

SECTION 1

Let's Get Started!

The CLF-C02 Exam





The CLF-C02 Exam

Level: Foundational

Length: 90 minutes

Format: 65 questions

Cost: \$100 USD

Delivery Method: Testing center or online

Scoring:

- Scaled score between 100 – 1000
- Minimum passing score of 700



The CLF-C02 Exam

Question format:

- **Multiple-choice:** Has one correct response and three incorrect responses
- **Multiple-response:** Has two or more correct responses out of five or more options



The CLF-C02 Exam

Domain 1: Cloud Concepts

- Task Statement 1.1: Define the benefits of the AWS Cloud
- Task Statement 1.2: Identify design principles of the AWS Cloud
- Task Statement 1.3: Understand the benefits of and strategies for migration to the AWS Cloud
- Task Statement 1.4: Understand concepts of cloud economics



The CLF-C02 Exam

Domain 2: Security and Compliance

- Task Statement 2.1: Understand the AWS shared responsibility model
- Task Statement 2.2: Understand AWS Cloud security, governance, and compliance concepts
- Task Statement 2.3: Identify AWS access management capabilities
- Task Statement 2.4: Identify components and resources for security



The CLF-C02 Exam

Domain 3: Cloud Technology and Services

- Task Statement 3.1: Define methods of deploying and operating in the AWS Cloud
- Task Statement 3.2: Define the AWS global infrastructure
- Task Statement 3.3: Identify AWS compute services
- Task Statement 3.4: Identify AWS database services
- Task Statement 3.5: Identify AWS network services
- Task Statement 3.6: Identify AWS storage services
- Task Statement 3.7: Identify AWS artificial intelligence and machine learning (AI/ML) services and analytics services
- Task Statement 3.8: Identify services from other in-scope AWS service categories



The CLF-C02 Exam

Domain 4: Billing, Pricing, and Support

- Task Statement 4.1: Compare AWS pricing models
- Task Statement 4.2: Understand resources for billing, budget, and cost management
- Task Statement 4.3: Identify AWS technical resources and AWS Support options

SECTION 2

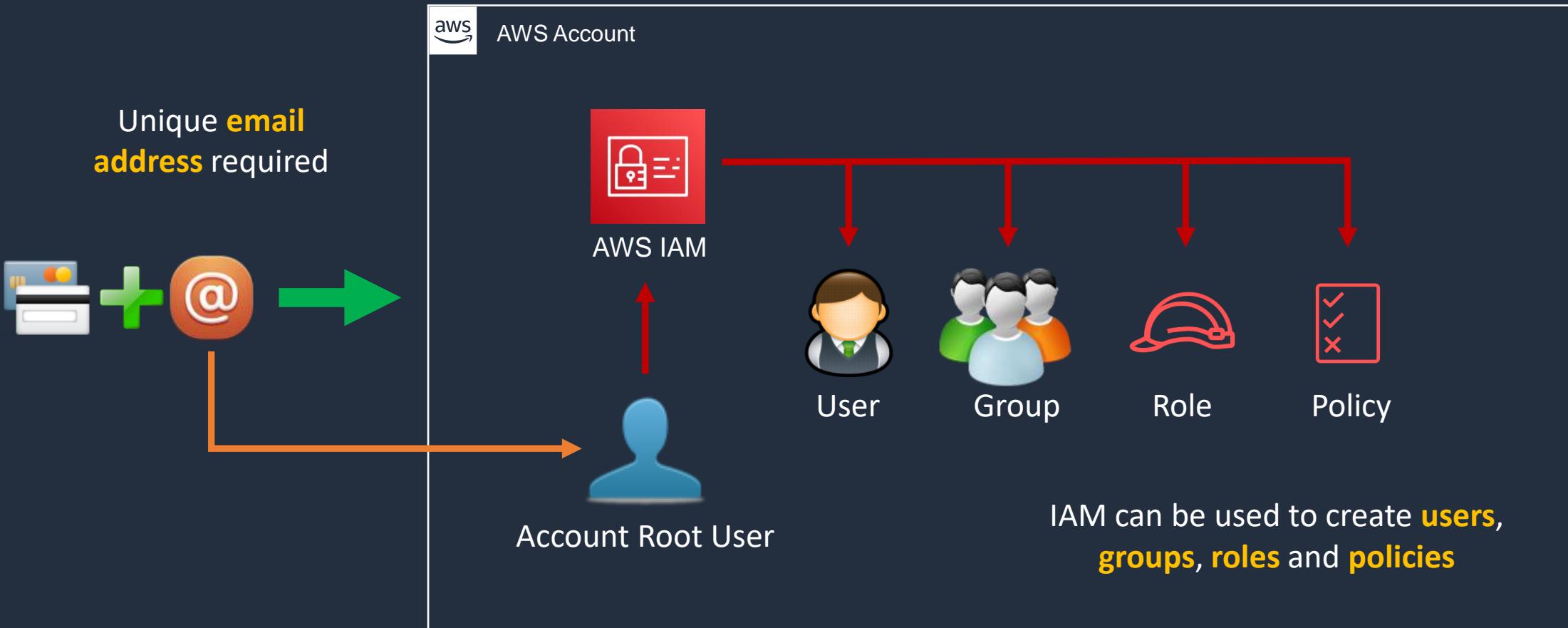
Create AWS Free Tier Account

AWS Account Overview



AWS Account Overview

It's an IAM best practice to create **individual users**
and to avoid using the **Root** account



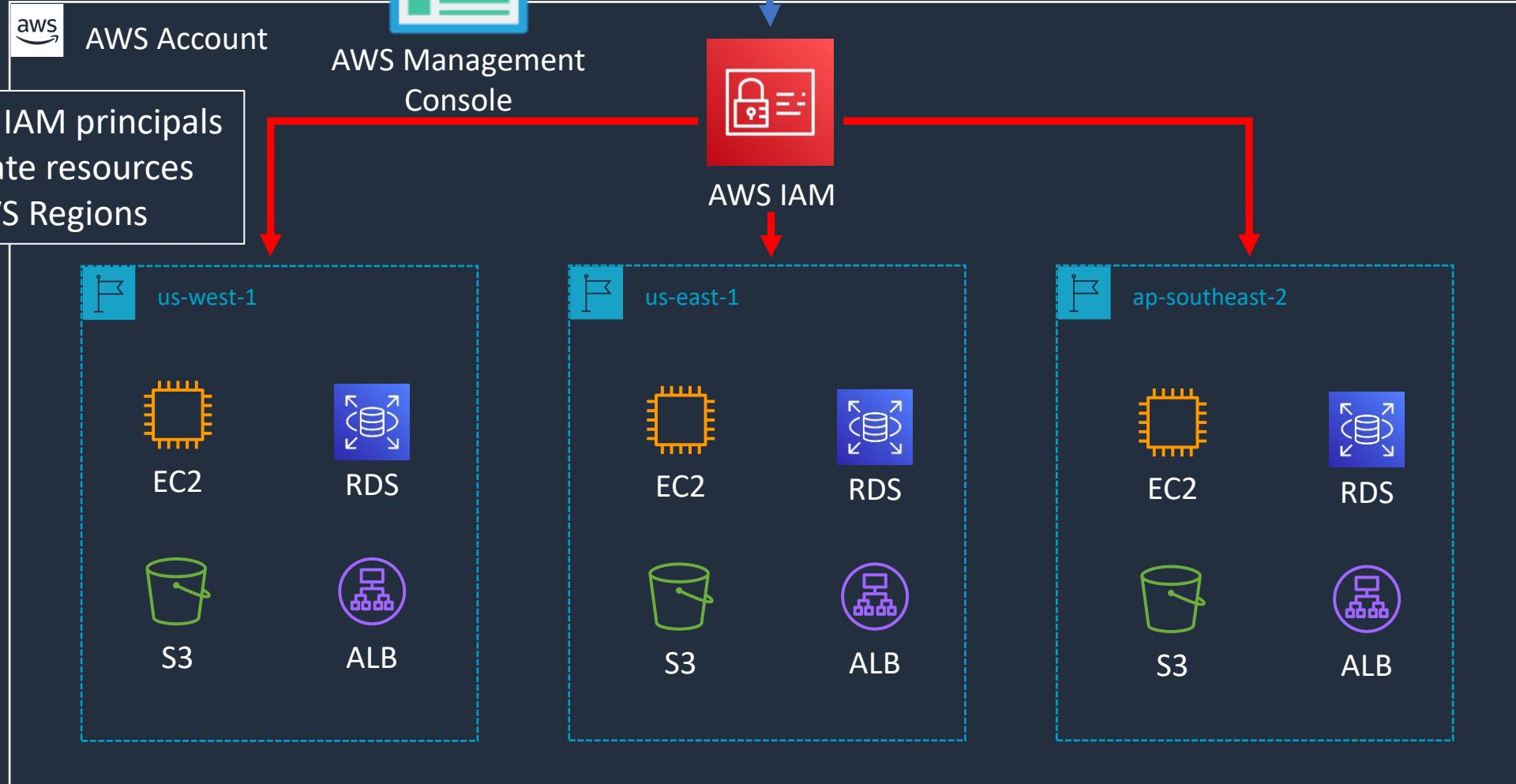
The Root user has **full control**
over the account

IAM can be used to create **users**,
groups, **roles** and **policies**



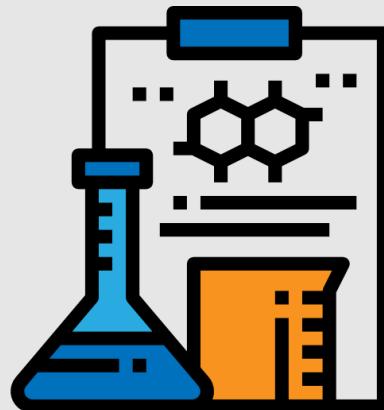
AWS Account Overview

Authentication: IAM principals authenticate to IAM using the console, API, or CLI



All AWS **identities** and **resources** are created within the AWS account

Create your AWS Free Tier Account



aws What you need...



Credit card for setting up the account and paying any bills



Unique email address for this account

john@gmail.com



Check if you can use a **dynamic alias** with an existing email address



john+ACCOUNT-ALIAS-1@gmail.com

john+ACCOUNT-ALIAS-2@gmail.com



AWS account name / alias



Phone to receive an **SMS** verification code

Configure Account and Create a Budget



Account Configuration

- Configure **Account Alias**
- Enable access to billing for **IAM users**
- Update **billing preferences**
- Create a **budget and alarm**

Install Tools and AWS CLI





Install Tools and Configure AWS CLI

- ✓ Download the code (*last lesson of this section*)
- ✓ Install Visual Studio Code
- ✓ Install the AWS CLI
- ✓ Access AWS CloudShell

SECTION 3

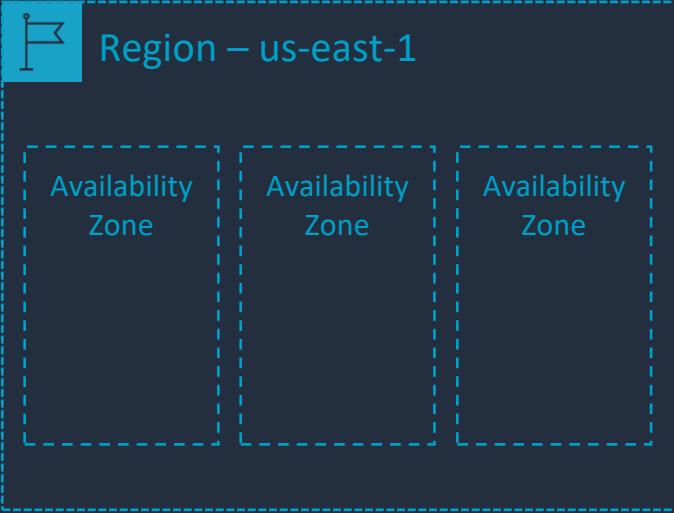
Amazon Web Services Fundamentals

The AWS Global Infrastructure





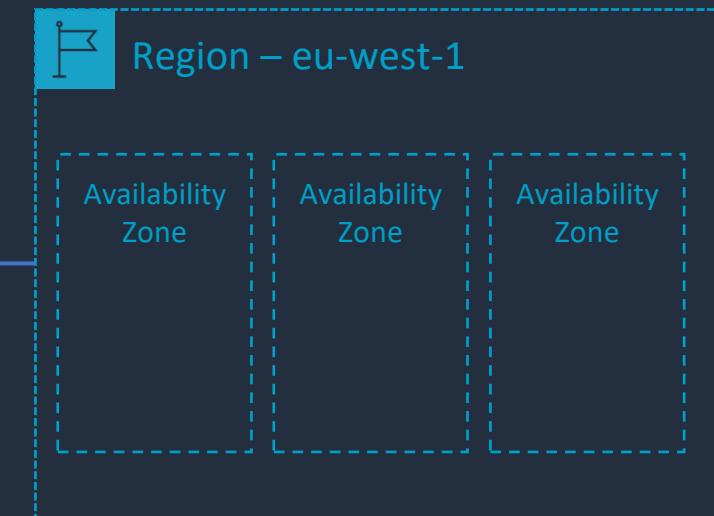
AWS Global Infrastructure



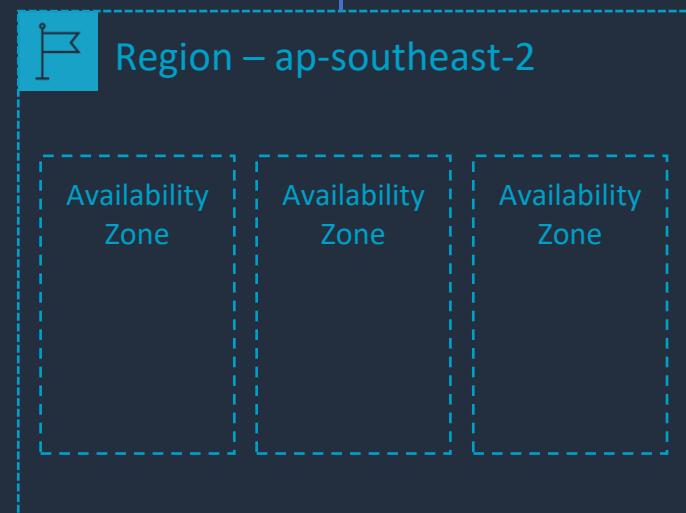
A **Region** is a separate physical location in the world



There are many **Regions** around the world



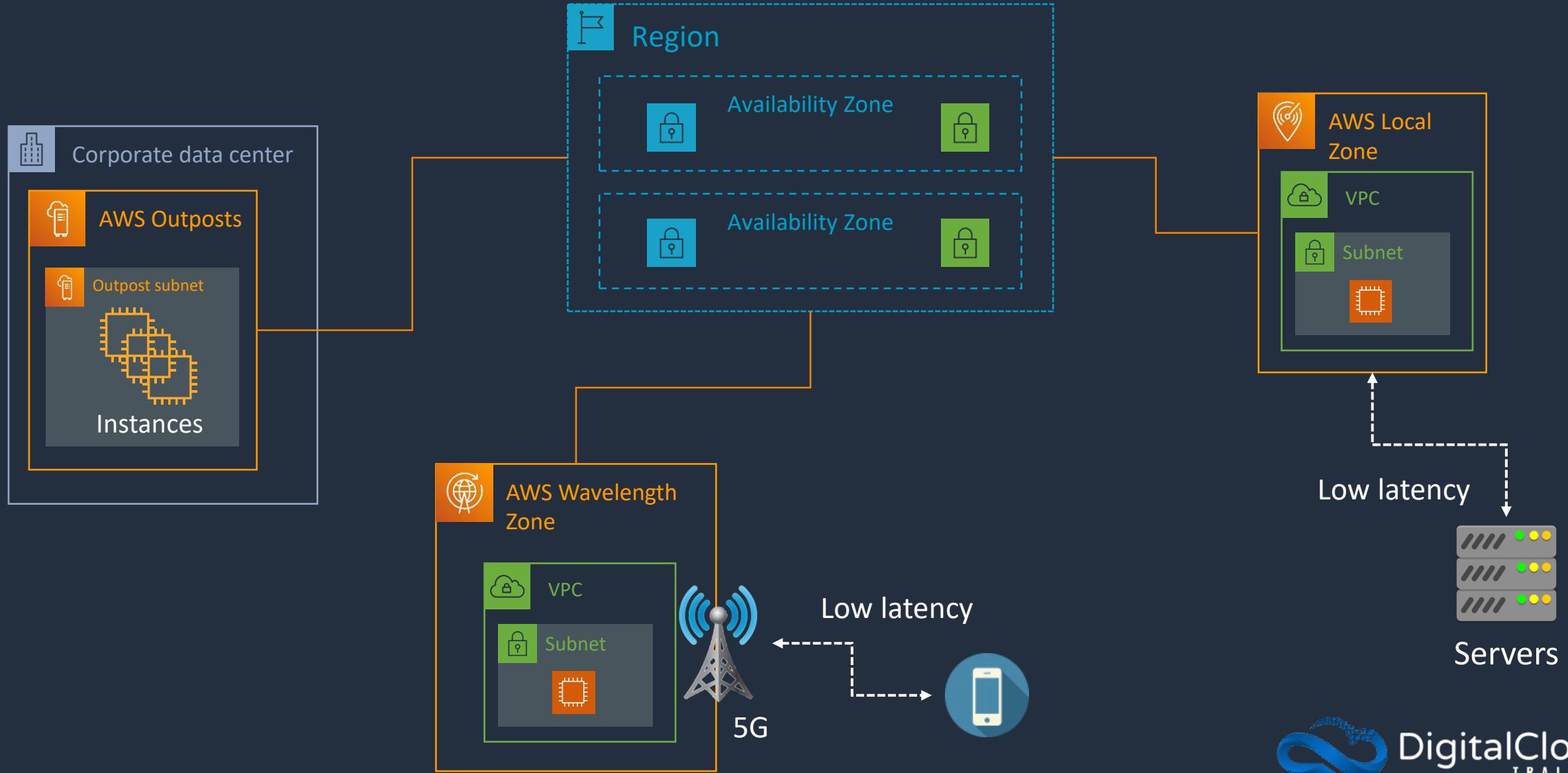
An Availability Zone is composed of **one** or **more** data centers



Each region consists of multiple **Availability Zones**

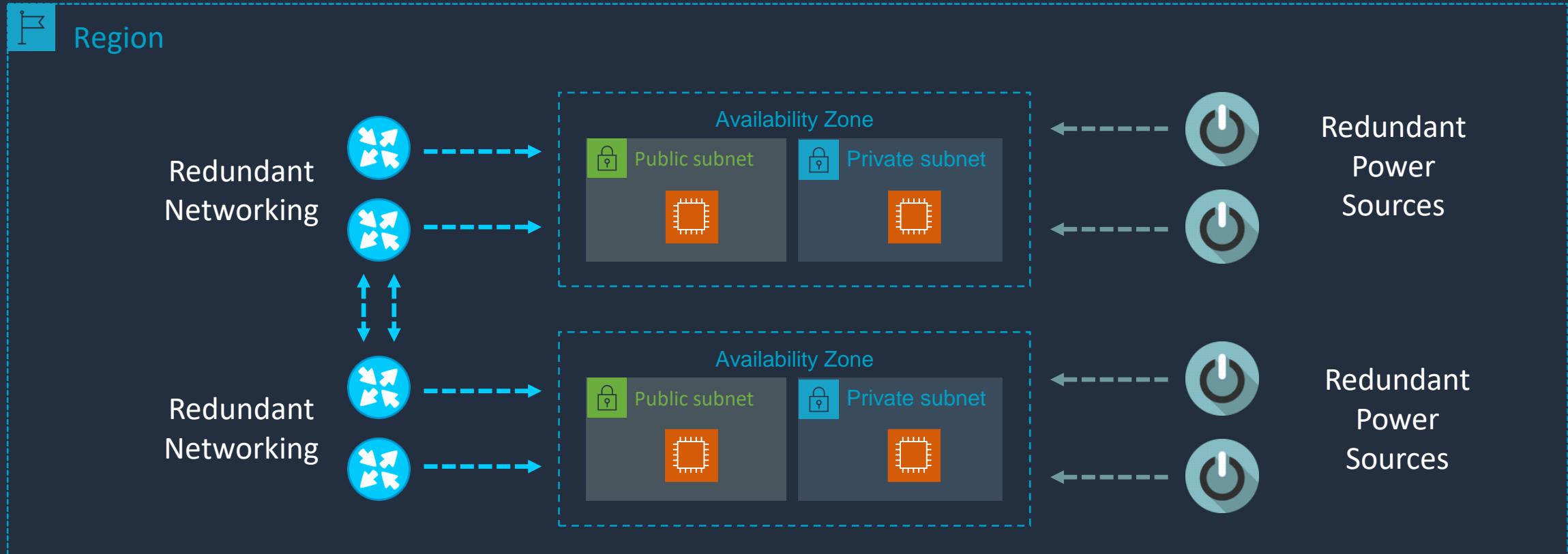


AWS Global Infrastructure



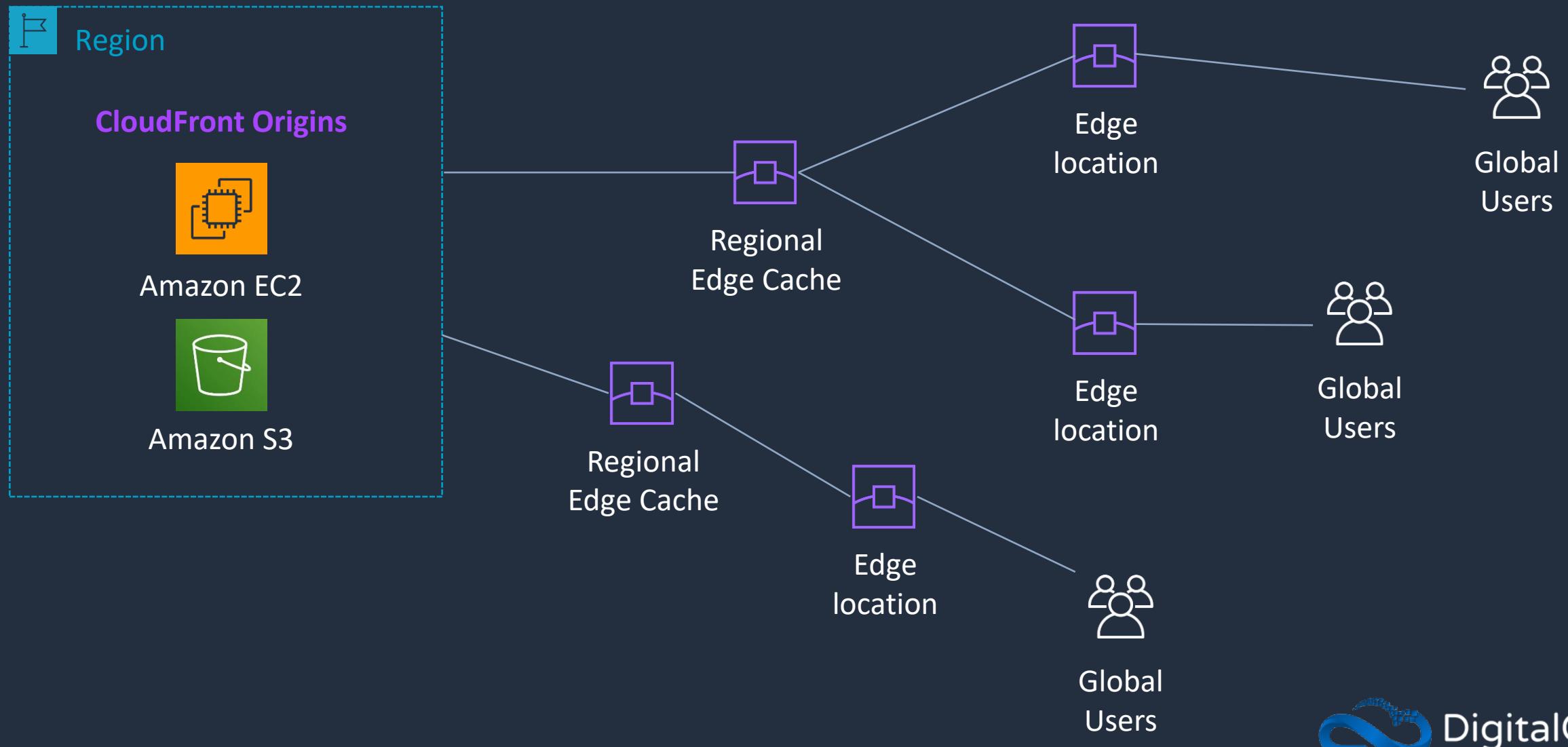


AWS Global Infrastructure



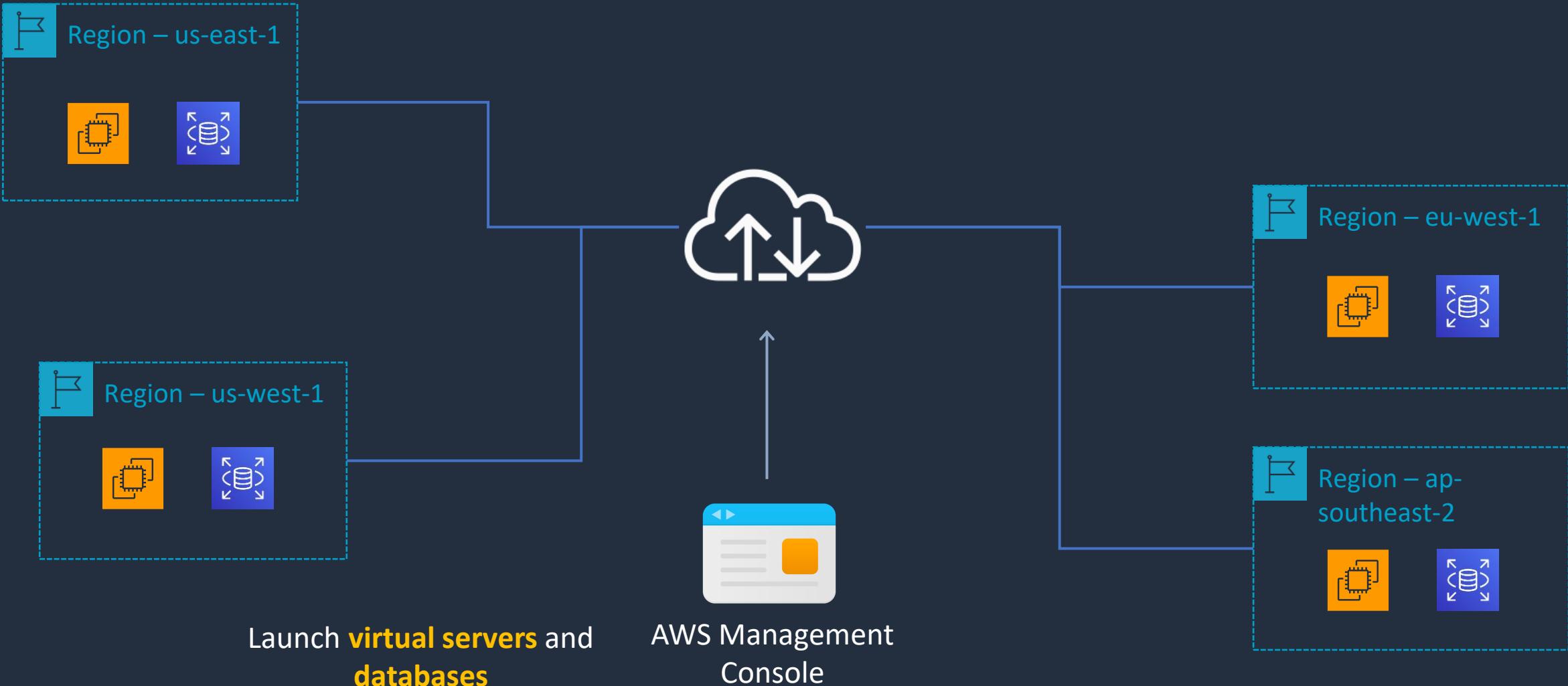


Amazon CloudFront





Deploying Services Globally

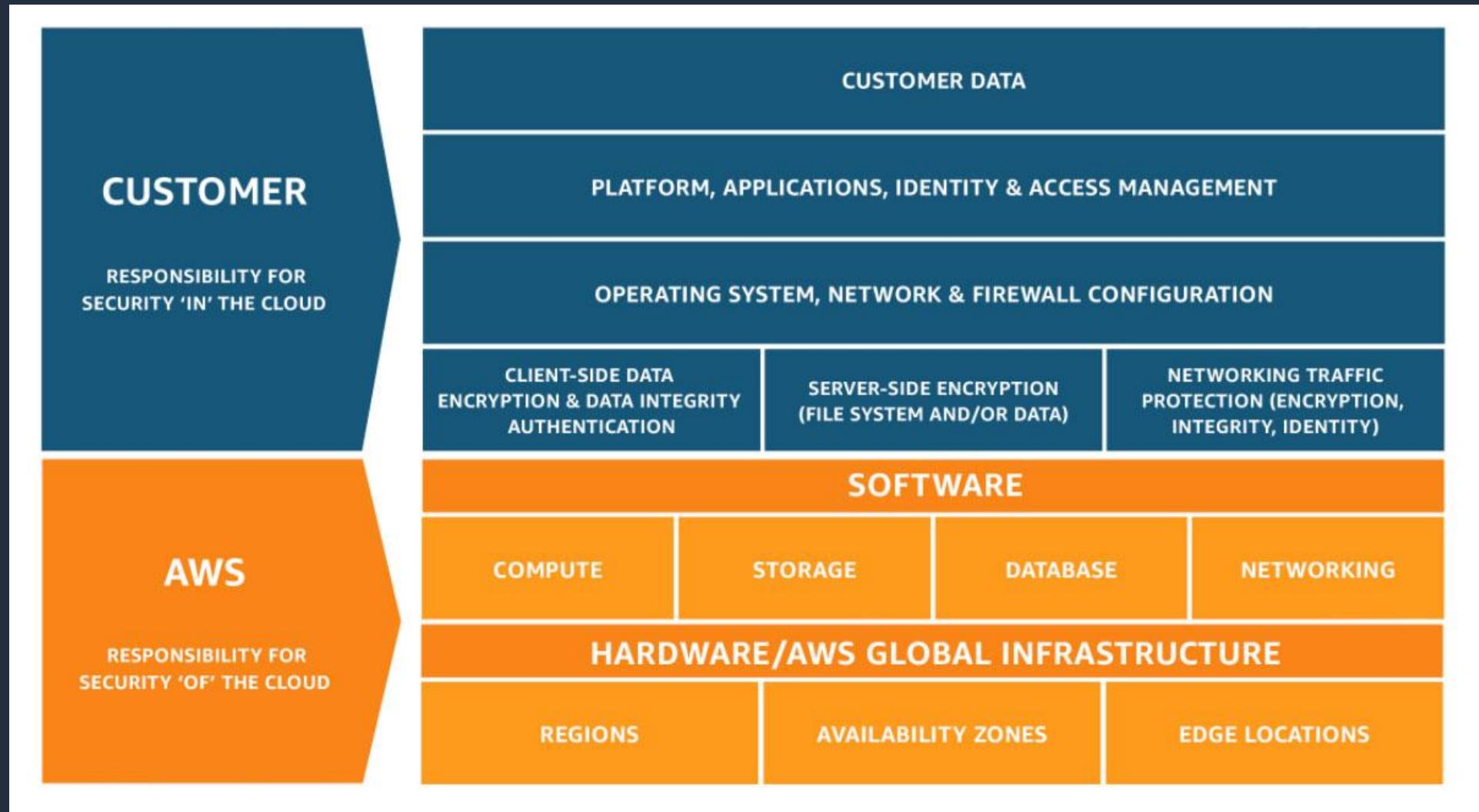


The AWS Shared Responsibility Model





The AWS Shared Responsibility Model





The AWS Shared Responsibility Model

CUSTOMER RESPONSIBILITY



Bucket with objects



Role



Multi-Factor Authentication



Security Group



Patch management



Staff training



Data encryption



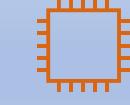
IAM User



Network ACL



SSL encryption



EC2 Instance



Auto Scaling



Elastic load balancer

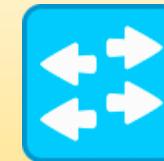
AWS RESPONSIBILITY



Data center security



Network router



Network switch



Storage



Database Server

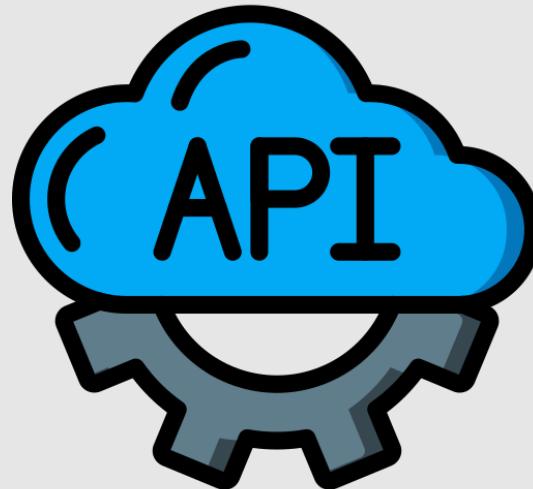


Server



Disk drive

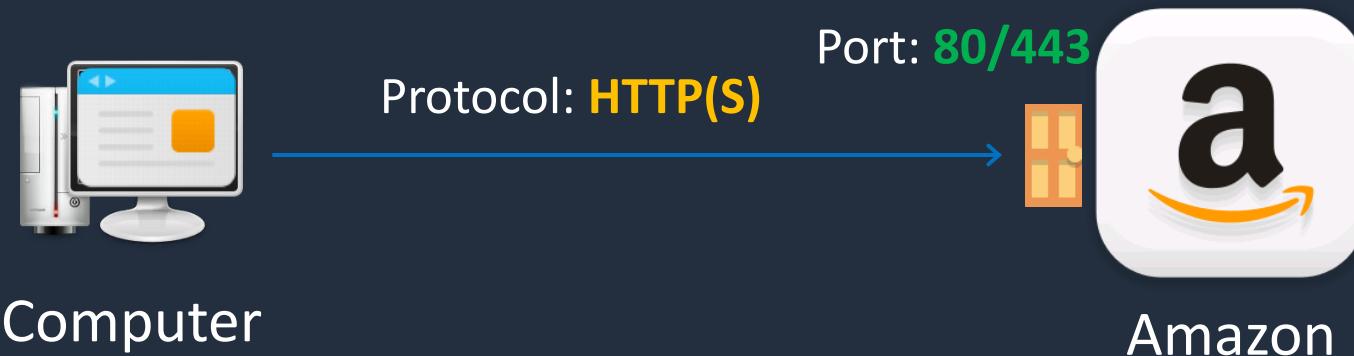
Application Programming Interfaces (APIs)





Ports and Protocols

A **protocol** is a language used for communication over a network



A **port** is like an open door behind which a specific service is waiting for connections



HTTP Methods

- **GET:** The GET method retrieves information
- **POST:** The POST method is used to submit data
- **PUT:** The PUT method replaces data
- **DELETE:** The DELETE method deletes data



HTTP Request

Browser issues an **HTTP GET** request to the web server



Computer



Amazon

The web server returns
the website **content**



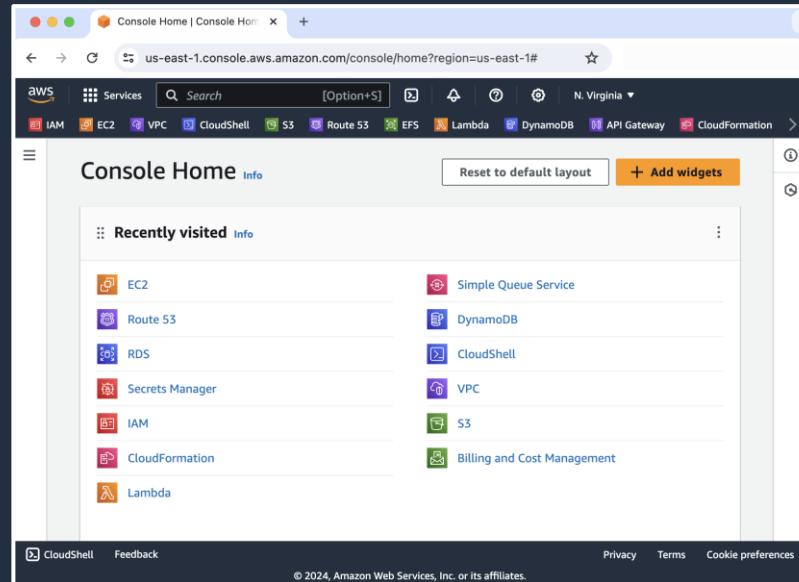
What are APIs?

- **Stands for** Application Programming Interface
- **APIs are** a set of rules and protocols that allow computer programs talk to each other
- **APIs assist with** sharing information and data between these programs
- **APIs leverage** standard protocols such as HTTP



AWS Example

Create a new **user account**



Browser sends **HTTP requests** to the **API**

AWS creates the new **user account**



The **API** defines specific **actions** you can request

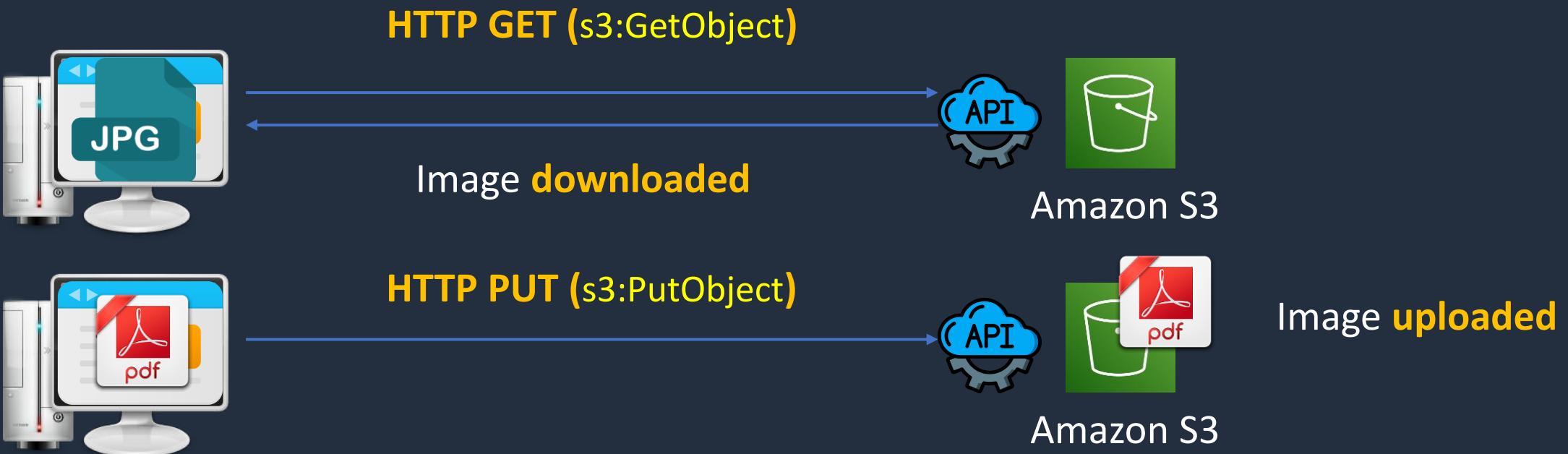
Every **action** you take on AWS is an **API call**



API Actions (AWS examples)

Amazon S3 (Simple Storage Service):

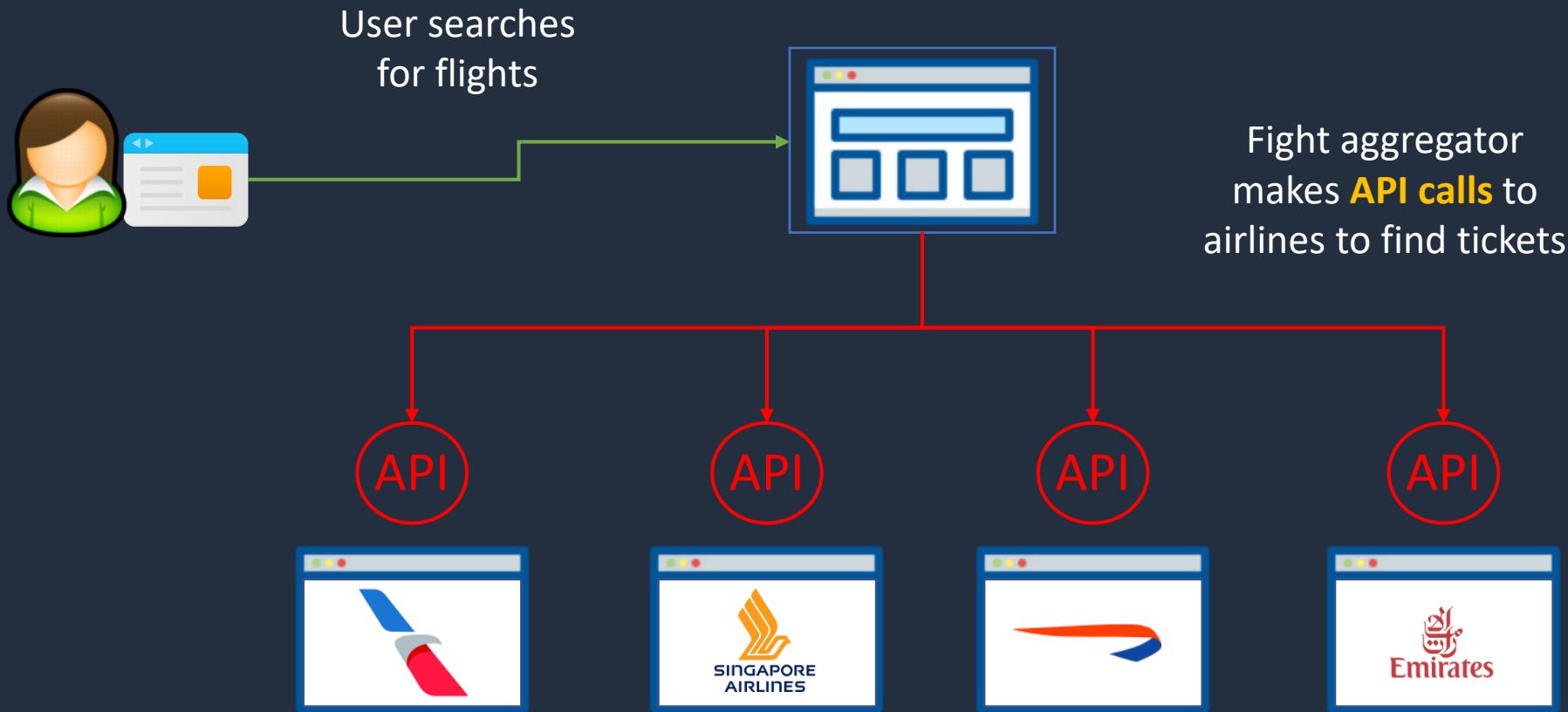
- **GetObject:** Retrieves objects from Amazon S3
- **PutObject:** Adds an object to a bucket





Flight Aggregator Example

Flight aggregator such as
Momondo or Skyscanner



AWS Pricing Fundamentals





AWS Pricing Fundamentals

Compute



Amount of resources such as CPU and RAM and **duration**

Storage



Quantity of **data stored / allocated**

Outbound Data Transfer



Quantity of data that is **transferred out** from all services



AWS Pricing Fundamentals

Pay-as-you-go

- Easily adapt to changing business needs
- Improved responsiveness to change
- Adapt based on needs, not forecasts



AWS Pricing Fundamentals

Save when you reserve

- Invest in reserved capacity (e.g. RDS and EC2)
- Save up to 75% compared to on-demand (pay-as-you-go)
- The more you pay upfront the greater the discount



AWS Pricing Fundamentals

Pay less by using more

- Pay less using volume-based discounts
- Tiered pricing means the more you use the lower the unit pricing

The 6 Advantages of Cloud Computing





The 6 Advantages of Cloud Computing

1. Trade capital expense for variable expense

CAPEX



Purchase servers



Tax deductible over depreciation lifetime

OPEX



Pay as you go



Tax deductible in same year



The 6 Advantages of Cloud Computing

2. Benefit from massive economies of scale





The 6 Advantages of Cloud Computing

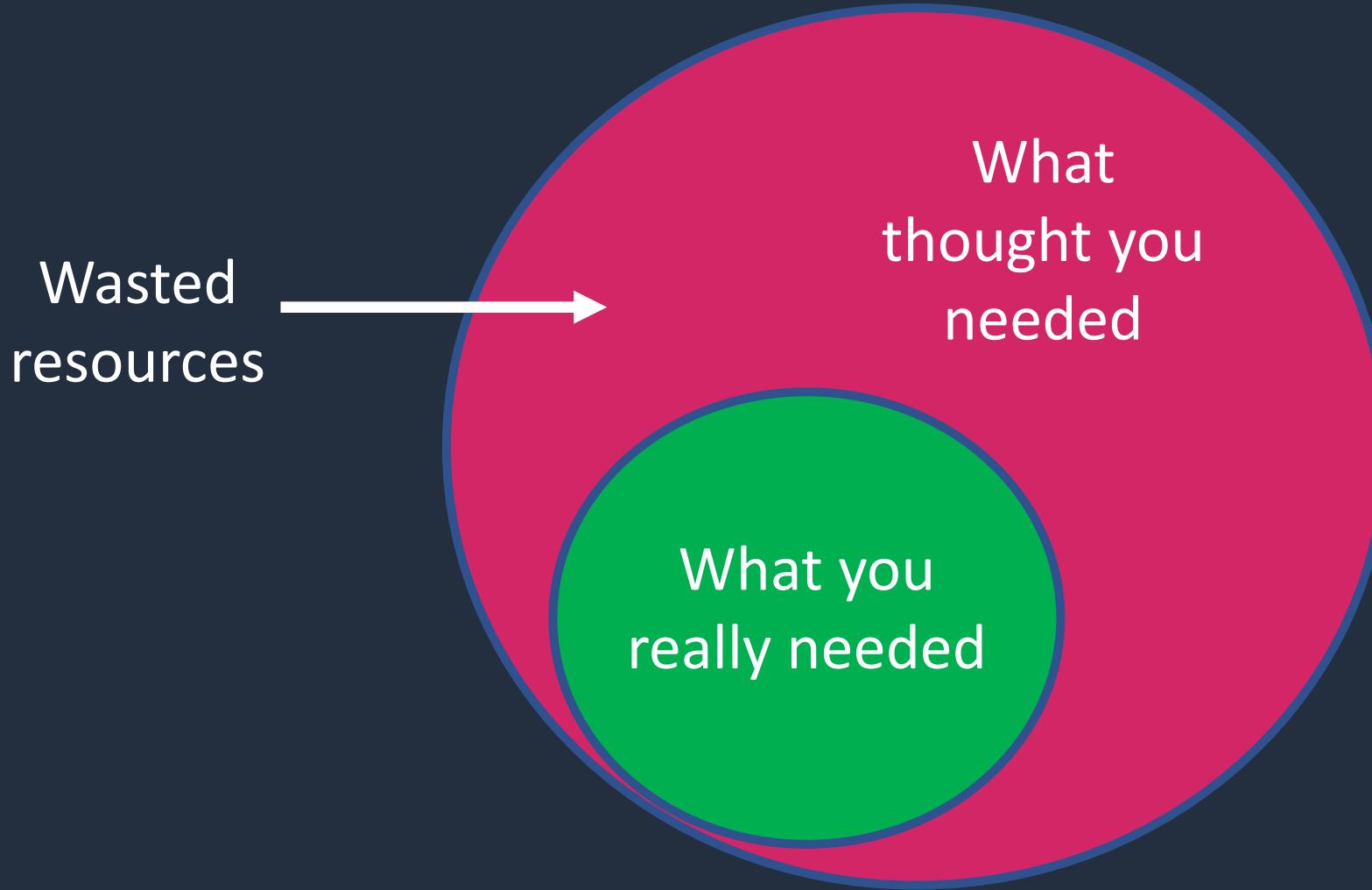
2. Benefit from massive economies of scale

- Aggregated usage across hundreds of thousands of customers = lower variable costs for customers



The 6 Advantages of Cloud Computing

3. Stop guessing capacity





The 6 Advantages of Cloud Computing

4. Increase speed and agility



Speed = deploy resources easily and quickly

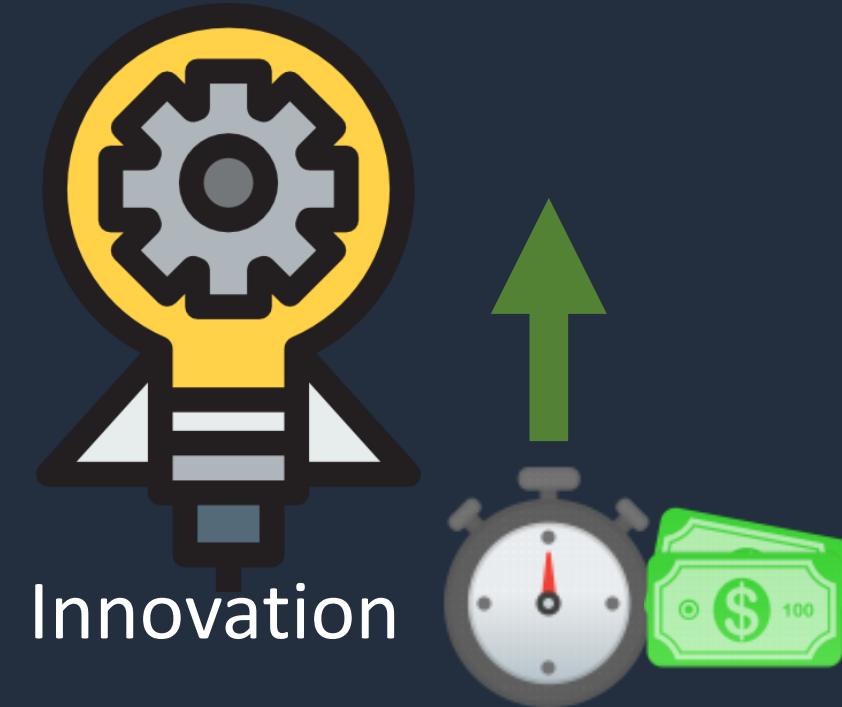


Agility = react to change ; speed to market



The 6 Advantages of Cloud Computing

5. Stop spending money running and maintaining data centers





The 6 Advantages of Cloud Computing

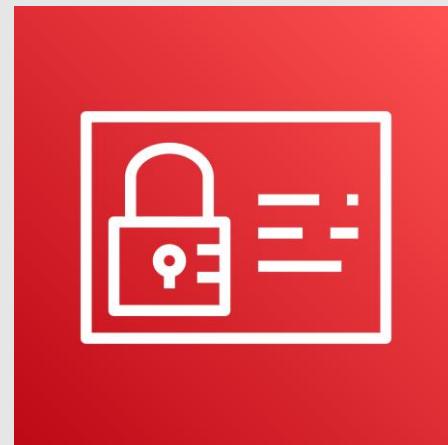
6. Go global in minutes



SECTION 4

AWS Authentication and Access Control

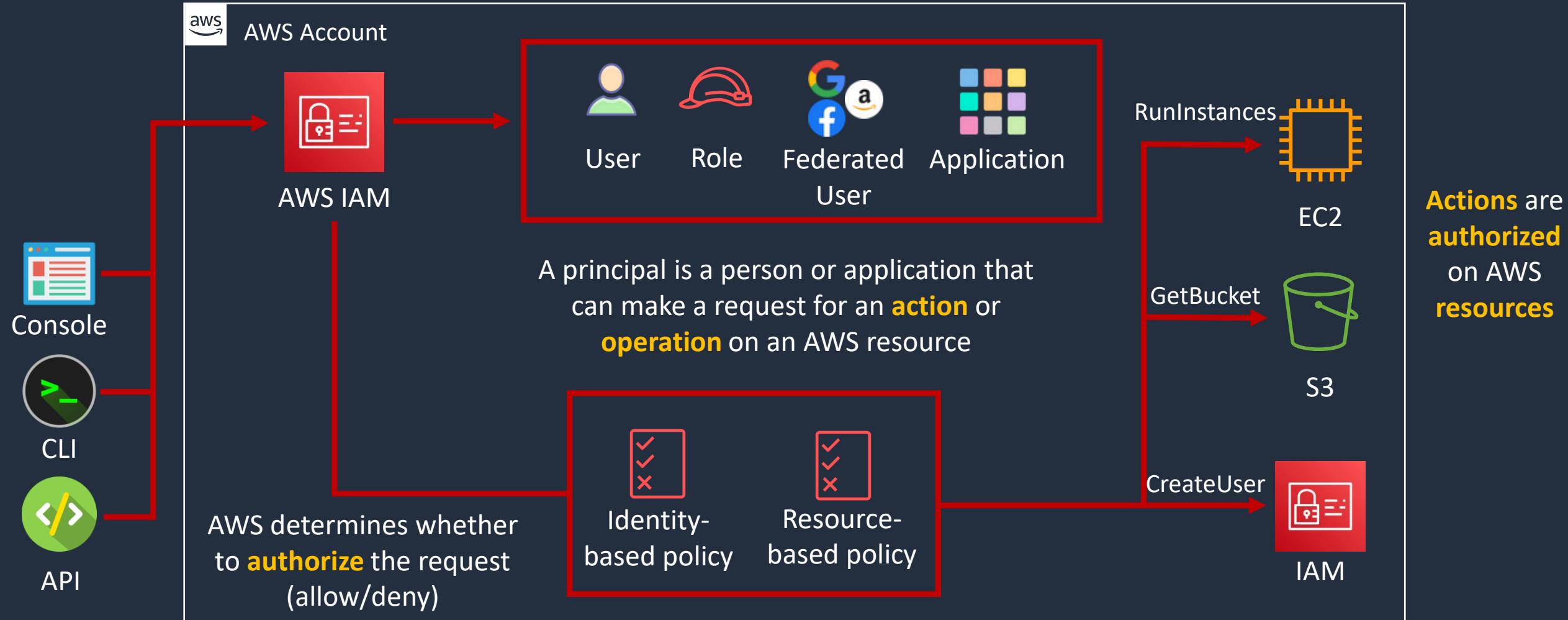
AWS Identity and Access Management (IAM)





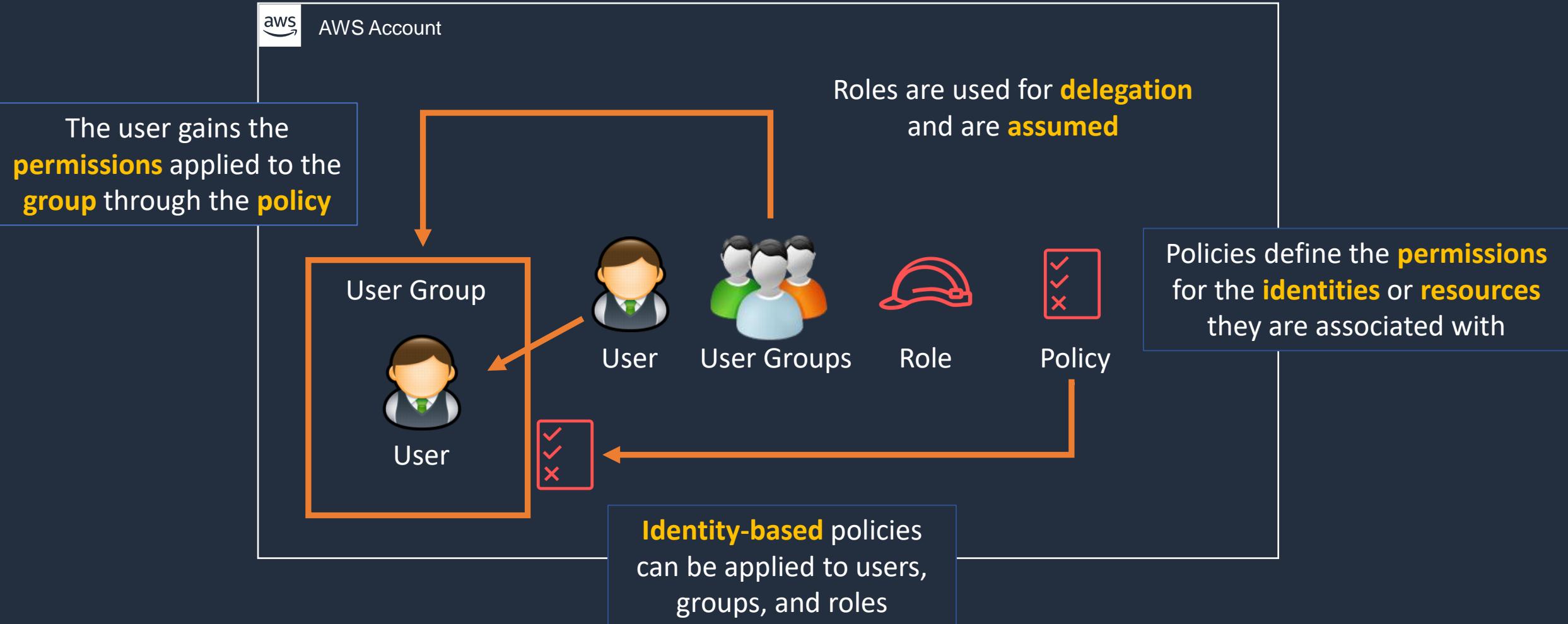
AWS Identity and Access Management (IAM)

