Lifecycle rule actions

Choose the actions you want this rule to perform. Per-request fees apply. **Learn more** ↗ or see **Amazon S3 pricing** ↗

- ☐ Transition *current* versions of objects between storage classes
- ☐ Transition *previous* versions of objects between storage classes
- ☐ Expire *current* versions of objects
- ☐ Permanently delete *previous* versions of objects
- ☐ Delete expired delete markers or incomplete multipart uploads

When a lifecycle rule is scoped with tags, these actions are unavailable.

ASG Scaling Policy

Predictive scaling

Dynamic scaling

Scheduled Action
Specific time or event
Time :09:00 am

Target tracking

When: CPU >50
How: AWS
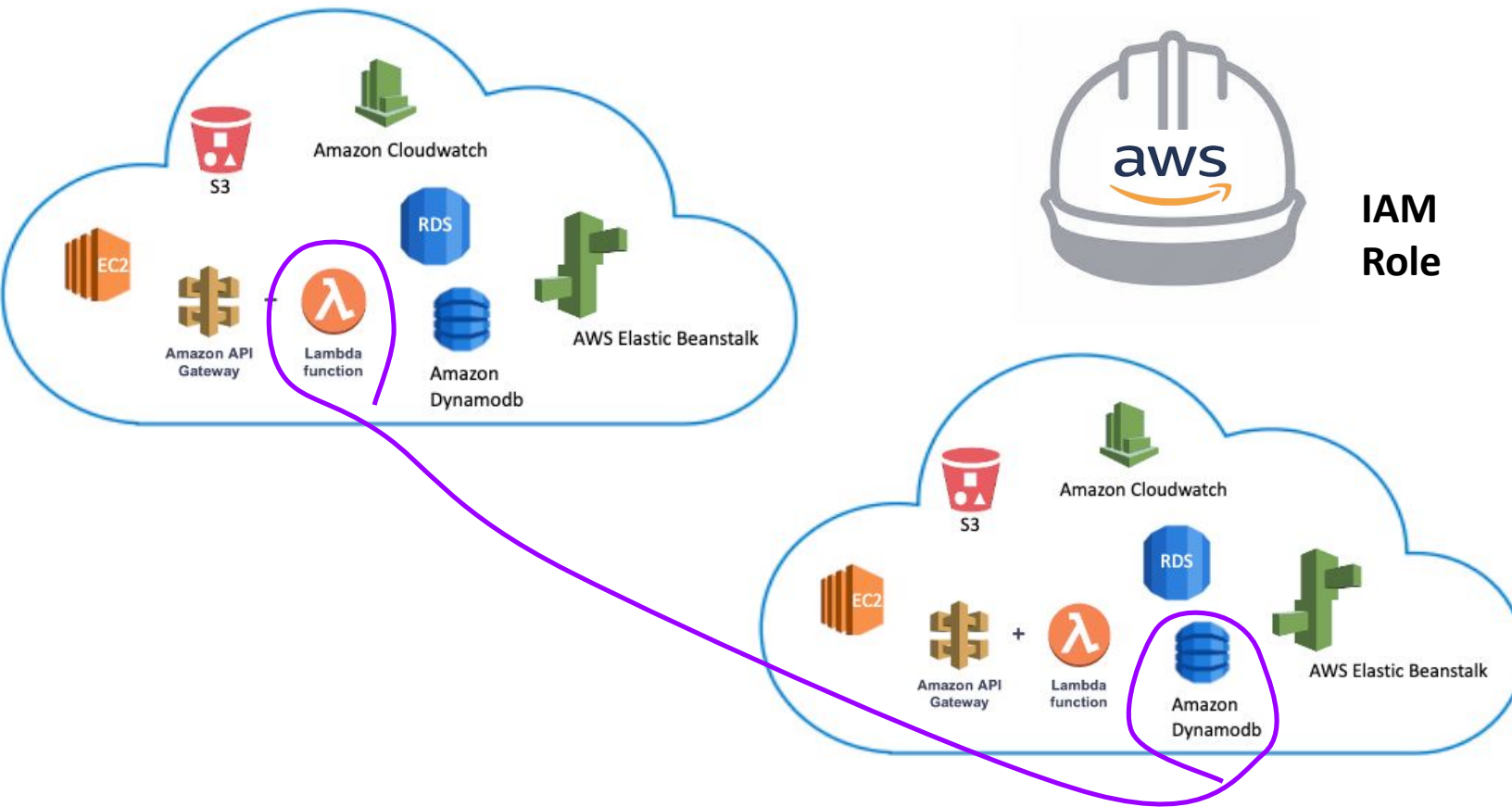determine itself

Simple

When: CPU >50
How: Add 1 EC2
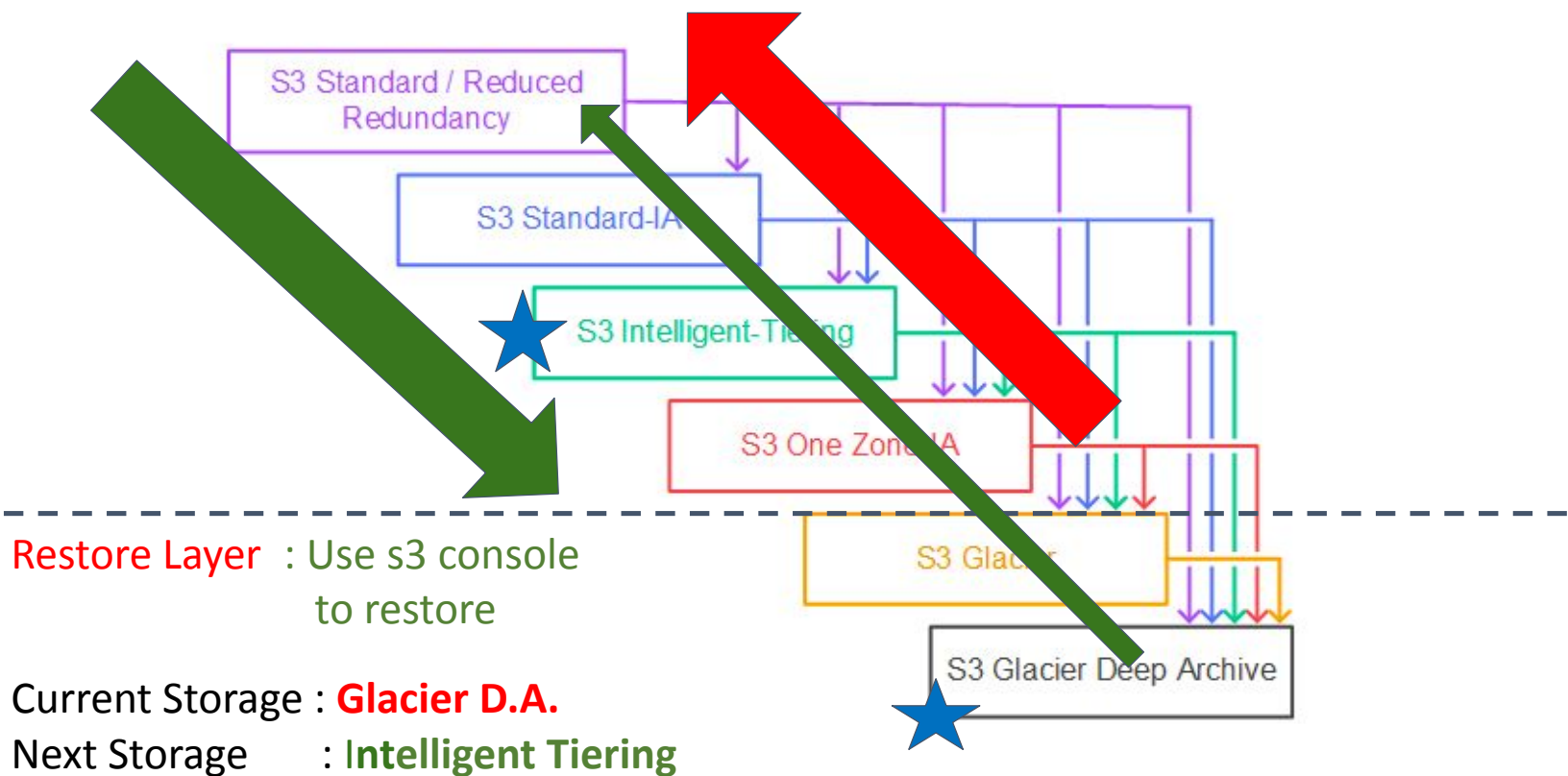
Step

Step 1:
- When: 50<CPU<80
- How: Add 1 EC2

Step:2
- When: CPU >80
- How: Add 2 EC2

IAM Role

S3 Lifecycle Configuration-AWS console or CLI

S3 Standard / Reduced Redundancy

S3 Standard-IA

S3 Intelligent-Tiering

S3 One Zone IA

S3 Glacier

S3 Glacier Deep Archive

Restore Layer : Use s3 console to restore

Current Storage : **Glacier D.A.**
Next Storage : **Intelligent Tiering**

Amazon FSx file systems

FSX (N)

Amazon FSx for NetApp ONTAP

Fully managed shared storage built on NetApp's popular ONTAP file system.

FSX z=

Amazon FSx for OpenZFS

Fully managed shared storage built on the popular OpenZFS file system.

FSX □

Amazon FSx for Windows File Server

Fully managed shared storage built on Windows Server.

FSX ⌂

Amazon FSx for Lustre

Fully managed shared storage built on the world's most popular high-performance file system.

EFS

- For Linux Instance
- Can't write/read S3

- Compatible with Windows Active Directory

- HPC
- Compatible with S3

- Compatible with FSx File Gateway

Cost Savings Plan

1 year/1000 dollars/limit

Compute
Saving Plans

EC2
Fargate
Lambda

%66 Cost Saving

EC2 Instance
Saving Plans

EC2

%72 Cost Saving

Reserved Instances

1 year/1500 dollars/limitless

Convertible
RI (Reserved Instance)

EC2

%66 Cost Saving

Standart
RI (Reserved Instance)

EC2

%72 Cost Saving

convertible to the other size of instance

You are building an automated transcription service where Amazon EC2 worker instances process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. Customers fetch the text files frequently. You do not know about the storage capacity requirements. Which storage option would be both cost-efficient and highly available in this situation?
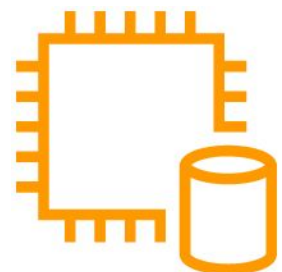
Amazon EBS

Amazon Glacier

amazon S3

Instance Store

Network ACL: acl-02fec58ef42e8e6e9

Default NACL

Details	**Inbound Rules**	Outbound Rules	Subnet associations	Tags

Edit inbound rules

View [All rules ▼]

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Edit outbound rules

View [All rules ▼]

