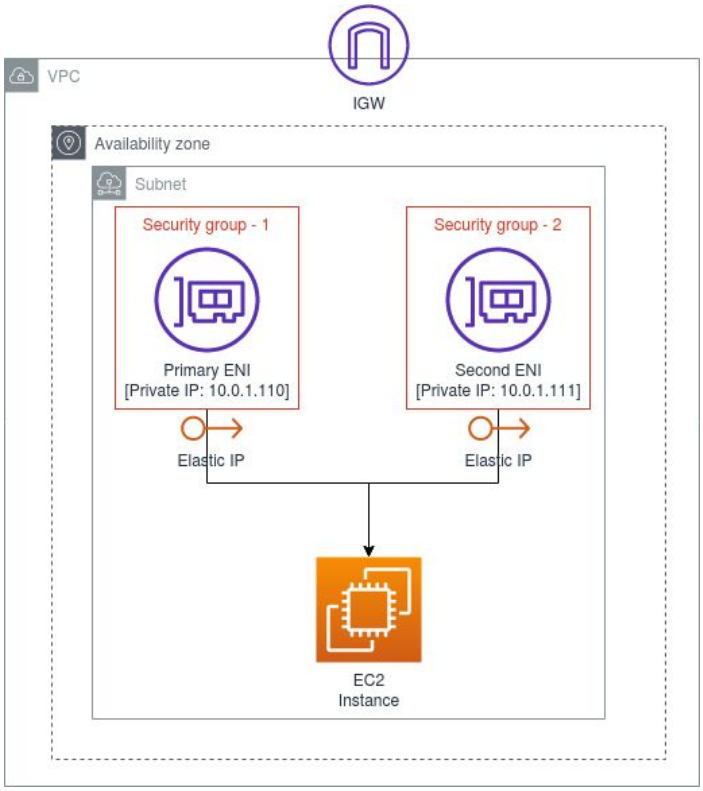
ENI → ENA → EFA

ENI	ENA	EFA
• Upto 10 GBPS • VMDq • TCP/IP • Multiple ENI/instance • Traffic can traverse across subnets • VPC Networking, General purpose • Default	• Upto 25 GBPS • SR-IOV • TCP/IP • Single setting/per instance • Traffic can traverses across subnets • Low latency apps • Optional on supported instance type	• Upto 100 GBPS • OS-Bypass • SRD • One EFA per instance • OS Bypass traffic is limited to single subnet and is not routable • HPC and ML Apps • Optional on supported instance type



Exam tip: HPC & Machine Learning >>>>>> EFA

On-Premises

What will be migrated ? | **Which Service will be used ?**

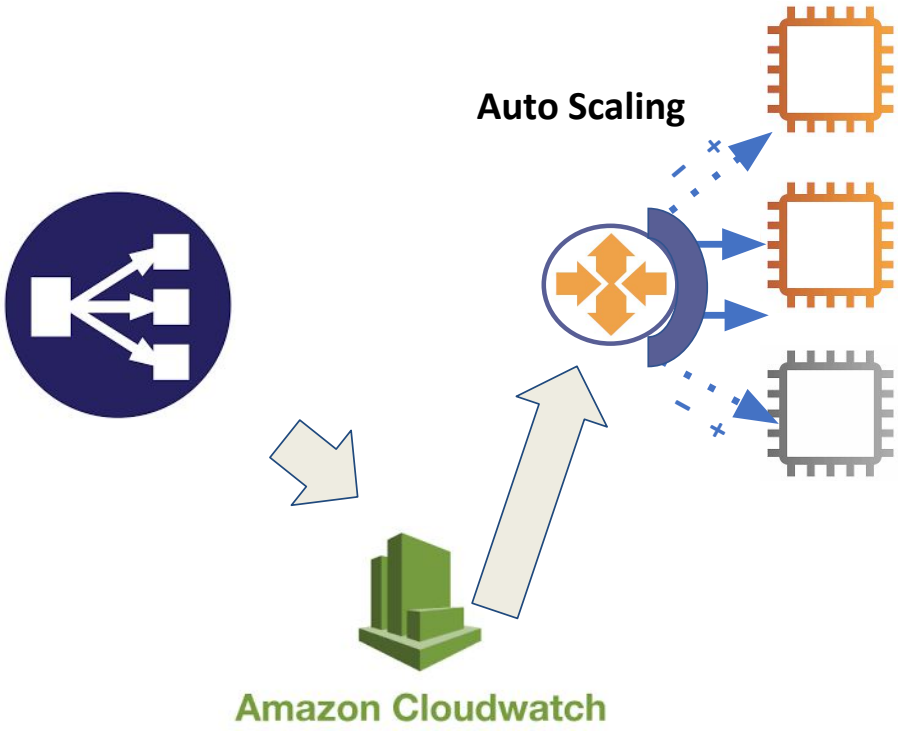
What will be migrated ?	Which Service will be used ?
DATA	DataSync
DATABASE	Database Migration Service
VM SERVER	Server Migration Service

Physical data transfer device

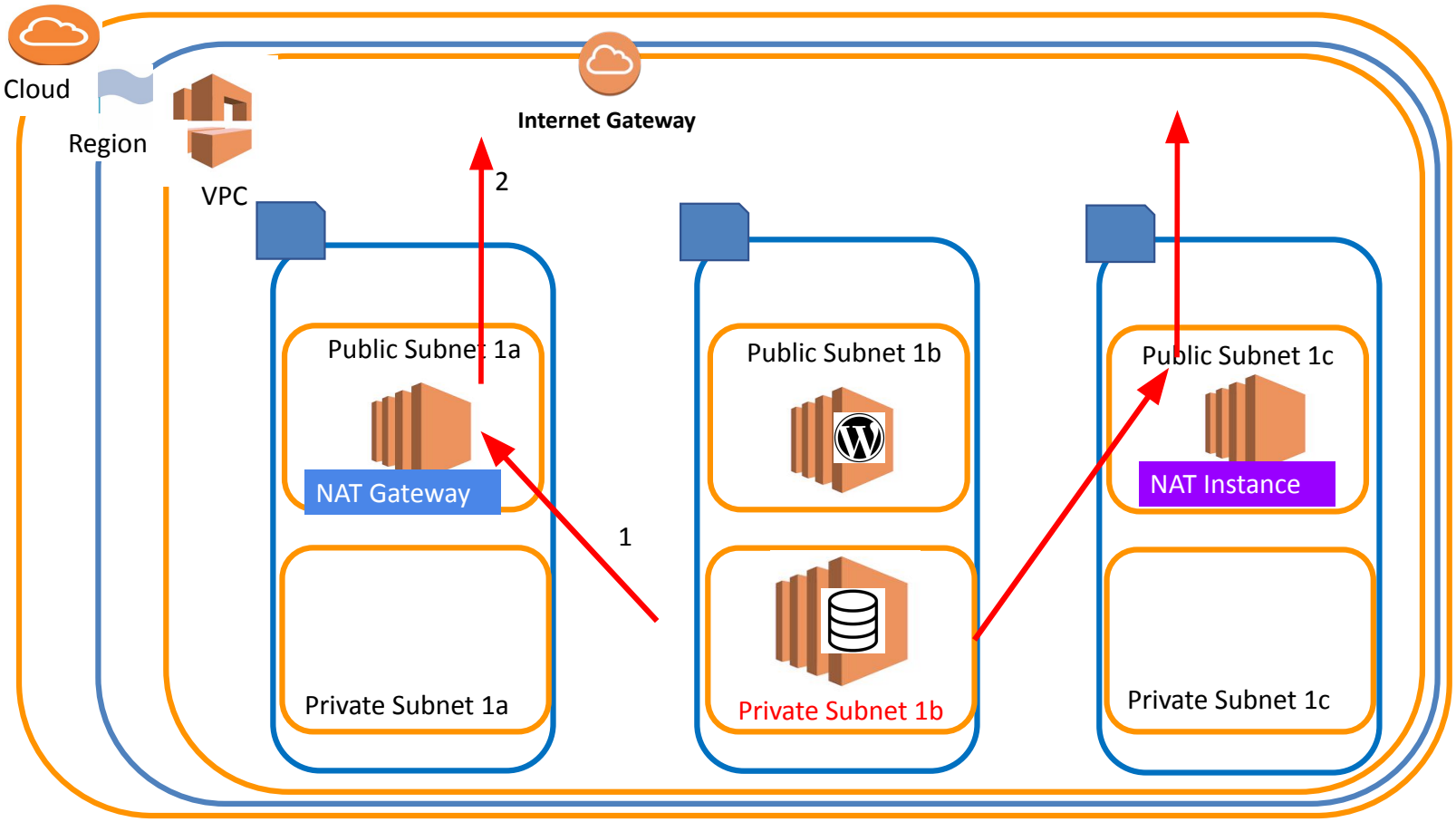
Snowball

Migration Hub

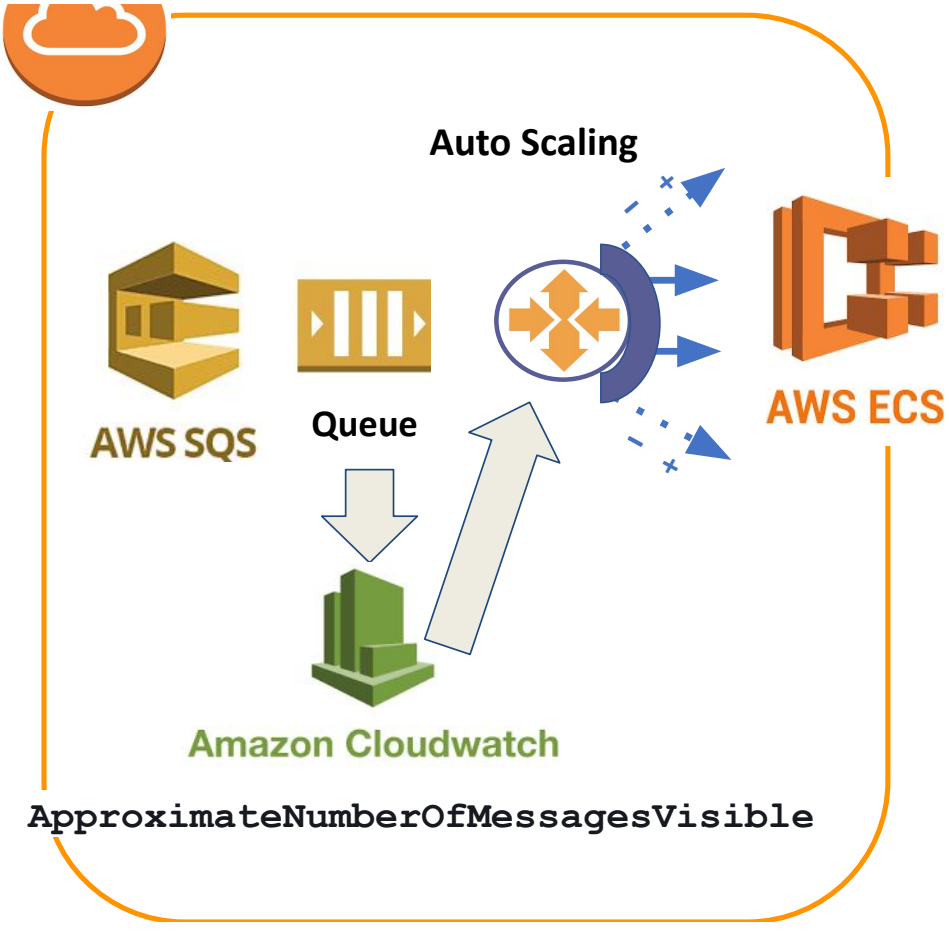
Real time Streaming | Capture | Transfer/Load | Analyze

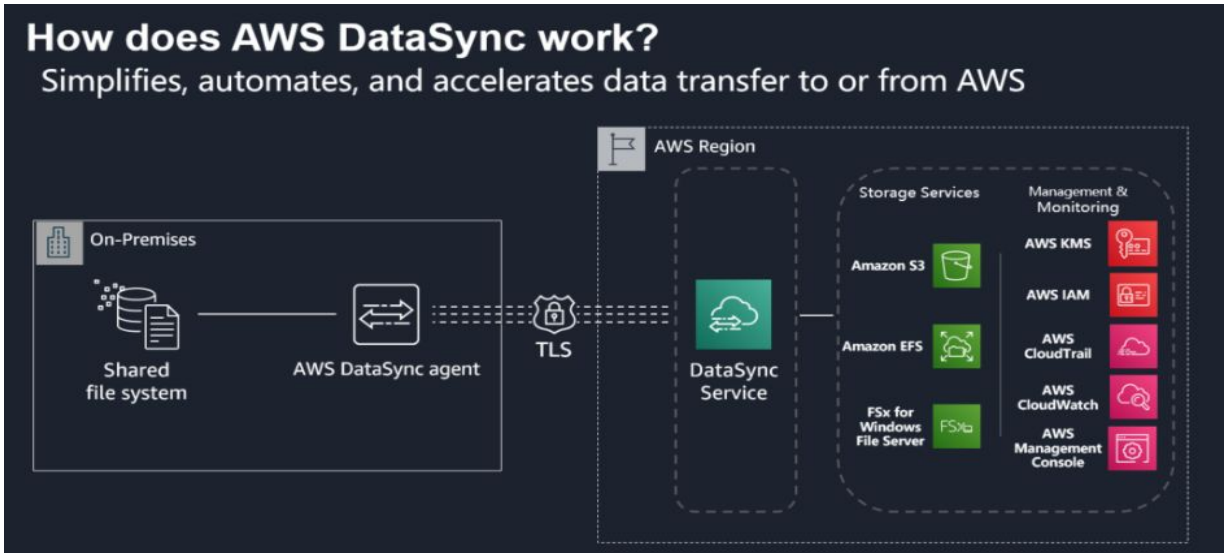


CPU utilization

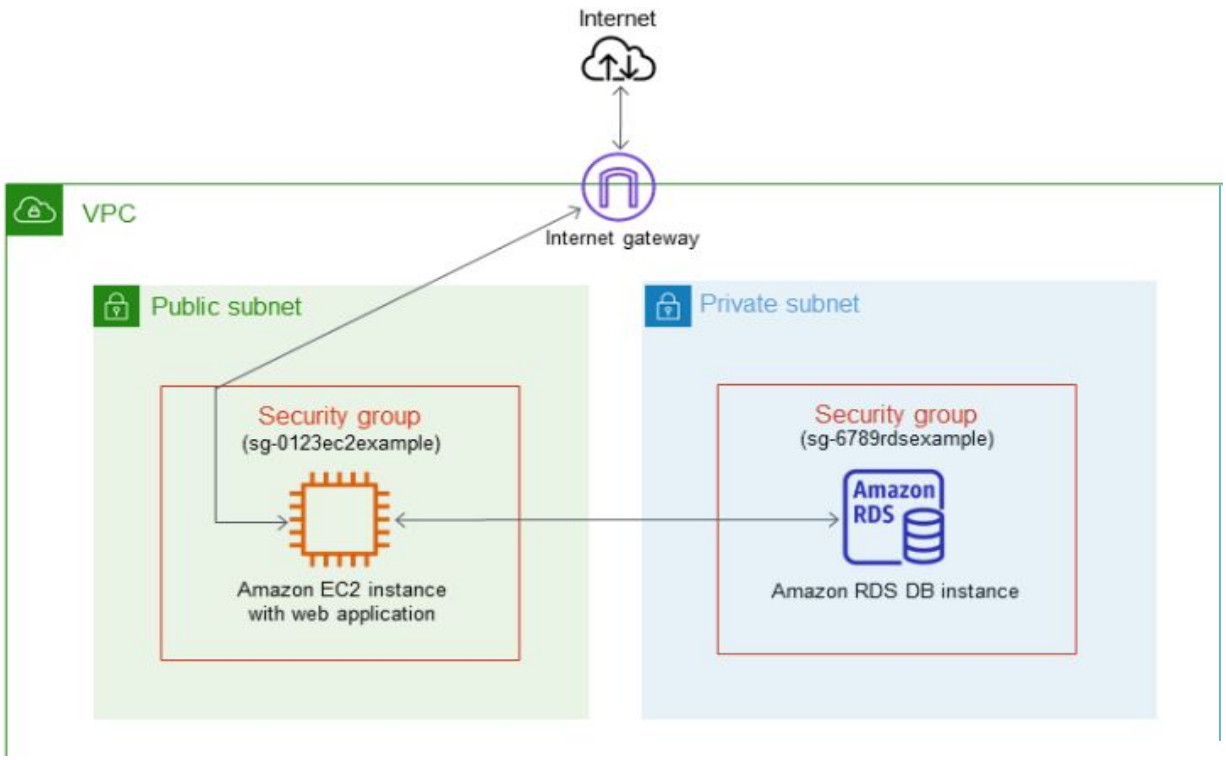

Cloud
Region
VPC
Internet Gateway
2
1
Public Subnet 1a
NAT Gateway
Private Subnet 1a
Public Subnet 1b
Private Subnet 1b
Public Subnet 1c
NAT Instance
Private Subnet 1c

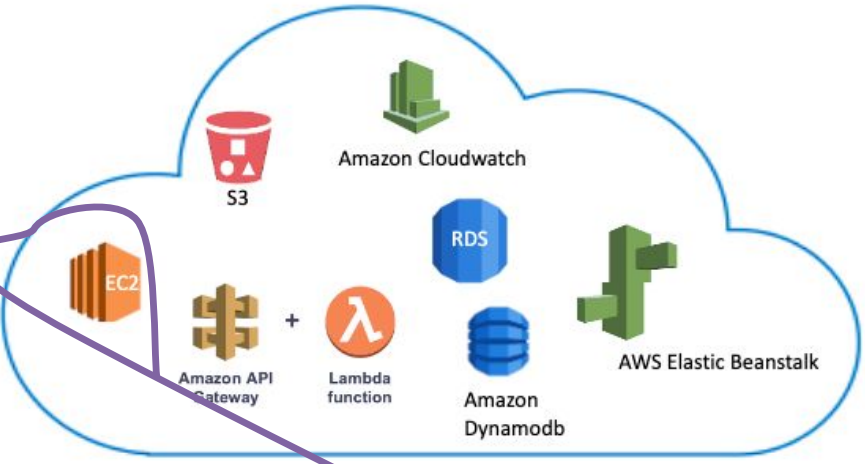
Data Center


Auto Scaling
AWS SQS
Queue
AWS ECS
Amazon Cloudwatch
ApproximateNumberOfMessagesVisible



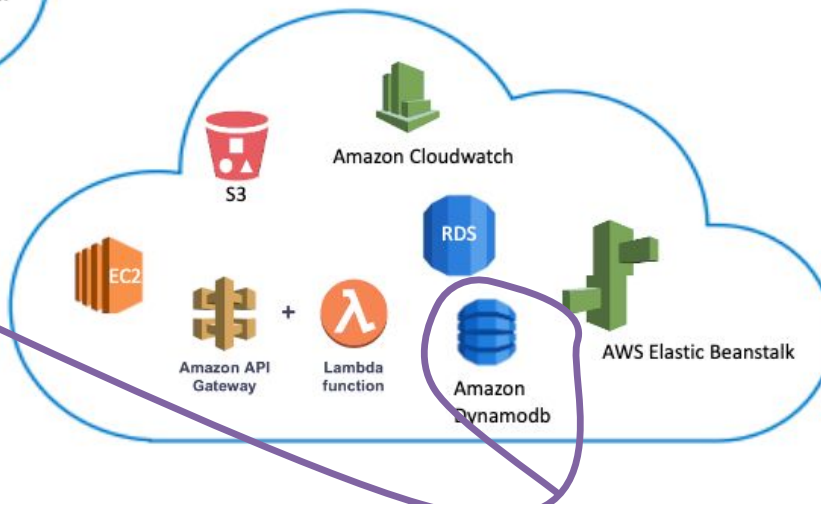
- **Public endpoints**:
- **Federal Information Processing Standard (FIPS) endpoints**: USA and Canada
- **Virtual private cloud (VPC) endpoints**: If you use a VPC endpoint, all communication from DataSync to AWS occurs through the endpoint in your AWS VPC. This establishes a private connection between your self-managed storage system, your VPC, and AWS services, providing extra security as your data is copied over the network.