IAM Principals must be **authenticated** to send requests (with a few exceptions)



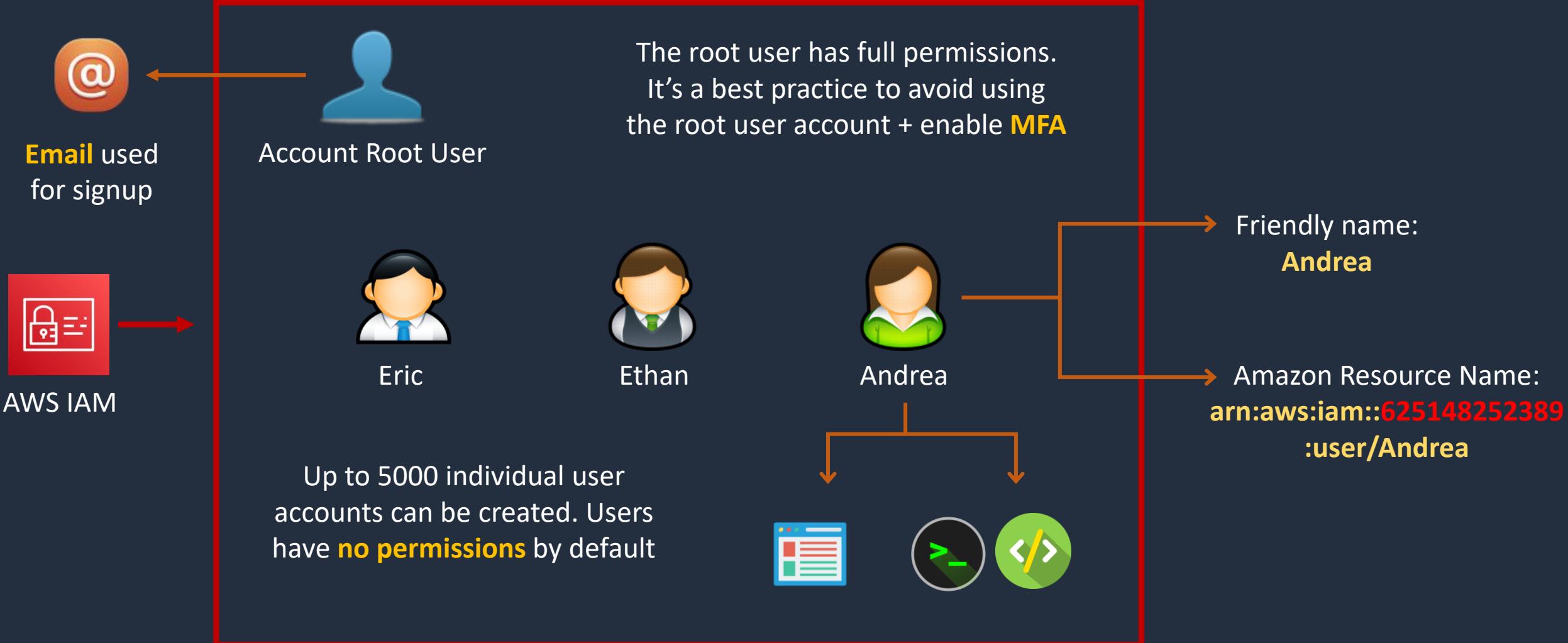


Users, User Groups, Roles and Policies



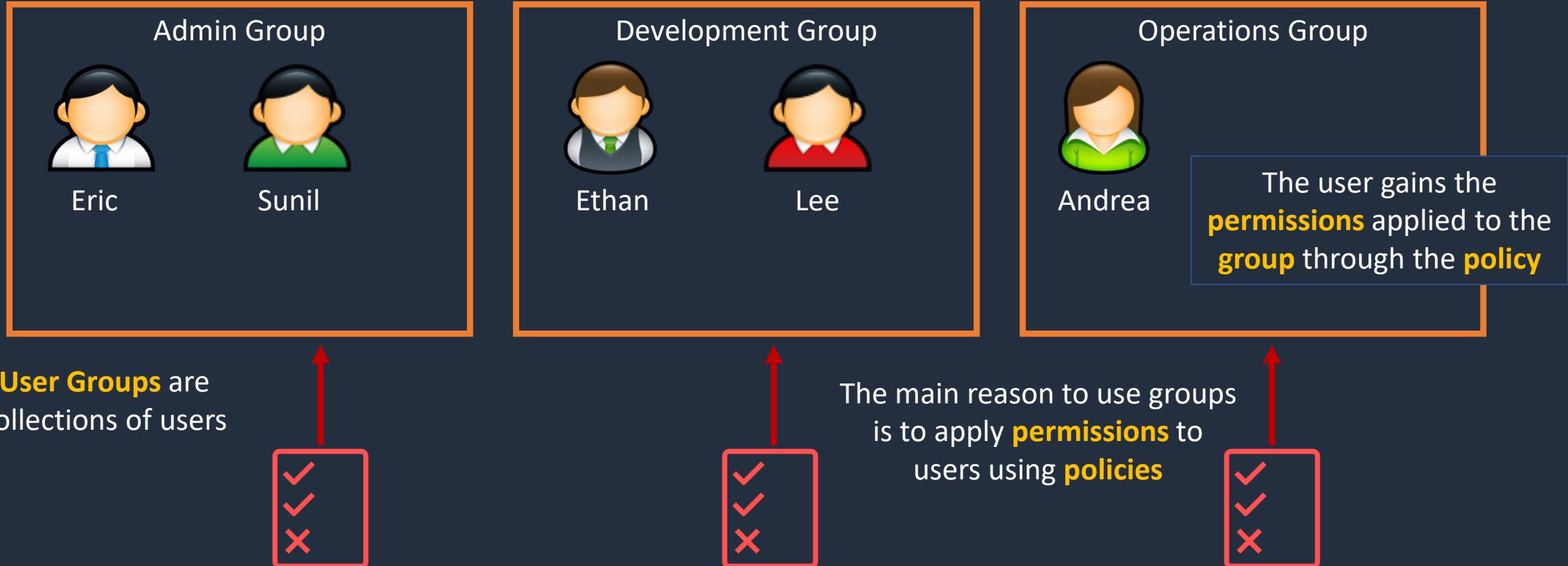


IAM Users



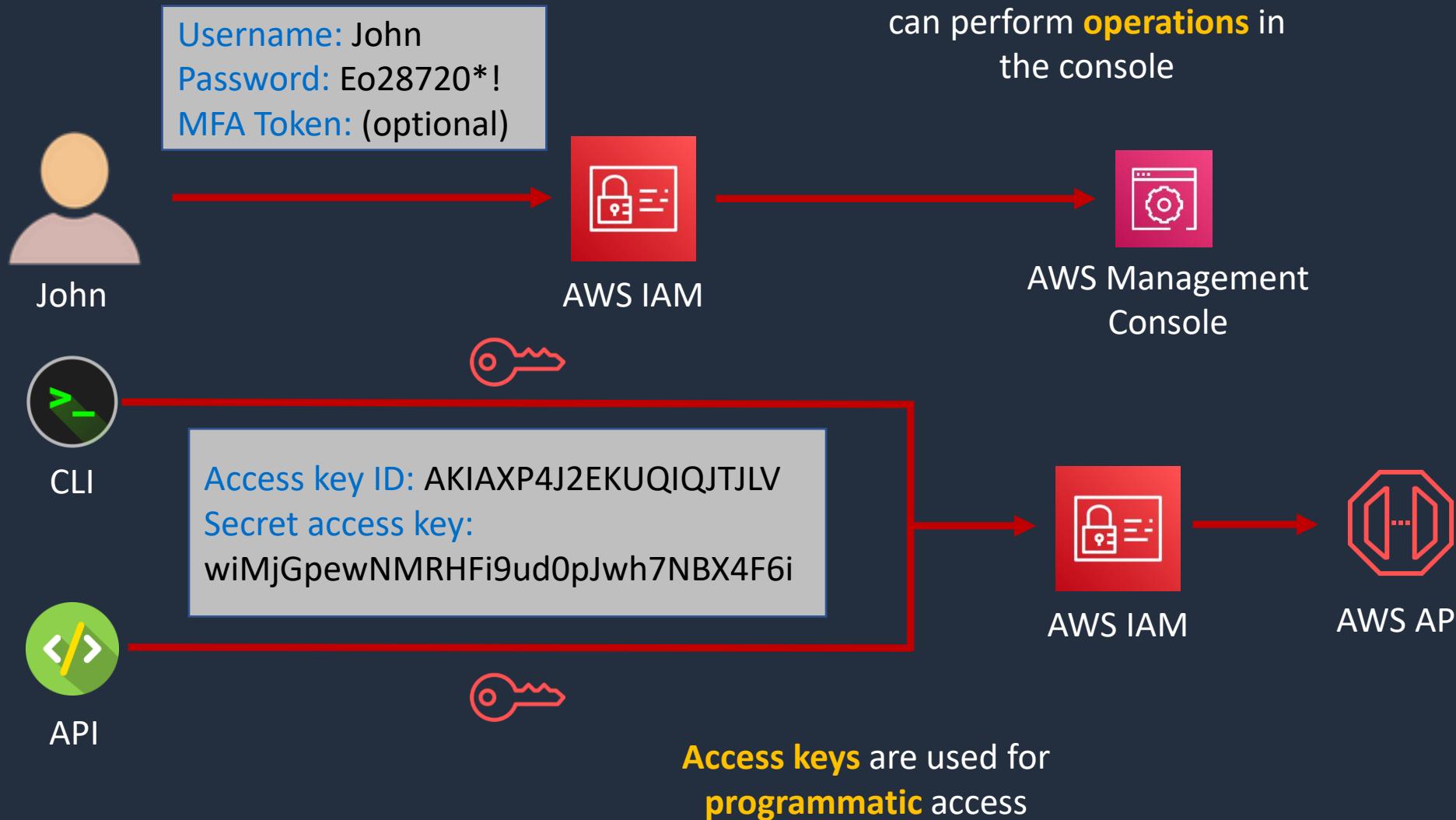


IAM User Groups





IAM Authentication Methods





Root User vs IAM User

User	Login Details	Permissions
 Root User	 Email address	 Full - Unrestricted
 IAM User	Friendly name: John + AWS account ID or Alias	 IAM Permissions Policy

Creating IAM Users and Groups

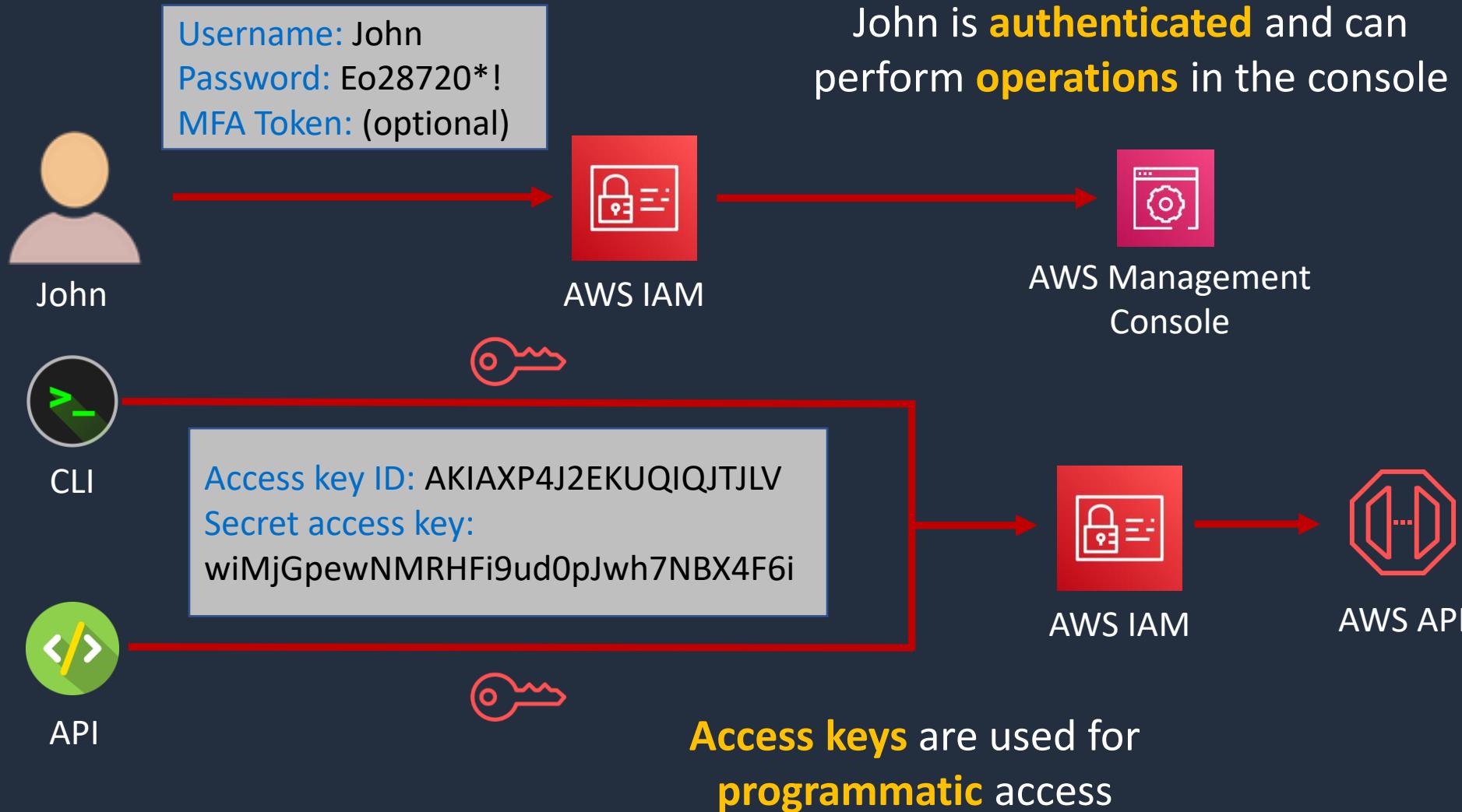


IAM Authentication and MFA





IAM Authentication Methods





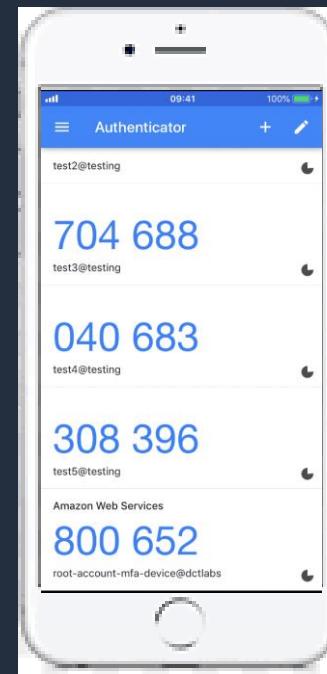
Multi-Factor Authentication

Something you **know**:

EJPx!*21p9%

Password

Something you **have**:



Something you **are**:





Multi-Factor Authentication

Something you **know**:



IAM User

EJPx!*21p9%

Password

Something you **have**:



Virtual MFA

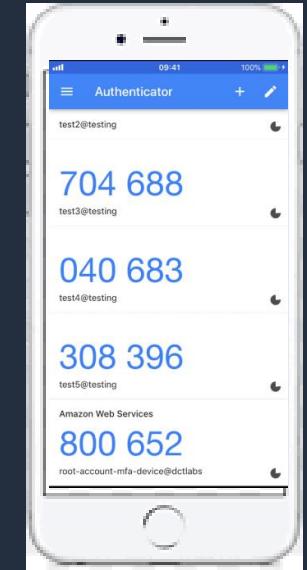
e.g. Google Authenticator on
your smart phone



Hardware device



Security keys and **time-based
one-time password (TOTP)**
tokens



Setup Multi-Factor Authentication (MFA)



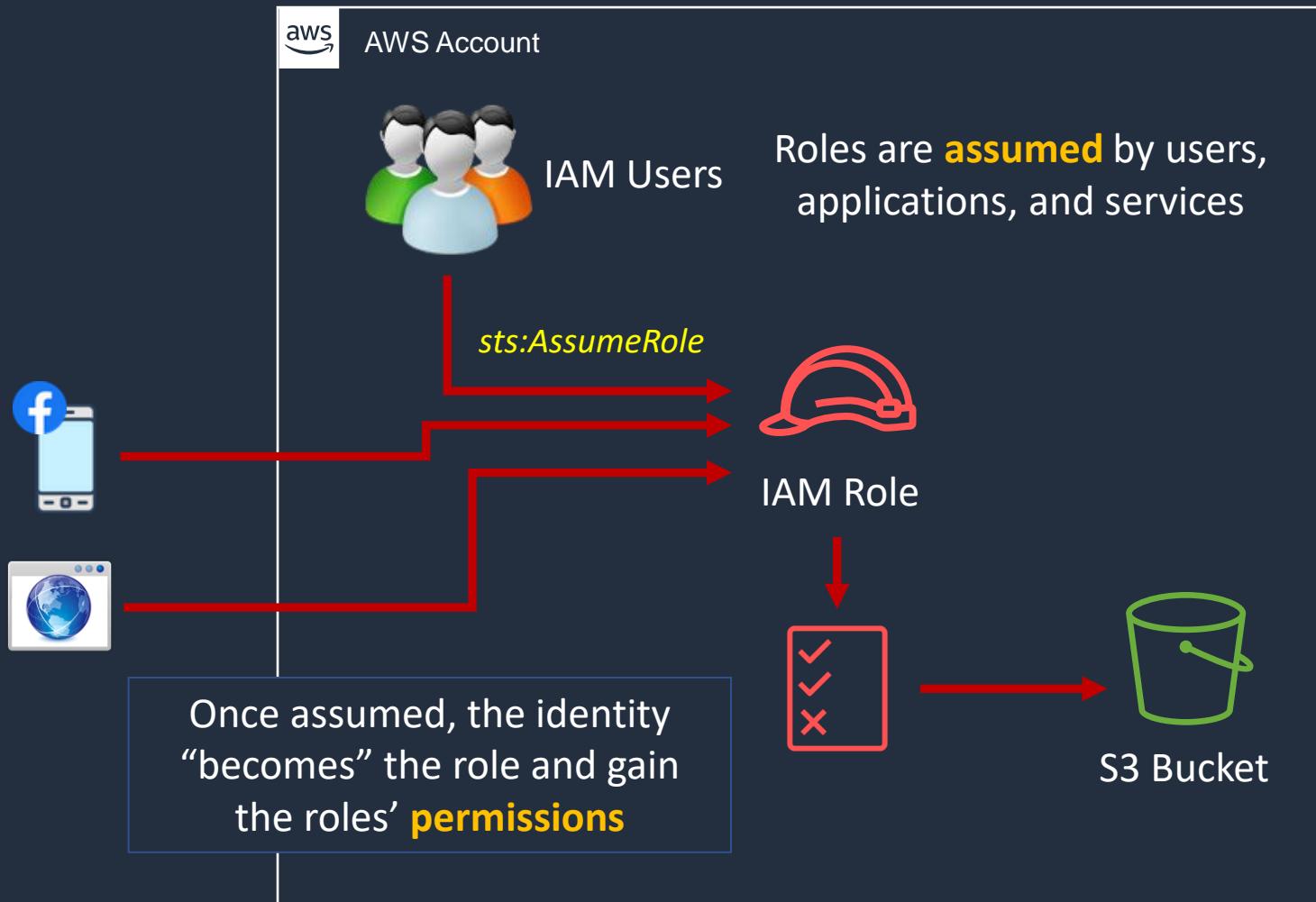
IAM Roles and Policies





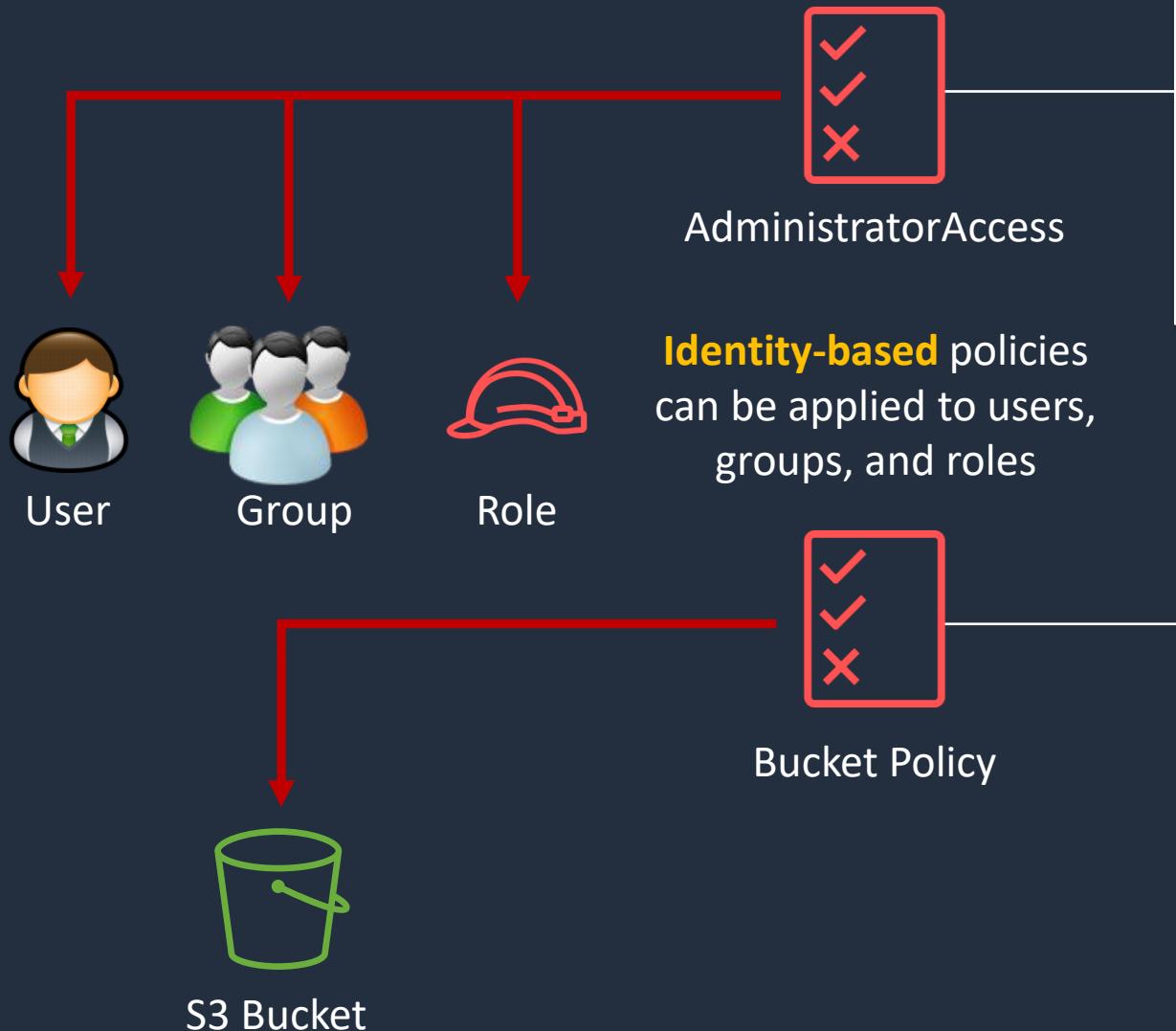
IAM Roles

An **IAM role** is an IAM **identity** that has specific **permissions**





IAM Policies



Policies are **documents** that define **permissions** and are written in **JSON**

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "*",  
      "Resource": "*"  
    }  
  ]  
}
```

All permissions are **implicitly denied** by default

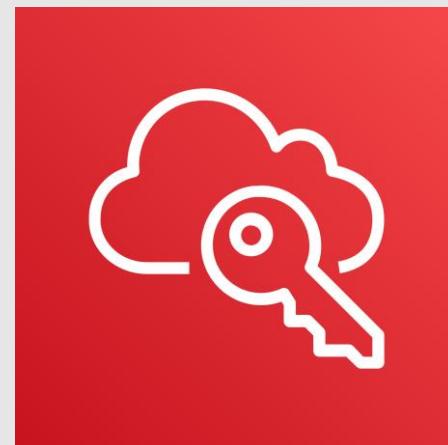
```
{  
  "Version": "2012-10-17",  
  "Id": "Policy1561964929358",  
  "Statement": [  
    {  
      "Sid": "Stmt1561964454052",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::515148227241:user/Paul"  
      },  
      "Action": "s3:*",  
      "Resource": "arn:aws:s3:::dctcompany",  
      "Condition": {  
        "StringLike": {  
          "s3:prefix": "Confidential/*"  
        }  
      }  
    }  
  ]  
}
```

Resource-based policies apply to **resources** such as S3 buckets

Switching IAM Roles



IAM Identity Center

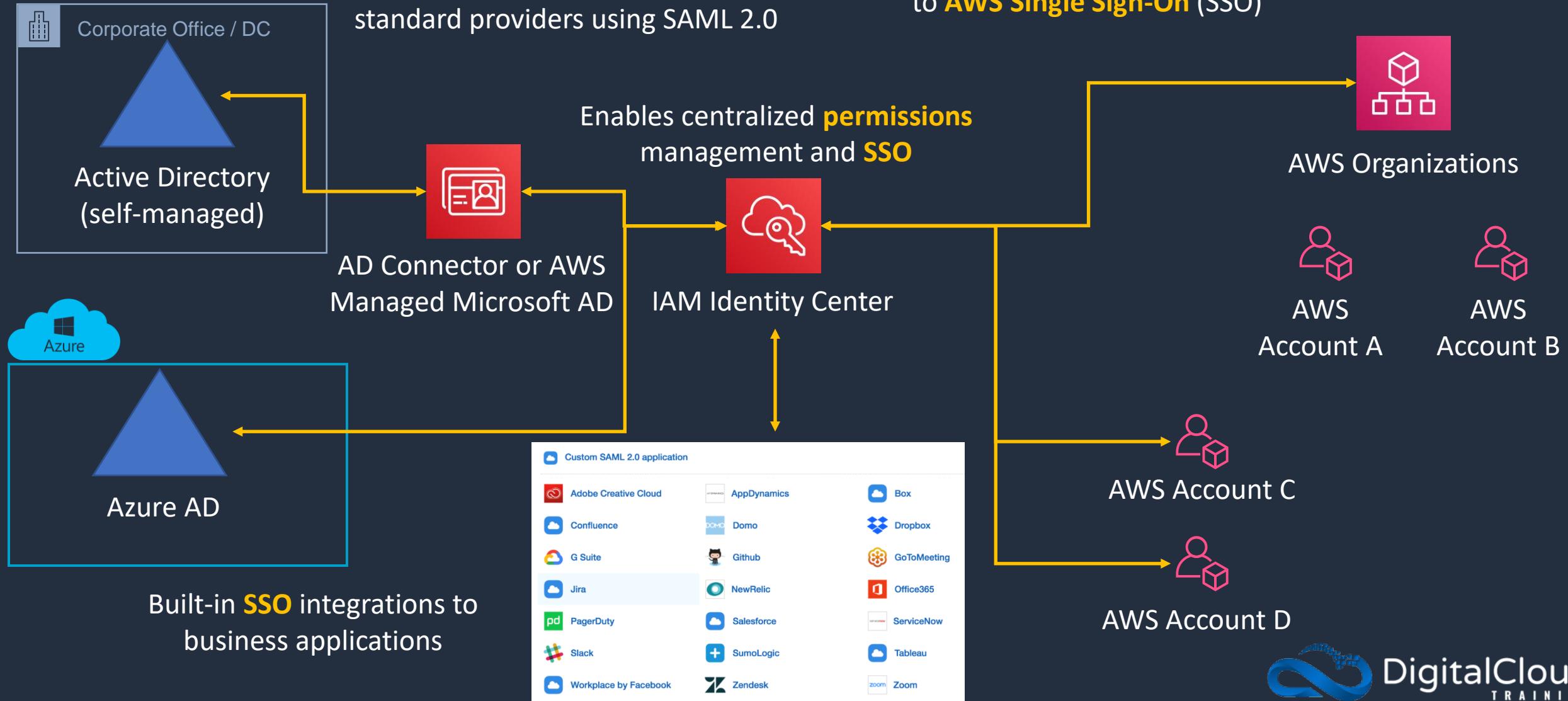




IAM Identity Center

Identity sources can be Identity Center directory, Active Directory and standard providers using SAML 2.0

IAM Identity Center is the successor to **AWS Single Sign-On (SSO)**





IAM vs IAM Identity Center

Feature/Use Case	AWS IAM	IAM Identity Center
Primary Purpose	Manage access to AWS services and resources	Centralize identity management and provide single sign-on access to AWS accounts and business applications
Identity Federation	Supports federation with external IdPs using SAML and OpenID Connect	Built-in federation with external IdPs, streamlined for ease of setup and management
Multi-Account Access	Requires more complex setup for cross-account access	Simplifies granting users access to multiple AWS accounts and applications with a single login
Integration with Business Applications	Limited to AWS services; requires custom setup for non-AWS applications	Provides SSO access to commonly used business applications (like Salesforce, Office 365) in addition to AWS accounts
Single Sign-On (SSO) Capability	Enables SSO through federation, but setup is complex and manual	Offers a more user-friendly and simplified SSO setup for both AWS and non-AWS applications



IAM vs IAM Identity Center – Use Cases

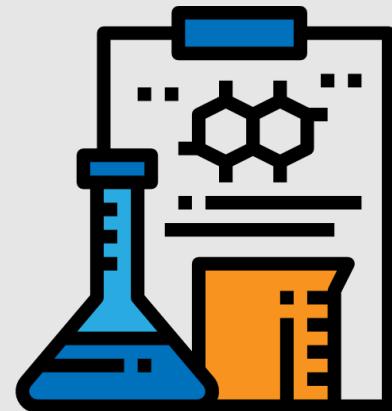
AWS IAM

- Managing AWS resources and permissions
- Creating and managing IAM users and roles within AWS
- Federating with external IdPs for SSO to AWS services
- Programmatic Access Management
- Fine-grained access control

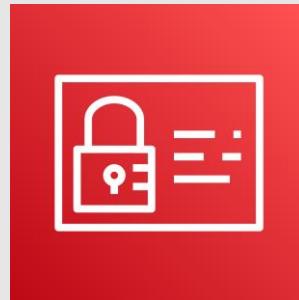
IAM Identity Center

- Providing SSO access to AWS and non-AWS applications
- Centralizing identity management across multiple AWS accounts
- Integrating with external directory services
- Streamlining Access to Business Applications
- Enhancing User Experience with a User Portal

IAM Identity Center in Action



IAM Best Practices





AWS IAM Best Practices

- Lock away your AWS account root user access keys
- Create individual IAM users
- Use groups to assign permissions to IAM users
- Grant least privilege
- Get started using permissions with AWS managed policies
- Use customer managed policies instead of inline policies
- Use access levels to review IAM permissions
- Configure a strong password policy for your users
- Enable MFA



AWS IAM Best Practices

- Use roles for applications that run on Amazon EC2 instances
- Use roles to delegate permissions
- Do not share access keys
- Rotate credentials regularly
- Remove unnecessary credentials
- Use policy conditions for extra security
- Monitor activity in your AWS account

SECTION 5

AWS Compute Services

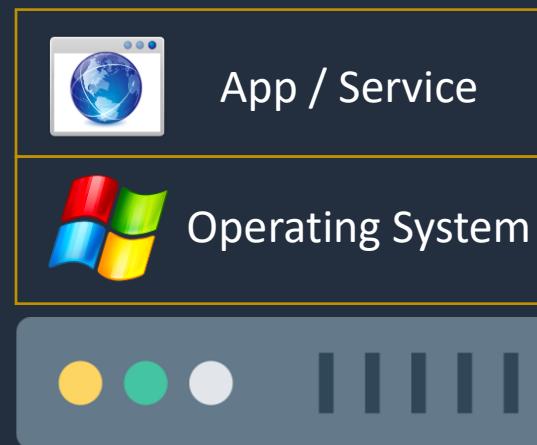
Server Virtualization





Server Without Virtualization

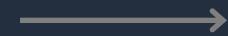
Application / Service



Operating System



Hardware



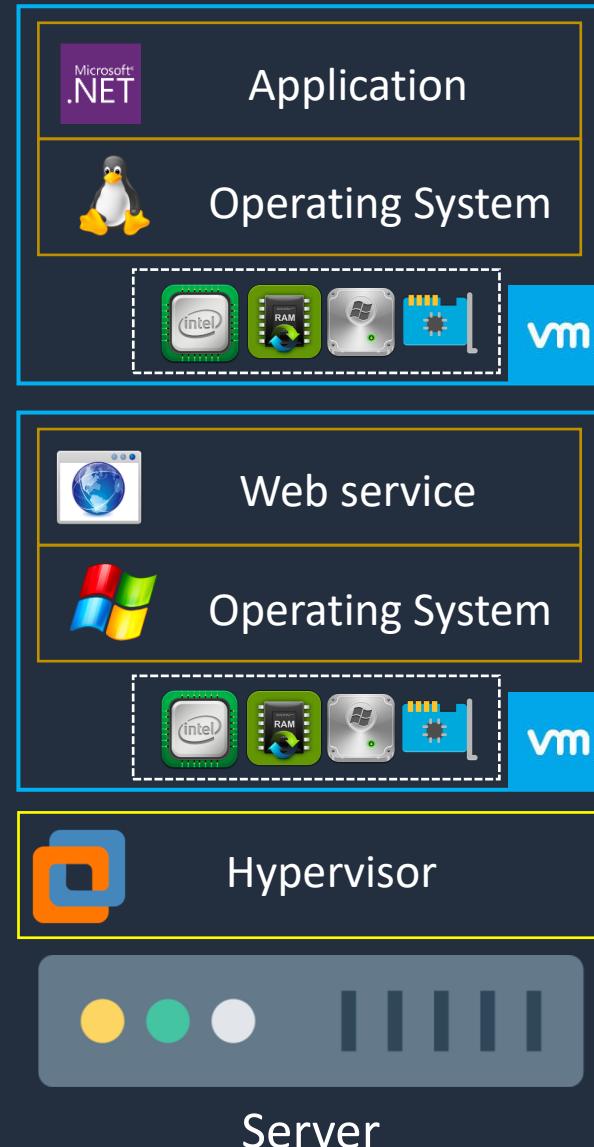
Limitations:

- OS is tied to hardware
- Underutilized resources
- Higher costs
- Scalability constraints
- Longer deployment times

Server With Virtualization

This is known as a **virtual server** or **virtual machine**

The **hypervisor** creates a layer of abstraction

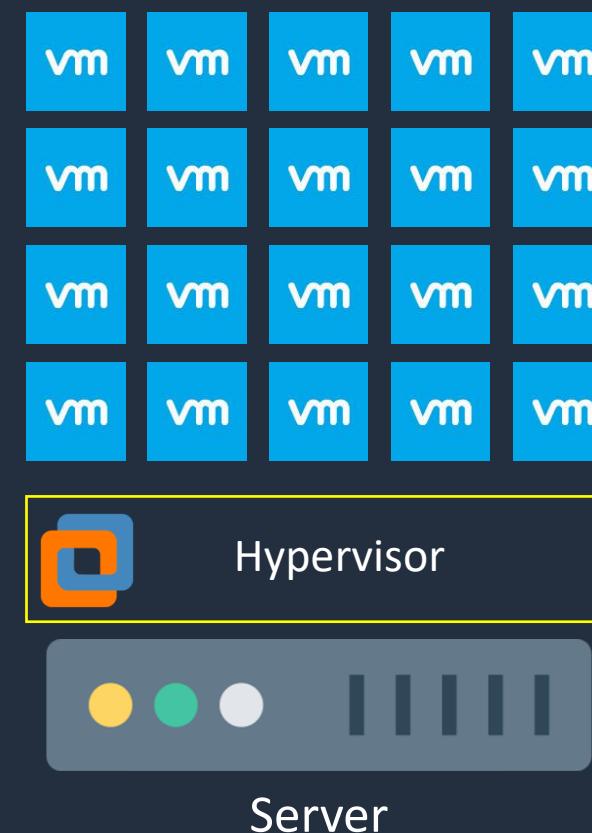


Many VMs can run on the same **physical hardware**

The hypervisor allocates physical resources to the VM



Server With Virtualization



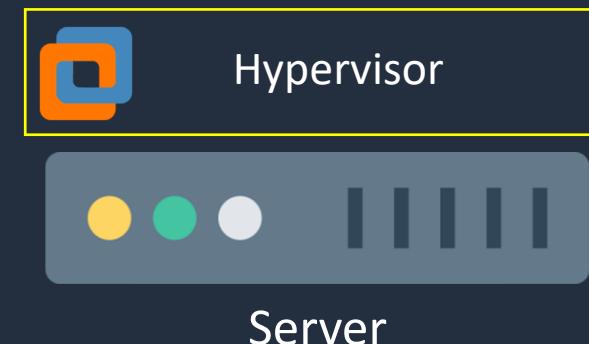


Server Virtualization: Portability

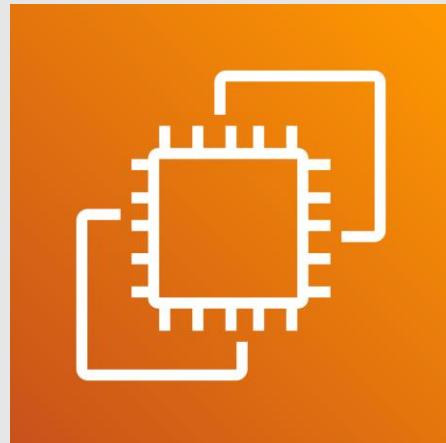


Benefits:

- VM is portable
- Better resource utilization
- Lower costs
- Improved scalability
- Quick deployment times



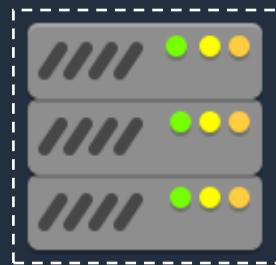
Amazon EC2 Overview



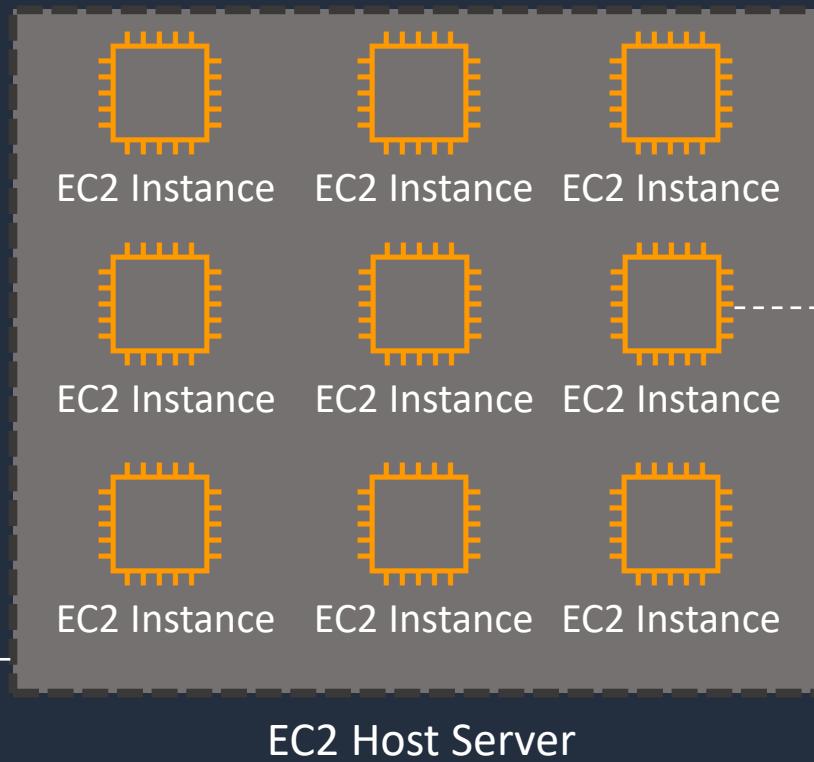


Amazon Elastic Compute Cloud (EC2)

EC2 hosts are
managed by AWS



EC2 instances run Windows,
Linux, or MacOS



An **EC2 instance** is
a virtual server



A selection of **instance types**
come with varying combinations
of CPU, memory, storage and
networking

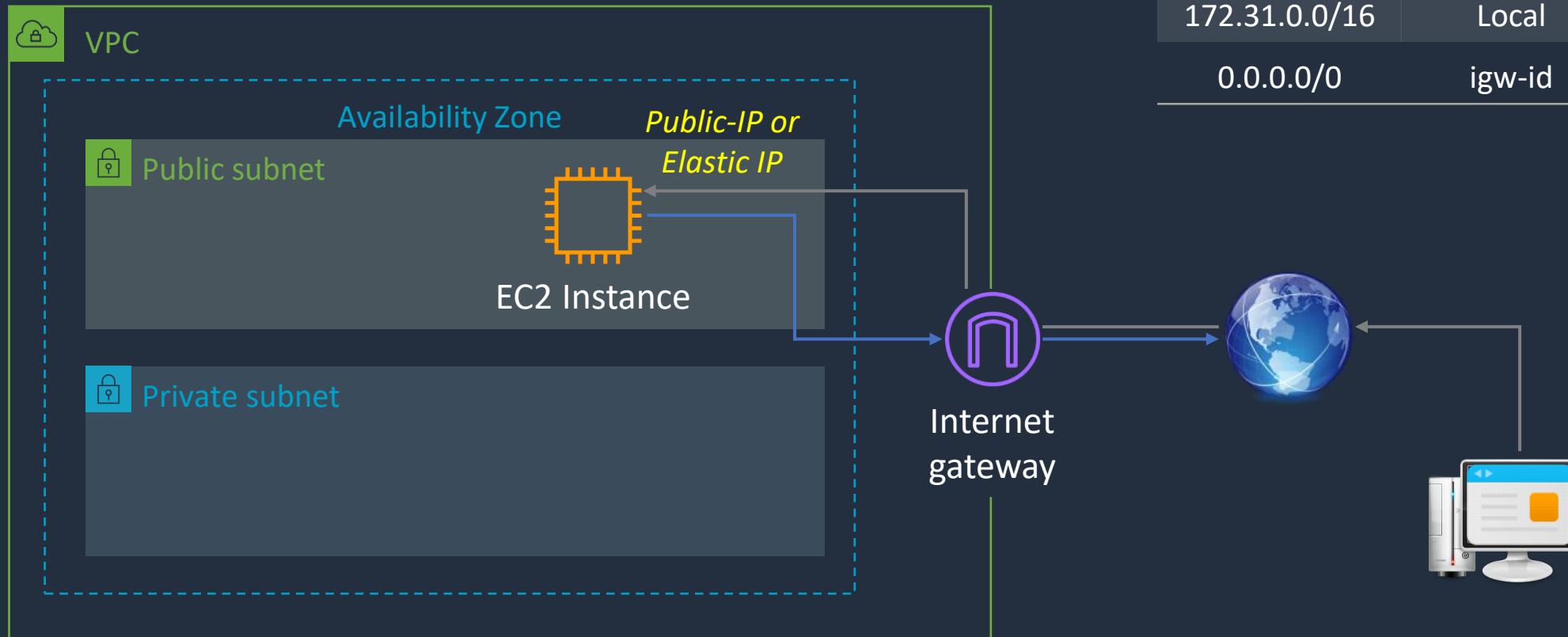


Public, Private, and Elastic IP addresses

Type	Description
Public IP address	<p>Lost when the instance is stopped</p> <p>Used in Public Subnets</p> <p>No charge</p> <p>Associated with a private IP address on the instance</p> <p>Cannot be moved between instances</p>
Private IP address	<p>Retained when the instance is stopped</p> <p>Used in Public and Private Subnets</p>
Elastic IP address	<p>Static Public IP address</p> <p>You are charged if not used</p> <p>Associated with a private IP address on the instance</p> <p>Can be moved between instances and Elastic Network Adapters</p>

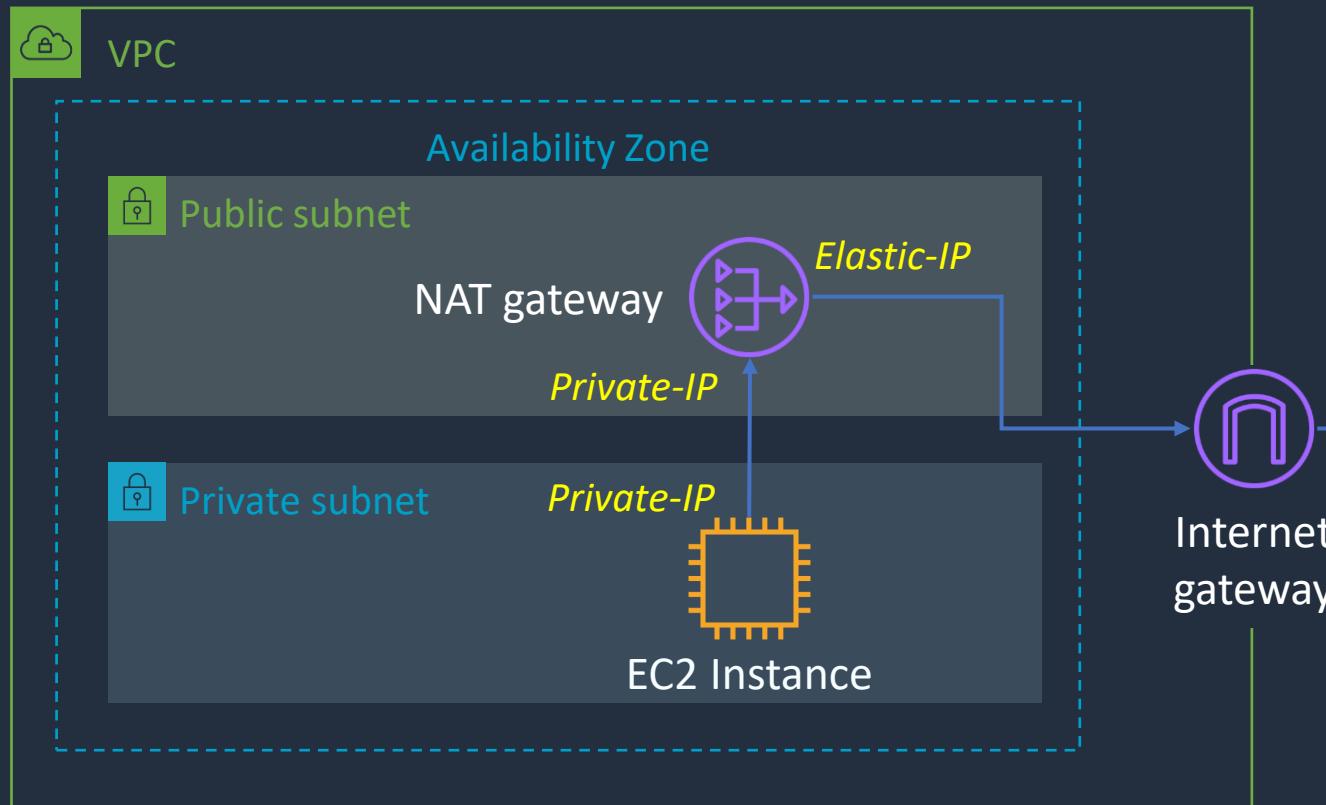


Public Subnets





Public Subnets



Public Subnet Route Table

Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	igw-id

Private Subnet Route Table

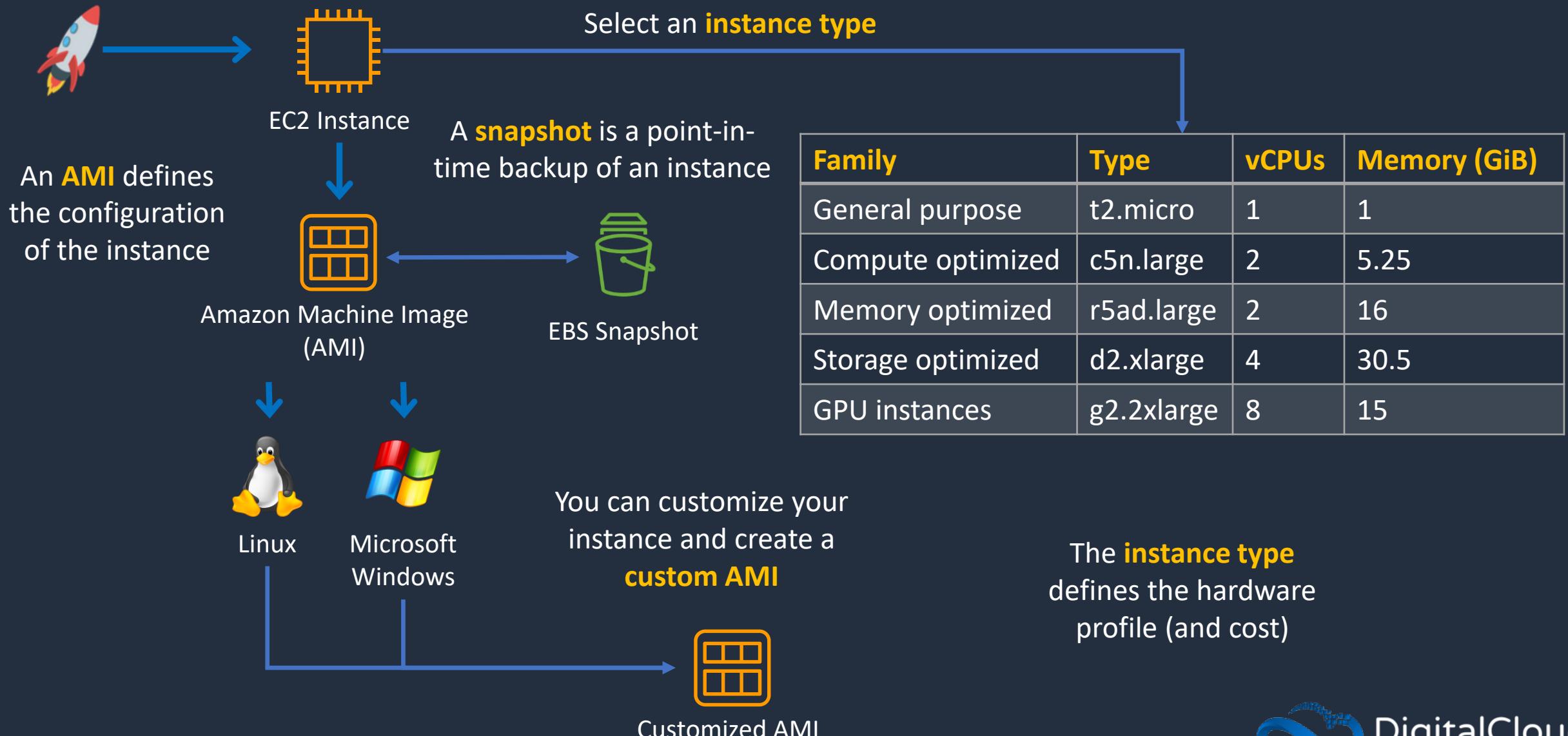
Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	nat-gateway-id

Launching Amazon EC2 Instances





Launching an EC2 Instance



Connecting to Amazon EC2



Amazon EC2 User Data and Metadata





Amazon EC2 User Data

The code is run when the instance starts for the **first time**



AWS Management Console

Batch and **PowerShell** scripts can be run on Windows

User data i As text As file Input is already base64 encoded

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
```

Limited to
16 KB



EC2 Instance

EC2 Instance with a
web service is
launched



Amazon EC2 Metadata

- Instance metadata is data about your EC2 instance
- Instance metadata is available at <http://169.254.169.254/latest/meta-data>
- Examples:



```
[ec2-user@ip-172-31-42-248 ~]$ curl http://169.254.169.254/latest/meta-data
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hibernation/
hostname
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
```



Amazon EC2 Metadata

- Examples ctd.:

```
[ec2-user@ip-172-31-42-248 ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4  
172.31.42.248[ec2-user@ip-172-31-42-248 ~]$
```

```
[ec2-user@ip-172-31-42-248 ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4  
3.26.54.18[ec2-user@ip-172-31-42-248 ~]$
```

