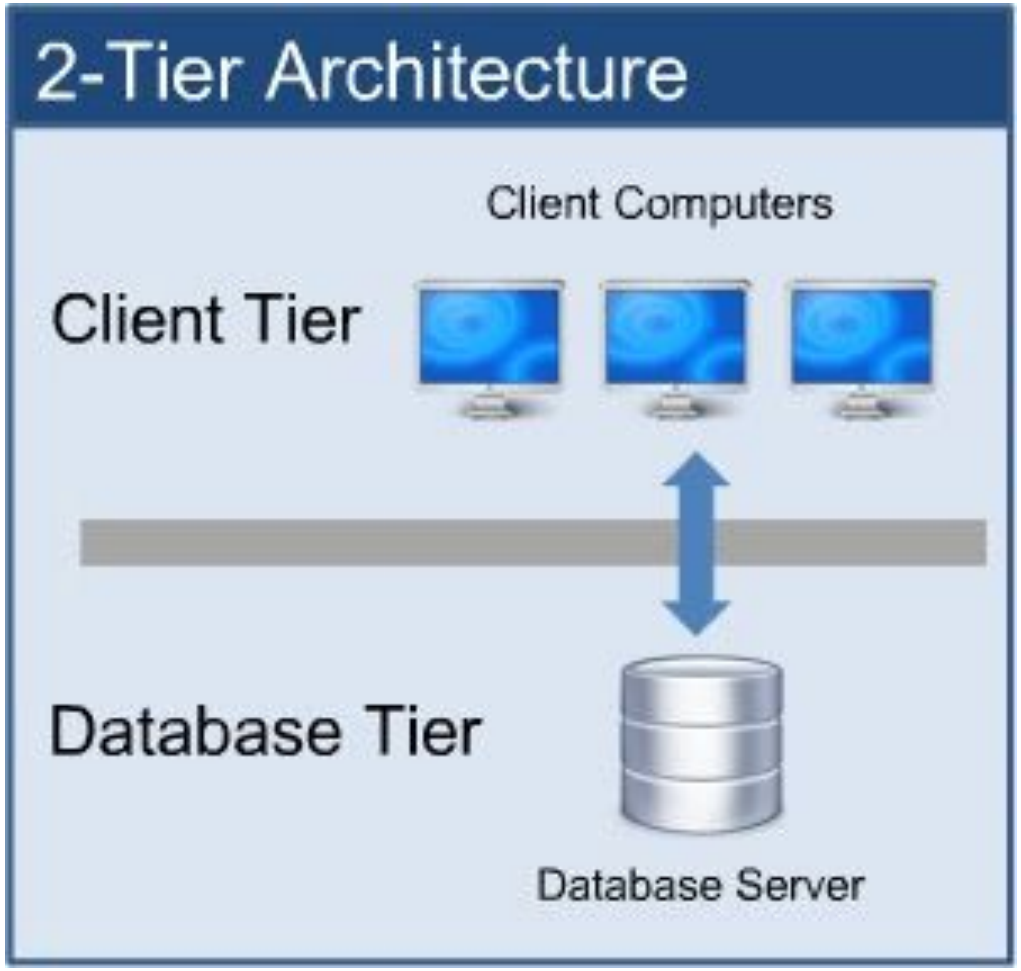
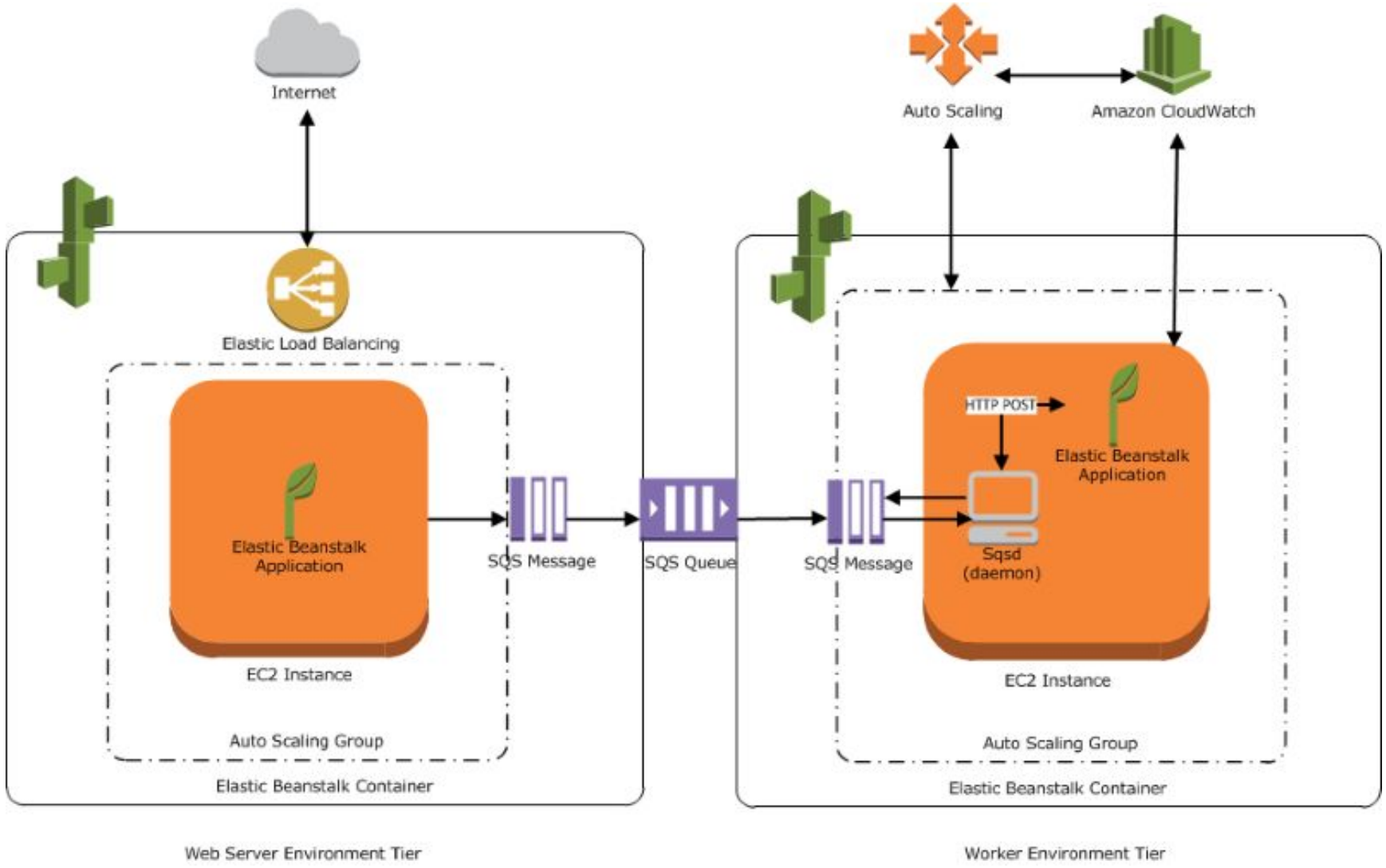
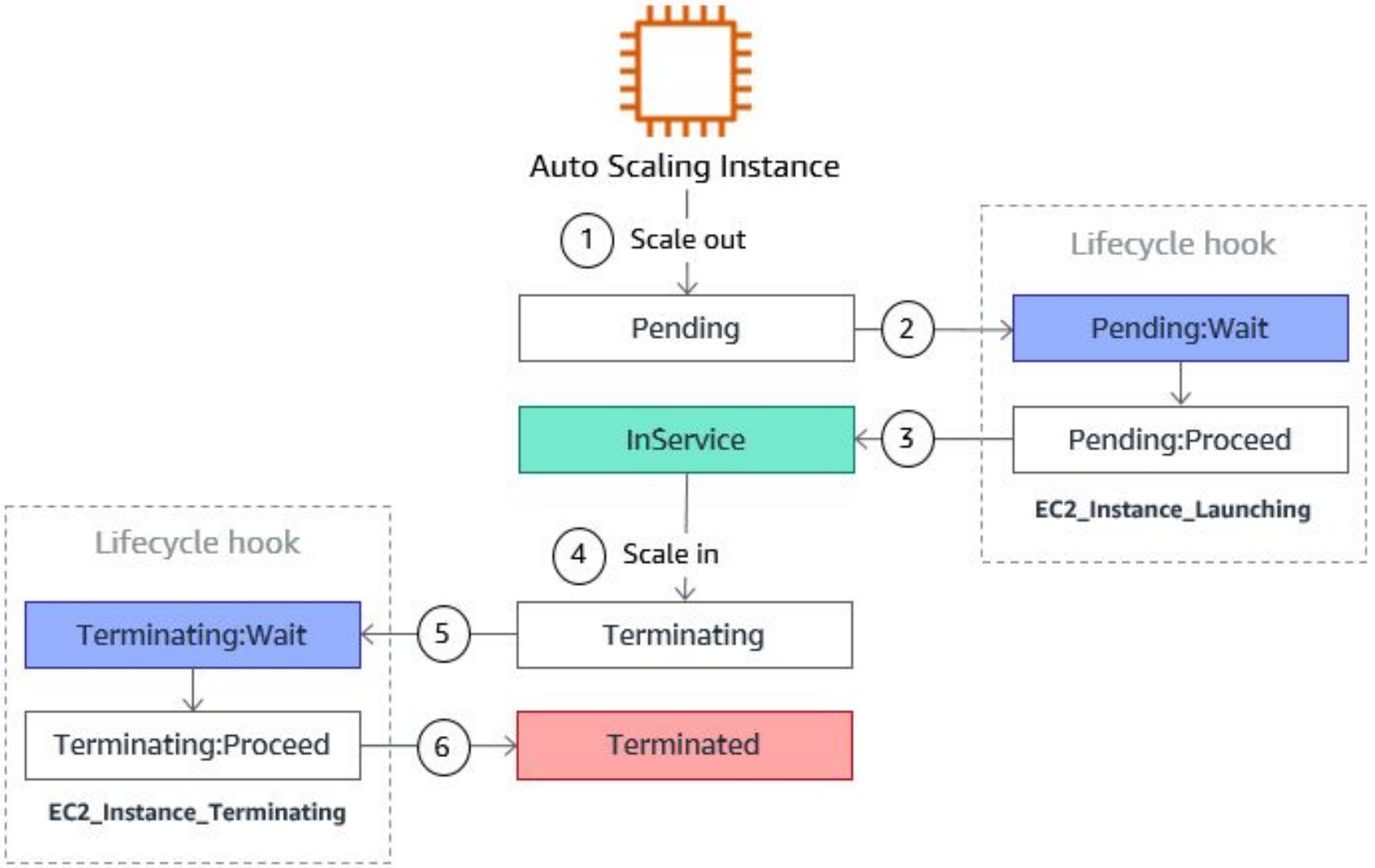
CSAA Test 1

CLARUSWAY
WAY TO REINVENT YOURSELF


2-Tier Architecture
Client Computers
Client Tier
Database Tier
Database Server



https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html

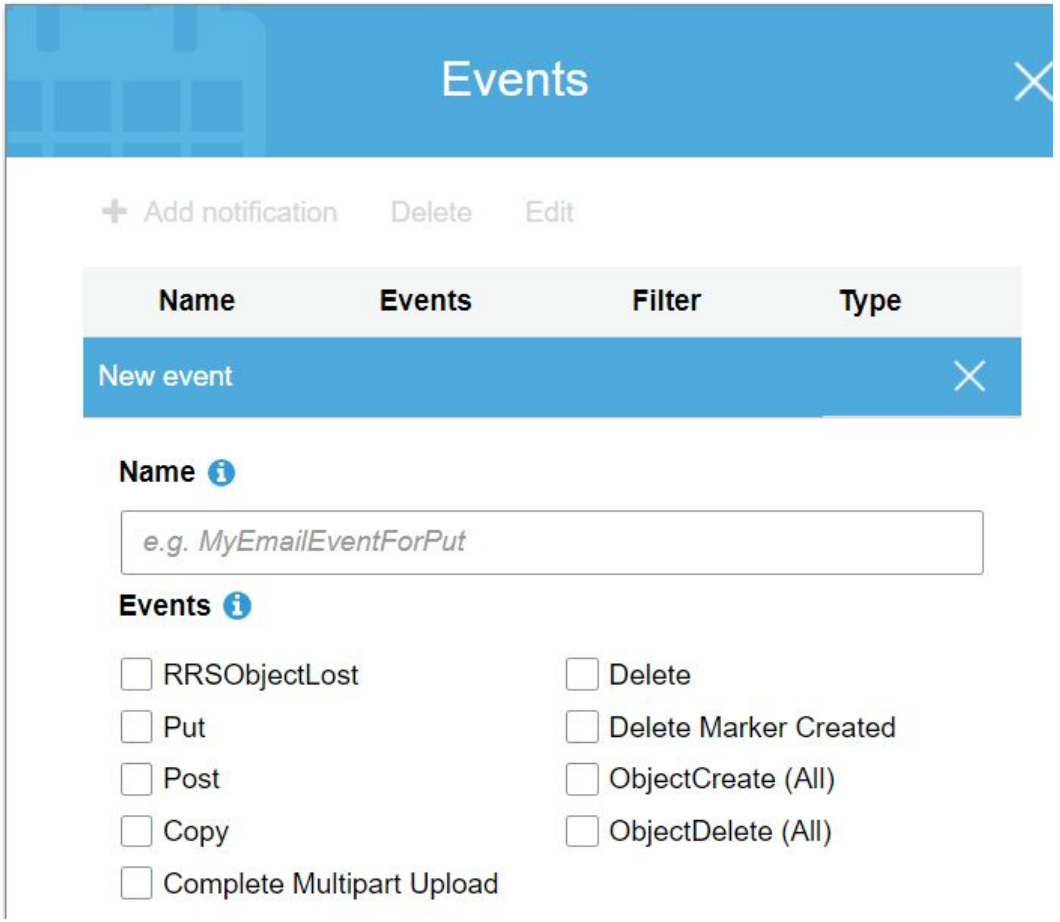


When a scale-in event occurs, a lifecycle hook pauses the instance before it is terminated and sends you a notification using Amazon EventBridge. While the instance is in the wait state, you can invoke an AWS Lambda function or connect to the instance to download logs or other data before the instance is fully terminated.