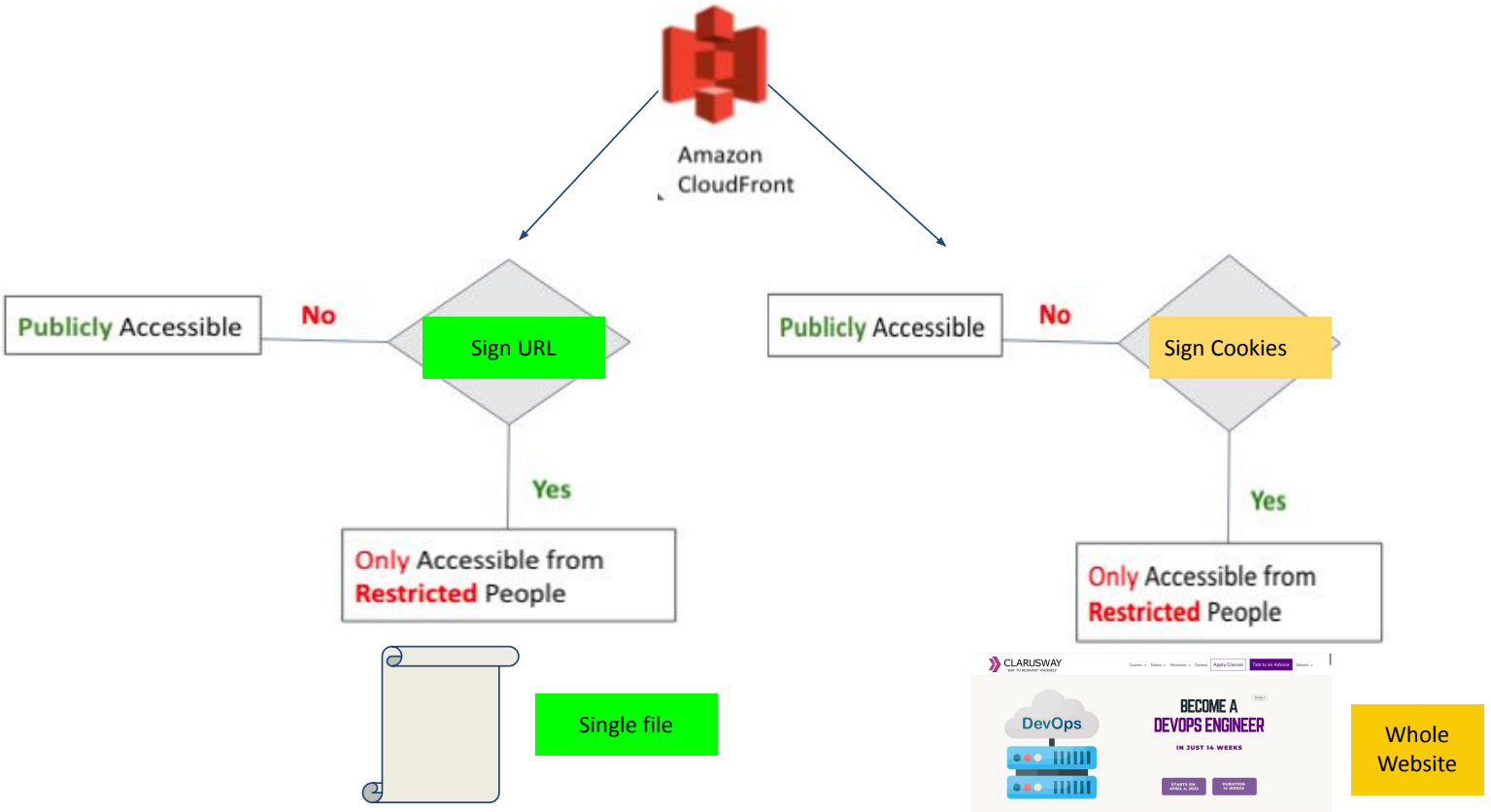


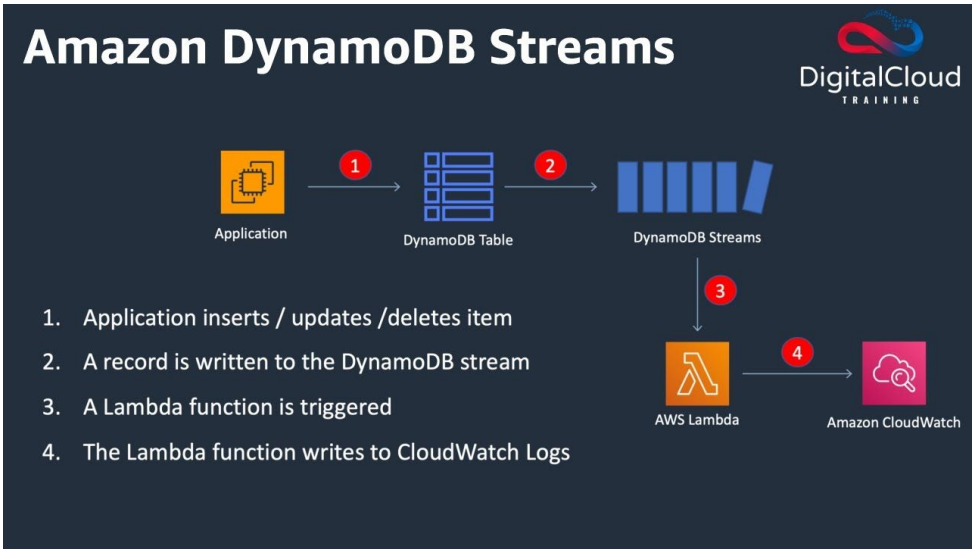

Amazon Cloudwatch
S3
RDS
EC2
Amazon API Gateway
Lambda function
Amazon Dynamodb
AWS Elastic Beanstalk


aws

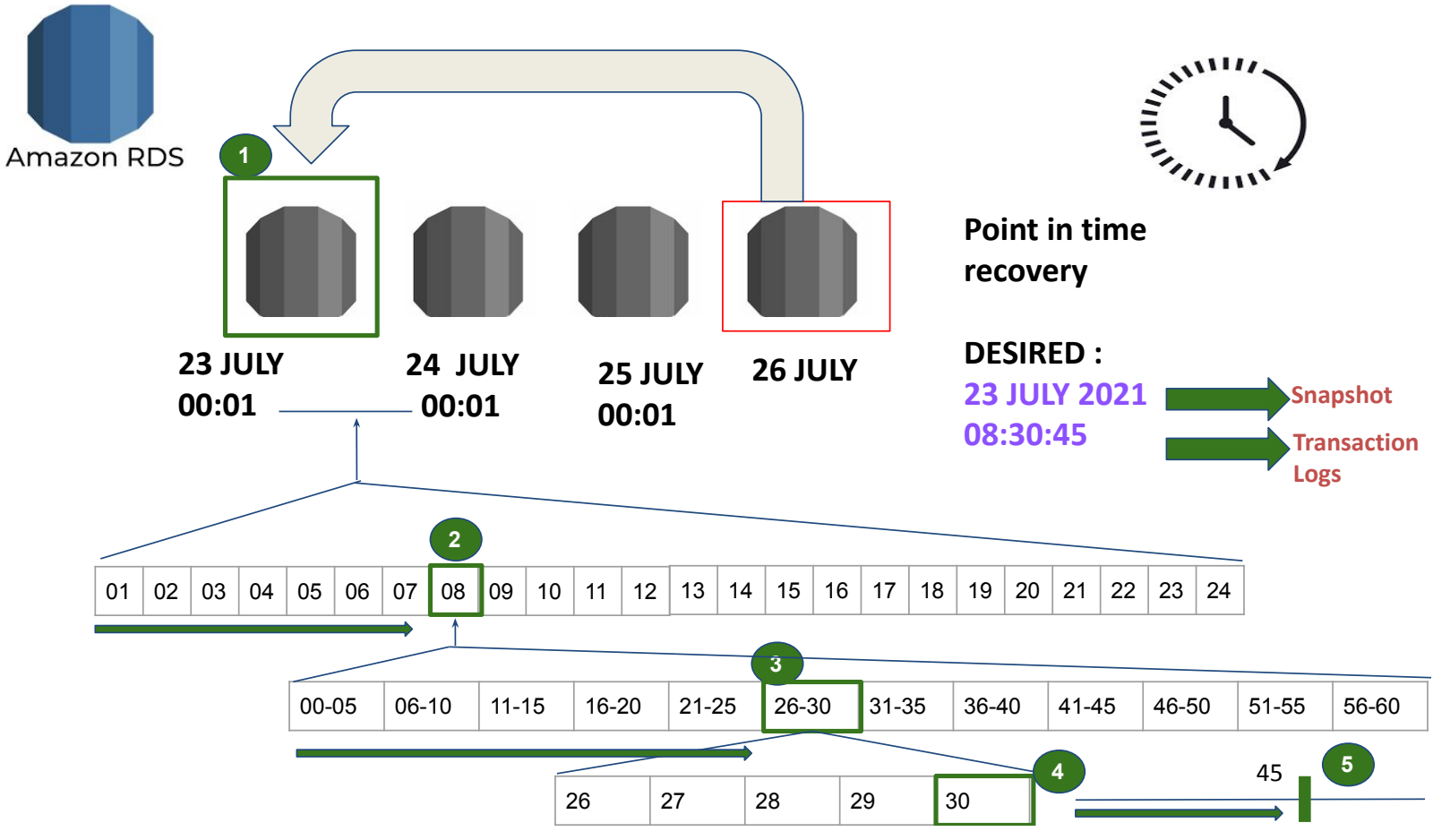
IAM Role

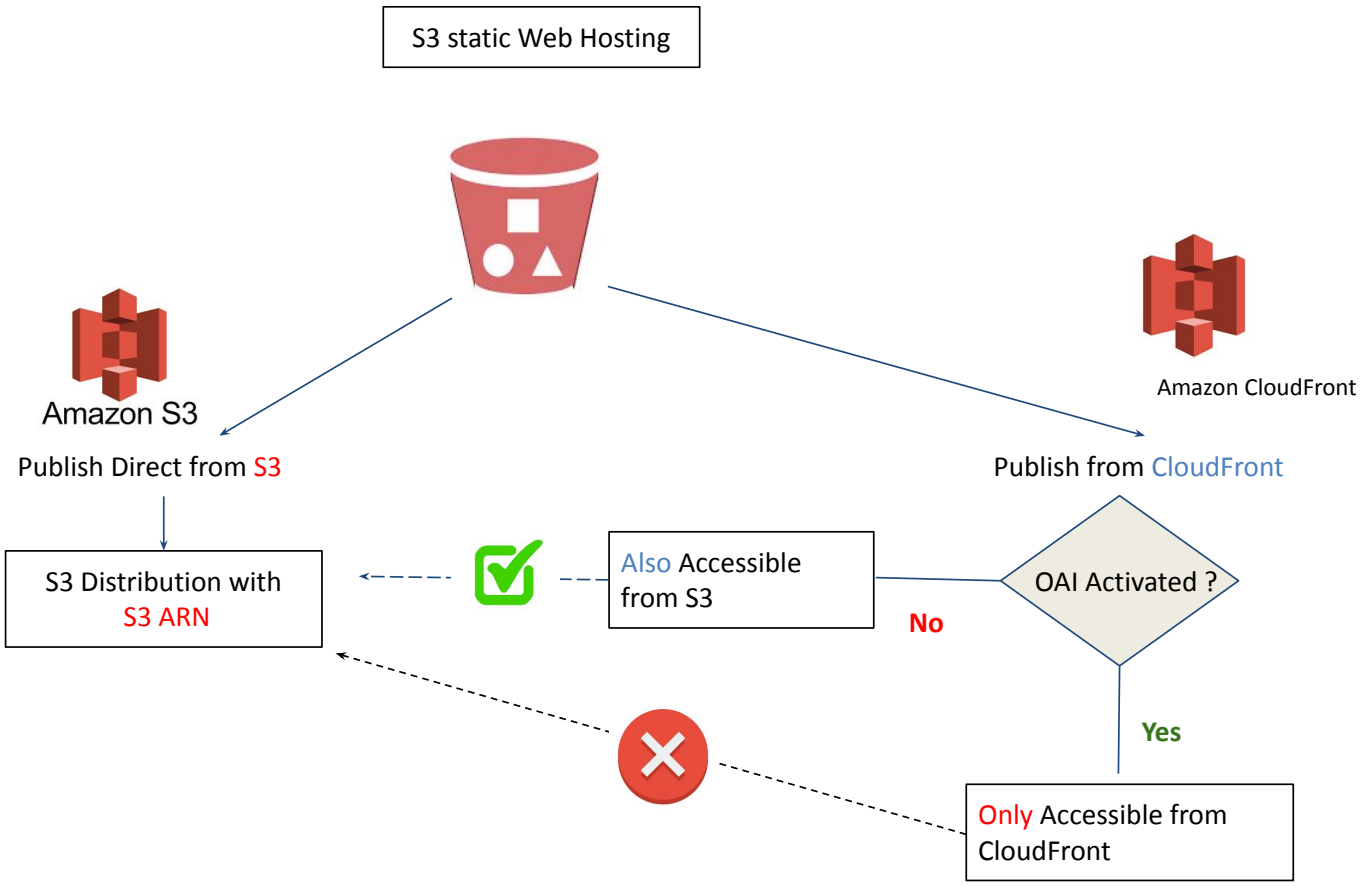

Amazon Cloudwatch
S3
RDS
EC2
Amazon API Gateway
Lambda function
Amazon Dynamodb
AWS Elastic Beanstalk

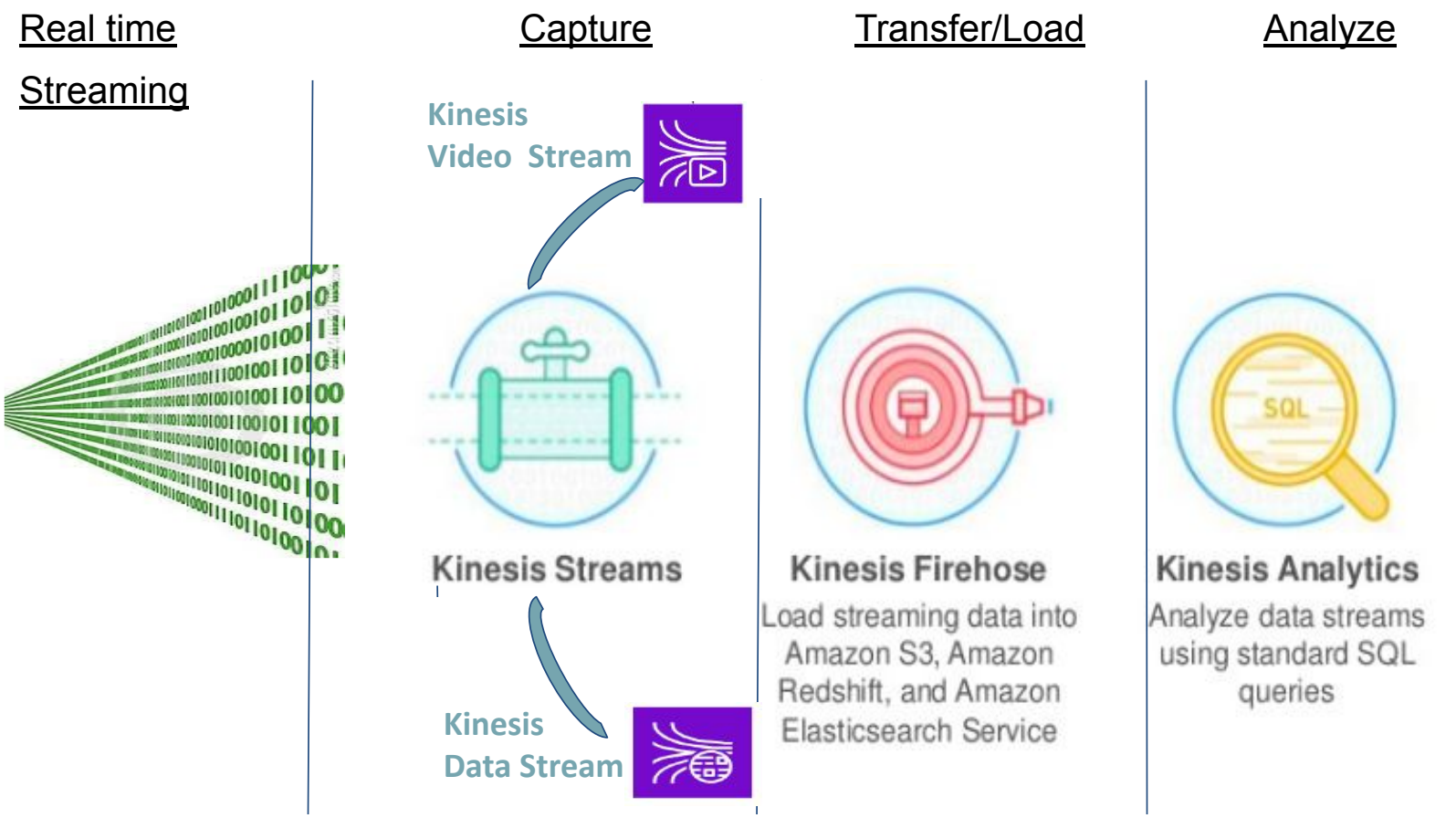

Amazon CloudFront
Publicly Accessible
No
Sign URL
Yes
Only Accessible from Restricted People
Single file
Publicly Accessible
No
Sign Cookies
Yes
Only Accessible from Restricted People
CLARUSWAY
DevOps
BECOME A DEVOPS ENGINEER
IN JUST 14 WEEKS
Whole Website