Create a Website with User Data





Amazon EC2 User Data

The code is run when the instance starts for the **first time**

AWS Management Console

Batch and **PowerShell** scripts can be run on Windows

User data (i) As text As file Input is already base64 encoded

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
```

Limited to
16 KB



EC2 Instance

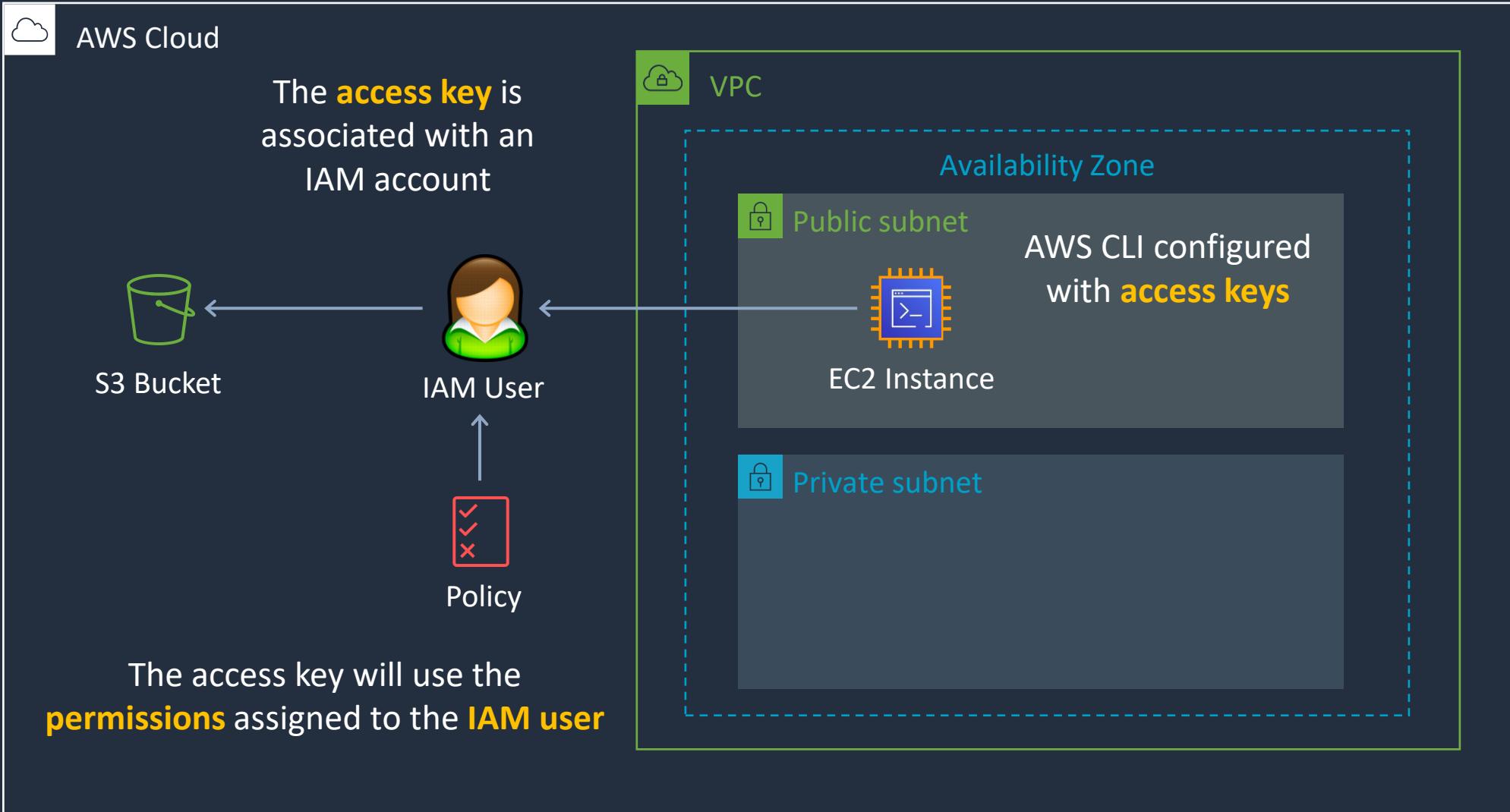
EC2 Instance with a **web service** is launched

Access Keys and IAM Roles with EC2



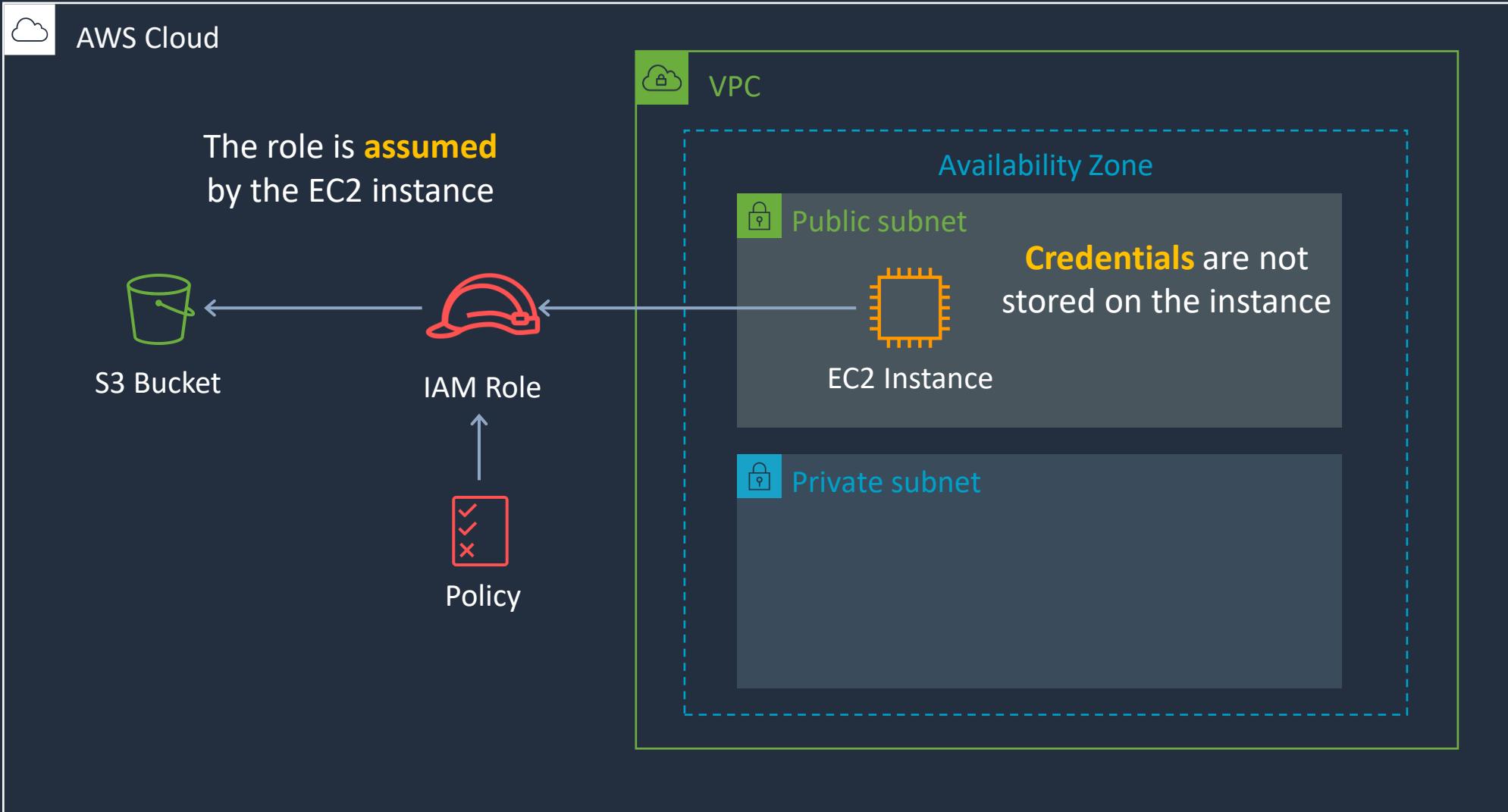


Using Access Keys with Amazon EC2

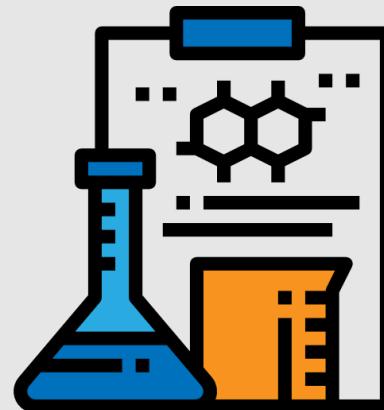




Using Access Keys with Amazon EC2



Practice with Access Keys and IAM Roles



AWS Batch





AWS Batch



Launch a **Batch Job**



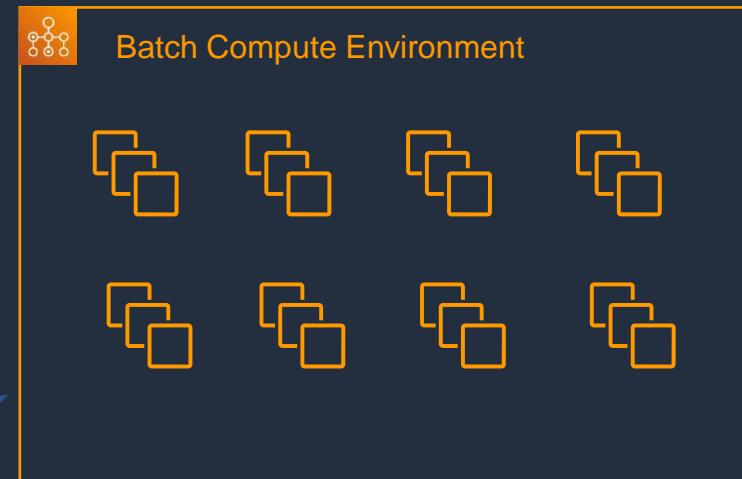
Job **Definition**



A job is submitted to a **queue** until **scheduled** onto a compute environment

A job is a unit of work such as a **shell script**, **executable** or **Docker container image**

Batch **launches**, **manages**, and **terminates** resources as required (EC2 and ECS/Fargate)



Managed or **unmanaged** resources used to run the job

Amazon LightSail





Amazon LightSail

- Low cost and ideal for users with less technical expertise
- Compute, storage, and network
- Preconfigured virtual servers

Amazon's Simple Cloud Server

Amazon Lightsail - Powerful virtual servers built for reliability & performance

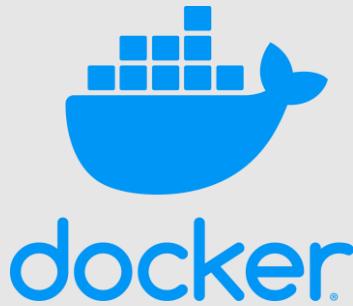
The advertisement features a dark blue background with a grid pattern. At the top left is a circular badge with the text "FREE TIER OFFER" at the top and "1 MONTH FREE*" below it. To the right are two circular icons: one for "Linux" showing a terminal prompt and one for "Windows Server" showing the Windows logo. Below each icon is a price: "Starting at \$3.50/month" for Linux and "Starting at \$8/month" for Windows Server.

1 Month Free Trial Starting at \$3.50/month Starting at \$8/month

- Virtual servers, databases and load balancers
- SSH and RDP access
- Can access Amazon VPC

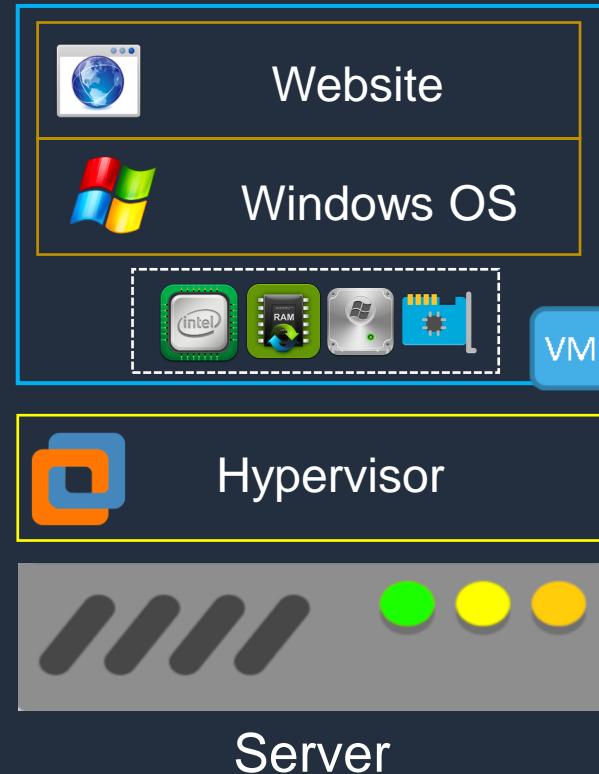
Exam tip: typically comes up in use cases where an easy method of deploying a virtual server is required by a user with little or no AWS expertise

Docker Containers and Microservices



Server Virtualization vs Containers

Every VM-instance needs an **operating system** which uses significant resources





Docker Containers

A **container** includes all the code, settings, and dependencies for running the application

Containers **start up** very **quickly**



Containers are very resource **efficient**

Each container is **isolated** from other containers



Docker Containers

- Docker utilizes containerization to package an application and its dependencies into a single **container image**
- Docker provides **Docker Hub**, a cloud-based registry service for sharing container images and automating workflows
- Containers are lightweight because they share the host system's kernel
- Docker is ideal for **microservices** architectures and building **cloud-native** applications



Cloud-Native Applications

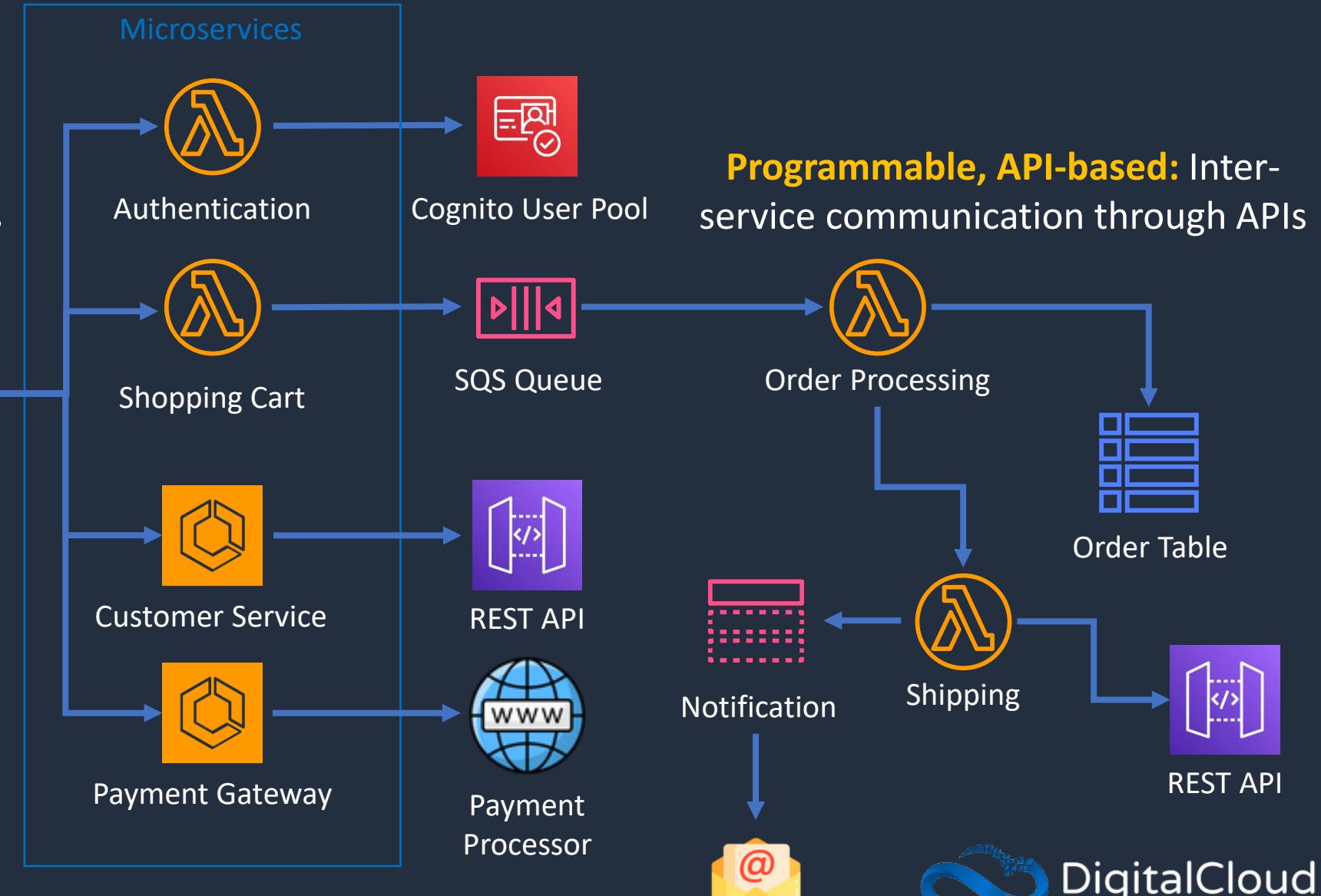
Microservices architecture:

Applications are structured as a collection of **loosely coupled**, independently deployable services, each running its own process



Containers and Functions:

Code runs in Docker containers and Lambda functions for isolation, elasticity, and cost-efficiency





Microservices: Attributes and Benefits

Microservices Attribute	Microservices Benefit
Use of Application Programming Interfaces (APIs)	Easier integrations between application components; assists with loose coupling
Independently deployable blocks of code	Can be scaled and maintained independently
Business-oriented architecture	Development organized around business capabilities; teams may be cross-functional and services may be reused
Flexible use of technologies	Each microservice can be written using different technologies (e.g. programming languages)
Speed and agility	Fast to deploy and update. Easy to include high availability and fault tolerance for each microservice

Amazon Elastic Container Service (ECS)





Amazon ECS

ECS **Services** are used to maintain a **desired count** of tasks

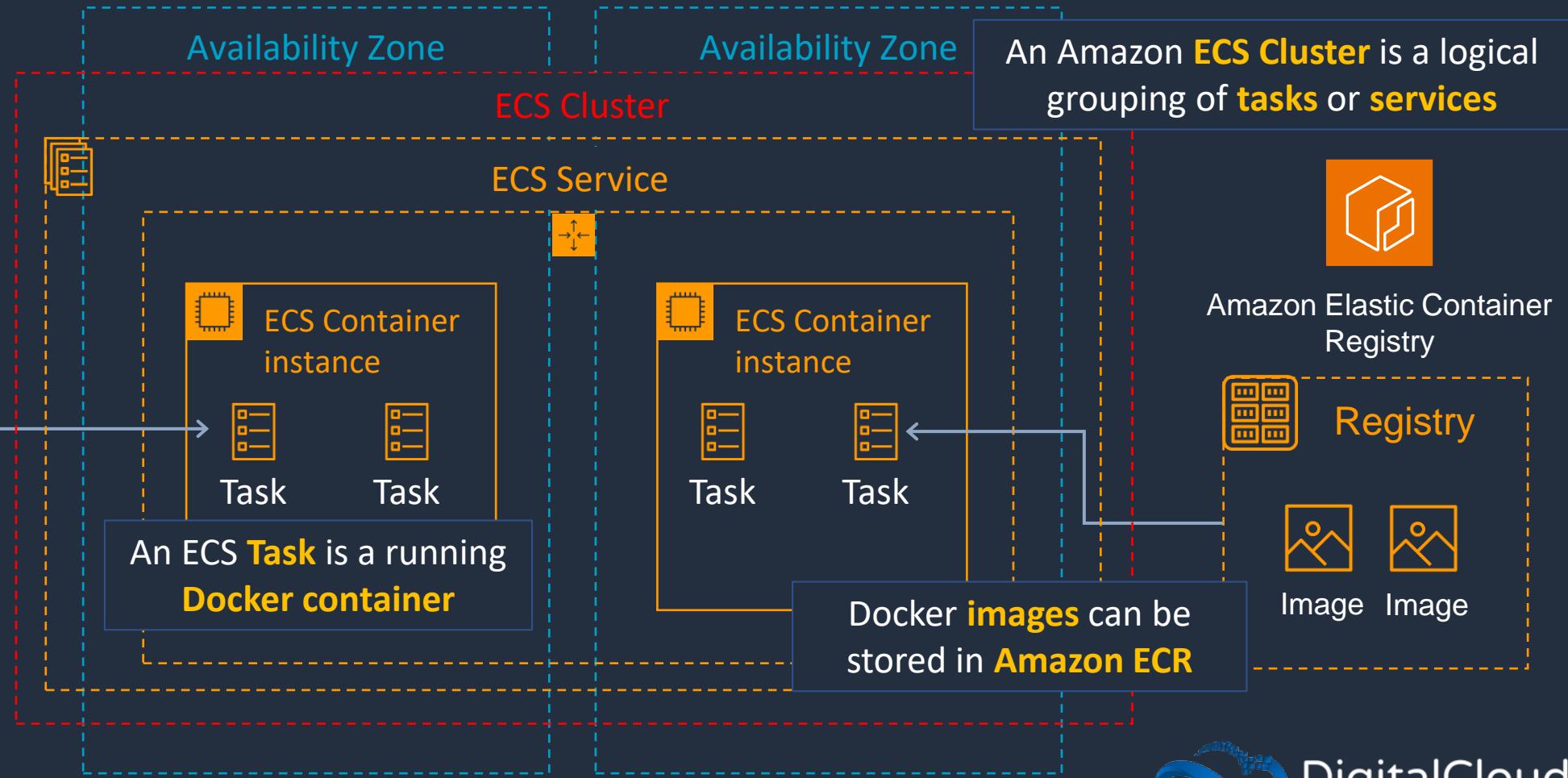
An ECS **Task** is created from a **Task Definition**

Task Definition

```
{
  "containerDefinitions": [
    {
      "name": "wordpress",
      "links": [
        "mysql"
      ],
      "image": "wordpress",
      "essential": true,
      "portMappings": [
        {
          "containerPort": 80,
          "hostPort": 80
        }
      ],
      "memory": 500,
      "cpu": 10
    }
  ]
}
```



Amazon Elastic Container Service





Amazon ECS Key Features

- **Serverless with AWS Fargate** – managed for you and fully scalable
- **Fully managed container orchestration** – control plane is managed for you
- **Docker support** – run and manage Docker containers with integration into the Docker Compose CLI
- **Windows container support** – ECS supports management of Windows containers
- **Elastic Load Balancing integration** – distribute traffic across containers using ALB or NLB
- **Amazon ECS Anywhere** – enables the use of Amazon ECS control plane to manage on-premises implementations



Amazon ECS Components

Elastic Container Service (ECS)	Description
Cluster	Logical grouping of tasks or services
Container instance	EC2 instance running the the ECS agent
Task Definition	Blueprint that describes how a docker container should launch
Task	A running container using settings in a task definition
Image	A Docker image referenced in the task definition
Service	Defines long running tasks – can control task count with Auto Scaling and attach an ELB



Amazon ECS Images

- Containers are created from a read-only template called an **image** which has the instructions for creating a Docker container
- Images are built from a **Dockerfile**
- Only Docker containers are supported on ECS
- Images are stored in a registry such as DockerHub or Amazon Elastic Container Registry (ECR)
- ECR is a managed AWS Docker registry service that is secure, scalable and reliable
- ECR supports private Docker repositories with resource-based permissions using AWS IAM in order to access repositories and images
- You can use the Docker CLI to push, pull and manage images



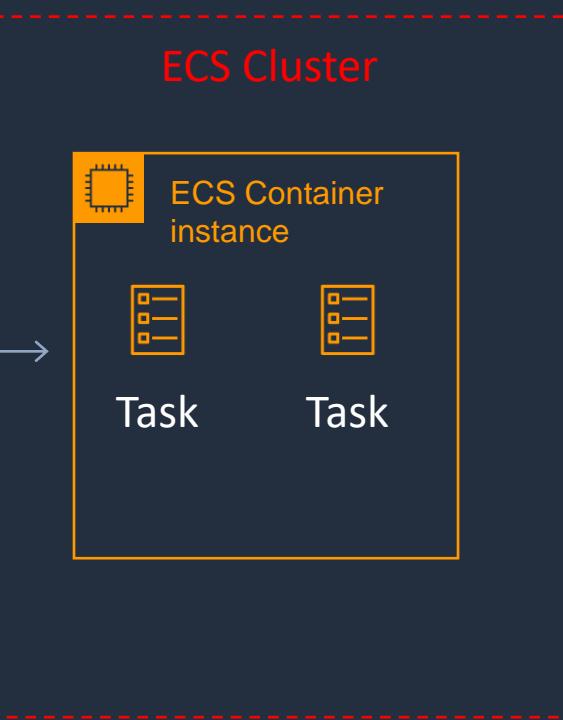


Amazon ECS Tasks and Task Definitions

- A task definition is required to run Docker containers in Amazon ECS
- A task definition is a text file in JSON format that describes one or more containers, up to a maximum of 10
- Task definitions use Docker images to launch containers

Task Definition