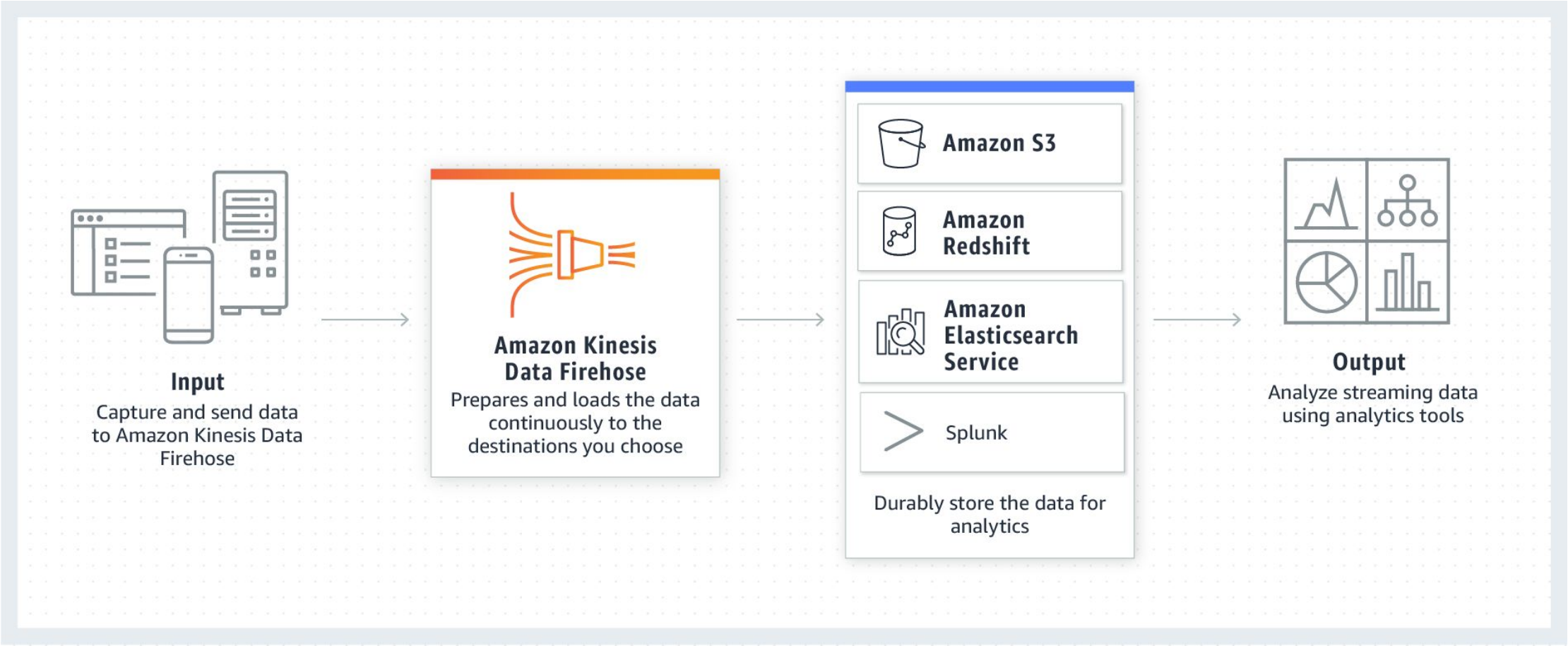
	AZ-1	AZ-2	AZ-3
A	2	2	2
B	3	3	0
C	4	2	2
D	6	6	0
E	3	3	3

LAMBDA

S3 EVENT NOTIFICATION

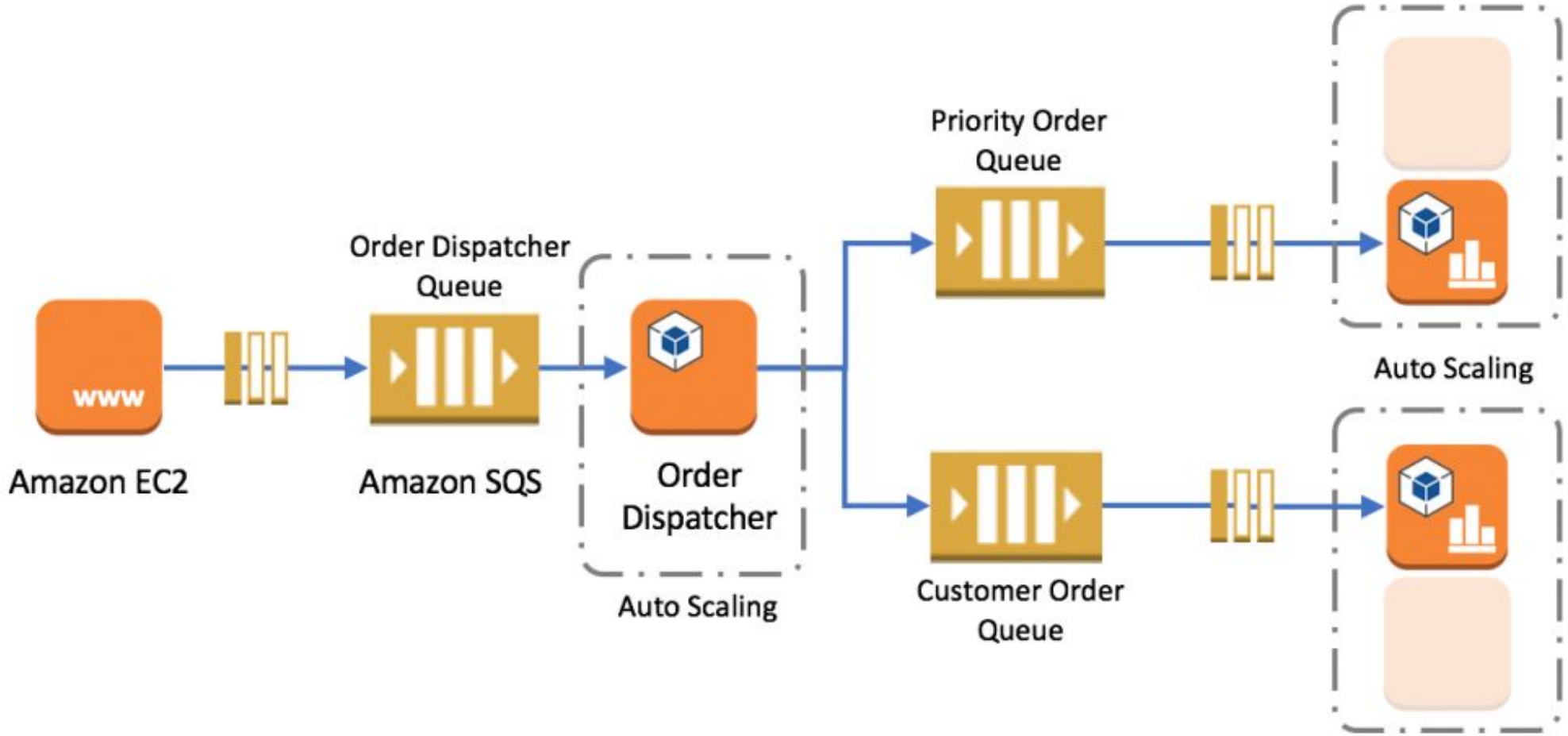


KINESIS

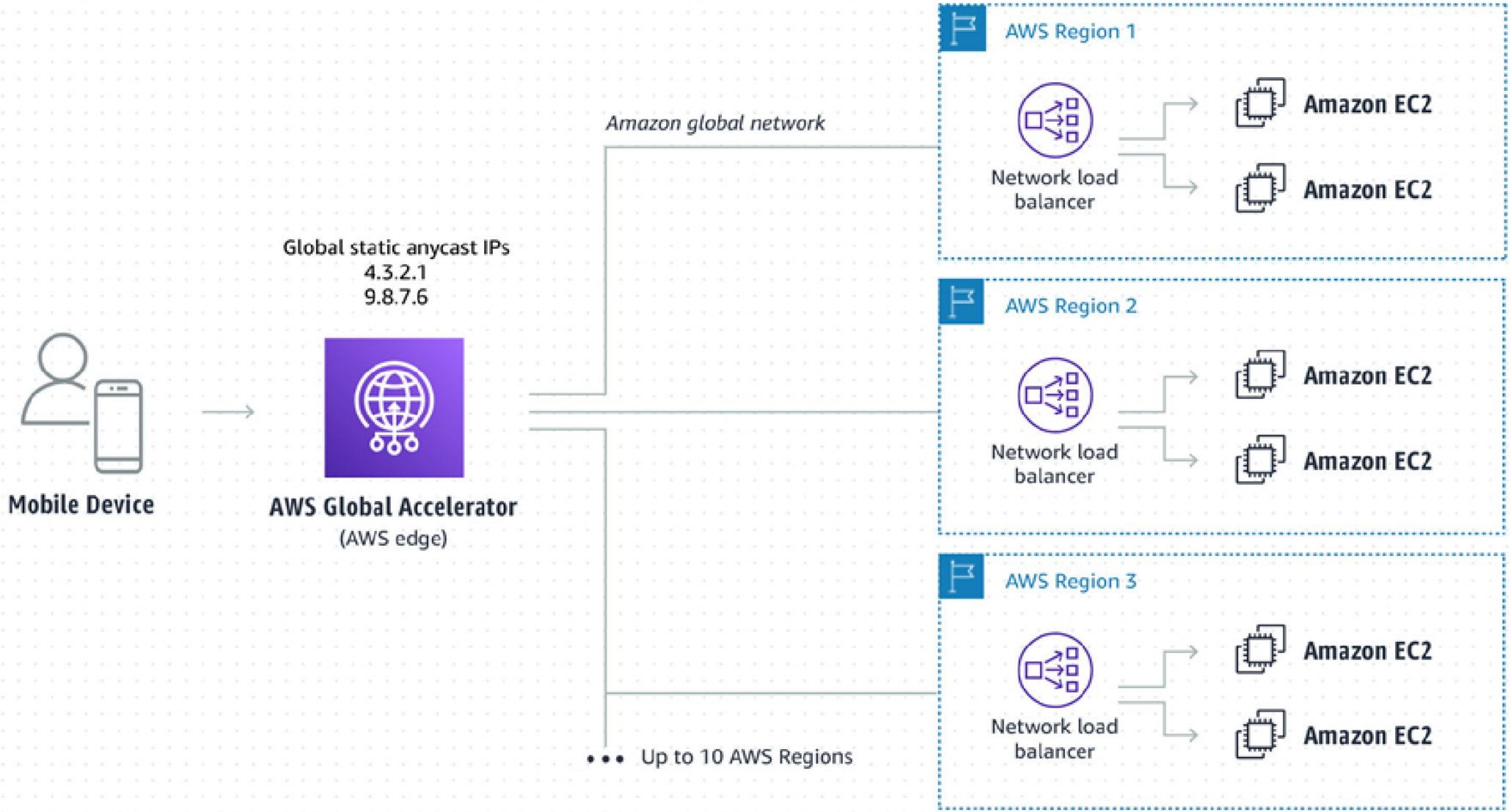


KINESIS is used to collect, process and analyze real-time data

SQS



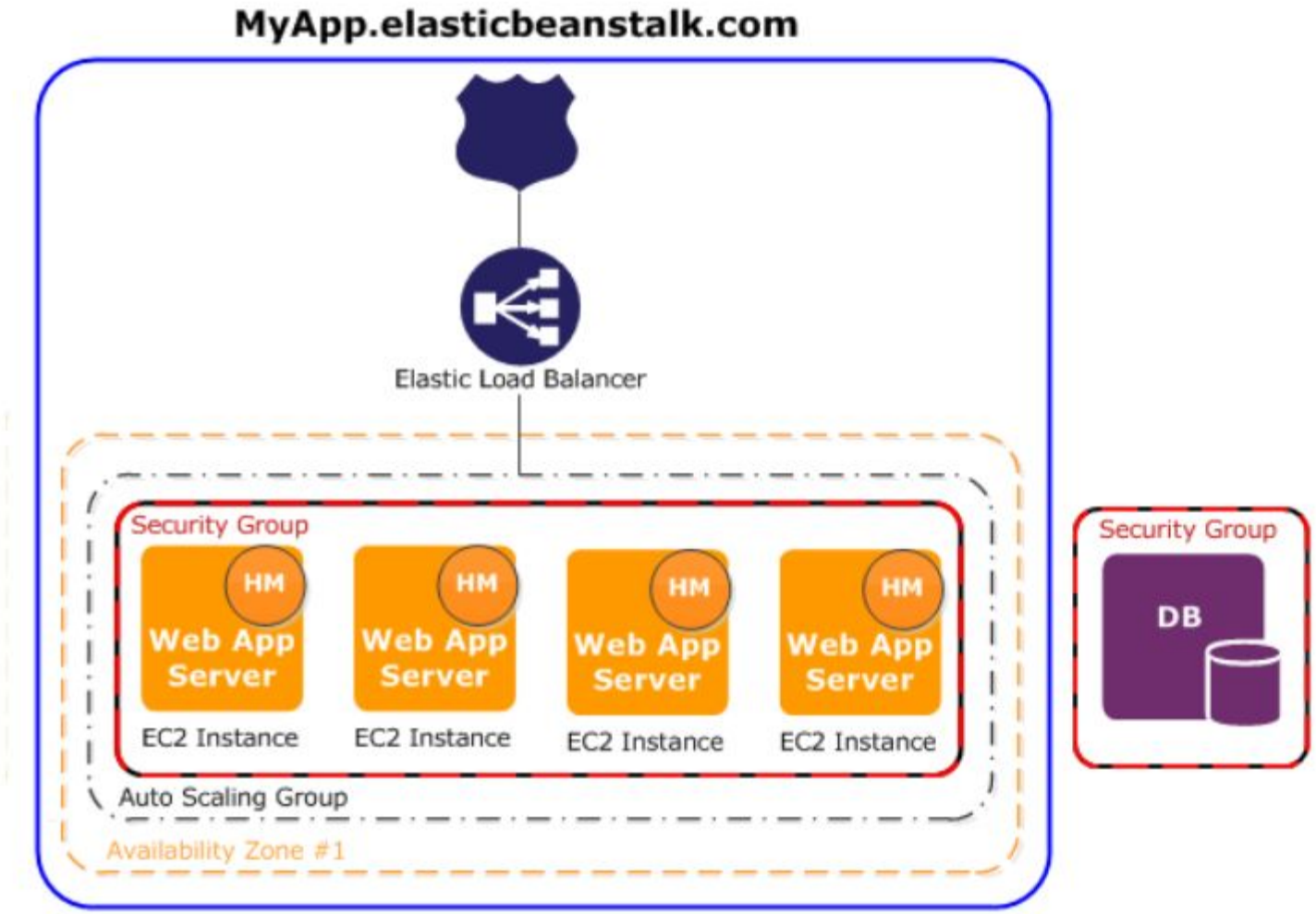
SQS MAX FİLE SİZE = 2 GB

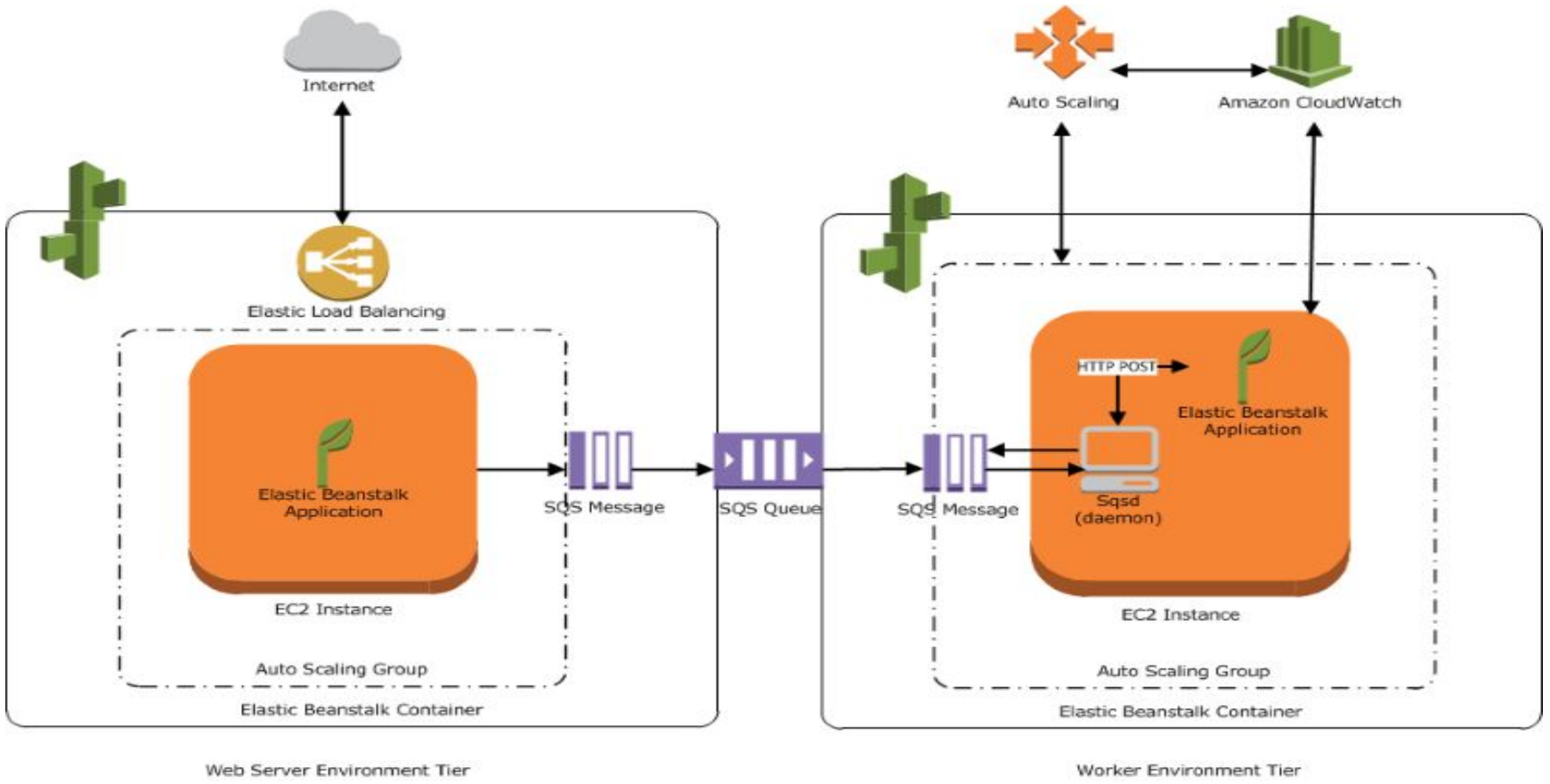

AWS Region 1
Amazon EC2
Network load balancer
Amazon EC2
Amazon global network
Global static anycast IPs
4.3.2.1
9.8.7.6
AWS Region 2
Amazon EC2
Network load balancer
Amazon EC2
Mobile Device
AWS Global Accelerator
(AWS edge)
AWS Region 3
Amazon EC2
Network load balancer
Amazon EC2
Up to 10 AWS Regions

Q: How is AWS Global Accelerator different from a DNS-based traffic management solution?