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

On-Premises

| DATA | ➡ | DataSync | ➡ |

| DATABASE | ➡ | Database Migration Service | ➡ |

| VM SERVER | ➡ | Server Migration Service | ➡ |

VM Import/Export

Track the process of the migration (All kind)   **Migration Hub**

**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
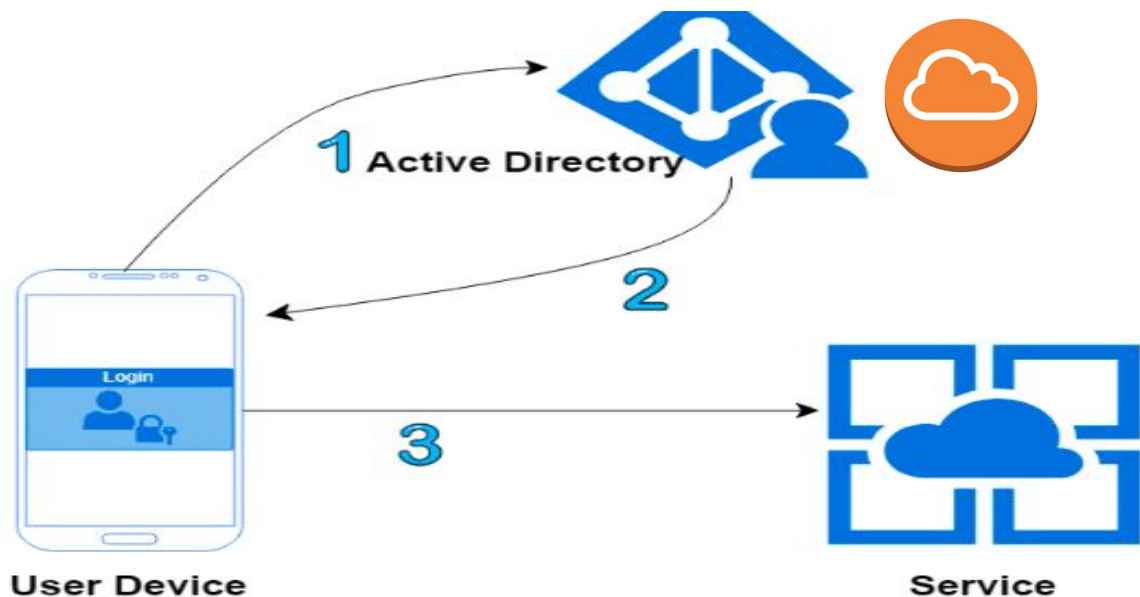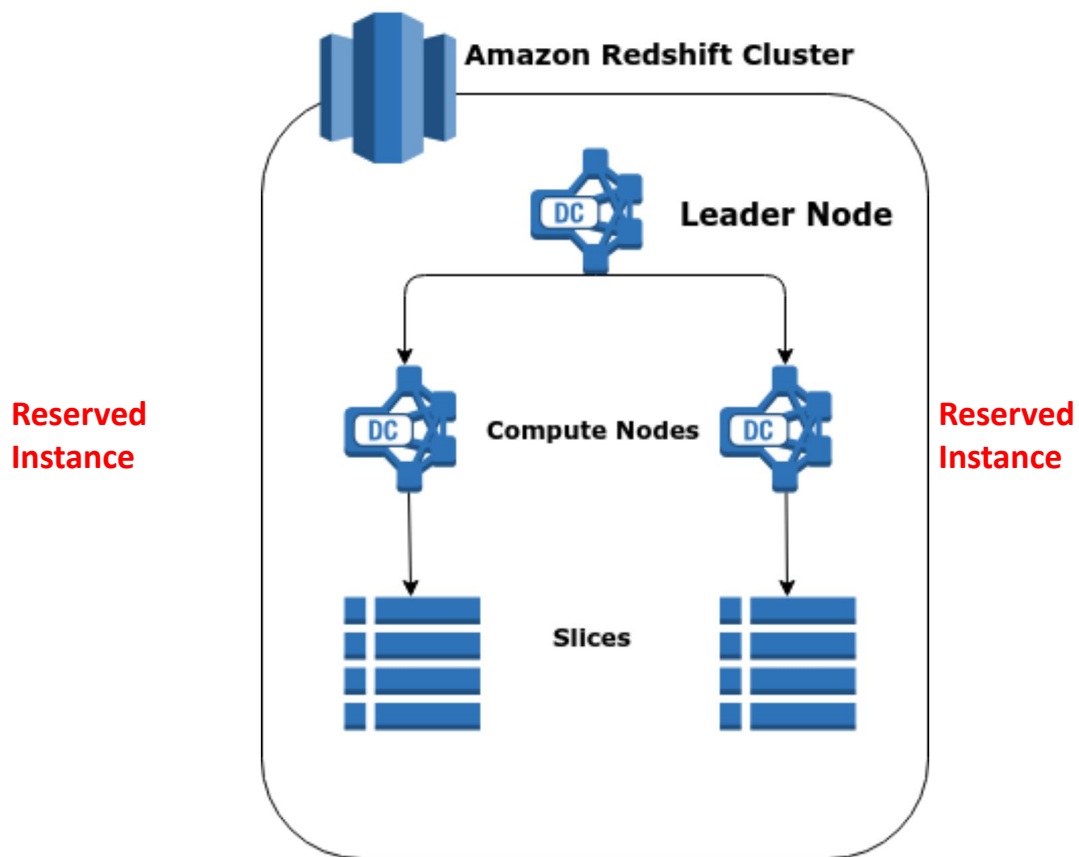queries
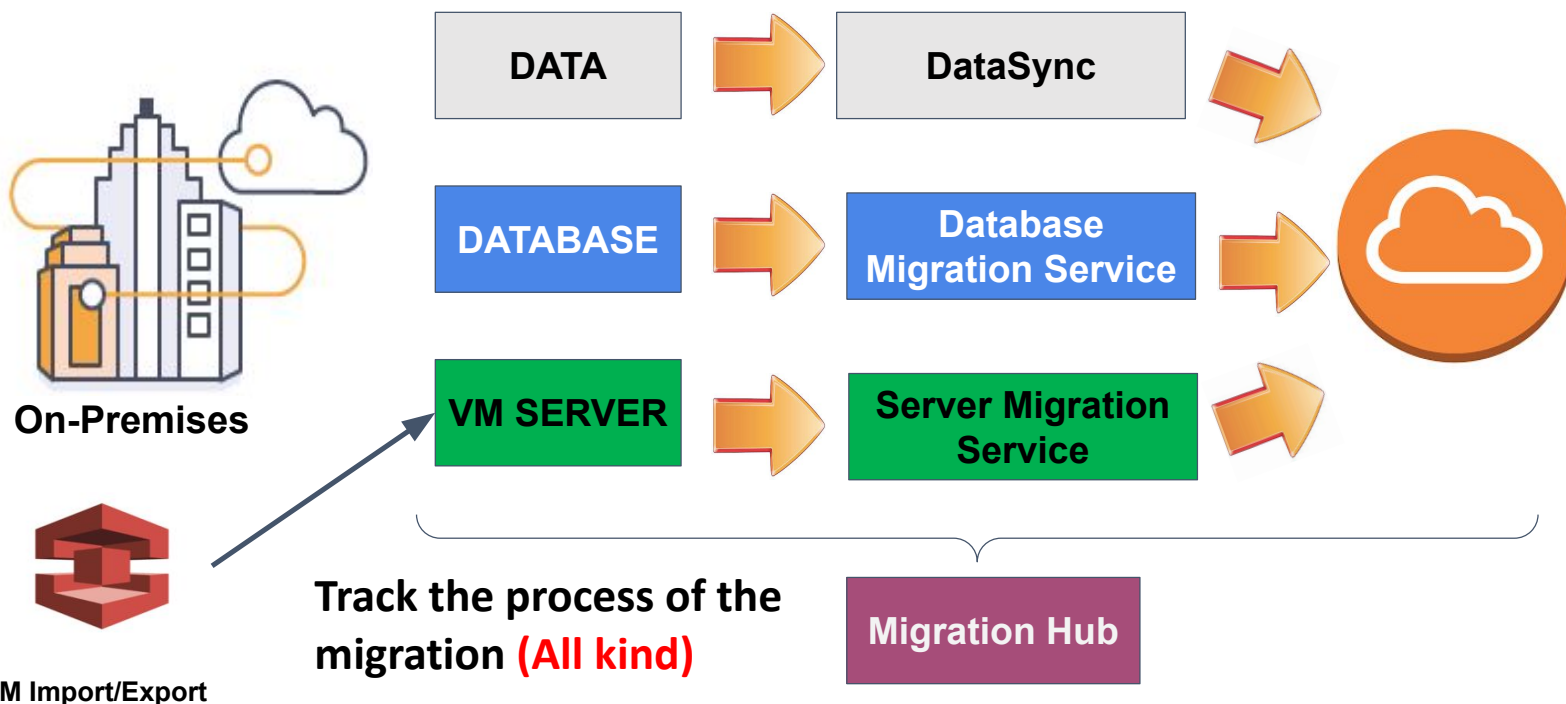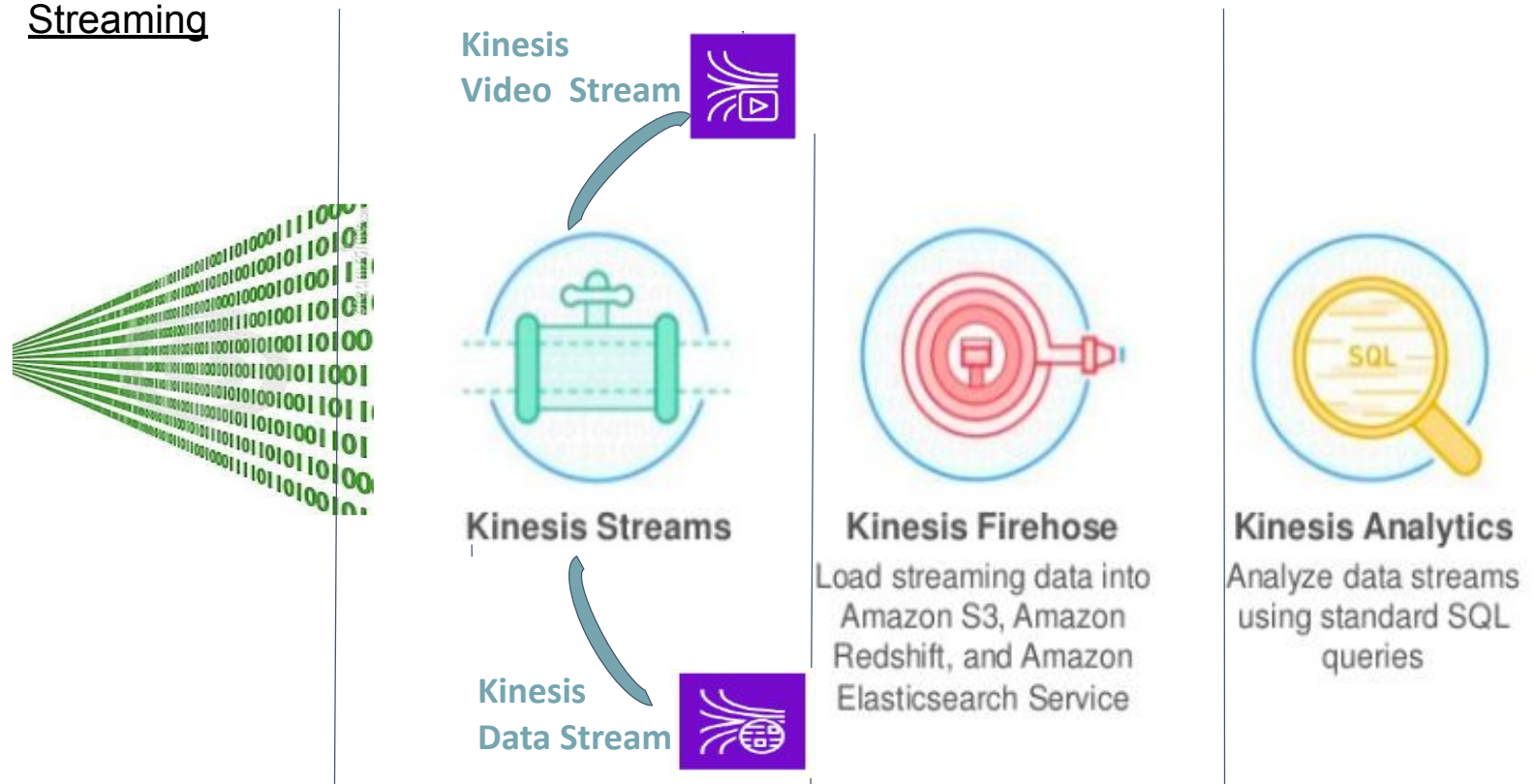
Your company authenticates users in a very disconnected network requiring each user to have several username/password combinations for different applications. You have been assigned a task of consolidating and migrating services to the cloud and reducing the number of usernames and passwords, employees need to use. What would you recommend?

1 **Active Directory**

2

3

Login

User Device

Service

Amazon Redshift Cluster

Leader Node

Compute Nodes

Slices

Reserved Instance

Reserved Instance

What will be migrated ?

Which Service wiil be used ?

On-Premises

DATA ➡ DataSync ➡

DATABASE ➡ Database Migration Service ➡

VM SERVER ➡ Server Migration Service ➡

Physical data transfer device

Snowball

Migration Hub

Linux operating system

Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.

200　　　○ Add to web ACL

PHP application

Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands.

100　　　○ Add to web ACL

POSIX operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not been allowed.

100　　　○ Add to web ACL

SQL database

Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries.

200　　　○ Add to web ACL

Windows operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code.
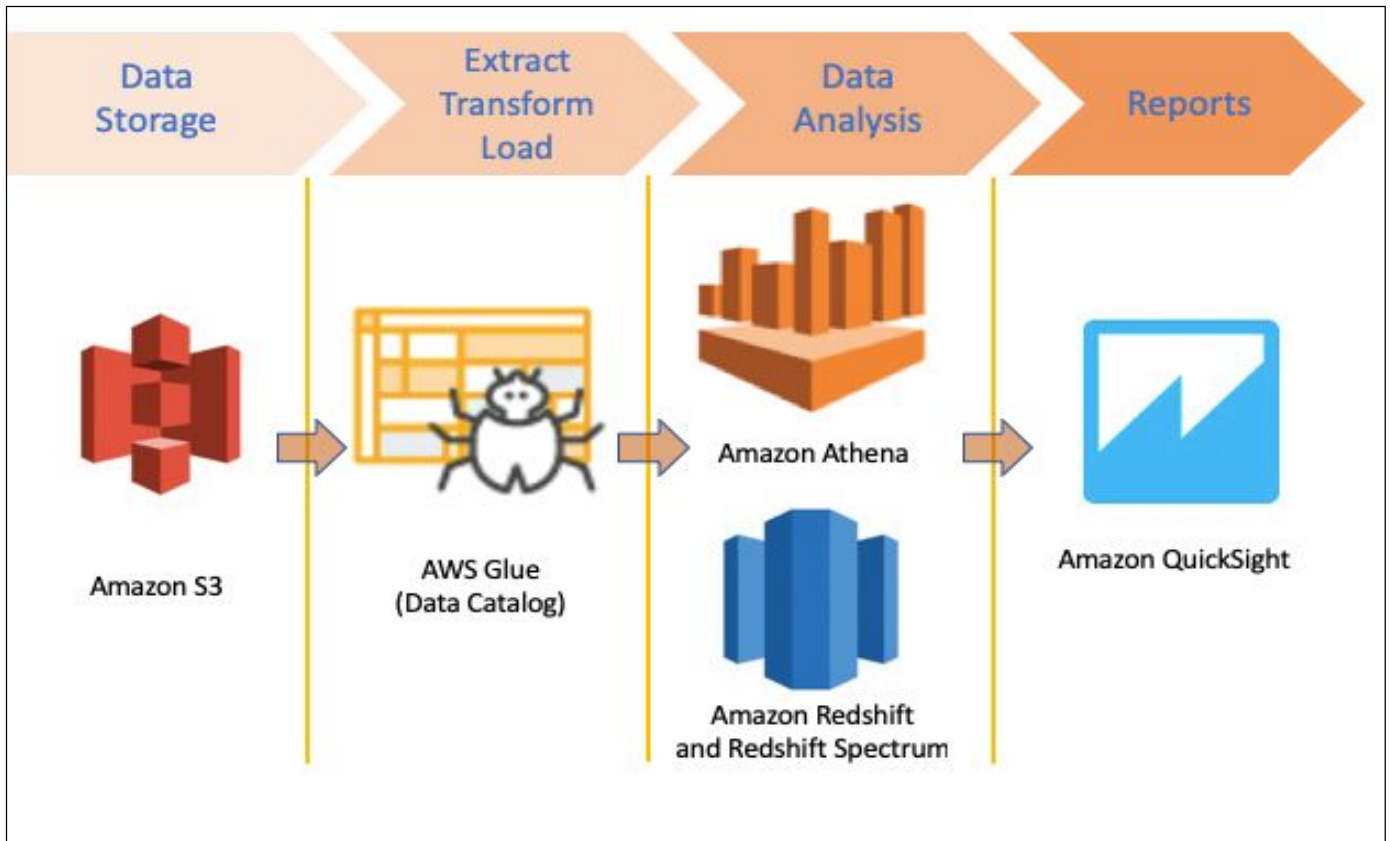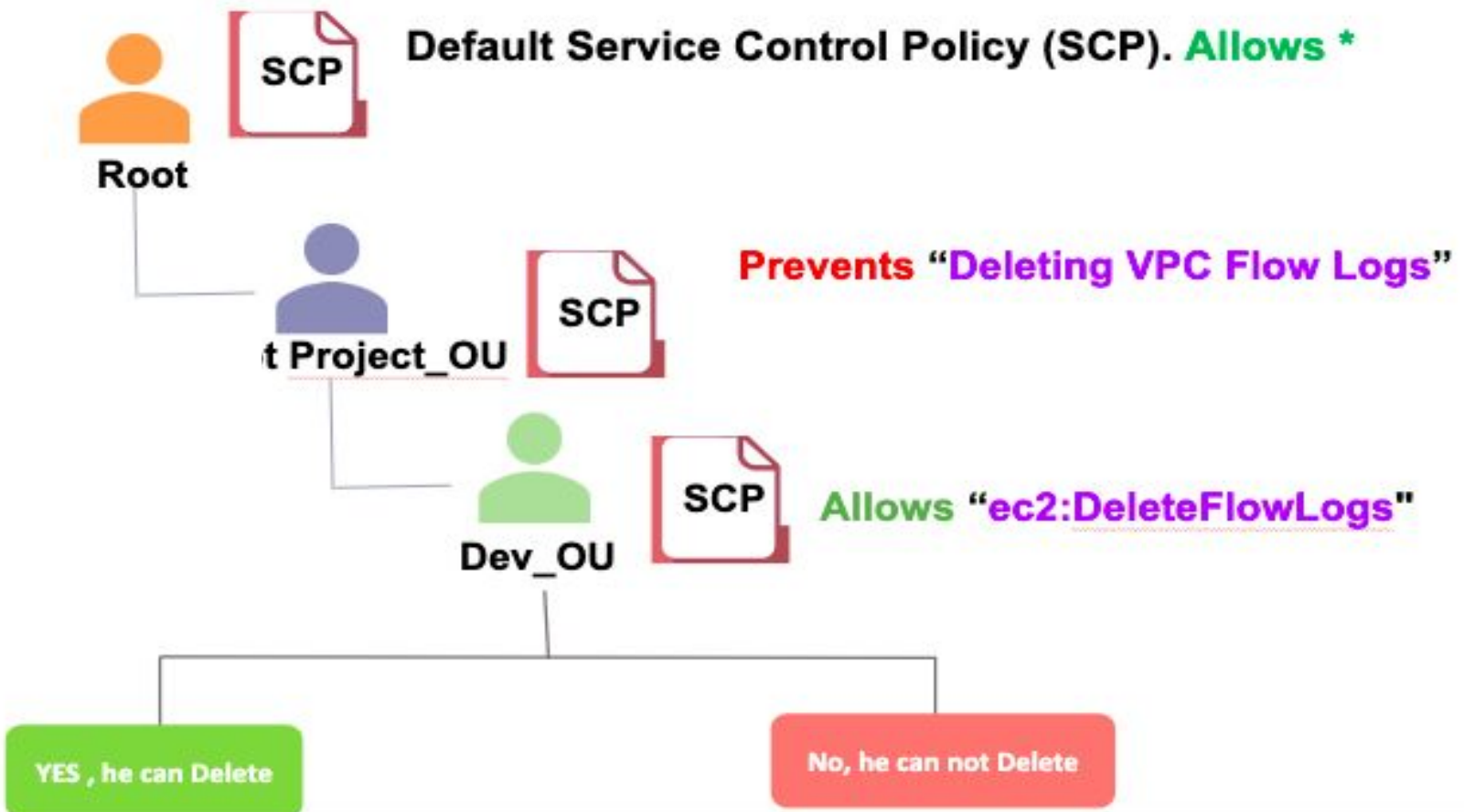
200　　　○ Add to web ACL