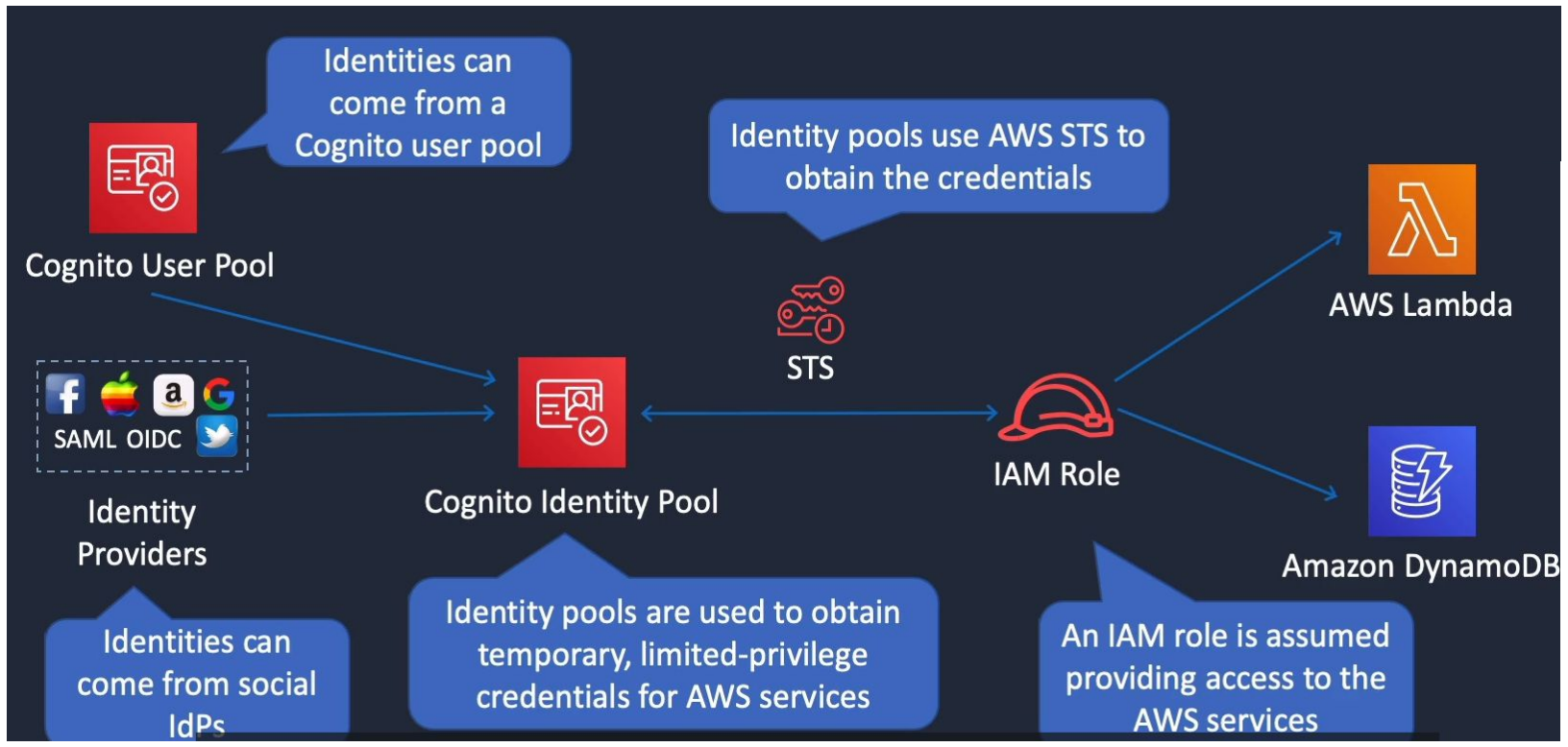


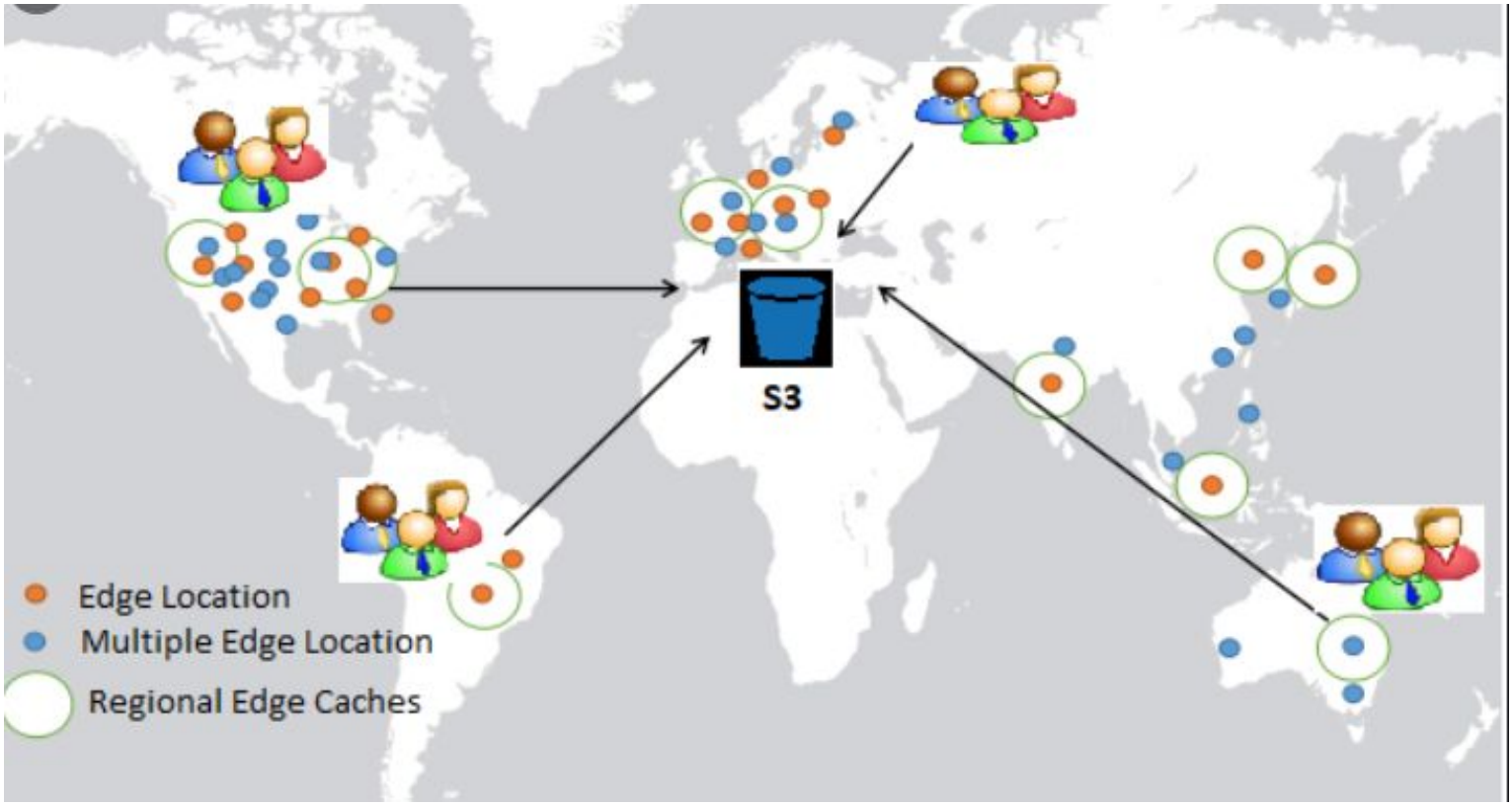
When enabled, DynamoDB Streams captures a time-ordered sequence of item-level modifications in a DynamoDB table and durably stores the information for **up to 24 hours. Applications can access a series of stream *records*, which contain an item change, from a DynamoDB stream in near real time.**



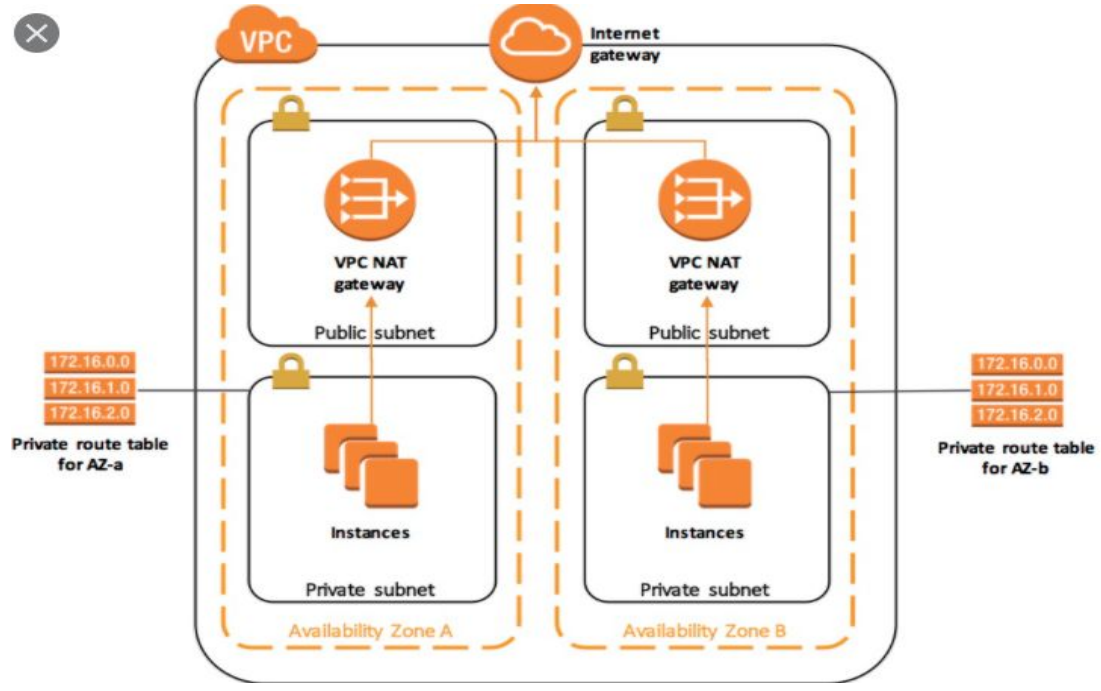

S3 static Web Hosting
Amazon S3
Amazon CloudFront
Publish Direct from S3
Publish from CloudFront
S3 Distribution with S3 ARN
Also Accessible from S3
OAI Activated ?
No
Yes
Only Accessible from CloudFront


Real time Streaming
Capture
Transfer/Load
Analyze
Kinesis Video Stream
Kinesis Streams
Kinesis Data Stream
Kinesis Firehose
Load streaming data into Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service
SQL
Kinesis Analytics
Analyze data streams using standard SQL queries


What will be migrated ?
Which Service wiil be used ?
DATA
DataSync
DATABASE
Database Migration Service
VM SERVER
Server Migration Service
On-Premises
Physical data transfer device
Snowball
Migration Hub
Identities can come from a Cognito user pool
Cognito User Pool
Identity pools use AWS STS to obtain the credentials
STS
AWS Lambda
SAML OIDC
Identity Providers
Cognito Identity Pool
IAM Role
Amazon DynamoDB
Identities can come from social IdPs
Identity pools are used to obtain temporary, limited-privilege credentials for AWS services
An IAM role is assumed providing access to the AWS services



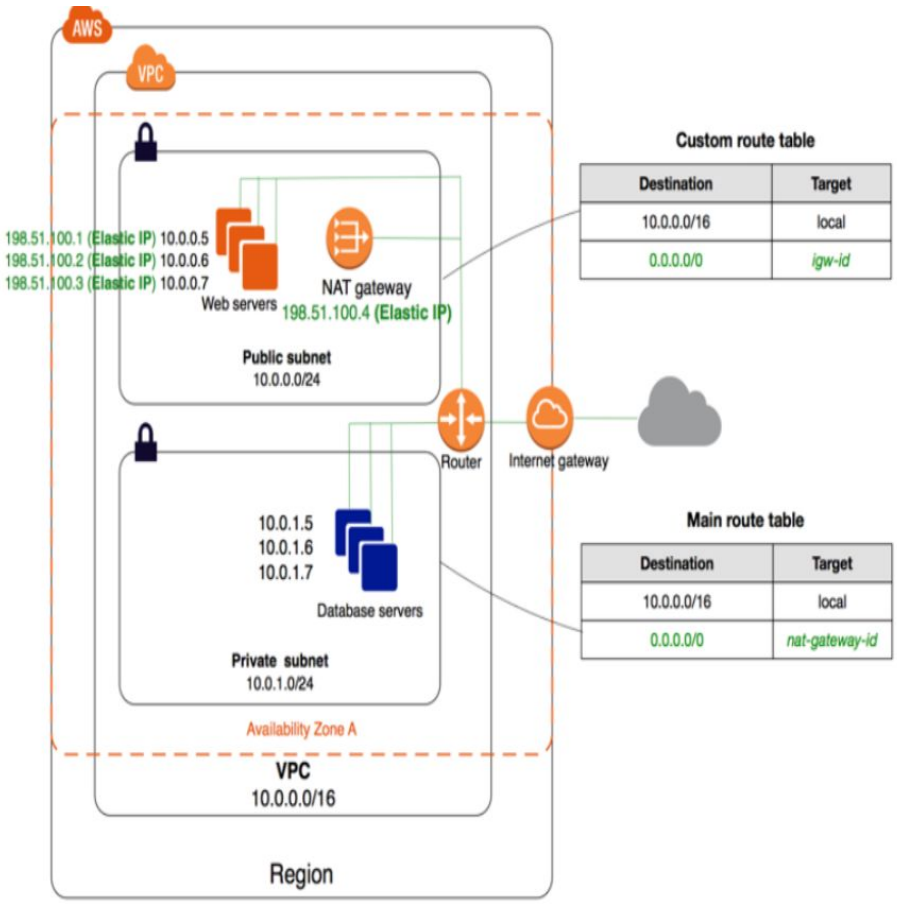
If you have resources in multiple Availability Zones and they share one NAT Gateway, in the event that the NAT Gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT Gateway in each Availability Zone and configure your routing to ensure that resources use the NAT Gateway in the same Availability Zone.

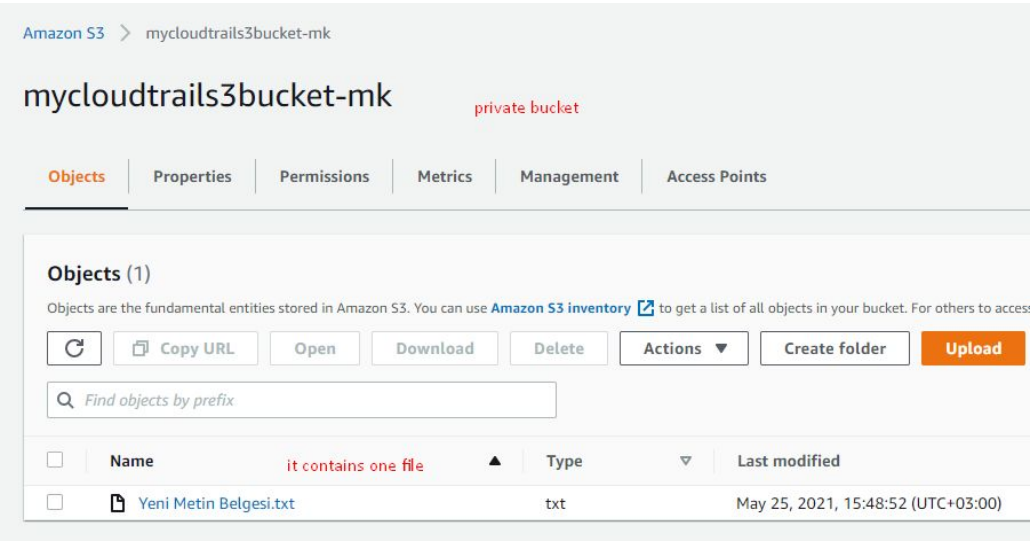


Amazon Aurora Key Features

Aurora Feature	Benefit
High performance and scalability	Offers high performance, self-healing storage that scales up to 64TB, point-in-time recovery and continuous backup to S3
DB compatibility	Compatible with existing MySQL and PostgreSQL open source databases
Aurora Replicas	In-region read scaling and failover target – up to 15 (can use Auto Scaling)
MySQL Read Replicas	Cross-region cluster with read scaling and failover target – up to 5 (each can have up to 15 Aurora Replicas)
Global Database	Cross-region cluster with read scaling (fast replication / low latency reads). Can remove secondary and promote
Multi-Master	Scales out writes within a region. In preview currently and will not appear on the exam
Serverless	On-demand, autoscaling configuration for Amazon Aurora - does not support read replicas or public IPs (can only access through VPC or Direct Connect - not VPN)

Throughput **5x MySQL RDS**
3x PostgreSQL RDS





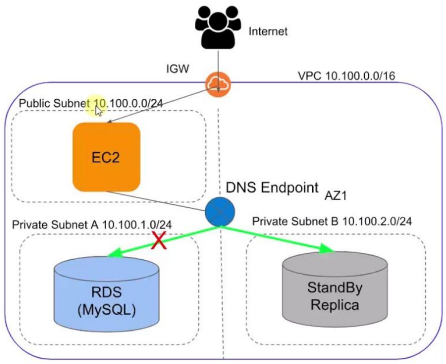

```
$ aws s3 presign s3://mycloudtrails3bucket-mk/"Yeni Metin Belgesi.txt" --expires-in 30
https://mycloudtrails3bucket-mk.s3.us-east-1.amazonaws.com/Yeni%20Metin%20Belgesi.txt?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAY3YMFVJJYLFDLWV5%2F20210525%2Fus-east-1%2Fs3
%2Faws4_request&X-Amz-Date=20210525T125743Z&X-Amz-Expires=30&X-Amz-SignedHeaders=host&X-Amz-
Signature=b02d2c978829ff3bed34001380b8b9e0b51262727d2b37391c4b5c12e0d6f31c
```

In the question : there will be a rds mysql and is expected a high number of read and writes. Which ebs types supports this?

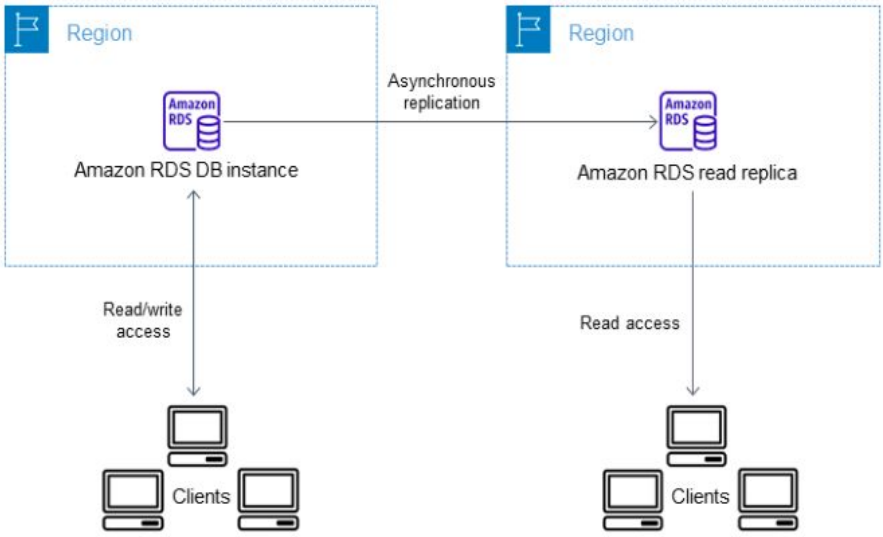
	Solid State Drives (SSD)					Hard Disk Drives (HDD)	
Volume Type	EBS Provisioned IOPS SSD (io2 Block Express)	EBS Provisioned IOPS SSD (io2)	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp3) announced Dec 1, 2020	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Short Description	Highest performance SSD volume designed for business-critical latency-sensitive **transactional workloads**	**Highest performance** and highest durability SSD volume designed for **latency-sensitive transactional workloads**	Highest performance SSD volume designed for **latency-sensitive transactional workloads**	**Lowest cost SSD volume that balances price performance for a wide variety of transactional workloads**	General Purpose SSD volume that **balances price performance for a wide variety of transactional workloads**	**Low cost HDD volume designed for frequently accessed, throughput intensive workloads**	**Lowest cost HDD volume designed for less frequently accessed workloads**
Durability	99.999%		99.8% - 99.9% durability			99.8% - 99.9% durability	
Use Cases	Largest, most I/O intensive, mission critical deployments of NoSQL and relational **databases** such as Oracle, SAP HANA, Microsoft SQL Server, and SAS Analytics	I/O-intensive NoSQL and relational **databases**	I/O-intensive NoSQL and relational **databases**	Virtual desktops, medium sized single instance **databases** such as Microsoft SQL Server and Oracle, latency sensitive interactive applications, boot volumes, and dev/test environments	Virtual desktops, medium sized single instance **databases** such as Microsoft SQL Server and Oracle, latency sensitive interactive applications, boot volumes, and dev/test environments	**Big data, data warehouses, log processing**	**Colder data requiring fewer scans per day**

With Amazon RDS, you can create a MariaDB, MySQL, Oracle, or PostgreSQL read replica in a different AWS Region from the source DB instance. Creating a cross-Region read replica isn't supported for SQL Server on Amazon RDS.

RDS Multi-AZ Failover



Availability - Failover-Senkron



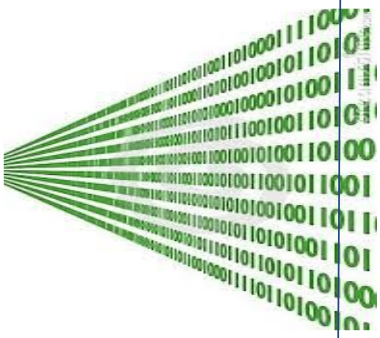
Performance- Asenkron

Real time Streaming

Capture

Transfer/Load

Analyze



Kinesis Video Stream

Kinesis Streams

Kinesis Data Stream

Kinesis Firehose

Load streaming data into Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service

Kinesis Analytics

Analyze data streams using standard SQL queries

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-f52d178f (172.31.0.0/16) | default-vpc

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
i-0667836734e141b24	Cloudwatch_instance	stopped	launch-wizard-40	us-east-1d	subnet-ed49bccc	172.31.80.0/20
i-09a81ac9ed47f33a3	pet-clinic-demo-server	stopped	launch-wizard-21	us-east-1f	subnet-3246e63c	172.31.64.0/20
i-0c8b559e55c99cfe1	Jenkins Server of tomy-jenkinsserver-p...	stopped	tomy-jenkinsserver-petclinic-JenkinsS...	us-east-1f	subnet-3246e63c	172.31.64.0/20
i-030841b79c0f01e67	tyler-nexus-server	stopped	Nexus-SG	us-east-1f	subnet-3246e63c	172.31.64.0/20
i-090276ecb3211442a	Jenkins Server of walter-petclinic	stopped	walter-petclinic-JenkinsServerSecurity...	us-east-1f	subnet-3246e63c	172.31.64.0/20

Cross-zone load balancing distributes traffic evenly across all targets in the Availability Zones enabled for the load balancer.