A: First, some client devices and internet resolvers cache DNS answers for long periods of time. So when you make a configuration update, or there's an application failure or change in your routing preference, you don't know how long it will take before all of your users receive updated IP addresses. With AWS Global Accelerator, you don't have to rely on the IP address caching settings of client devices. Change propagation takes a matter of seconds, which reduces your application downtime. Second, with Global Accelerator, you get static IP addresses that provide a fixed entry point to your applications. This lets you easily move your endpoints between Availability Zones or between AWS Regions, without having to update the DNS configuration or client-facing applications.

This following diagram illustrates an example Elastic Beanstalk architecture for a web server environment tier and shows h the components in that type of environment tier work together. The remainder of this section discusses all the component more detail.





Supported platform versions

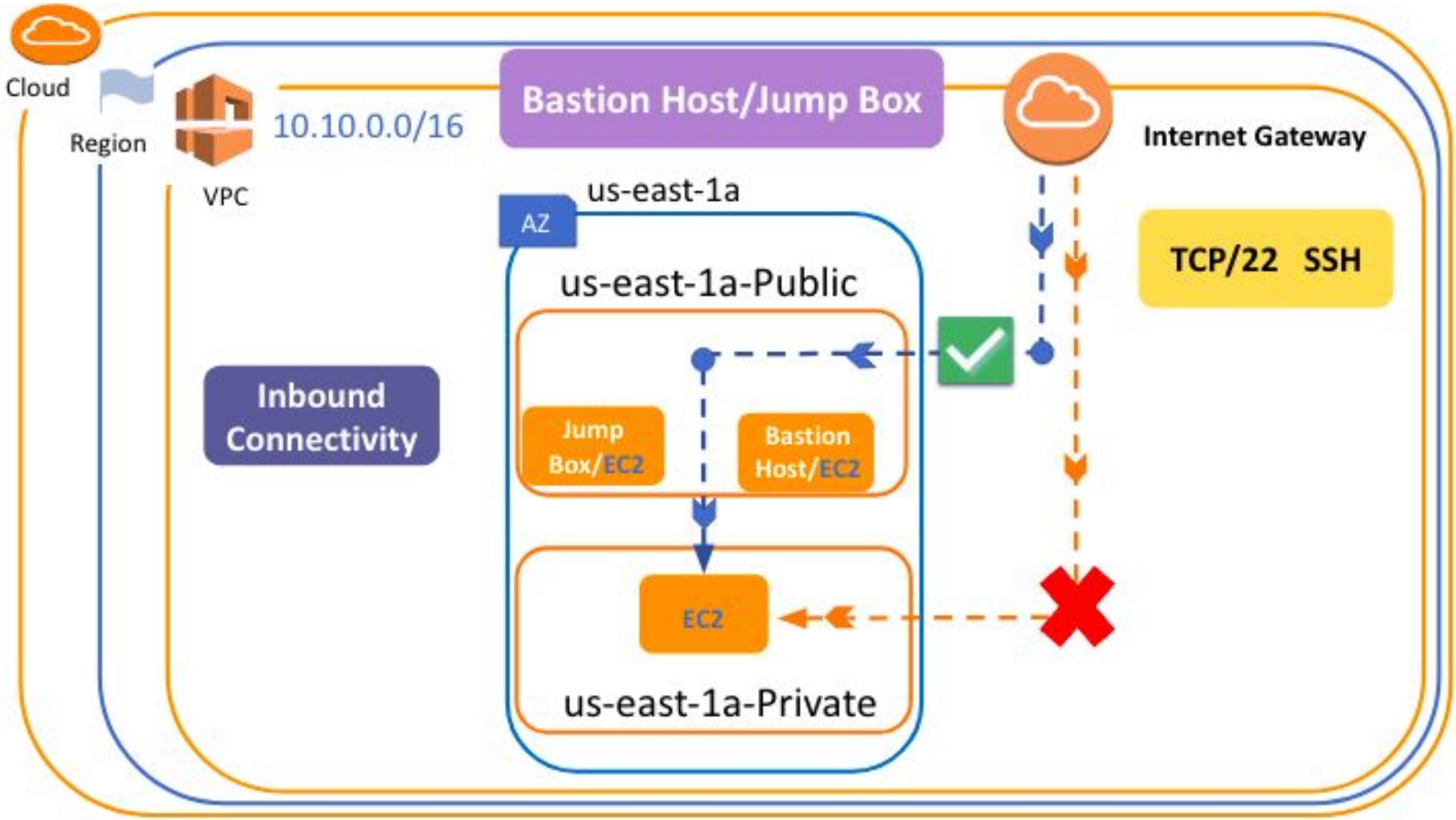
- Docker
- Multicontainer Docker
- Preconfigured Docker
- Go
- Java SE
- Tomcat
- .NET Core on Linux
- .NET on Windows Server
- Node.js
- PHP
- Python
- Ruby

	Throughput Optimized HDD	Cold HDD
Volume type	`st1`	`sc1`
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Big data • Data warehouses • Log processing	• Throughput-oriented storage for data that is infrequently accessed • Scenarios where the lowest storage cost is important

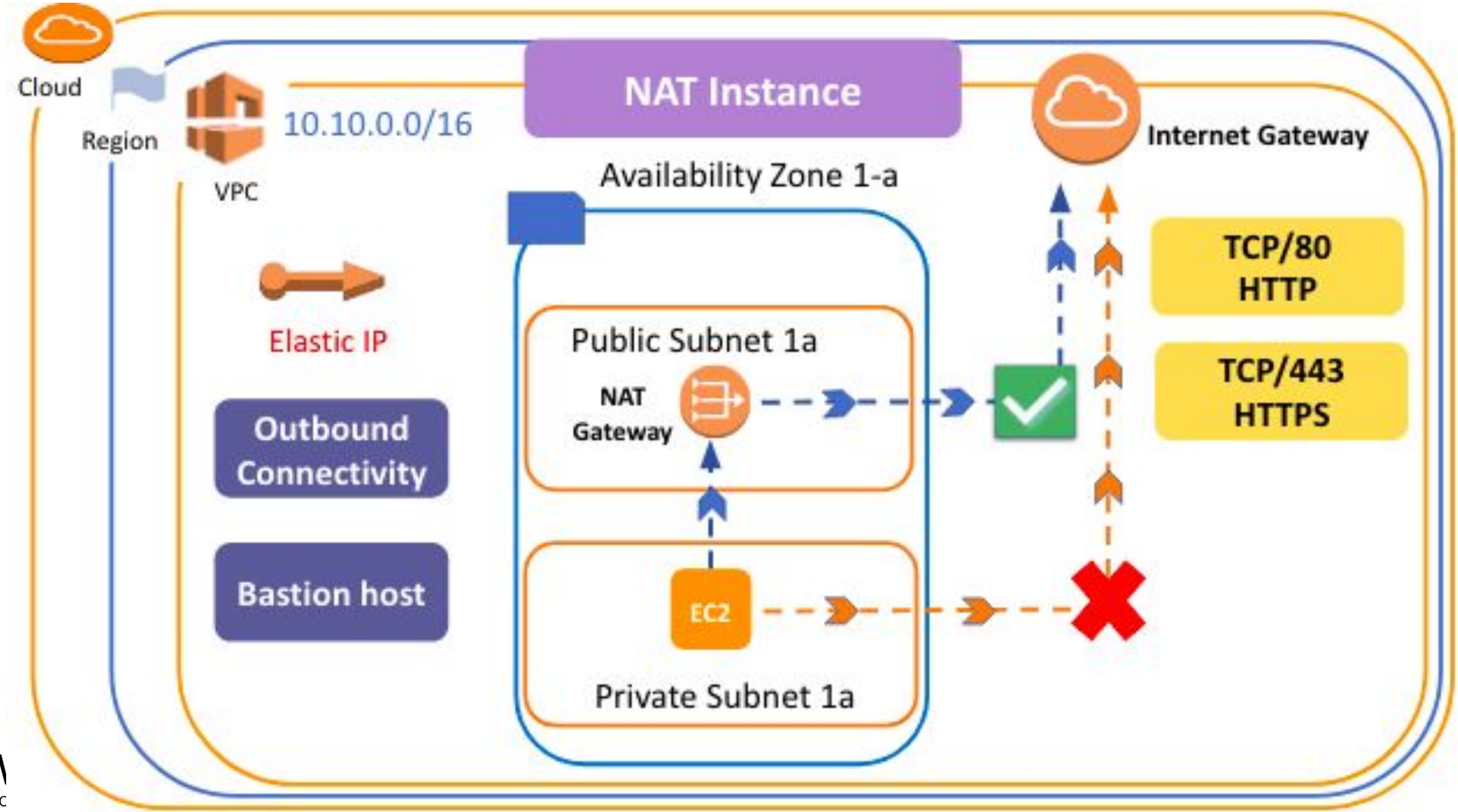
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