WordPress application

The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites

100　　　○ Add to web ACL

Default Service Control Policy (SCP). Allows *

Prevents "Deleting VPC Flow Logs"

Allows "ec2:DeleteFlowLogs"

Root

t Project_OU

Dev_OU

YES , he can Delete

No, he can not Delete

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

AWS Organization-1   AWS Organization-2

IT

Technical

Supply

Technical

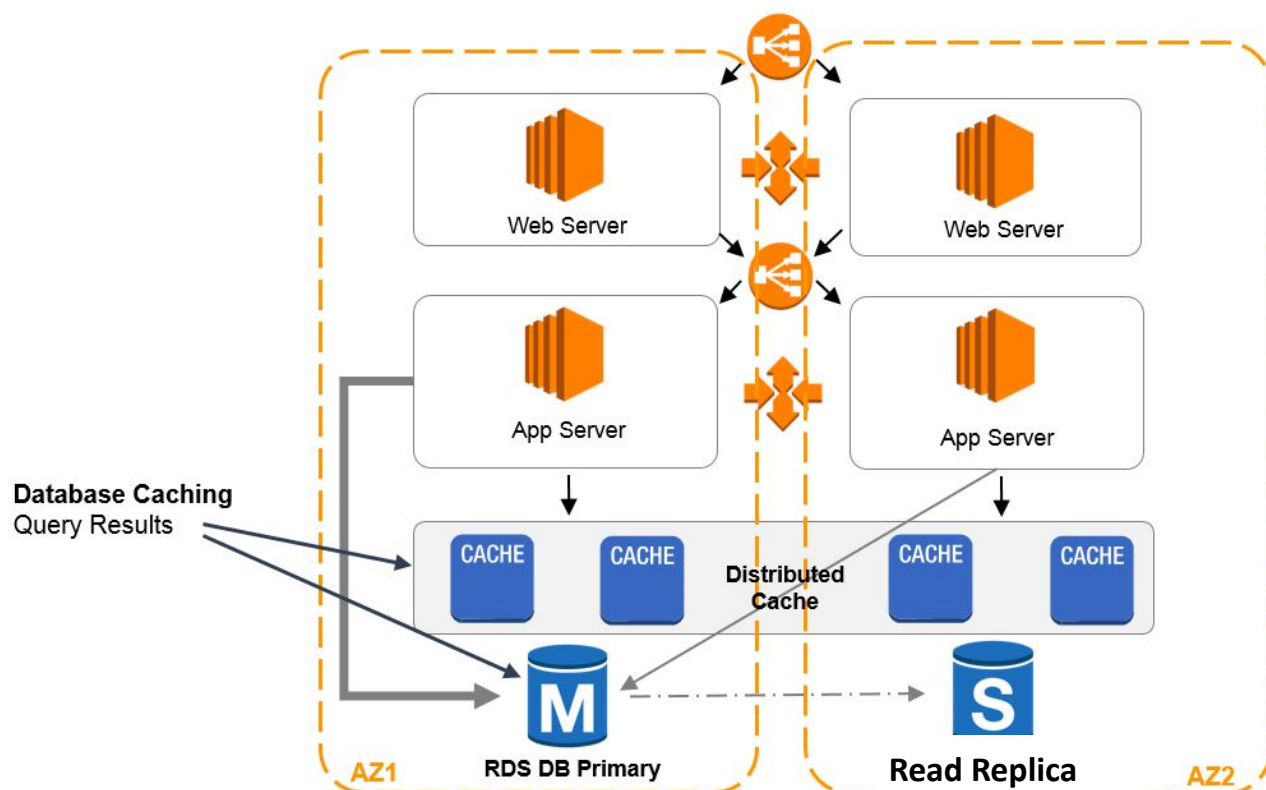|	Policy name ▾	Description
○ ▸	🟧 AmazonAPIGatewayAdministrator	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
○ ▸	🟧 AmazonAPIGatewayInvokeFullAccess	Provides full access to invoke APIs in Amazon API Gateway.
○ ▸	🟧 AmazonAPIGatewayPushToCloudWatchLogs	Allows API Gateway to push logs to user's account.
○ ▸	🟧 AmazonAugmentedAIIntegratedAPIAccess	Provides access to perform all operations Amazon Augmented AI resources, including FlowDefinitions, HumanTaskUis...
○ ▸	🟧 AmazonDynamoDBFullAccesswithDataPipeline	Provides full access to Amazon DynamoDB including Export/Import using AWS Data Pipeline via the AWS Manageme...
○ ▸	🟧 AmazonEC2RoleforDataPipelineRole	Default policy for the Amazon EC2 Role for Data Pipeline service role.
○ ▸	🟧 AmazonMQApiFullAccess	Provides full access to AmazonMQ via our API/SDK.
○ ▸	🟧 AmazonMQApiReadOnlyAccess	Provides read only access to AmazonMQ via our API/SDK.
○ ▸	🟧 APIGatewayServiceRolePolicy	Allows API Gateway to manage associated AWS Resources on behalf of the customer.
○ ▸	🟧 AWSDataPipeline_FullAccess	Provides full access to Data Pipeline, list access for S3, DynamoDB, Redshift, RDS, SNS, and IAM roles, and passRole...
○ ▸	🟧 AWSDataPipeline_PowerUser	Provides full access to Data Pipeline, list access for S3, DynamoDB, Redshift, RDS, SNS, and IAM roles, and passRole...
○ ▸	🟧 AWSDataPipelineRole	Default policy for the AWS Data Pipeline service role.

Which type of record?

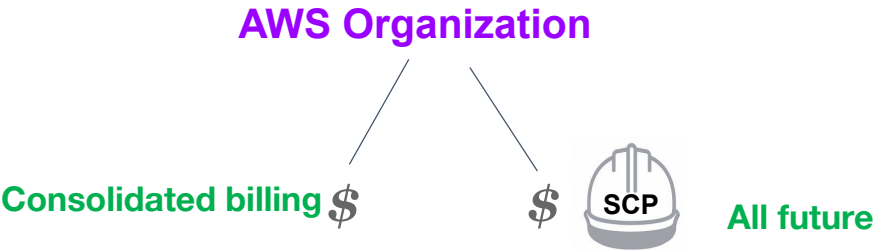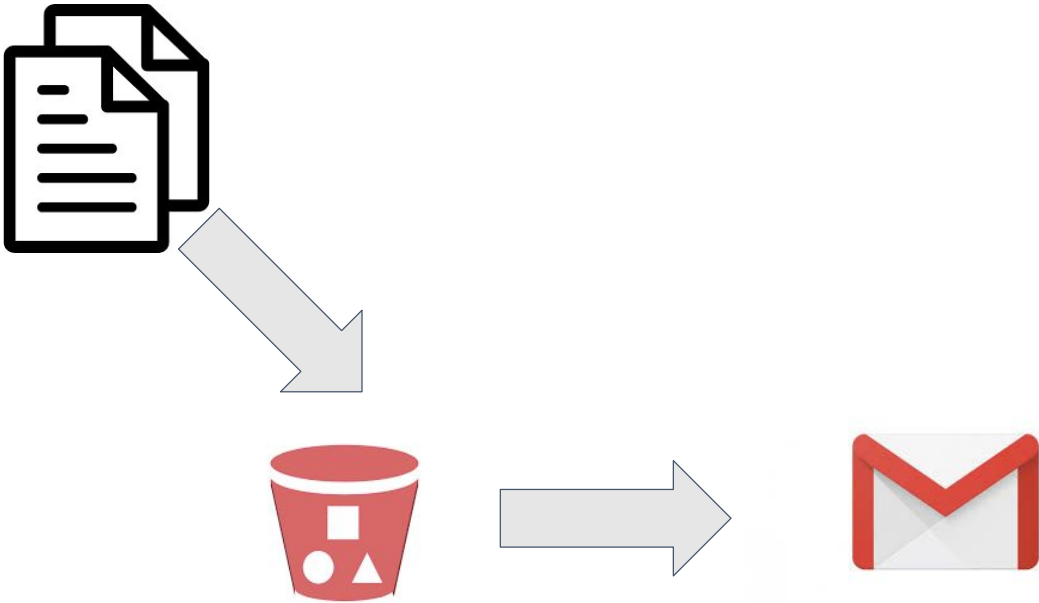| Create Domain **Variations** via Sub Domains	**Mapping Value**	**Value Type**	**Record Type**
www.clarusway.us	👉 Point out	🔵 **IP of Server** **1.2.3.4.5**	⮕ A AAA
		🔵 **Another Domain** **www.xxxxx.com**	⮕ CNAME
		🔵 **AWS End point** **S3 Bucket url** **Load Balancer** **DNS** **CloudFront**	⮕ **Alias**
		🔵 Etc..	⮕ MX

Record Value type determines the record type

There is an urgent requirement to monitor some database metrics for a database hosted on AWS and send notifications. Which AWS services can accomplish this? (Select Two)

A. Amazon Simple Email Service

B. Amazon CloudWatch

C. Amazon Simple Queue Service

D. Amazon Route 53

E. Amazon Simple Notification Service

Database Caching Diagram

Database Caching
Query Results

Distributed Cache

CACHE CACHE CACHE CACHE

Web Server   Web Server

App Server   App Server

RDS DB Primary   Read Replica

AZ1   AZ2

AWS Organization

Consolidated billing $ $ SCP   **All future**

Account A separately : **8TB usage = 8** $

0   10 TB

Account B separately : **4 TB usage = 4** $ *pay $1 for each TB in the first 10 TB*   *pay $0.5 for TB after 10 TB*

+--------------
        12 $

Consolidated billing : 10 TB x 1 $= 10 $ for the first 10 TB
                     2TB X 0.5 = 1 $ for the next 2 TB

+--------------
        11 $

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

AWS

VPC

EC2 instance
Private IP: 10.0.0.5

10.0.0.6

Subnet: us-east-2a
10.0.0.0/24

10.0.1.7

Subnet: us-east-2b
10.0.1.0/24

VPC A - service consumer
10.0.0.0/16

VPC

Target 1

Subnet: us-east-2a

Network
load balancer

Target 2

Subnet: us-east-2b

Endpoint service vpce-svc-1234

VPC B - service provider
10.2.0.0/16

Region: us-east-2

Services

- AWS App Mesh
- Amazon Aurora
- AWS Certificate Manager Private Certificate Authority
- AWS CodeBuild
- Amazon EC2
- EC2 Image Builder
- AWS Glue
- AWS License Manager
- AWS Network Firewall
- AWS Outposts
- AWS Resource Groups
- Amazon Route 53
- Amazon VPC

AWS License Manager

Define rules for your licensed software → Attach licensing rules during launch and proactively control usage → Search inventory and track licenses brought in post launch → Use alerts to control and centrally manage licenses across all AWS accounts and on premises

Root Device → Snapshot → Copy Snapshot → Encryption of Copied Snapshot → EC2 / Encrypted Root Device

Amazon RDS Database → Snapshot → Copy Snapshot → Encryption of Copied Snapshot → Amazon RDS Encrypted Database

You currently manage a set of web servers hosted on EC2 Servers with public IP addresses. These IP addresses are mapped to domain names. There was an urgent maintenance activity that had to be carried out on the servers. The servers had to be stopped and restarted. Now the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier. Which of the following could be a reason for this?

A. The Route 53 hosted zone needs to be restarted.

B. The network interfaces need to initialized again.

C. The public IP addresses need to be associated with the ENI again.

D. The public IP addresses have changed after the instance was stopped and started again.

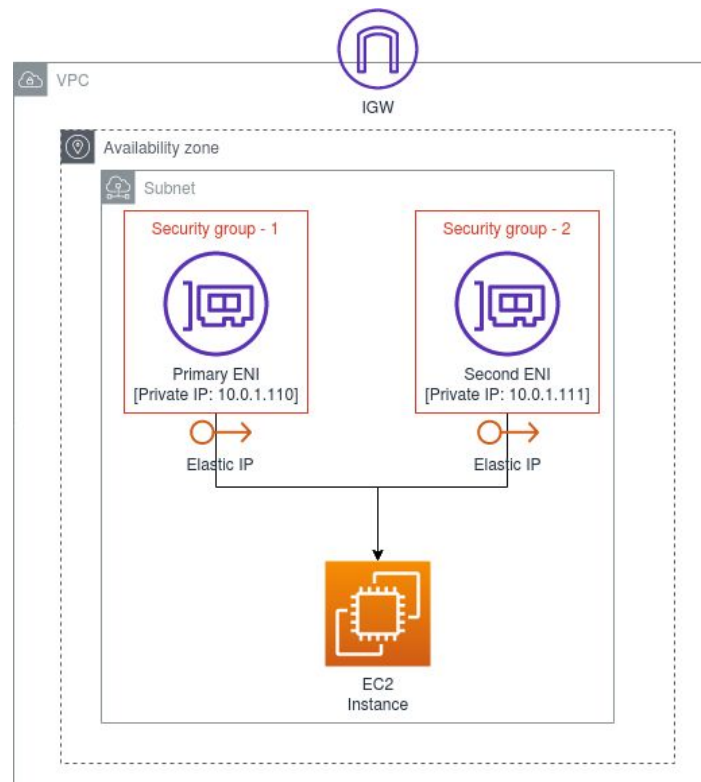**CloudWatch** vs **CloudTrail**
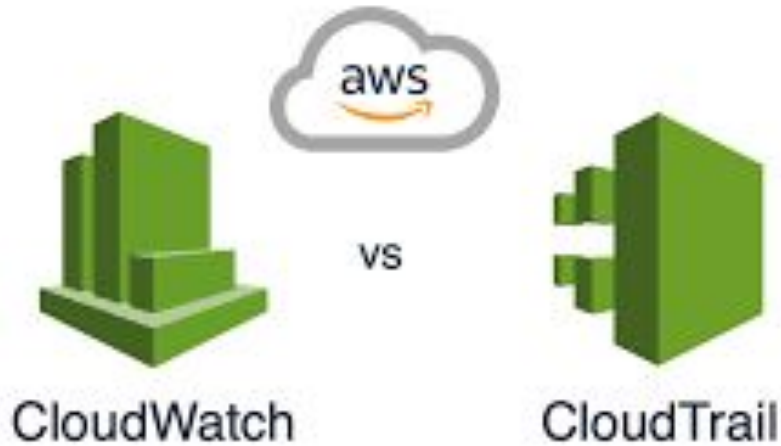
ENI — ENA — EFA

ENI
- Upto 10 GBPS
- VMDq
- TCP/IP
- Multiple ENI/instance
- Traffic can traverse across subnets
- VPC Networking, General purpose
- Default

ENA
- Upto 25 GBPS
- SR-IOV
- TCP/IP
- Single setting/per instance
- Traffic can traverses across subnets
- Low latency apps
- Optional on supported instance type