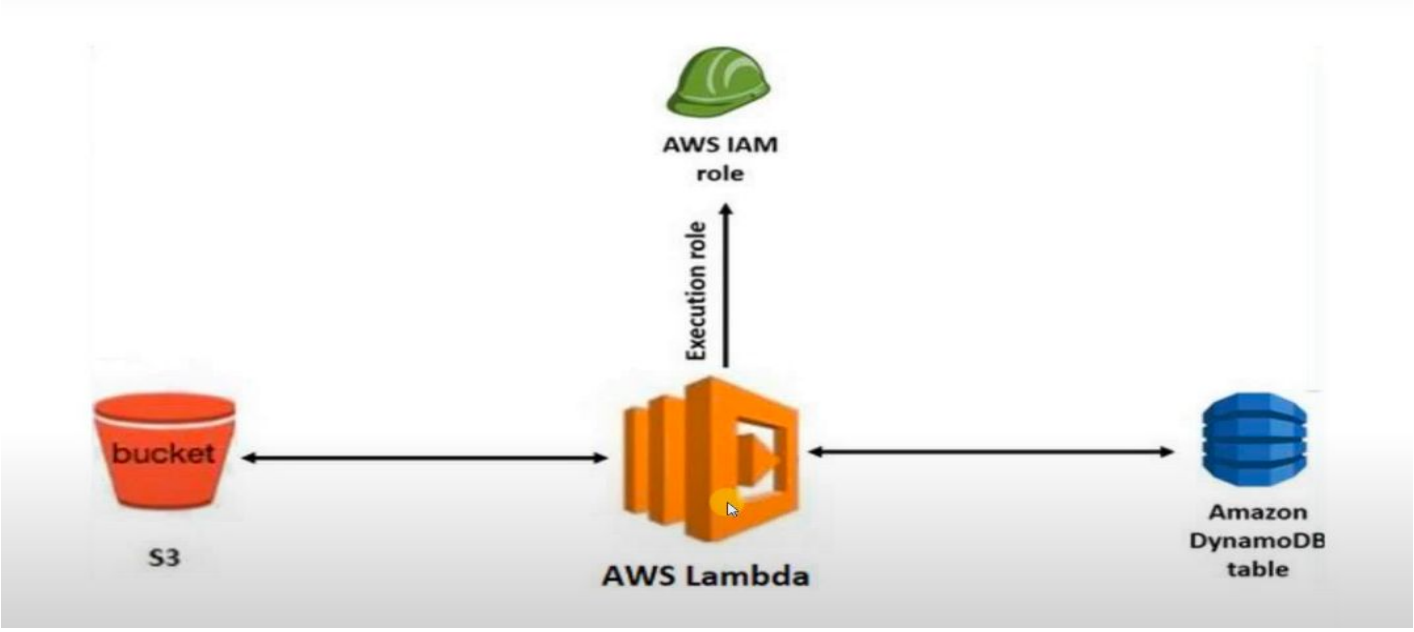
Availability Zone Distribution

1 instance in us-east-1d

Enable Cross-Zone Load Balancing

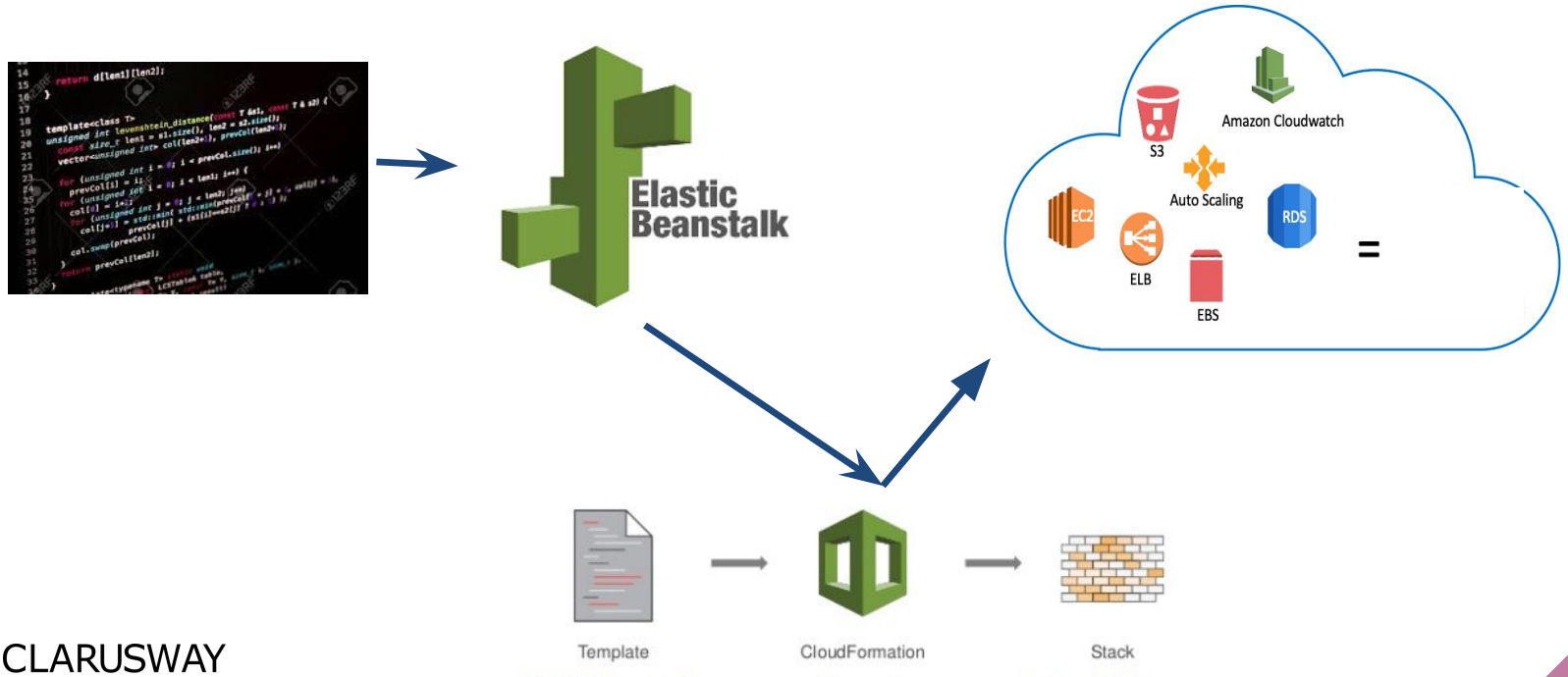
Enable Connection Draining 300 seconds

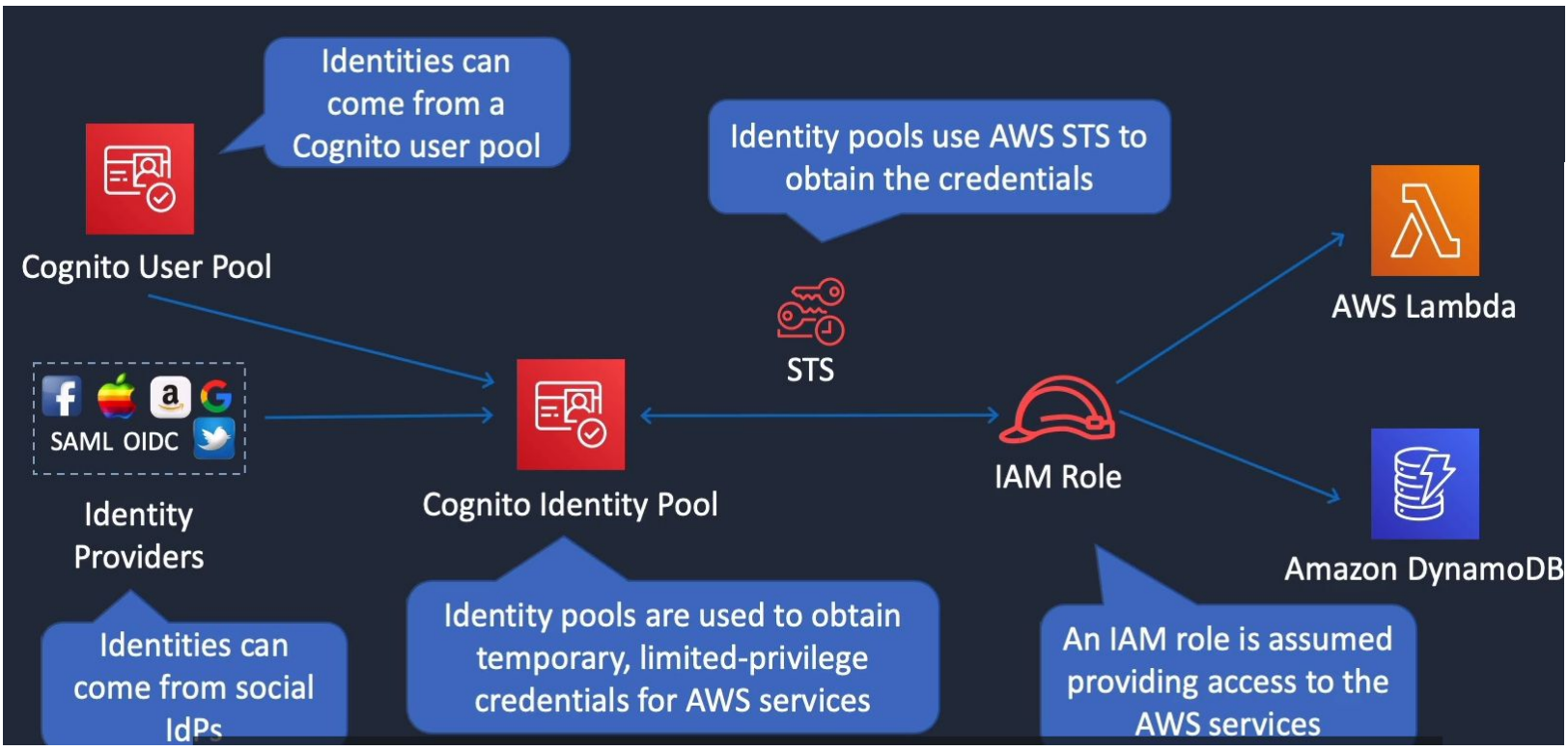
Exam tip: DynamoDb and Metadata



Introduction to Elastic Beanstalk

Why AWS Elastic Beanstalk?

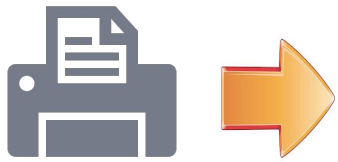




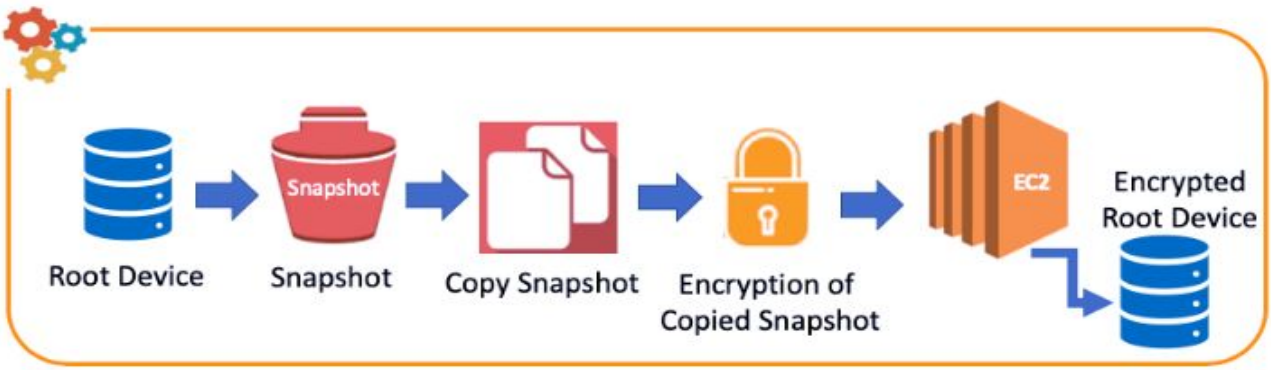
Storage Classes

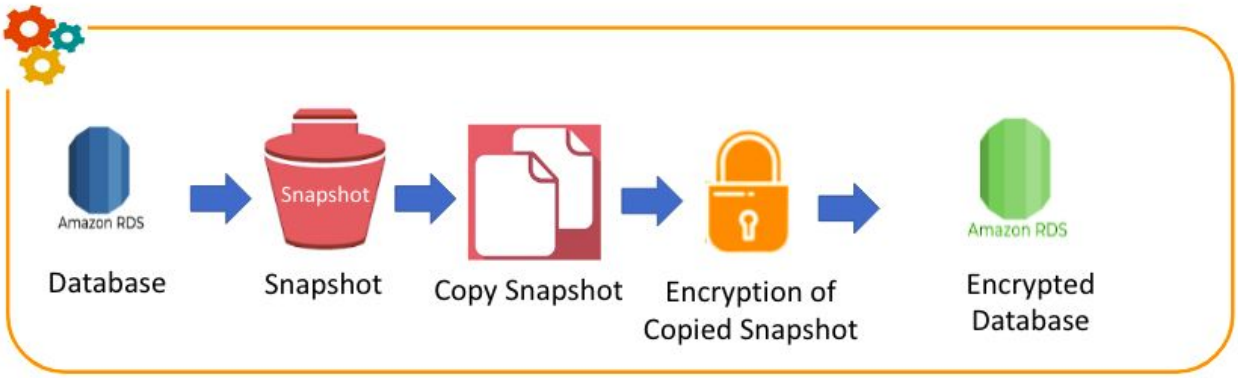
Standard IA (Infrequent Access)

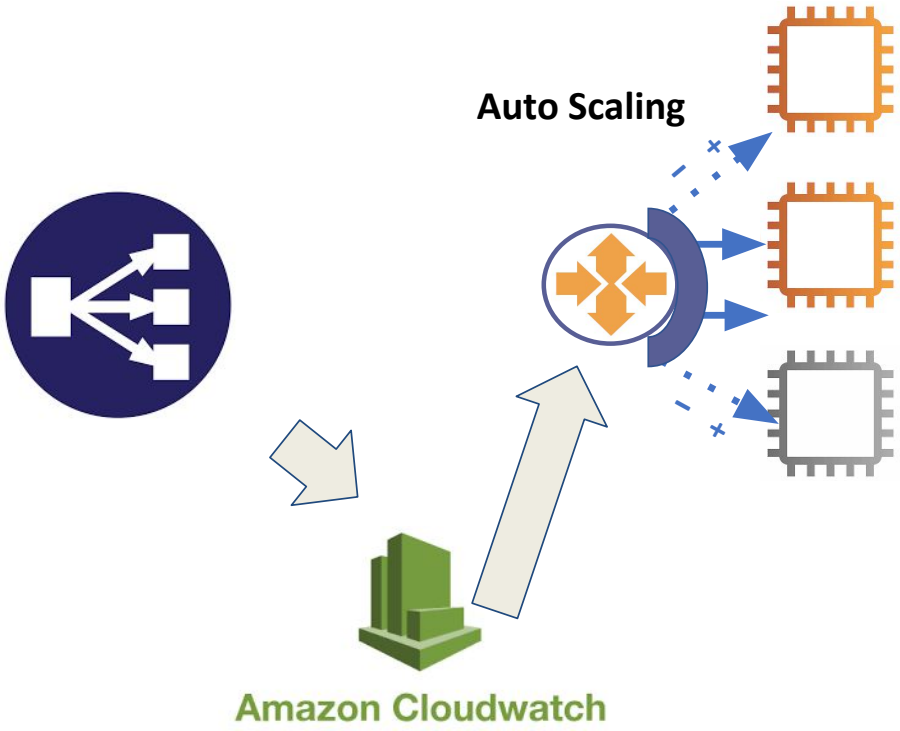
Infrequently Accessed Data



- Standard IA (Infrequent Access) is a convenient for infrequently accessed files
- But in case of access, it provides you to reach the file quickly.
- In fact, it designed for the data which requires less frequent access, but with longer storage time than the Standard class
- It is cheaper than Standard class as long as you access **infrequently.**



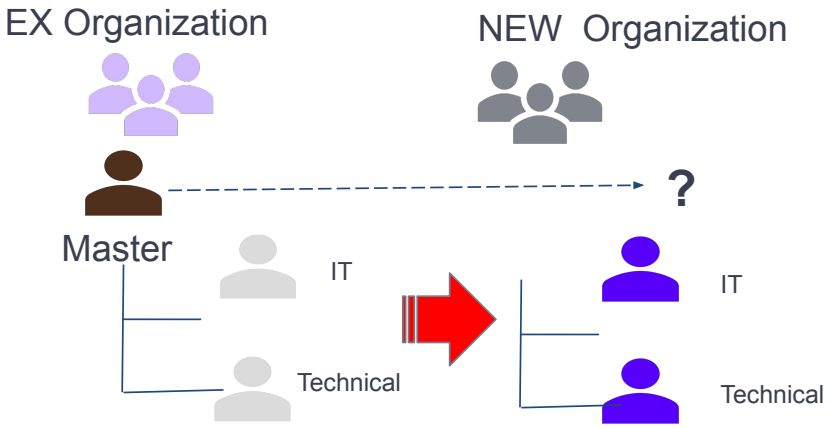


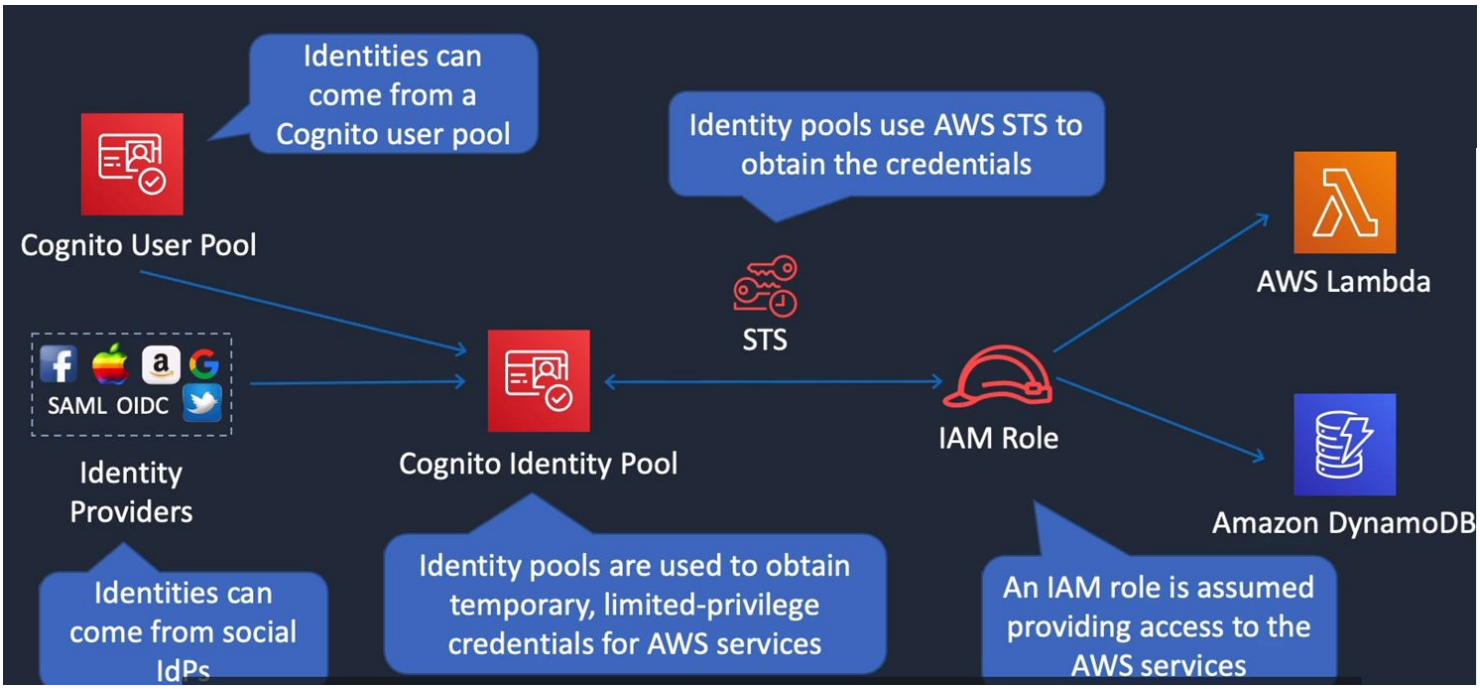


CPU utilization

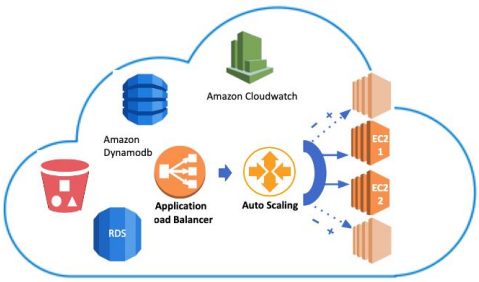
MEMBER AND MASTER ACCOUNT LEAVING PROCESS