https://aws.amazon.com/ebs/features/

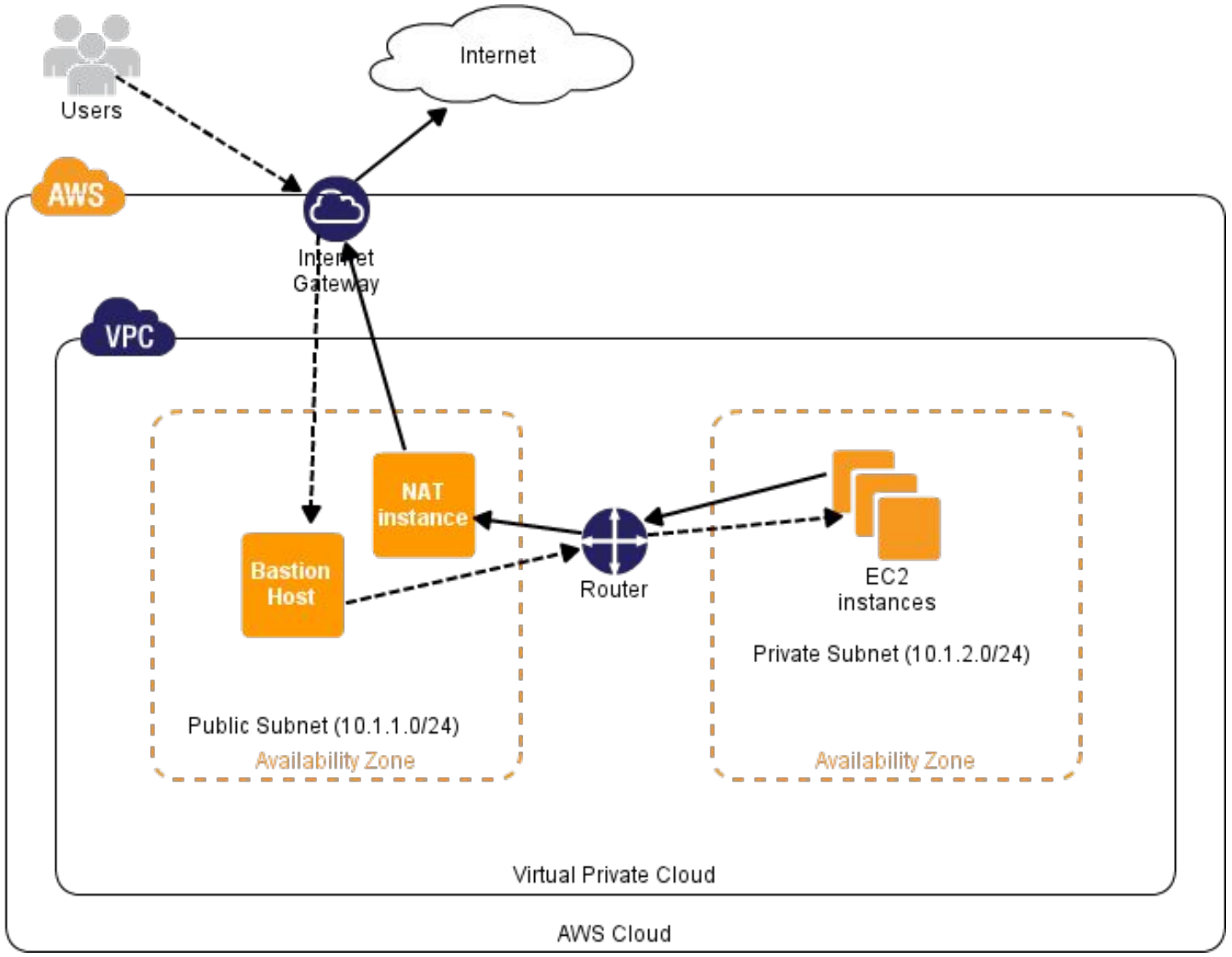
BASTION HOST



NAT INSTANCE



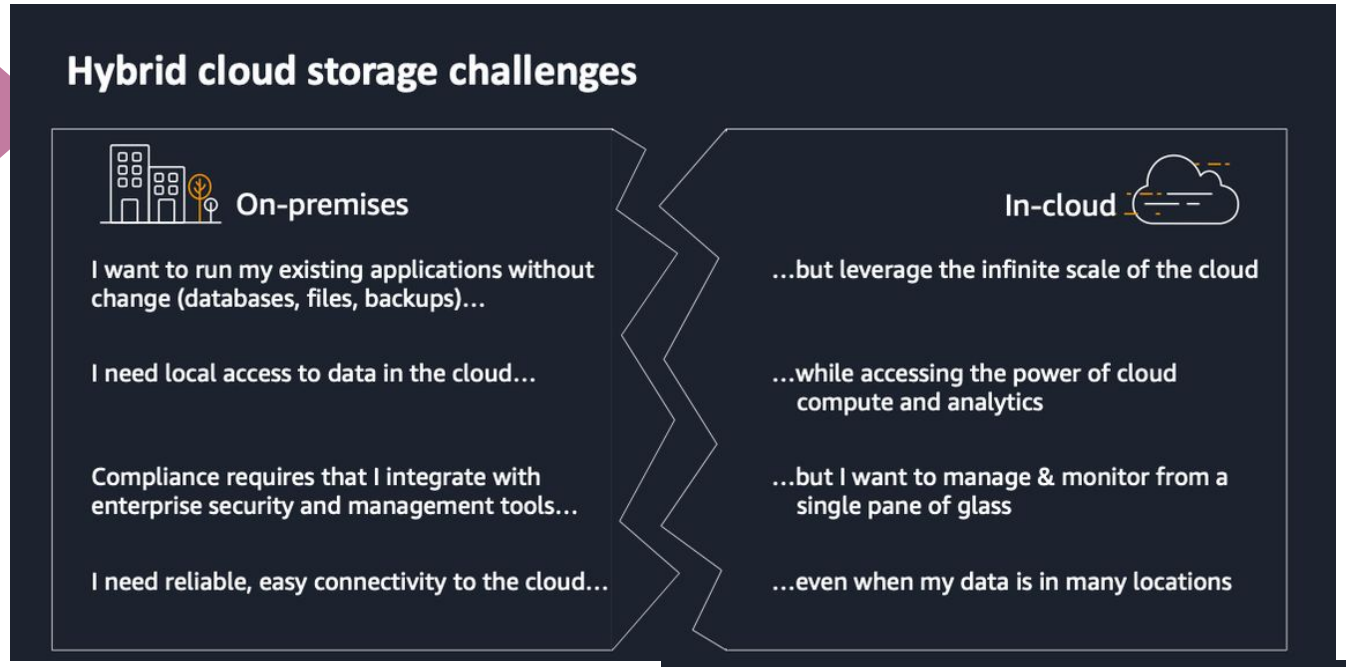
BASTION HOST VS NAT INSTANCE

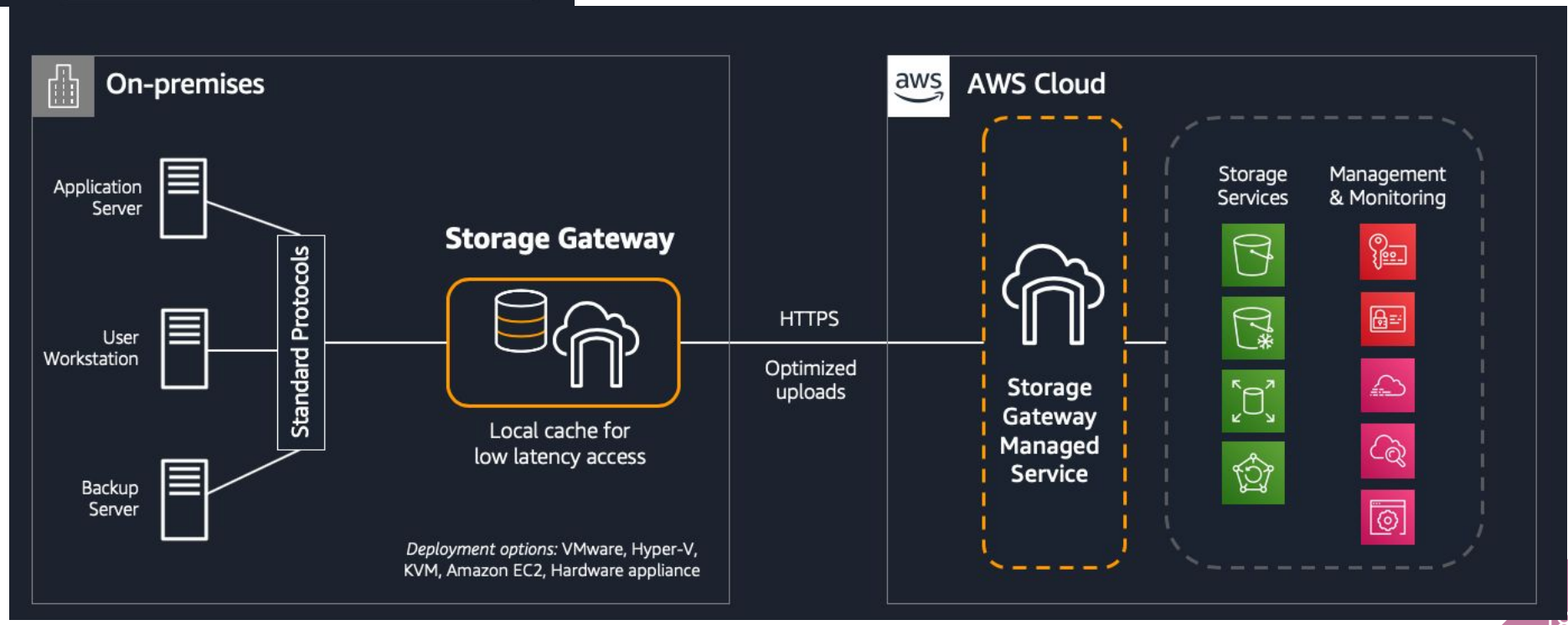


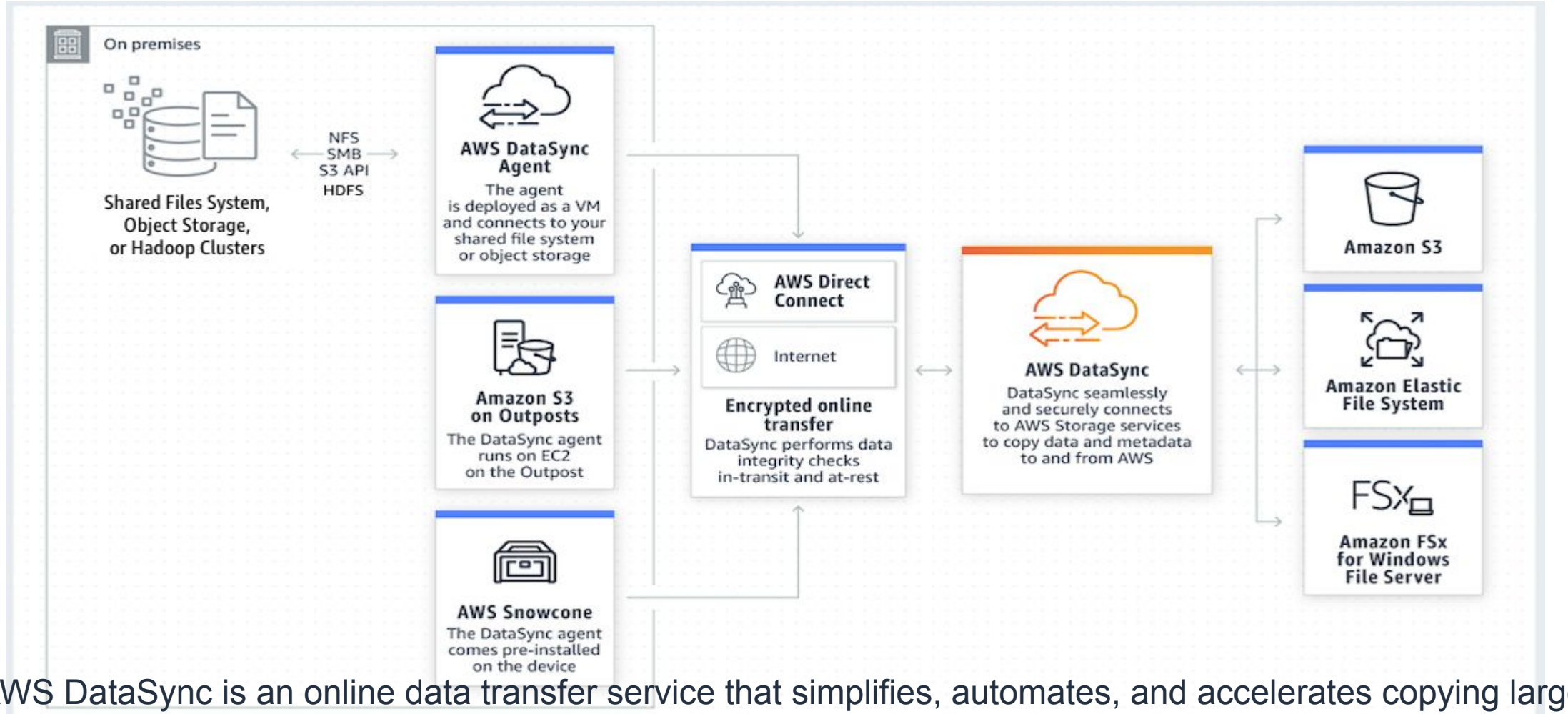
S3 Glacier Archives - Retrieval Options

Expedited	Expedited retrievals allow you to quickly access your data stored in the S3 Glacier Flexible Retrieval storage class or S3 Intelligent-Tiering Archive Access tier when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using **Expedited retrievals are typically made available within 1–5 minutes.**
Standard	Standard retrievals allow you to access any of your archives within several hours. **Standard retrievals typically complete within 3–5 hours.** This is the default option for retrieval requests that do not specify the retrieval option.
Bulk	Bulk retrievals are S3 Glacier's lowest-cost retrieval option, which you can use to retrieve large amounts, even petabytes, of data inexpensively in a day. **Bulk retrievals typically complete within 5–12 hours.**

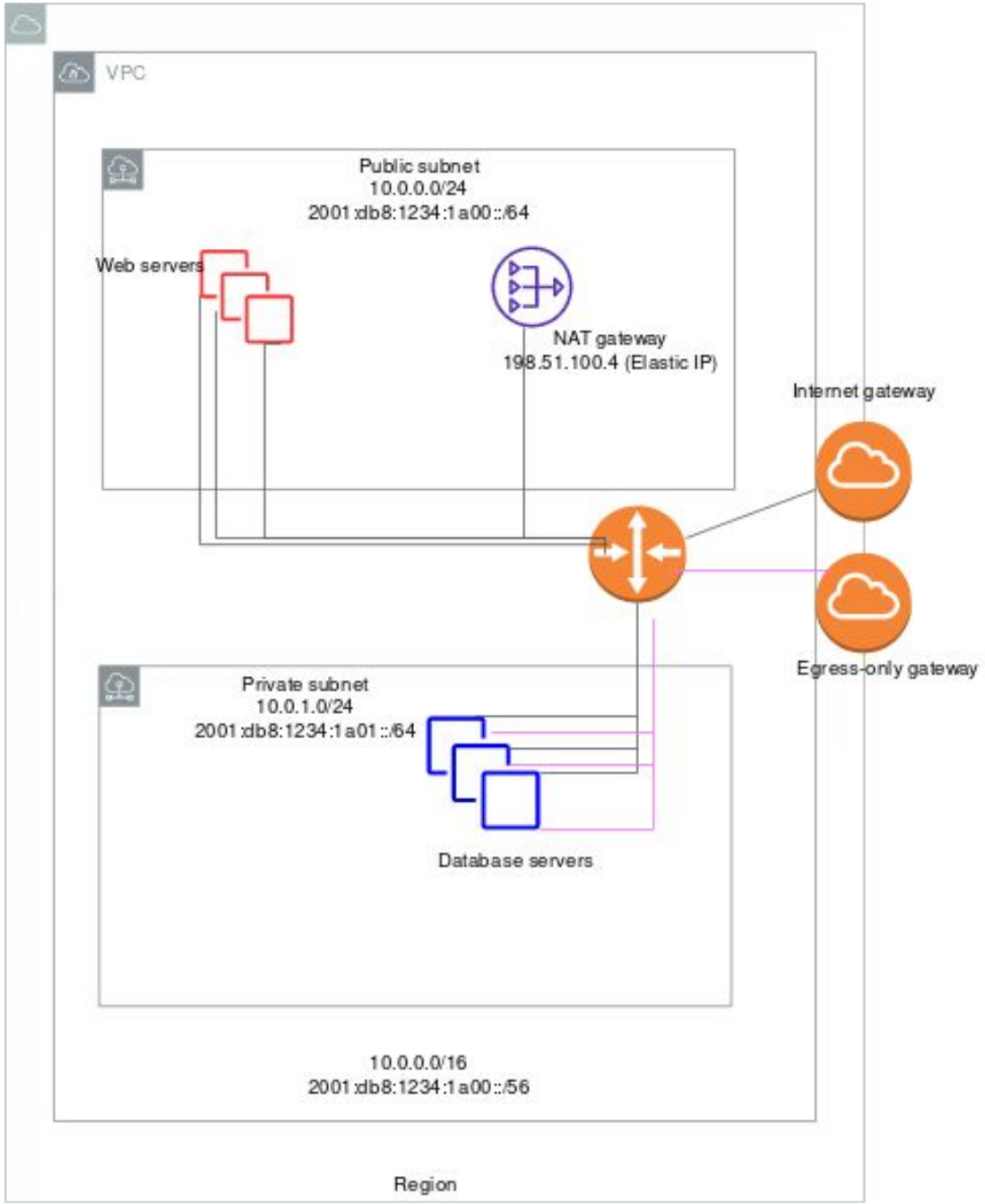
STORAGE GATEWAY



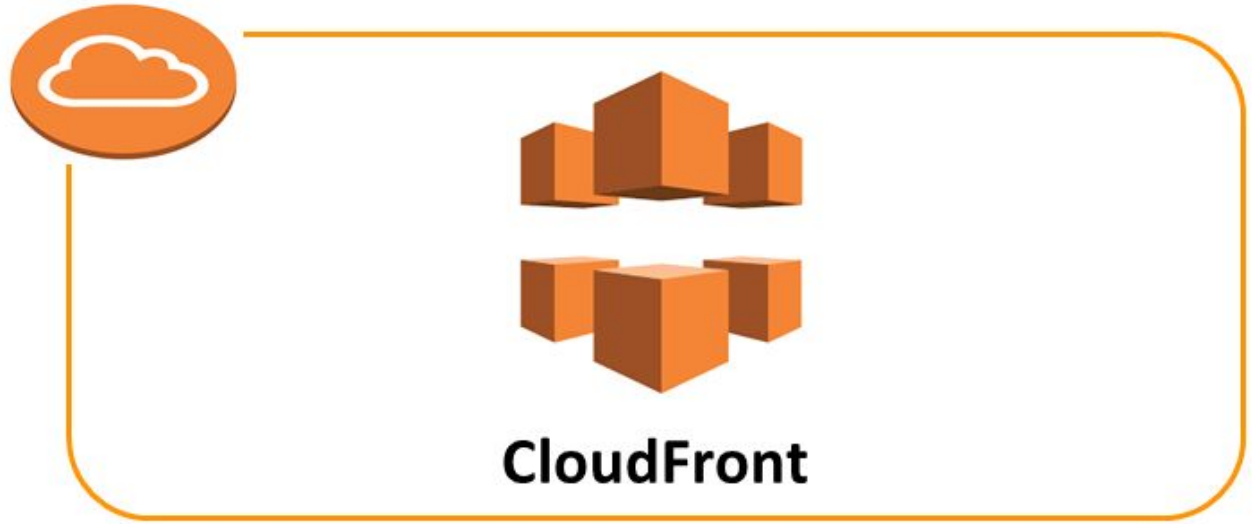




AWS DataSync is an online data transfer service that simplifies, automates, and accelerates copying large amounts of data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services. DataSync can copy data between Network File System (NFS), Server Message Block (SMB) file servers, Hadoop Distributed File Systems (HDFS), self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.


VPC
Public subnet
10.0.0.0/24
2001:db8:1234:1a00::/64
Web servers
NAT gateway
198.51.100.4 (Elastic IP)
Internet gateway
Egress-only gateway
Private subnet
10.0.1.0/24
2001:db8:1234:1a01::/64
Database servers
10.0.0.0/16
2001:db8:1234:1a00::/56
Region

CloudFront



- CloudFront is the **Content Delivery Network (CDN)** of AWS.
- Basically, it is a globally distributed network located on different geographical places.

CloudFront

- The aim of this service is to **provide faster distribution** to the dynamic or the static web contents.

- World-wide distributed data centers which are called **edge locations** are the backbone of CloudFront.

IAM roles

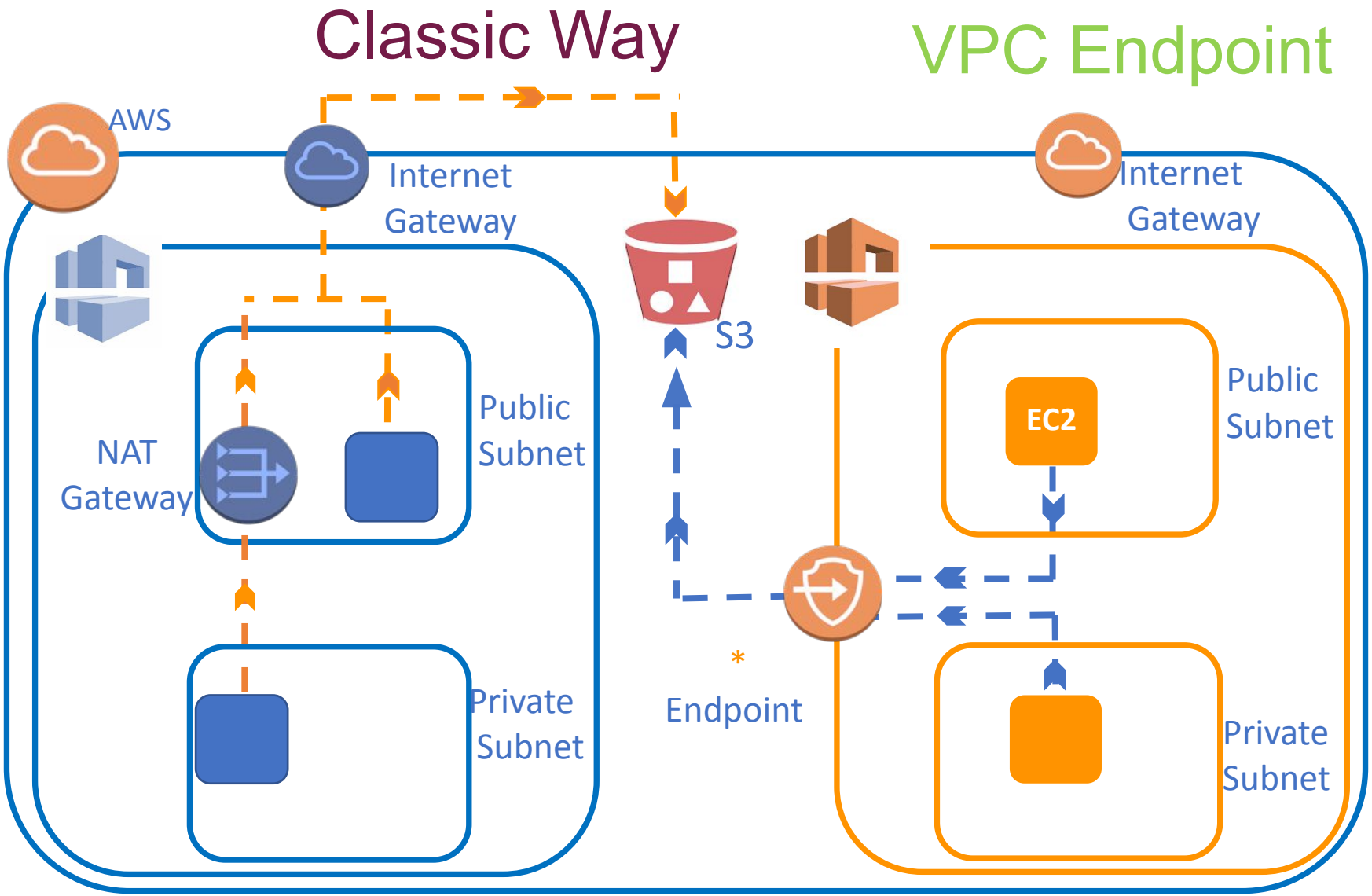
You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources.