```
{  
  "containerDefinitions": [  
    {  
      "name": "wordpress",  
      "links": [  
        "mysql"  
      ],  
      "image": "wordpress",  
      "essential": true,  
      "portMappings": [  
        {  
          "containerPort": 80,  
          "hostPort": 80  
        }  
      ],  
      "memory": 500,  
      "cpu": 10  
    }  
  ]  
}
```

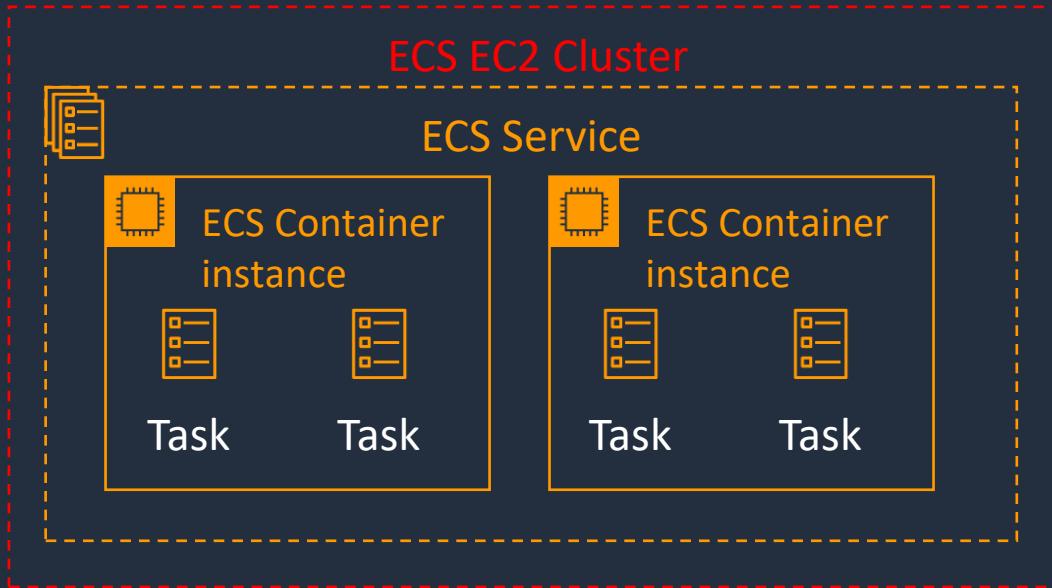




Launch Types – EC2 and Fargate



Registry:
ECR, Docker Hub, Self-hosted

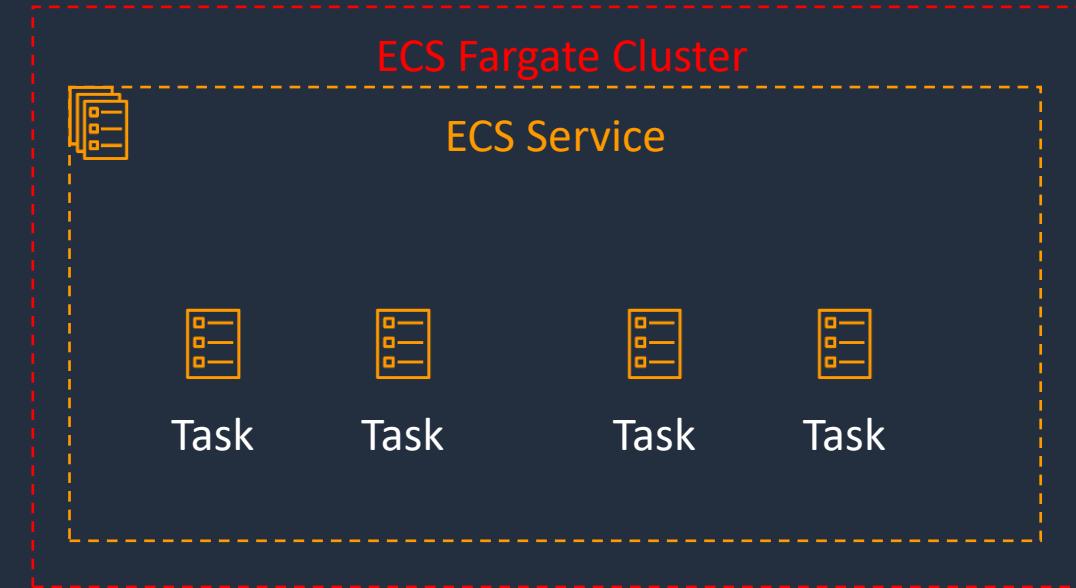


EC2 Launch Type:

- You explicitly provision EC2 instances
- You're responsible for managing EC2 instances
- Charged per running EC2 instance
- EFS, FSx, and EBS integration
- You handle cluster optimization
- More granular control over infrastructure



Registry:
ECR, Docker Hub

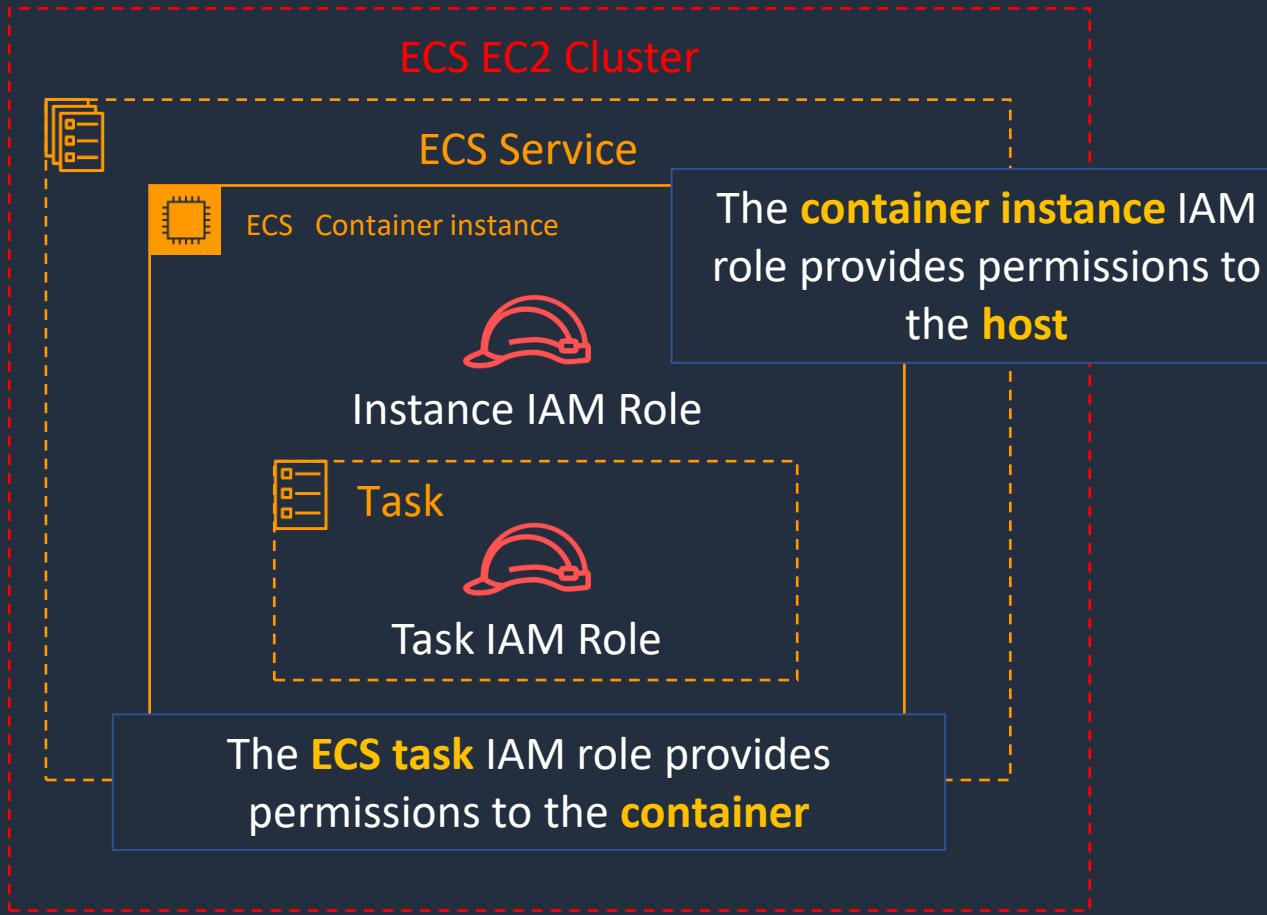


Fargate Launch Type:

- Fargate automatically provisions resources
- Fargate provisions and manages compute
- Charged for running tasks
- EFS integration only
- Fargate handles cluster optimization
- Limited control



ECS and IAM Roles



NOTE: With the Fargate launch type the container instance role is replaced with the **Task Execution Role**

AmazonEC2ContainerServiceforEC2Role

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2:DescribeTags",  
        "ecs>CreateCluster",  
        "ecs>DeregisterContainerInstance",  
        "ecs>DiscoverPollEndpoint",  
        "ecs>Poll",  
        "ecs>RegisterContainerInstance",  
        "ecs>StartTelemetrySession",  
        "ecs>UpdateContainerInstancesState",  
        "ecs>Submit*",  
        "ecr>GetAuthorizationToken",  
        "ecr>BatchCheckLayerAvailability",  
        "ecr>GetDownloadUrlForLayer",  
        "ecr>BatchGetImage",  
        "logs>CreateLogStream",  
        "logs>PutLogEvents"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

Launch Docker Containers on AWS Fargate



SECTION 6

AWS Storage Services

Block vs File vs Object Storage





Block Storage



Hard Disk Drive (HDD)

- Also known as magnetic drives
- Older technology
- Much slower than SSD
- Much cheaper than SSD



Solid State Drive (SSD)

- Uses flash memory
- Newer technology
- MUCH faster than HDD
- More expensive than HDD

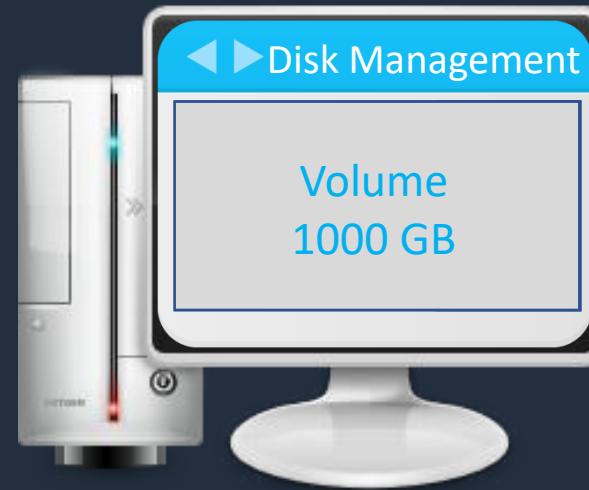


Block Storage

Hard drives are
block-based
storage systems



Hard Disk
Drive (HDD)



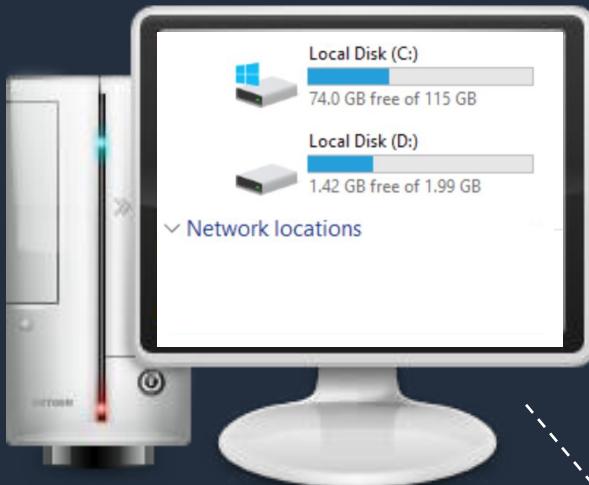
Hard drives are block-based storage systems

The Operating System
(OS) sees a volume. A
volume can be
partitioned and
formatted

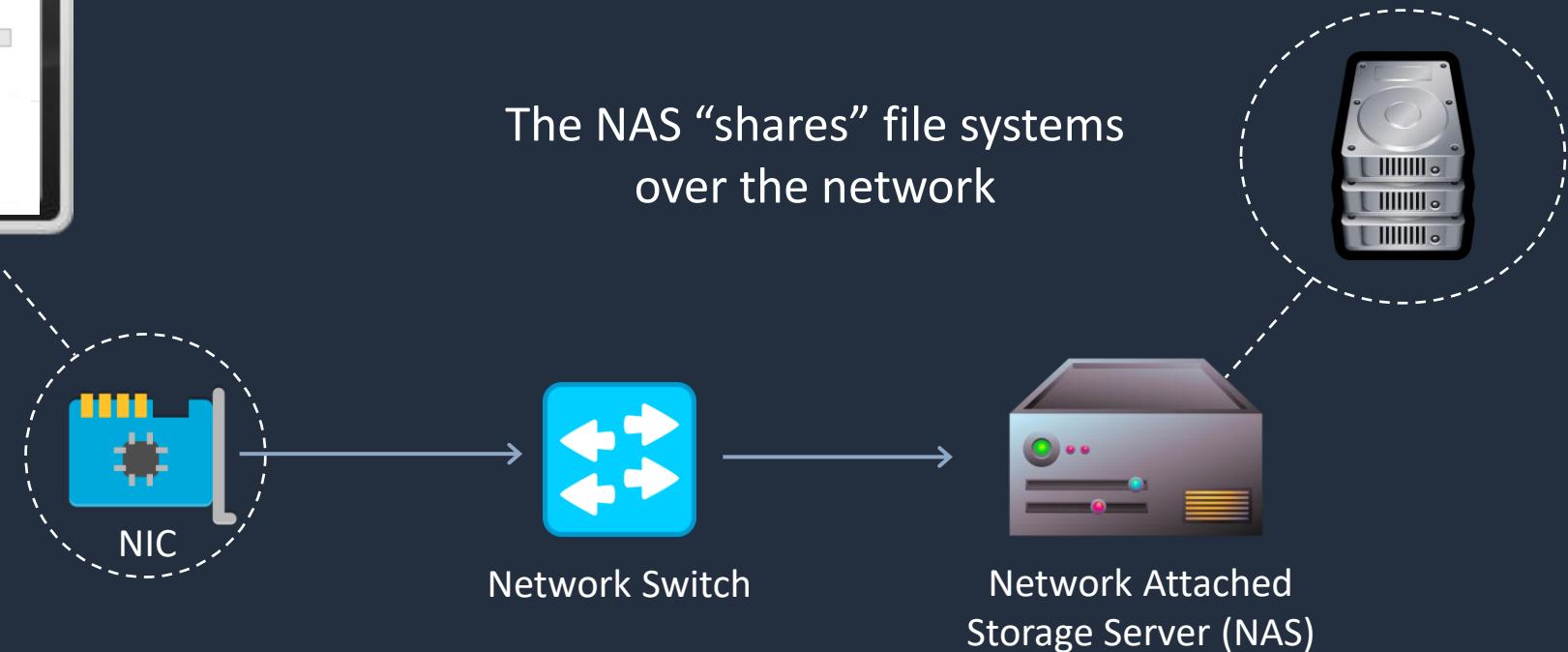


File Storage

The Operating System (OS) sees a **file system** that is mapped to a local drive letter



The NAS “shares” file systems over the network



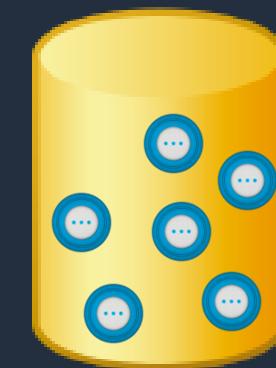
Object Storage Systems

User uploads **objects** using a web browser



The **HTTP protocol** is used with a **REST API** (e.g. GET, PUT, POST, SELECT, DELETE)

There is no hierarchy of objects in the container



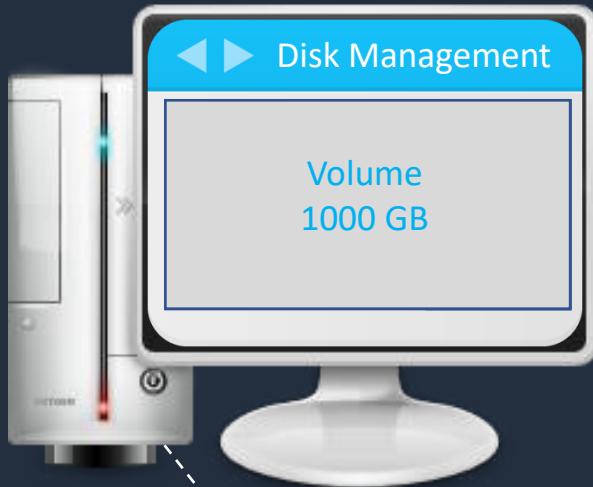
Object Storage Container

Objects can be files, videos, images etc.

Block vs File vs Object Storage

The OS sees **volumes** that can be partitioned and formatted

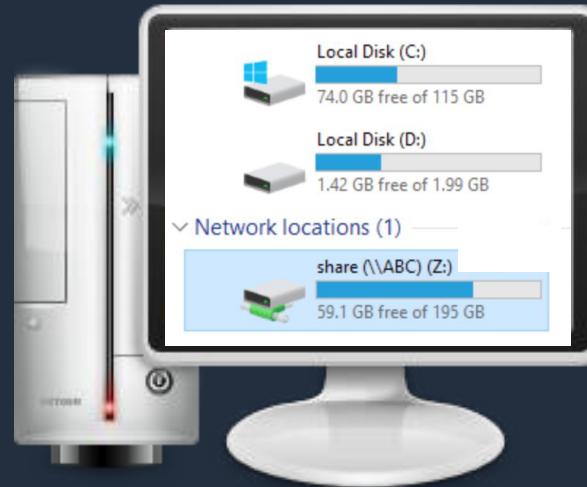
Block Storage



The OS reads/writes at the **block level**. Disks can be internal, or network attached

A filesystem can be shared by many users

File Storage



A filesystem is “**mounted**” to the OS using a network share

Massively scalable and low cost

Object Storage

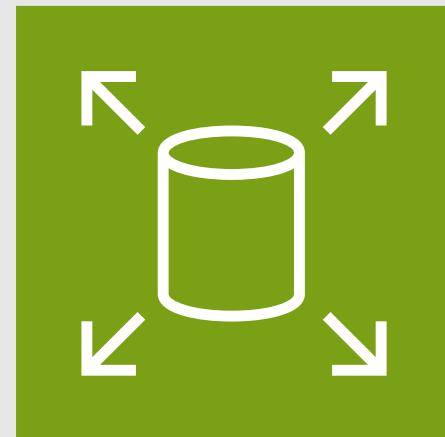


Object Storage Container

There is **no hierarchy** of objects in the container

Cannot be mounted but can be accessed programmatically using the **REST API**

Amazon EBS and Instance Stores





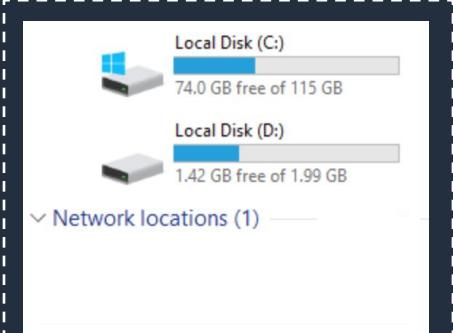
Amazon Elastic Block Store (EBS)

EBS volumes exist within an **Availability Zone**

Availability Zone



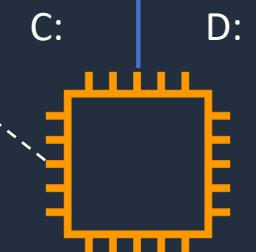
The volume is automatically replicated **within the AZ**



EBS Volume

EBS Volume

The volume is **attached** over a network

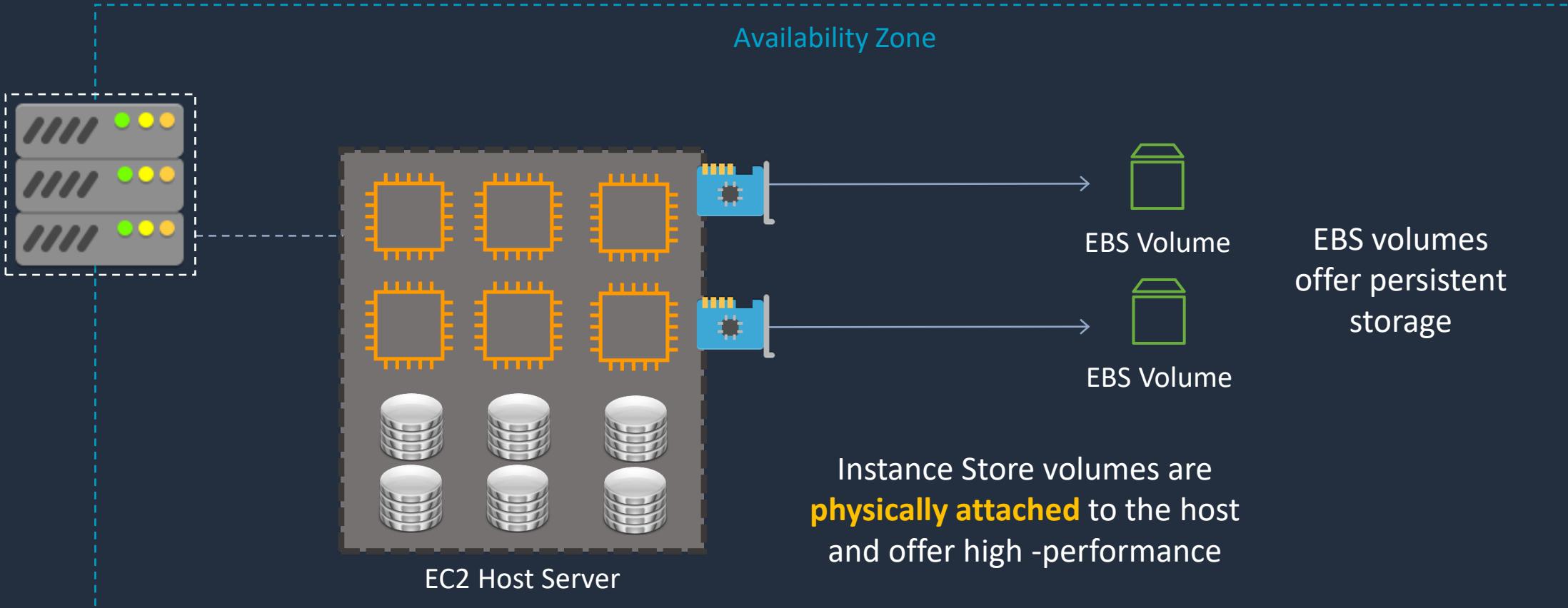


EC2 Instance



Amazon EBS vs Instance Store

EBS volumes are **attached** over the **network**

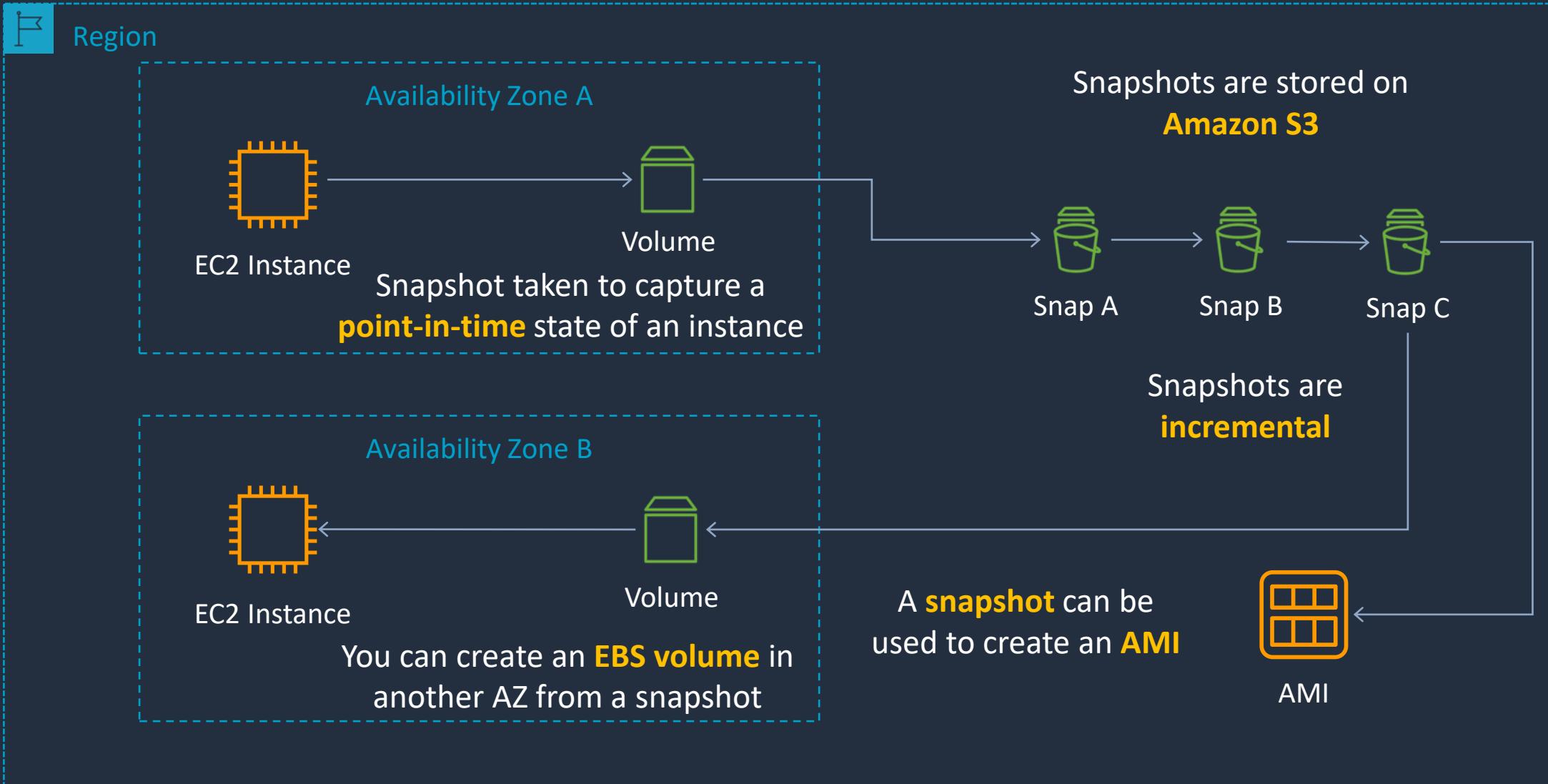


Instance Store volumes are **ephemeral** (non-persistent)

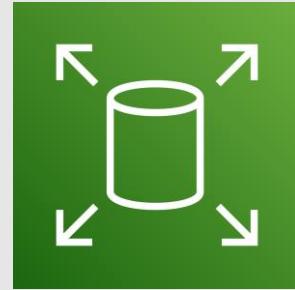
EBS volumes offer persistent storage



Amazon EBS Snapshots

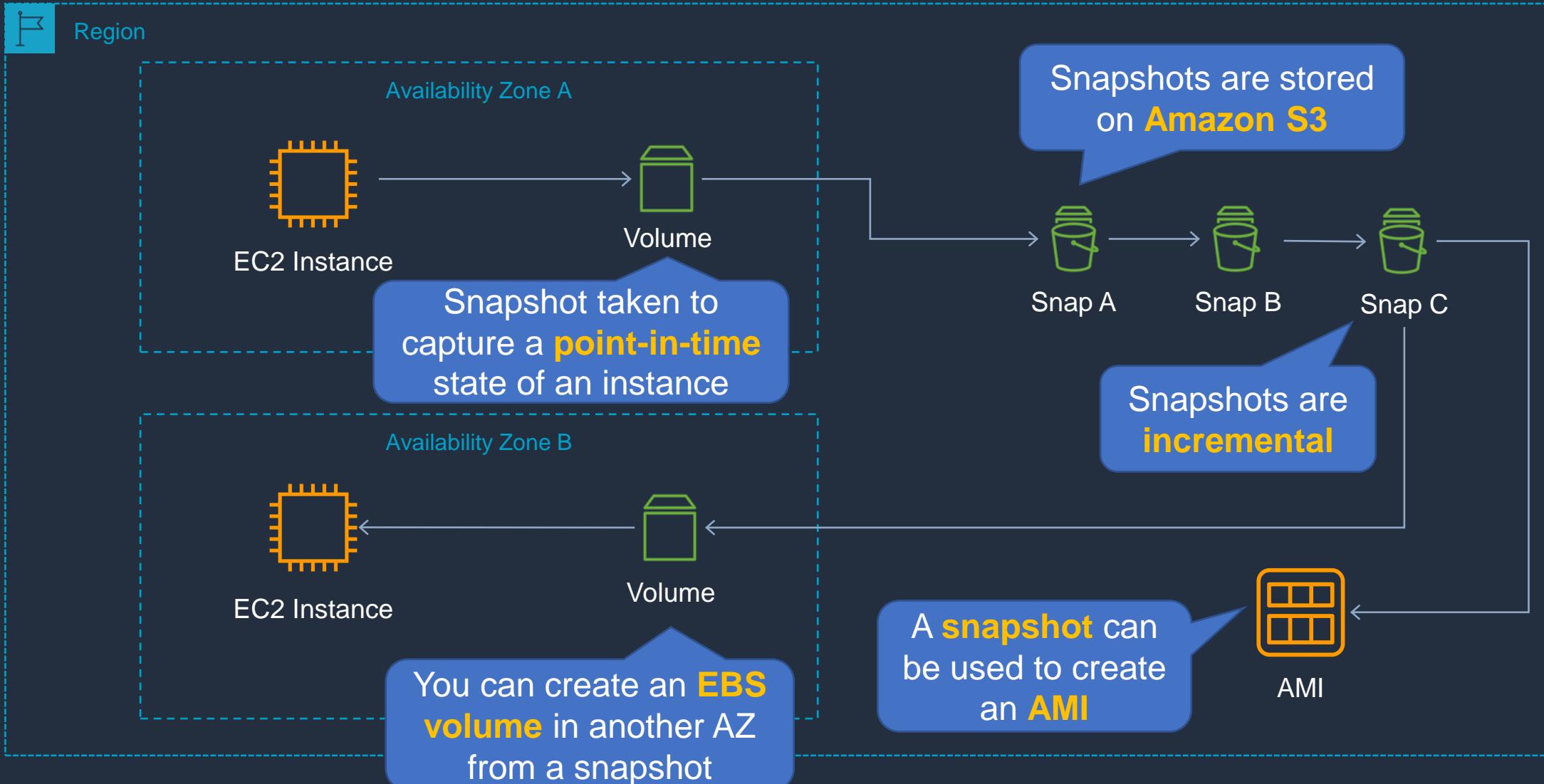


Amazon EBS Snapshots and DLM





Amazon EBS Snapshots

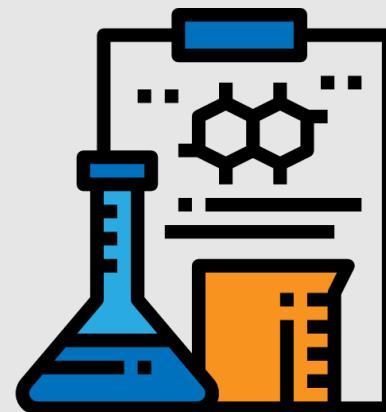




Amazon Data Lifecycle Manager (DLM)

- DLM automates the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs
- DLM helps with the following:
 - Protects valuable data by enforcing a regular backup schedule
 - Create standardized AMIs that can be refreshed at regular intervals
 - Retain backups as required by auditors or internal compliance
 - Reduce storage costs by deleting outdated backups
 - Create disaster recovery backup policies that back up data to isolated accounts

Create and Attach an EBS Volume



EBS Snapshots and AMIs



Amazon Elastic File System (EFS)

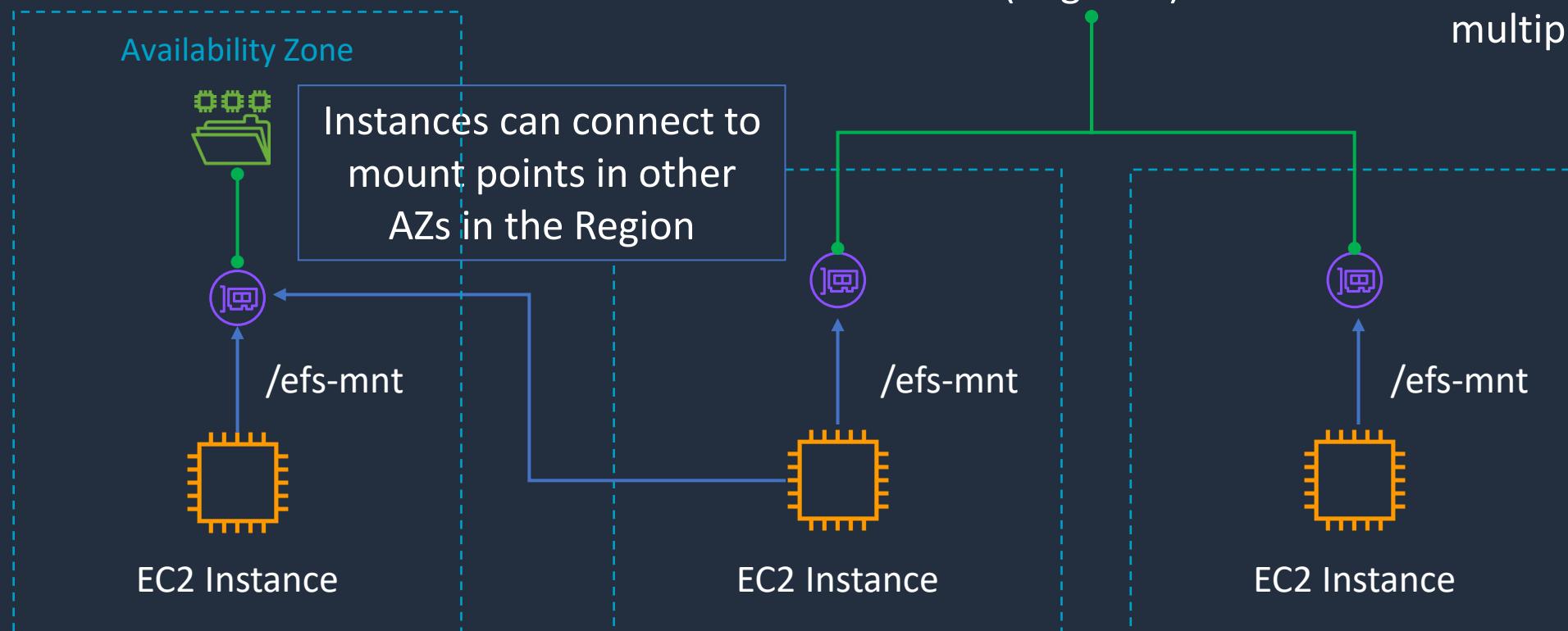




Amazon Elastic File System (EFS)

Note: EFS supports **Linux** only

One Zone file systems have mount targets in a single AZ



Regional file systems have mount targets in multiple AZs

The connection protocol is **NFS**

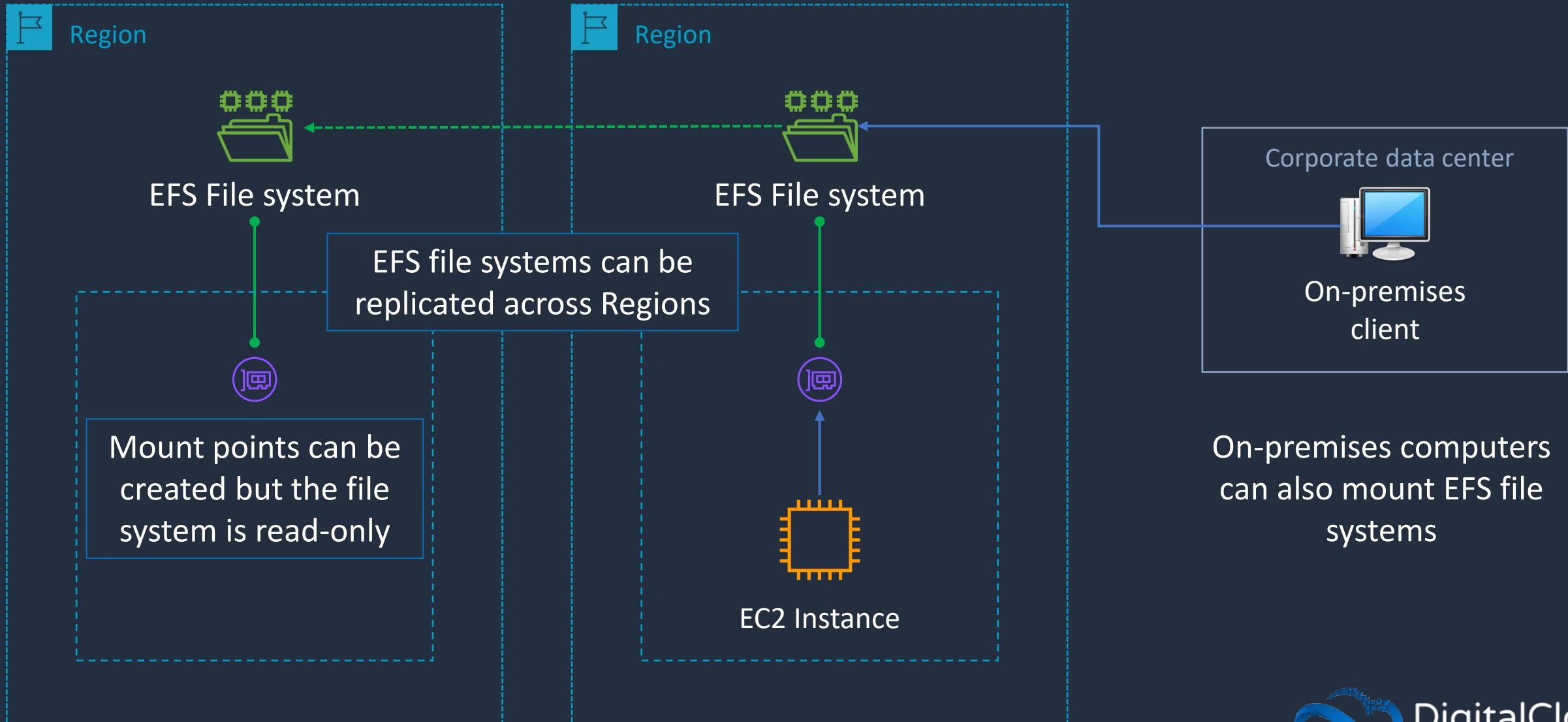


Amazon Elastic File System (EFS)

- **Data consistency** – write operations for Regional file systems are durably stored across Availability Zones
- **File locking** – NFS client applications can use NFS v4 file locking for read and write operations on EFS files
- **Storage classes** – there are three options:
 - **EFS Standard** – uses SSDs for low latency performance
 - **EFS Infrequent Access (IA)** – cost effective option
 - **EFS Archive** – even cheaper for less active data (archival)
- **Durability** – all storage classes offer 11 9s of durability



Amazon Elastic File System (EFS)





Amazon Elastic File System (EFS)

- **EFS Replication** – data is replicated across Regions for disaster recovery purposes with RPO/RTO in the minutes
- **Automatic Backup** – EFS integrates with AWS Backup for automatic file system backups
- **Performance options** – there are two options:
 - **Provisioned throughput** – Specify a level of throughput that the file system can drive independent of the file system's size
 - **Bursting throughput** – Throughput scales with the amount of storage and supports bursting to higher levels

Amazon Simple Storage Service (S3)





Amazon Simple Storage Service (S3)



S3 Bucket



A **bucket** is a container for objects

An **object** is a file you upload

You can store millions of **objects** in a **bucket**



Accessing objects in a bucket:

`https://bucket.s3.aws-region.amazonaws.com/key`
`https://s3.aws-region.amazonaws.com/bucket/key`

The **HTTP protocol** is used with a **REST API** (e.g. GET, PUT, POST, SELECT, DELETE)



Amazon Simple Storage Service (S3)



Bucket

A **bucket** is a container for objects

<http://bucket.s3.amazonaws.com>

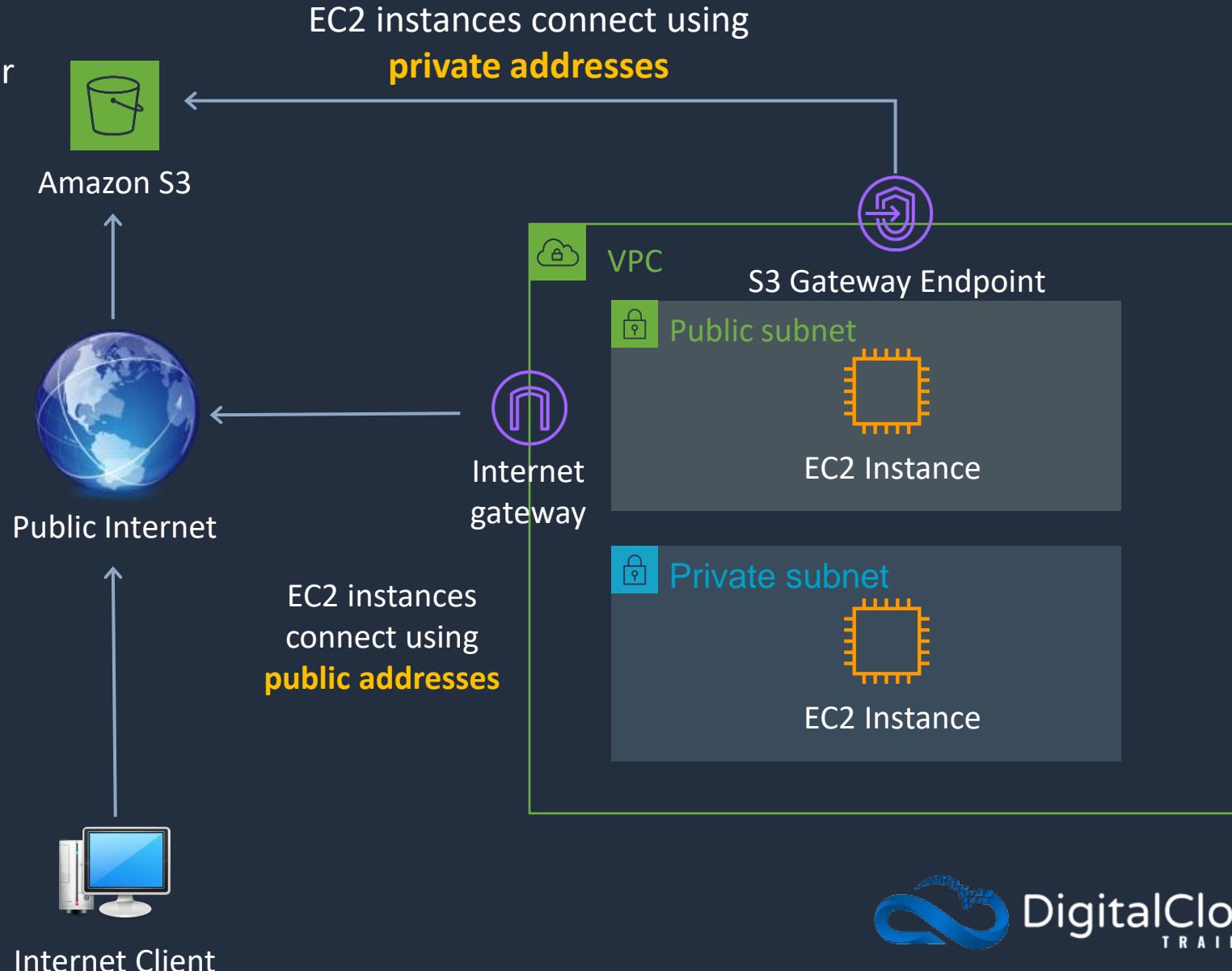
<http://s3.amazonaws.com/bucket>



Object

An object consists of:

- Key (name of objects)
- Version ID
- Value (actual data)
- Metadata
- Subresources
- Access control information





File Storage vs Object Storage

File Share



- Data stored in directories
- A hierarchy of directories can be formed
- File systems are mounted to an operating system
- Function like local storage
- Network connection is maintained
- Example is Amazon EFS

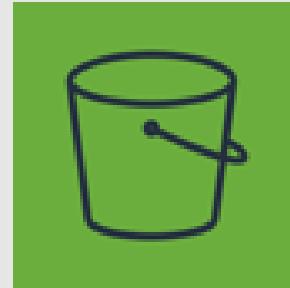
Object Store



`http://bucket.s3.aws-region.amazonaws.com`

- Data stored in buckets
- Flat namespace (no hierarchy)
- Hierarchy can be mimicked with prefixes
- Accessed by **REST API** and cannot be mounted
- Network connection is completed after each request
- Example is Amazon S3

Amazon S3 Storage Classes





Durability and Availability in S3

Durability

Durability is protection against:

- Data loss
- Data corruption
- S3 offers 11 9s durability (99.99999999)

If you store 10 million objects, then you expect to lose one object every 10,000 years!

Availability

Availability is a measurement of:

- The amount of time the data is available to you
- Expressed as a percent of time per year
- E.g. 99.99%



S3 Storage Classes

	S3 Standard	S3 Intelligent Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128KB	128KB	128KB	40KB	40KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval fee	N/A	N/A	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Working with S3 Buckets and Objects



S3 Versioning, Replication and Lifecycle Rules





Amazon S3 Versioning

- Versioning is a means of keeping **multiple variants** of an **object** in the same bucket
- Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket
- Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite



Amazon S3 Replication

Cross-Region Replication (CRR)



Buckets must have **versioning** enabled





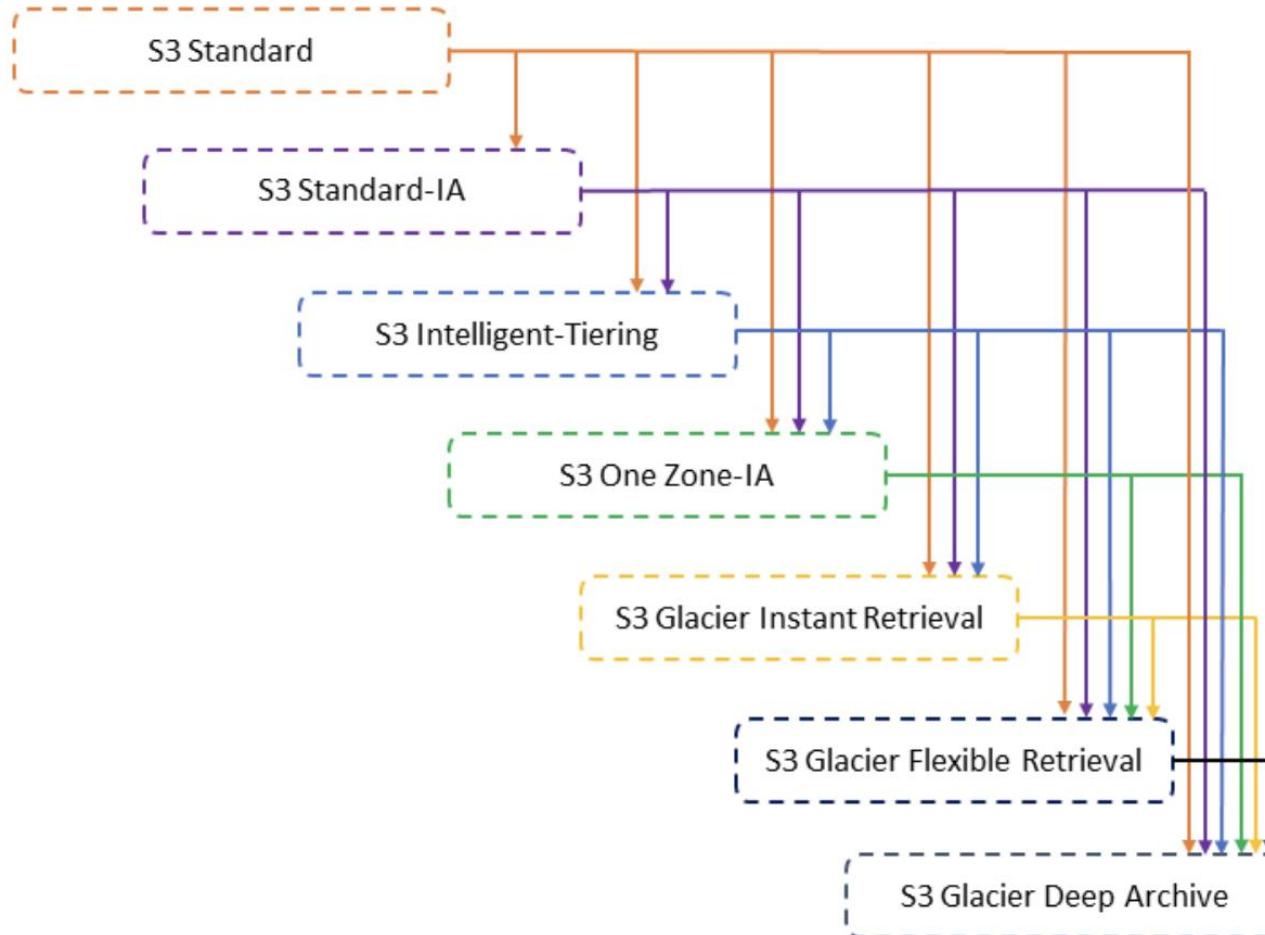
S3 Lifecycle Management

There are two types of actions:

- **Transition actions** - Define when objects transition to another storage class
- **Expiration actions** - Define when objects expire (deleted by S3)



S3 LM: Supported Transitions



<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

Configure Replication and Lifecycle



Create an Amazon S3 Static Website



S3 Permissions and Bucket Policies



Amazon FSx



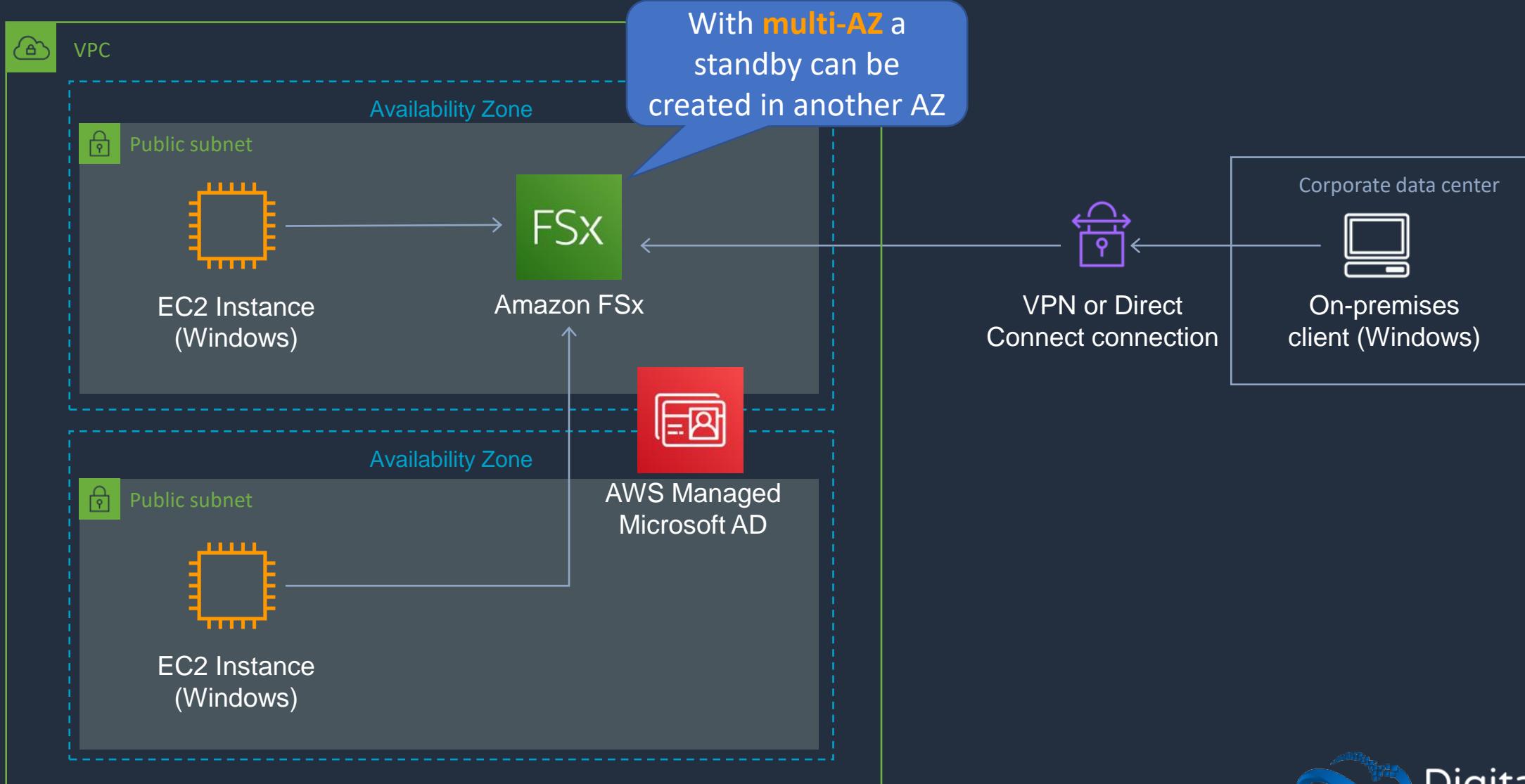
Amazon FSx

- Amazon FSx provides fully managed third-party file systems
- Amazon FSx provides you with two file systems to choose from:
 - **Amazon FSx for Windows File Server** for Windows-based applications
 - **Amazon FSx for Lustre** for compute-intensive workloads

Amazon FSx for Windows File Server

- Provides a fully managed native Microsoft Windows file system
- Full support for the SMB protocol, Windows NTFS, and Microsoft Active Directory (AD) integration
- Supports Windows-native file system features:
 - Access Control Lists (ACLs), shadow copies, and user quotas.
 - NTFS file systems that can be accessed from up to thousands of compute instances using the SMB protocol
- **High availability:** replicates data within an Availability Zone (AZ)
- **Multi-AZ:** file systems include an active and standby file server in separate AZs

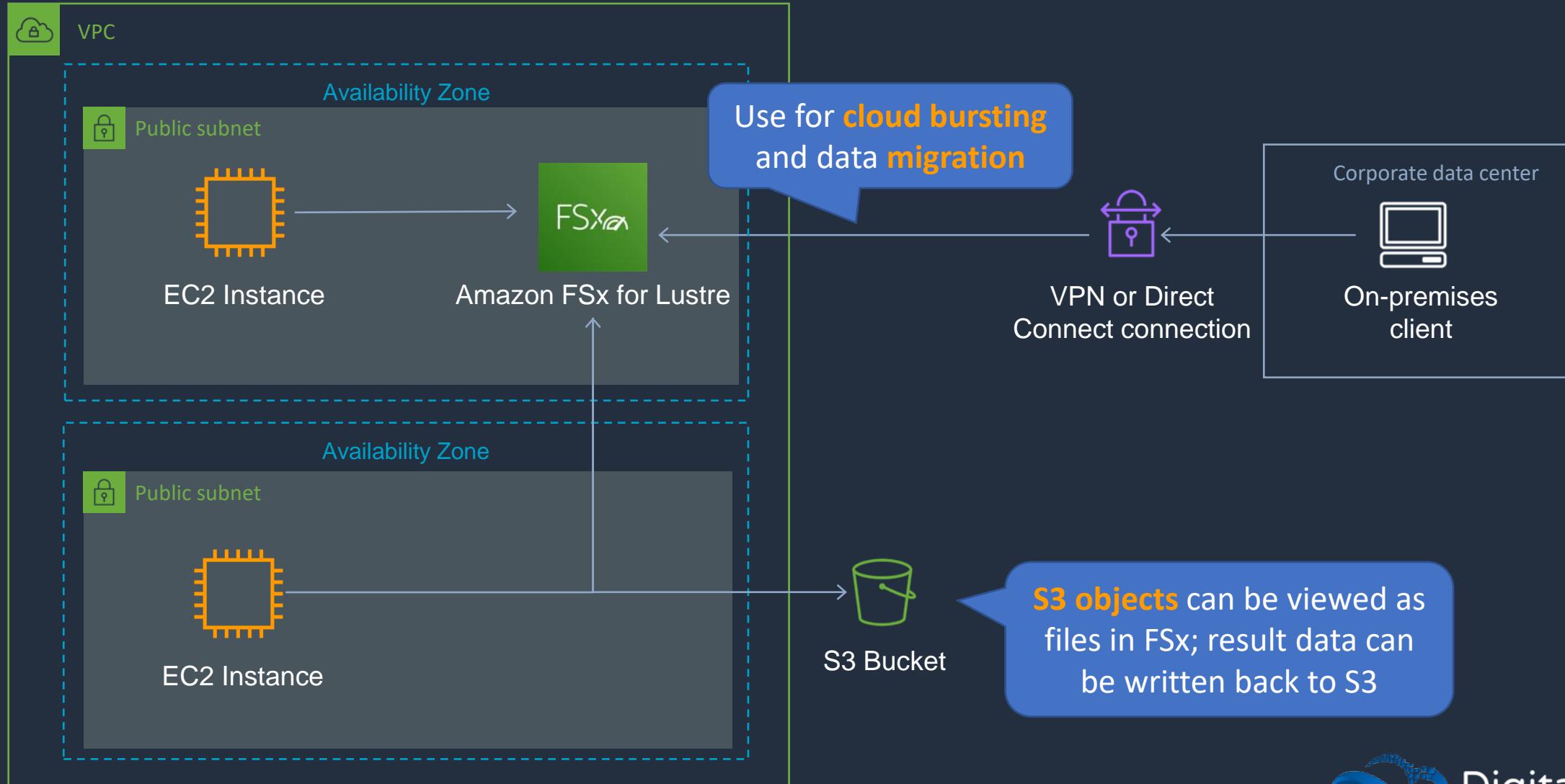
Amazon FSx for Windows File Server



Amazon FSx for Lustre

- High-performance file system optimized for fast processing of workloads such as:
 - Machine learning
 - High performance computing (HPC)
 - Video processing
 - Financial modeling
 - Electronic design automation (EDA)
- Works natively with S3, letting you transparently access your S3 objects as files
- Your S3 objects are presented as files in your file system, and you can write your results back to S3
- Provides a POSIX-compliant file system interface

Amazon FSx for Lustre



Archiving with S3 Glacier





Amazon S3 Glacier

- Amazon S3 Glacier (S3 Glacier) is a secure and durable service for low-cost data archiving and long-term backup
- Extremely low cost and you pay only for what you need with no commitments of upfront fees
- Three classes are:
- **S3 Glacier Instant Retrieval** - Use for archiving data that is rarely accessed and requires milliseconds retrieval
- **S3 Glacier Flexible Retrieval** - Use for archives where portions of the data might need to be retrieved in minutes
- **S3 Glacier Deep Archive** - Use for archiving data that rarely needs to be accessed



Amazon S3 Glacier

- Three options for access to archives, listed in the table below:

	Expedited	Standard	Bulk
Data access time	1-5 minutes	3-5 hours	5-12 hours
Data access time (Glacier DA)	N/A	12 hours	48 hours

- Expedited is available for data stored in the S3 Glacier Flexible Retrieval storage class or the S3 Intelligent-Tiering Archive Access tier



Object Lock and Glacier Vault Lock

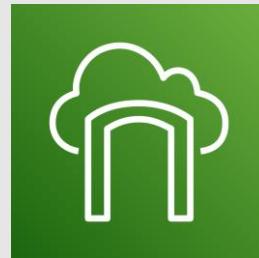
S3 Object Lock

- Store objects using a write-once-read-many (WORM) model
- Prevent objects from being deleted or overwritten for a fixed time or indefinitely

S3 Glacier Vault Lock

- Also used to enforce a WORM model
- Can apply a policy and lock the policy from future edits
- Use for compliance objectives and data retention

AWS Storage Gateway



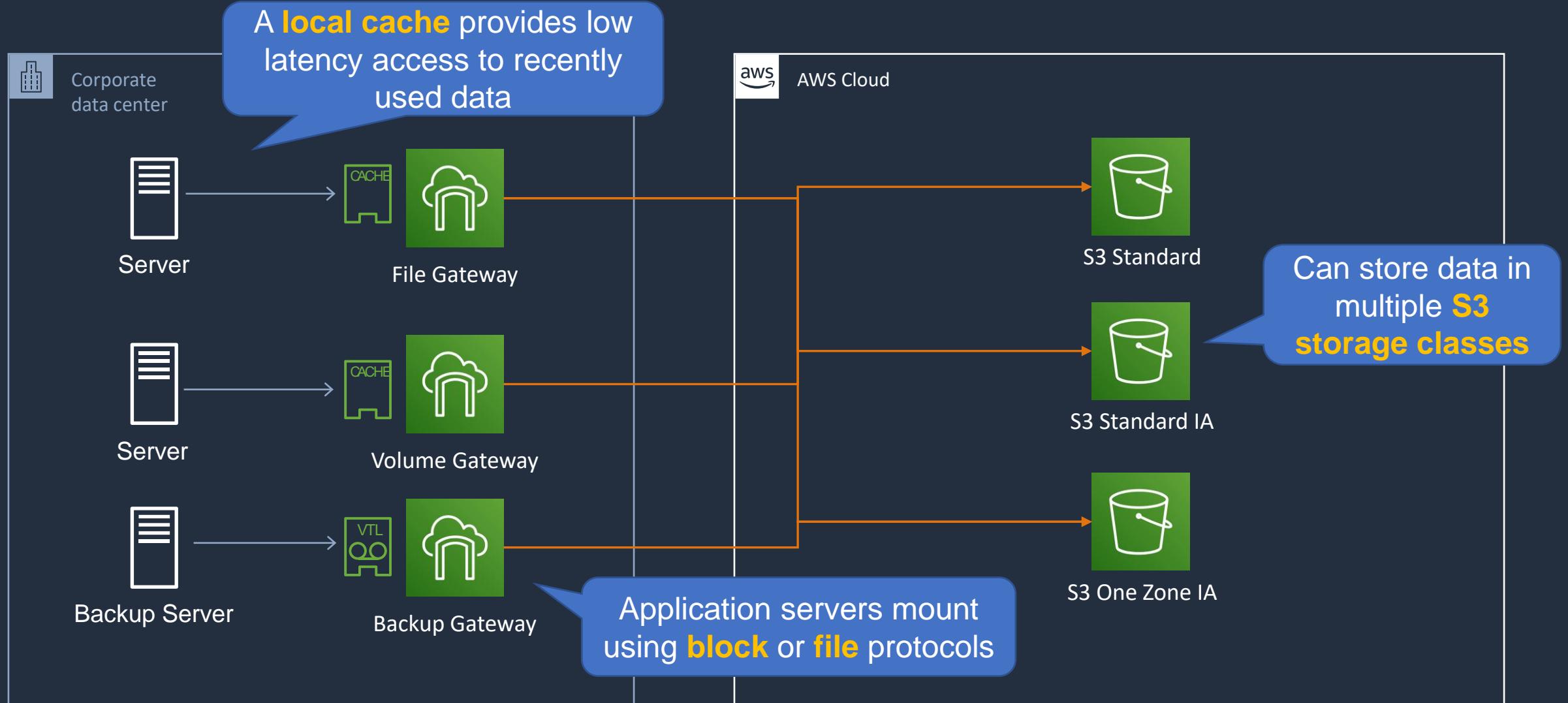


AWS Storage Gateway

- Hybrid cloud storage service
- Access cloud storage from on-premises applications
- Enables access to proprietary object storage (S3) using standard protocols
- Use cases:
 - Moving backups to the cloud
 - Using on-premises file shares backed by cloud storage
 - Low latency access to data in AWS for on-premises applications
 - Disaster recovery



AWS Storage Gateway



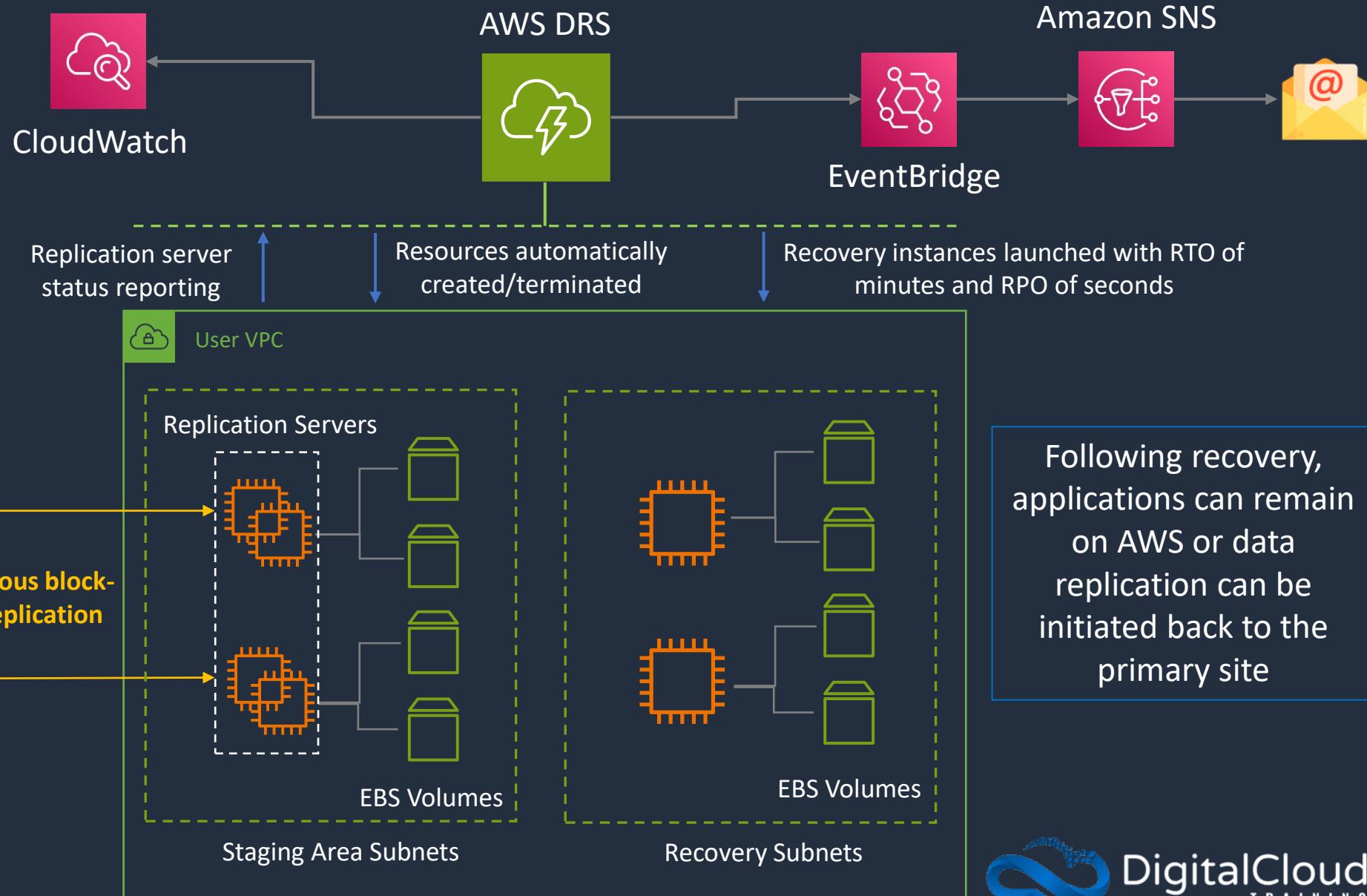
AWS Elastic Disaster Recovery





AWS Elastic Disaster Recovery (AWS DRS)

Can recover applications on AWS from physical infrastructure, VMware vSphere, Microsoft Hyper-V, and Cloud





AWS Elastic Disaster Recovery (AWS DRS)

What is AWS Elastic Disaster Recovery?

- **Application Recovery:** A service designed to protect and recover critical applications quickly at a lower cost
- **Reduced Downtime:** Ensures minimal downtime in the event of application failures by quickly recovering your applications in AWS

You can recover applications on AWS from:

- **Physical servers:** Applications running on physical servers in your data center
- **Virtual Machines:** Applications running on virtual machines (VMware vSphere, Microsoft Hyper-V)
- **Cloud infrastructure:** Recover applications from other cloud platforms such as Azure or Google Cloud to AWS
- **AWS Cloud:** Amazon EC2 instances in a different AWS Region



AWS Elastic Disaster Recovery (AWS DRS)

Recovery Process

- **Staging Area:** Initially, the replicated data is stored in a low-cost staging area in AWS. This staging area is used to maintain the replicated data until it is needed for recovery
- **Recovery Servers:** During a disaster recovery event, the systems are fully restored onto AWS servers. This ensures quick recovery and resumption of business operations
- **Conversion:** AWS DRS handles the conversion of your on-premises or cloud servers to AWS-compatible formats automatically, which aids in a smoother recovery process

SECTION 7

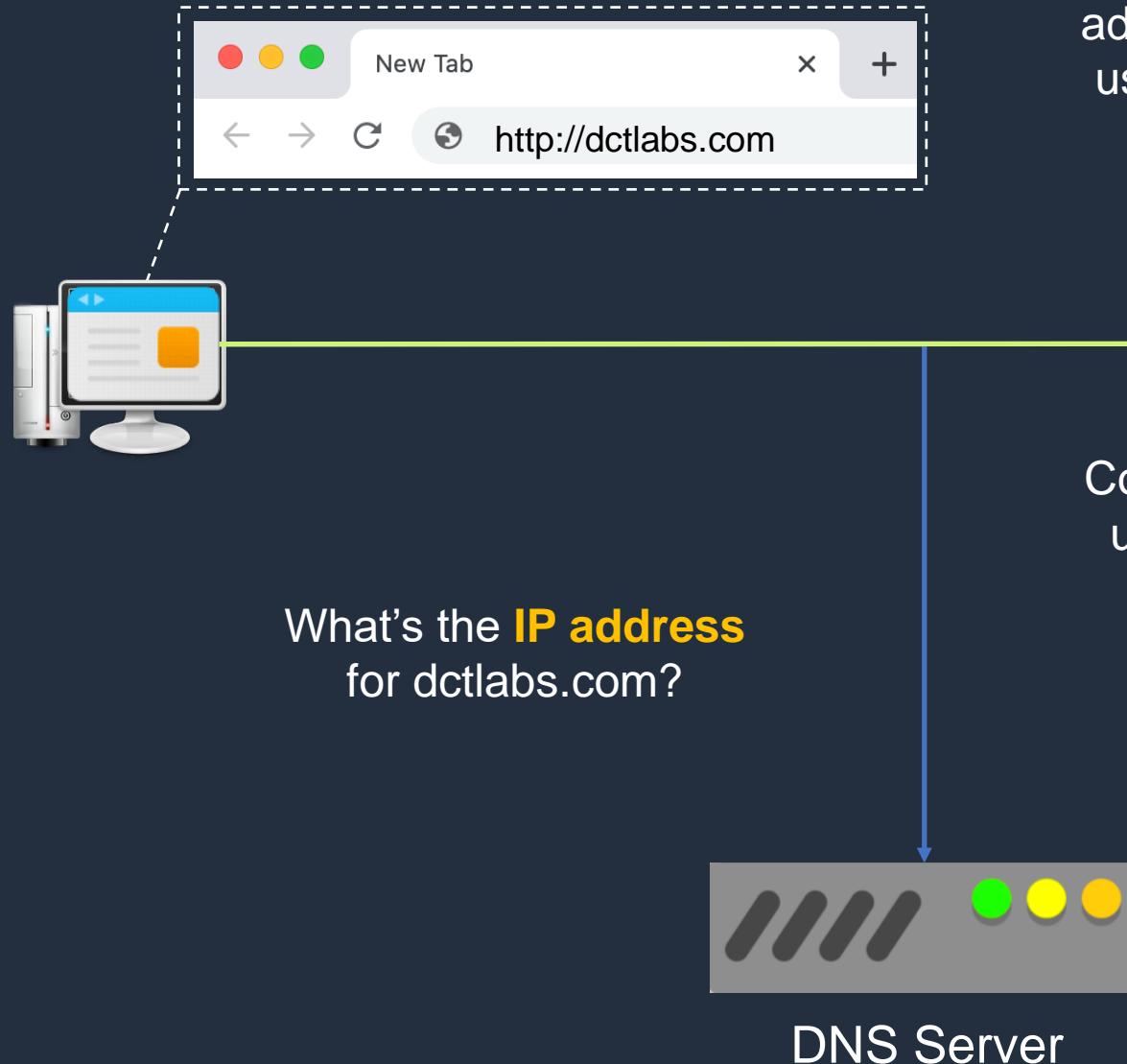
DNS, Elastic Load Balancing, and Auto Scaling

DNS and Amazon Route 53





The Domain Name System



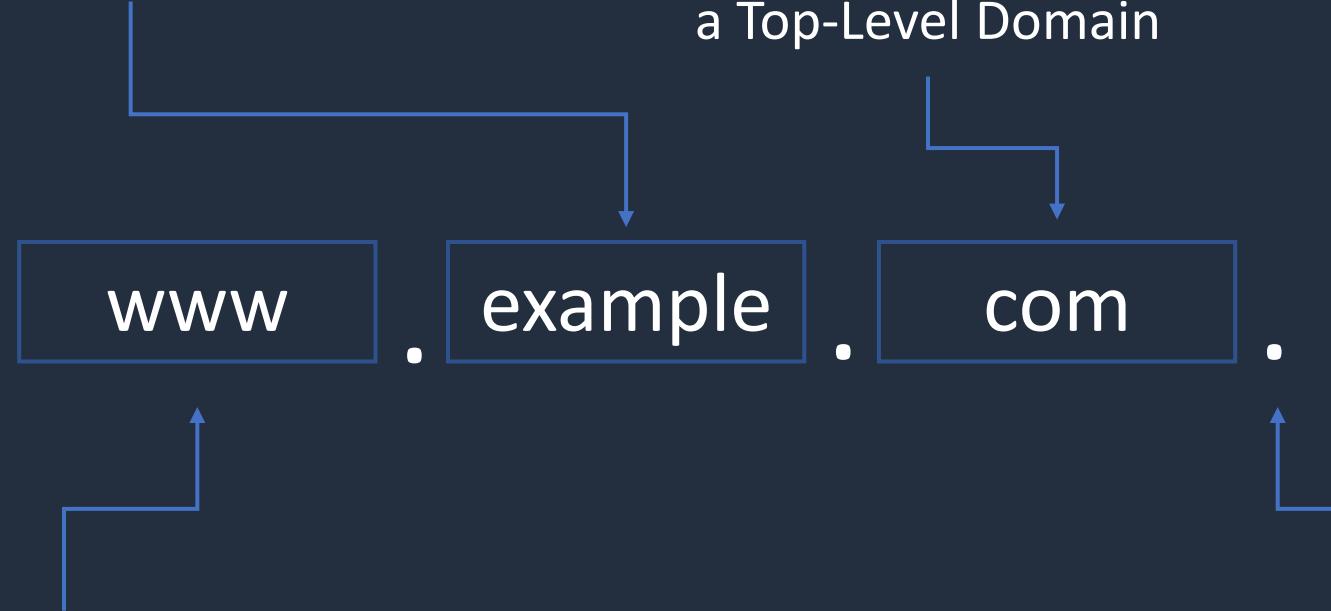
IP addresses are the addresses computers use to communicate



Fully Qualified Domain Names (FQDNs)

Example is a subdomain

com is an example of
a Top-Level Domain



www is a hostname within
the example subdomain

The **root domain** is represented by a
“.” And is not usually visible in a DNS
name



Subdomains

support is a subdomain
of amazon.com

A **subdomain** is subdivision of a domain name for organizing a set of related resources or services



mail is a subdomain
of google.com



DNS Zones and Records

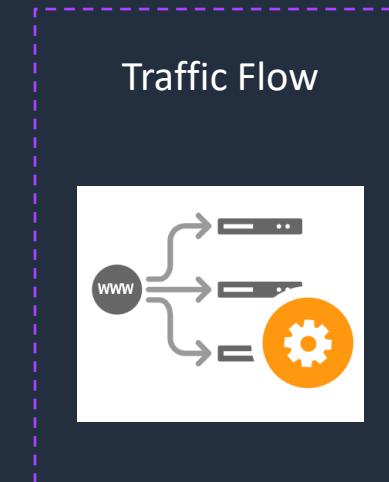
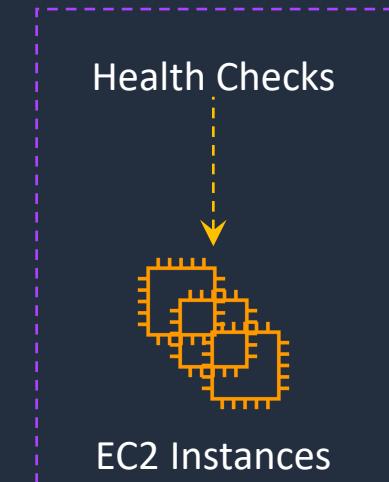
Record Type	Description
A	Maps a domain name to an IP address (e.g. dctlabs.com to 52.23.21.43)
CNAME	Maps a domain name to another domain name (e.g. mail.dctlabs.com to mailserver1.net)
MX	Returns the mail servers for a domain name
TXT	Associates text with a domain name (used for verification, authorization etc.)
SRV	Maps a domain name to a specific service or protocol (e.g. a Kerberos server)
NS	Specifies the authoritative DNS servers for a particular domain
SOA	Start of Authority record stores important information about the domain



Amazon Route 53

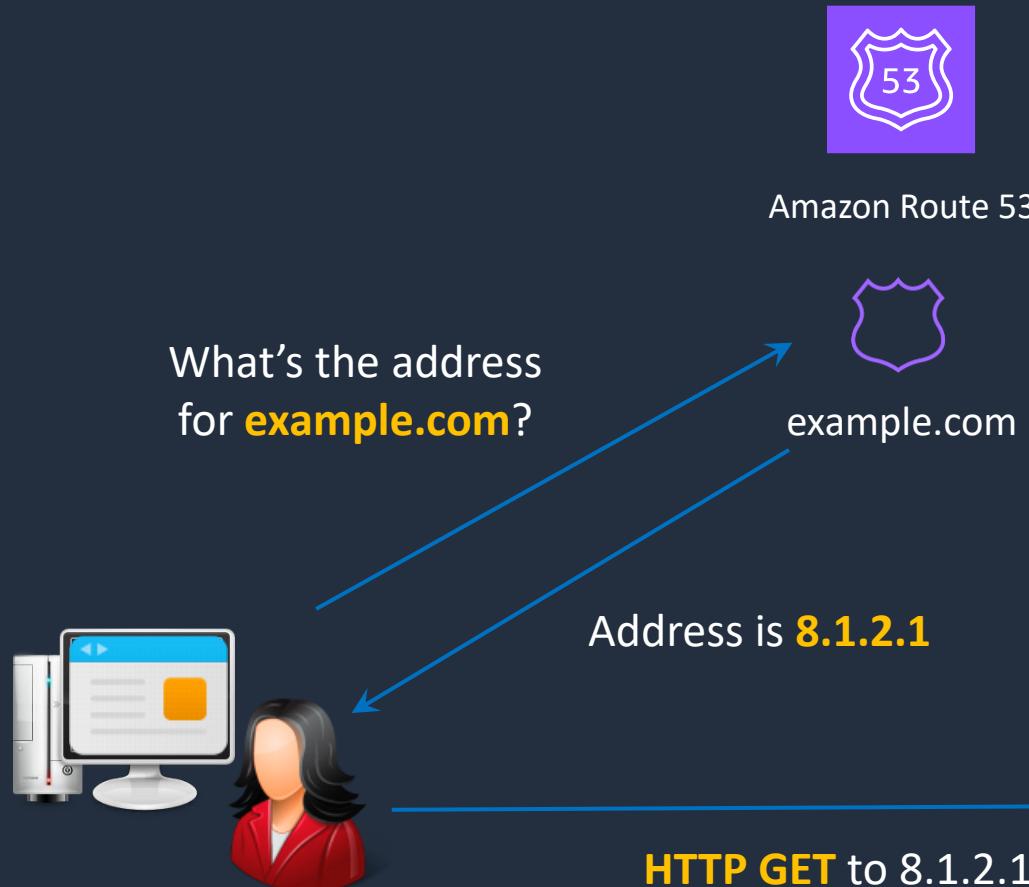


Amazon Route 53

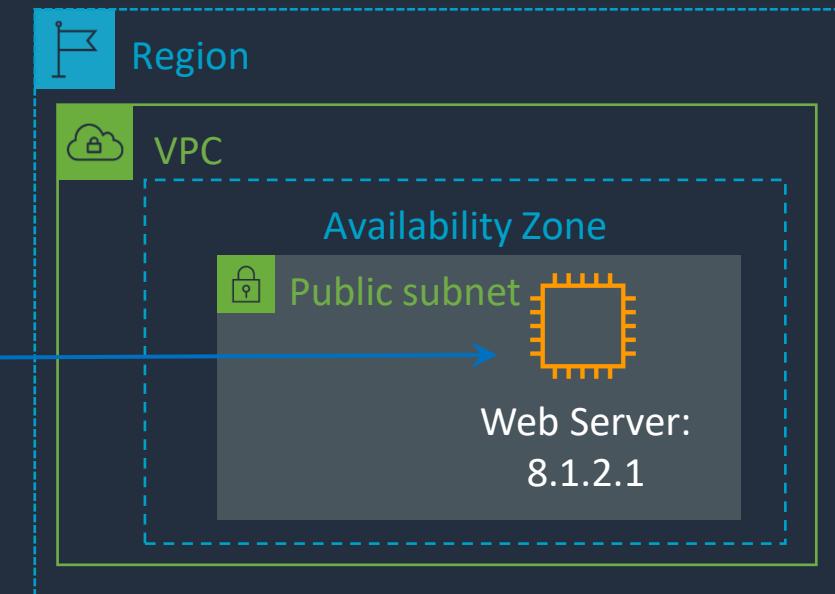




DNS Resolution with Route 53



A **hosted zone** represents a set of records belonging to a domain



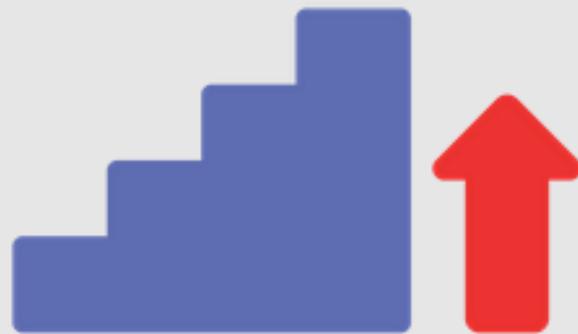
Route 53 Routing Policies

Routing Policy	What it does
Simple	Simple DNS response providing the IP address associated with a name
Failover	If primary is down (based on health checks), routes to secondary destination
Geolocation	Uses geographic location client is in (e.g. Europe) to route to the closest region
Geoproximity	Routes to the closest region within a geographic area
Latency	Directs based on the lowest latency route to resources
Multivalue answer	Returns several IP addresses and functions as a basic load balancer
Weighted	Uses the relative weights assigned to resources
IP Based	Route based on the originating IP address of the traffic

Register Domain with Route 53 (Optional)



Scaling Up vs Scaling Out





Stateful vs Stateless Applications

Stateless

No “state” is recorded about the user's session



Person checks a weather website

Stateful

Amazon stores information about **activity**

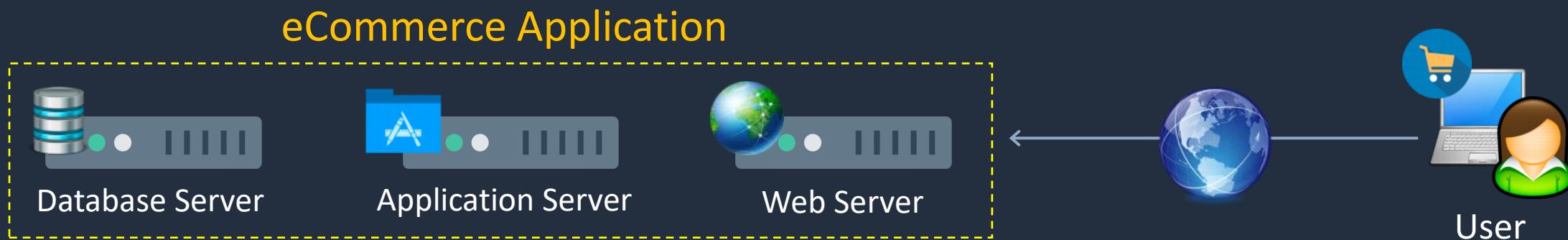


Person browses / purchases on Amazon



Stateful vs Stateless Applications

No data is stored on the web server, it is **stateless**



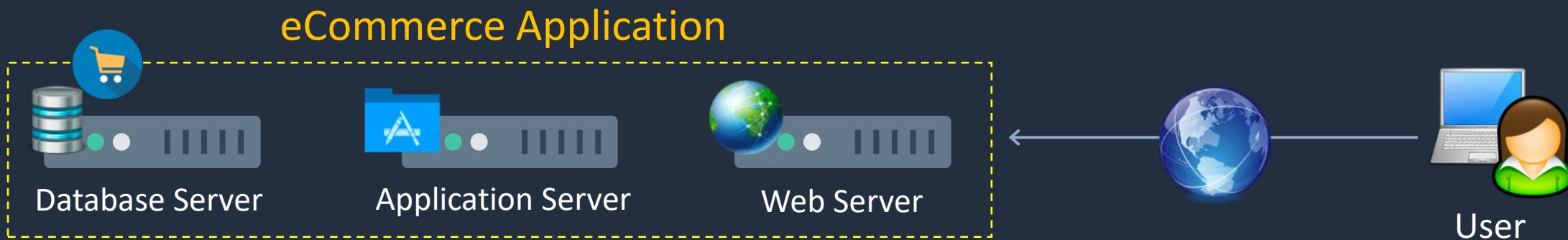
When the user purchases, the application layer processes the order and records the data in the database. This is **stateful**

The cart items are stored in cookies on the computer



Stateful vs Stateless Applications

No data is stored on the web server, it is **stateless**



When the user purchases, the application layer processes the order and records the data in the database. This is **stateful**

The cart items are stored in cookies on the computer



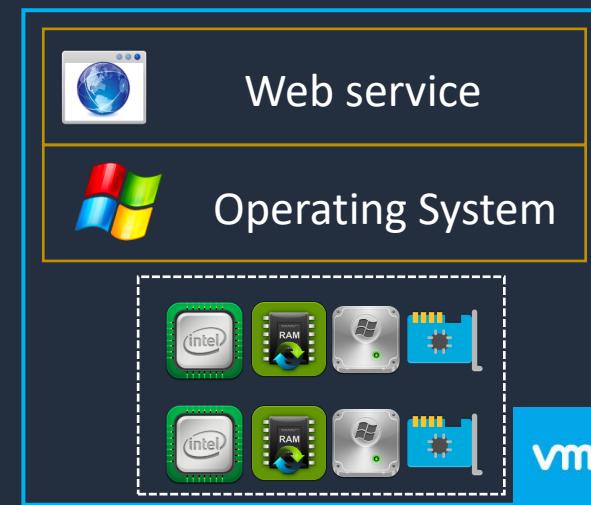
Scalability and Elasticity: Scaling Up





Scalability and Elasticity: Scaling Up

Scaling up means adding resources to the server



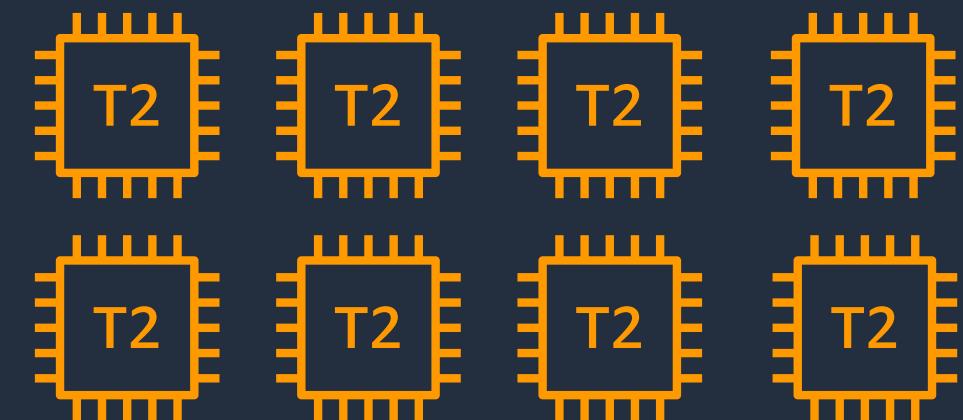
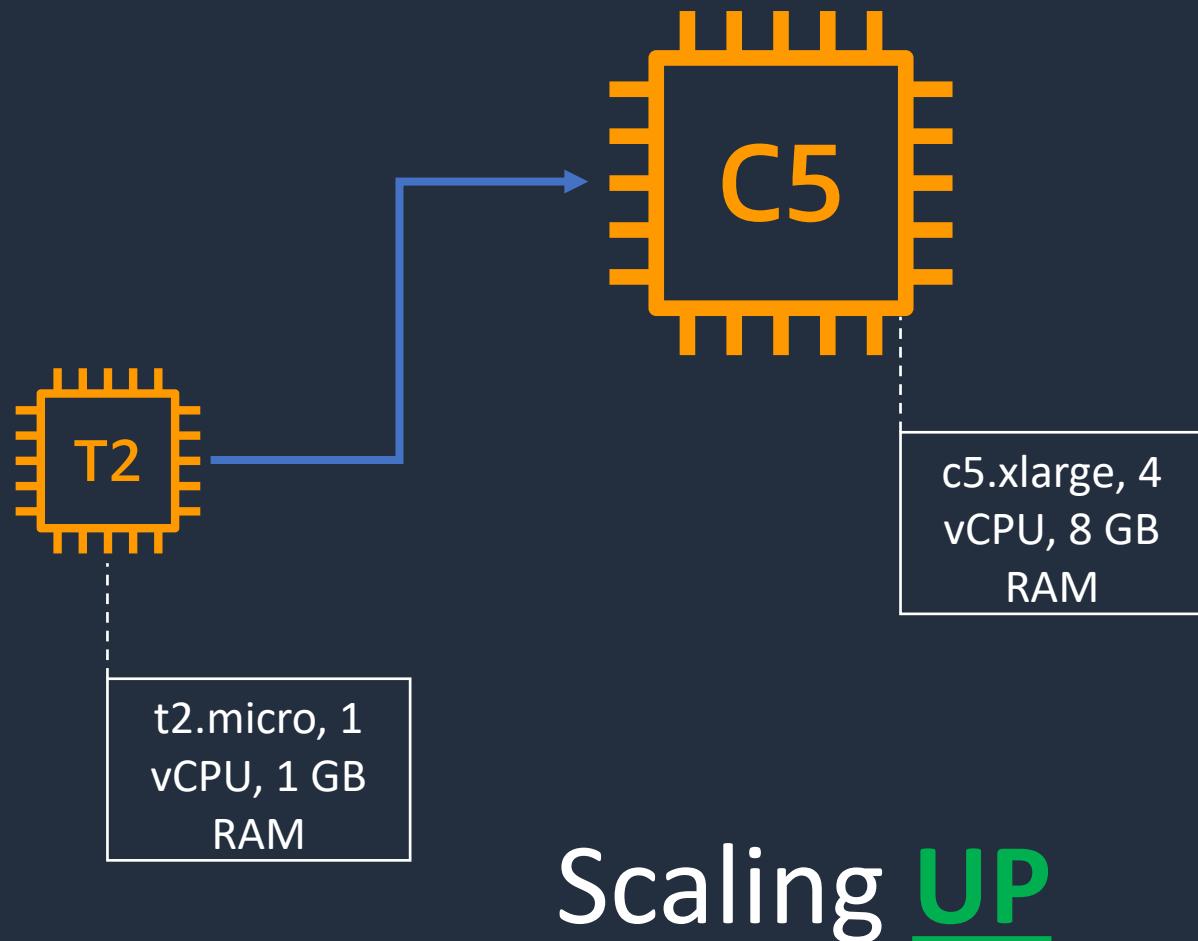


Scalability and Elasticity: Scaling Out





Scaling Up vs Out



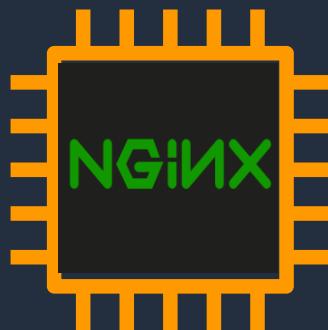


Which scaling model should be used?



Scale UP

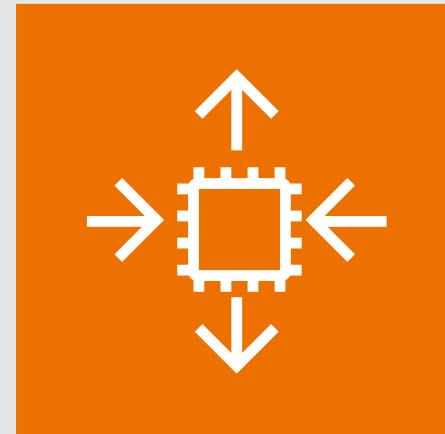
EC2 with MySQL DB



Scale OUT

EC2 with **Static** Website

Amazon EC2 Auto Scaling





Amazon EC2 Auto Scaling

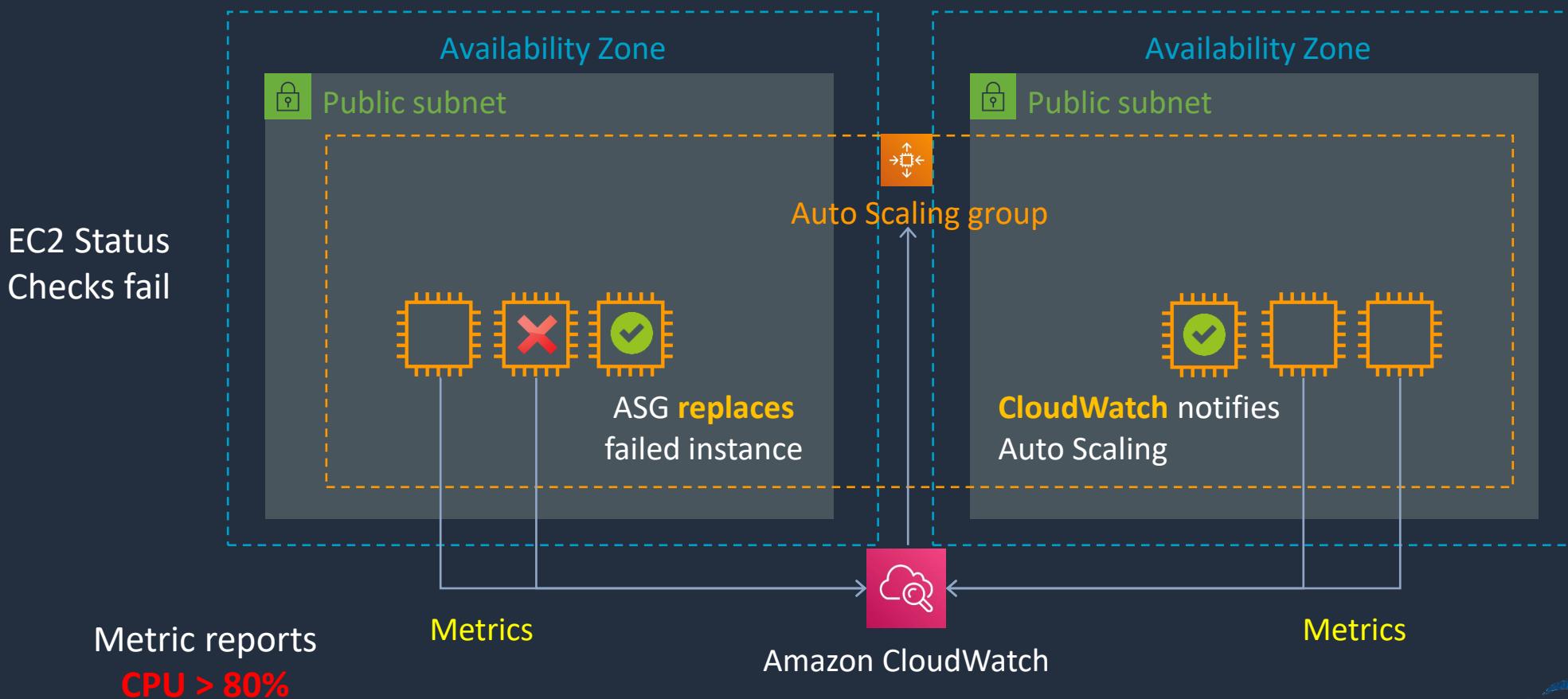
- Automatically **launches** and **terminates** instances
- Maintain **availability** and **scale** capacity
- Works with EC2, ECS, and EKS
- Integrates with many AWS services, including:
 - CloudWatch for monitoring and scaling
 - Elastic Load Balancing for distributing connections
 - EC2 Spot Instances for cost optimization
 - Amazon VPC for deploying instances across AZs



Amazon EC2 Auto Scaling

1. Automatic scaling
2. Maintaining availability

Auto Scaling launches
an extra instance





Amazon EC2 Auto Scaling

- Scaling is horizontal (scales out)
- Provides **elasticity** and **scalability**
- Responds to EC2 status checks and CloudWatch metrics
- Can scale based on demand (performance) or on a schedule
- Scaling policies define how to respond to changes in demand



Configuration of an Auto Scaling Group

A **Launch Template**

specifies the EC2 instance configuration



Launch Template

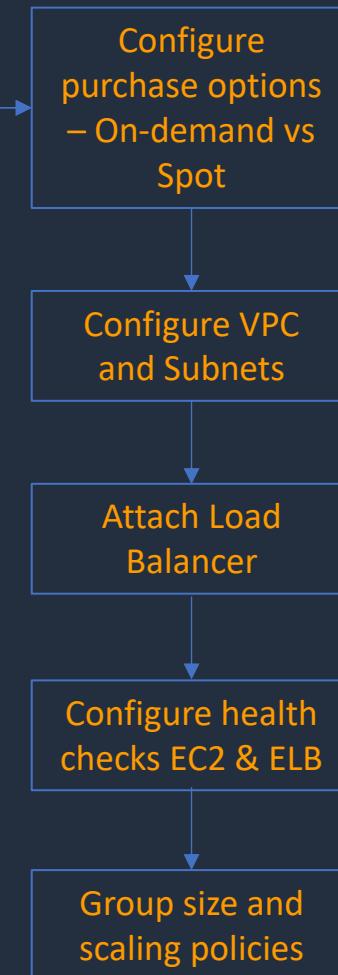
- AMI and instance type
- EBS volumes
- Security groups
- Key pair
- IAM instance profile
- User data
- Shutdown behavior
- Termination protection
- Placement group name
- Capacity reservation
- Tenancy
- Purchasing option (e.g. Spot)



Launch Config

- AMI and instance type
- EBS volumes
- Security groups
- Key pair
- Purchasing option (e.g. Spot)
- IAM instance profile
- User data

Launch Configurations are replaced by launch templates and have fewer features





Amazon EC2 Auto Scaling

- **Health checks**
 - EC2 = EC2 status checks
 - ELB = Uses the ELB health checks **in addition** to EC2 status checks
- **Health check grace period**
 - How long to wait before checking the health status of the instance
 - Auto Scaling does not act on health checks until grace period expires

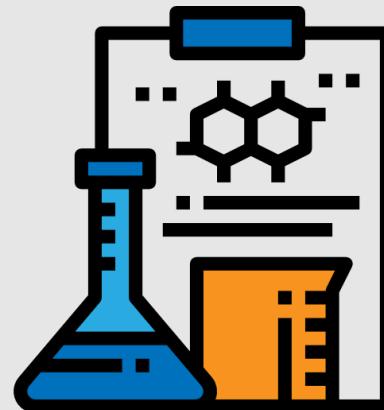


Amazon EC2 Auto Scaling

Types of Auto Scaling:

- **Manual** – make changes to ASG size manually
- **Dynamic** – automatically scales based on demand
- **Predictive** – uses Machine Learning to predict
- **Scheduled** – scales based on a schedule

Create an Auto Scaling Group



Amazon Elastic Load Balancing





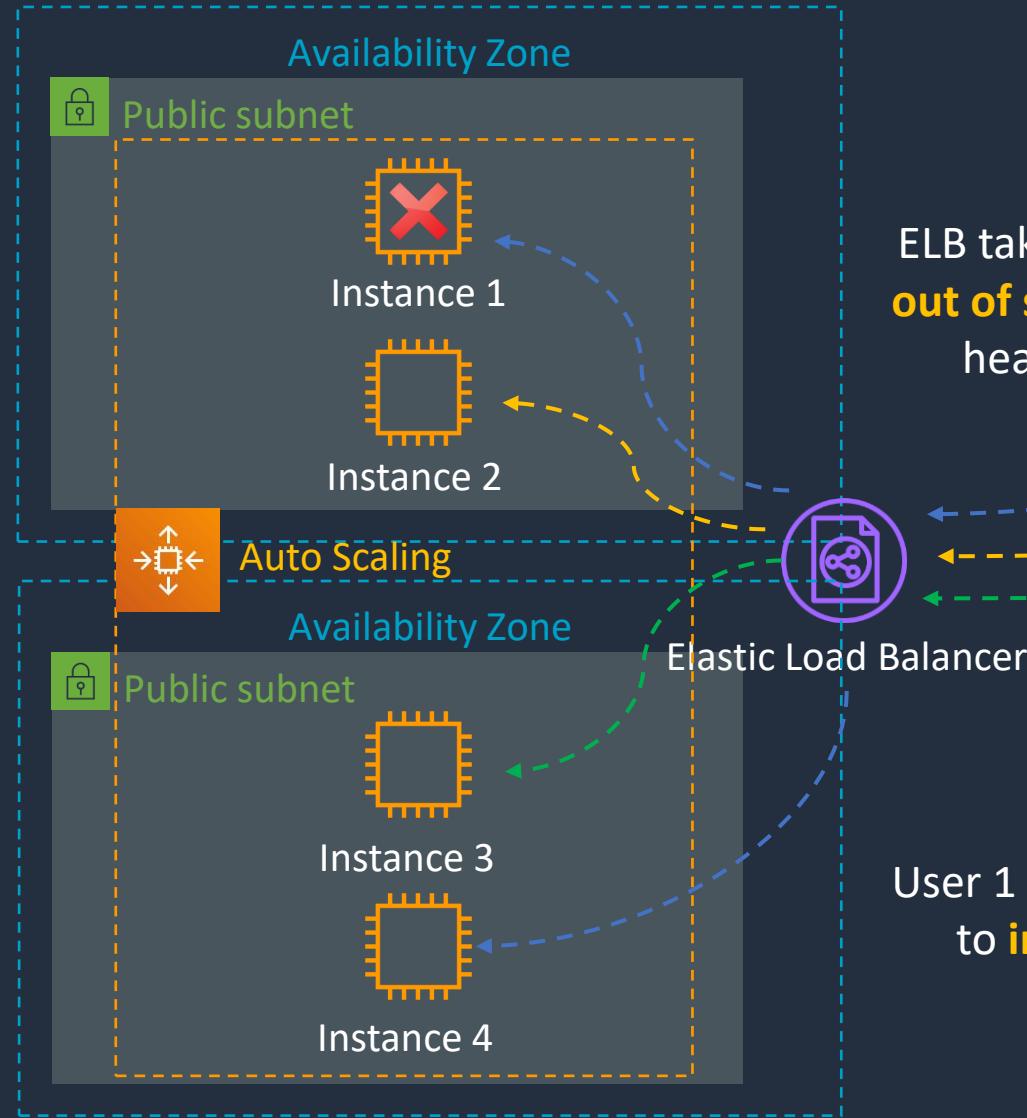
Amazon Elastic Load Balancing

- Provides high availability and fault tolerance
- Targets include:
 - Amazon EC2 instances
 - Amazon ECS containers
 - IP addresses
 - Lambda functions
 - Other load balancers



Amazon Elastic Load Balancing

EC2 Auto Scaling
terminates
instance 1



ELB takes instance 1
out of service (failed
health check)

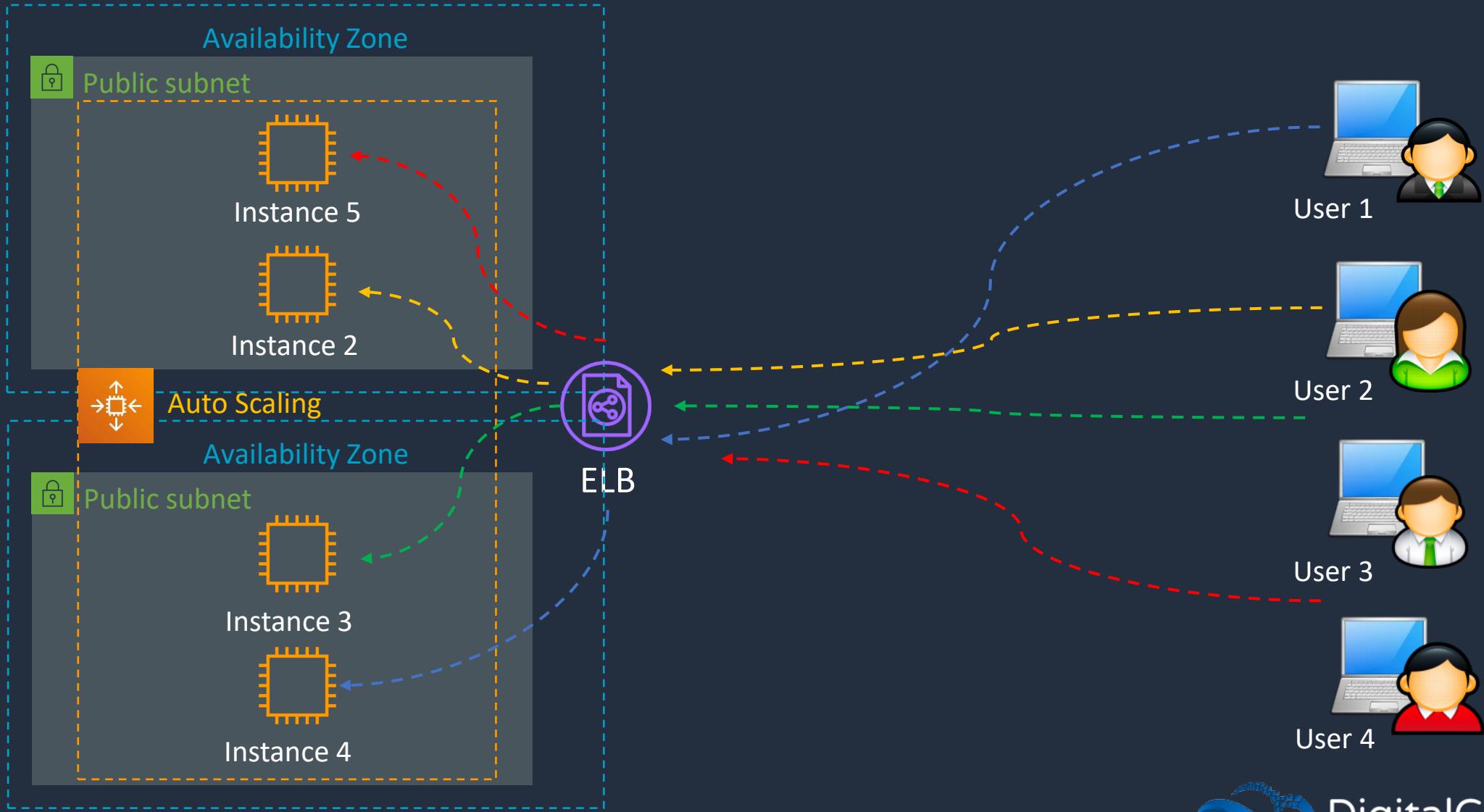
User 1 is connected
to **instance 4**





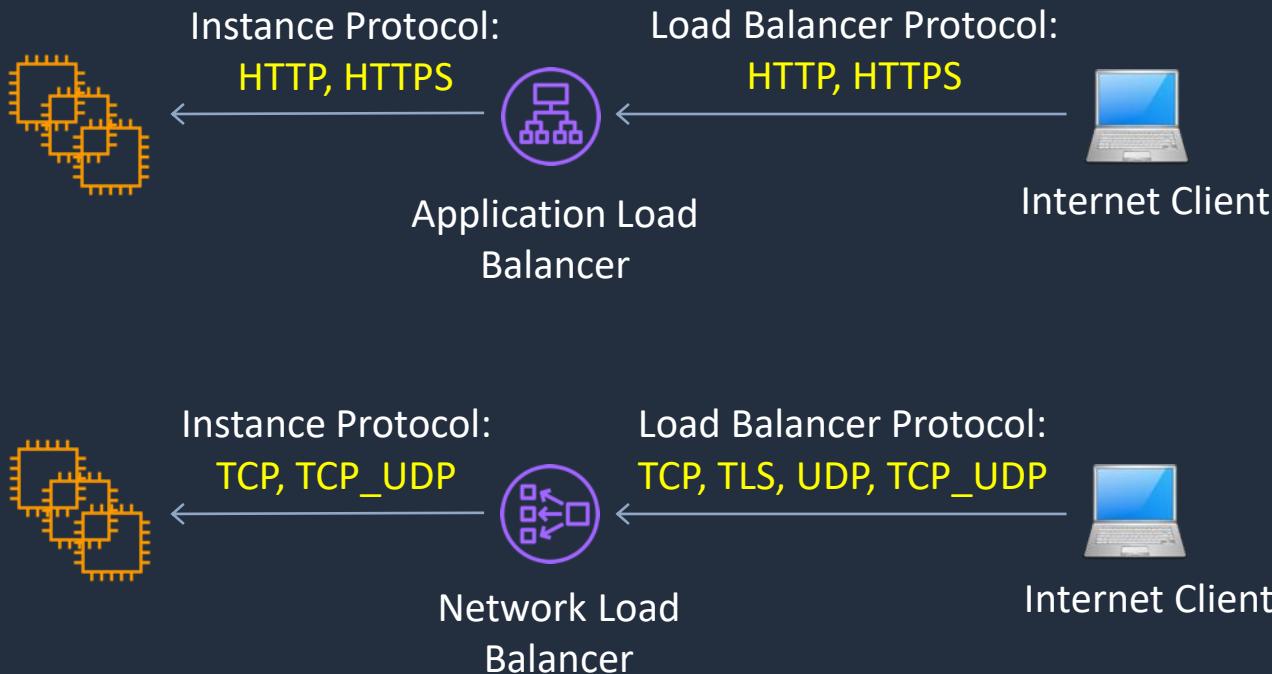
Amazon Elastic Load Balancing

EC2 Auto Scaling
launches
instance 5





Types of Elastic Load Balancer (ELB)



Application Load Balancer

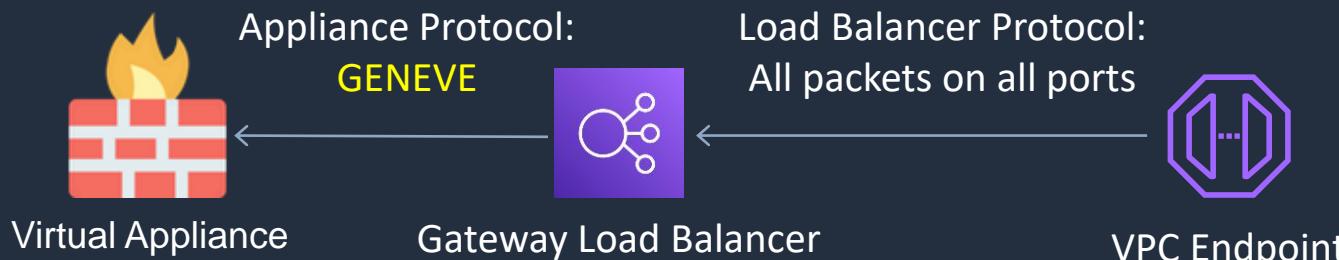
- Operates at the request level
- Routes based on the content of the request (L7)
- Supports path-based routing, host-based routing, query string parameter-based routing, and source IP address-based routing
- Supports instances, IP addresses, Lambda functions and containers as targets

Network Load Balancer

- Operates at the connection level
- Routes connections based on IP protocol data (L4)
- Offers ultra high performance, low latency and TLS offloading at scale
- Can have a static IP / Elastic IP
- Supports UDP and static IP addresses as targets



Types of Elastic Load Balancer (ELB)



Gateway Load Balancer

- Used in front of virtual appliances such as firewalls, IDS/IPS, and deep packet inspection systems
- Operates at Layer 3 – listens for all packets on all ports
- Forwards traffic to the TG specified in the listener rules
- Exchanges traffic with appliances using the GENEVE protocol on port 6081



ELB Use Cases

Application Load Balancer

- Web applications with L7 routing (HTTP/HTTPS)
- Microservices architectures (e.g. Docker containers)
- Lambda targets

Network Load Balancer

- TCP and UDP based applications
- Ultra-low latency
- Static IP addresses
- VPC endpoint services



ELB Use Cases

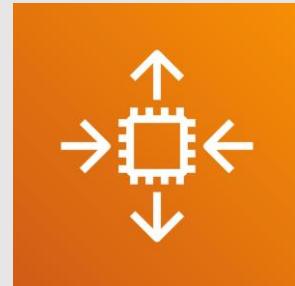
Gateway Load Balancer

- Deploy, scale and manage 3rd party virtual network appliances
- Centralized inspection and monitoring
- Firewalls, intrusion detection and prevention systems, and deep packet inspection systems

Create an Application Load Balancer



Scaling Policies

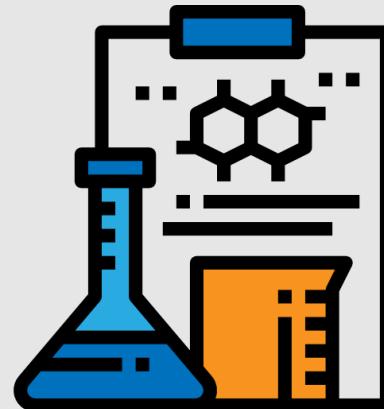




Scaling Policies

- **Target Tracking** – Attempts to keep the group at or close to the metric
- **Simple Scaling** – Adjust group size based on a metric
- **Step Scaling** – Adjust group size based on a metric – adjustments vary based on the size of the alarm breach
- **Scheduled Scaling** – Adjust the group size at a specific time

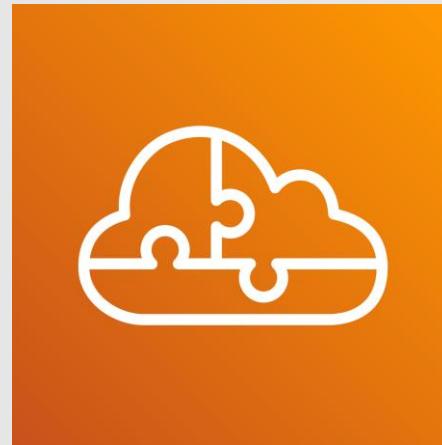
Create a Scaling Policy



SECTION 8

Application Services

Serverless Services and Event-Driven Architecture



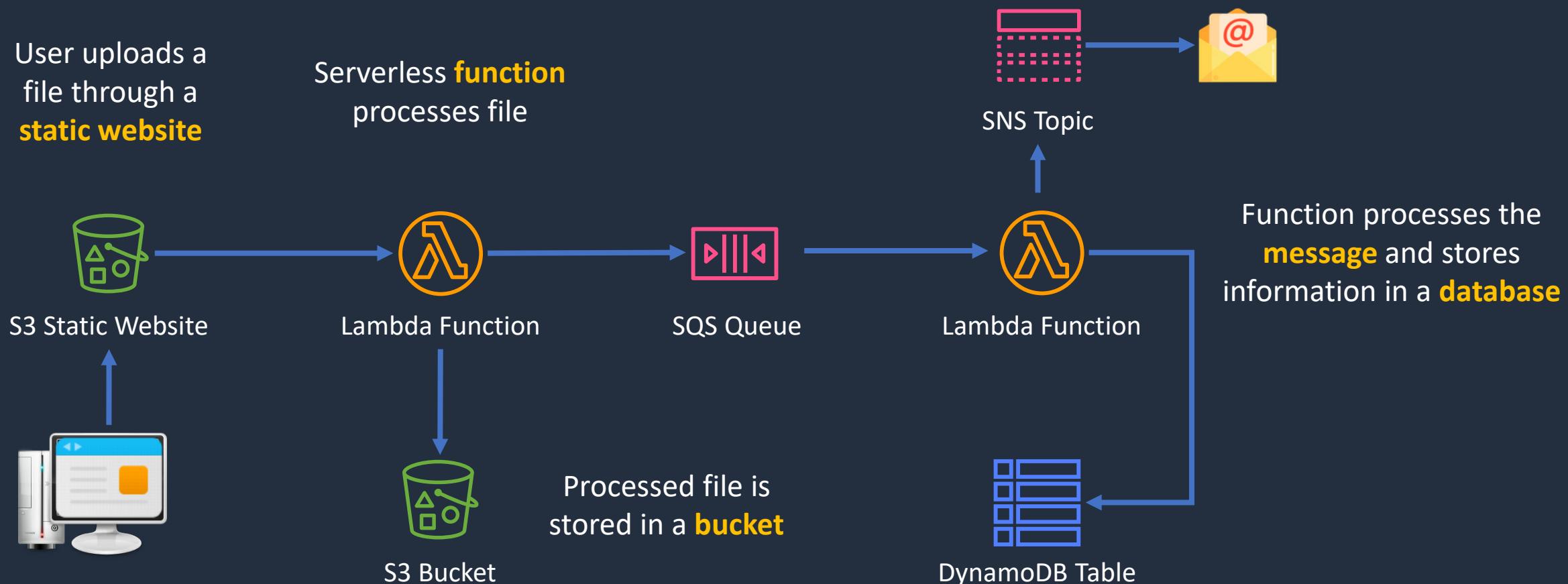


Serverless Services

- With serverless there are **no instances** to manage
- You don't need to provision hardware
- There is no management of operating systems or software
- Capacity provisioning and patching is handled automatically
- Provides automatic scaling and high availability
- Can be very cheap!



Serverless Services and Event-Driven Architecture



AWS Lambda





AWS Lambda

Pricing is based on memory assigned and the duration of function execution

Functions are invoked based on **events** and the code is then executed