1. Remove the **member account** from the old Organization.
2. Send an invite to the member account from the new Organization.
3. Accept the invite to the new Organization from the member account.
4. Delete the old Organization.
5. Send an invite to the master account
6. Accept the invite to the new Organization from the master account





Component	Description
Templates	The JSON or YAML text file that contains the instructions for building out the AWS environment
Stacks	The entire environment described by the template and created, updated, and deleted as a single unit
StackSets	AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation
Change Sets	A summary of proposed changes to your stack that will allow you to see how those changes might impact your existing resources before implementing them



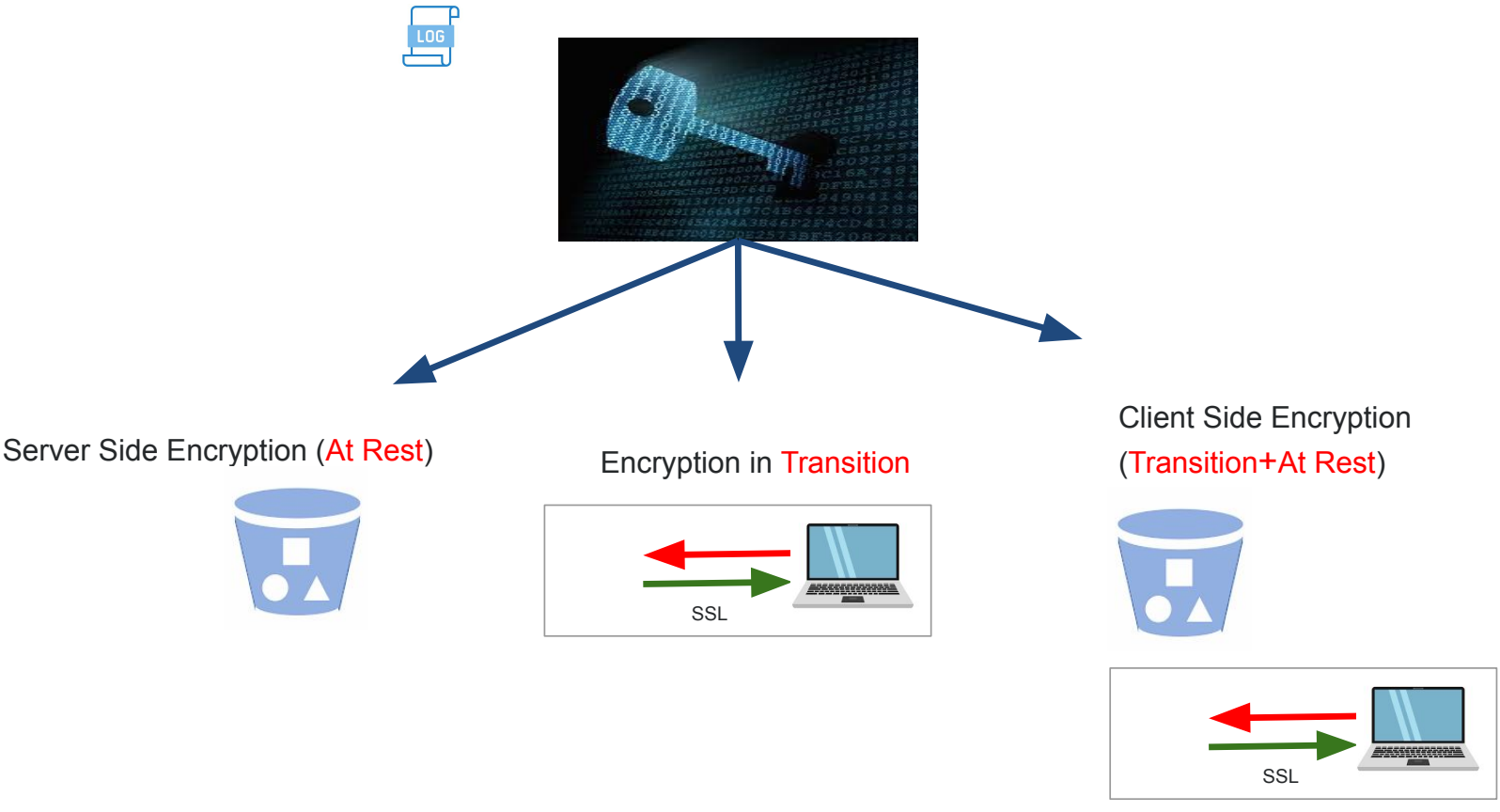
OpsWorks Stacks **CloudFormation** **Elastic Beanstalk**

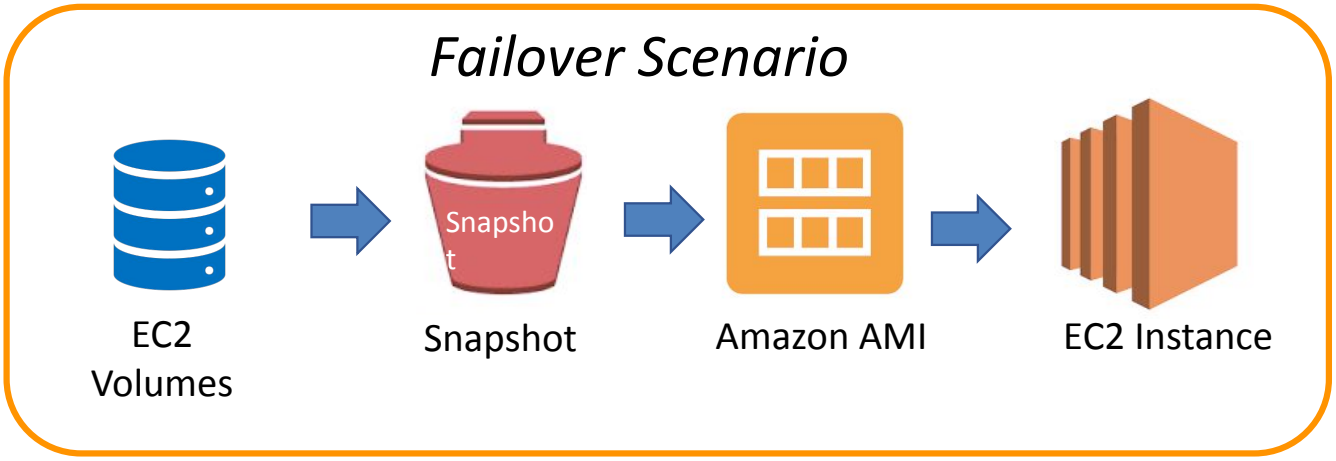
Multi-Value Answer Policies let you configure Route53 to return multiple values such as IP addresses for your web-servers, in response to DNS queries.

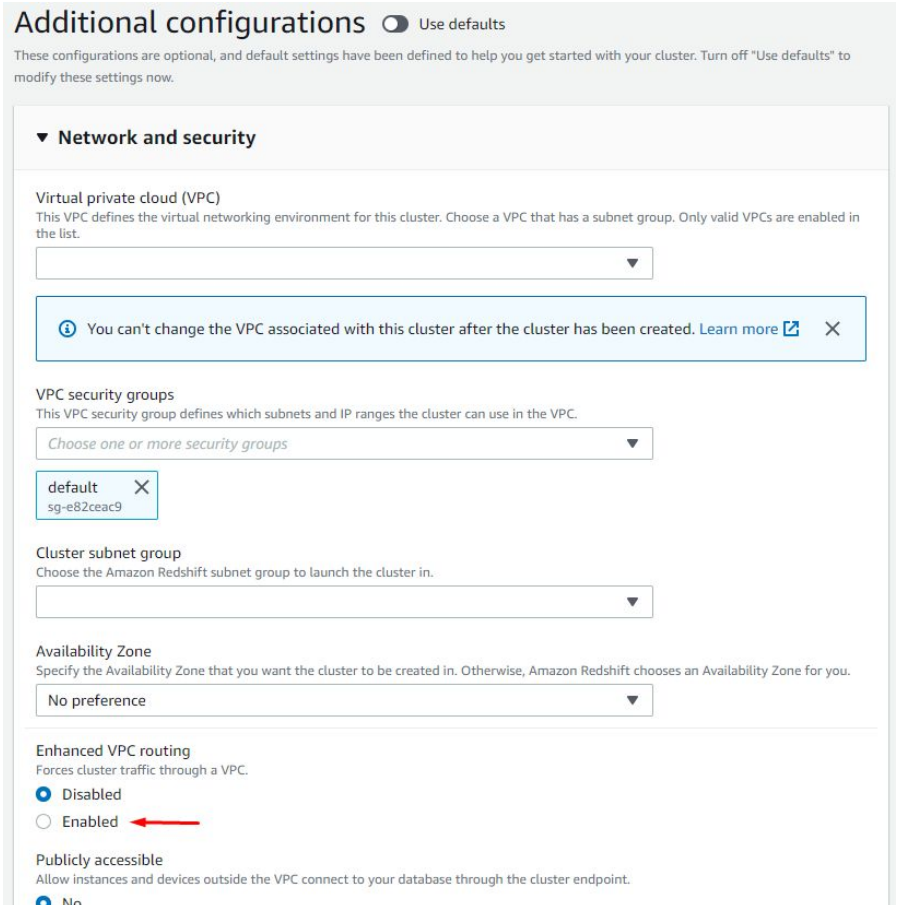
Multiple values can be specified for almost any record. Route53 automatically performs health-checks on resources and only returns values of ones deemed healthy.

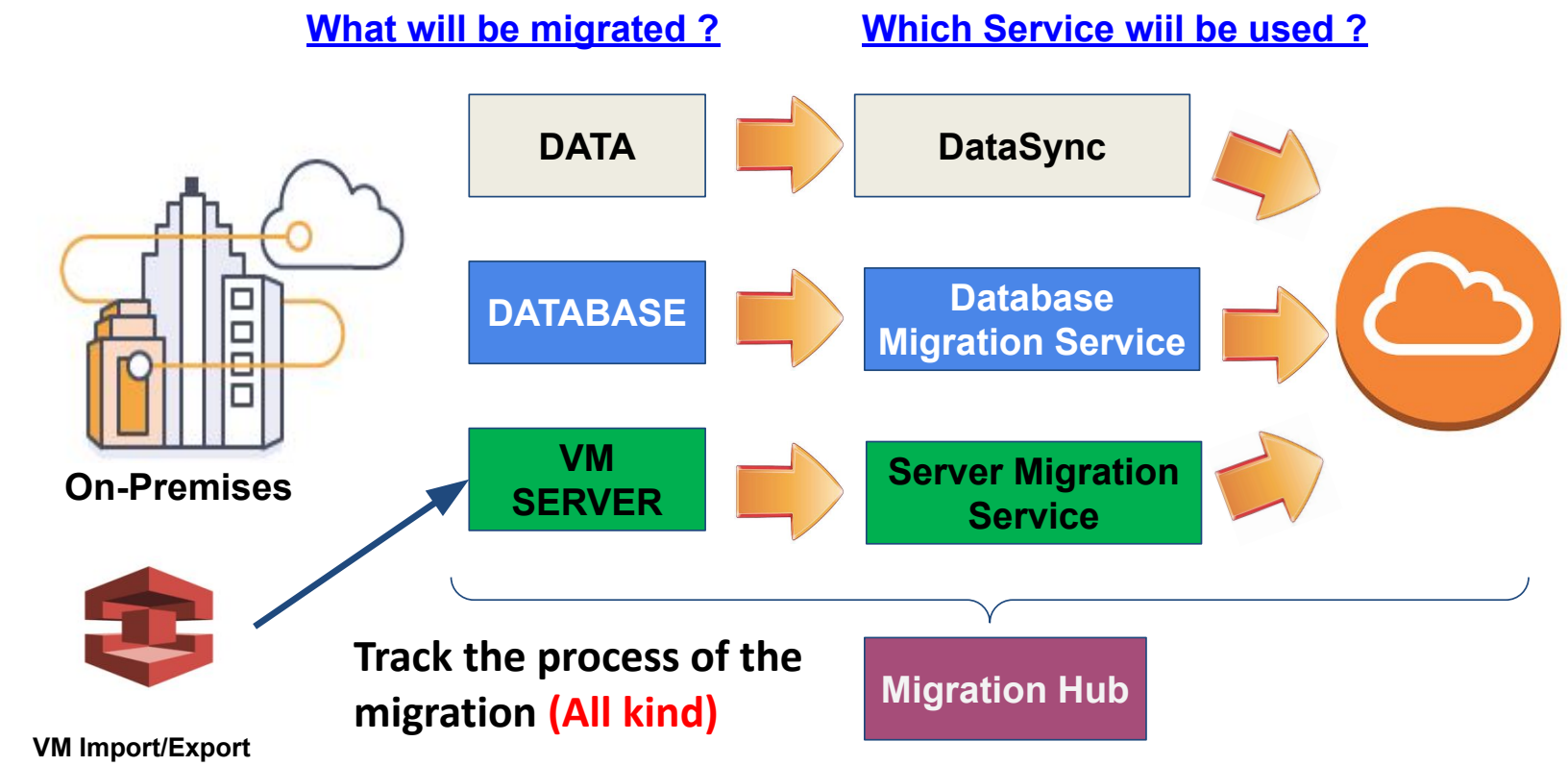
Similar to Simple Routing, however with an added health check for your record set resources.

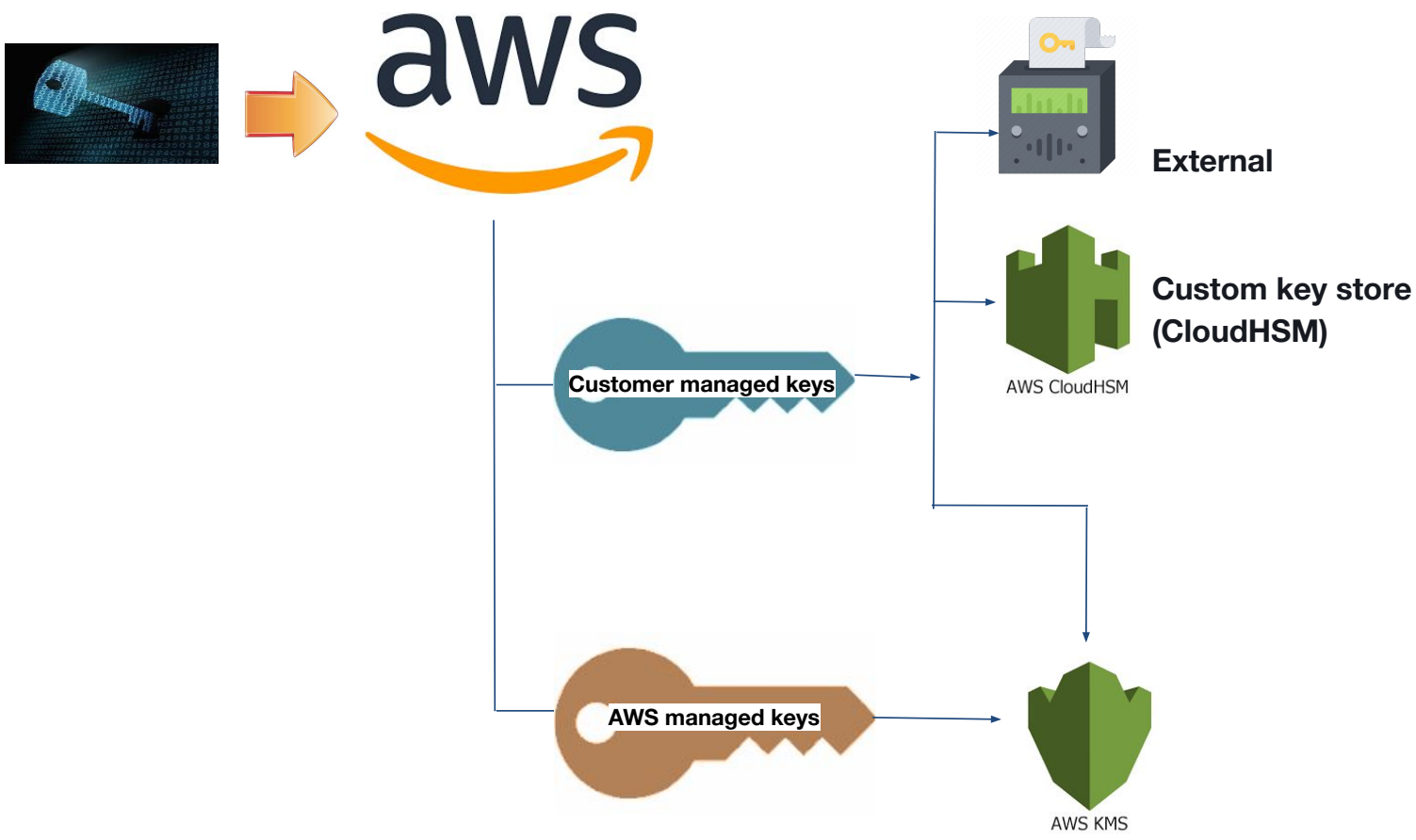
Exam tip: Weighted Routing Policy is for blue-green deployment




Failover Scenario
Snapsho
t
EC2
Volumes
Snapshot
Amazon AMI
EC2 Instance


Additional configurations
Use defaults
These configurations are optional, and default settings have been defined to help you get started with your cluster. Turn off "Use defaults" to modify these settings now.
Network and security
Virtual private cloud (VPC)
This VPC defines the virtual networking environment for this cluster. Choose a VPC that has a subnet group. Only valid VPCs are enabled in the list.
You can't change the VPC associated with this cluster after the cluster has been created. Learn more
VPC security groups
This VPC security group defines which subnets and IP ranges the cluster can use in the VPC.
Choose one or more security groups
default
sg-e82ceac9
Cluster subnet group
Choose the Amazon Redshift subnet group to launch the cluster in.
Availability Zone
Specify the Availability Zone that you want the cluster to be created in. Otherwise, Amazon Redshift chooses an Availability Zone for you.
No preference
Enhanced VPC routing
Forces cluster traffic through a VPC.
Disabled
Enabled
Publicly accessible
Allow instances and devices outside the VPC connect to your database through the cluster endpoint.


What will be migrated ?
Which Service wiil be used ?
DATA
DataSync
DATABASE
Database Migration Service
VM SERVER
Server Migration Service
On-Premises
VM Import/Export
Track the process of the migration (All kind)
Migration Hub


aws
External
Custom key store (CloudHSM)
AWS CloudHSM
Customer managed keys
AWS managed keys
AWS KMS

Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

Author from scratch
Start with a simple Hello World example.

Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.

Container image
Select a container image to deploy for your function.