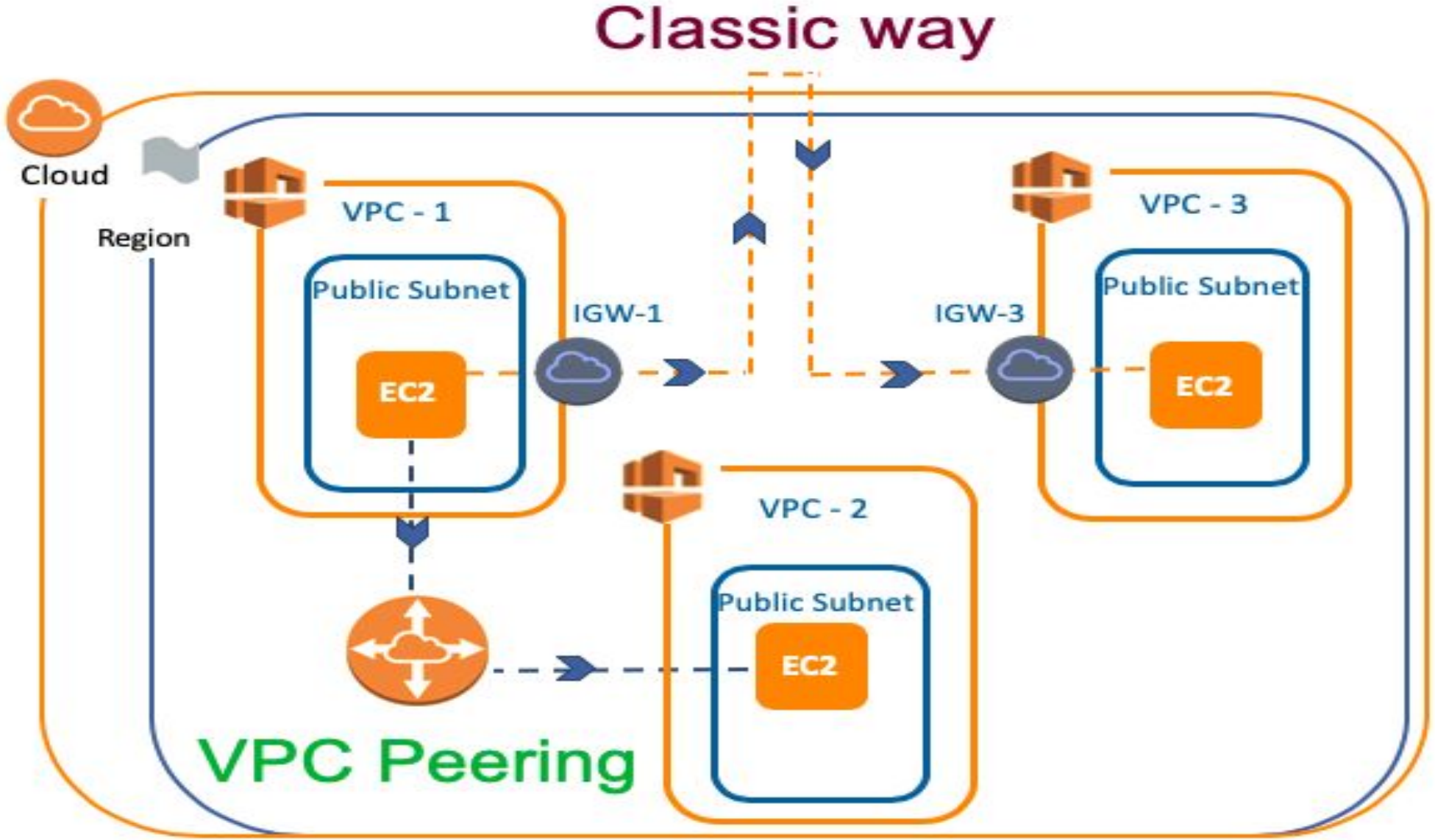
For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them).

Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.

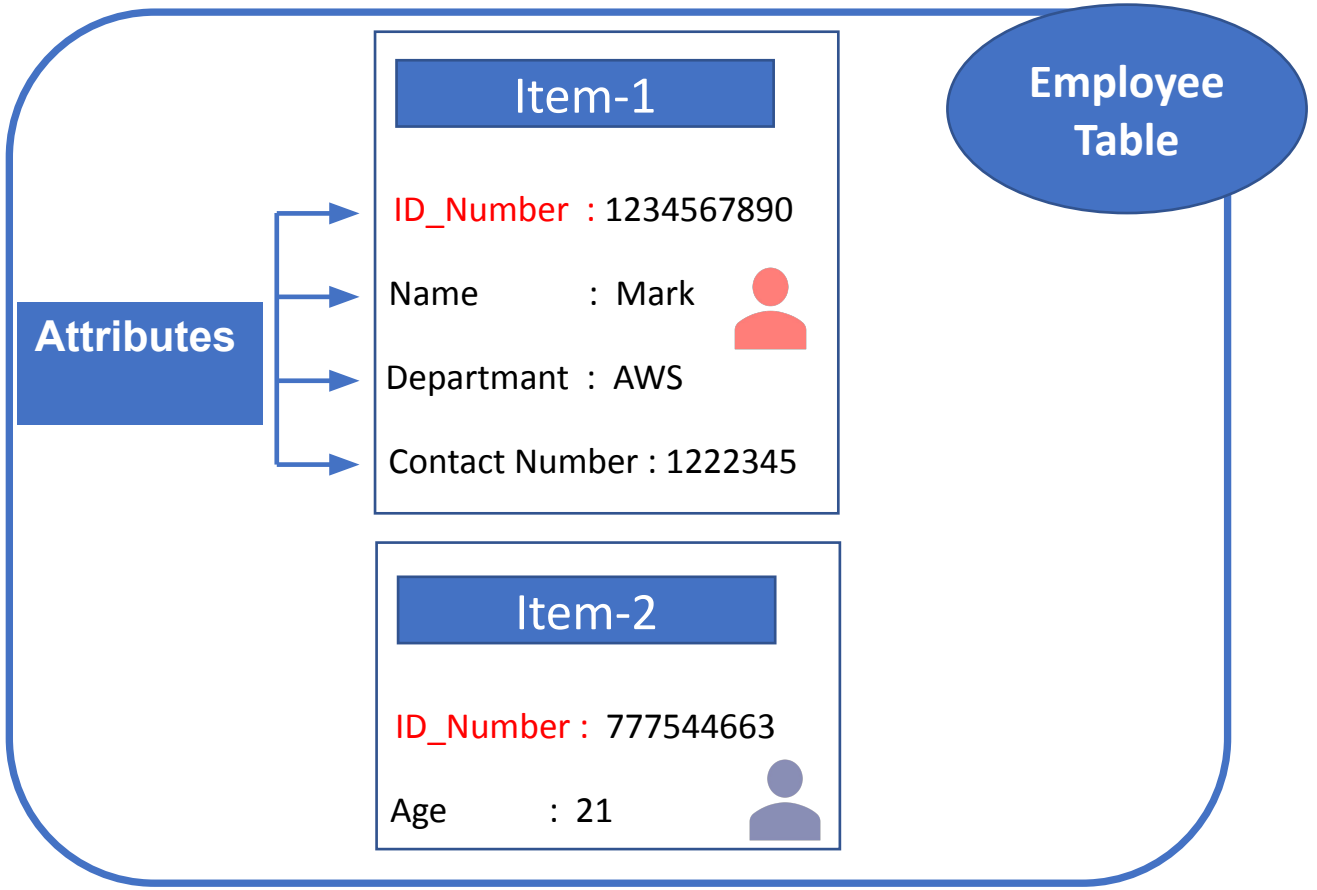
AWS Key Management Service

What is AWS Key Management Service?
AWS Key Management Service (AWS KMS) is a secured service to create and control the encryption keys. It is integrated with other AWS services such as Amazon EBS, Amazon S3 to provide data at rest security with encryption keys.
KMS is a global service but keys are regional which means you can't send keys
outside the region in which they are created.


Classic Way
VPC Endpoint
AWS
Internet Gateway
Internet Gateway
S3
NAT Gateway
Public Subnet
Private Subnet
EC2
Public Subnet
Private Subnet
*
Endpoint


Classic way
Cloud
Region
VPC - 1
Public Subnet
EC2
IGW-1
IGW-3
VPC - 3
Public Subnet
EC2
VPC - 2
Public Subnet
EC2
VPC Peering


amazon
DynamoDB

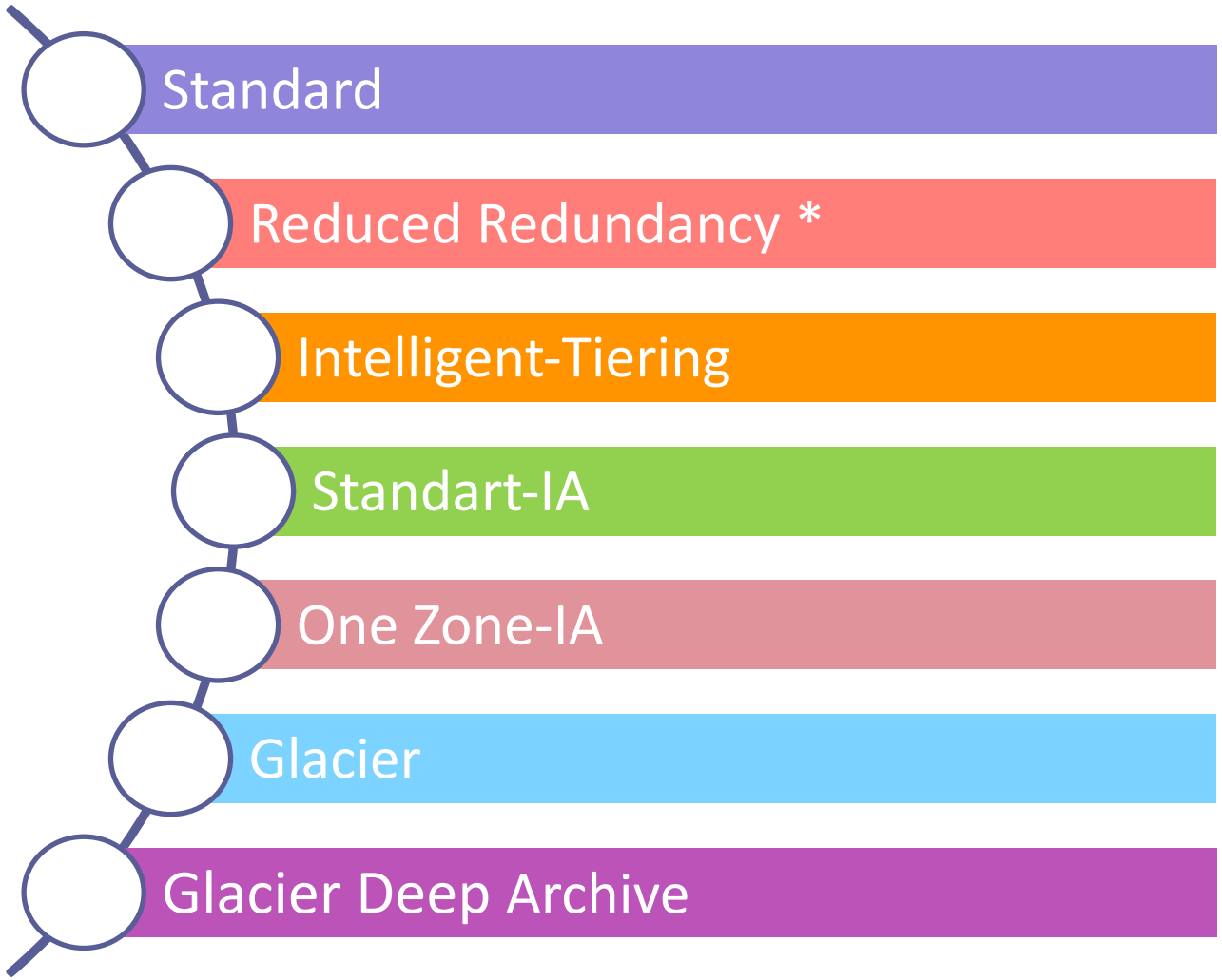

Employee Table
Item-1
ID_Number : 1234567890
Name : Mark
Departmant : AWS
Contact Number : 1222345
Attributes
Item-2
ID_Number : 777544663
Age : 21

Query String

A **query string** is a part of a uniform resource locator (URL) that assigns values to specified parameters. A query string commonly includes fields added to a base URL by a Web browser or other client application, for example as part of an HTML, choosing the appearance of a page, or jumping to positions in multimedia content