```
import json

def lambda_handler(event, context):
    # Print the event to CloudWatch Logs
    print("Received event: " + json.dumps(event))

    # Return a response
    return {
        'statusCode': 200,
        'body': json.dumps('Event logged successfully!')
    }
```

Code is executed





AWS Lambda

- **Languages** – Lambda natively supports Java, Go, PowerShell, Node.js, C#, Python, and Ruby code
- **Execution Role (IAM Role)** – this role grants the function permissions to access AWS services and resources
- **Monitoring and Logging** – integrates with Amazon CloudWatch
- **Memory and Timeout** – you can specify the amount of memory allocated to a function and the maximum execution time
- **Note:** The maximum execution time is 15 minutes



Lambda Function Invocation

- Lambda functions run in response to events from various AWS services or direct invocation from the AWS SDKs or API
- Functions can be invoked synchronously or asynchronously:
 - With **synchronous** invocation, applications wait for the function to process the event and return a response
 - With **asynchronous** invocation, Lambda queues the event for processing and returns a response immediately
- Lambda scales horizontally by running multiple instances of a function in parallel, up to the concurrency limit





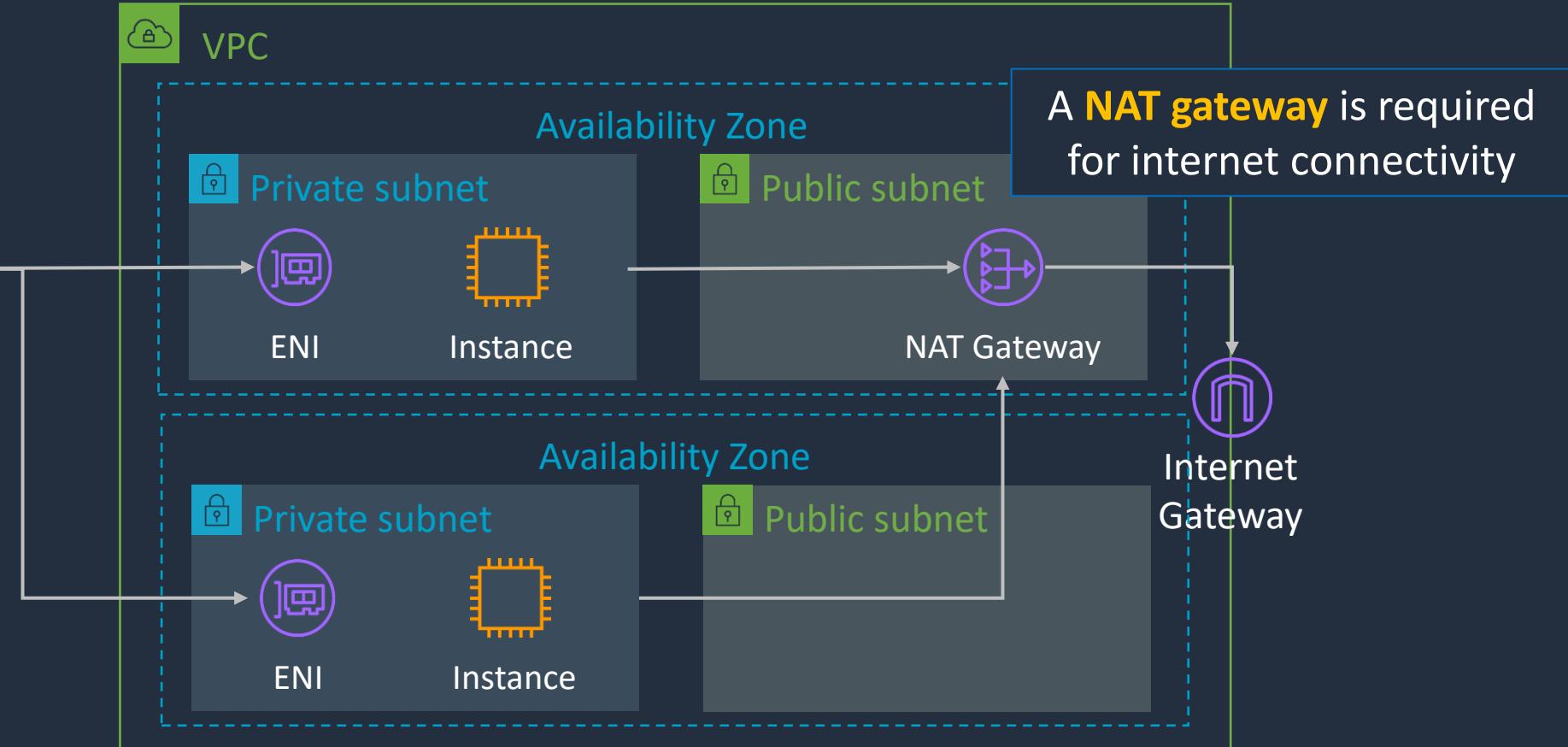
Connecting Lambda to an Amazon VPC

Must select the VPC, subnets,
and security group

Lambda functions are
Regional and do not have
VPC access by default



Lambda functions can be
connected to a VPC

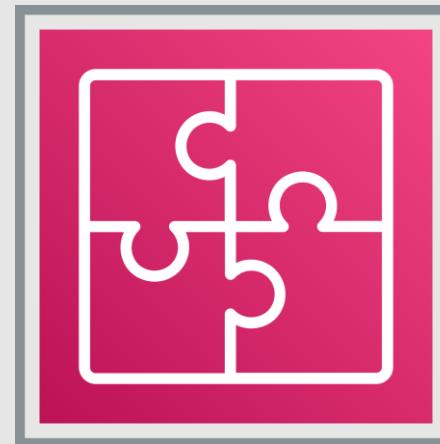


The function **execution role** must have
permissions create the ENIs

Create an AWS Lambda Function

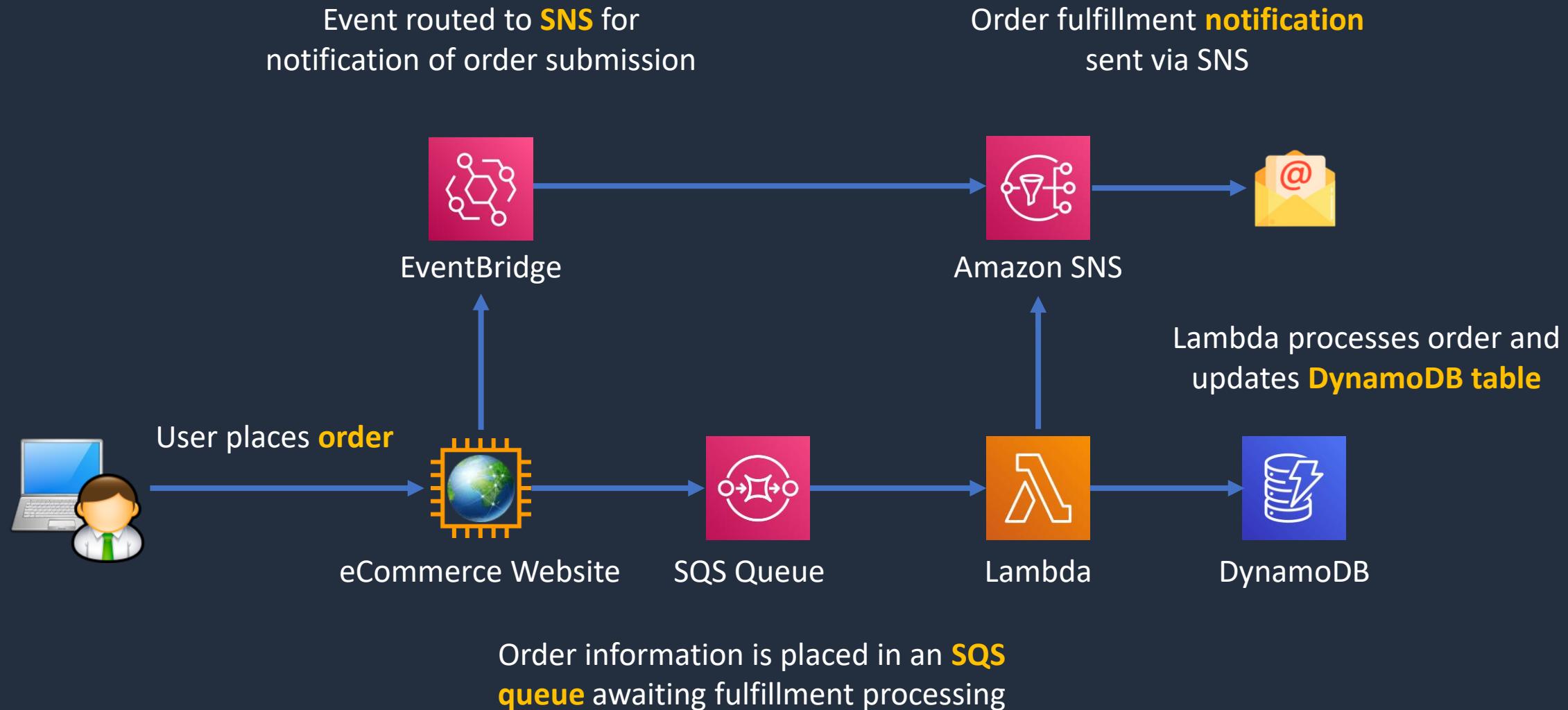


Application Integration Services



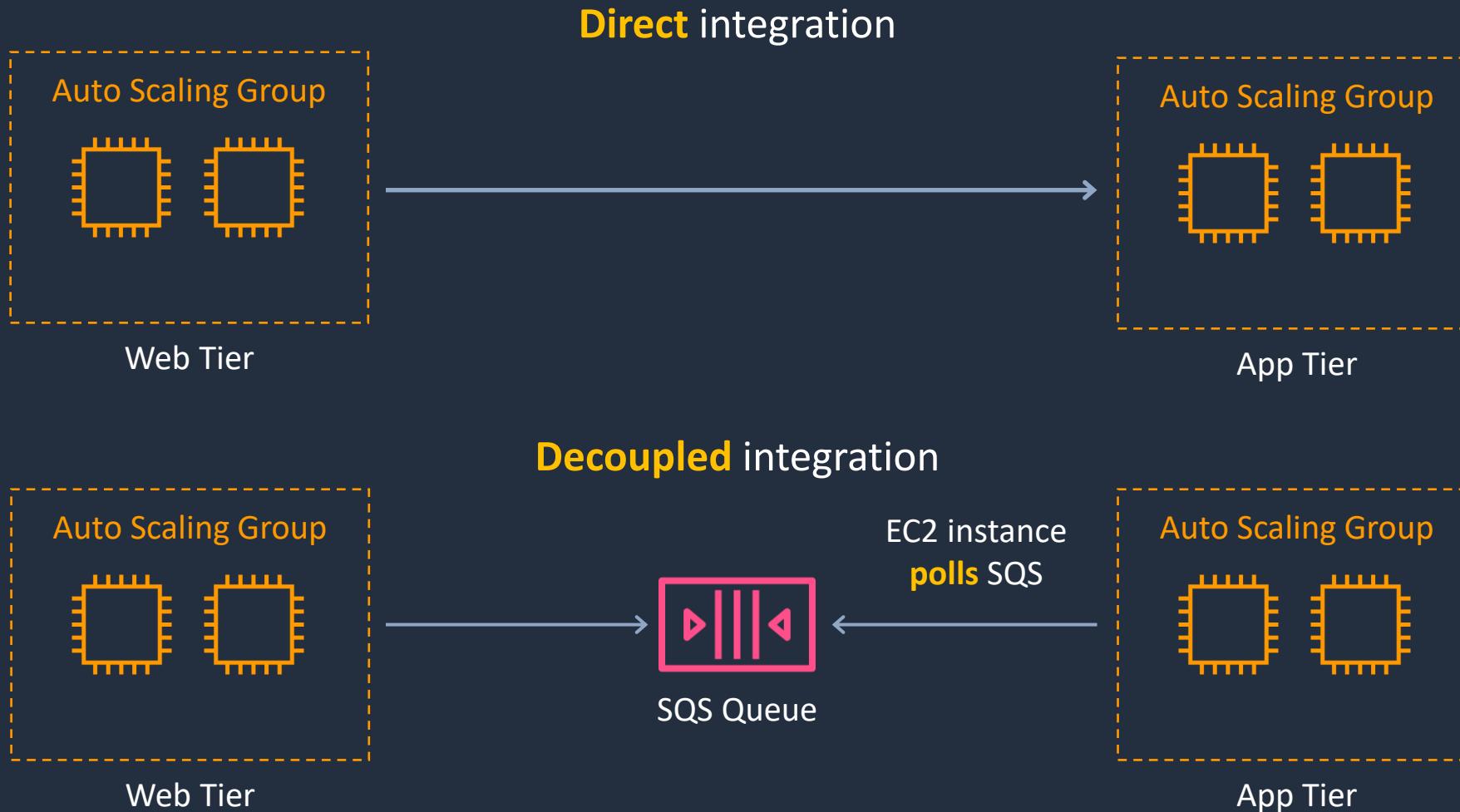


Event-Driven Architecture



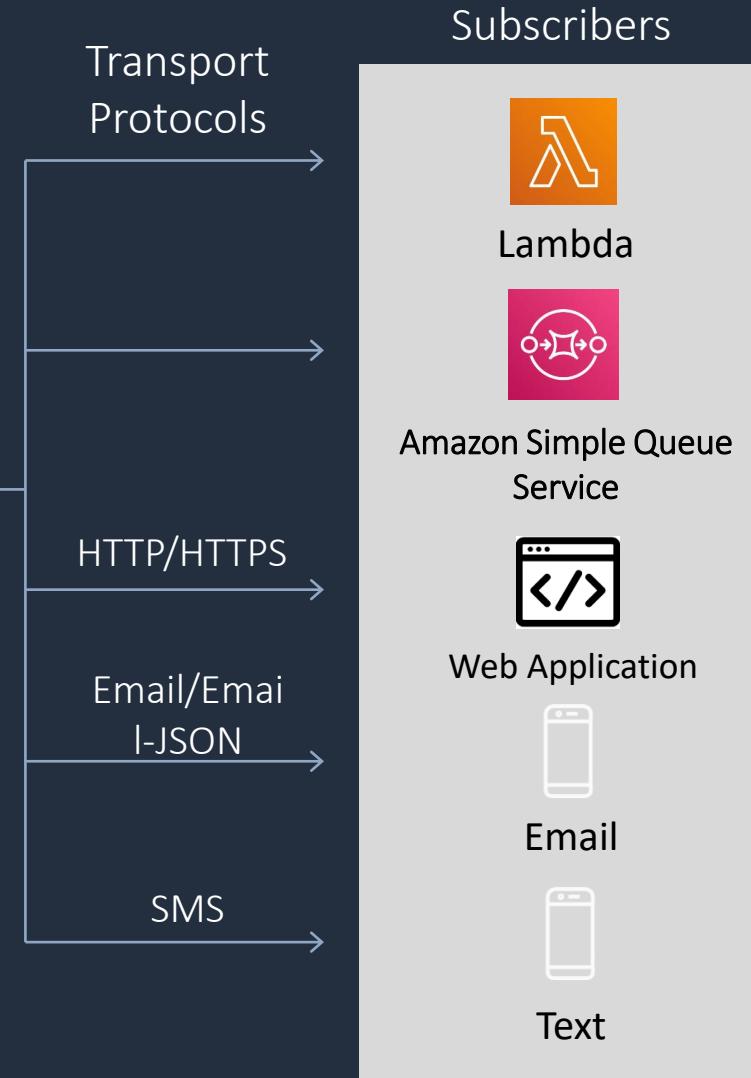
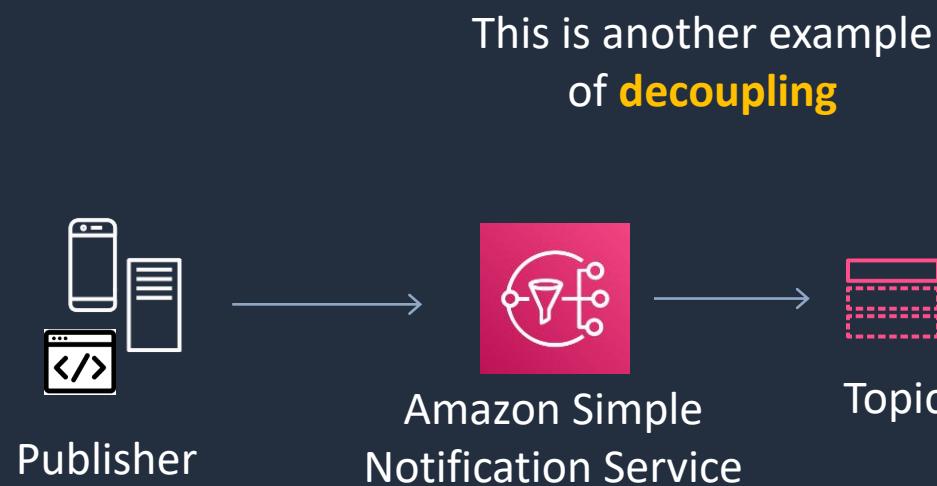


Amazon Simple Queue Service (SQS)





Amazon Simple Notification Service (SNS)

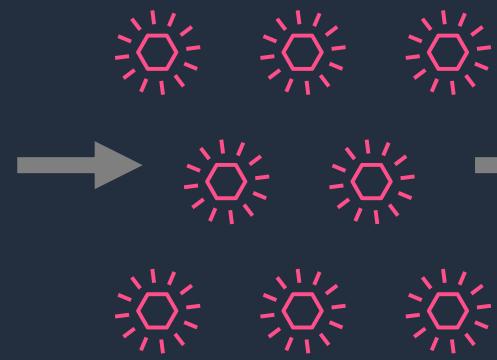




Amazon EventBridge

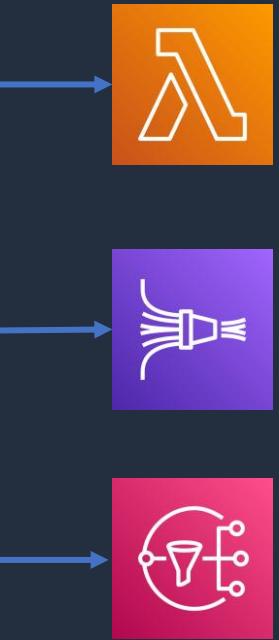
Amazon EventBridge is a serverless event bus that connects
loosely coupled application components together

Event Sources



EventBridge
event bus

Rules





Application Integration Services Comparison

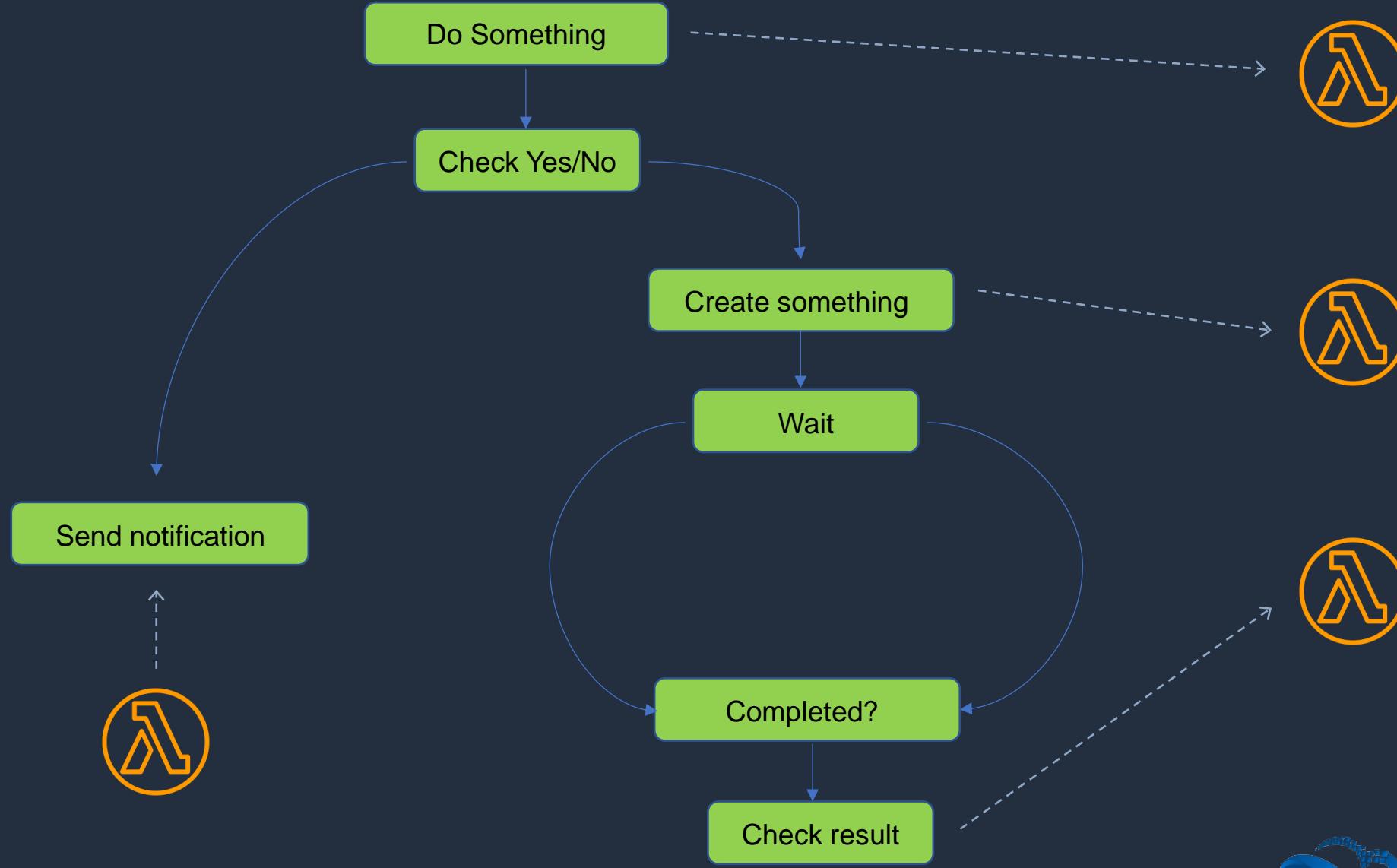
Service	What it does	Example use cases
Simple Queue Service	Messaging queue; store and forward patterns	Building distributed / decoupled applications
Simple Notification Service	Set up, operate, and send notifications from the cloud	Send email notification when CloudWatch alarm is triggered
Step Functions	Coordination of AWS services with visual workflow	Order processing workflows
Amazon MQ	Message broker service for Apache Active MQ and RabbitMQ	Need a message queue that supports industry standard APIs and protocols
Amazon EventBridge	Serverless event bus for connecting applications and AWS services	Create event driven applications

AWS Step Functions





AWS Step Functions





AWS Step Functions

- AWS Step Functions is used to build distributed applications as a series of steps in a visual workflow.
- You can quickly build and run state machines to execute the steps of your application

How it works:

1. Define the steps of your workflow in the **JSON-based Amazon States Language**.
The visual console automatically graphs each step in the order of execution
2. Start an execution to visualize and verify the steps of your application are operating as intended. The console highlights the real-time status of each step and provides a detailed history of every execution
3. AWS Step Functions **operates and scales** the steps of your **application** and **underlying compute** for you to help ensure your application executes reliably under increasing demand

Amazon EventBridge / CloudWatch Events





Amazon EventBridge

EventBridge used to be known as **CloudWatch Events**

Event Source



Rule

Send **SNS** notification



EventBridge
event bus

Event

Target





Amazon EventBridge

Event matching pattern
You can use pre-defined pattern provided by a service or create a custom pattern

Pre-defined pattern by service
 Custom pattern

Service provider
AWS services or custom/partner services

AWS

Service name
The name of partner service selected as the event source

EC2

Event type
The type of events as the source of the matching pattern

EC2 Instance State-change Notification

Any state
 Specific state(s)

terminated X

Any instance
 Specific instance Id(s)

i-1234567890abcdef0

Event pattern

Copy Edit