Browse serverless app repository
Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

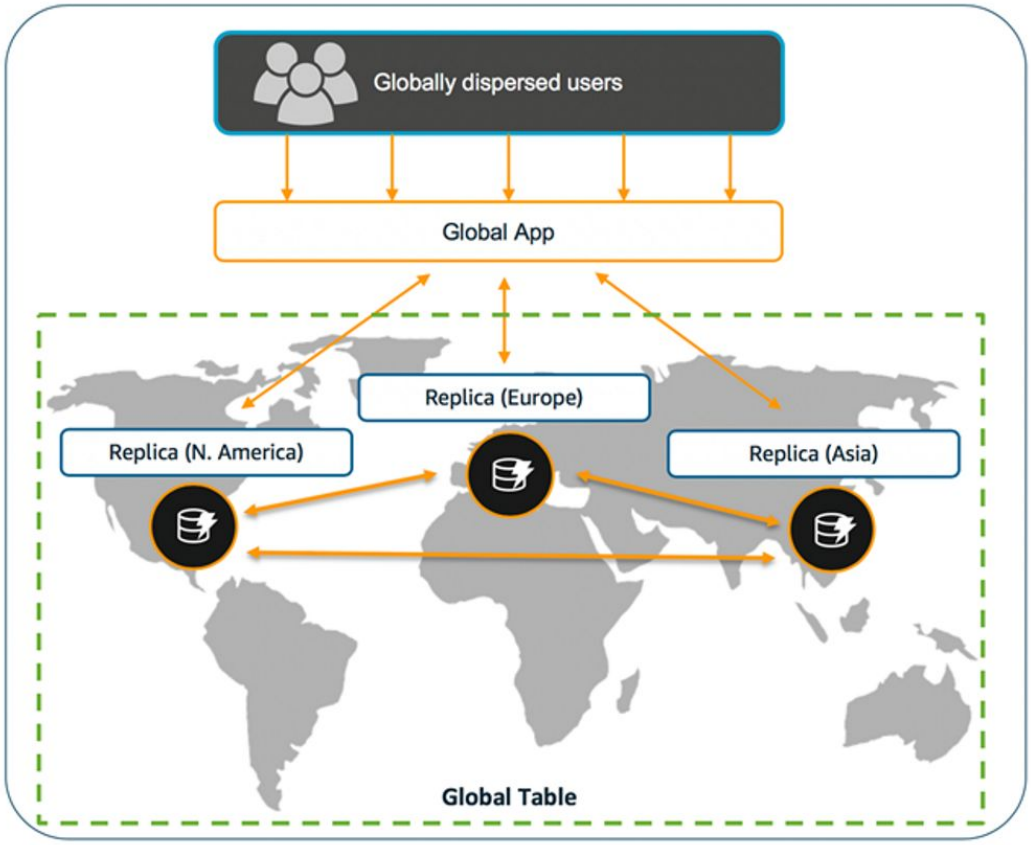
Function name
Enter a name that describes the purpose of your function.

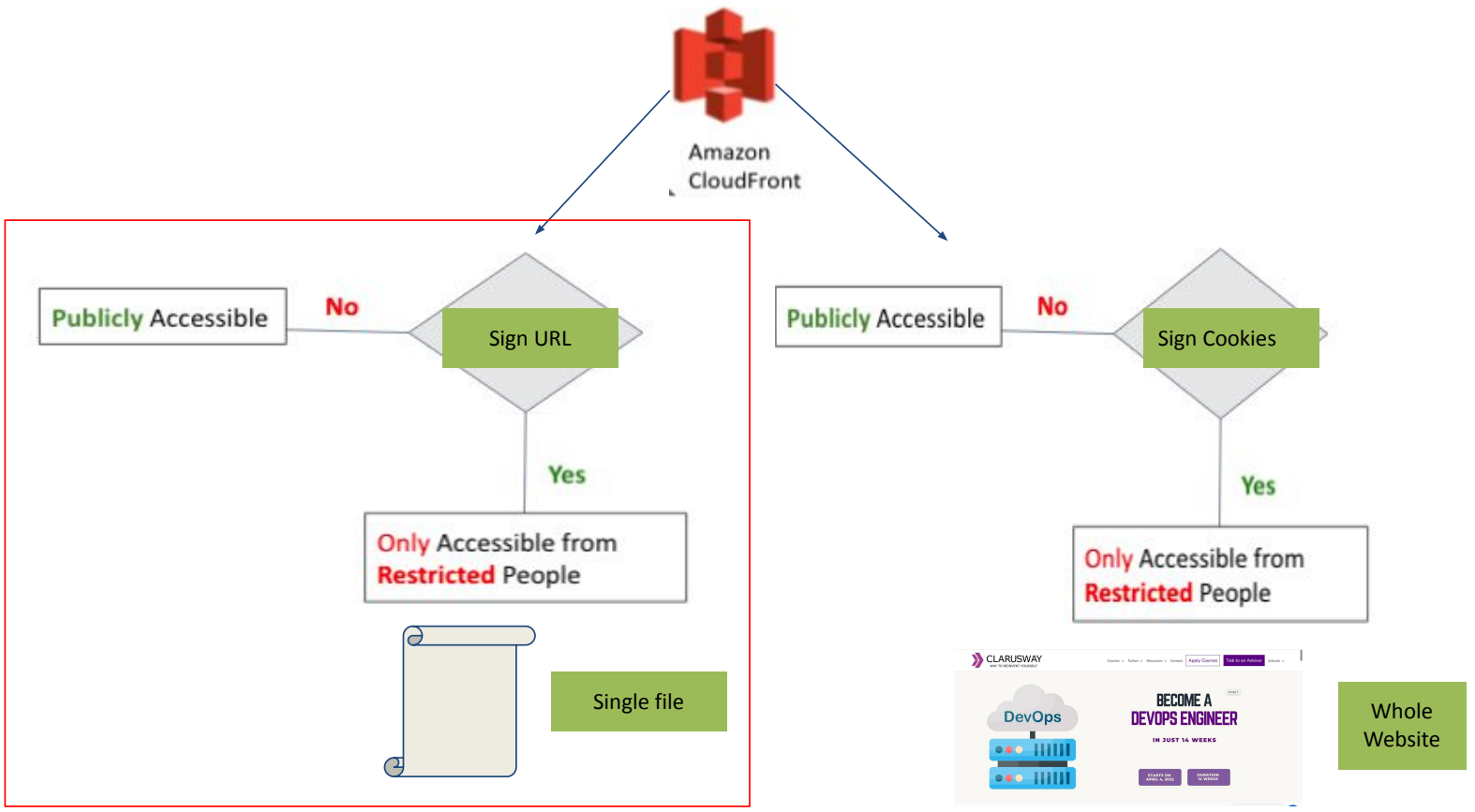
myFunctionName

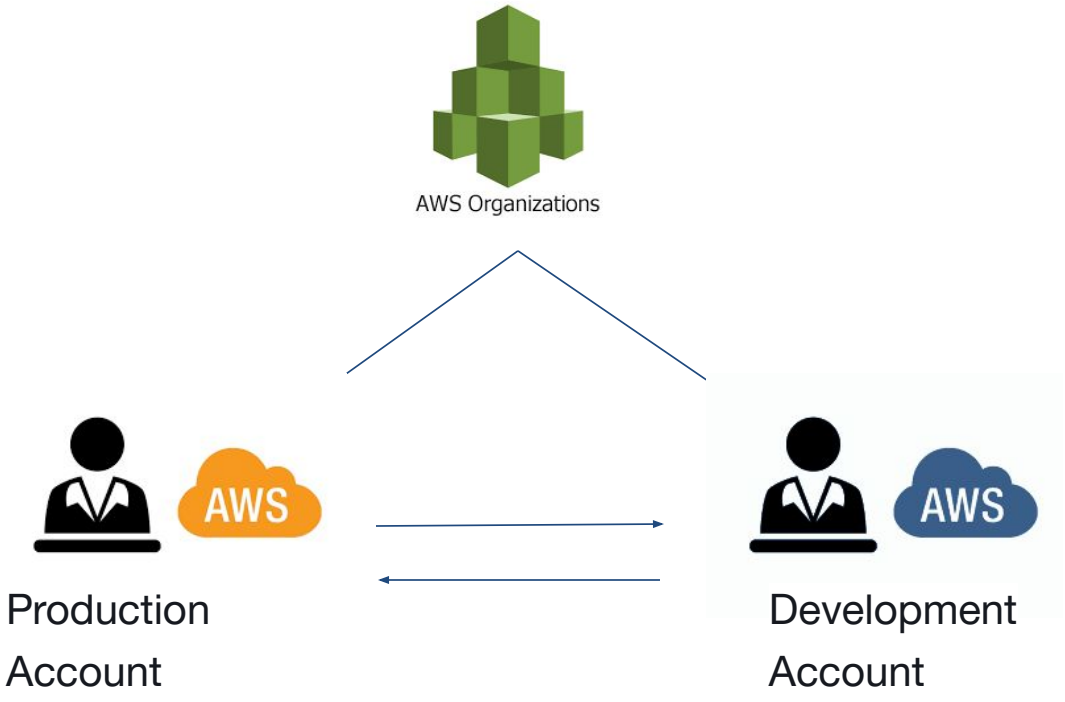
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

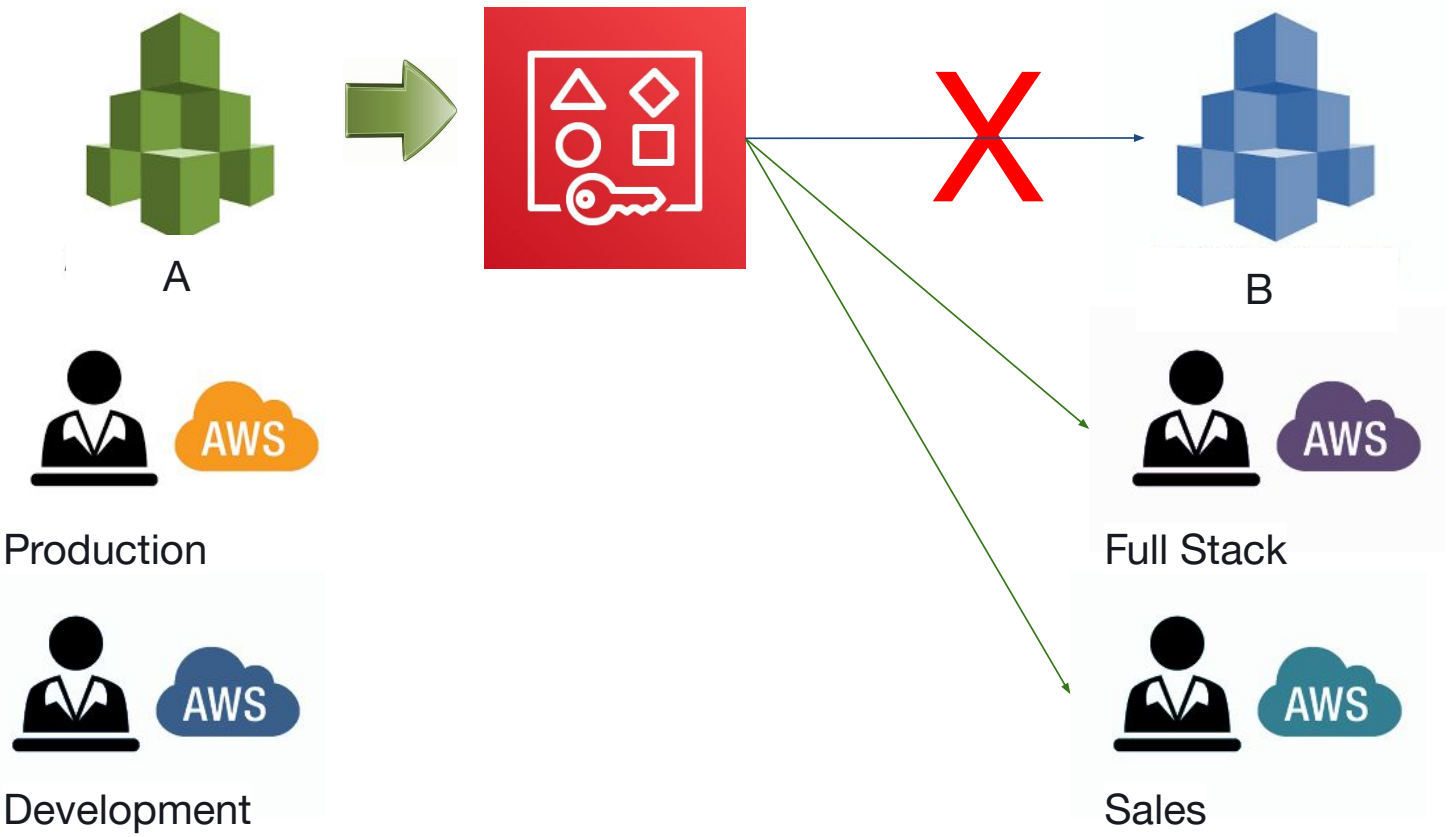
.NET Core 3.1 (C#/PowerShell)

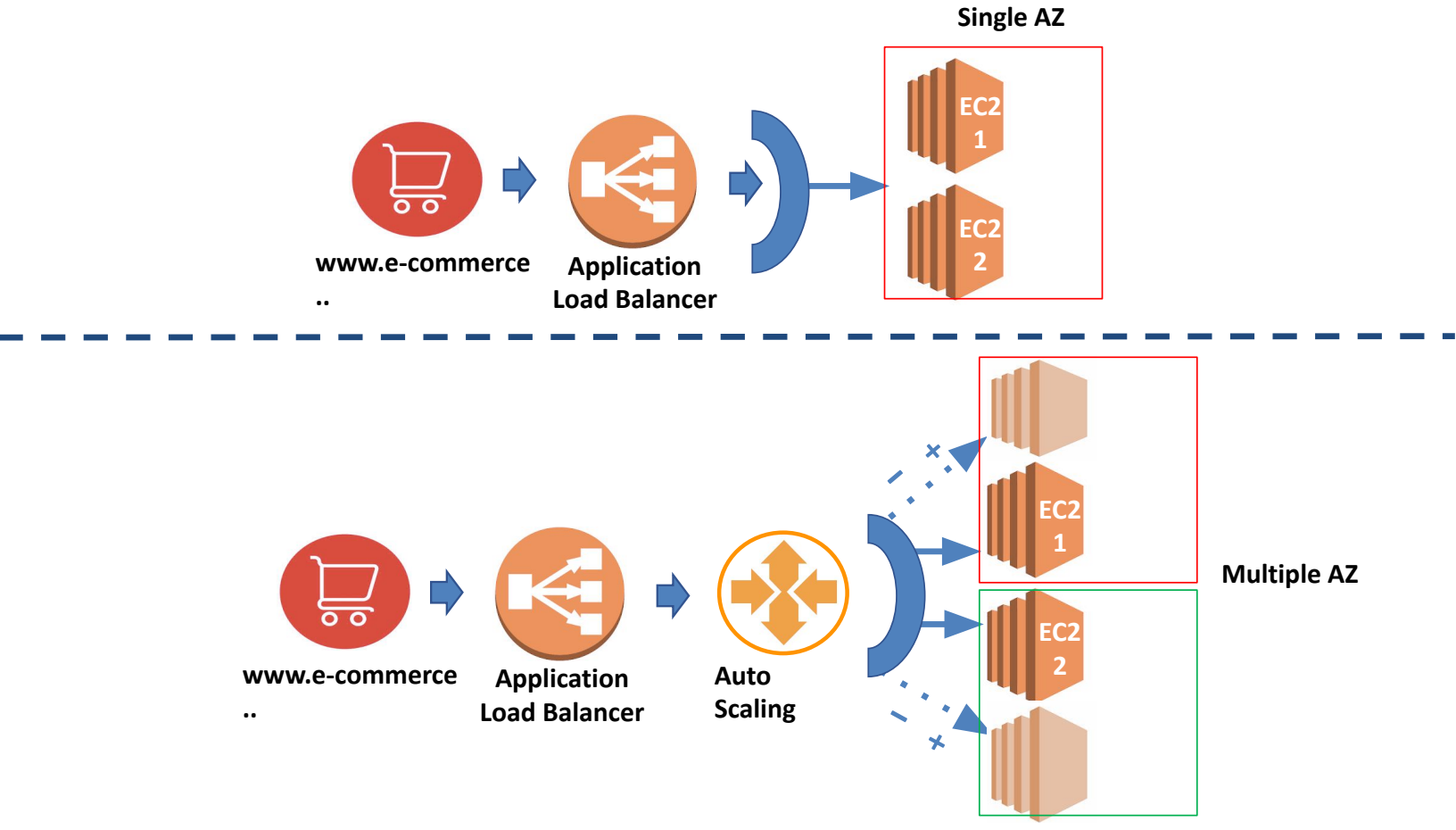


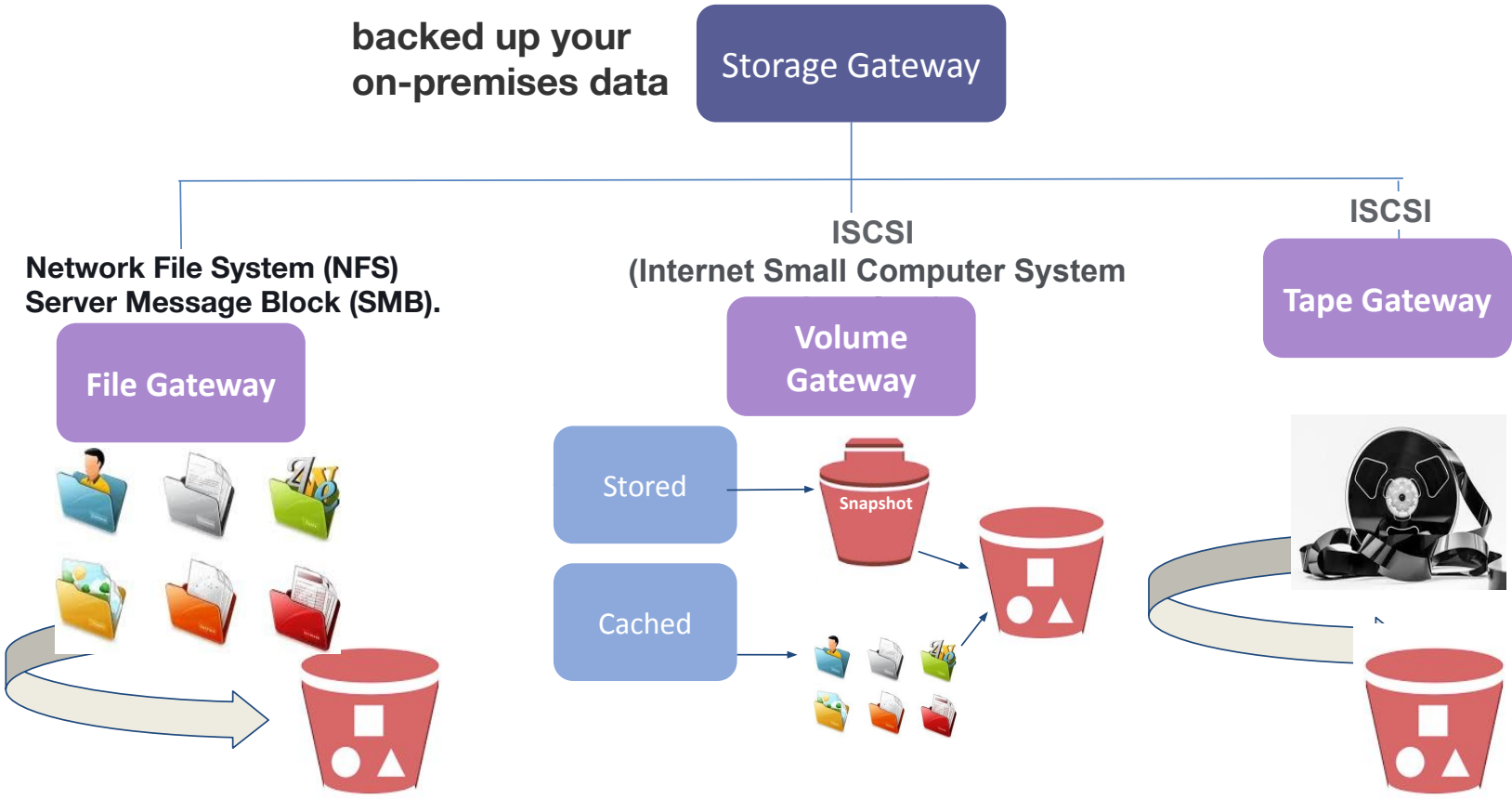




- [x] Enable resource sharing in AWS Organizations with RAM


A
B
AWS
Production
AWS
Full Stack
AWS
Development
AWS
Sales


Single AZ
EC2 1
EC2 2
www.e-commerce ..
Application Load Balancer
EC2 1
EC2 2
www.e-commerce ..
Application Load Balancer
Auto Scaling
Multiple AZ



Info: The term **legacy** database commonly refers to a database that has been in use for many years and is therefore unsuitable for modern apps and environments.