EFA
- 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

VPC — IGW

Availability zone

Subnet

Security group - 1
Primary ENI
[Private IP: 10.0.1.110]
Elastic IP

Security group - 2
Second ENI
[Private IP: 10.0.1.111]
Elastic IP

EC2 Instance

Real time Streaming

Capture

Transfer/Load

Analyze

Kinesis Video Stream

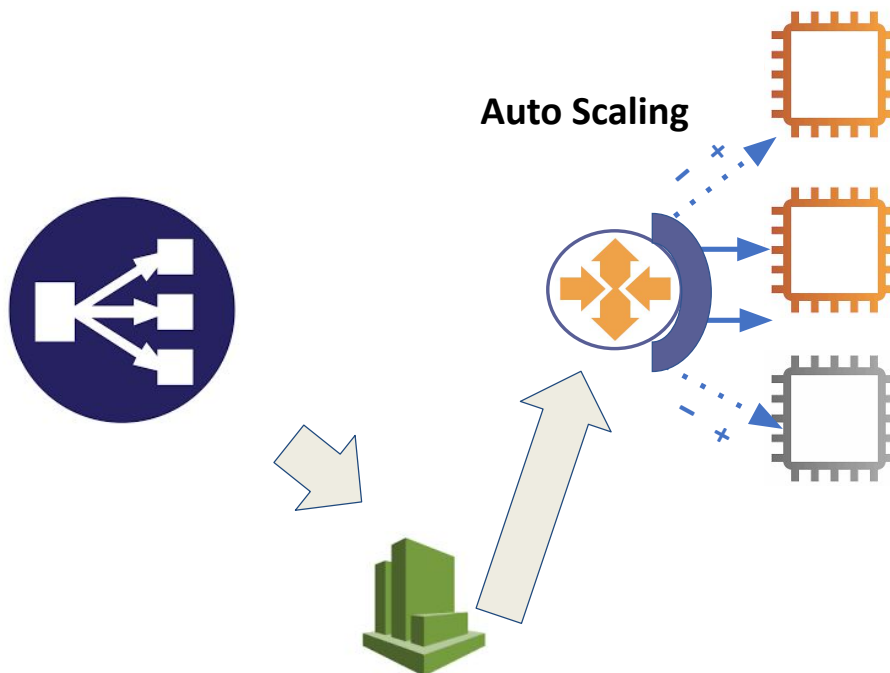**Kinesis Streams**

Kinesis Data Stream

Kinesis Firehose

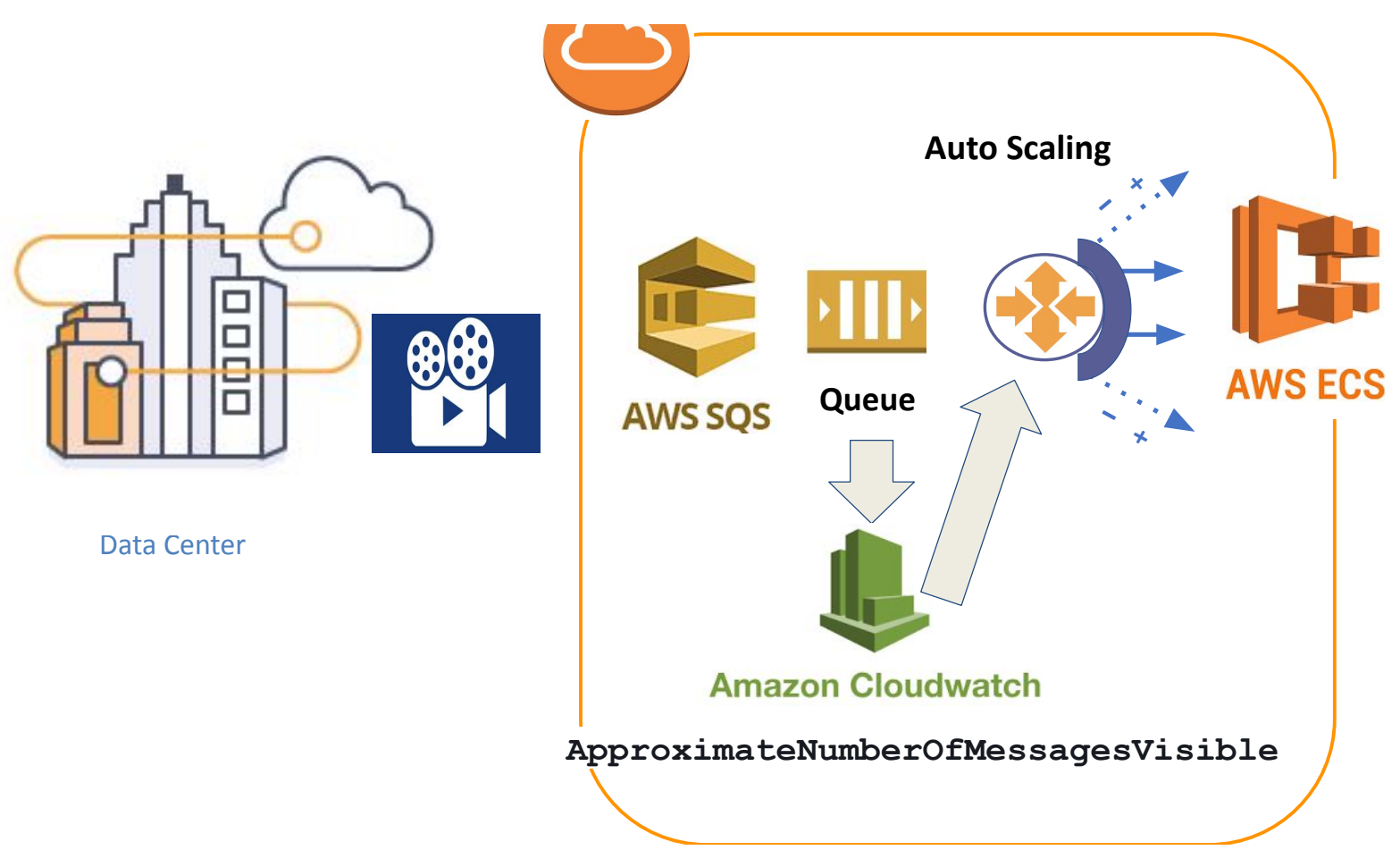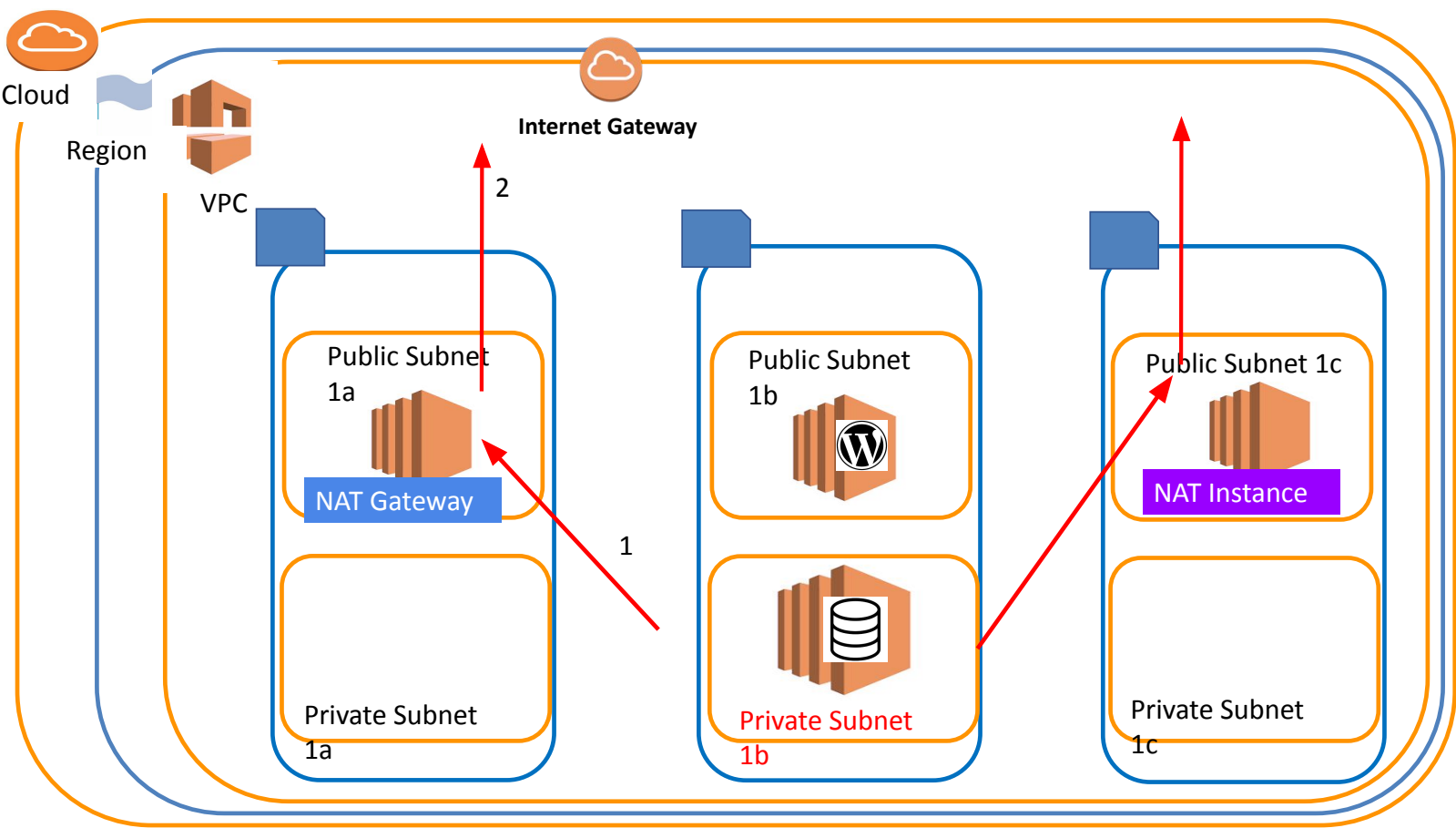Load streaming data into Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service