```
1 {
2     "source": ["aws.ec2"],
3     "detail-type": ["EC2 Instance State-change Notification"]
4     "detail": {
5         "state": ["terminated"],
6         "instance-id": ["i-1234567890abcdef0"]
7     }
8 }
```

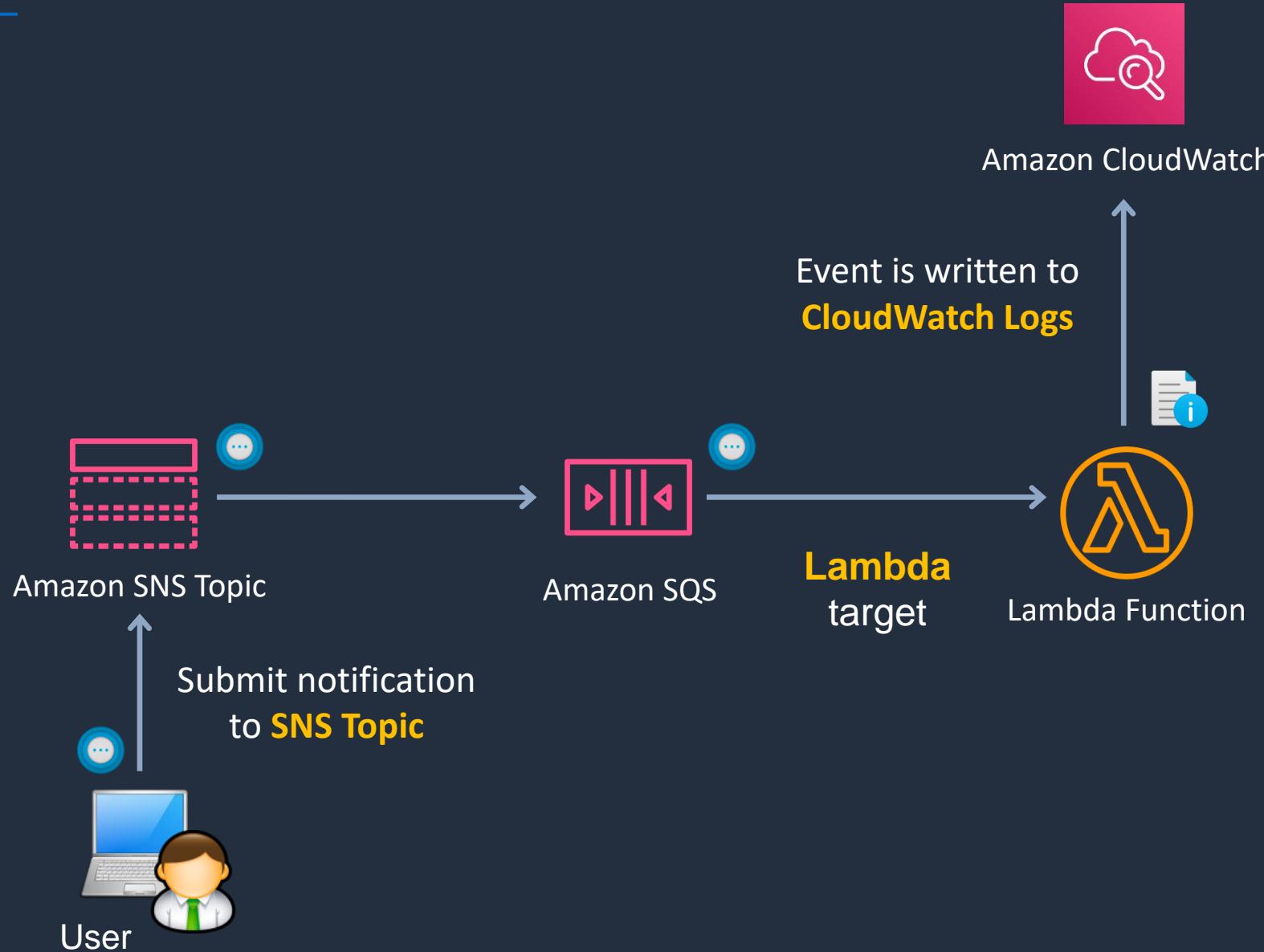
```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "EC2 Instance State-change Notification",
    "source": "aws.ec2",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-west-1",
    "resources": [
        "arn:aws:ec2:us-west-1:123456789012:instance/i-1234567890abcdef0"
    ],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "state": "terminated"
    }
}
```

Create an Event-Driven Application

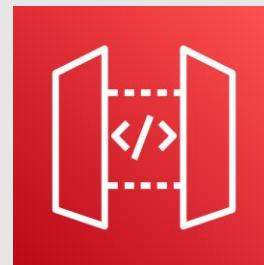




Simple Event-Driven Application

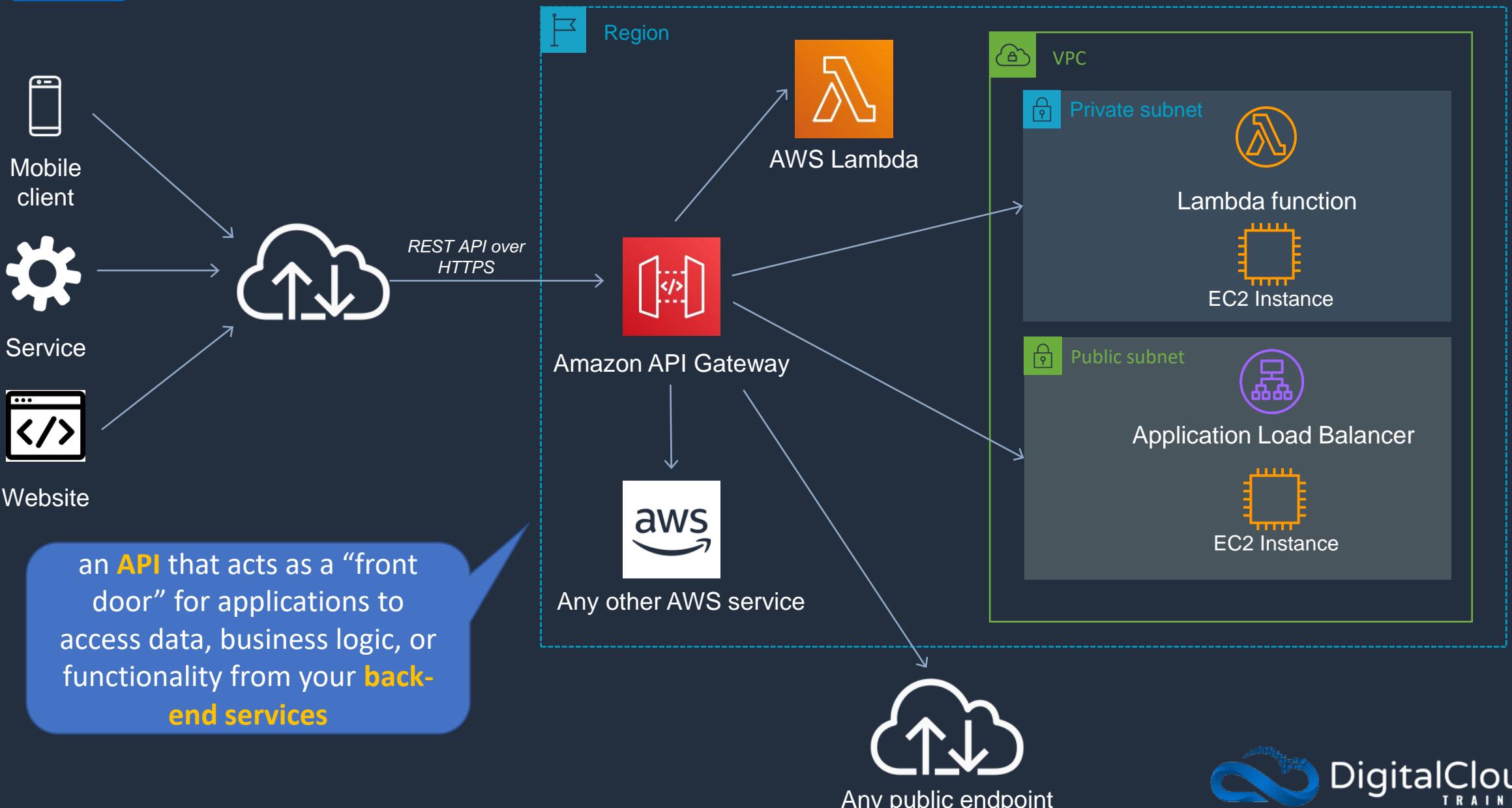


Amazon API Gateway





Amazon API Gateway



SECTION 9

Amazon VPC, Networking, and Hybrid

Amazon Virtual Private Cloud (VPC)

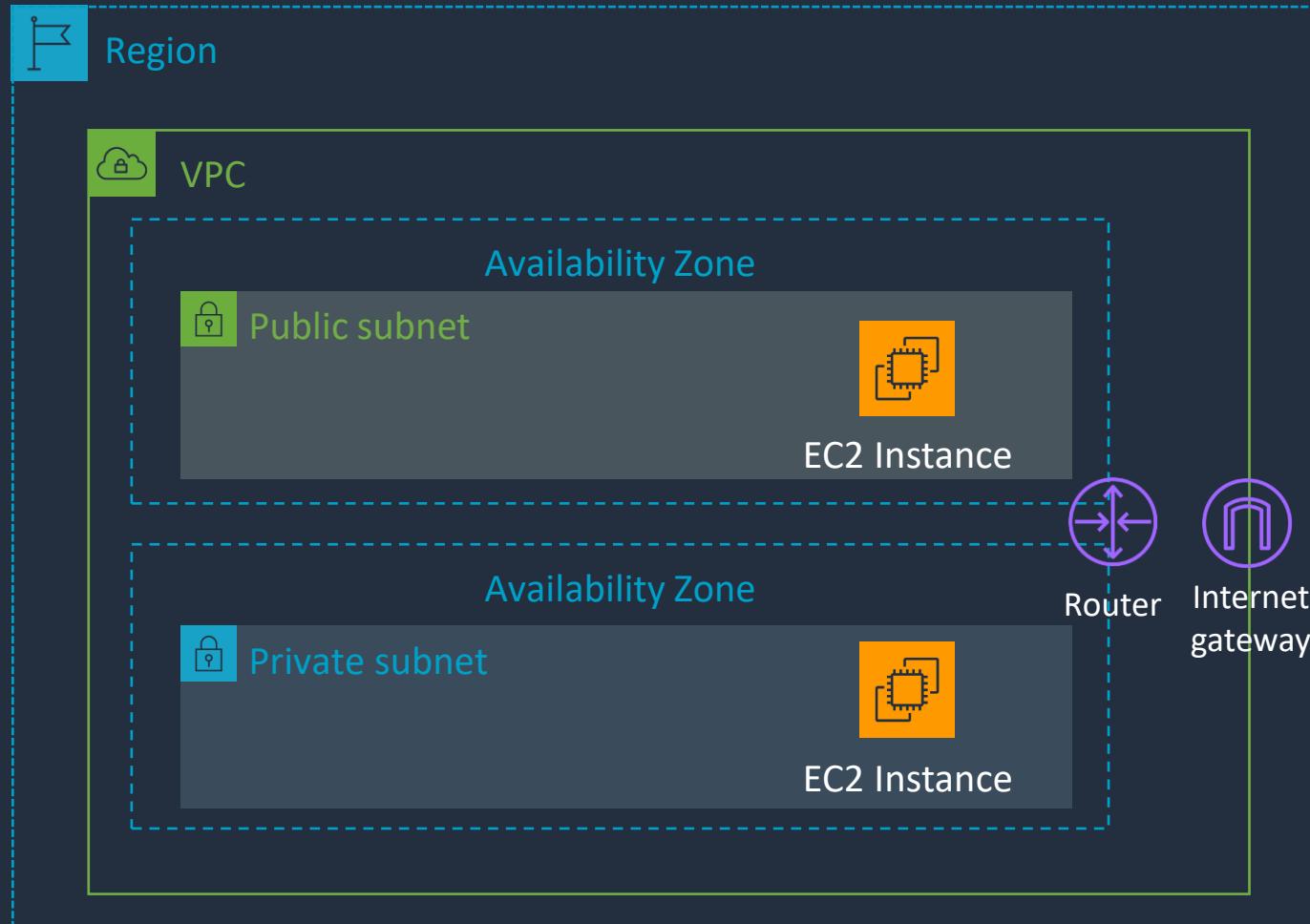




Amazon VPC

A **VPC** is a logically isolated portion of the AWS cloud within a region

Subnets are created within **AZs**



You can launch **EC2 instances** into your VPC subnets

Main Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

The **route table** is used to configure the VPC router

An **Internet Gateway** is used to connect to the Internet



Amazon VPC

Each **VPC** has a different block of IP addresses

CIDR stands for Classless Interdomain Routing



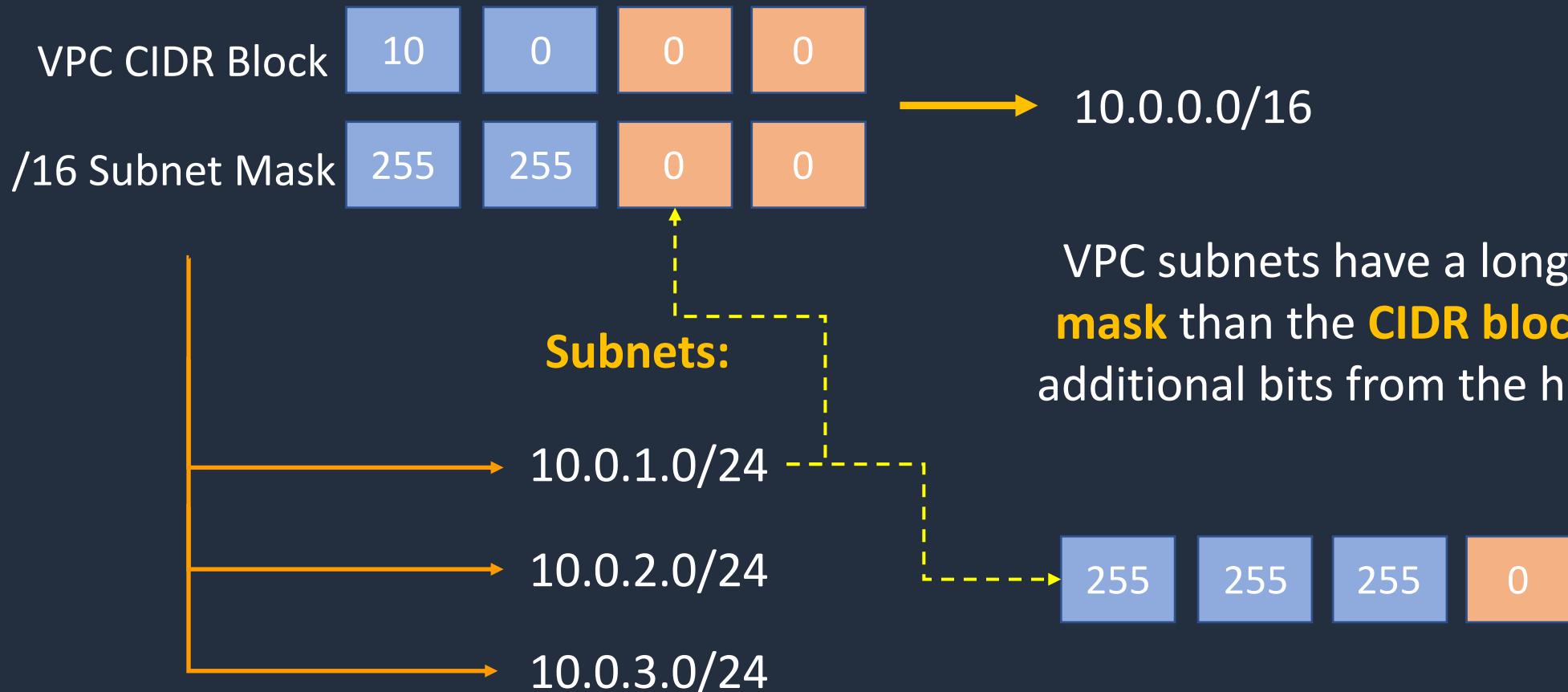
Each subnet has a block of **IP addresses** from the CIDR block



You can create **multiple VPCs** within each region



VPC CIDR Blocks and Subnets

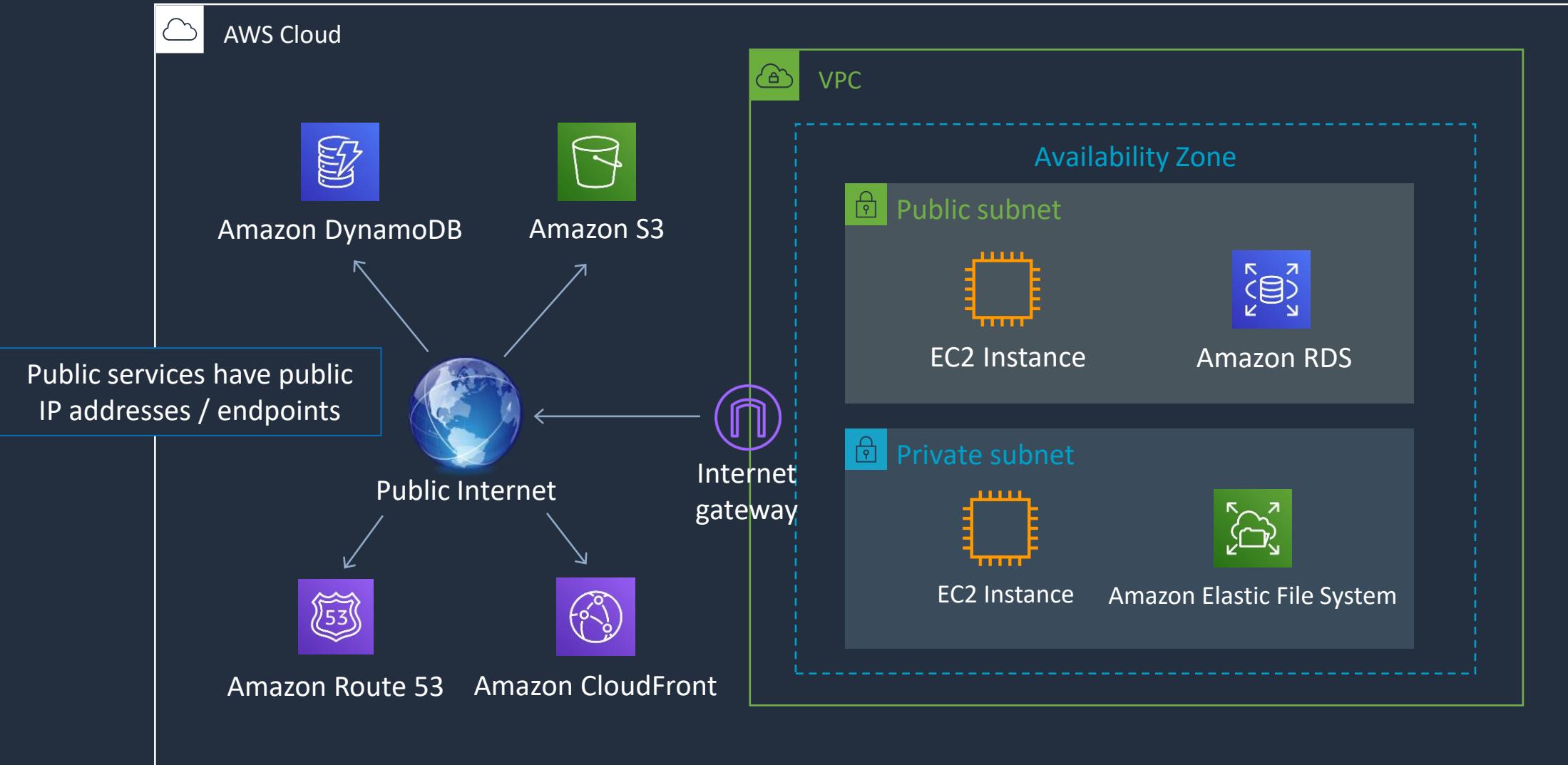


VPC subnets have a longer **subnet mask** than the **CIDR block** by using additional bits from the host portion



AWS Public and Private Services

Private services can have public IP addresses but exist within the VPC

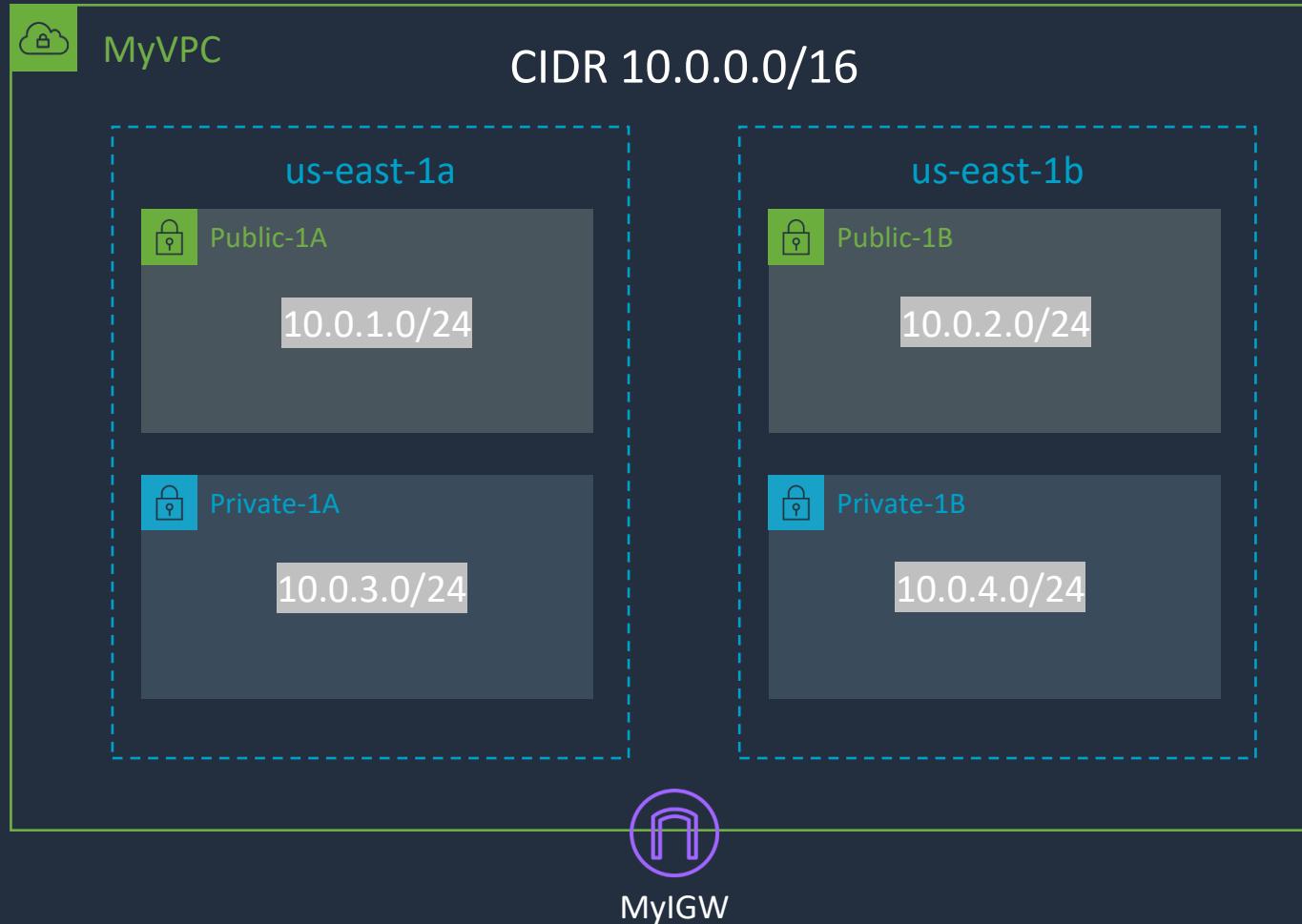


Create a Custom VPC





Custom VPC



Main Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Private-RT Route Table

Destination	Target
10.0.0.0/16	Local

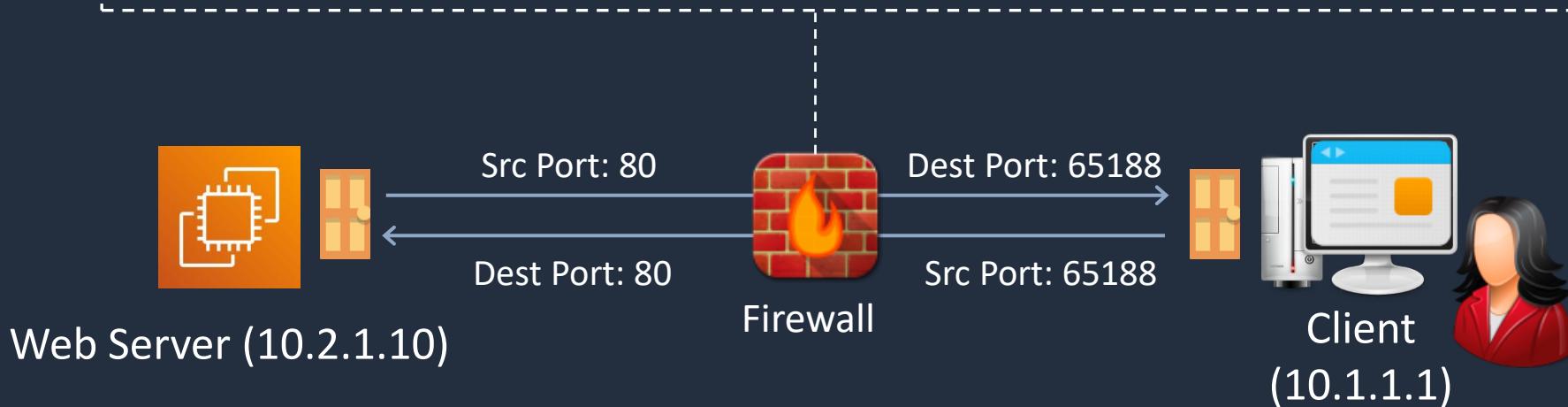
Security Groups and Network ACLs





Stateful vs Stateless Firewalls

PROTOCOL	SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT
HTTP	10.1.1.1	10.2.1.10	65188	80
HTTP	10.2.1.10	10.1.1.1	80	65188

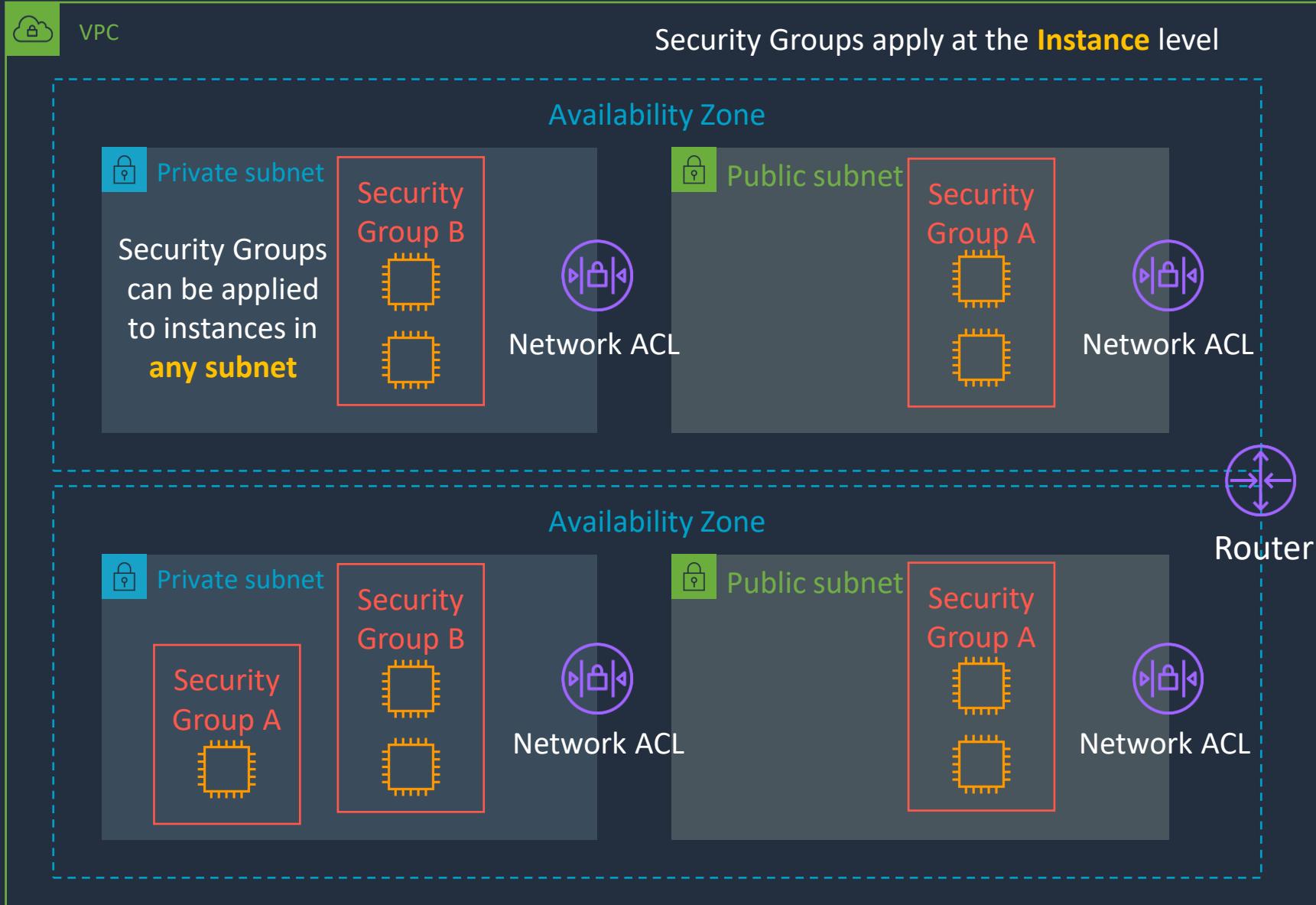


A **stateful** firewall
allows the return
traffic automatically

A **stateless** firewall
checks for an allow
rule for **both**
connections



Security Groups and Network ACLs

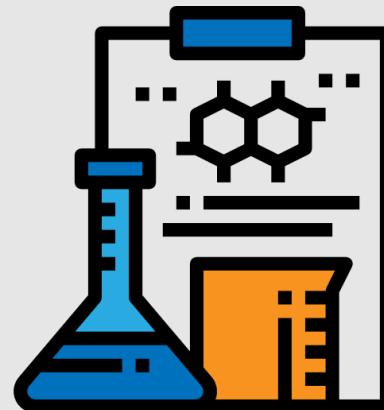




Security Groups & Network Access Control Lists (NACLs)

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

Using Security Groups and NACLs



Public, Private and Elastic IP Addresses



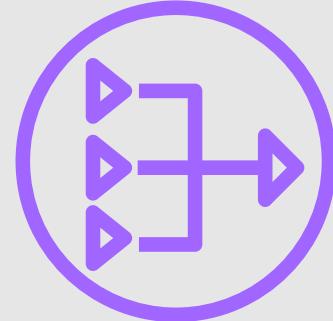
→ Public, Private and Elastic IP addresses

Name	Description
Public IP address	<p>Lost when the instance is stopped</p> <p>Used in Public Subnets</p> <p>No charge</p> <p>Associated with a private IP address on the instance</p> <p>Cannot be moved between instances</p>
Private IP address	<p>Retained when the instance is stopped</p> <p>Used in Public and Private Subnets</p>
Elastic IP address	<p>Static Public IP address</p> <p>You are charged if not used</p> <p>Associated with a private IP address on the instance</p> <p>Can be moved between instances and Elastic Network Adapters</p>

Working with IP Addresses

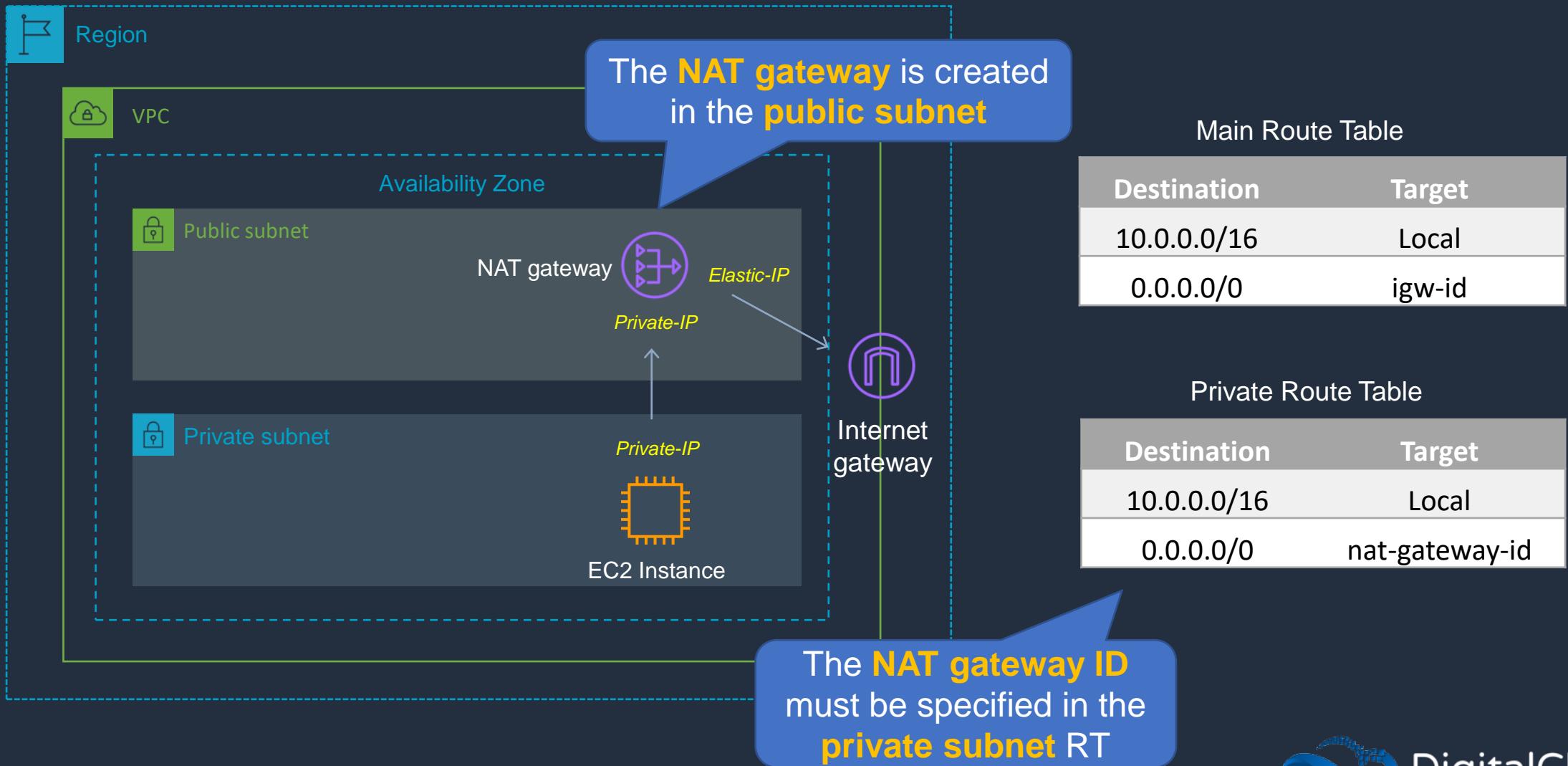


NAT Gateways and NAT Instances



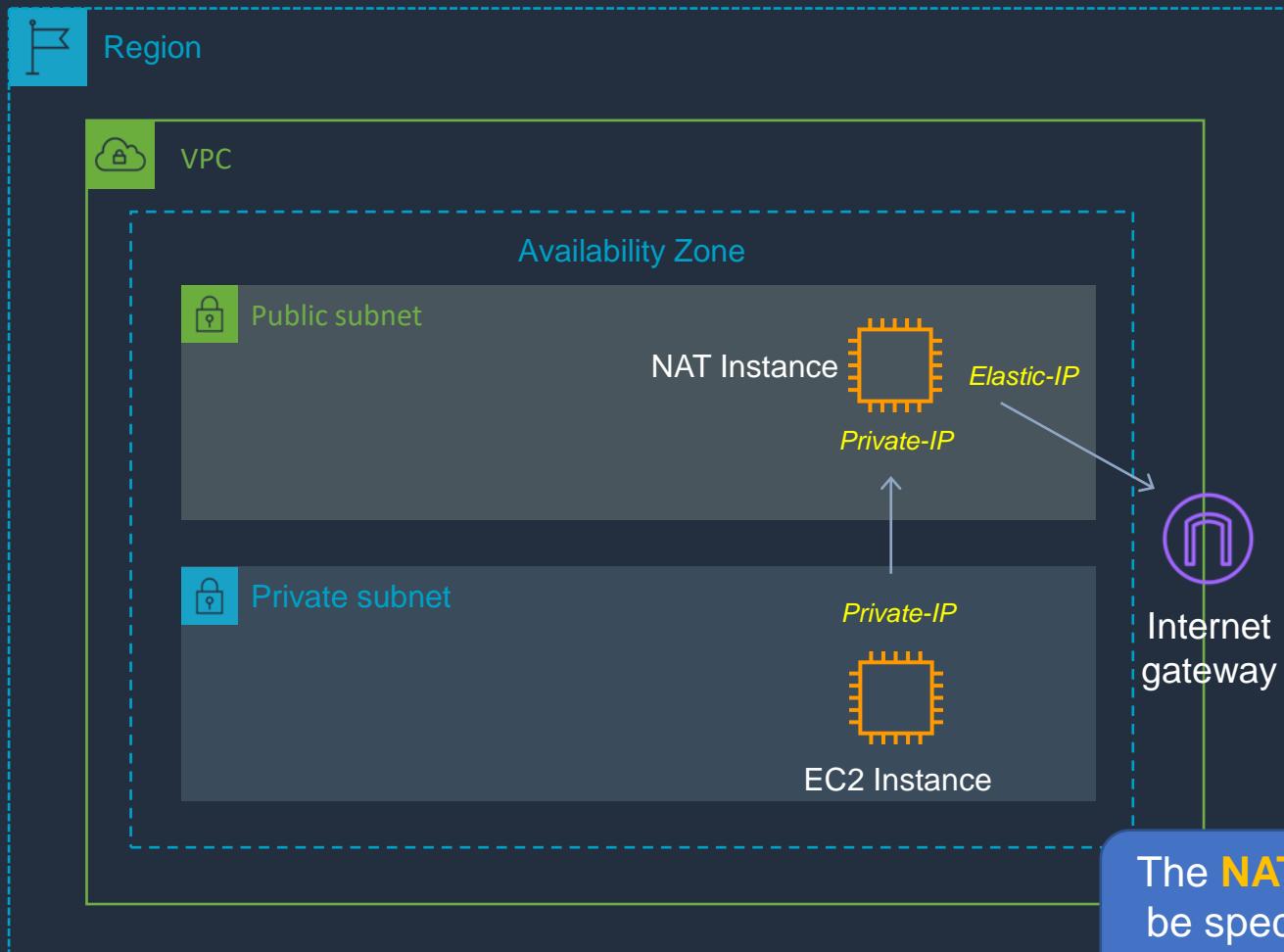


NAT Gateways





NAT Instances



Main Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-instance-id

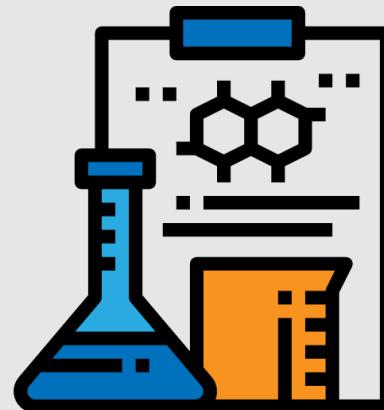
The **NAT instance ID** must
be specified in the **private**
subnet RT



NAT Instance vs NAT Gateway

NAT Instance	NAT Gateway
Managed by you (e.g. software updates)	Managed by AWS
Scale up (instance type) manually and use enhanced networking	Elastic scalability up to 45 Gbps
No high availability – scripted/auto-scaled HA possible using multiple NATs in multiple subnets	Provides automatic high availability within an AZ and can be placed in multiple AZs

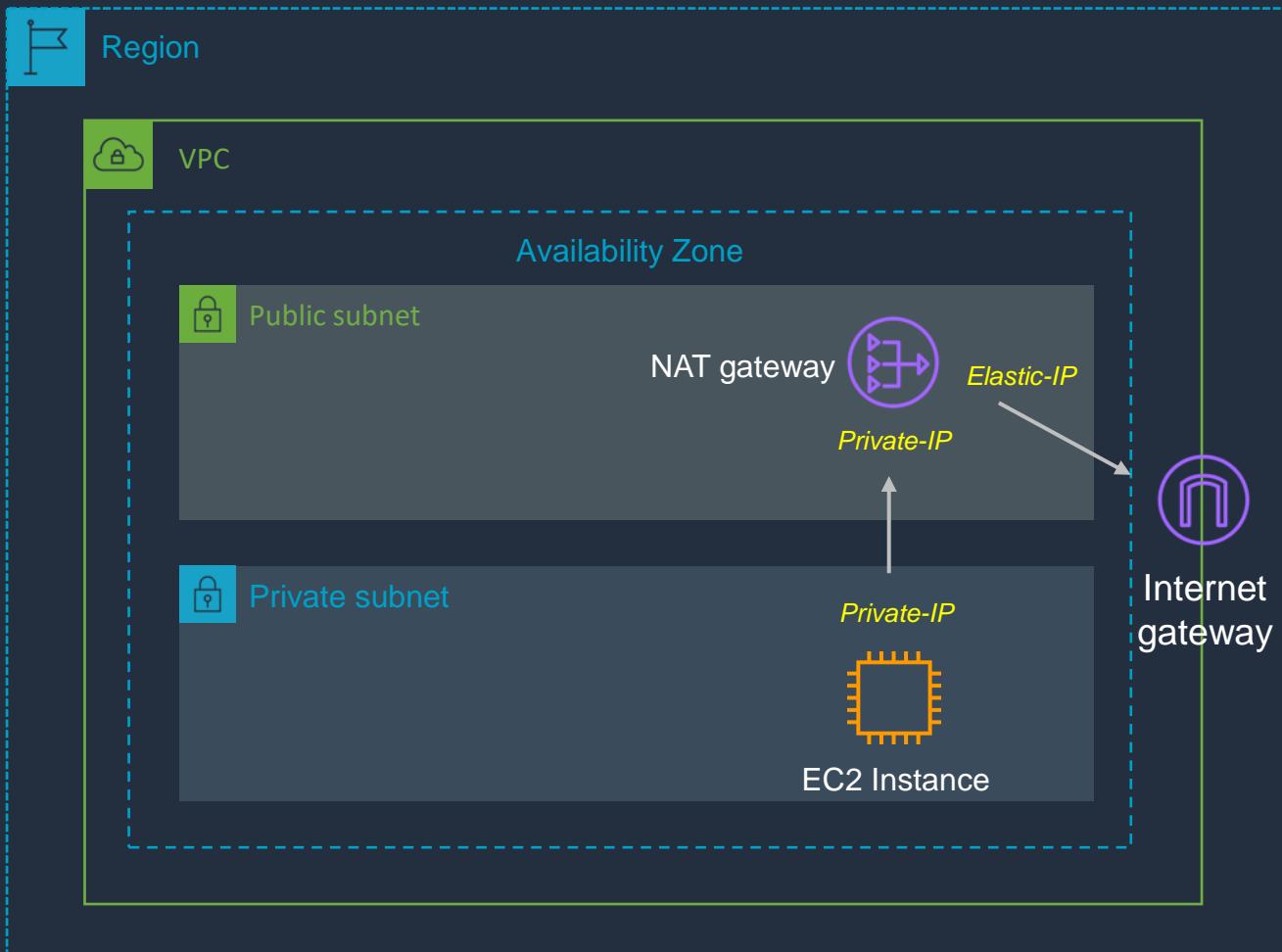
Deploy a NAT Gateway





NAT Gateways

The **NAT gateway** is created in the **public subnet**



Main Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-gateway-id

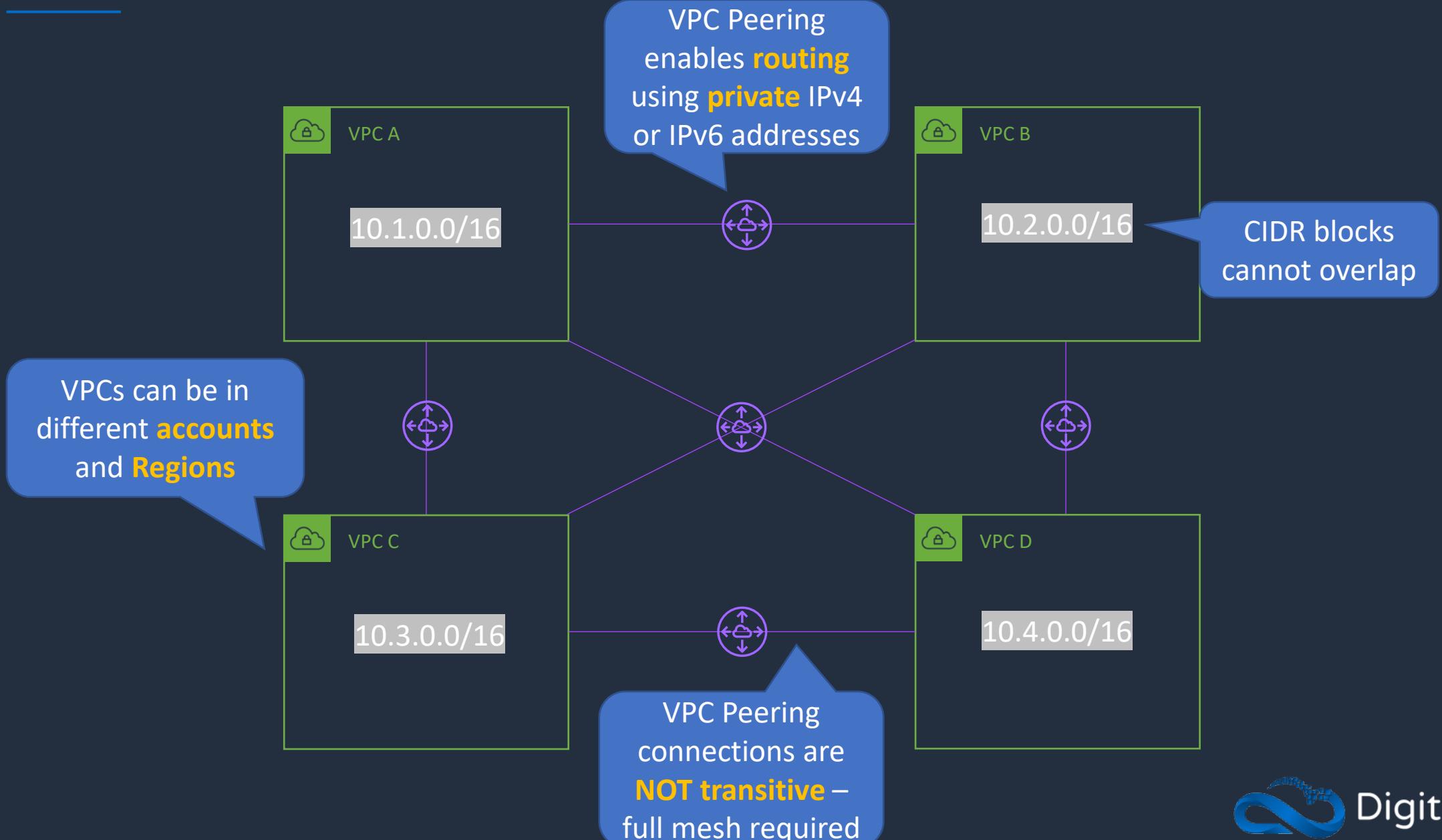
The **NAT gateway ID** must be specified in the **private subnet RT**

Amazon VPC Peering

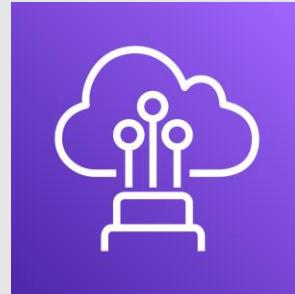




VPC Peering

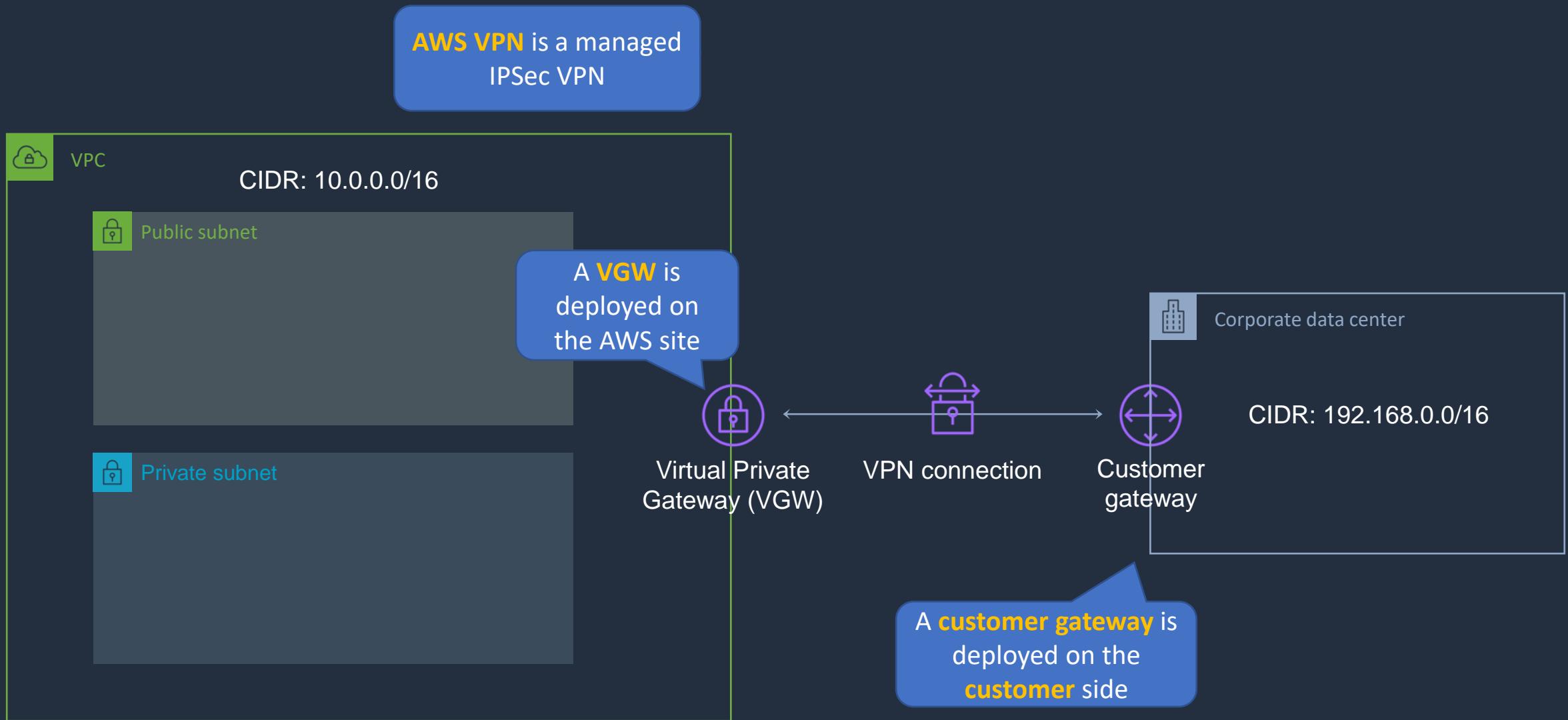


Amazon VPN and AWS Direct Connect



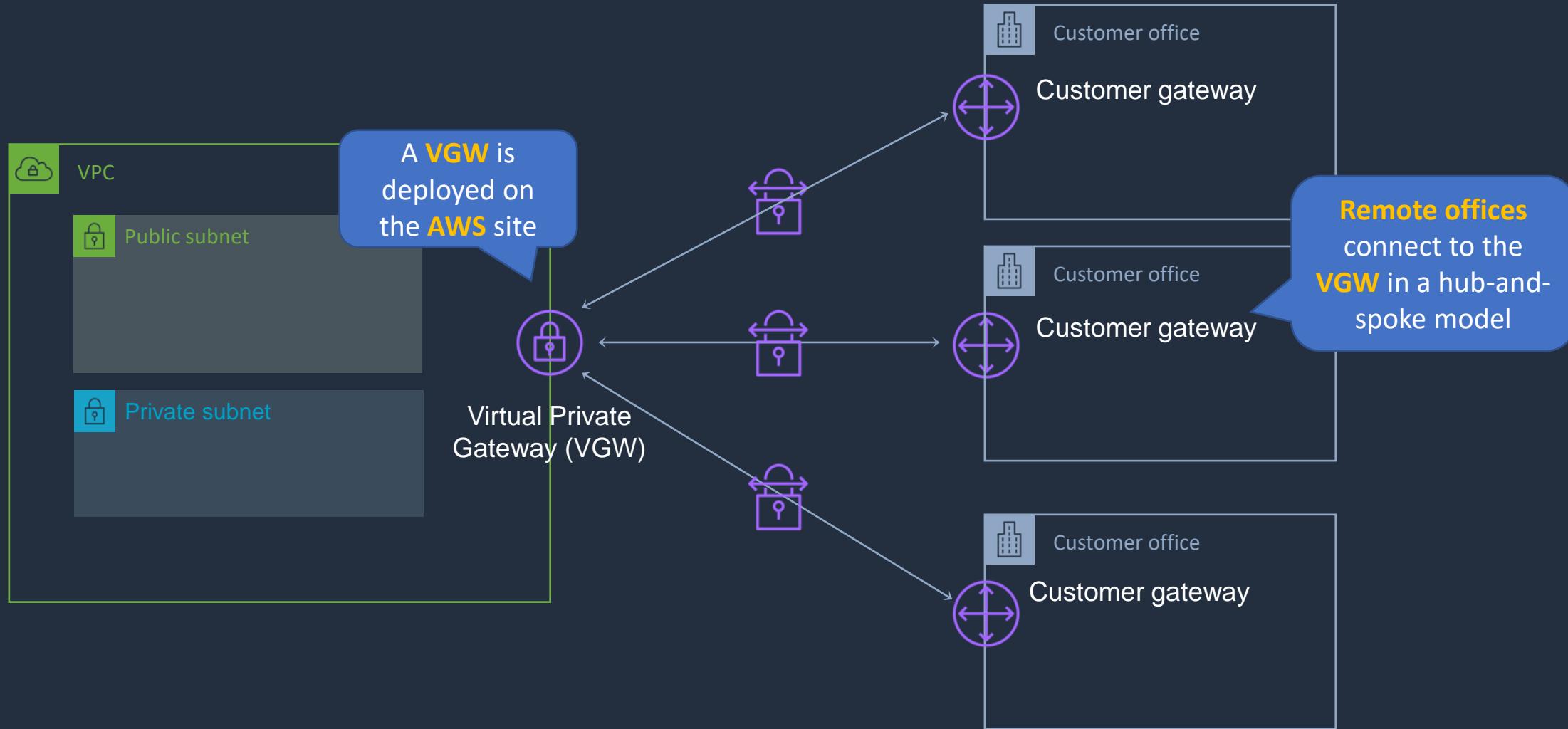


AWS Site-to-Site VPN





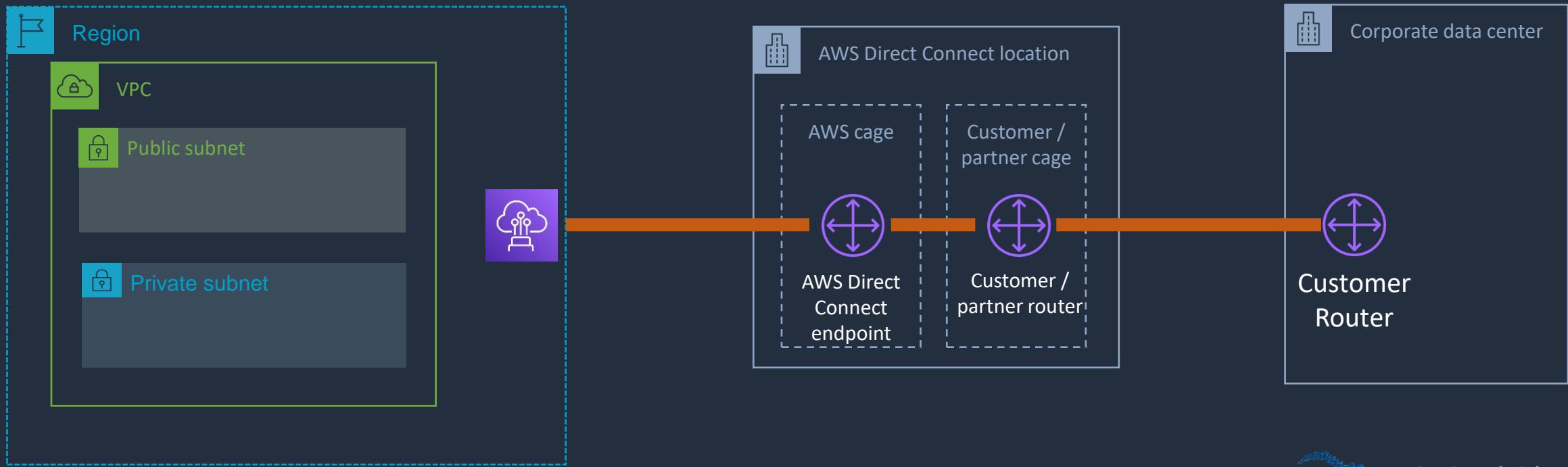
AWS VPN CloudHub





AWS Direct Connect

- **Private** connectivity between AWS and your data center / office
- Consistent network experience – increased **speed/latency** & **bandwidth/throughput**
- Lower costs for organizations that transfer **large** volumes of data



AWS Transit Gateway

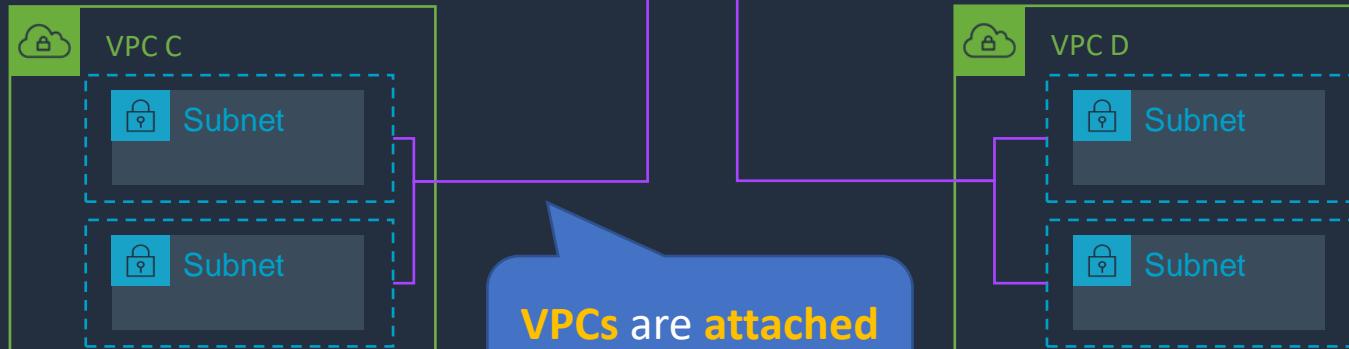




AWS Transit Gateway



Transit Gateway is a network transit hub that interconnects **VPCs** and **on-premises** networks



VPCs are attached to Transit Gateway



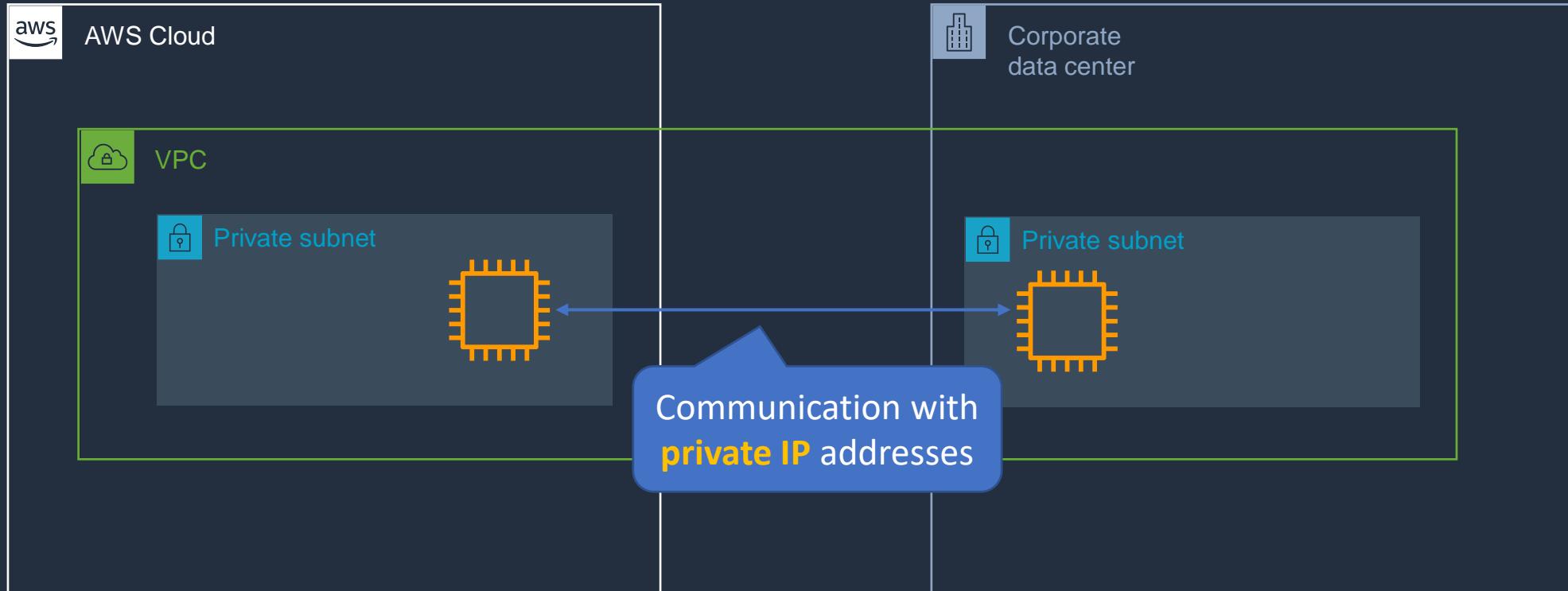
TGWs can be attached to **VPNs, Direct Connect Gateways, 3rd party appliances and TGWs** in other Regions/accounts

AWS Outposts





AWS Outposts





AWS Outposts

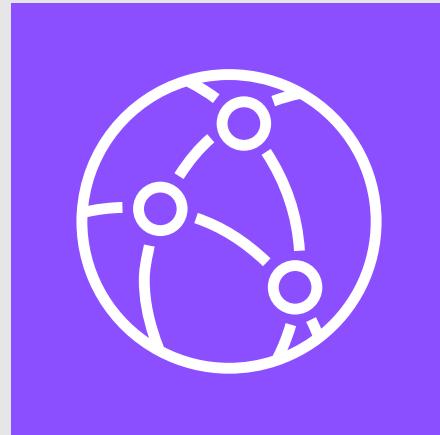
Services you can run on AWS Outposts include:

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon VPC
- Amazon ECS/EKS
- Amazon RDS
- Amazon EMR

SECTION 10

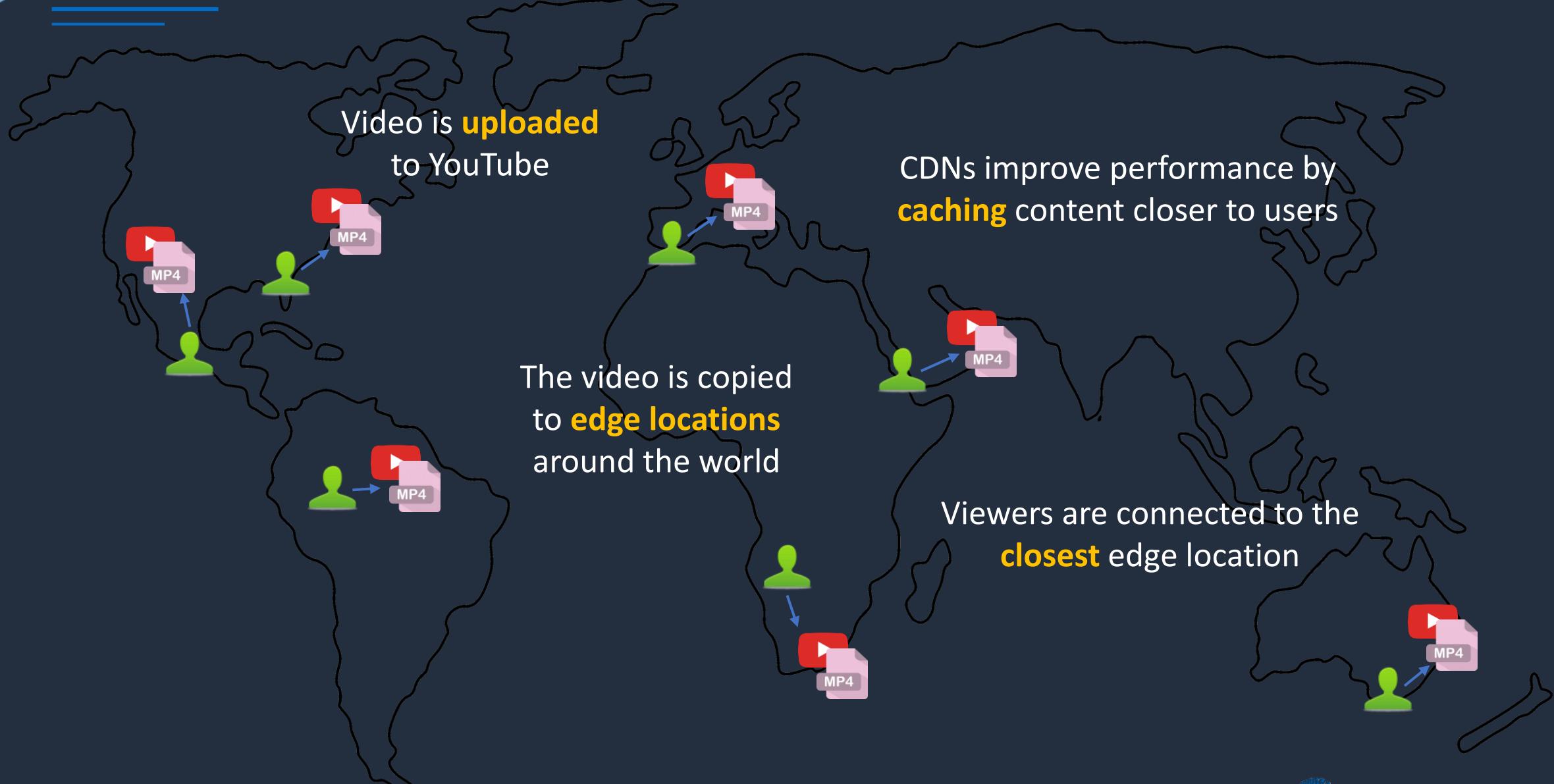
Deployment and Automation

Amazon CloudFront





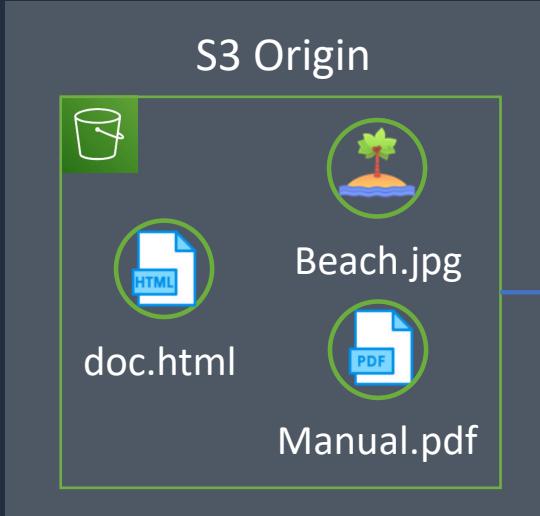
Content Delivery Network (CDN)



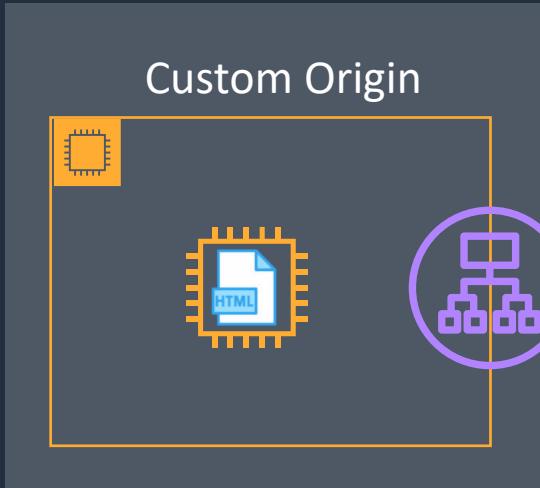


Amazon CloudFront

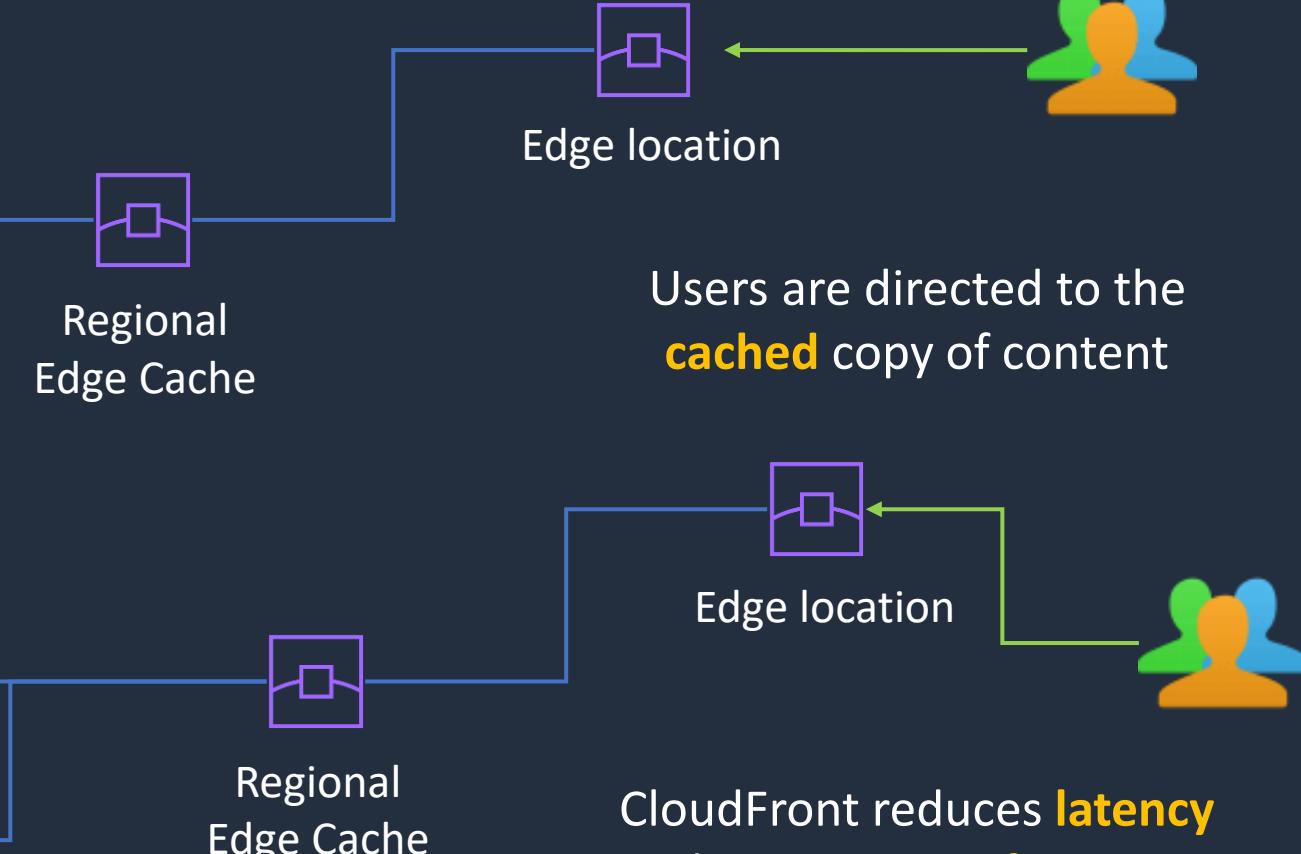
CloudFront Distribution



CloudFront Distribution



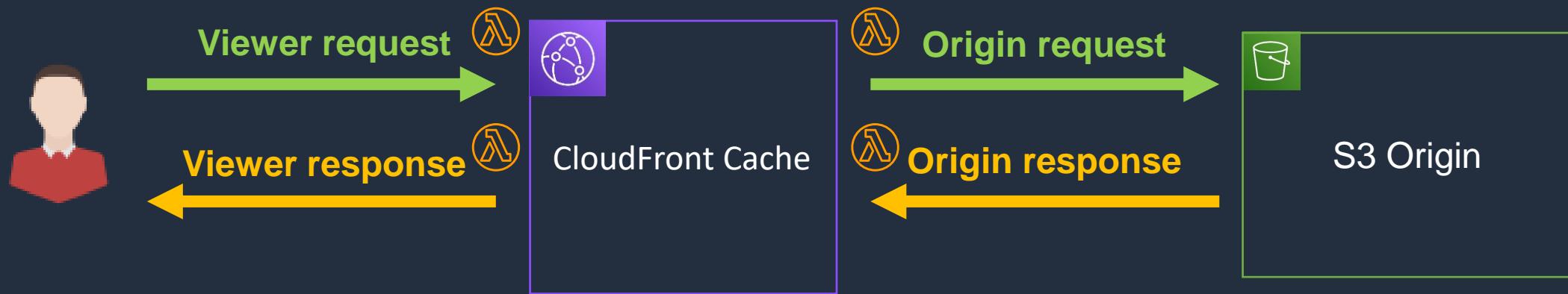
Content from the **origins** gets
cached around the world





Amazon CloudFront

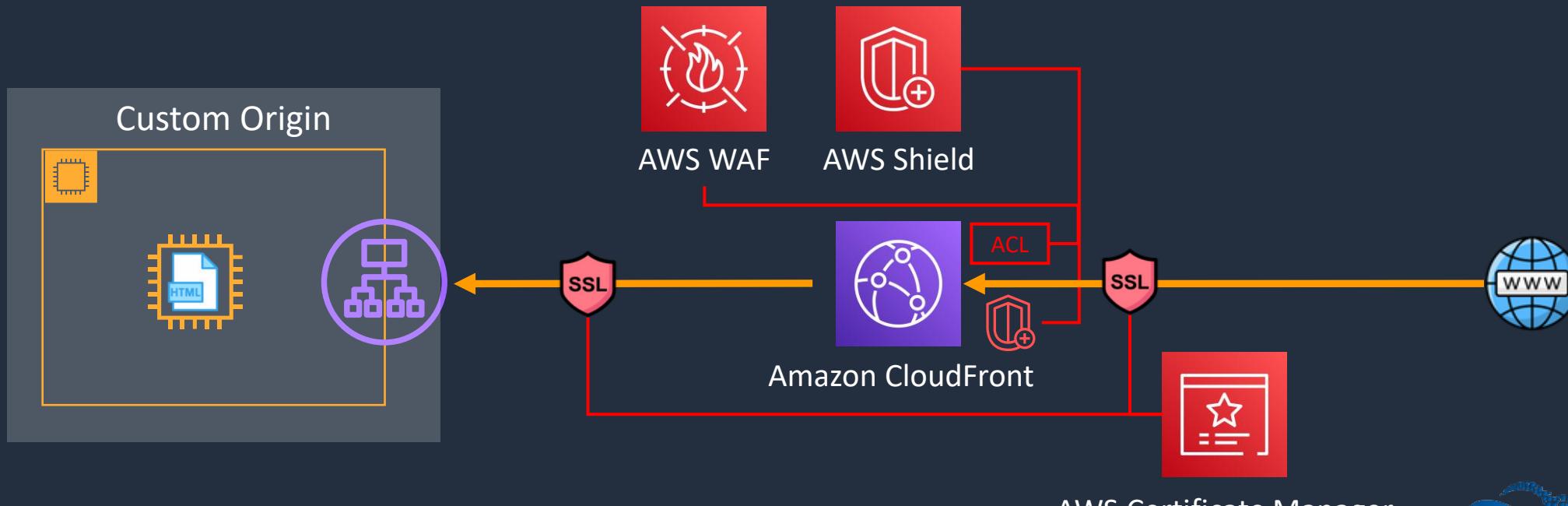
- CloudFront utilizes the AWS Global Network for low latency, high performance connectivity
- Delivers static and dynamic content and optimizes delivery based on content type
- Supports live streaming and video on demand (VOD)
- Lambda@Edge enables processing data with Lambda functions closer to users





Amazon CloudFront

- Uses HTTPS and integrates with AWS ACM for managing SSL/TLS certificates
- Integrates with AWS Shield and AWS WAF for additional security protection
- Content can also be protected with features including signed cookies, signed URLs, and origin access identity (OAI)



Create a Secure CloudFront Distribution

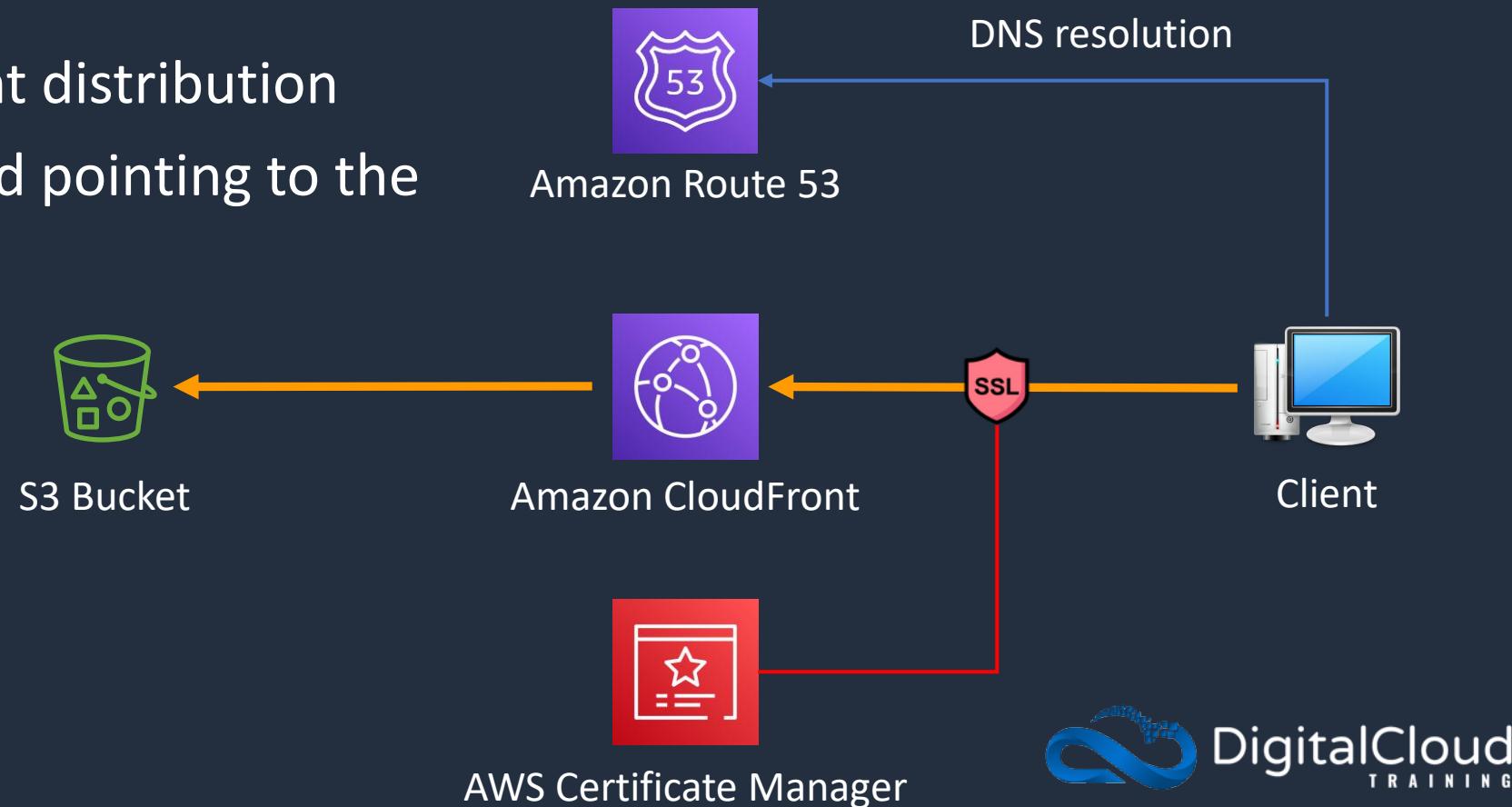




Amazon CloudFront Distribution

We will create:

- An Amazon S3 bucket
- An AWS Certificate Manager SSL/TLS certificate
- An Amazon CloudFront distribution
- A Route 53 alias record pointing to the distribution



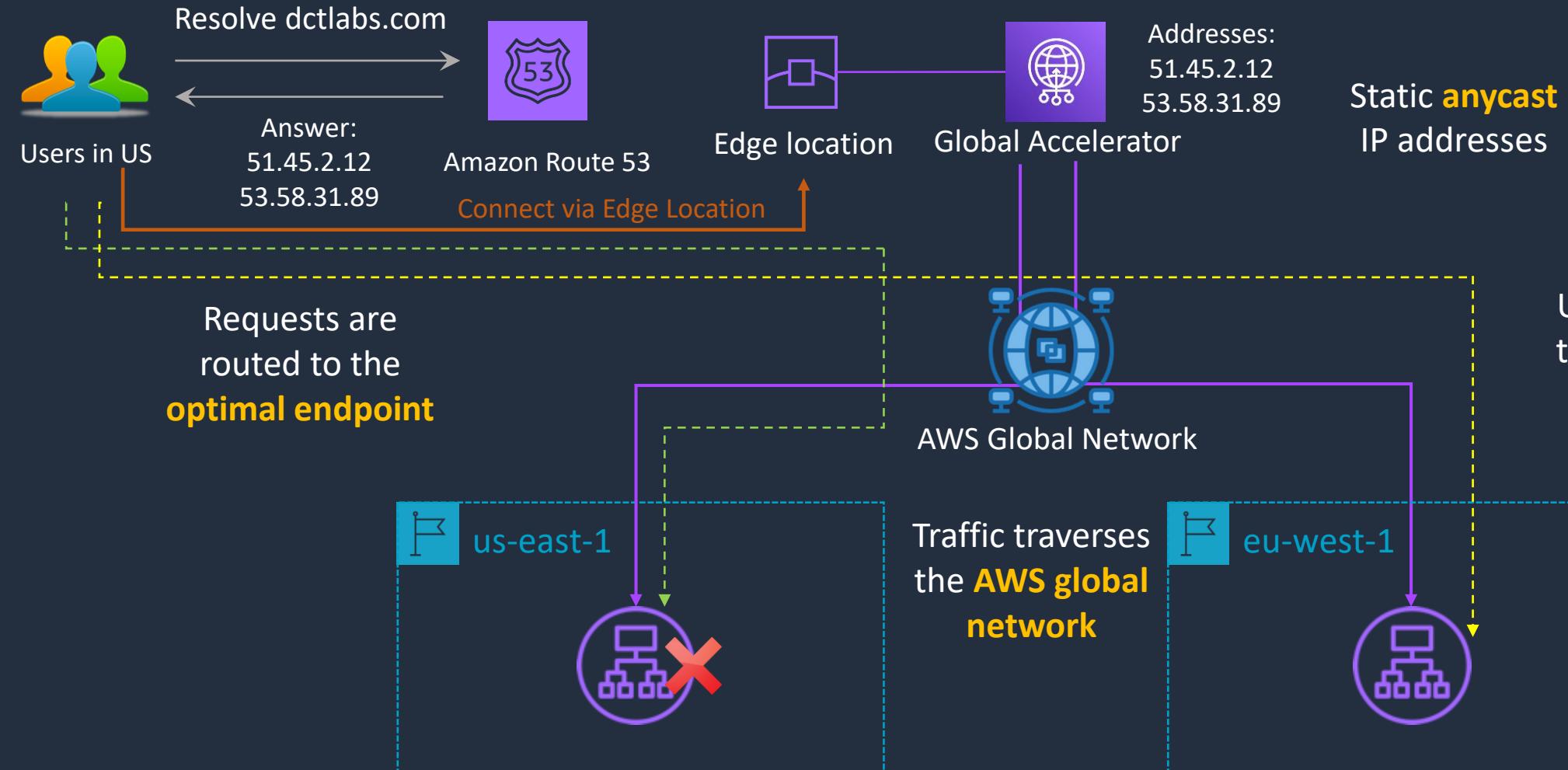
AWS Global Accelerator



AWS Global Accelerator



User traffic ingresses using
the closest **Edge Location**

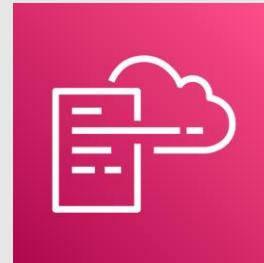




AWS Global Accelerator

- **Network Layer:** Operates at the network layer (Layer 4 of the OSI model)
- **IP Address:** Provides static IP addresses as a fixed entry point to your applications
- **Performance:** Improves performance by leveraging the AWS global network backbone, reducing internet latency and jitter
- **Health Checks:** Performs health checks and automatically reroutes traffic to healthy endpoints
- **Application Protocols:** Supports TCP and UDP traffic, making it suitable for a wide range of applications, including those requiring non-HTTP protocols
- **Use Cases:** Ideal for non-HTTP use cases such as gaming (UDP traffic), IoT, VoIP, or for services where having a static IP address is beneficial

Infrastructure as Code with AWS CloudFormation





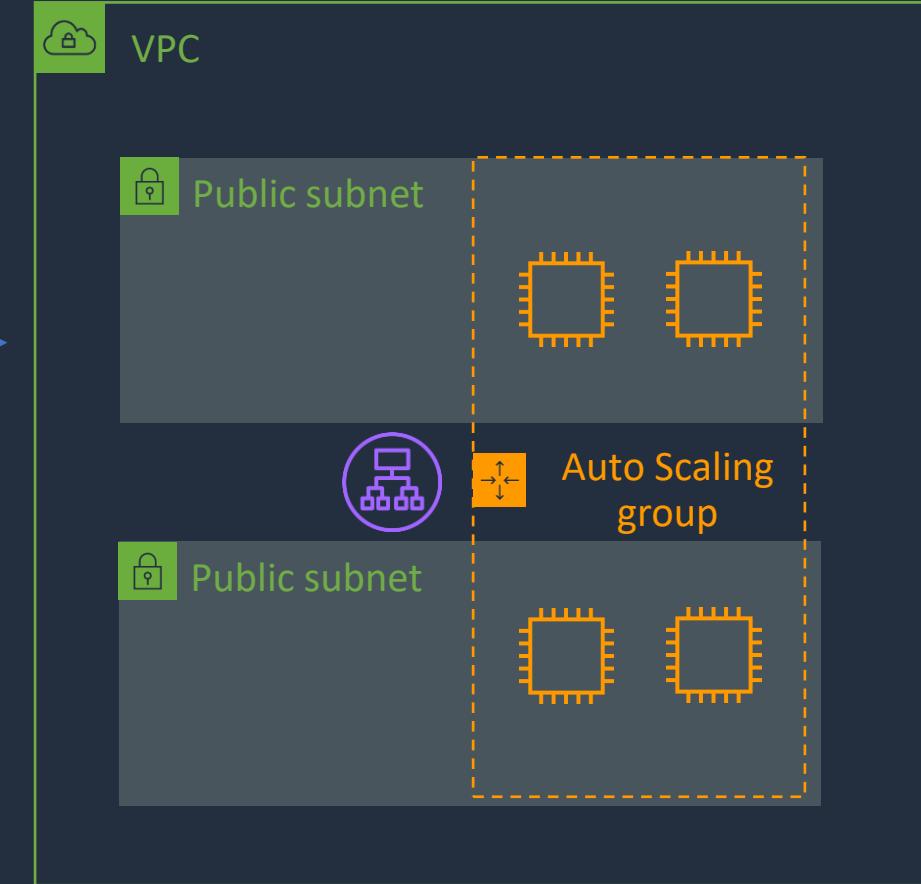
AWS CloudFormation

Infrastructure patterns are defined in a **template** file using **code**



CloudFormation **builds** your infrastructure according to the **template**