- DMS create a replication instance for migrating. Your databases are fully operational when migrating.

- Homogeneous database migrations **(Oracle to Oracle)** **(Engine conversion)**
Heterogenous database migrations **(Microsoft SQL to Aurora)**

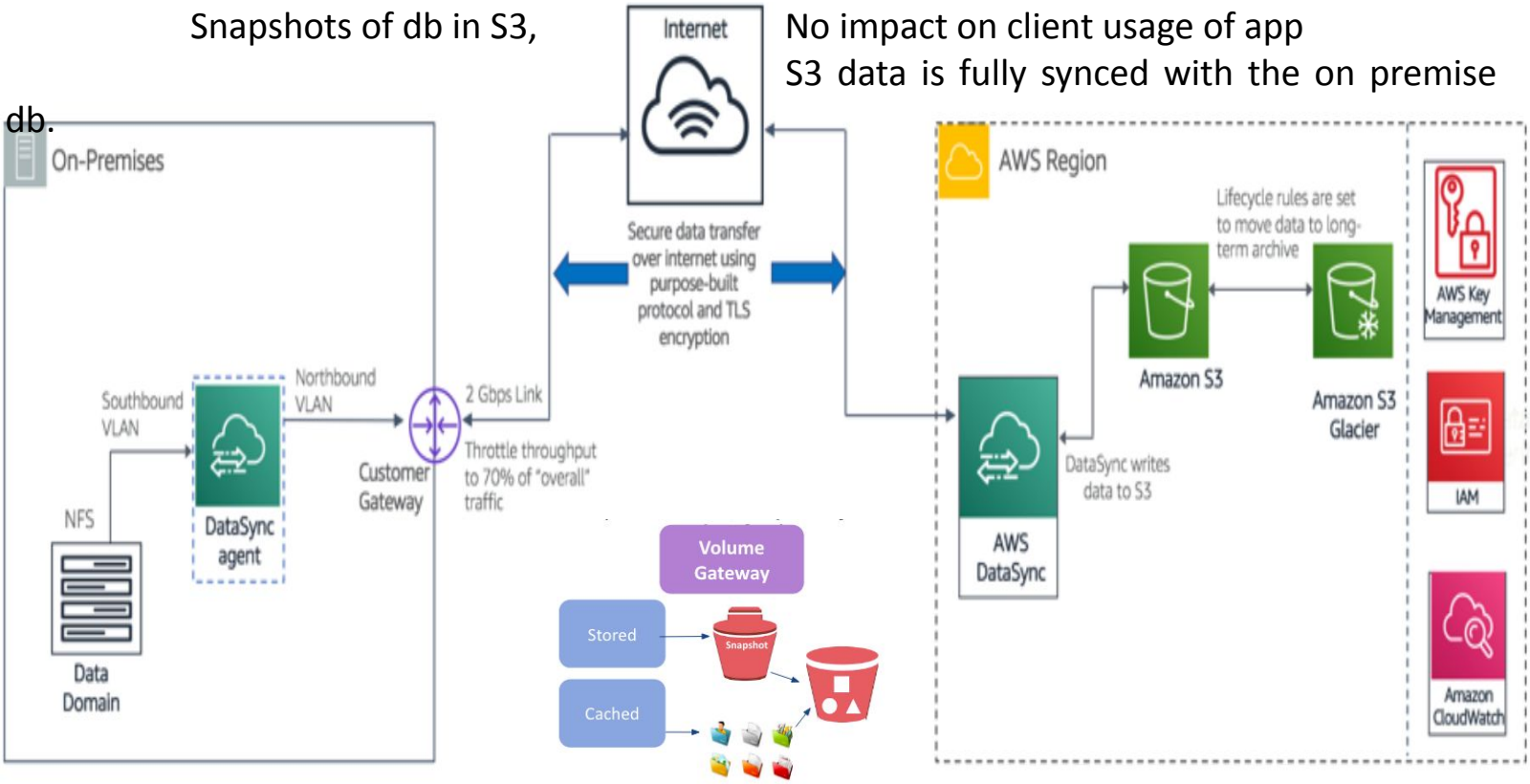
- Use **SCT (Schema conversion tool)** from one schema to another schema for **Heterogenous migrations**

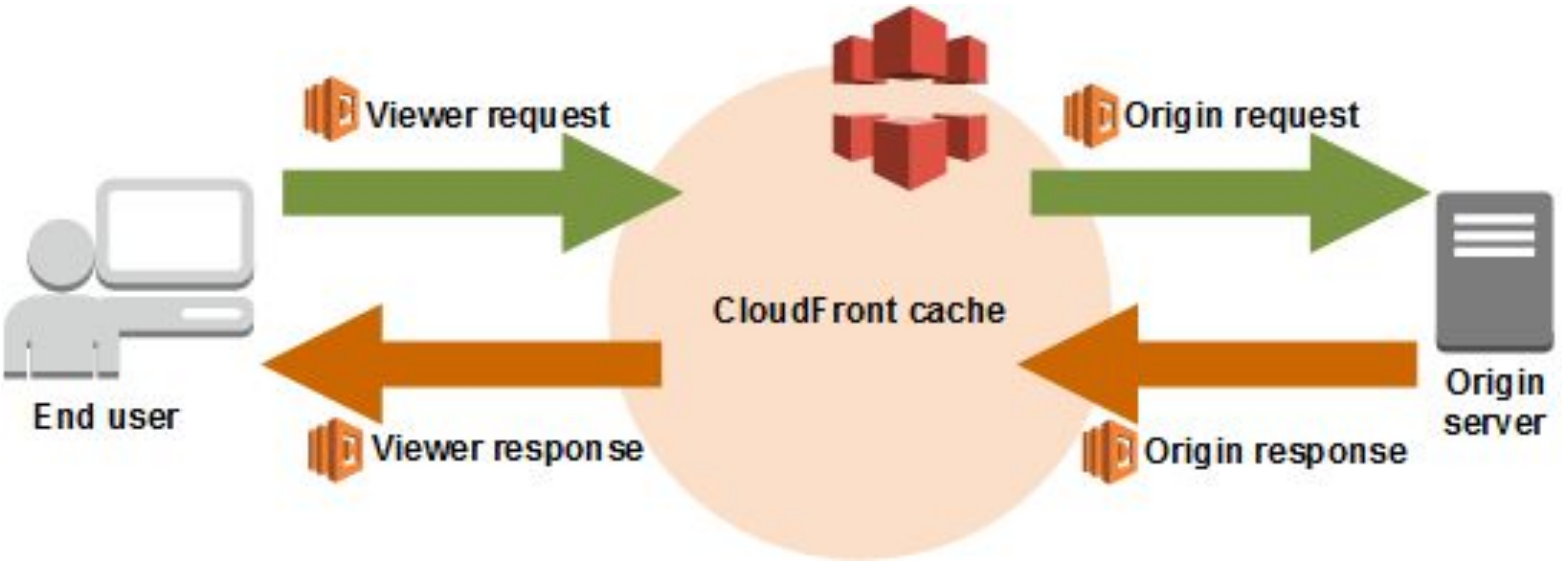
From Legacy to DynamoDb >>>>>>> Heterogenous database migrations

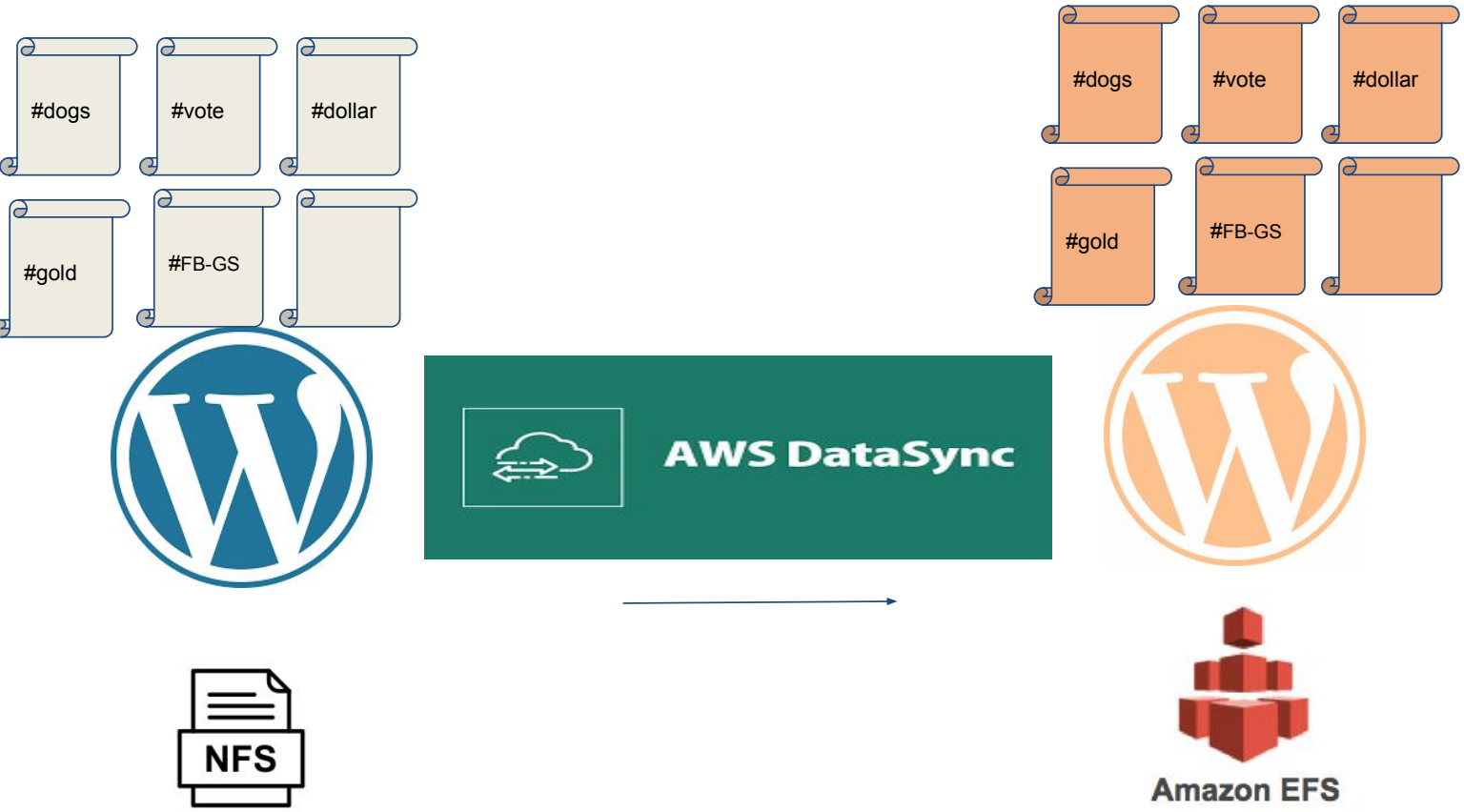
SCT (Schema conversion tool)

KEY words: Transfer db to AWS ,
Snapshots of db in S3,

No impact on client usage of app
S3 data is fully synced with the on premise db.







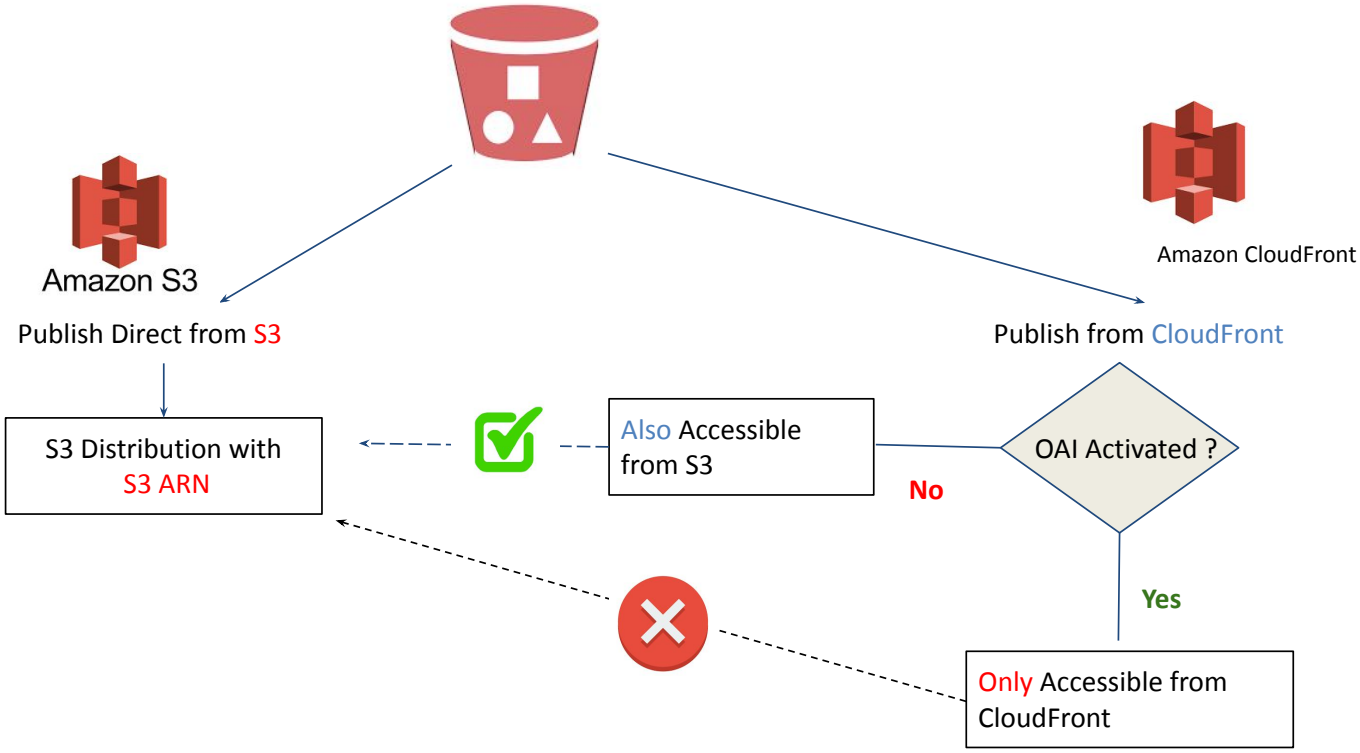
Architecting for the Cloud AWS Best Practices

A stateless application is an application that does not need knowledge of previous interactions and does not store session information. For example, an application that, given the same input, provides the same response to any end user, is a stateless application.

Couple :

Lambda=Stateless

- **Source of the distribution** >>>> OAI >>> from Where
- **Restricted user** >>>> Pre Sign url/cookies >>>> Who (Slide-10)



Edit Behavior

Default Cache Behavior Settings

Path Pattern Default (*)

Origin or Origin Group S3-media-sharing-website-bucket

Viewer Protocol Policy
- (•) HTTP and HTTPS
- ( ) Redirect HTTP to HTTPS
- ( ) HTTPS Only

by default it is http and https.

Allowed HTTP Methods
- (•) GET, HEAD
- ( ) GET, HEAD, OPTIONS
- ( ) GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Field-level Encryption Config

Cached HTTP Methods GET, HEAD (Cached by default)

Cache and origin request settings
- (•) Use a cache policy and origin request policy
- ( ) Use legacy cache settings

Cache Policy Managed-CachingOptimized — Create a new policy

View policy details

Learn More

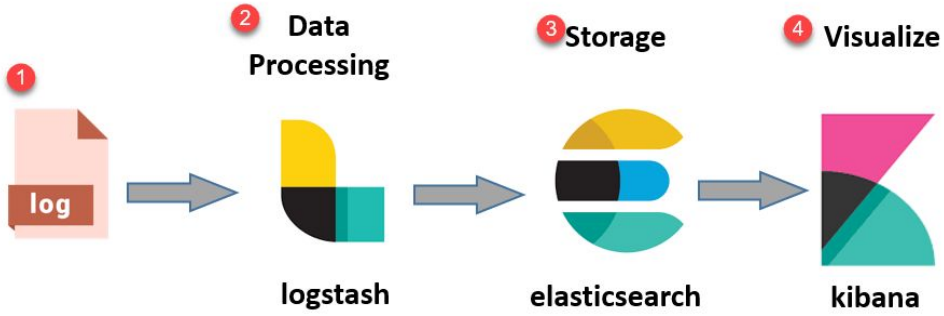
Origin Request Policy — Create a new policy