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html

Storage Classes

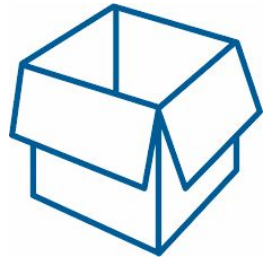


* Not recommended by AWS

Storage Classes

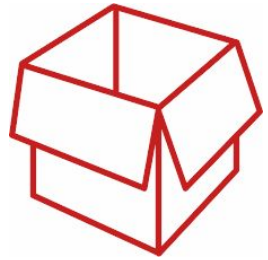
Intelligent Tier

Unpredictable
Access Patterns



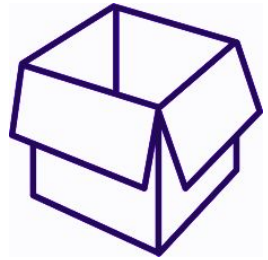
Frequent Access Tier

30 consecutive days after last access



Infrequent Access Tier

90 consecutive days after the last access



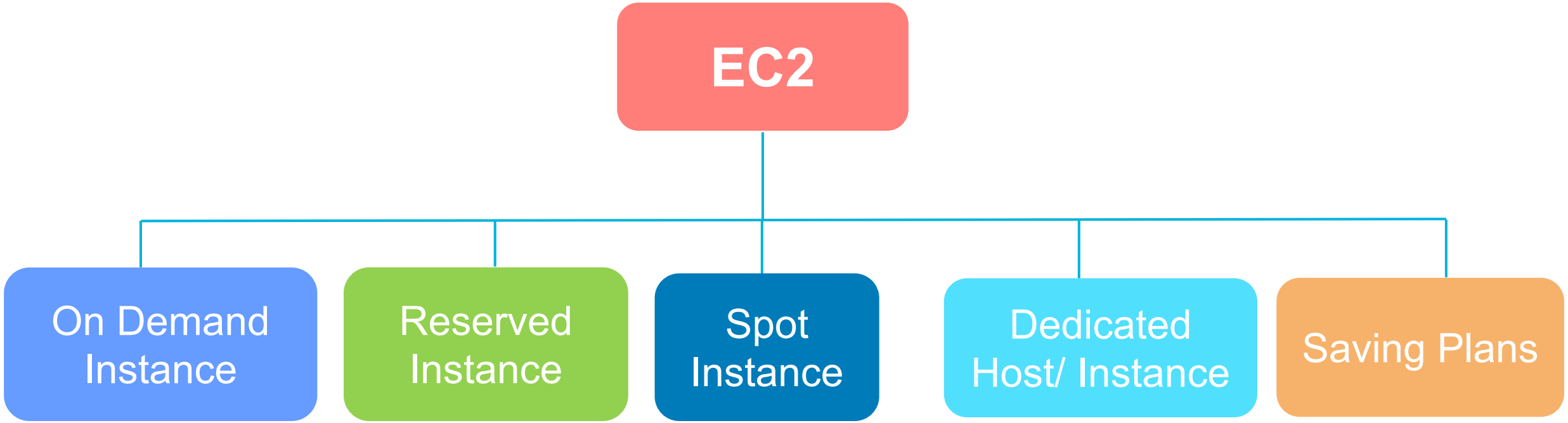
Archive Access tier

180 consecutive days after the last access

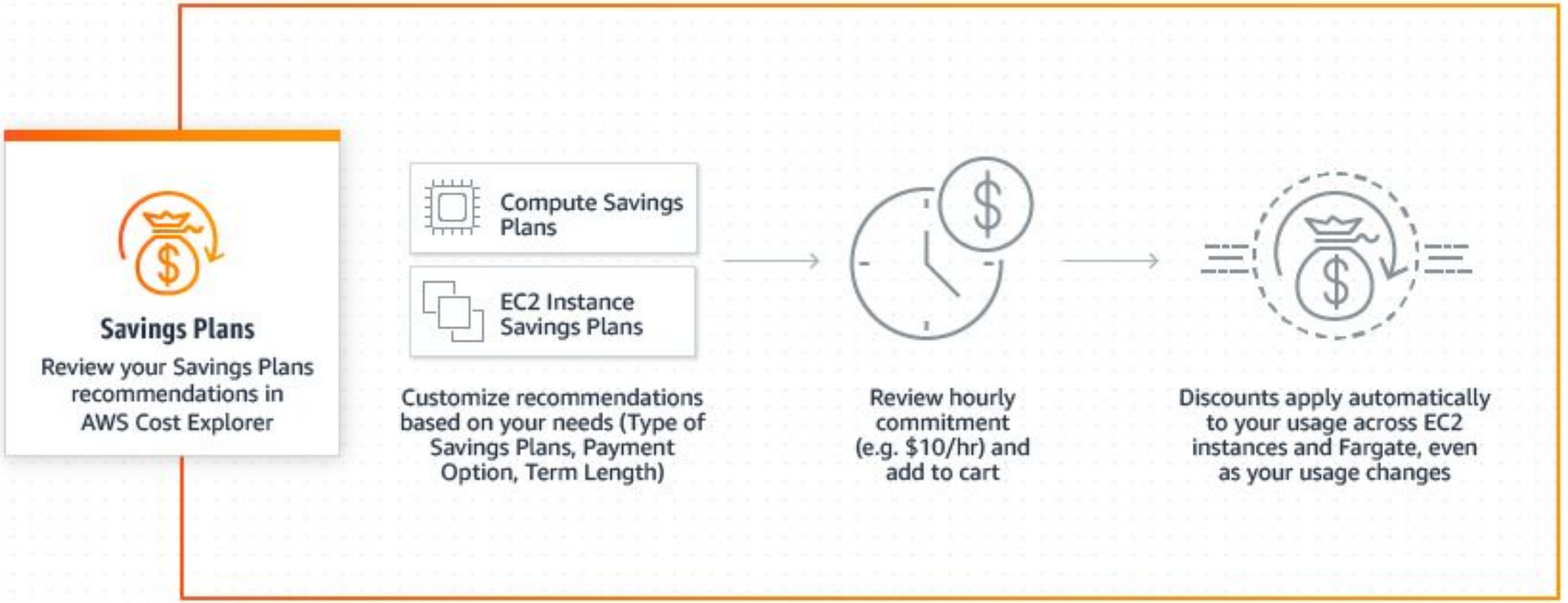
Deep Archive Access tier

- It is designed to optimize storage costs by automatically moving data to the most cost-effective storage access tier.
- There are 4 access tiers.
- It is ideal, if your access patterns are unknown or unpredictable.

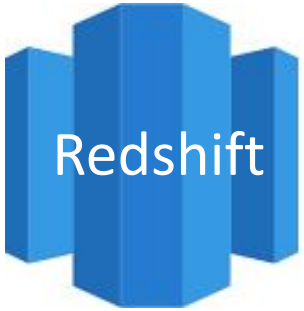
Pricing Model of Instances



Pricing Model of Instances

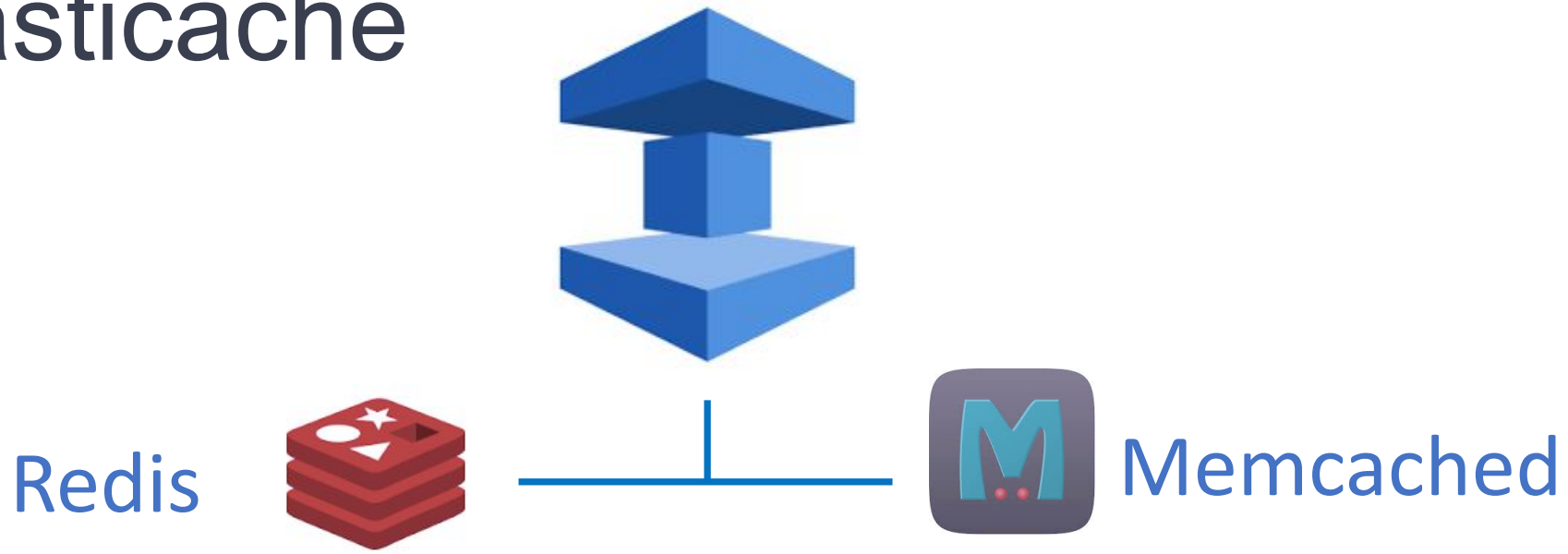


Amazon Redshift

Database	Data Warehouse
	
OLTP (Online Transaction Processing)	OLAP (Online Analytical Processing)
Used for data storing and managing	Used for data analyzing

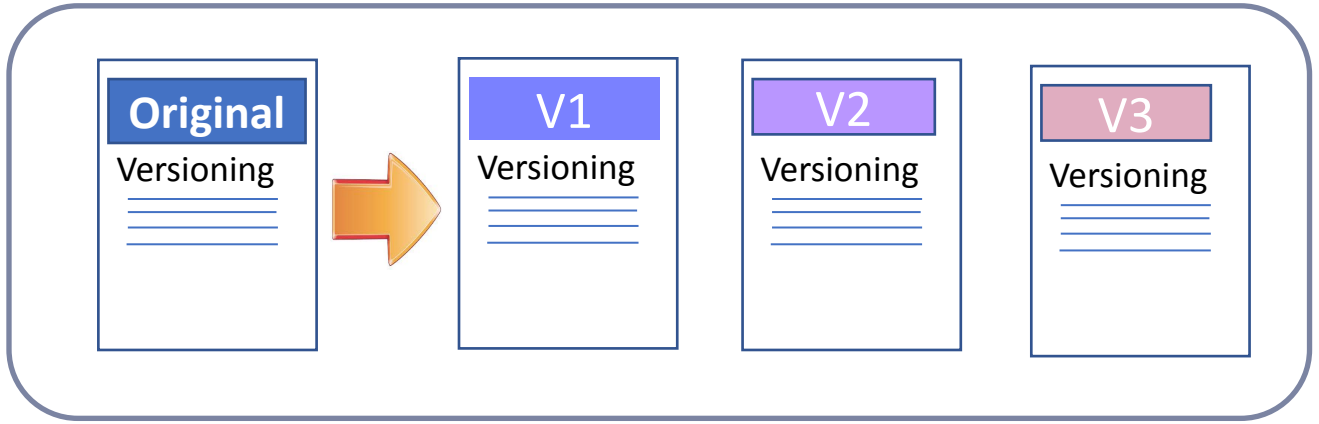
- Since the analyzing process causes an extra workload on database we prefer to use data warehouse
- Amazon Redshift is a fully managed, cloud-based, petabyte-scale data warehouse service by Amazon Web Services (AWS).
- Amazon Redshift is an efficient solution to collect and store all your data to analyze.

AWS Elasticache



- Elasticache is an **In-Memory Cache service of AWS.**
- In-Memory Cache is a **temporary and fast** storage component. These components are used to reduce the workload of the main data storage device such as a database.
- AWS offers Redis and Memcached in-memory cache option which are popular in market.

Versioning



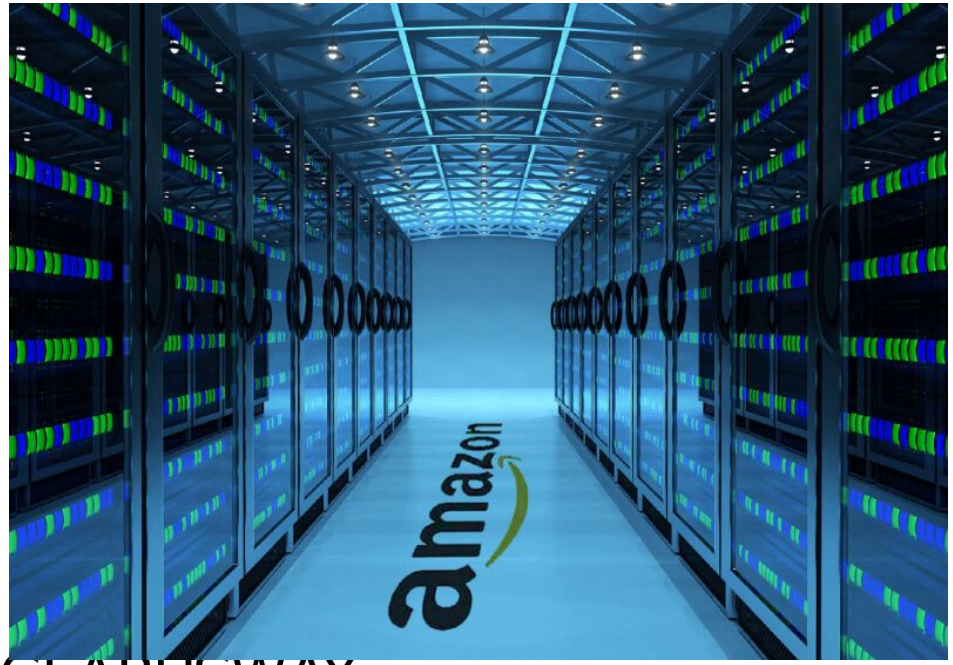
- Versioning is a way to keep multiple versions (deleted and changed versions) of an object in a bucket.

- By using versioning, all unwanted user behavior and program errors can be quickly recovered.

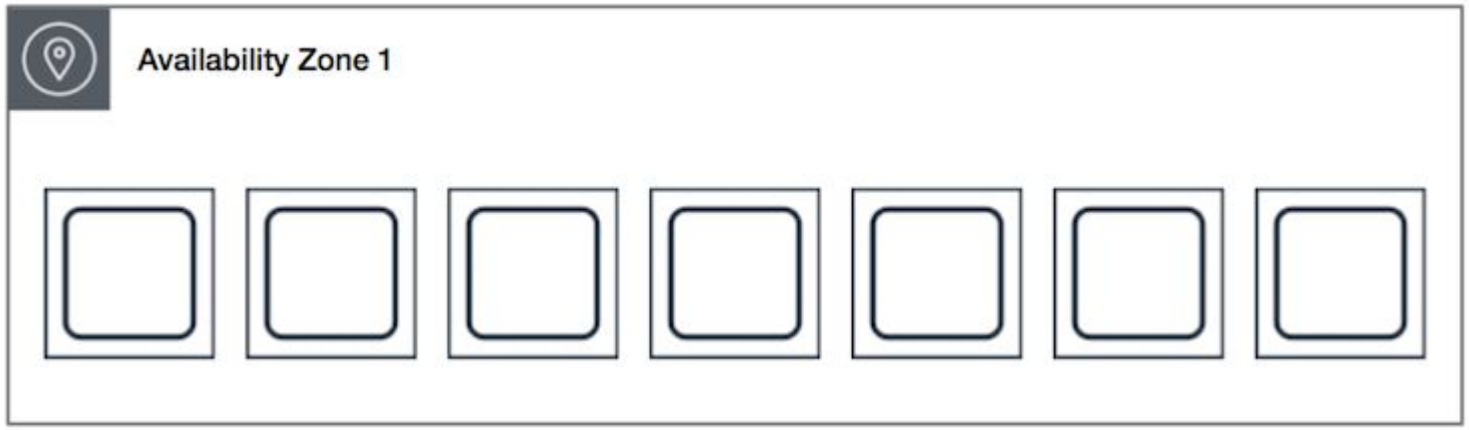
	General Purpose SSD		Provisioned IOPS SSD		
Volume type	gp3	gp2	io2 Block Express ‡	io2	io1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Low-latency interactive apps • Development and test environments		Workloads that require: • Sub-millisecond latency • Sustained IOPS performance • More than 64,000 IOPS or 1,000 MiB/s of throughput	• Workloads that require sustained IOPS performance or more than 16,000 IOPS • I/O-intensive database workloads	

Placement groups

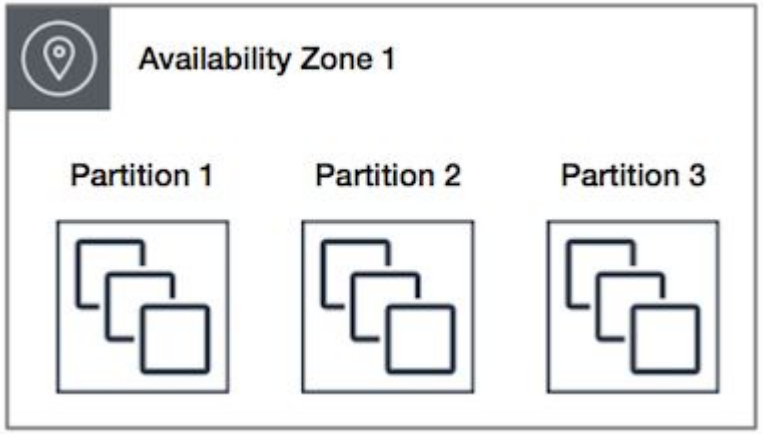
Cluster placement groups



spread placement group



Partition placement groups



https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

What is Amazon FSx for Windows File Server?

- Amazon FSx for Windows File Server is an FSx solution that offers a scalable and shared file storage system on the Microsoft Windows server.
- Using the Server Message Block (SMB) protocol with Amazon FSx Can access file storage systems from multiple windows servers.
- It offers to choose from HDD and SSD storage, offers high throughput, and IOPS with sub-millisecond latencies for Windows workloads.
- Using SMB protocol, Amazon FSx can connect file systems to Amazon EC2, Amazon ECS, Amazon WorkSpaces, Amazon AppStream 2.0 instances, and on-premises servers using AWS Direct Connect or AWS VPN.
- It provides high availability (Multi-AZ deployments) with an active and standby file server in separate AZs.
- It automatically and synchronously replicates data in the standby Availability Zone (AZ) to manage failover.
- Using AWS DataSync with Amazon FSx helps to migrate self-managed file systems to Windows storage systems.
- It offers identity-based authentication using Microsoft Active Directory (AD).
- It automatically encrypts data at rest with the help of AWS Key Management Service (AWS KMS). It uses SMB Kerberos session keys to encrypt data in transit.

What is Amazon FSx for Lustre?