Kinesis Analytics

Analyze data streams using standard SQL queries

Auto Scaling

Amazon Cloudwatch

`CPU utilization`

Cloud

Region

VPC

Internet Gateway

2

Public Subnet 1a

NAT Gateway

1

Private Subnet 1a

Public Subnet 1b

Private Subnet 1b

Public Subnet 1c

NAT Instance

Private Subnet 1c

Data Center

Auto Scaling

AWS SQS

Queue

Amazon Cloudwatch

AWS ECS

ApproximateNumberOfMessagesVisible

How does AWS DataSync work?
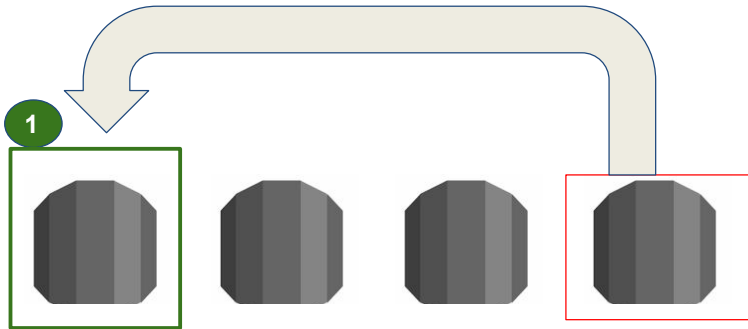Simplifies, automates, and accelerates data transfer to or from AWS
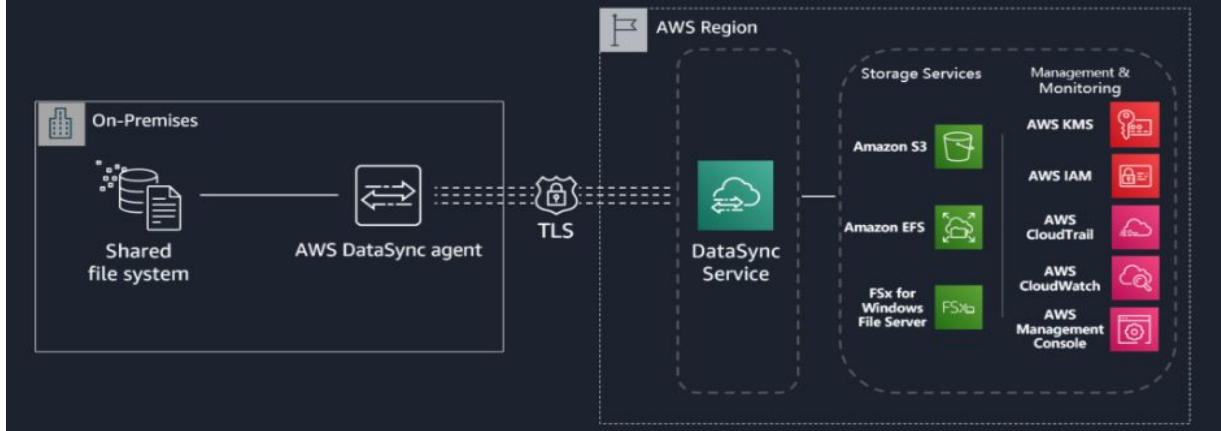
- **Public endpoints**:
- **Federal Information Processing Standard (FIPS) endpoints**: USA and Canada
- **Virtual private cloud (VPC) endpoints**: If you use a VPC endpoint, all communication from DataSync to AWS occurs through the endpoint in your AWS VPC. This establishes a private connection between your self-managed storage system, your VPC, and AWS services, providing extra security as your data is copied over the network.
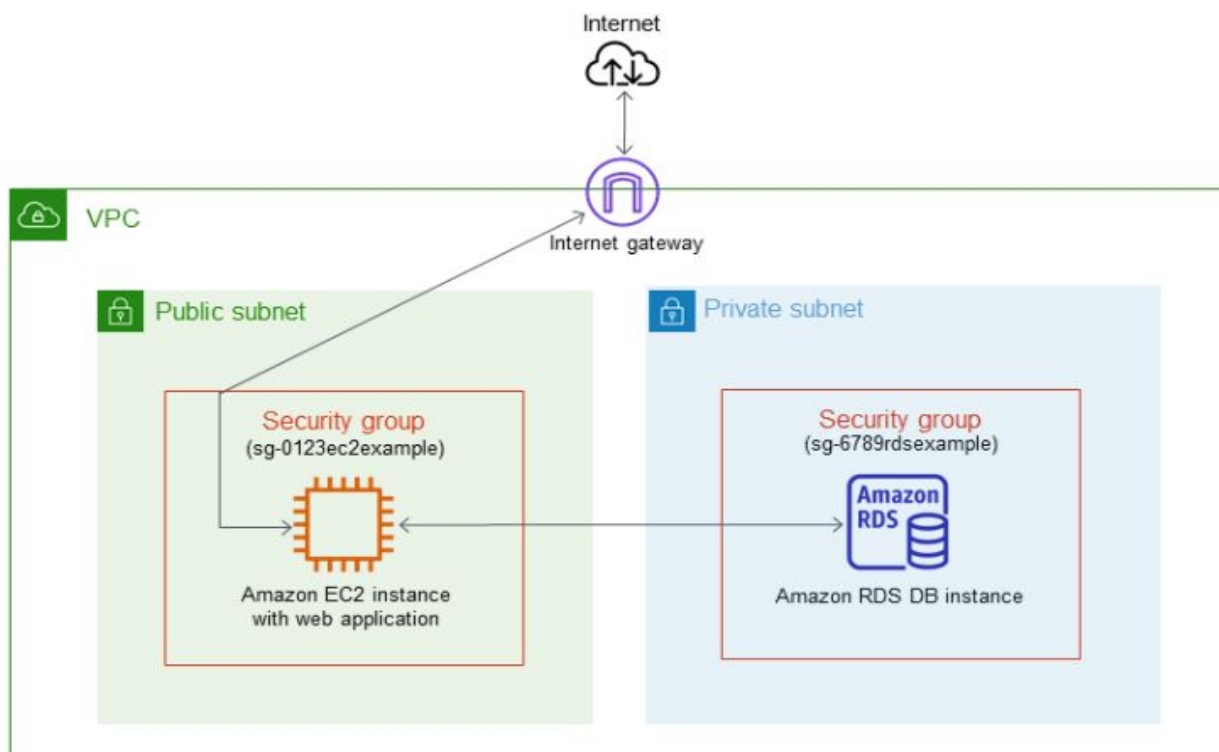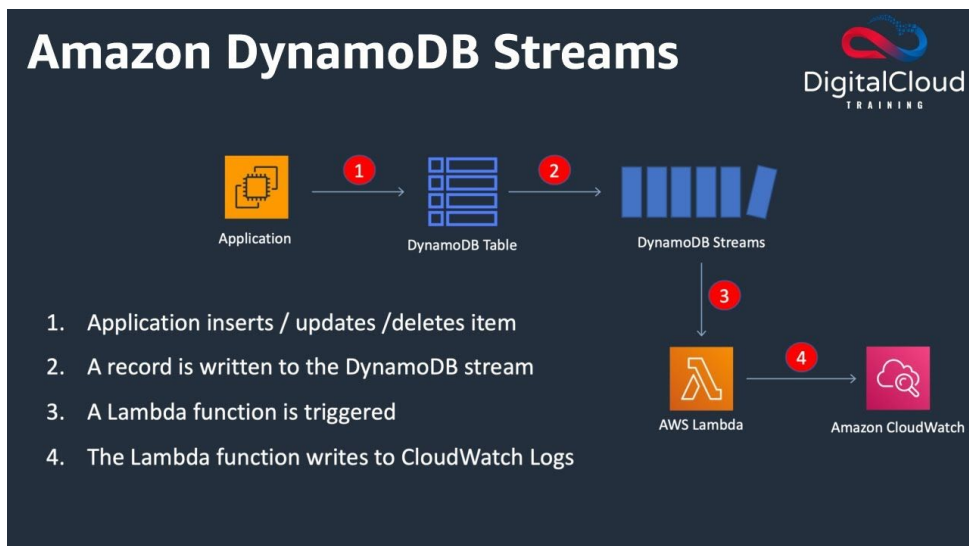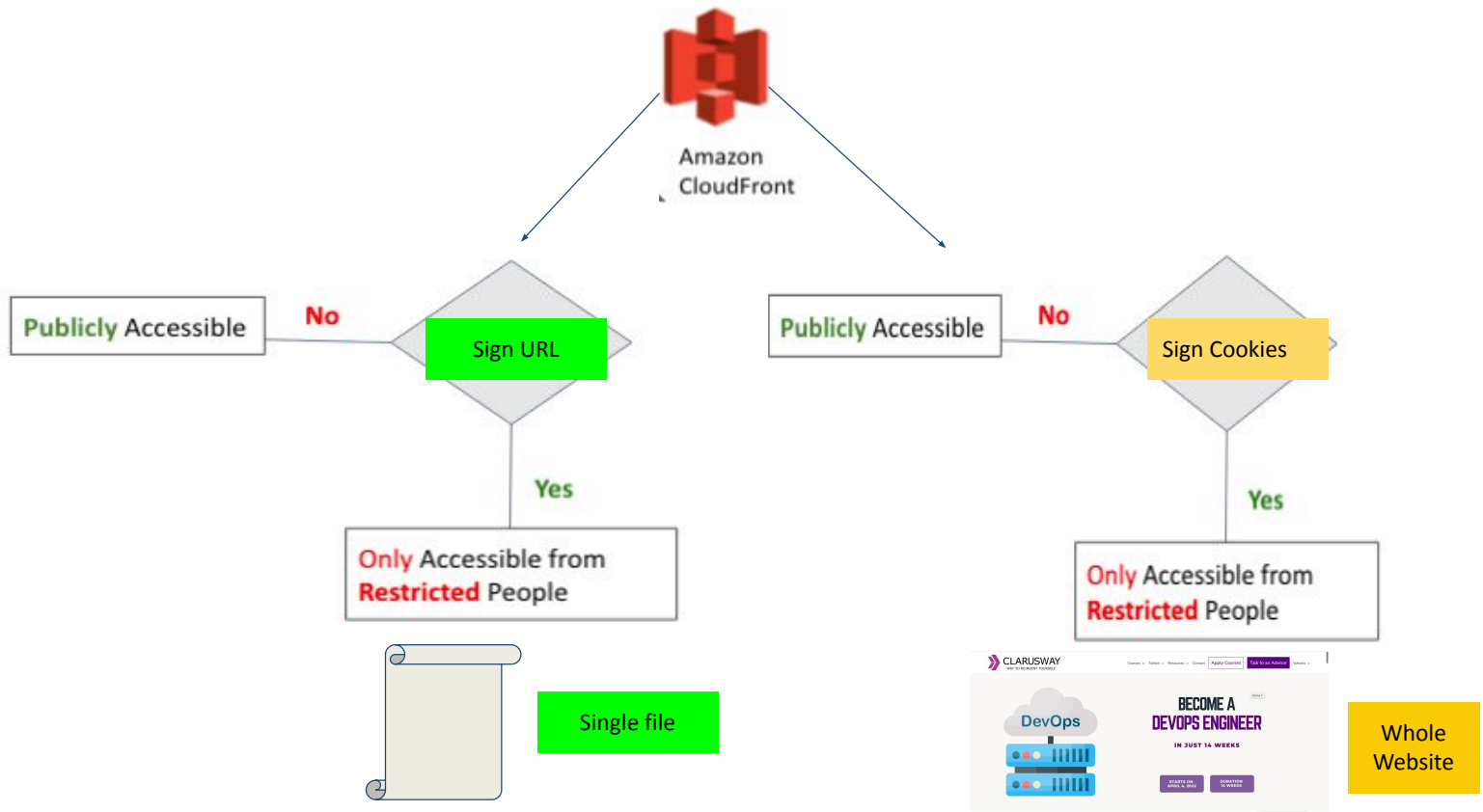
When enabled, DynamoDB Streams captures a time-ordered sequence of item-level modifications in a DynamoDB table and durably stores the information for **up to 24 hours. Applications can access a series of stream** *records***, which contain an item change, from a DynamoDB stream in near real time.**
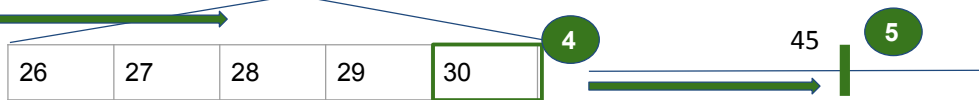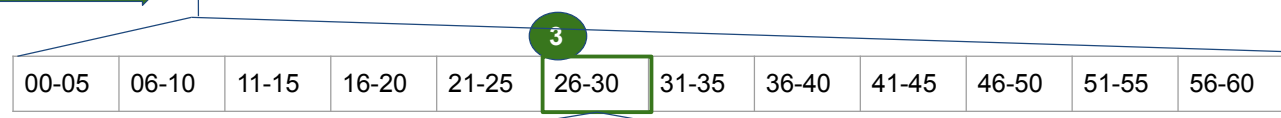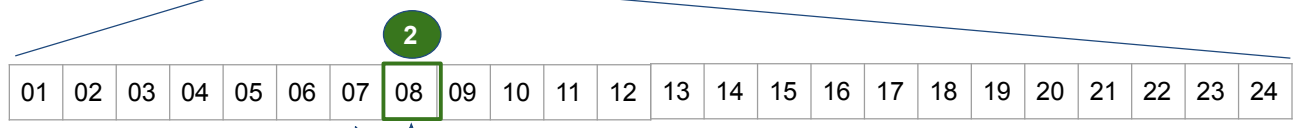
Amazon RDS

Point in time recovery

01 JAN 00:01

02 JAN 00:01

03 JAN 00:01

04 JAN

00:01
08:30:45

Snapshot

Transaction Logs

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

00-05	06-10	11-15	16-20	21-25	26-30	31-35	36-40	41-45	46-50	51-55	56-60

26	27	28	29	30

45

S3 static Web Hosting

Amazon S3

Publish Direct from S3

Amazon CloudFront

Publish from CloudFront

S3 Distribution with S3 ARN

Also Accessible from S3

OAI Activated ?

No

Only Accessible from CloudFront

Yes

Real time
Streaming

Capture

Transfer/Load

Analyze

Kinesis
Video Stream

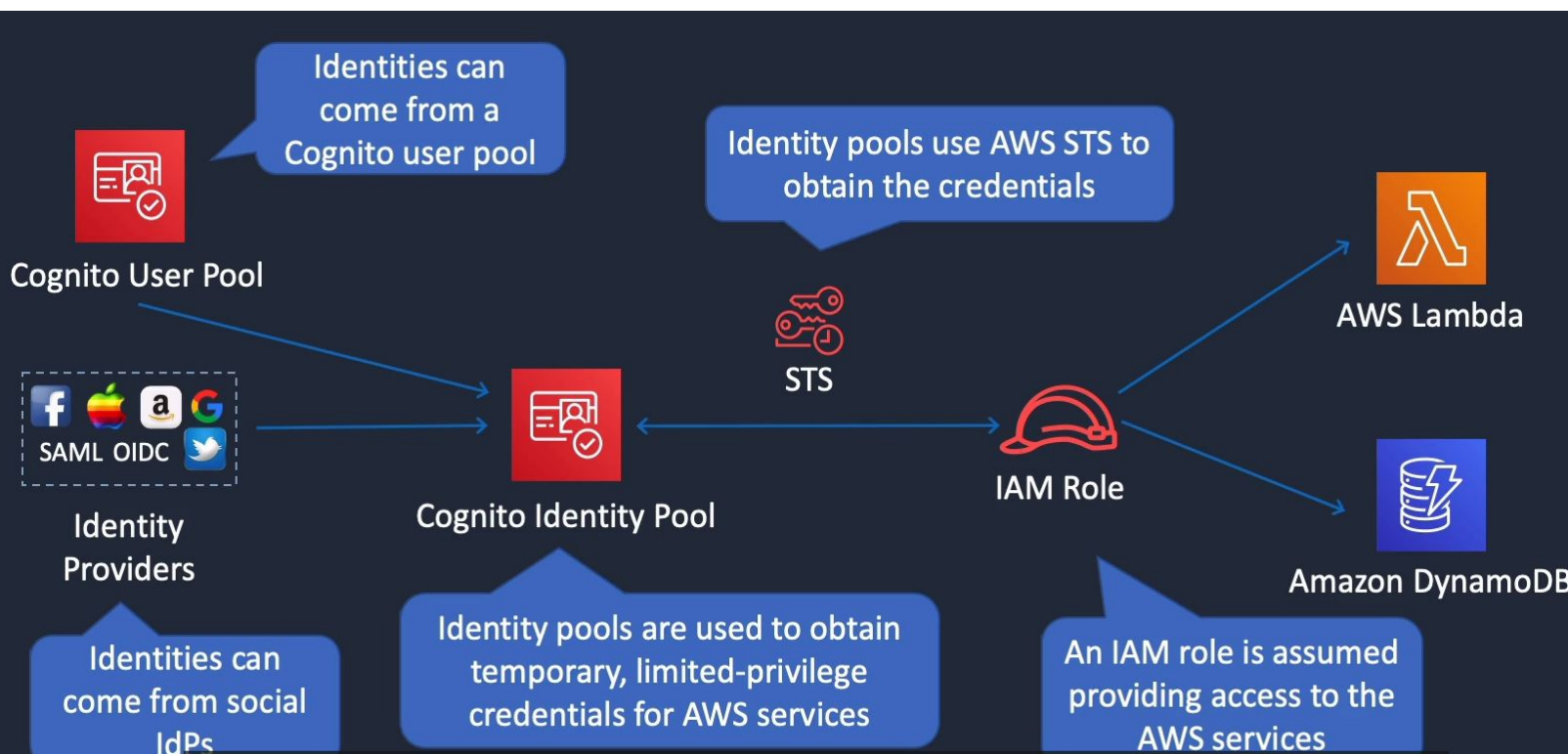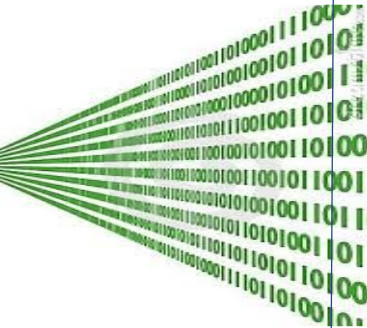Kinesis Streams

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

Identities can
come from a
Cognito user pool

Cognito User Pool

SAML OIDC

Identity
Providers

Identities can
come from social
IdPs

Identity pools use AWS STS to
obtain the credentials

STS

Cognito Identity Pool

Identity pools are used to obtain
temporary, limited-privilege
credentials for AWS services

IAM Role

An IAM role is assumed
providing access to the
AWS services

AWS Lambda

Amazon DynamoDB

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 Managed Grafana
Highly scalable, highly available managed service for Grafana

Create Grafana workspaces
Create a workspace that is automatically built, packaged, deployed, and managed for you

Manage user access
Grant users in your corporate directories access to the workspace with AWS IAM Identity Center

Connect to multiple data sources
Add multiple data sources including AWS services, other cloud services, and self-managed data sources

Set up dashboards
Visualize, analyze, and correlate metrics, logs, and trace data across sources all in one console

Centralize third-party ISV data
Optionally upgrade to Grafana Enterprise to add more data sources

Amazon S3 > mycloudtrails3bucket-mk

mycloudtrails3bucket-mk   private bucket

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** ⤢ to get a list of all objects in your bucket. For others to access
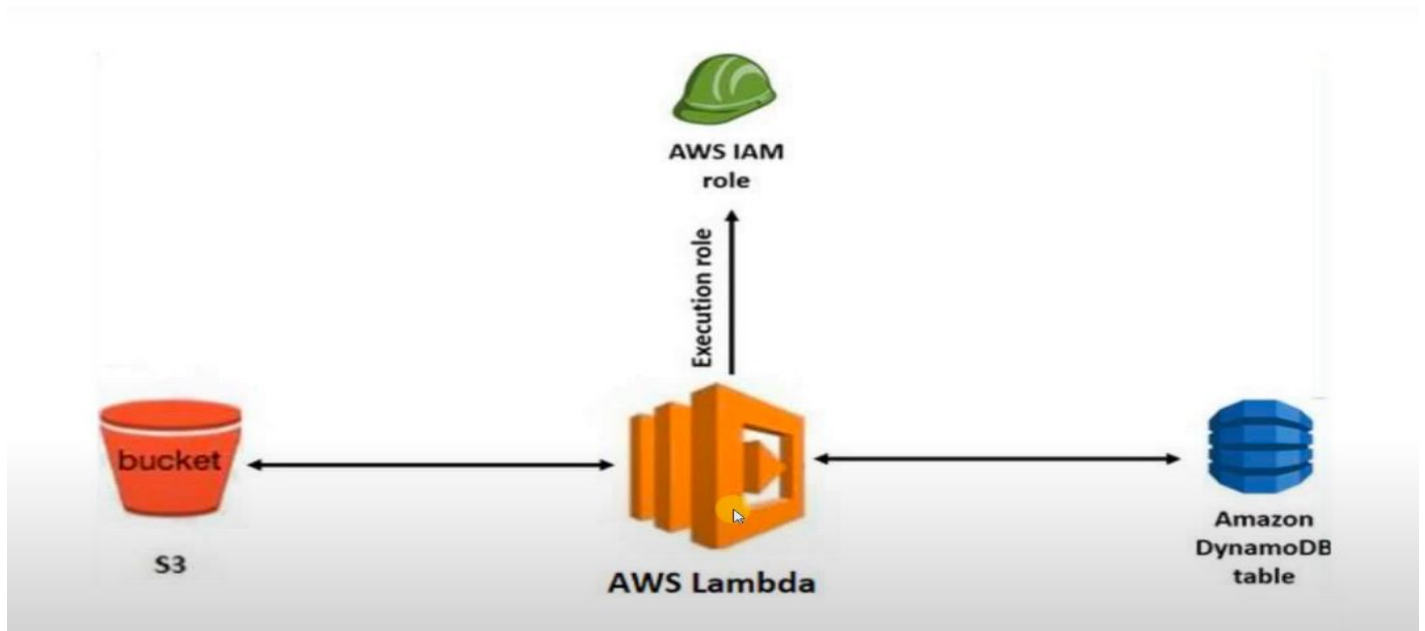
| C | Copy URL | Open | Download | Delete | Actions ▼ | Create folder | **Upload** |