View policy details

Learn More

Smooth Streaming
- ( ) Yes
- (•) No

Restrict Viewer Access (Use Signed URLs or Signed Cookies)
- ( ) Yes
- (•) No



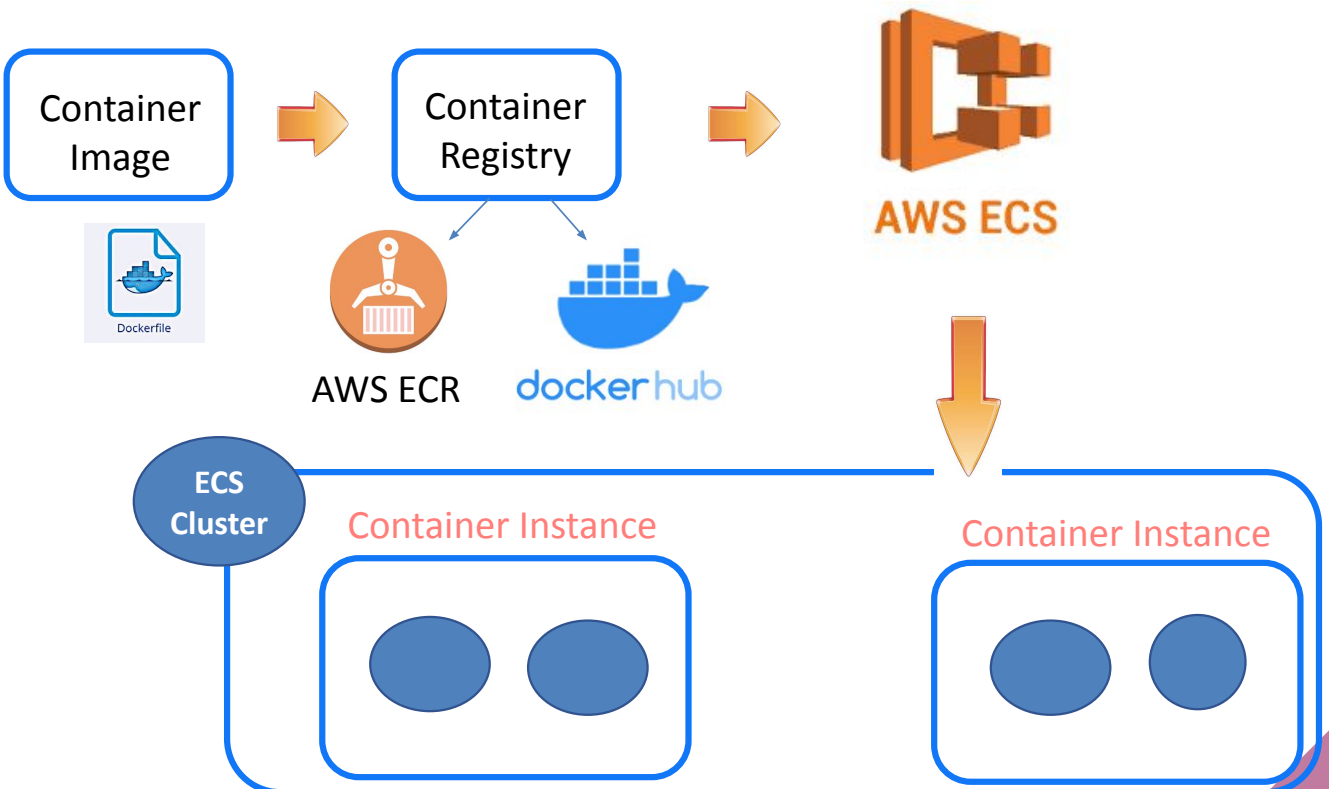
Not open source till January 21, 2021

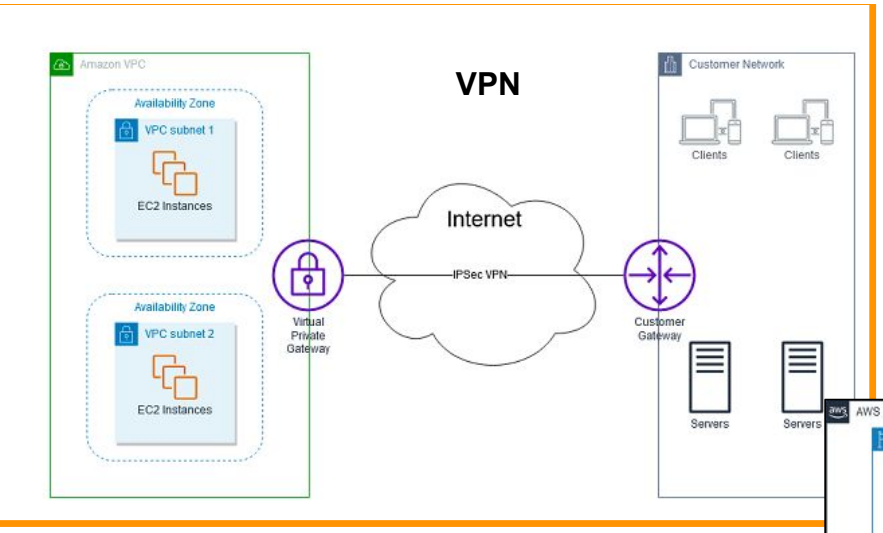
AWS Lambda

OpenSearch

Amazon OpenSearch Service

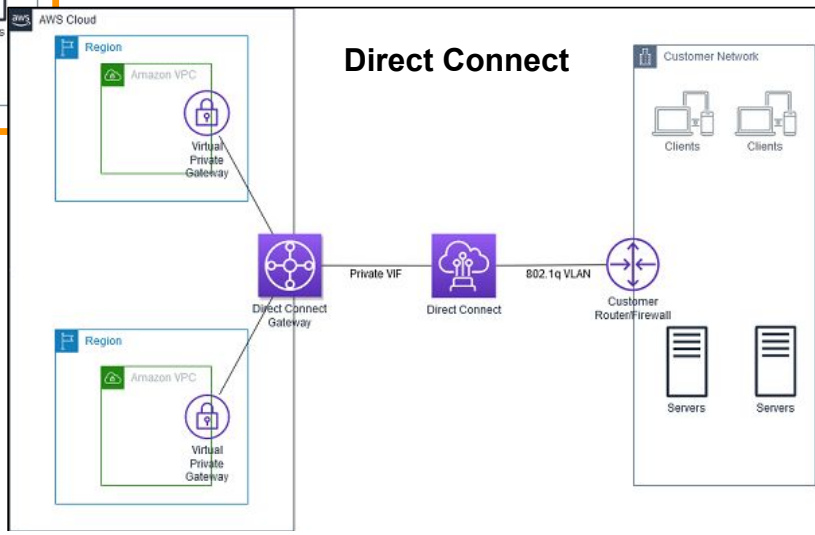
Data Firehouse	- (built-in support)
S3	+
Cloudwatch Logs	- (use Cloudwatch Subscription)
AIOT	- (use MQTT)





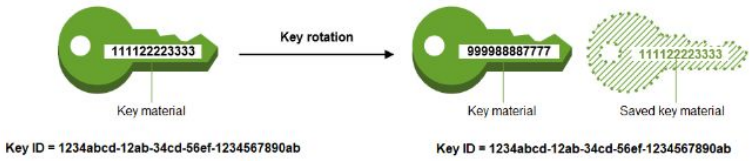
Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure."

VPN connections are very cheap (**$37.20**/month
Built in a few minutes

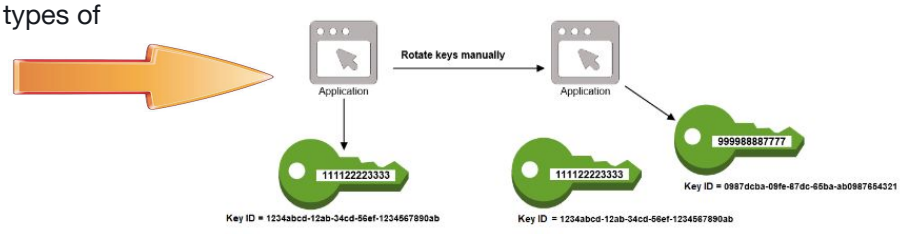


Rotating AWS KMS keys

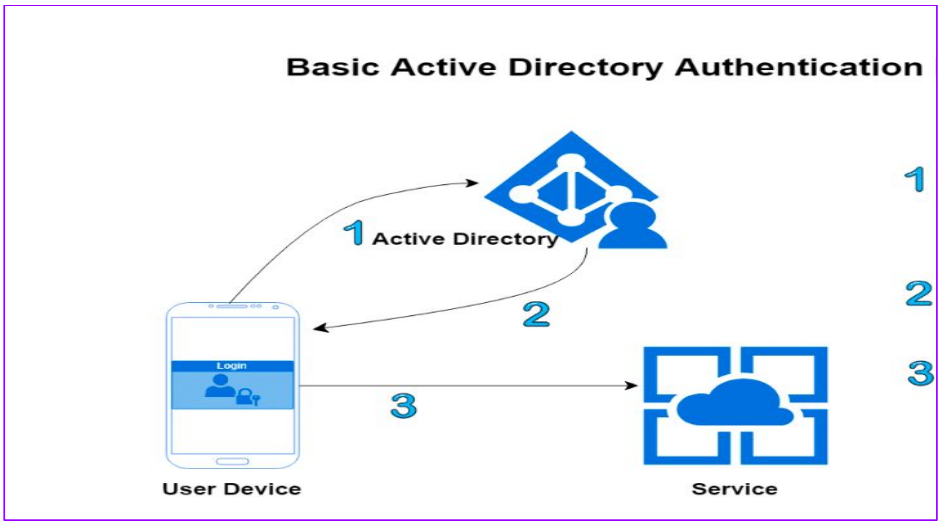
Automatic key rotation is supported only on symmetric KMS keys



Automatic key rotation is *not* supported on the following types of KMS keys, but you can rotate these KMS keys manually.



- Asymmetric KMS keys
- KMS keys in custom key stores
- KMS keys with imported key material

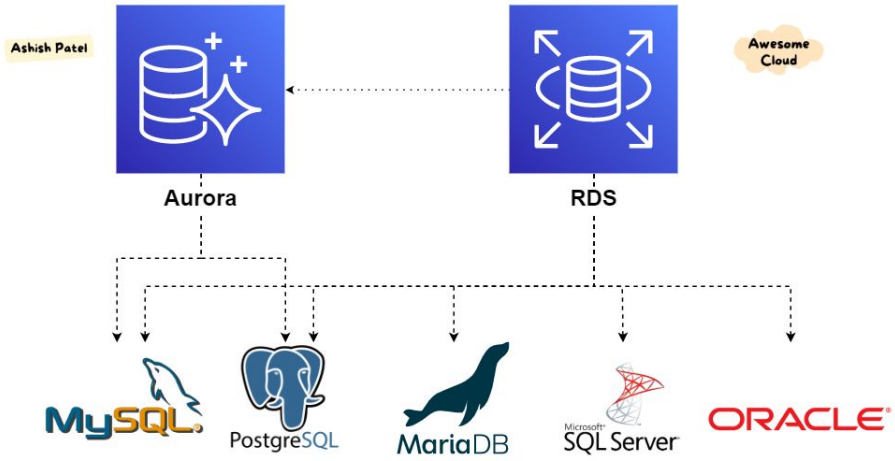


AWS Directory Service for Microsoft Active Directory

Simple AD

AD Connector

Amazon Cognito



RDS Mysql can grow to 16 Tb
Aurora (Mysql) automatically up to 64 Tb.

In the question : Migrate 5 tb Mysql to AWS. 5Tb will increase in the future.

Getting started wizard

Step 1: Create identity pool

Step 2: Set permissions

Create new identity pool

Identity pools are used to store end user identities. To declare a new identity pool, enter a unique name.

Identity pool name* kibana_identities

Example: My App Name

Unauthenticated identities

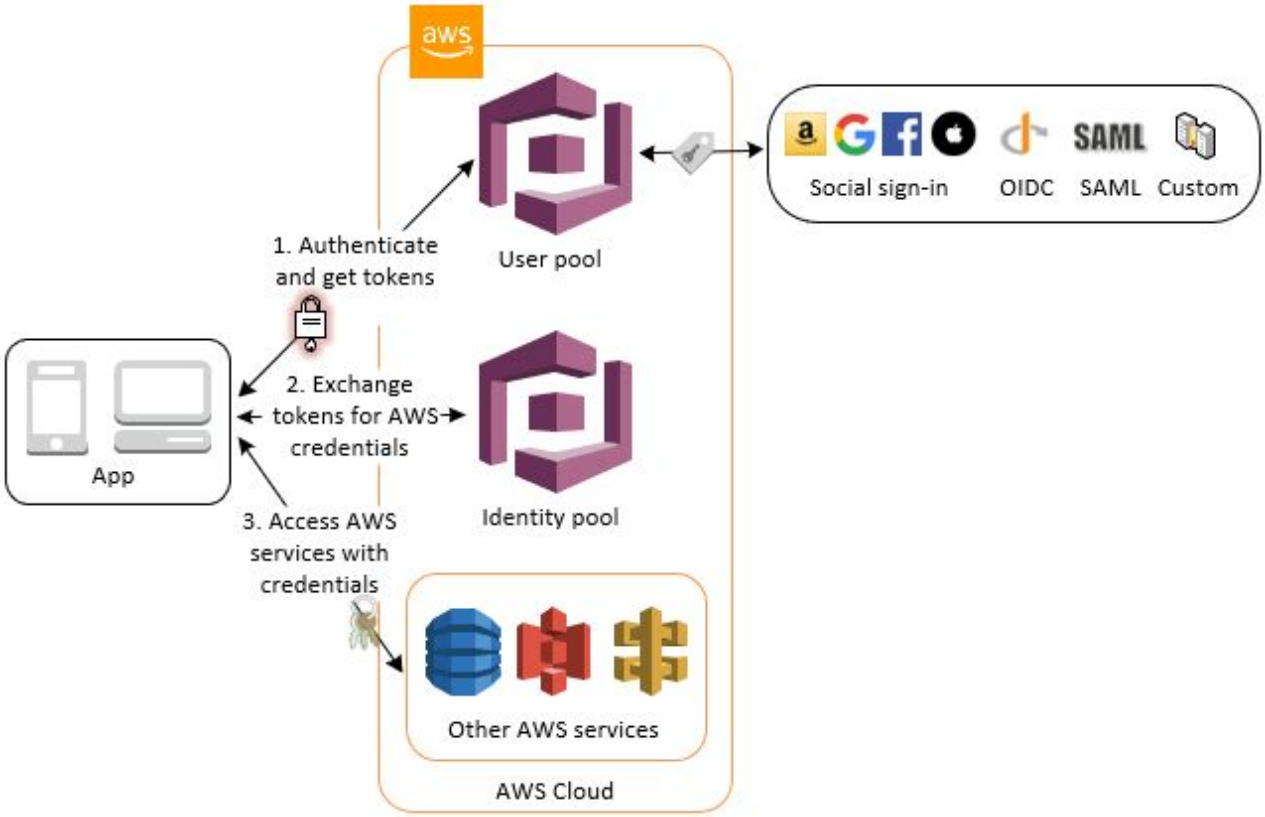
Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials for users who do not authenticate with an identity provider. If your application allows customers to use the application without logging in, you can enable access for unauthenticated identities. Learn more about unauthenticated identities.

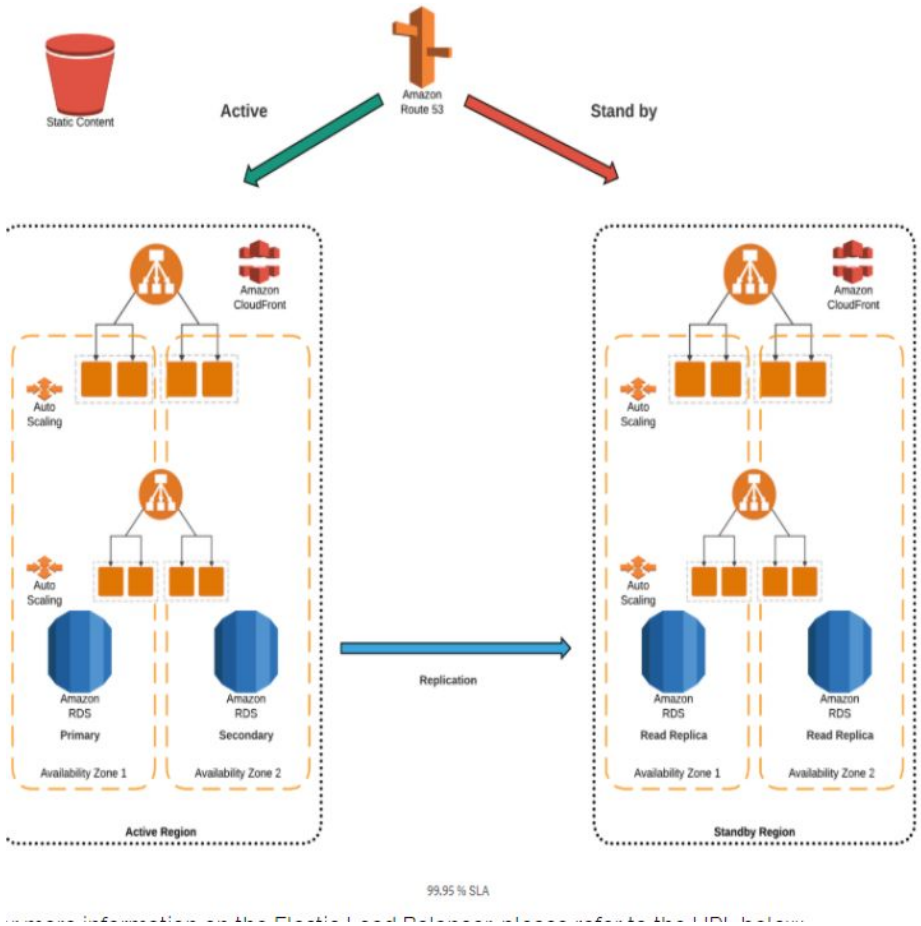
☑ Enable access to unauthenticated identities

Authentication providers

*** Required**

Cancel **Create Pool**





User

User IP: 7.8.9.10/32

Connection Request	
No	Type-Port
1	SSH-22

EC2

Security Group-Inbound

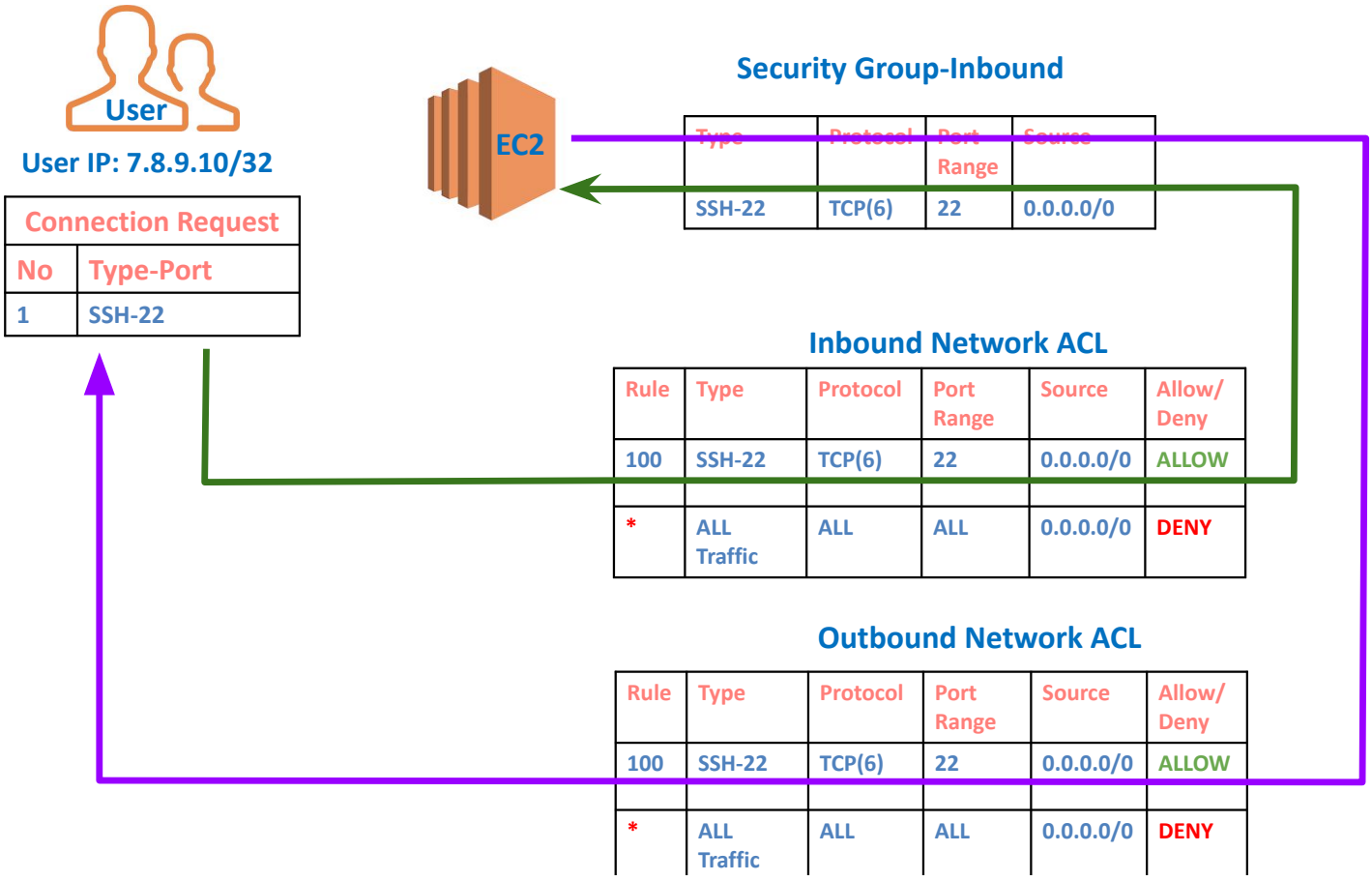
Type	Protocol	Port Range	Source
SSH-22	TCP(6)	22	0.0.0.0/0

Inbound Network ACL

Rule	Type	Protocol	Port Range	Source	Allow/ Deny
100	SSH-22	TCP(6)	22	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Outbound Network ACL

Rule	Type	Protocol	Port Range	Source	Allow/ Deny
100	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



The 12 requirements of PCI are:

Install and maintain a firewall configuration to protect cardholder data
Do not use vendor-supplied defaults for system passwords and other security parameters
Protect stored cardholder data
Encrypt transmission of cardholder data across open, public networks
Use and regularly update anti-virus software or programs
Develop and maintain secure systems and applications
Restrict access to cardholder data by business need to know
Assign a unique ID to each person with computer access
Restrict physical access to cardholder data
Track and monitor all access to network resources and cardholder data
Regularly test security systems and processes
Maintain a policy that addresses information security for all personnel

PCI Payment Card Industry

CSAA Practice Test 2

Osvaldo

02 April 2022