```
1 "AWSTemplateFormatVersion": "2010-09-09",
2
3 "Description": "AWS CloudFormation Sample Template WordPress_Multi_AZ: WordPress is web
4
5 "Parameters": {
6   "VpcId": {
7     "Type": "AWS::EC2::VPC::Id",
8     "Description": "VpcId of your existing Virtual Private Cloud (VPC)",
9     "ConstraintDescription": "must be the VPC Id of an existing Virtual Private Cloud."
10 },
11
12 "Subnets": {
13   "Type": "List<AWS::EC2::Subnet::Id>",
14   "Description": "The list of SubnetIds in your Virtual Private Cloud (VPC)",
15   "ConstraintDescription": "must be a list of at least two existing subnets associated
16 },
```





AWS CloudFormation

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

Creating and Updating Stacks



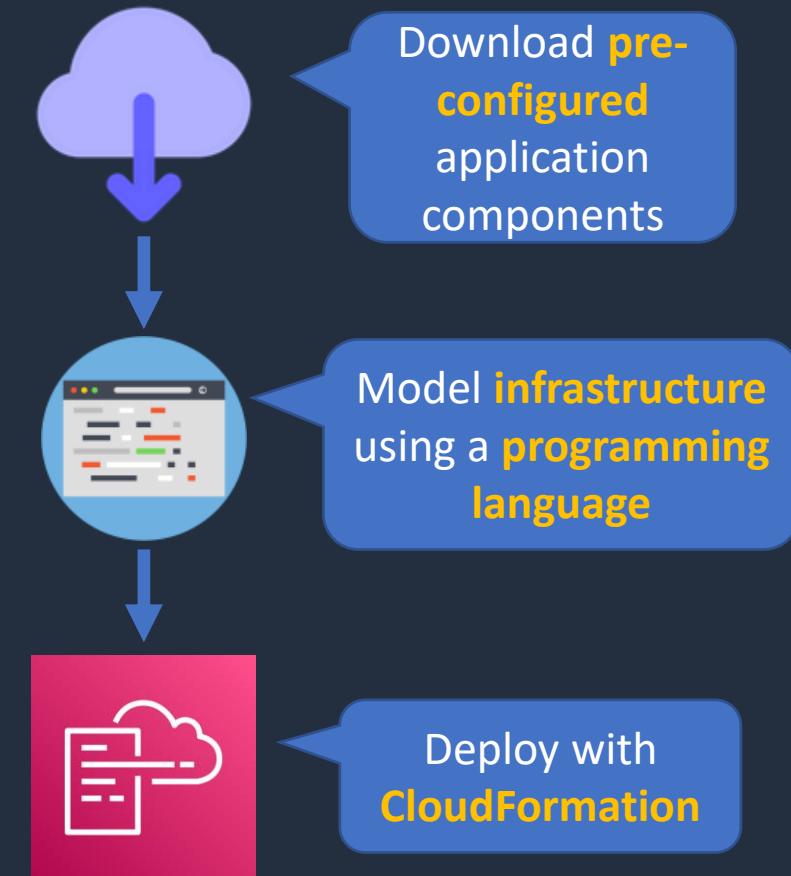
AWS Cloud Development Kit (CDK)





AWS Cloud Development Kit

- Open-source software development framework to define your cloud application resources using **familiar programming languages**
- Preconfigures cloud resources with proven defaults using **constructs**
- Provisions your resources using **AWS CloudFormation**
- Enables you to model application infrastructure using TypeScript, Python, Java, and .NET
- Use existing IDE, testing tools, and workflow patterns



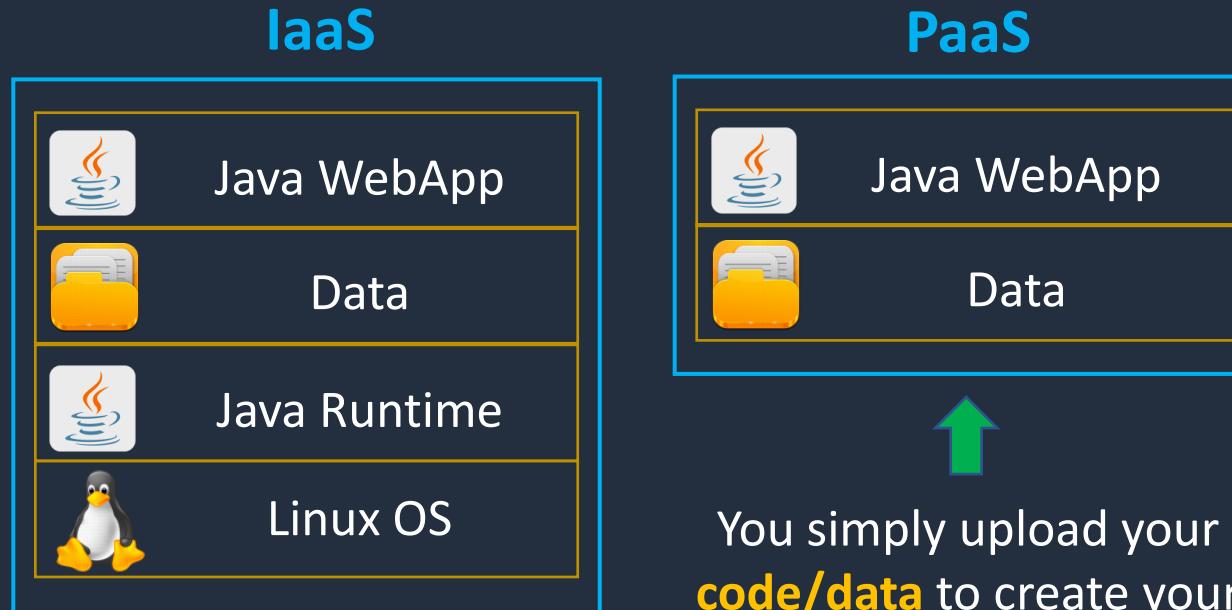
Platform as a Service with AWS Elastic Beanstalk





Cloud Service Models: Comparison

Example is
Amazon EC2

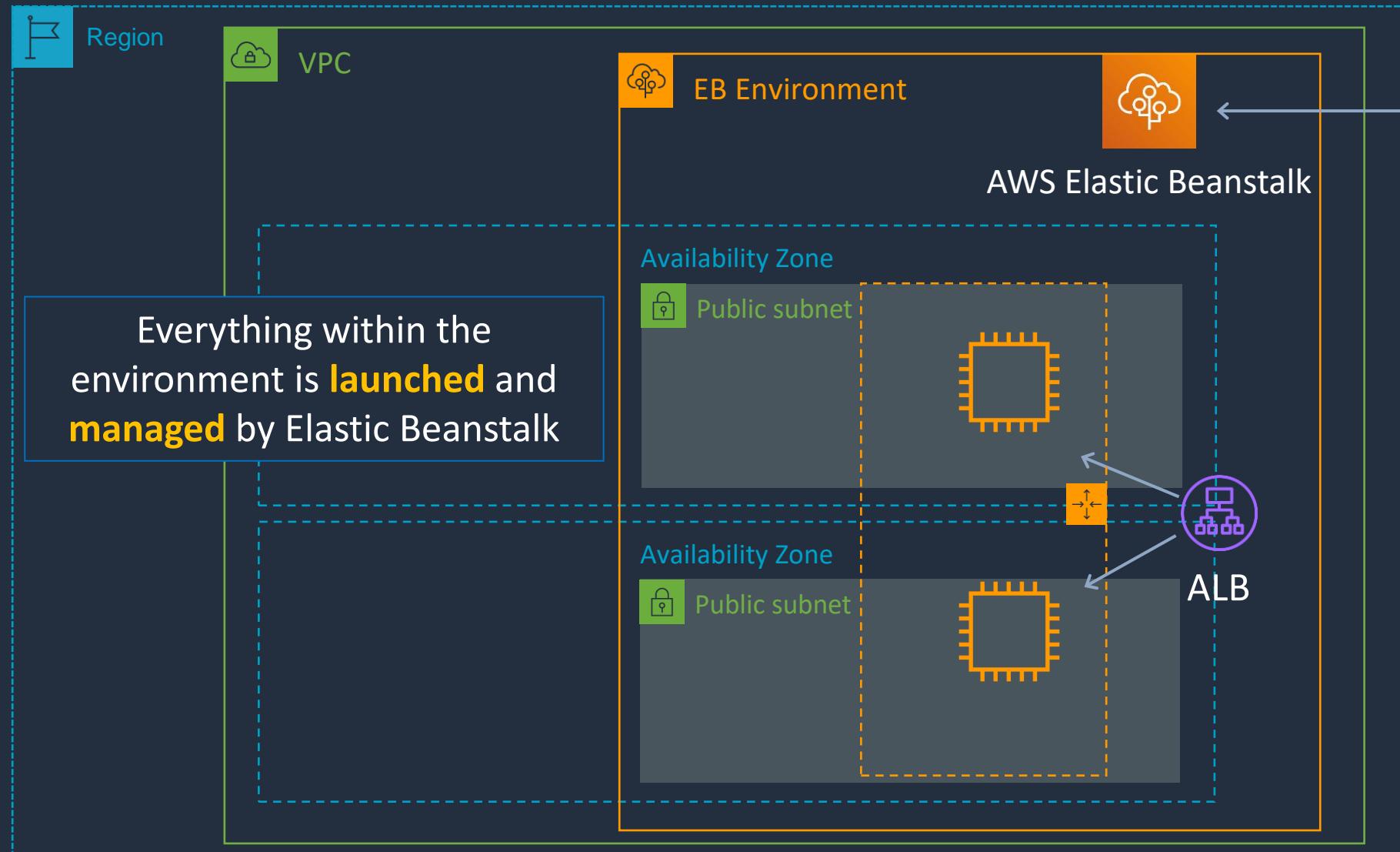


You manage from the
virtual server upwards

Example is **AWS Elastic Beanstalk**



AWS Elastic Beanstalk



Upload **source code** in ZIP file



Developer Client



AWS Elastic Beanstalk

- Supports many application platforms including:
 - Java, .NET, Node.js, PHP, Ruby, Python, Go, and Docker
- Uses core AWS services including EC2, ECS, Auto Scaling, and Elastic Load Balancing
- Elastic Beanstalk provides a UI to monitor and manage the health of applications
- Managed platform updates deploy the latest versions of software and patches



AWS Elastic Beanstalk

There are several **layers**

Applications:

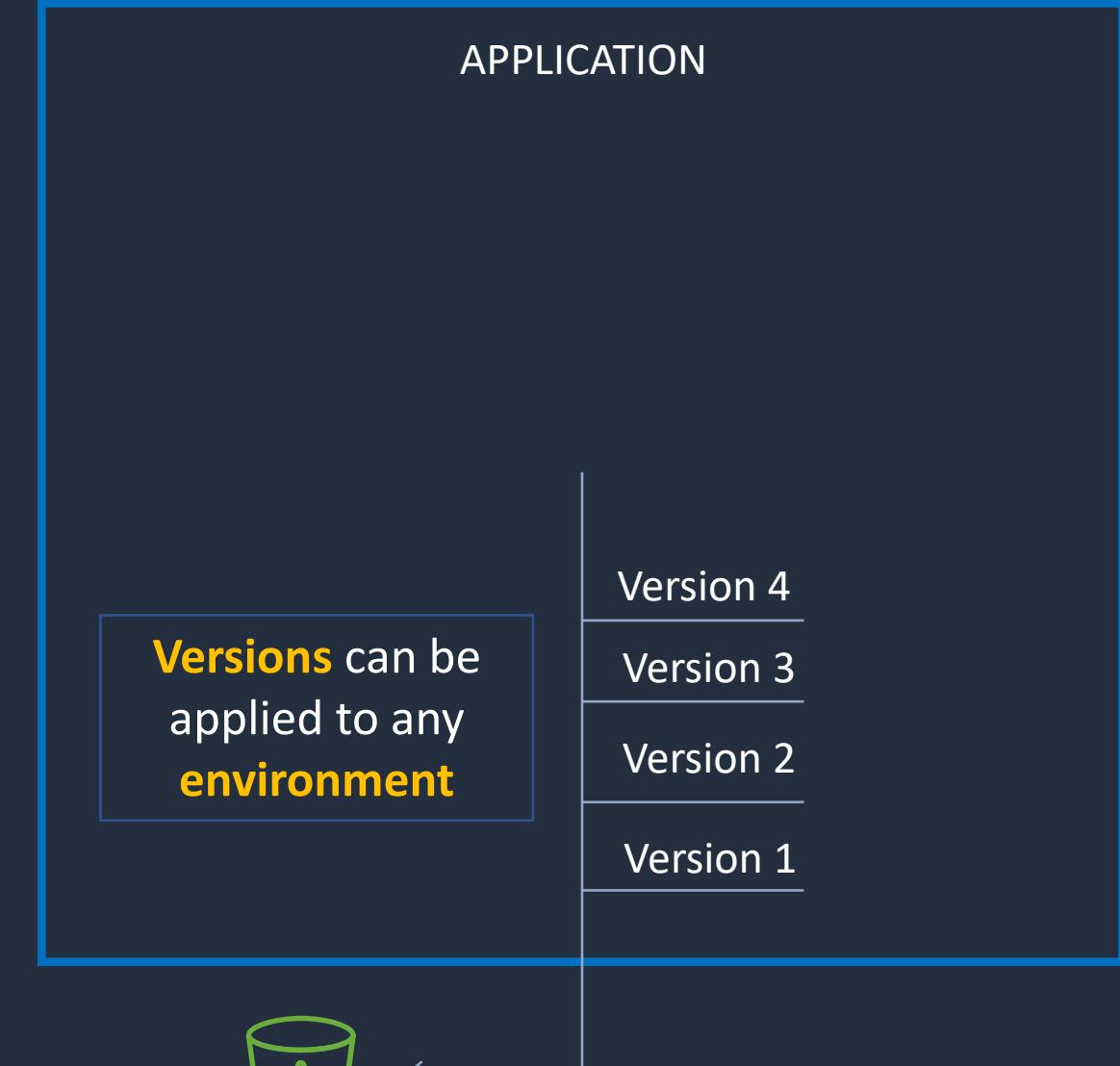
- Contain environments, environment configurations, and application versions
- You can have multiple application versions held within an application

APPLICATION



Application version

- A specific reference to a section of deployable code
- The application version will point typically to an Amazon S3 bucket containing the code



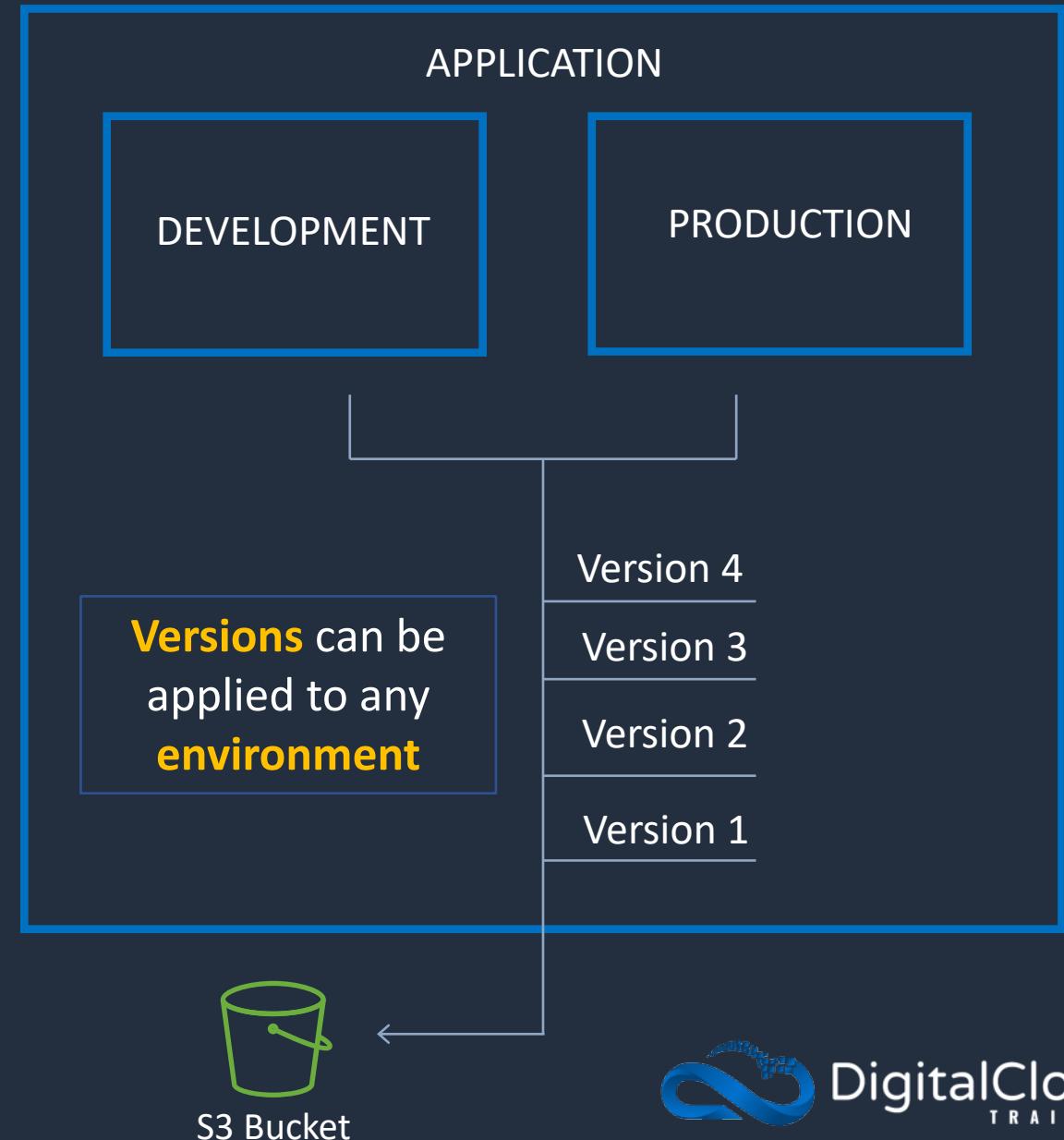
S3 Bucket



AWS Elastic Beanstalk

Environments:

- An application version that has been deployed on AWS resources
- The resources are configured and provisioned by AWS Elastic Beanstalk
- The environment is comprised of all the resources created by Elastic Beanstalk and not just an EC2 instance with your uploaded code



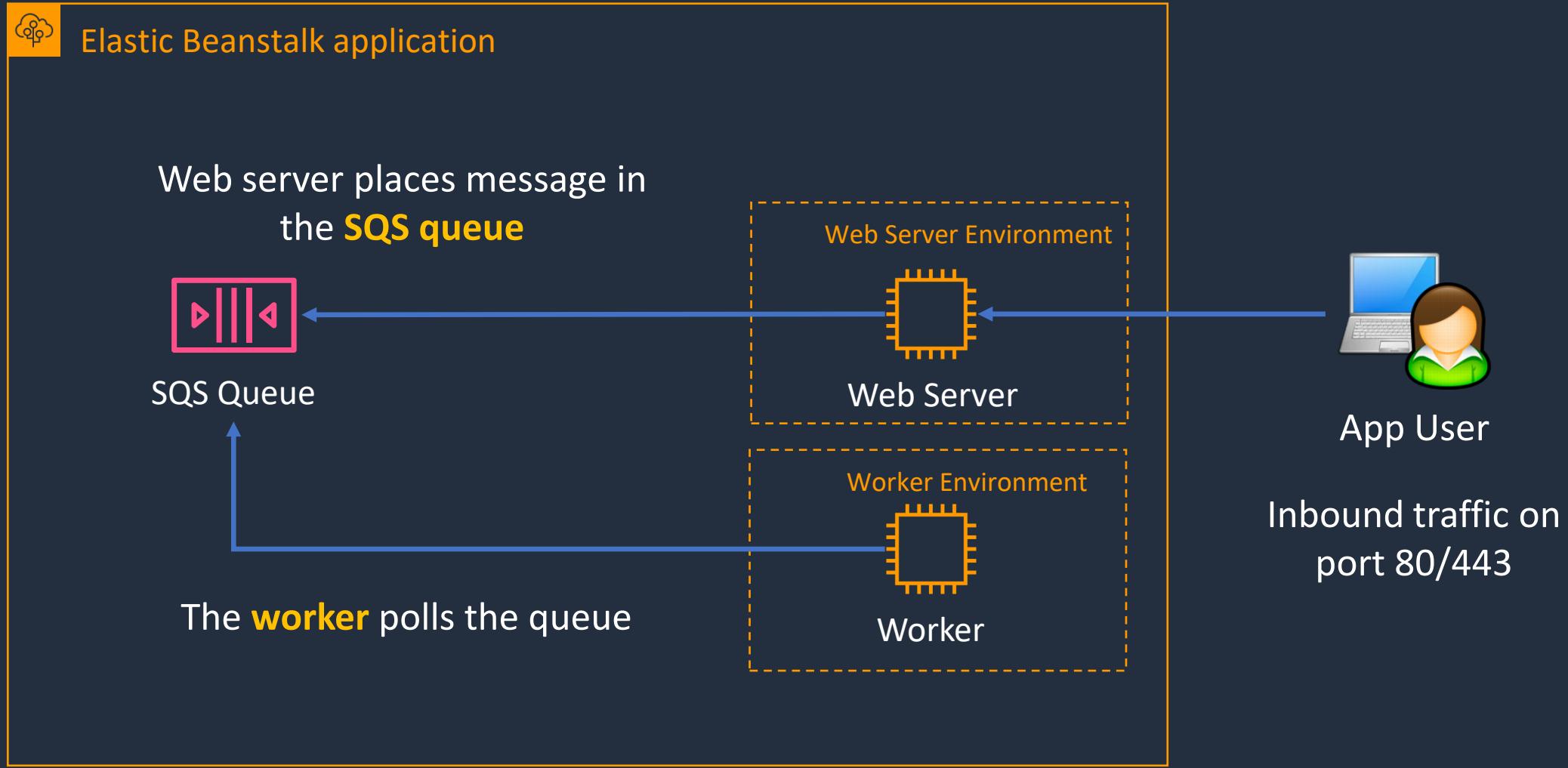


Web Servers and Workers

- **Web servers** are standard applications that listen for and then process HTTP requests, typically over port 80
- **Workers** are specialized applications that have a background processing task that listens for messages on an Amazon SQS queue
- **Workers** should be used for long-running tasks



AWS Elastic Beanstalk

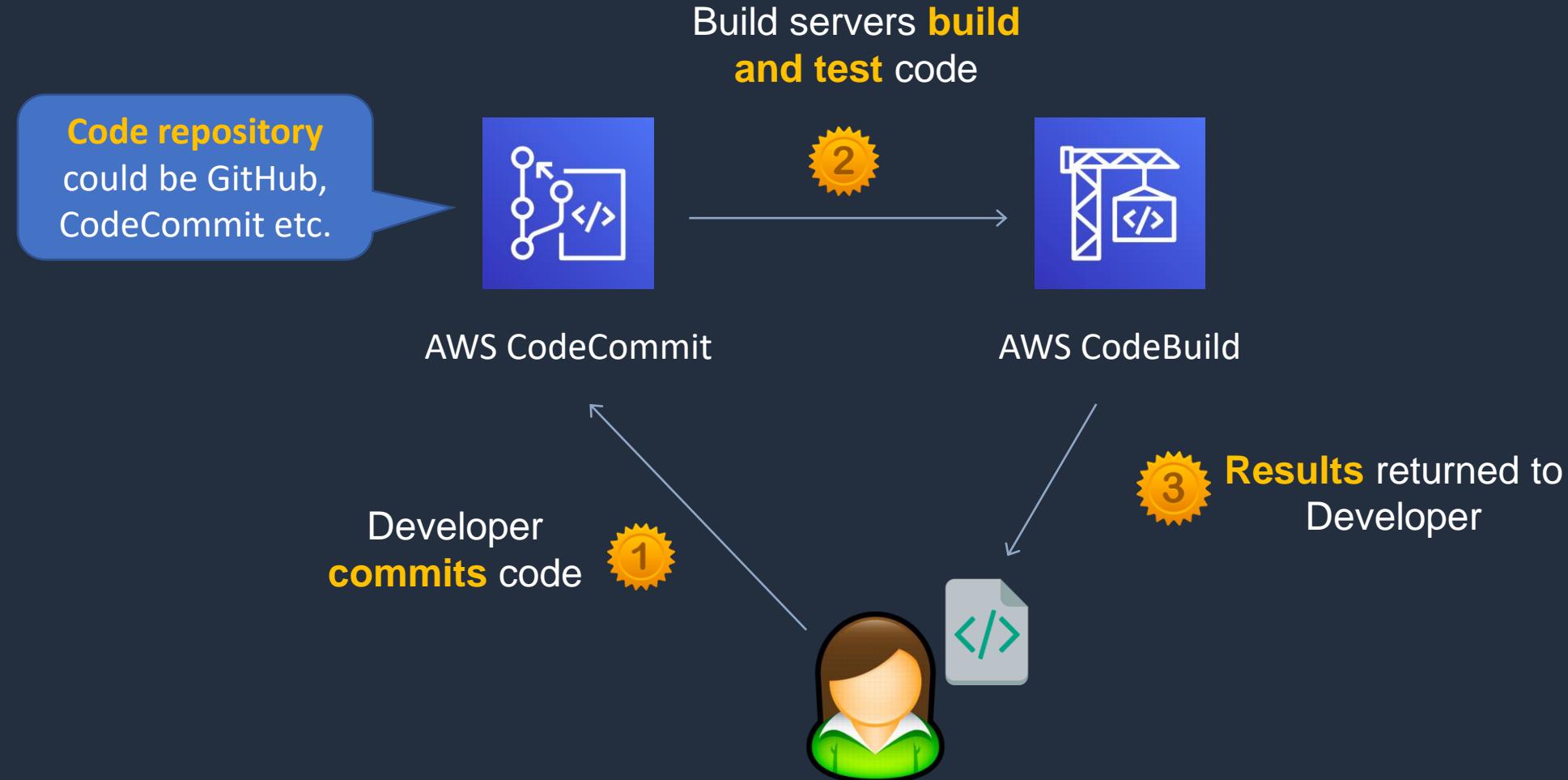


AWS Developer Tools (Code*)



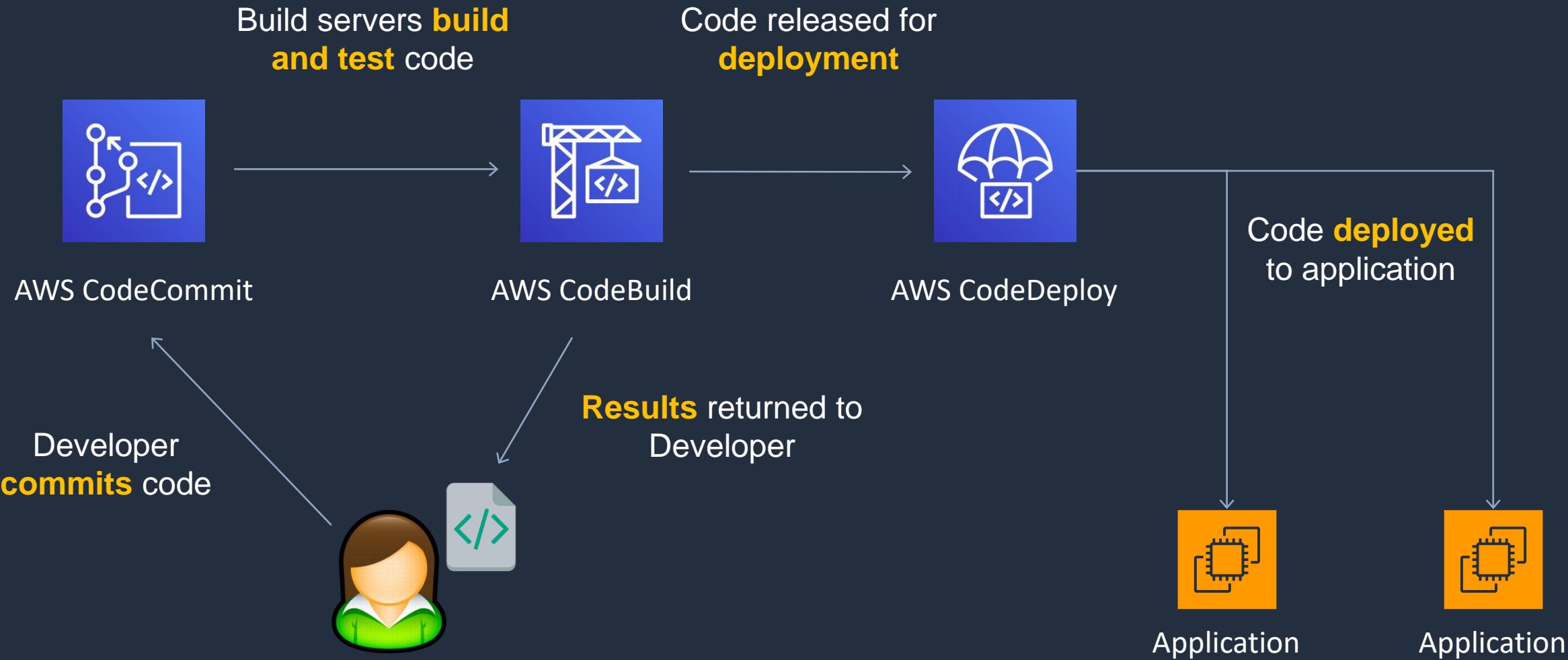


Continuous Integration





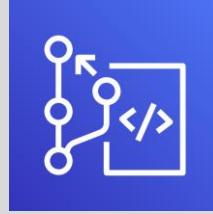
Continuous Integration and Continuous Delivery





Continuous Integration and Continuous Delivery

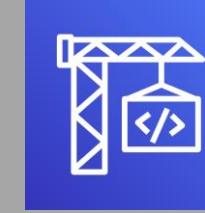
CODE



AWS CodeCommit

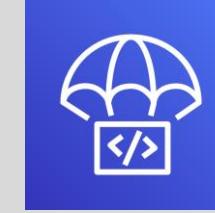
BUILD & TEST

AWS CodePipeline



AWS CodeBuild

DEPLOY

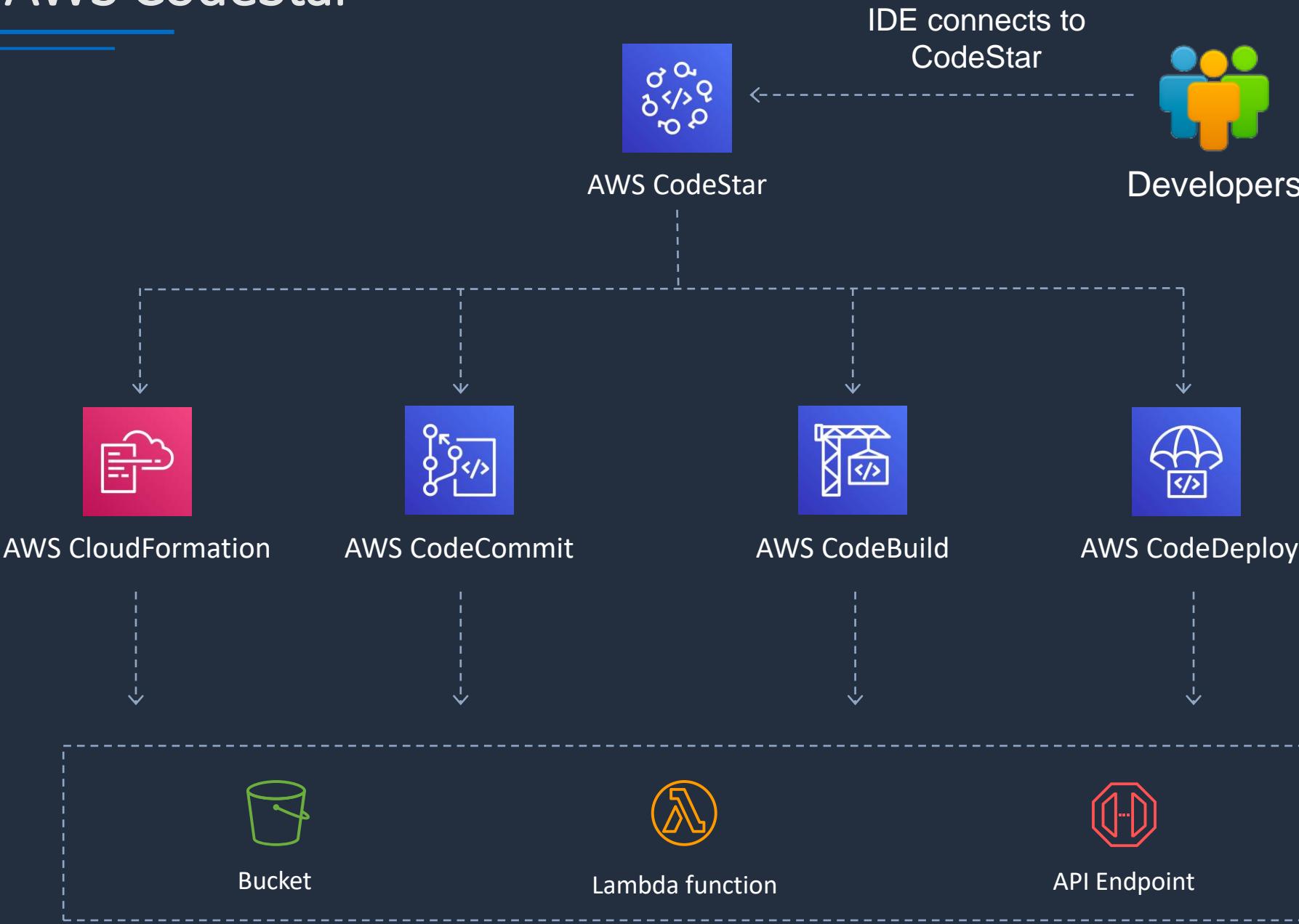


AWS CodeDeploy





AWS CodeStar



AWS Cloud9



- AWS Cloud9 is an integrated development environment (IDE)
- Used by developers to write, run, and debug code
- Editor provides syntax highlighting, code completion, and error checking
- Terminal is used to navigate the file system, run commands, and manage code
- Provides collaboration features that allow multiple developers to work on the same codebase simultaneously
- Provides a range of debugging tools to identify and fix errors in code
- Integrates with many AWS services including AWS Lambda, Amazon EC2, and AWS CodePipeline

AWS AppConfig





AWS AppConfig



- Create, manage, and deploy application configurations
- Capability of AWS Systems Manager
- A **configuration** is a collection of settings that influence the behavior of your application
- Applications can be hosted on:
 - Amazon EC2 instances
 - AWS Lambda
 - Mobile applications
 - IoT devices
- Reduces errors associated with configuration changes and streamlines deployment



AWS AppConfig



- Configurations can be stored in:
 - Amazon S3
 - AWS AppConfig
 - Systems Manager Parameter Store
 - Systems Manager Document Store
 - Bitbucket, GitHub, CodeCommit (via CodePipeline)
- Applications must be updated to check for and retrieve configuration data
- API actions include:
 - StartConfigurationSession
 - GetLatestConfiguration



AWS AppConfig



- Validators are used to ensure that configuration data is syntactically and semantically correct
- Validators are either:
 - JSON Schema Validators
 - AWS Lambda Validators
- Deployment type is either:
 - Linear – uses a growth factor which is a step %
 - Exponential – uses the exponential formula **G*(2^N)**
- Deployment strategies:
 - **AppConfig.AllAtOnce** – all targets at once
 - **AppConfig.Linear50PercentEvery30Seconds** – 50% of targets every 30 seconds



AWS AppConfig – Example Configurations

Enables or disables mobile payments and default payments on a per-region basis