Q Find objects by prefix

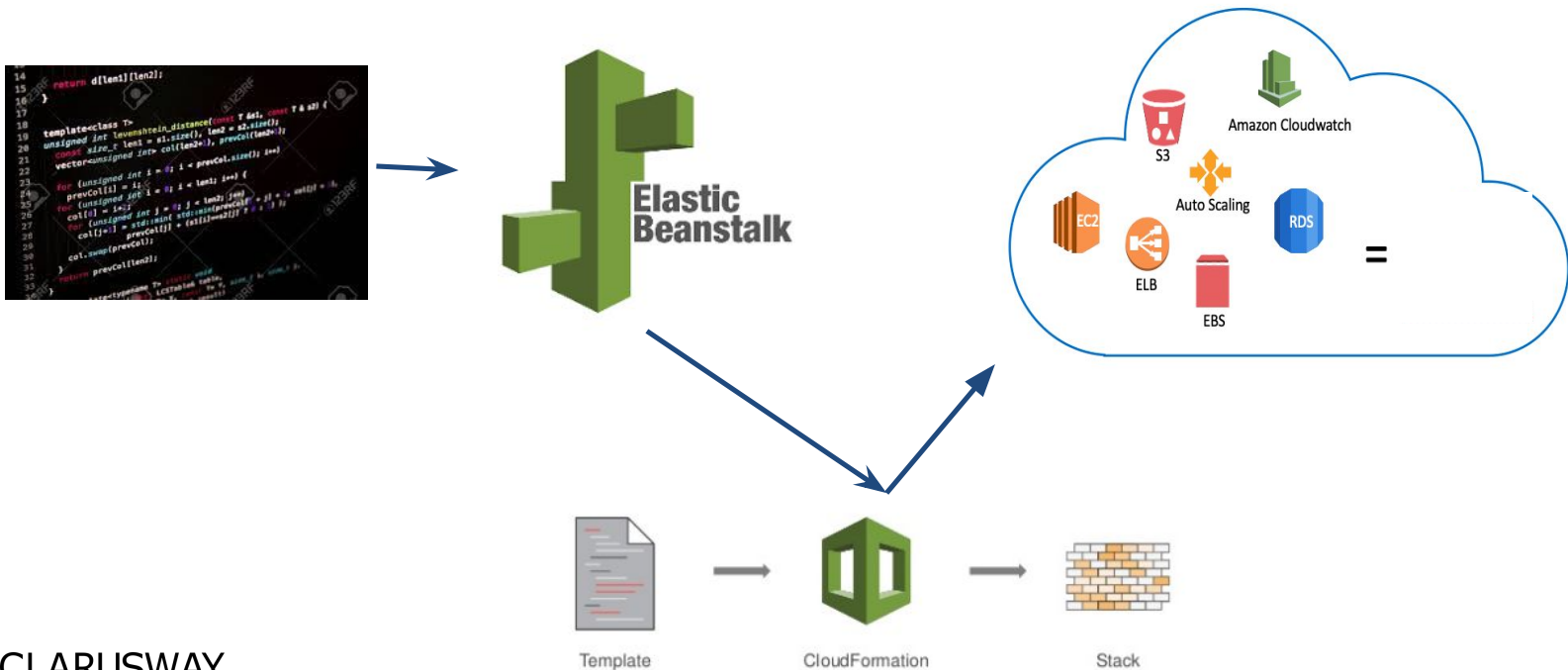|	Name it contains one file ▲	Type ▽	Last modified
☐	📄 Yeni Metin Belgesi.txt	txt	May 25, 2021, 15:48:52 (UTC+03:00)

```
$ 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  ←
```
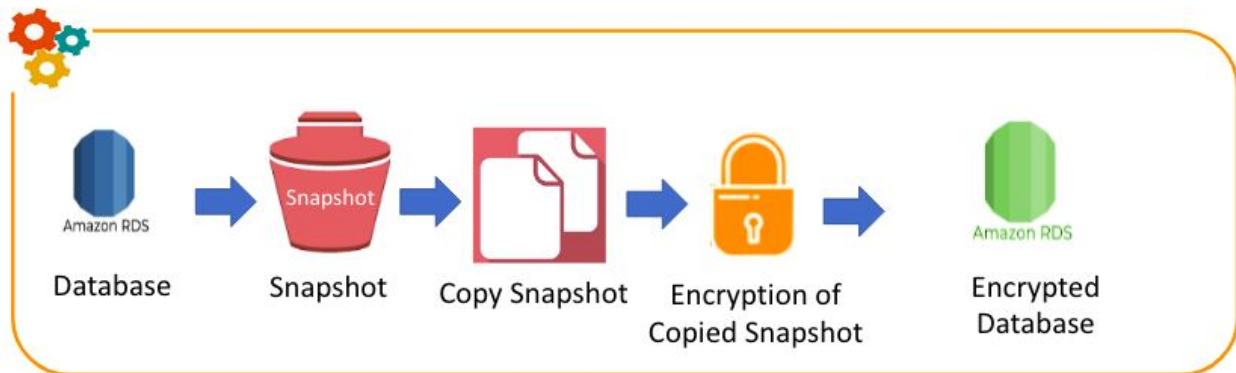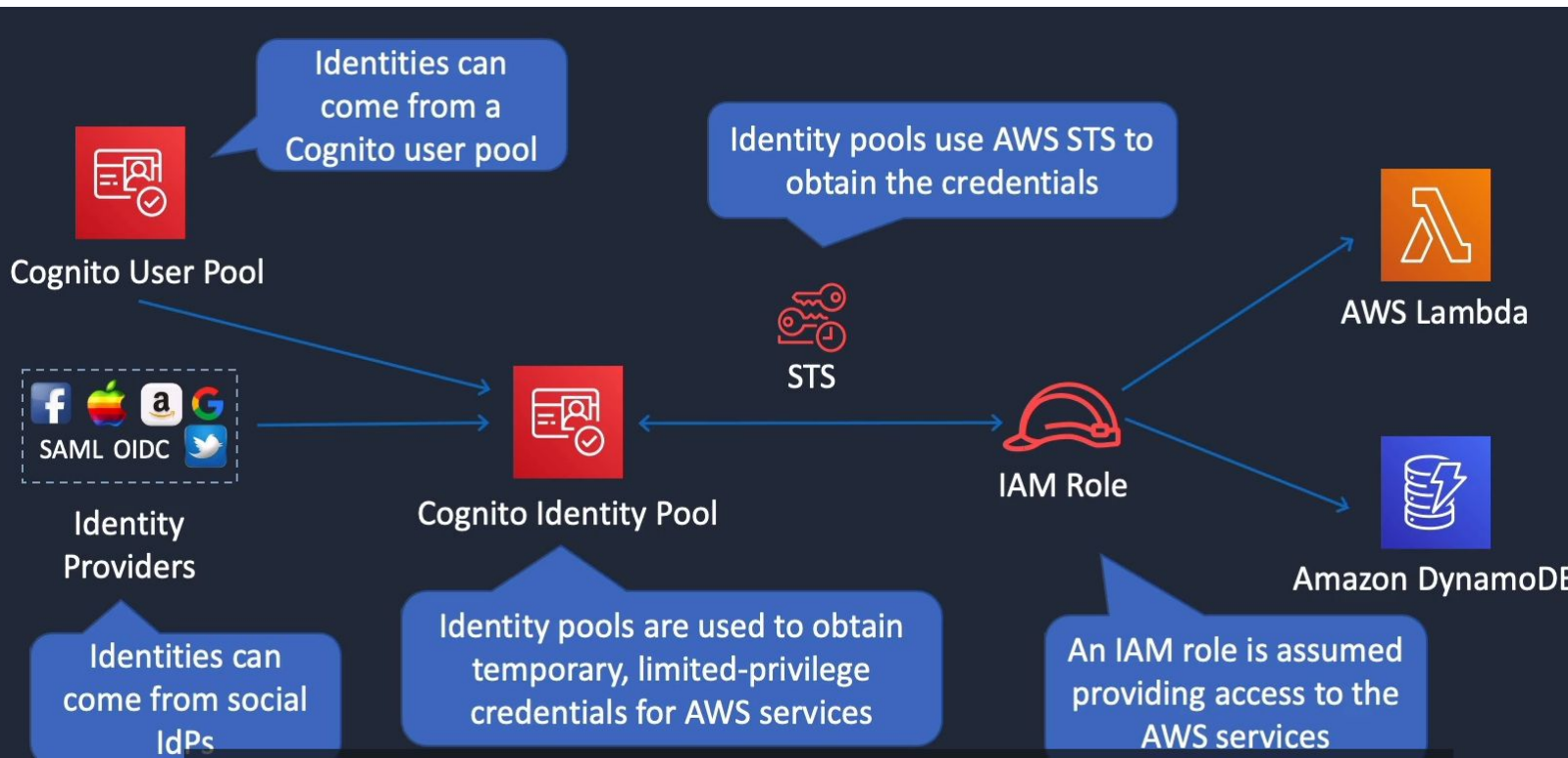
Introduction to Elastic Beanstalk
Why AWS Elastic Beanstalk?

Cognito User Pool

Identities can come from a 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

Root Device → Snapshot → Copy Snapshot → Encryption of Copied Snapshot → EC2 → Encrypted Root Device

Amazon RDS Database → Snapshot → Copy Snapshot → Encryption of Copied Snapshot → Encrypted Database (Amazon RDS)
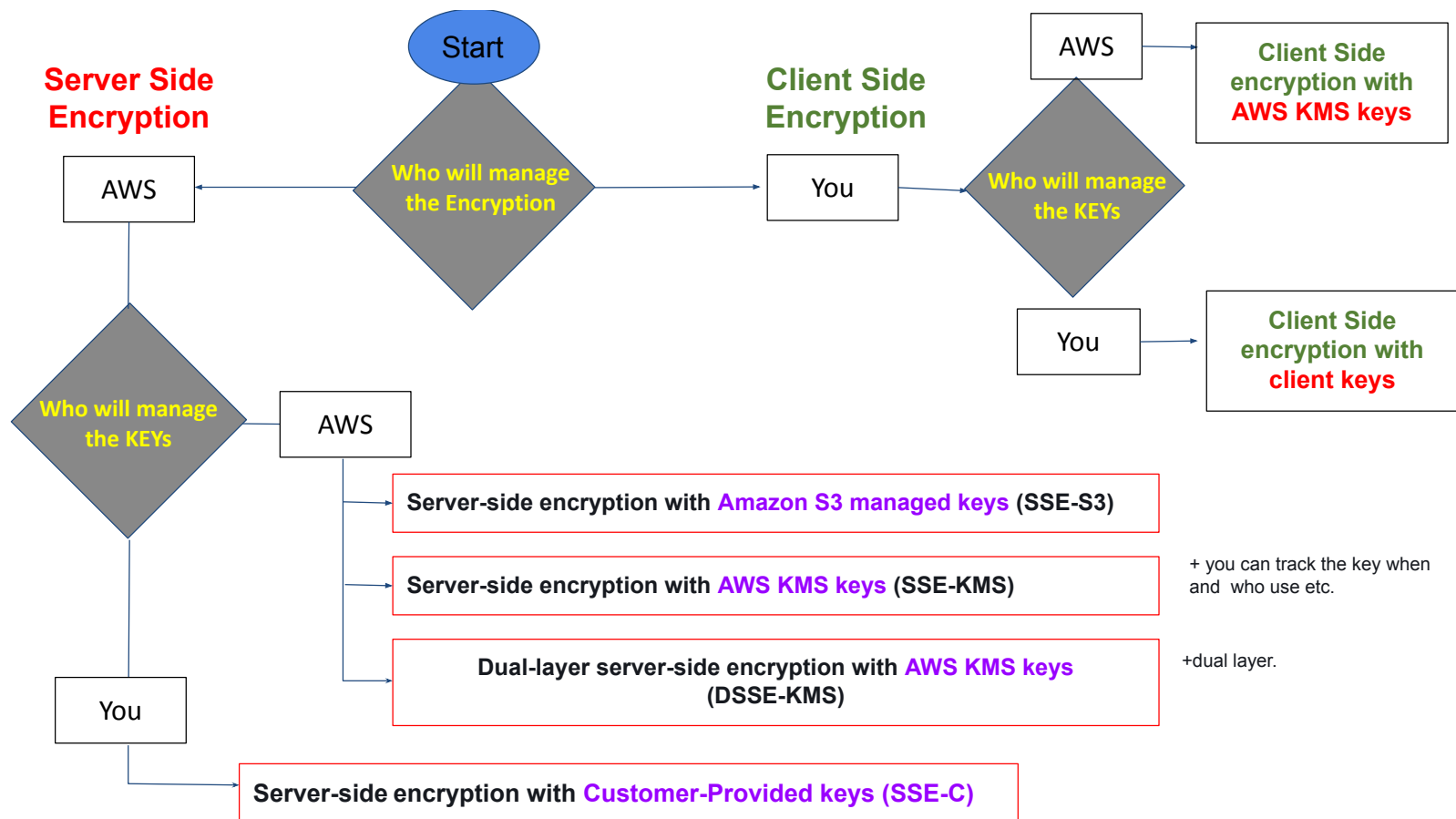
MEMBER AND MASTER ACCOUNT LEAVING PROCESS