- Amazon FSx for Lustre is an FSx solution that offers scalable storage for the Lustre system (parallel and high-performance file storage system).
- It supports fast processing workloads like custom electronic design automation (EDA) and high-performance computing (HPC).
- It provides shared file storage with hundreds of gigabytes of throughput, sub-millisecond latencies, and millions of IOPS.
- It offers a choice between SSD and HDD for storage.
- It integrates with Amazon S3 to process data concurrently using parallel data-transfer techniques.
- It stores datasets in S3 as files instead of objects and automatically updates with the latest data to run the workload.
- It offers to select unreplicated file systems for shorter-term data processing.
- It can be used with existing Linux-based applications without any changes.
- It offers network access control using POSIX permissions or Amazon VPC Security Groups.
- It easily provides data-at-rest and in-transit encryption.
- AWS Backup can also be used to backup Lustre file systems.
- It integrates with SageMaker to process machine learning workloads.

AWS Lambda

Lambda and API Gateway

- Alexa
- **API Gateway**
- CloudTrail
- CloudWatch Events
- CloudWatch Logs
- CloudFormation
- CloudFront (Lambda@Edge)
- CodeCommit
- CodePipeline
- Cognito
- Config
- DynamoDB
- EC2
- ElastiCache
- Elastic Load Balancing
- EFS
- IoT
- IoT Events
- Kinesis Firehose
- Kinesis Streams
- Lex
- RDS
- S3
- S3 Batch
- SES
- SNS
- SQS
- Step Functions
- X-Ray

Although you can trigger Lambda function in different way, the most common trigger of the Lambda function is API Gateway

Thanks to Lambda and API Gateway combination you can create fully automated system.

Auto Scaling

Auto Scaling Options

- Auto Scaling
  - Keep Initial Size
  - Scaling Policy
    - Dynamic Scaling
      - Target Tracking
      - Simple Scaling
      - Step Scaling
    - Predictive Scaling
    - Scheduled Action

What is AWS CloudTrail?

AWS CloudTrail is defined as a global service that permits users to enable operational and risk auditing of the AWS account.

It allows users to view, search, download, archive, analyze, and respond to account activity across the AWS infrastructure.

It records actions as an event taken by a user, role, or an AWS service in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

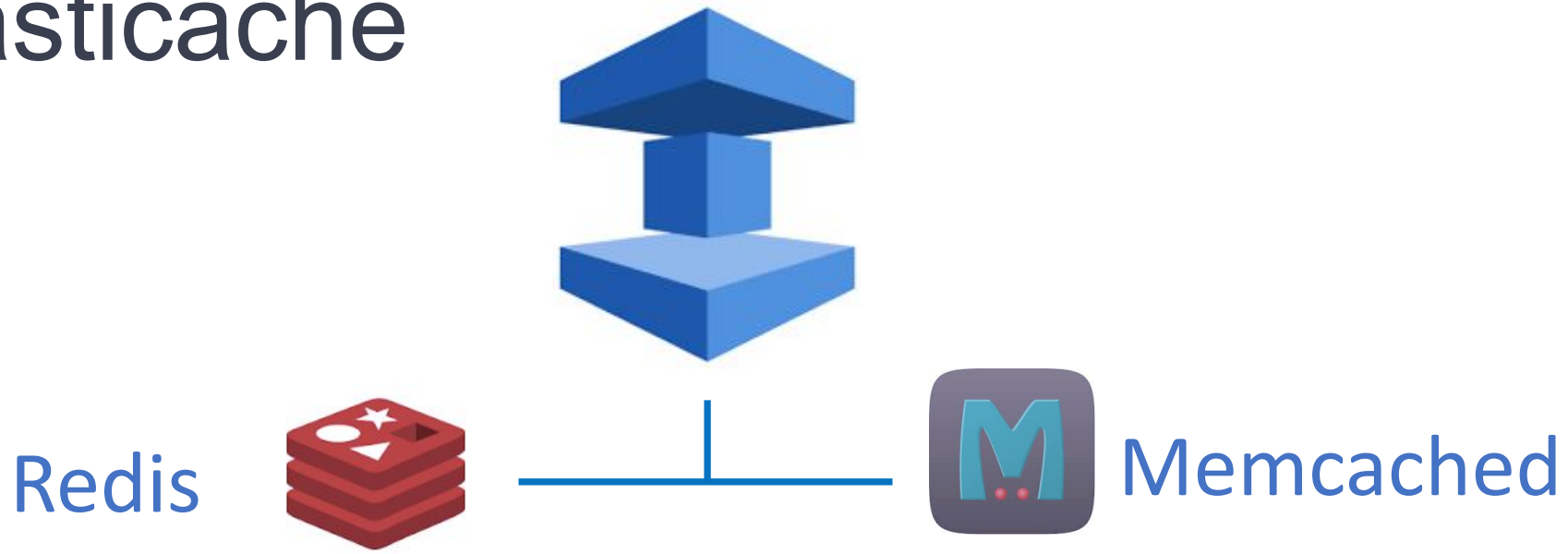
AWS CloudTrail mainly integrates with:

- Amazon S3 can be used to retrieve log files.
- Amazon SNS can be used to notify about log file delivery to the bucket with
Amazon Simple Queue Service (SQS).
- Amazon CloudWatch for monitoring and AWS Identity and Access Management (IAM) for security.

CloudTrail events of the past 90 days recorded by CloudTrail can be viewed in the CloudTrail console and can be downloaded in CSV or JSON file.
Trail log files can be aggregated from multiple accounts to a single bucket and can be shared between accounts.
AWS CloudTrail Insights enables AWS users to identify and respond to unusual activities of API calls by analyzing CloudTrail management events.
There are three types of CloudTrail events:

- Management events or control plane operations
  - Example - Amazon EC2 CreateSubnet API operations and CreateDefaultVpc API operations
- Data events
  - Example - S3 Bucket GetObject, DeleteObject, and PutObject API operations
- CloudTrail Insights events (unusual activity events)
  - Example - Amazon S3 deleteBucket API, Amazon EC2 AuthorizeSecurityGroupIngress API

AWS Elasticache



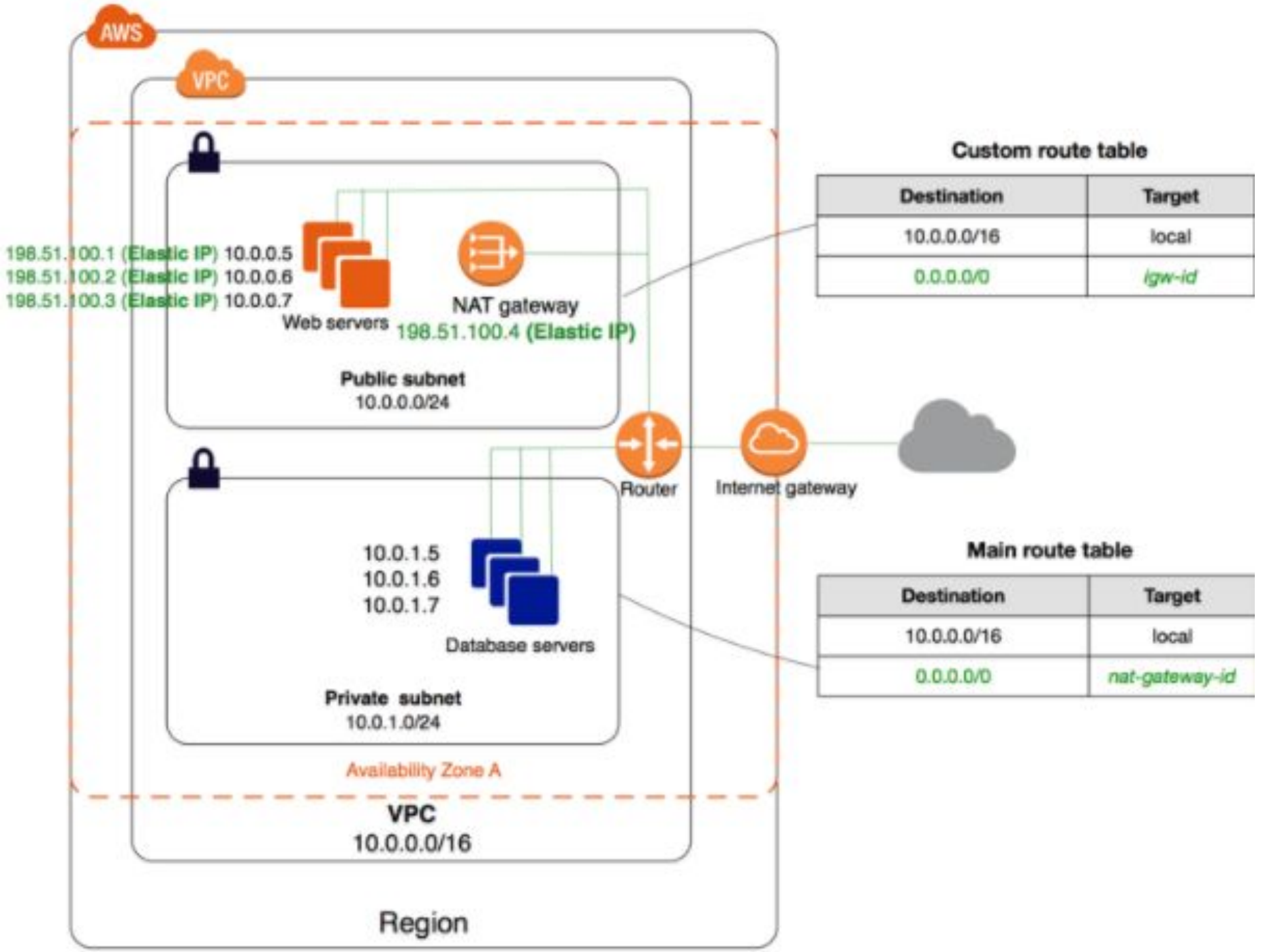
- Elasticache is an **In-Memory Cache service of AWS.**
- In-Memory Cache is a **temporary and fast** storage component. These components are used to reduce the workload of the main data storage device such as a database.
- AWS offers Redis and Memcached in-memory cache option which are popular in market.

AWS Elasticache

Before Elasticache

After Elasticache - First Query

After Elasticache - Second Query



Custom route table

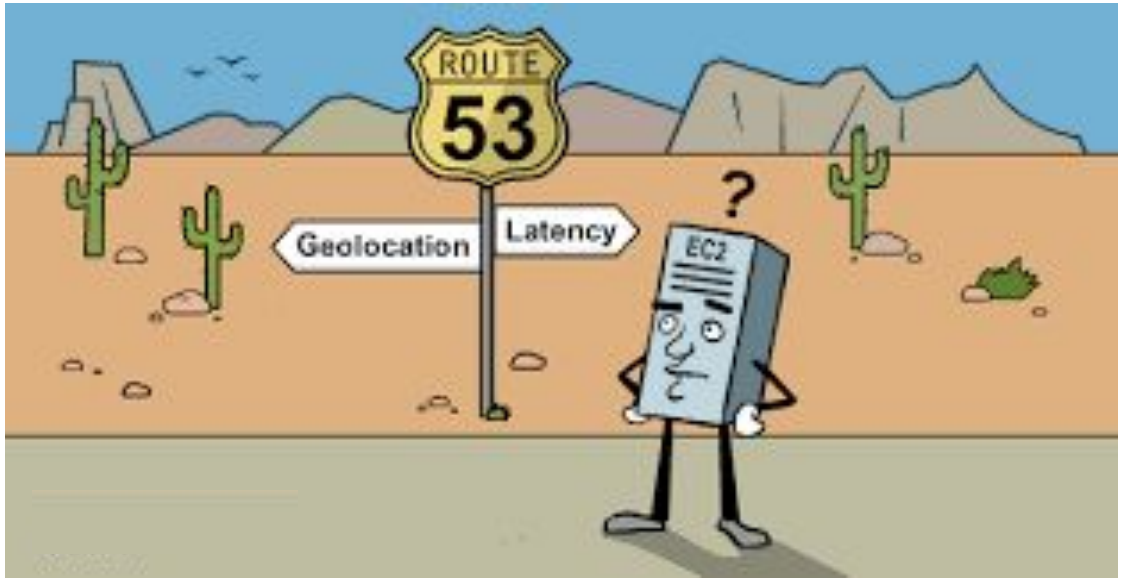
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

Routing Policies of Amazon Route 53

Routing Policies



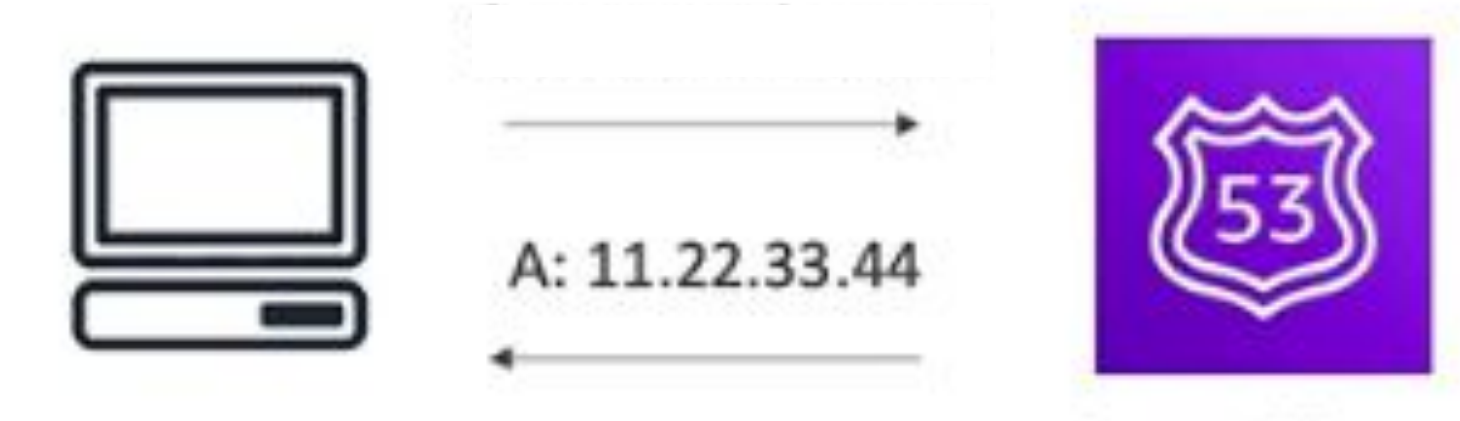
- Routing Policy is a component that is used for configuring the traffic **according to different types of scenarios**.

