and modify their catalog.

IAM permissions can be assigned to IAM users, groups, and roles.

When a user launches a product that has an IAM role assigned to it, AWS Service Catalog uses the role to launch the product's cloud resources using AWS CloudFormation.

AWS Service Catalog Components

Constraints:

Constraints control the ways that specific AWS resources can be deployed for a product.

User can use them to apply limits to products for governance or cost control.

There are two distinct types of AWS Service Catalog constraints:
template and **launch**.



AWS Trusted Advisor

Trusted Advisor



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS support provides support for users of Amazon Web Services.
- All users have access to account and billing help in the AWS Support Center.

AWS Support

- AWS Support offers a range of plans that provide access to tools and expertise that support the success and operational health of the AWS solutions.
- All support plans provide 24x7 access to customer service, AWS documentation, whitepapers, and support forums.

AWS Support Features

AWS Support offers four support plans:

- Basic
- Developer
- Business
- Enterprise

AWS Support Features

All AWS customers automatically have around-the-clock access to these features of the Basic support plan:

- Customer Service: one-on-one responses to account and billing questions
- Support forums
- Service health checks
- Documentation, whitepapers, and best-practice guides

AWS Support Case Management

User can sign in to the Support Center at

<https://console.aws.amazon.com/support/home#/> by using the email address and password associated with their AWS account.

There are three types of cases you can open:

- Account and Billing
- Service Limit Increase
- Technical Support

AWS Trusted Advisor

- AWS Trusted Advisor draws upon best practices learned from the aggregated operational history of serving hundreds of thousands of AWS customers.
- Trusted Advisor inspects user AWS environment and makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps.



AWS Managed Services

Managed Services



Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Trusted Advisor

Managed Services

- AWS Managed services include AWS Health check.
- AWS Health provides personalized information.

Managed Services

AWS Health:

AWS Health provides ongoing visibility into the state of the AWS resources, services, and accounts.

AWS Health provides relevant and timely information to help to manage events in progress, as well as be aware of and prepare for planned activities.

AWS Management Console

- The AWS Management Console is a web application for managing Amazon Web Services.
- The console provides an intuitive user interface for performing many AWS tasks such as working with Amazon S3 buckets, launching and connecting to Amazon EC2 instances, setting Amazon CloudWatch alarms, and so on.

AWS Command Line Interface

- The AWS CLI is an open source tool built on top of the AWS SDK for Python (Boto) that provides commands for interacting with AWS services.
- With less configuration, user can start using all of the functionality provided by the AWS Management Console using terminal program such as.
 - Linux shells
 - Windows command line
 - Remotely

AWS Tools for Windows Powershell

- The AWS Tools for Windows PowerShell and AWS Tools for PowerShell Core are PowerShell modules that are built on the functionality exposed by the AWS SDK for .NET.
- The AWS Tools for Windows PowerShell and AWS Tools for PowerShell Core are flexible in how they enable the user to handle credentials including support for the AWS IAM infrastructure.

Cloud Computing

Cloud computing is a type of **internet based computing** which provide the delivery of hosted services over the internet

It provide a network of remote servers to store, manage and process data over the internet.

Companies offering these computing services are called **cloud providers** and they charge for cloud computing services based on usage.

Example: Microsoft Window Azure, Amazon web services, Huawei Galax
cloud etc

Cloud Computing



Cloud Computing

Cloud Services

Cloud services are broadly divided into three categories:

1. Cloud Software as a Service (SaaS)
2. Cloud Platform as a Service (PaaS)
3. Cloud Infrastructure as a Service (IaaS)

These three models are independent of each other.

Cloud Computing

Cloud Software as a Service (SaaS)

Software as a service is a way of delivering applications over the Internet—as a service. The users manages access to the application, including security, availability, and performance.

SaaS customers have no hardware or software to buy, install, maintain or update.

Access to applications is easy by having internet connection.

Example: Google Apps, Salesforce, Workday, Cisco WebEx.

Cloud Computing

Cloud Platform as a Service (PaaS)

In Platform as a Service model, a cloud provider delivers hardware and software tools as a service to their users which are used for application development. A PaaS provider hosts the hardware and software on its own infrastructure.

PaaS allow developers to frequently change or upgrade operating system features. users access PaaS through a Web browser. PaaS charge for that access on a per-use basis or as a monthly fee for the access to platform.

Cloud Computing

Cloud Platform as a Service (PaaS)

Example of PaaS vendors are Salesforce.com's Force.com, Google and Amazon.

PaaS platforms for development and management of software are Appear IQ, Amazon Web Services (AWS) Elastic Beanstalk, Google App Engine.