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
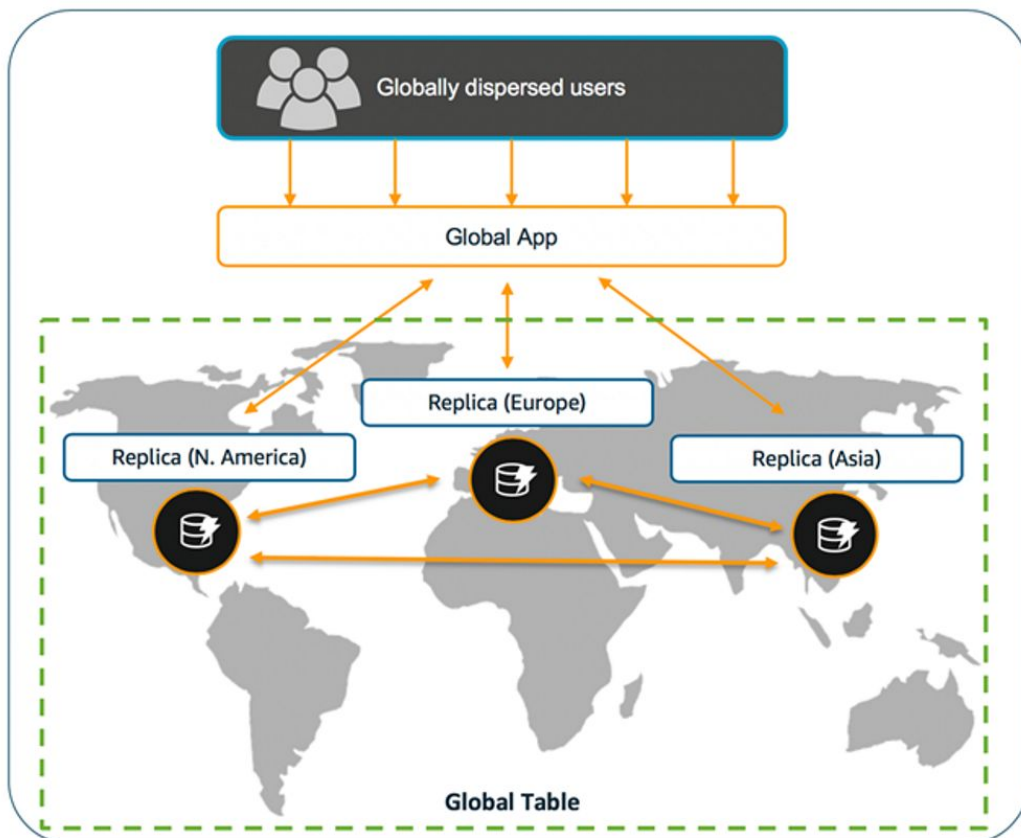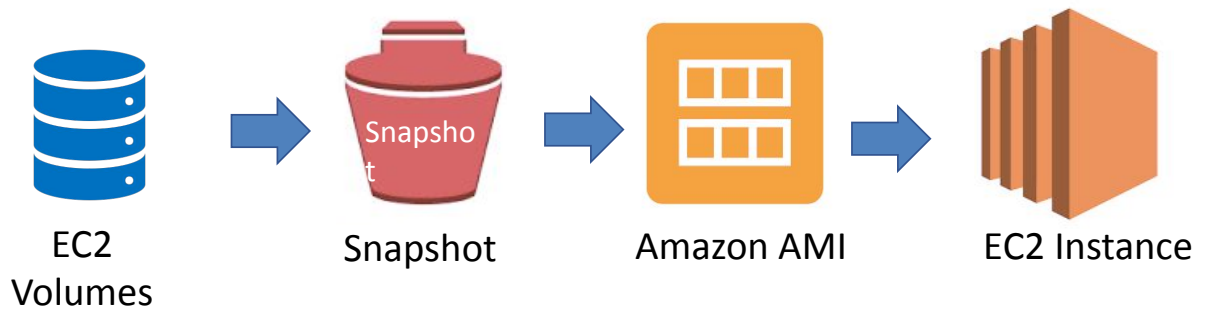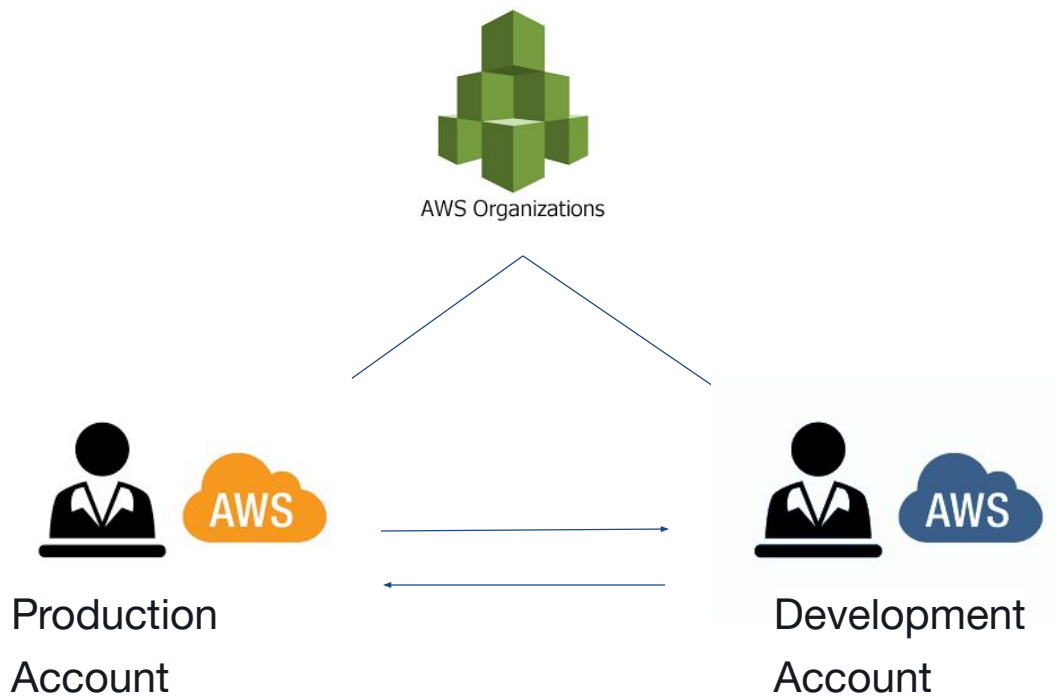6. Accept the invite to the new Organization from the master account
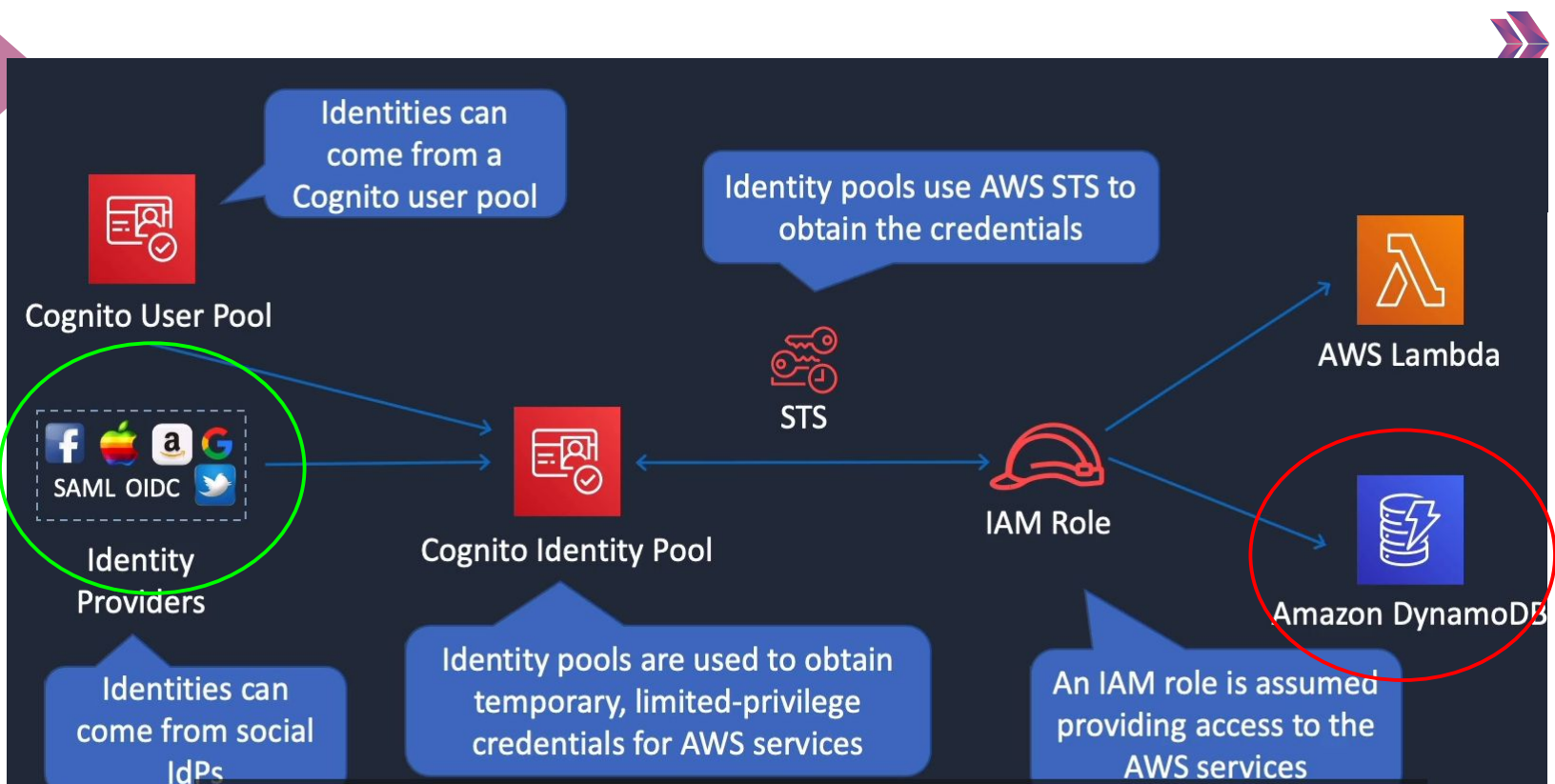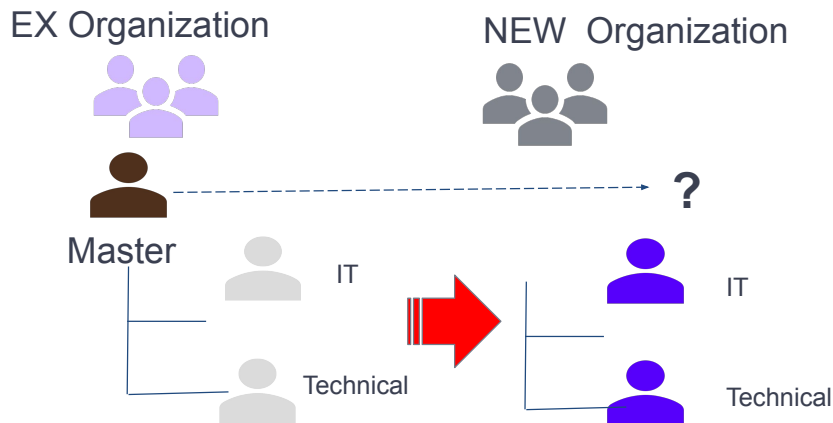
Component	Description
Templates	The JSON or YAML text file that contains the instructions for building out the AWS environment
Stacks	The entire environment described by the template and created, updated, and deleted as a single unit
StackSets	AWS CloudFormation StackSets extends the functionality of 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

Server Side Encryption

Client Side Encryption

Start

AWS

You

AWS → Client Side encryption with AWS KMS keys

You → Client Side encryption with client keys

Who will manage the Encryption

Who will manage the KEYs

Who will manage the KEYs

AWS

You

Server-side encryption with **Amazon S3 managed keys** (SSE-S3)

Server-side encryption with **AWS KMS keys** (SSE-KMS)

+ you can track the key when and who use etc.

Dual-layer server-side encryption with **AWS KMS keys** (DSSE-KMS)

+dual layer.

Server-side encryption with **Customer-Provided keys (SSE-C)**

Failover Scenario

EC2 Volumes → Snapshot → Amazon AMI → EC2 Instance

Globally dispersed users

Global App

Replica (Europe)

Replica (N. America)

Replica (Asia)

Global Table

AWS Organizations

Production
Account

Development
Account

✔ Enable resource sharing in AWS Organizations with RAM

**backed up your
on-premises data** Storage Gateway

ISCSI
(Internet Small Computer System

ISCSI

**Network File System (NFS)
Server Message Block (SMB).**

File Gateway
- **S3-SMB+NFS**
- **FSx -NFS**

**Volume
Gateway**

Tape Gateway

Stored → Snapshot

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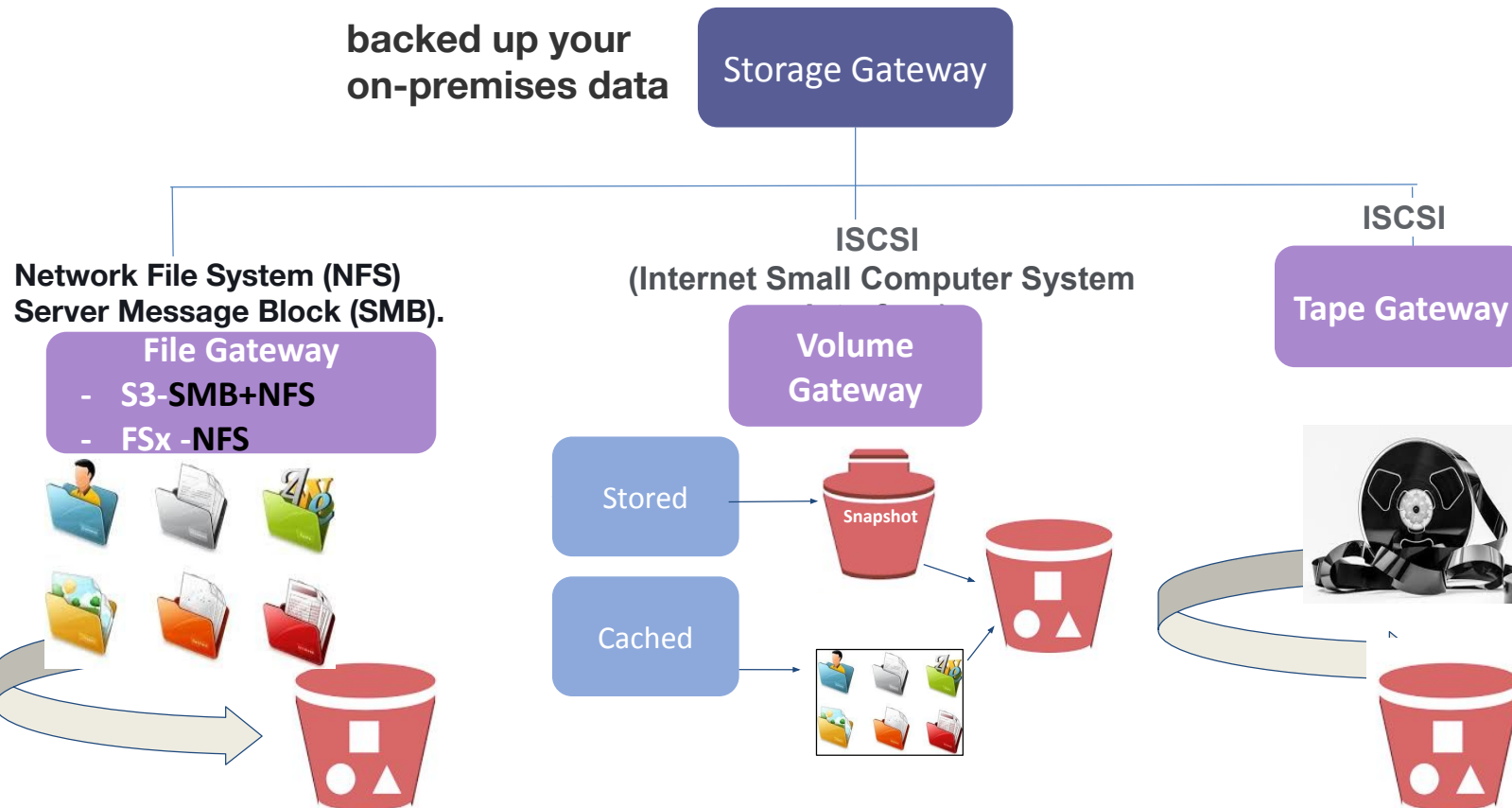
Info: The term **legacy** database commonly refers to a database that has been in use for many years and is therefore unsuitable for modern apps and environments.