- How traffic is routed depends on which **topic the policy is based on.**

Routing Policies of Amazon Route 53

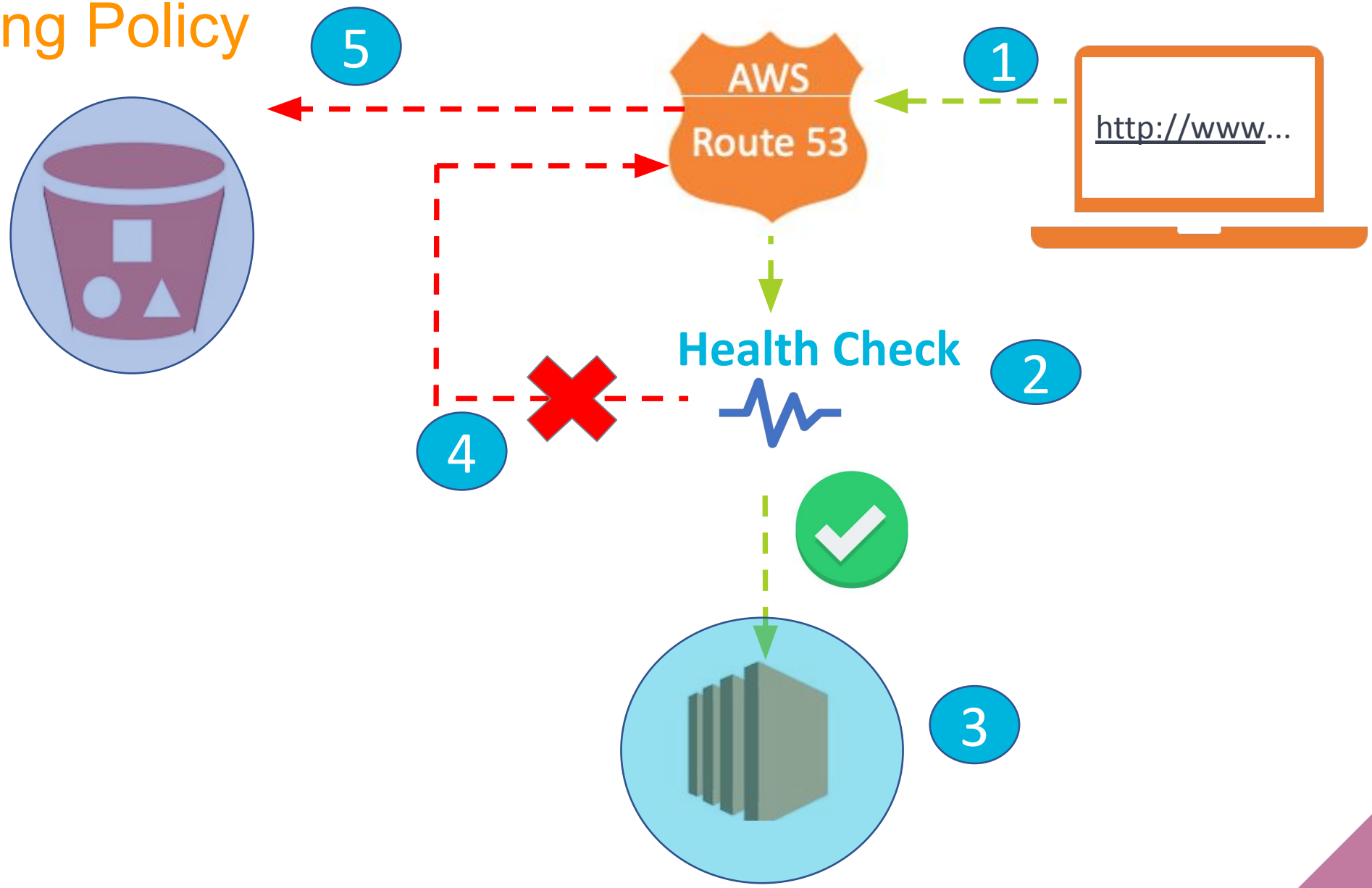
Simple Routing Policy

NO HEALTH CHECK



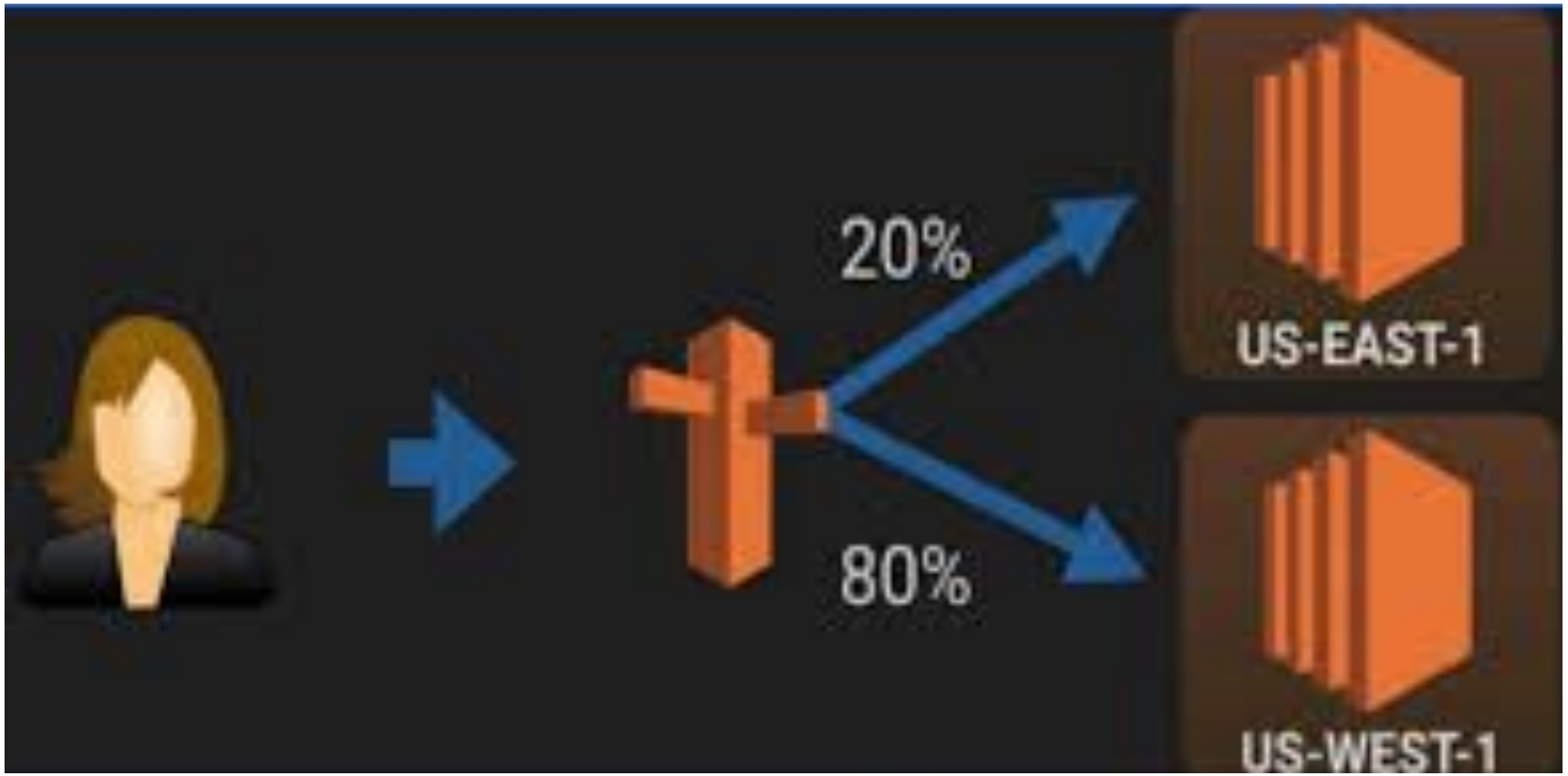
Routing Policies of Amazon Route 53

Failover Routing Policy



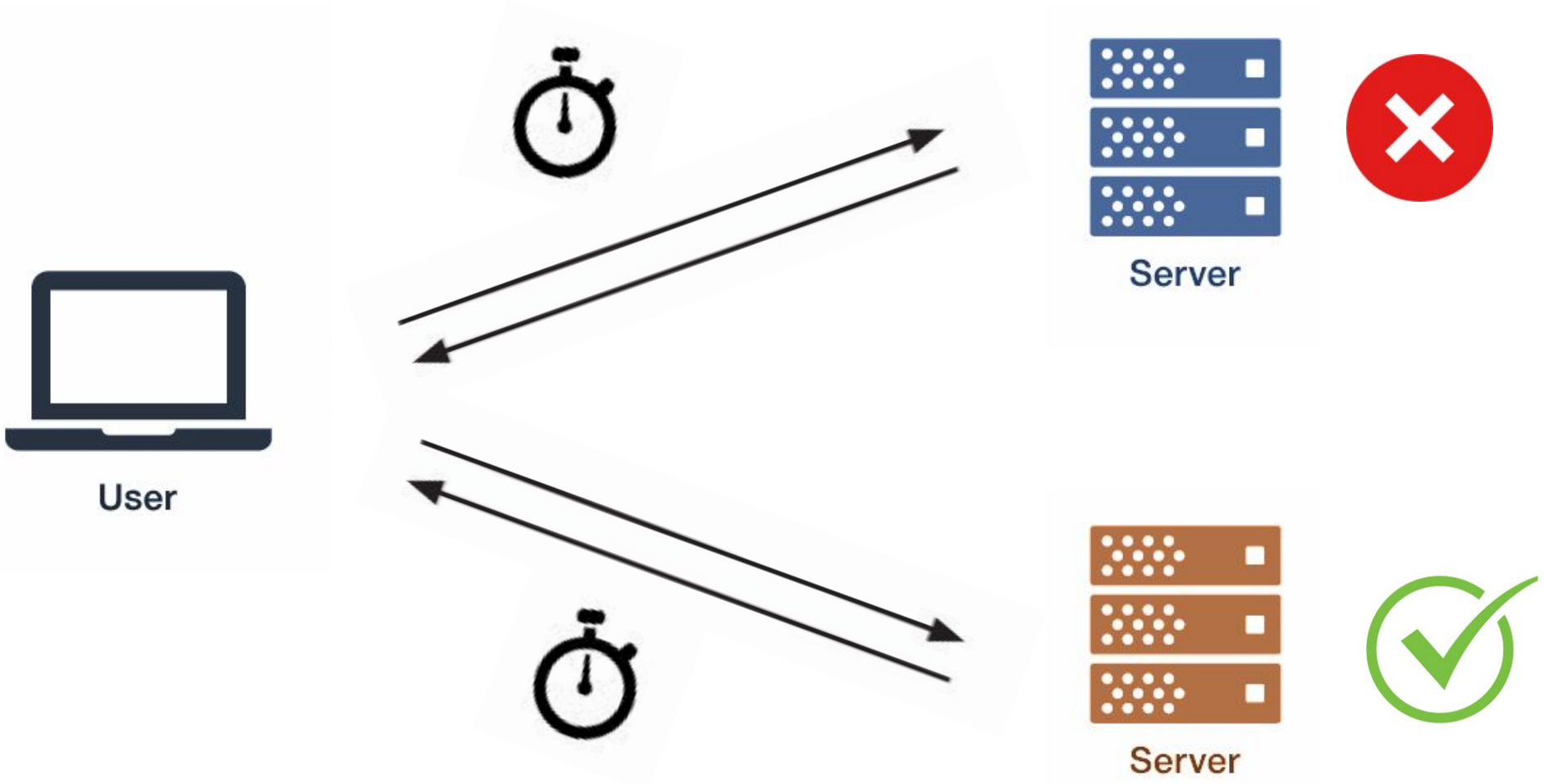
Routing Policies of Amazon Route 53

Weighted Routing Policy



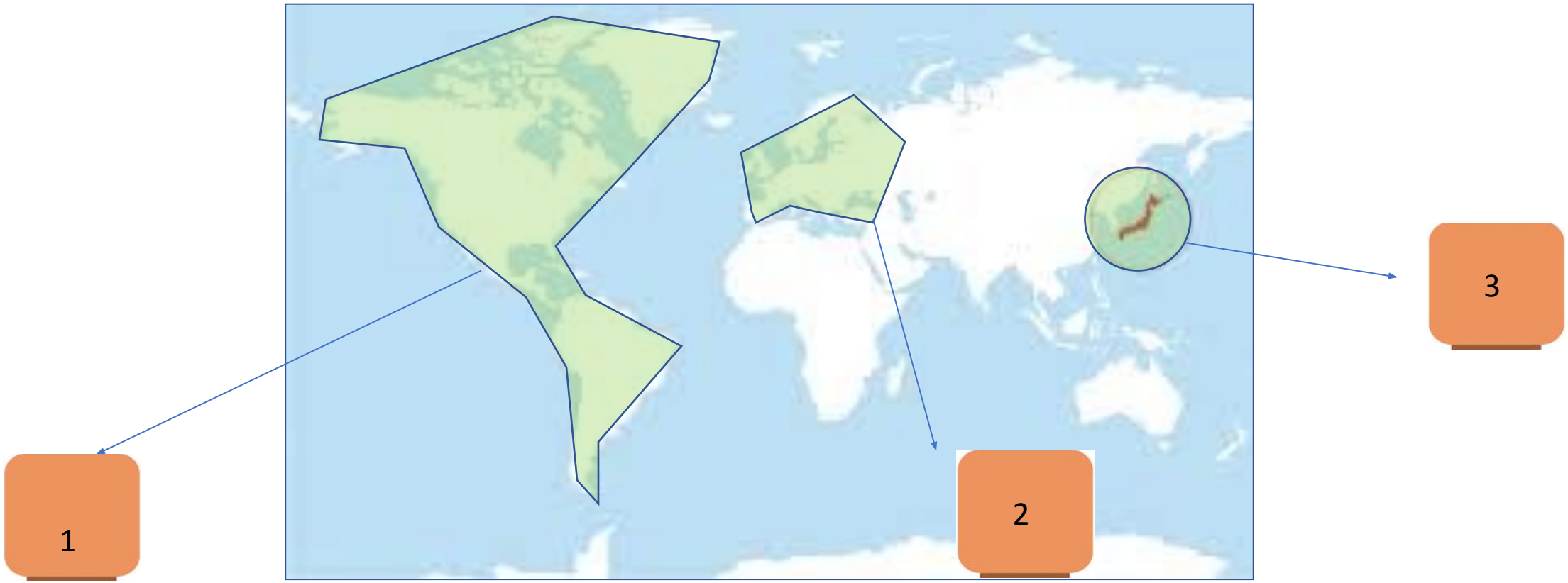
Routing Policies of Amazon Route 53

Latency Routing Policy



Routing Policies of Amazon Route 53

Geolocation Routing Policy

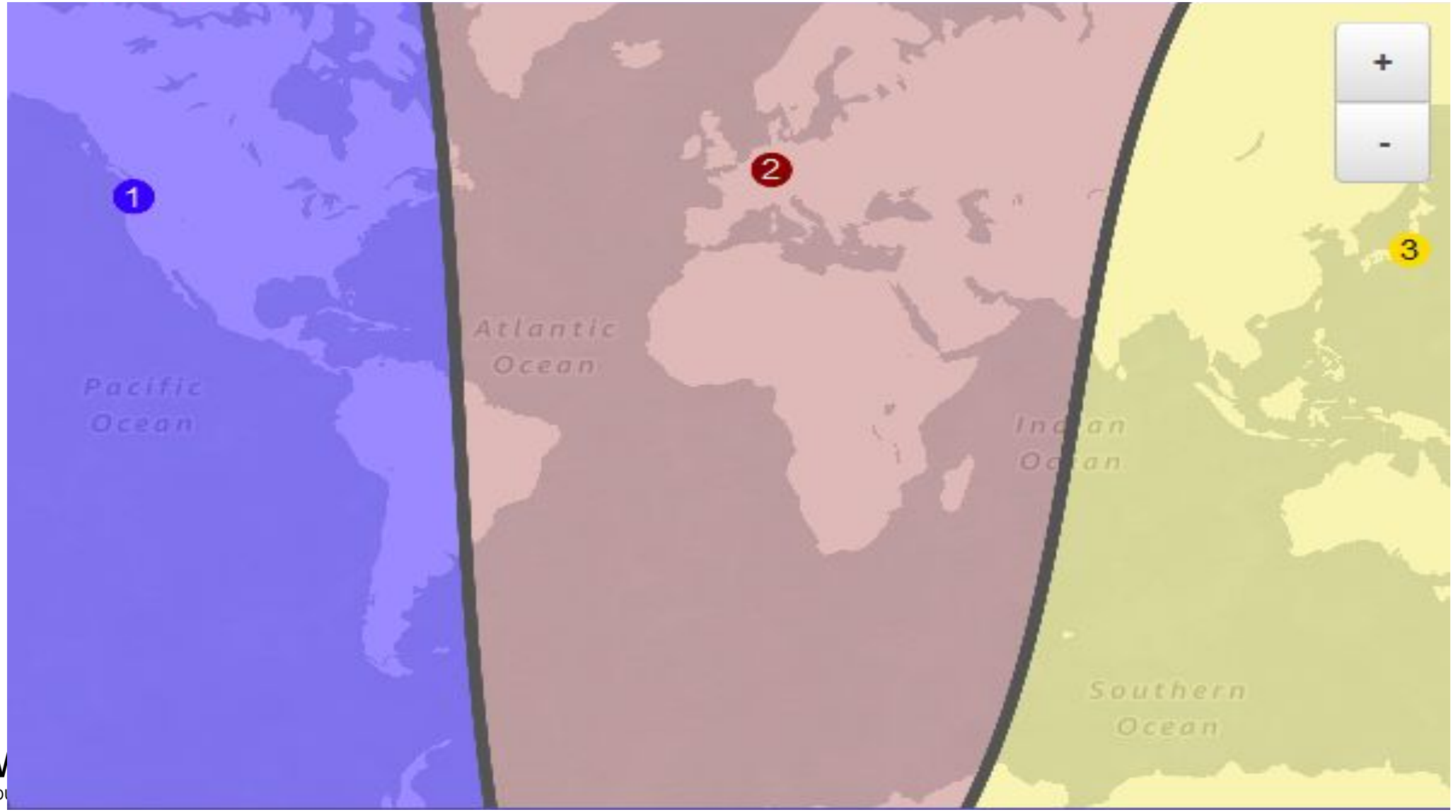


1- Country
2- Continent

It depends on where the user is

Routing Policies of Amazon Route 53

Geo Proximity Routing Policy



Routing Policies of Amazon Route 53

Multivalue Answer Routing Policy

	AZ-1	AZ-2	AZ-3
A	24	24	NO CHOICE
B	12	12	12
C	12	12	NO CHOICE
D	8	8	8

THANKS!

Any questions?

You can find me at:

- @armando
- armando@clarusway.com