Cloud Computing

Cloud Infrastructure as a Service (IaaS)

This cloud offer infrastructure resources such as hardware, software, server and storage.

Users can use these resources over internet and deploy application on them.

IaaS platforms offer highly scalable resources that can be adjusted on-demand.

Example: Amazon Web Services (AWS), Windows Azure, Google Compute Engine.

Cloud Computing

Advantages of Cloud Computing Services

1. Reduced Capital Cost
2. Device and Location independence
3. Scalability and Elasticity
4. Agility
5. Maintenance

Cloud Computing

Cloud Computing deployment models are

1. Cloud-based deployments
2. Hybrid deployments

Cloud Computing

Cloud-based deployment:

A cloud-based application is fully deployed in the cloud

All parts of the application run in the cloud.

Applications have either been created in the cloud or have been migrated from an existing infrastructure

This migration is done to take advantage of the benefits of cloud computing. It can be built on low-level infrastructure pieces or can use higher level services.

Cloud Computing

Hybrid deployment:

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources (that are not located in the cloud).

It is used to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to internal system.

Features of Cloud Computing

- On demand computing resources
- Elastic resources—Scale up or down quickly and easily to meet demand
- Metered service so you only pay for what you use
- Self service—All the IT resources you need with self-service access

Cloud infrastructure as a service

In the 2016 Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, for the 6th straight year, Gartner placed Amazon Web Services in the “Leaders” quadrant and named AWS as having both the furthest completeness of vision and the highest ability to execute.

Figure 1. Magic Quadrant for Cloud Infrastructure as a Service, Worldwide





Elastic Load Balancing

Elastic Load Balancing:

- Elastic Load balancing is a web service which distributes the application traffic across multiple EC2 instances within multiple Availability Zone.
- It is used to increase the fault tolerance of users applications.
- There are two type of load balancer such as: **Application Load Balancer** and **Classic Load Balancer**.

Elastic Load Balancing

- Elastic Load Balancing distributes incoming application traffic across multiple EC2 instances, in multiple Availability Zones.
- This increases the fault tolerance of user's applications.
- The load balancer serves as a single point of contact for clients

Elastic Load Balancing

- User's can configure health checks, which are used to monitor the health of the registered instances so that the load balancer can send requests only to the healthy instances.
- User's can also offload the work of encryption and decryption to their load balancer so that their instances can focus on their main work.

Elastic Load Balancing

Elastic Load Balancing supports two types of load balancers:

- Application Load Balancers
- Classic Load Balancers

load balancer can be choosed, according to the need of user's.

Elastic Load Balancing

Features	Classic Load Balancer	Application Load Balancer
Protocols	HTTP, HTTPS, SSL, TCP	HTTP, HTTPS
Platforms	EC2-Classic, EC2-VPC	EC2-VPC
Sticky Session	--	Load Balancer generated
Idle Connection Timeout	--	--
Connection Draining	--	--

Elastic Load Balancing

Features	Classic Load Balancer	Application Load Balancer
Health Check	--	Improved
Access Logs	--	Improved
HTTP/2 Support		--
Host-based Routing		--
Path-based Routing		--

Elastic Load Balancing

User's can create, access and manage their own load balancer using any of the following interfaces:

- AWS Management Console
- AWS Command Line interface (AWS-CLI)
- AWS SDKs
- Query API

Elastic Load Balancing

- AWS Management Console

Provides a web interface that can be used to access Elastic Load Balancing.

- AWS Command Line Interface (AWS CLI)

Provides commands for a broad set of AWS services, including Elastic Load Balancing

It is supported on Windows, Mac, and Linux.

Elastic Load Balancing

- AWS SDKs

Provides language-specific APIs

Also manage the connection details, such as calculating signatures, handling request retries, and error handling.

- Query API

Provides low-level API actions using HTTPS requests.

It provides the direct way to access Elastic Load Balancing, but it requires that user's application must handle low-level details such as generating the hash to sign the request, and error handling.

Elastic Load Balancing

Elastic load balancing works with these services to increase the availability and scalability of user's application:

- Amazon EC2
- Amazon ECS
- Amazon Route 53
- Amazon CloudWatch
- Autoscaling

Elastic Load Balancing

- Amazon EC2

Provide virtual servers to run user's application in cloud.

User's can configure their own load balancer to route the traffic to their EC2 instance.

- Amazon ECS

It Enables user's to run, stop, and manage their Docker containers on a cluster of EC2 instances.

User's can configure their load balancer to route traffic to their containers.

Elastic Load Balancing

- Amazon Route 53

It provide reliable and cost effective way to route viewer to websites by translating their domain names into their corresponding IP addresses.