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

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

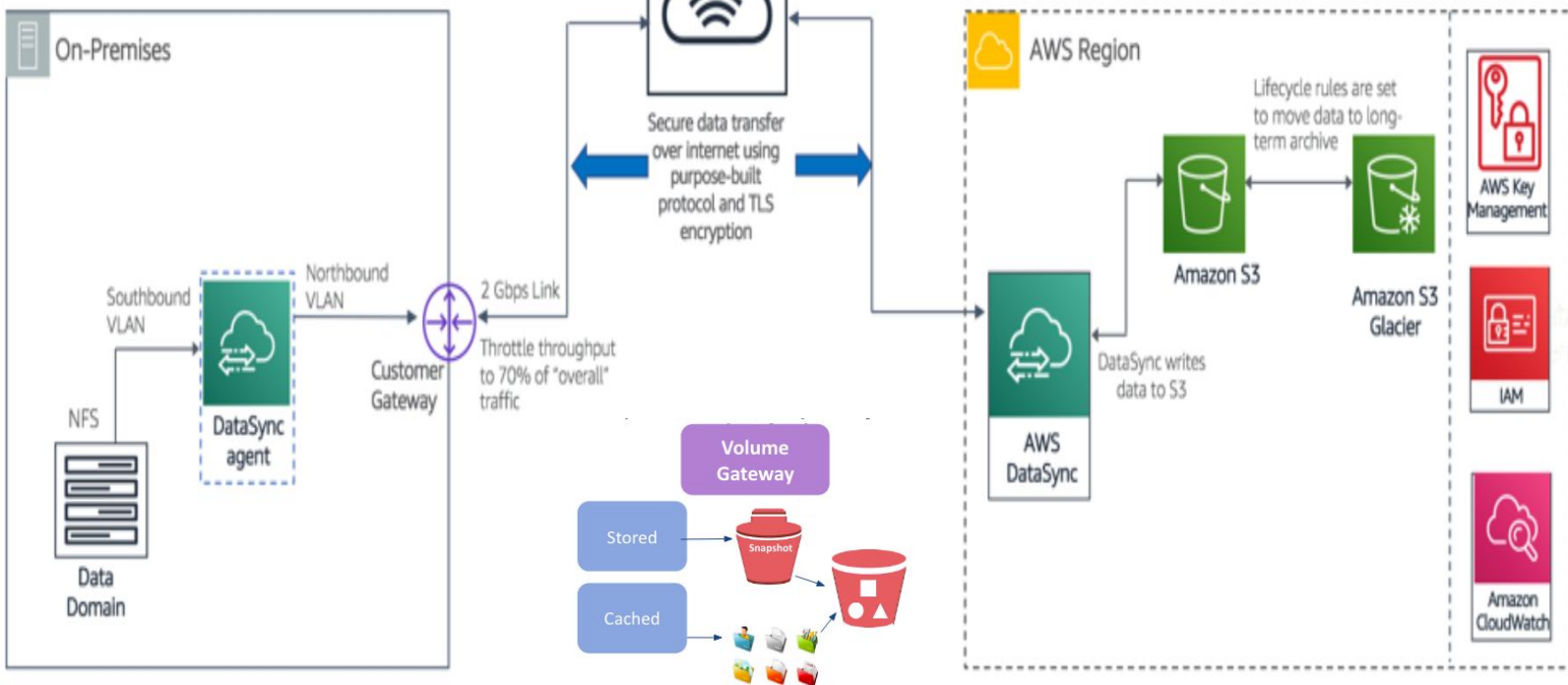- Use **SCT (Schema conversion tool)** from one schema to another schema for **Heterogenous migrations**

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

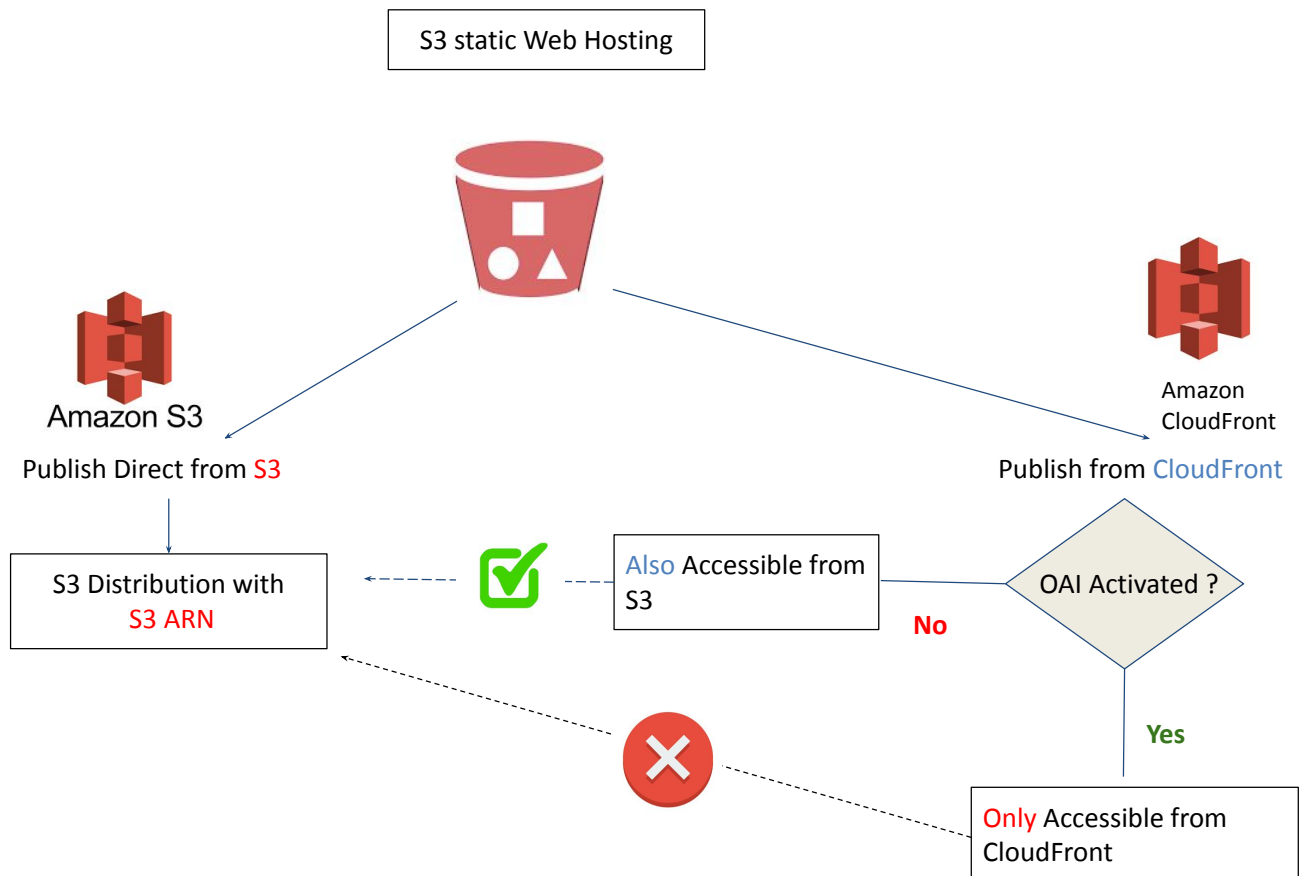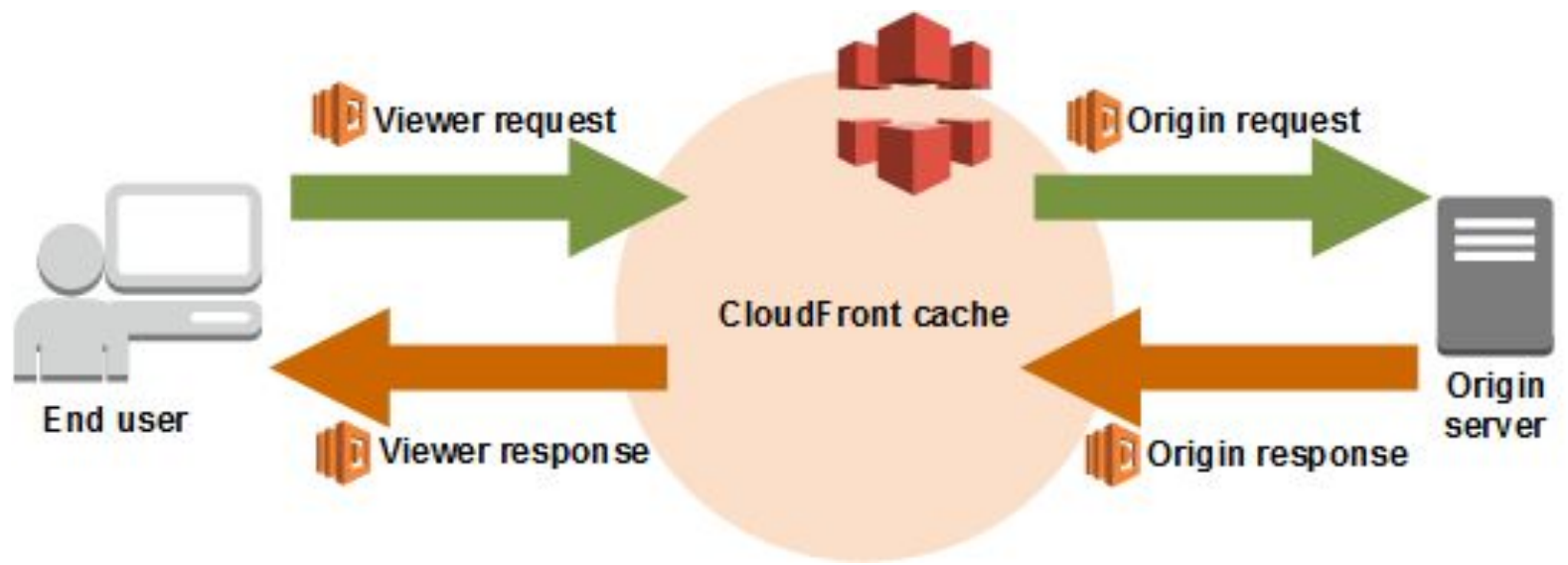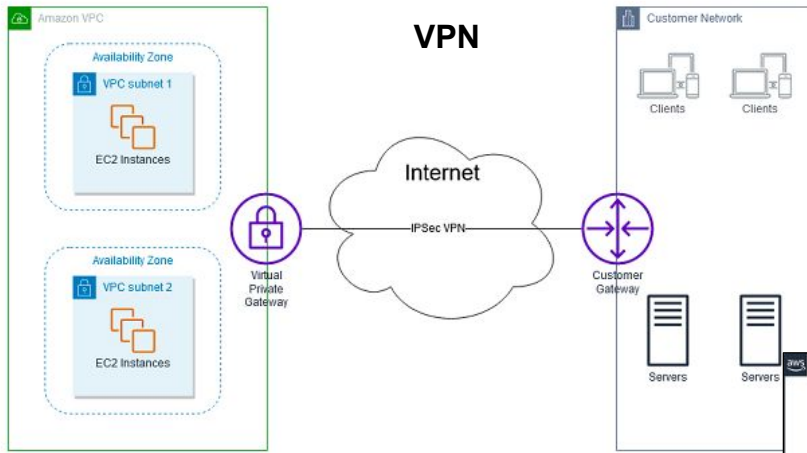**SCT (Schema conversion tool)**

KEY words: Transfer db to AWS ,
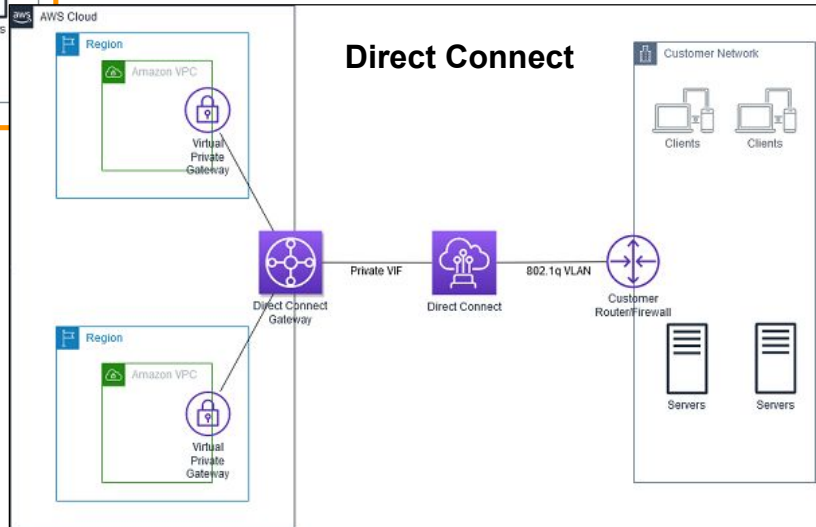   Snapshots of db in S3,   No impact on client usage of app
                        S3 data is fully synced with the on premise db.

End user — Viewer request → CloudFront cache → Origin request → Origin server

Viewer response ← CloudFront cache ← Origin response ← Origin server

S3 static Web Hosting

Amazon S3

Publish Direct from S3

S3 Distribution with S3 ARN

Amazon CloudFront

Publish from CloudFront

Also Accessible from S3

OAI Activated ?

No
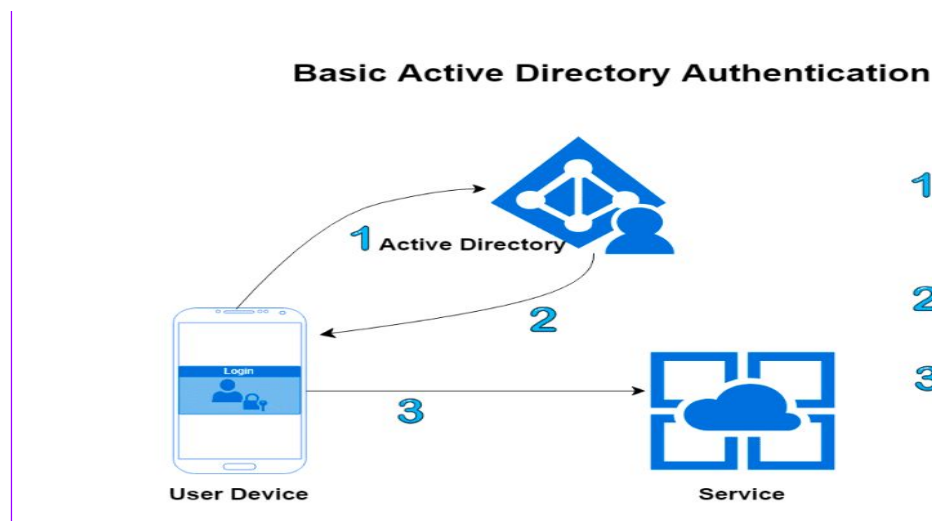
Yes

Only Accessible from CloudFront

VPN

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

Direct Connect

Basic Active Directory Authentication

AWS Directory Service for Microsoft Active Directory

Simple AD

AD Connector

Amazon Cognito

SAA 03 Practice Test 3
Osvaldo

Volume Gateway - Stored Mode

Entire dataset is stored in AWS and on-prem

Volume Gateway - Cache Mode

Frequently accessed data is stored on-prem