AWS assign their URLs to their resources i.e. to load balancer.

Amazon Route 53 help to get a website or web application up and running.

Elastic Load Balancing

- Amazon CloudWatch

It enables user's to monitor their load balancer and take action as needed.

For example, user's can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use this data to determine whether to launch additional instances to handle increased load or not.

Elastic Load Balancing

- Autoscaling

If user's enable Auto Scaling with Elastic Load Balancing

Then instances that are launched by Auto Scaling are automatically registered with the load balancer.

The instances that are terminated by Auto Scaling are automatically de-registered from the load balancer.

Elastic Load Balancing

How Elastic Load Balancing Works ?

- A load balancer accepts incoming traffic from **clients** and routes requests to its registered EC2 instances in one or more **Availability Zones**.
- Then load balancer monitors the health of its registered instances and routes traffic only to healthy instances.

Elastic Load Balancing

- User's can configure their load balancer by specifying one or more **listeners** to accept incoming traffic.
- A **listener** is a process that checks for connection requests.
- It is configured with a protocol and port number for connections from clients to the load balancer and a protocol and port number for connections from the load balancer to the instances.

Elastic Load Balancing

Elastic Load Balancing support two type of Load balancer:

- Classic Load Balancer :
registers the instances to the load balancer
- Application Load Balancers :
registers the instance as a target in a target group and route traffic to a target group.

END!

We wish you Best of Luck for your AWS Certification Exam

OUR TRAININGS ARE AVAILABLE WORLDWIDE FOR INDIVIDUALS AND CORPORATES

Afghanistan	Burundi	Eritrea	Jamaica	Mauritania	Philippines	Sweden
Albania	Cambodia	Estonia	Japan	Mauritius	Poland	Switzerland
Algeria	Cameroon	Ethiopia	Jordan	Mexico	Portugal	Syria
Andorra	Canada	Fiji	Kazakhstan	Micronesia	Qatar	Taiwan
Angola	Cabo Verde	Finland	Kenya	Moldova	Russia	Tajikistan
Antigua & Barbuda	Central African Republic	France	Kiribati	Monaco	Rwanda	Tanzania
Argentina	Chad	Gabon	Korea, North	Mongolia	Saint Kitts & Nevis	Thailand
Armenia	Chile	Gambia, The	Korea, South	Montenegro	Saint Lucia	Timor-Leste
Aruba	China	Georgia	Kosovo	Morocco	Saint Vincent Samoa	Togo
Australia	Colombia	Germany	Kuwait	Mozambique	San Marino	Tonga
Austria	Comoros	Ghana	Kyrgyzstan	Namibia	Sao Tome & Principe	Trinidad and
Azerbaijan	Congo, DR of the	Greece	Laos	Nauru	Saudi Arabia	Tobago
Bahamas, The	Congo, R of the	Grenada	Latvia	Nepal	Senegal	Tunisia
Bahrain	Costa Rica	Guatemala	Lebanon	Netherlands	Serbia	Turkey
Bangladesh	Cote d'Ivoire	Guinea	Lesotho	New Zealand	Seychelles	Turkmenistan
Barbados	Guinea-Bissau	Liberia	Nicaragua	Nicaragua	Sierra Leone	Tuvalu
Belarus	Croatia	Guyana	Libya	Niger	Singapore	Uganda
Belgium	Cuba	Haiti	Liechtenstein	Nigeria	Sint Maarten	Ukraine
Belize	Curacao	Holy See	Lithuania	North Korea	Slovakia	United Arab Emirates
Benin	Cyprus	Honduras	Luxembourg	Norway	Slovenia	United Kingdom
Bhutan	Czechia	Hong Kong	Macau	Oman	Solomon Islands	Uruguay
Bolivia	Denmark	Hungary	Macedonia	Pakistan	Somalia	Uzbekistan
Bosnia & Herzegovina	Djibouti	Iceland	Madagascar	Palau	South Africa	Vanuatu
Botswana	Dominica	India	Malawi	Palestinian Territories	South Korea	Venezuela
Brazil	Dominican Republic	Indonesia	Malaysia	Territories	South Sudan	Vietnam
Brunei	East Timor	Iran	Maldives	Panama	Spain	Yemen
Bulgaria	Ecuador	Iraq	Mali	Papua New Guinea	Sri Lanka	Zambia
Burkina Faso	Egypt	Ireland	Malta	Guinea	Sudan	Zimbabwe
Burma	El Salvador	Israel	Marshall Islands	Paraguay	Suriname	
	Equatorial Guinea	Italy	[Copyright © TELEOMA. All Rights Reserved]	Peru	Swaziland	

For any questions contact support@telcomatraining.com