```
{  
  "allow_mobile_payments": {  
    "enabled": false  
  },  
  "default_payments_per_region": {  
    "enabled": true  
  }  
}
```

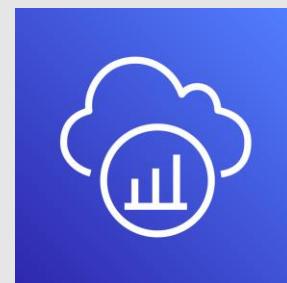


AWS AppConfig – Example Configurations

Enforces limits on how an application processes requests

```
{  
  "throttle-limits": {  
    "enabled": "true",  
    "throttles": [  
      {  
        "simultaneous_connections": 12  
      },  
      {  
        "tps_maximum": 5000  
      }  
    ],  
    "limit-background-tasks": [  
      true  
    ]  
  }  
}
```

AWS X-Ray



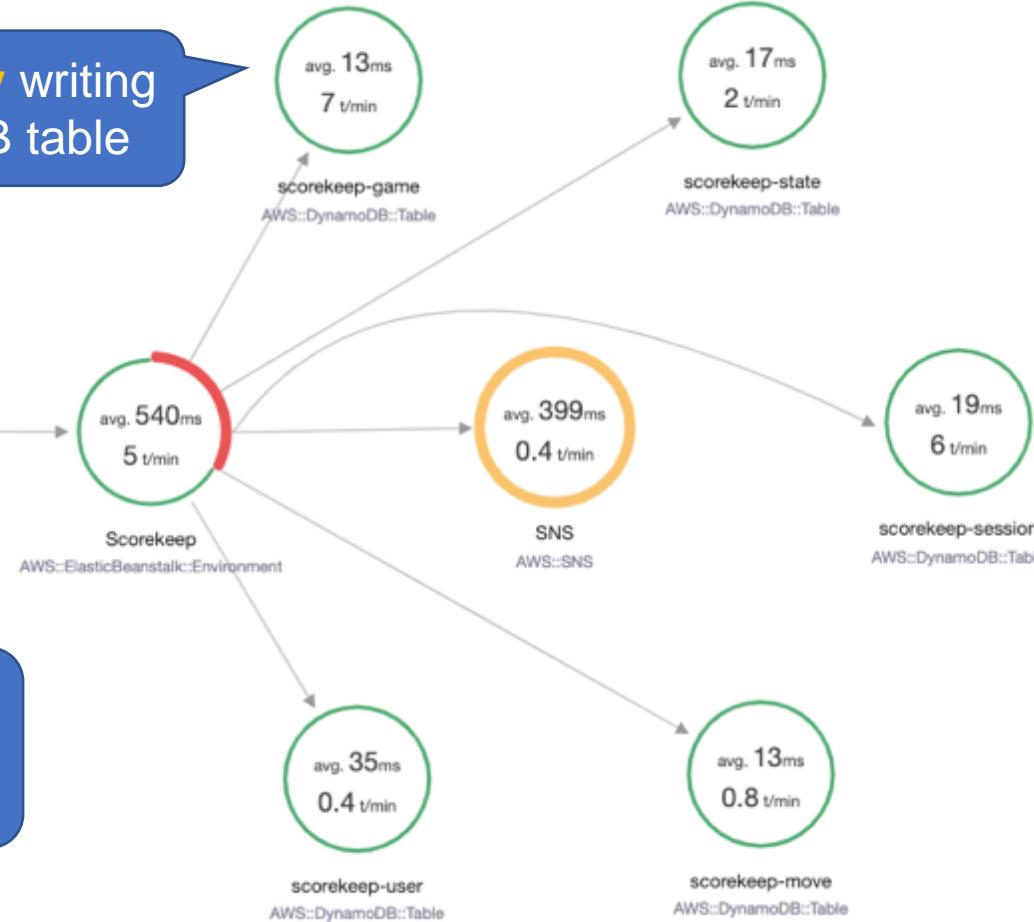


AWS X-Ray

Records **latency** writing to a DynamoDB table



Client



Records **latency** from client to application



DigitalCloud
TRAINING



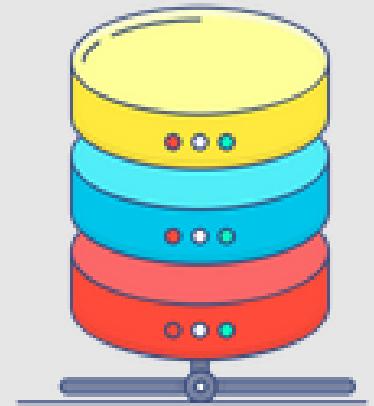
AWS X-Ray

- AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture
- AWS X-Ray supports applications running on:
 - Amazon EC2
 - Amazon ECS
 - AWS Lambda
 - AWS Elastic Beanstalk
- Need to integrate the X-Ray SDK with your application and install the X-Ray agent

SECTION 11

Databases and Analytics

Database Types and Use Cases





Relational vs Non-Relational

Key differences are how data are *managed* and how data are *stored*

Relational	Non-Relational
Organized by tables, rows and columns	Varied data storage models
Rigid schema (SQL)	Flexible schema (NoSQL) – data stored in key-value pairs, columns, documents or graphs
Rules enforced within database	Rules can be defined in application code (outside database)
Typically scaled vertically	Scales horizontally
Supports complex queries and joins	Unstructured, simple language that supports any kind of schema
Amazon RDS, Oracle, MySQL, IBM DB2, PostgreSQL	Amazon DynamoDB, MongoDB, Redis, Neo4j



Relational Databases

EmployeeID	FirstName	LastName	JobRole	Location
00001	Paul	Peterson	Senior Developer	Atlanta
00002	Kaleigh	Annette	Assistant Manager	Miami
00003	Carl	Wood	Sales Support	New York
00004	Vinni	Jones	Customer Service	Dallas
00005	Stefanie	Howard	IT Architect	Los Angeles

SQL is used for defining the structure of the database and its elements

SQL provides the tools for inserting, updating, deleting, and querying data within the database table

Example **Structured Query Language** (SQL) query:

```
SELECT FirstName  
FROM employees  
WHERE Location = Atlanta
```



Non-Relational Databases

NoSQL databases can be **key/value** and **document** stores

This is an example of a **key/value** store

Primary Key		Attributes				
Partition Key	Sort Key	sku	category	size	color	weight
john@example.com	1583975308	SKU-S523	T-Shirt	Small	Red	Light
chris@example.com	1583975613	SKU-J091	Pen		Blue	
chris@example.com	1583975449	SKU-A234	Mug			
sarah@example.com	1583976311	SKU-R873	Chair			
jenny@example.com	1583976323	SKU-I019	Plate	30		

There is no rigid schema so attributes can be missing or have different data types



Graph Databases

Graph databases like Amazon Neptune are designed to store, manage, and navigate relationships in data

Graph databases use:

- **Nodes** to represent entities
- **Edges** to represent relationships
- **Properties** to store information about nodes and edges





Operational vs Analytical

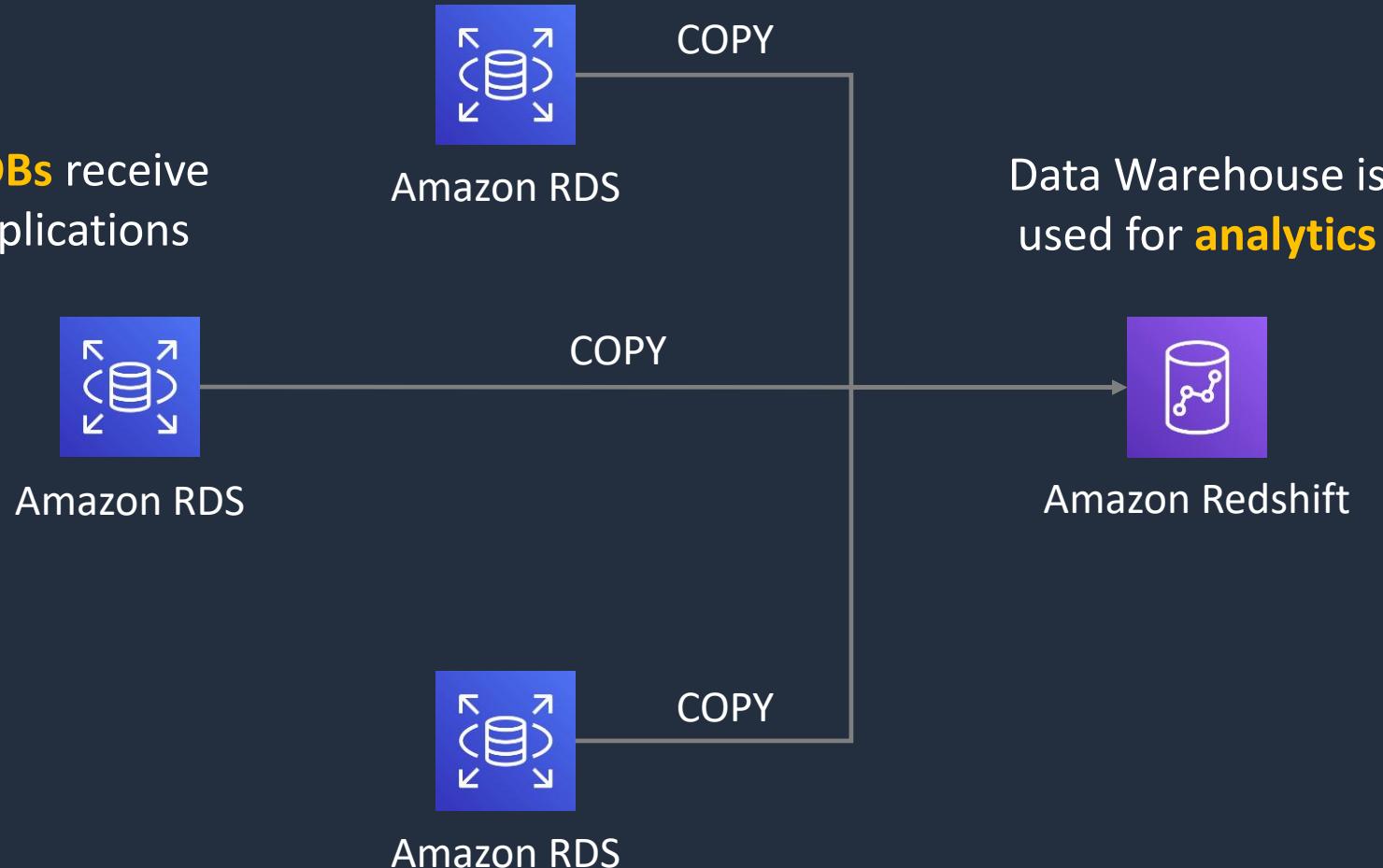
Key differences are **use cases** and how the database is **optimized**

Operational / transactional	Analytical
Online Transaction Processing (OLTP)	Online Analytics Processing (OLAP) – the source data comes from OLTP DBs
Production DBs that process transactions. E.g. adding customer records, checking stock availability (INSERT, UPDATE, DELETE)	Data warehouse. Typically, separated from the customer facing DBs. Data is extracted for decision making
Short transactions and simple queries	Long transactions and complex queries
Relational examples: Amazon RDS, Oracle, IBM DB2, MySQL	Relational examples: Amazon RedShift, Teradata, HP Vertica
Non-relational examples: MongoDB, Cassandra, Neo4j, HBase	Non-relational examples: Amazon EMR, MapReduce



Operational vs Analytical

Operational DBs receive data from applications





AWS Databases

Data Store	Use Case
Database on EC2	<ul style="list-style-type: none">• Need full control over instance and database• Third-party database engine (not available in RDS)
Amazon RDS	<ul style="list-style-type: none">• Need traditional relational database• e.g. Oracle, PostgreSQL, Microsoft SQL, MariaDB, MySQL• Data is well-formed and structured
Amazon DynamoDB	<ul style="list-style-type: none">• NoSQL database• In-memory performance• High I/O needs• Dynamic scaling
Amazon RedShift	<ul style="list-style-type: none">• Data warehouse for large volumes of aggregated data
Amazon ElastiCache	<ul style="list-style-type: none">• Fast temporary storage for small amounts of data• In-memory database

Amazon Relational Database Service (RDS)

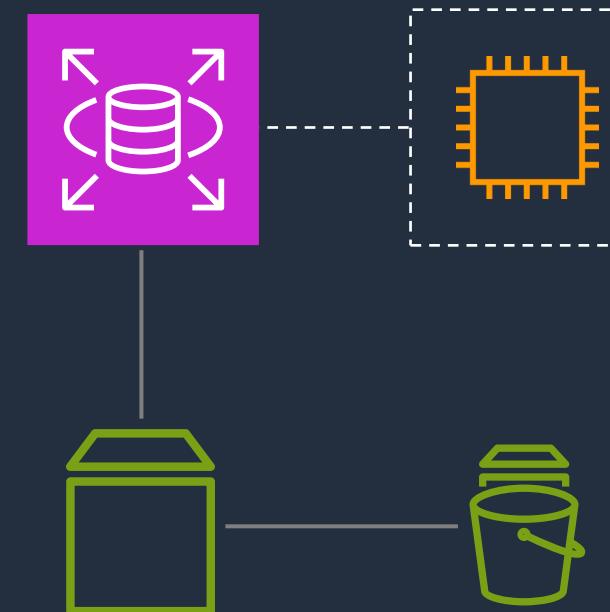




Amazon RDS

- Managed **relational** database service
- Used for online transaction processing (OLTP) use cases
- Runs on Amazon EC2 instances

A DB instance can contain
multiple user-created databases



You must choose the
DB instance type

RDS uses **Amazon EBS** volumes
for storage

Backups can be taken using
EBS snapshots



Amazon RDS

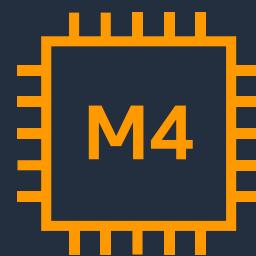
Amazon RDS offers a choice of database engines:

- **Amazon Aurora** – (MySQL and PostgreSQL compatible)
- **MySQL** – One of the most popular open-source relational database management systems
- **PostgreSQL** – An advanced open-source relational database that supports both SQL (relational) and JSON (non-relational) querying
- **Oracle** – Offers support for Oracle Database under two licensing models: "License Included" and "Bring Your Own License (BYOL)"
- **Microsoft SQL Server** – Supports several editions of Microsoft SQL Server
- **MariaDB** – A community-developed fork of MySQL intended to remain free under the GNU GPL



Amazon RDS – Scaling up (vertically)

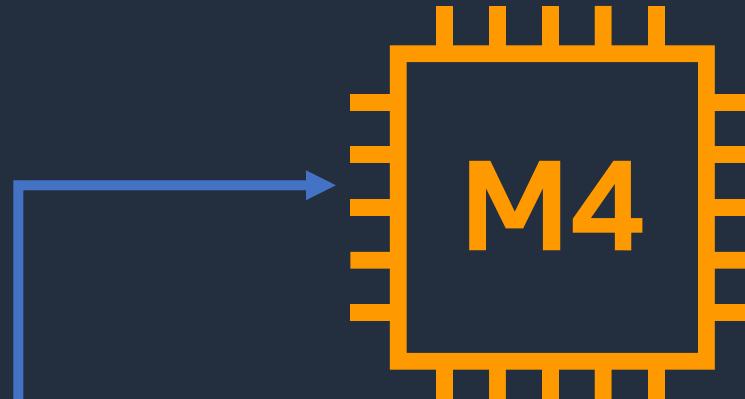
RDS scales up by changing
the **instance type**



M4 instance

db.m4.large 2 vCPUs,
8 GiB RAM

The database must shut
down and restart

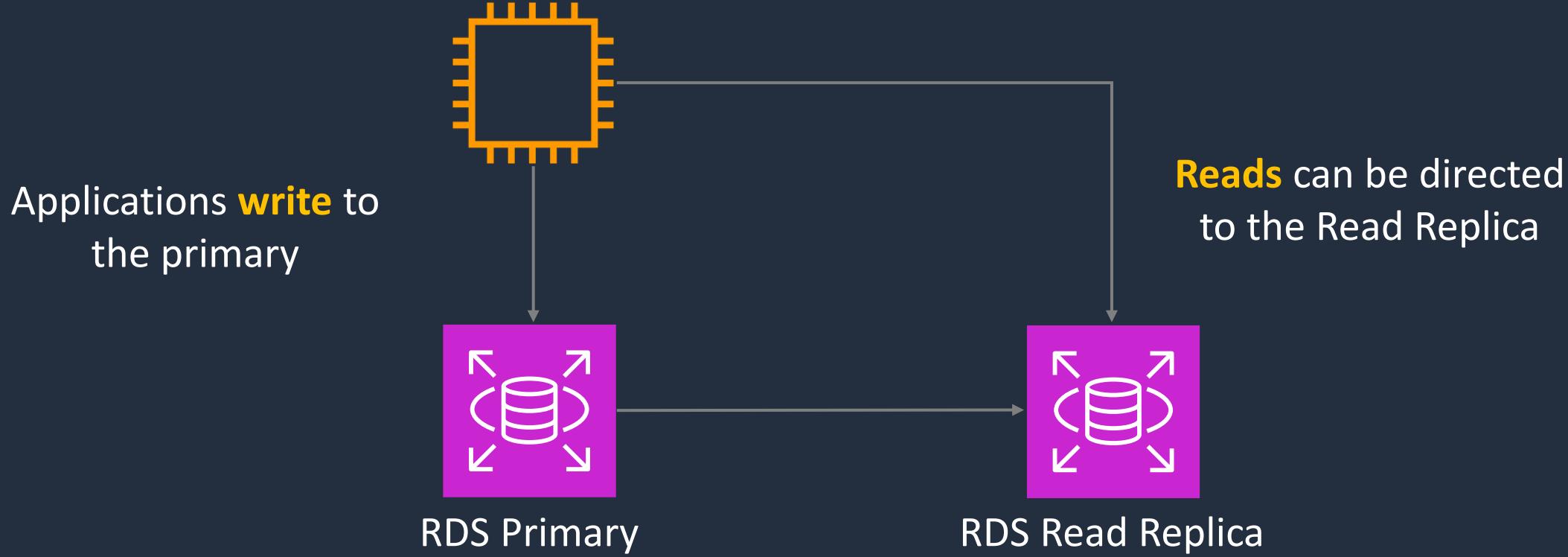


M4 Instance
db.m4.2xlarge 4
vCPUs, 32 GiB RAM

Scaling up is required for
better **write** performance



Amazon RDS – Scaling out (horizontally)

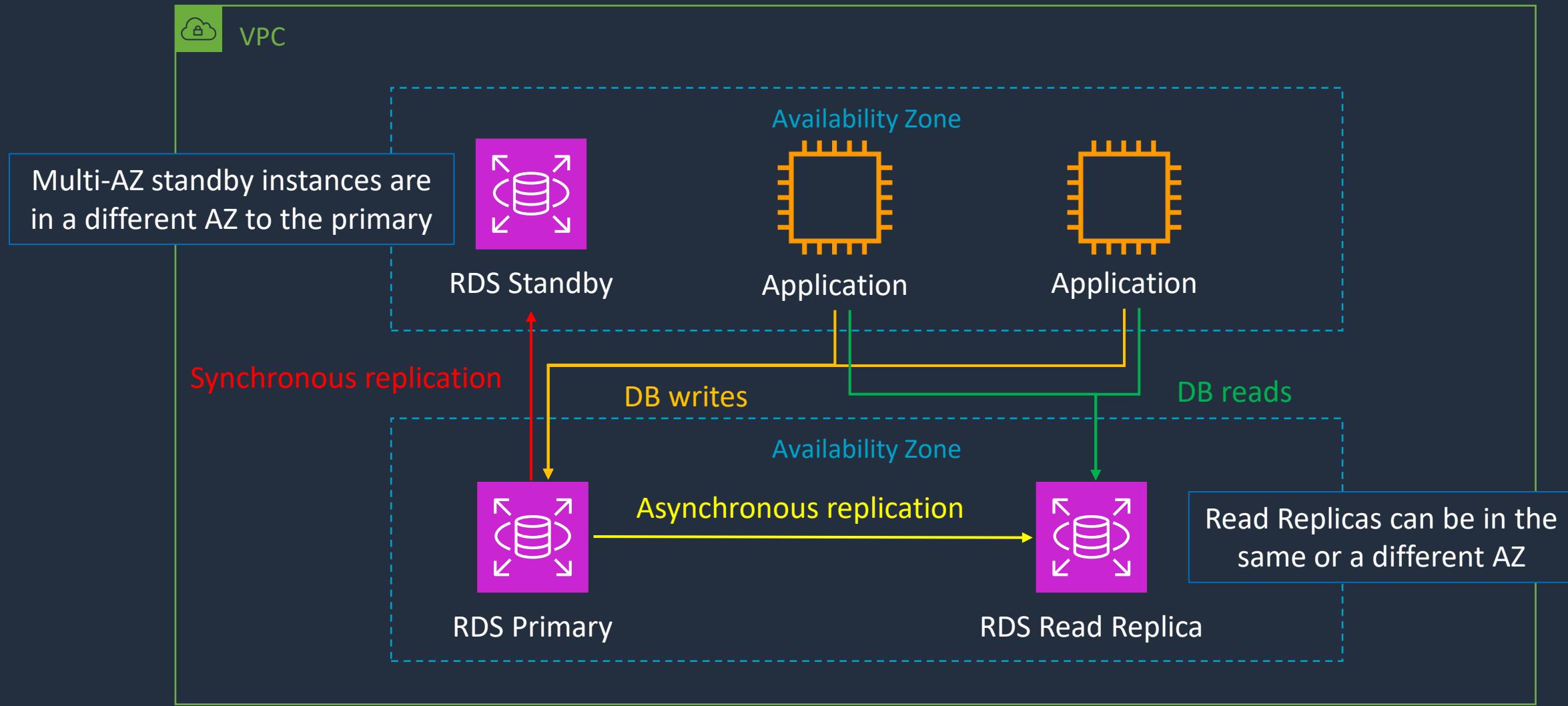


RDS scales **reads** horizontally with Read Replicas



Amazon RDS Multi AZ

Multi-AZ deployments enable automatic **disaster recovery (DR)**



Create an Amazon RDS Database



Amazon Aurora





Amazon Aurora

- Amazon Aurora is an AWS database offering in the RDS family
- Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud
- Amazon Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases
- Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 128TB per database instance

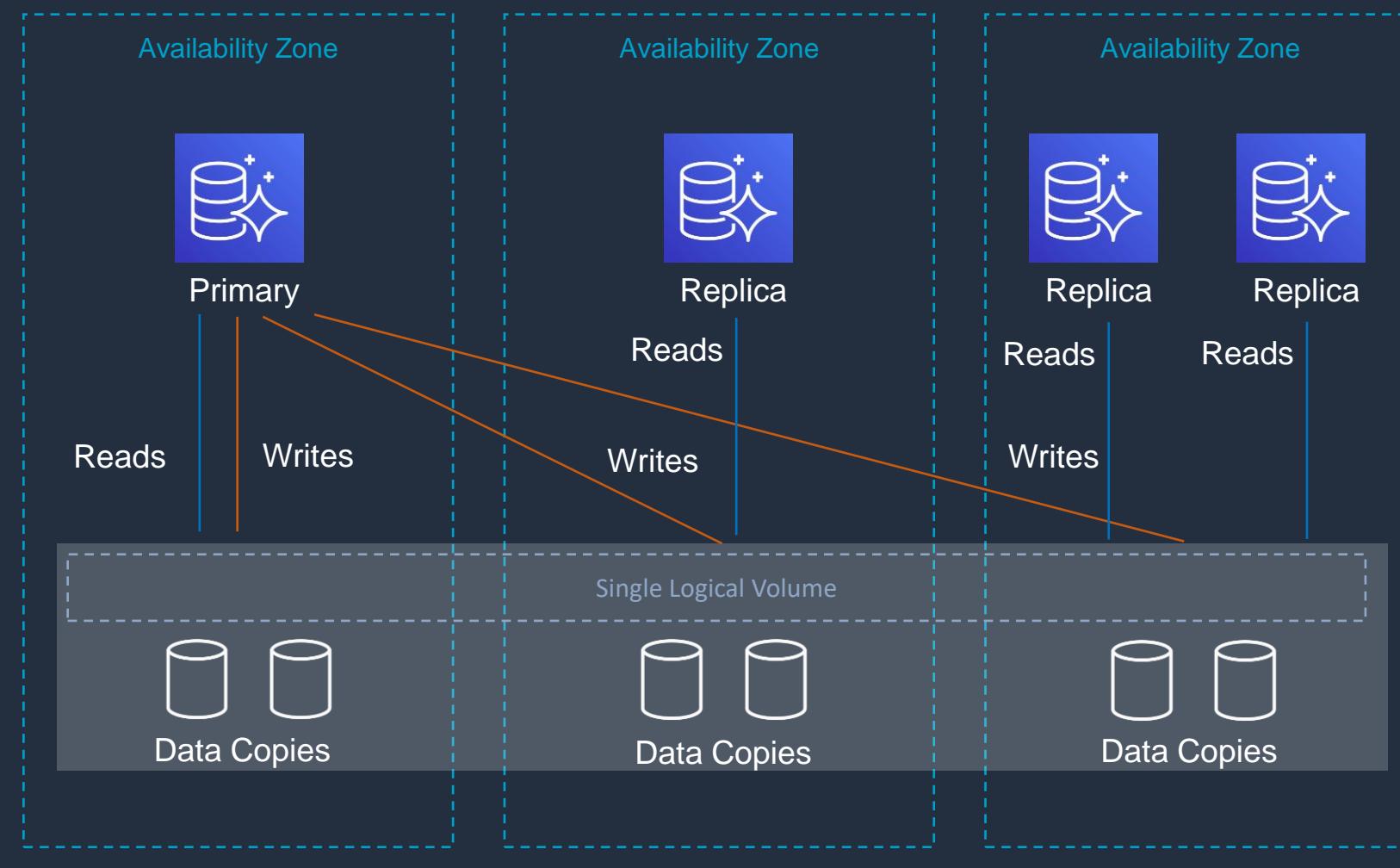


Aurora Fault Tolerance and Aurora Replicas



Region

Aurora Replicas are **within a region**



Aurora Fault Tolerance

- Fault tolerance across 3 AZs
- Single logical volume
- Aurora Replicas scale-out read requests
- Up to 15 Aurora Replicas with **sub-10ms** replica lag
- Aurora Replicas are independent endpoints
- Can **promote** Aurora Replica to be a new primary or create new primary
- Set priority (tiers) on Aurora Replicas to control order of promotion
- Can use **Auto Scaling** to add replicas



Amazon Aurora Key Features

Aurora Feature	Benefit
High performance and scalability	Offers high performance, self-healing storage that scales up to 128TB, 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 (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
Serverless	On-demand, autoscaling configuration for Amazon Aurora



Amazon Aurora Replicas

Feature	Aurora Replica	MySQL Replica
Number of replicas	Up to 15	Up to 5
Replication type	Asynchronous (milliseconds)	Asynchronous (seconds)
Performance impact on primary	Low	High
Replica location	In-region	Cross-region
Act as failover target	Yes (no data loss)	Yes (potentially minutes of data loss)
Automated failover	Yes	No
Support for user-defined replication delay	No	Yes
Support for different data or schema vs. primary	No	Yes

Amazon DynamoDB





Amazon DynamoDB

- DynamoDB is a fully managed NoSQL database service
- DynamoDB is a fully serverless service
- Key/value store and document store
- Low latency access to data (milliseconds)
- Offers push button scaling with no downtime



Data is stored in **partitions** which are replicated across multiple AZs in a Region



DynamoDB Features

DynamoDB Feature	Benefit
Serverless	Fully managed, fault tolerant, service
Highly available	99.99% availability SLA – 99.999% for Global Tables!
NoSQL type of database	Flexible schema, good for when data is not well structured or unpredictable
Horizontal scaling	Seamless scalability to any scale with push button scaling or Auto Scaling
DynamoDB Streams	Captures a time-ordered sequence of item-level modifications in a DynamoDB table
Transaction options	Strongly consistent or eventually consistent reads, support for ACID transactions
Backup	Point-in-time recovery down to the second in last 35 days; On-demand backup and restore
Global Tables	Fully managed multi-region, multi-master solution



DynamoDB Core Components

The basic DynamoDB components are:



Tables



Items



Attributes

userid	orderid	book	price	date
user001	1000092	ISBN100..	9.99	2020.04..
user002	1000102	ISBN100..	24.99	2020.03..
user003	1000168	ISBN2X0..	12.50	2020.04..



Amazon DynamoDB Pricing

Amazon DynamoDB pricing is primarily based on:

- **Provisioned Throughput:** You can choose provisioned capacity, paying for the amount of reads and writes per second that you allocate for your table
- **On-Demand Capacity:** You pay for the read and write requests your application performs on your tables without managing capacity planning
- **Storage Costs:** You pay for the data storage your tables consume
- **Additional features:** Costs apply for using Global Tables, DynamoDB Streams, backup and restore, and data transfer

Create an Amazon DynamoDB Table

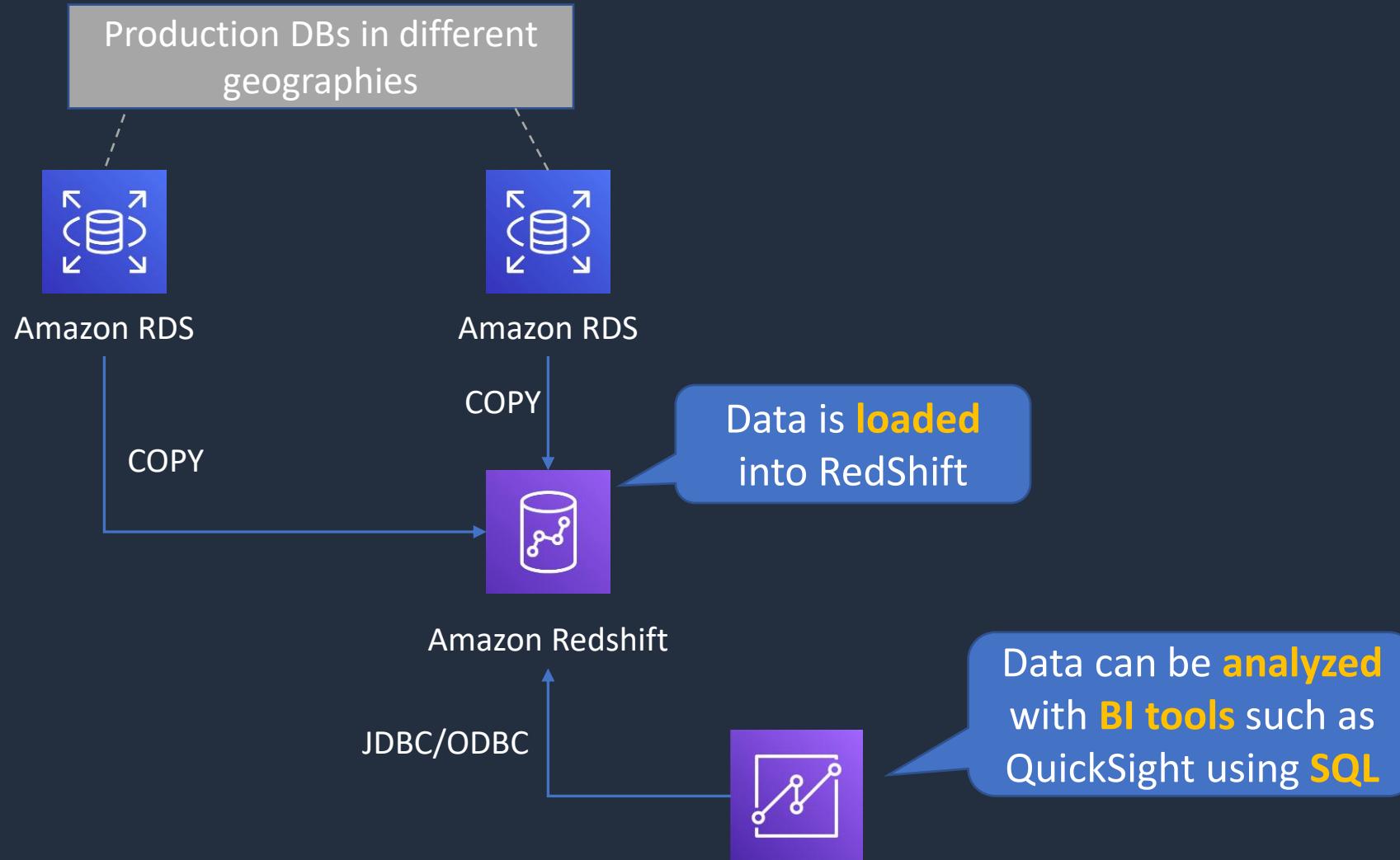


Amazon RedShift





Amazon Redshift

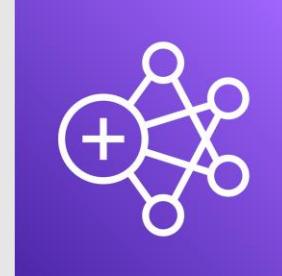




Amazon RedShift

- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools
- RedShift is a SQL based data warehouse used for analytics applications
- RedShift is a relational database that is used for Online Analytics Processing (OLAP) use cases
- RedShift uses Amazon EC2 instances, so you must choose an instance family/type
- RedShift always keeps three copies of your data
- RedShift provides continuous/incremental backups

Amazon Elastic Map Reduce (EMR)



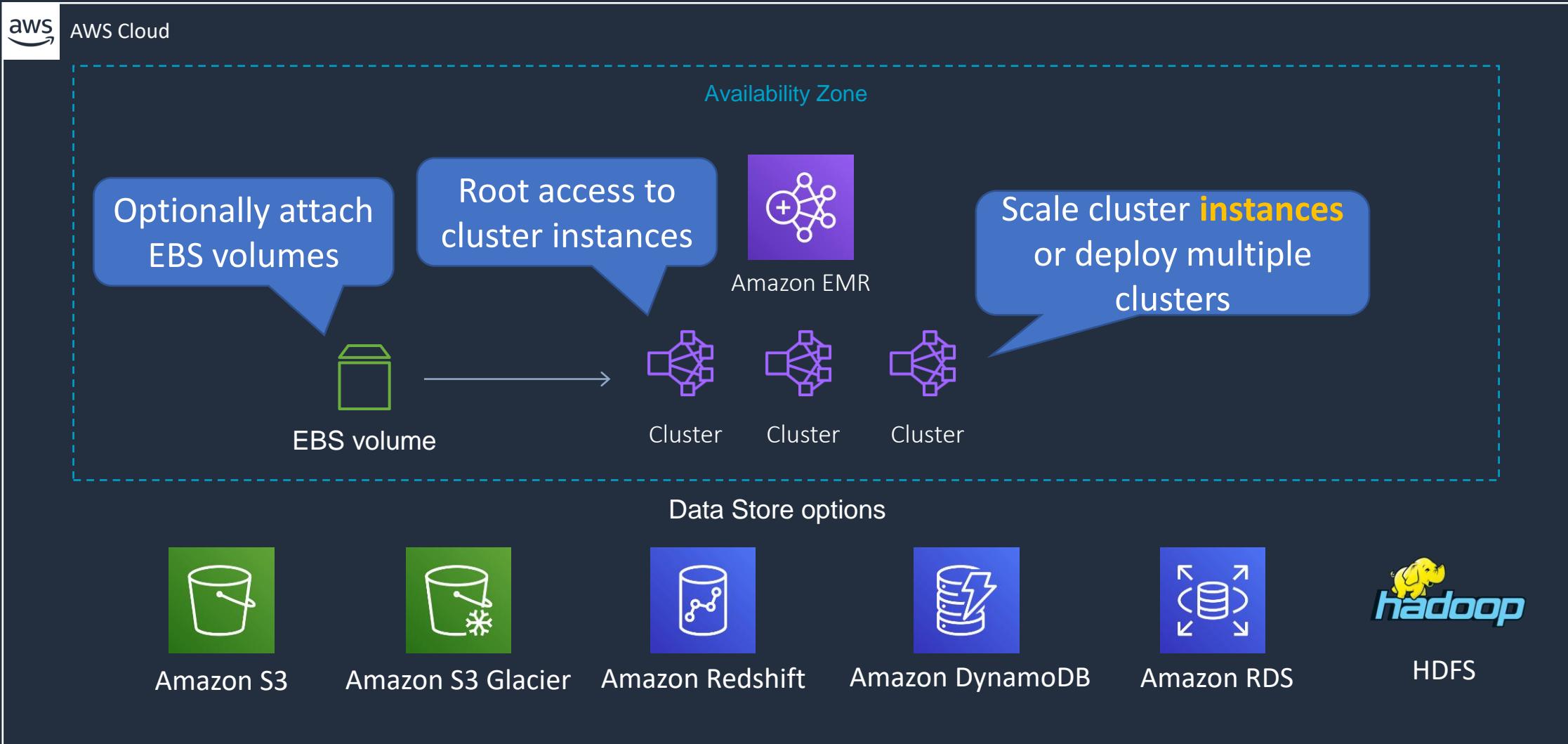


Amazon EMR

- Managed cluster platform that simplifies running big data frameworks including **Apache Hadoop** and **Apache Spark**
- Used for processing data for analytics and business intelligence
- Can also be used for transforming and moving large amounts of data
- Performs extract, transform, and load (ETL) functions



Amazon EMR



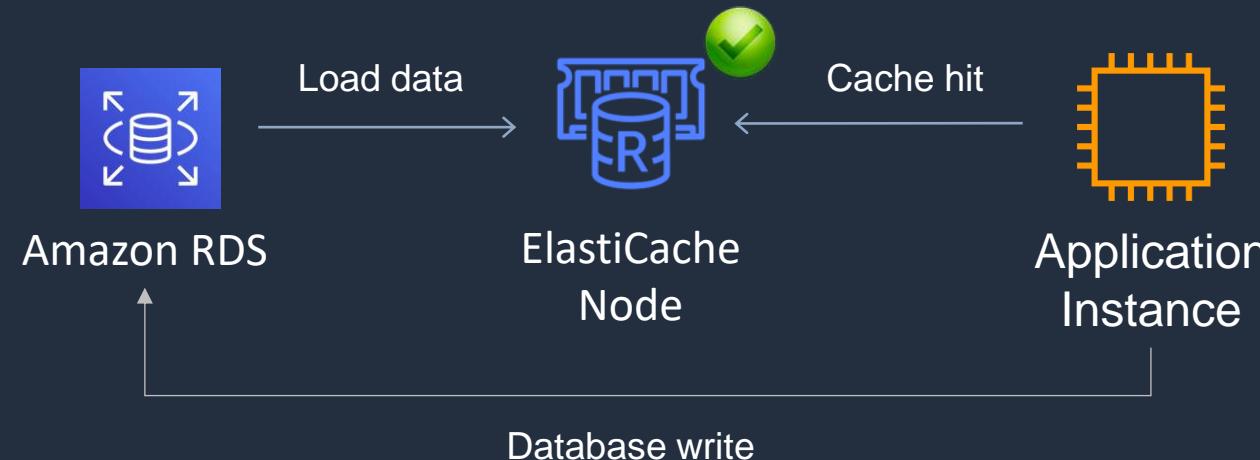
Amazon ElastiCache





Amazon ElastiCache

- Fully managed implementations **Redis** and **Memcached**
- ElastiCache is a **key/value** store
- In-memory database offering high performance and low latency
- Can be put in front of databases such as RDS and DynamoDB



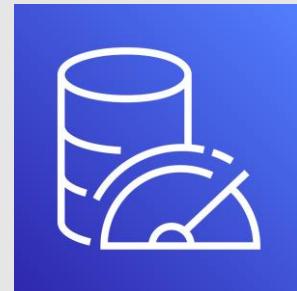


Amazon ElastiCache

- ElastiCache nodes run on Amazon EC2 instances, so you must choose an instance family/type

Use Case	Benefit
Web session store	In cases with load-balanced web servers, store web session information in Redis so if a server is lost, the session info is not lost, and another web server can pick it up
Database caching	Use Memcached in front of AWS RDS to cache popular queries to offload work from RDS and return results faster to users
Leaderboards	Use Redis to provide a live leaderboard for millions of users of your mobile app
Streaming data dashboards	Provide a landing spot for streaming sensor data on the factory floor, providing live real-time dashboard displays

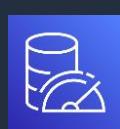
Amazon MemoryDB for Redis





Amazon MemoryDB for Redis

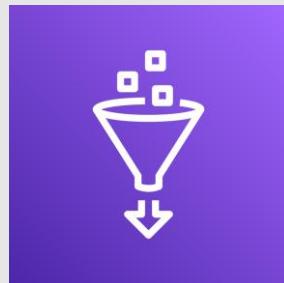
- Redis-compatible, durable, in-memory database service that delivers ultra-fast performance
- Entire dataset is stored in memory – entire DB solution
- Purpose-built for modern applications with microservices architectures
- Build applications using the same flexible and friendly Redis data structures, APIs, and commands
- Microsecond read and single-digit millisecond write latency and high throughput
- Data stored durably across multiple AZs using a distributed transactional log
- Supports write scaling with sharding and read scaling by adding replicas



MemoryDB for Redis vs ElastiCache

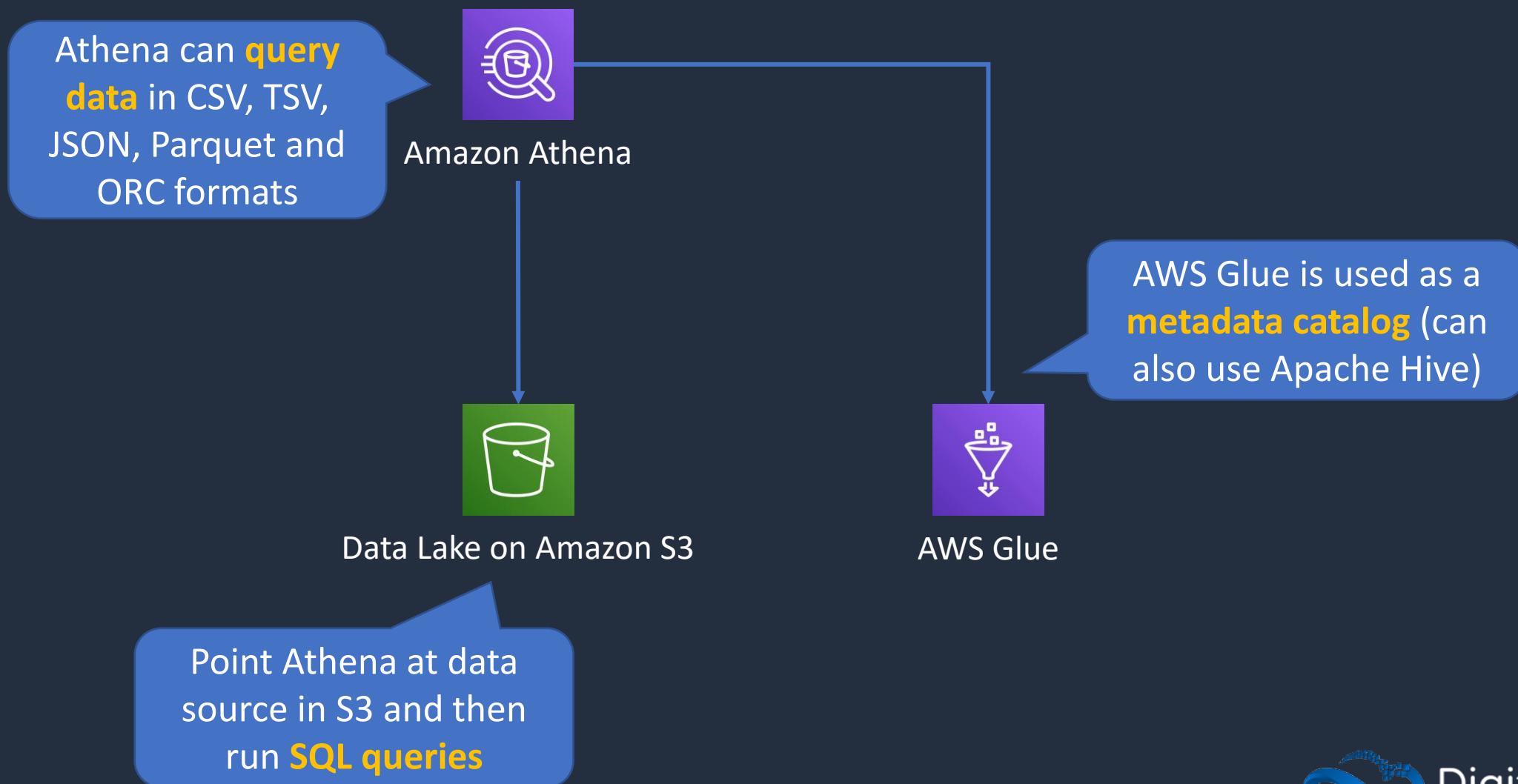
- Use ElastiCache for caching DB queries
- Use MemoryDB for a full DB solution combining DB and cache
- MemoryDB offers higher performance with lower latency
- MemoryDB offers strong consistency for primary nodes and eventual consistency for replica nodes
- With ElastiCache there can be some inconsistency and latency depending on the engine and caching strategy

Amazon Athena and AWS Glue





Amazon Athena and AWS Glue





Amazon Athena

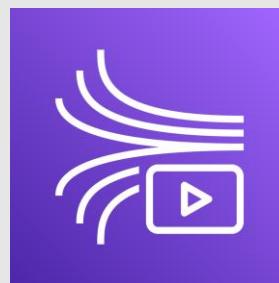
- Athena queries data in S3 using SQL
- Can be connected to other data sources with Lambda
- Data can be in CSV, TSV, JSON, Parquet and ORC formats
- Uses a managed Data Catalog (AWS Glue) to store information and schemas about the databases and tables



AWS Glue

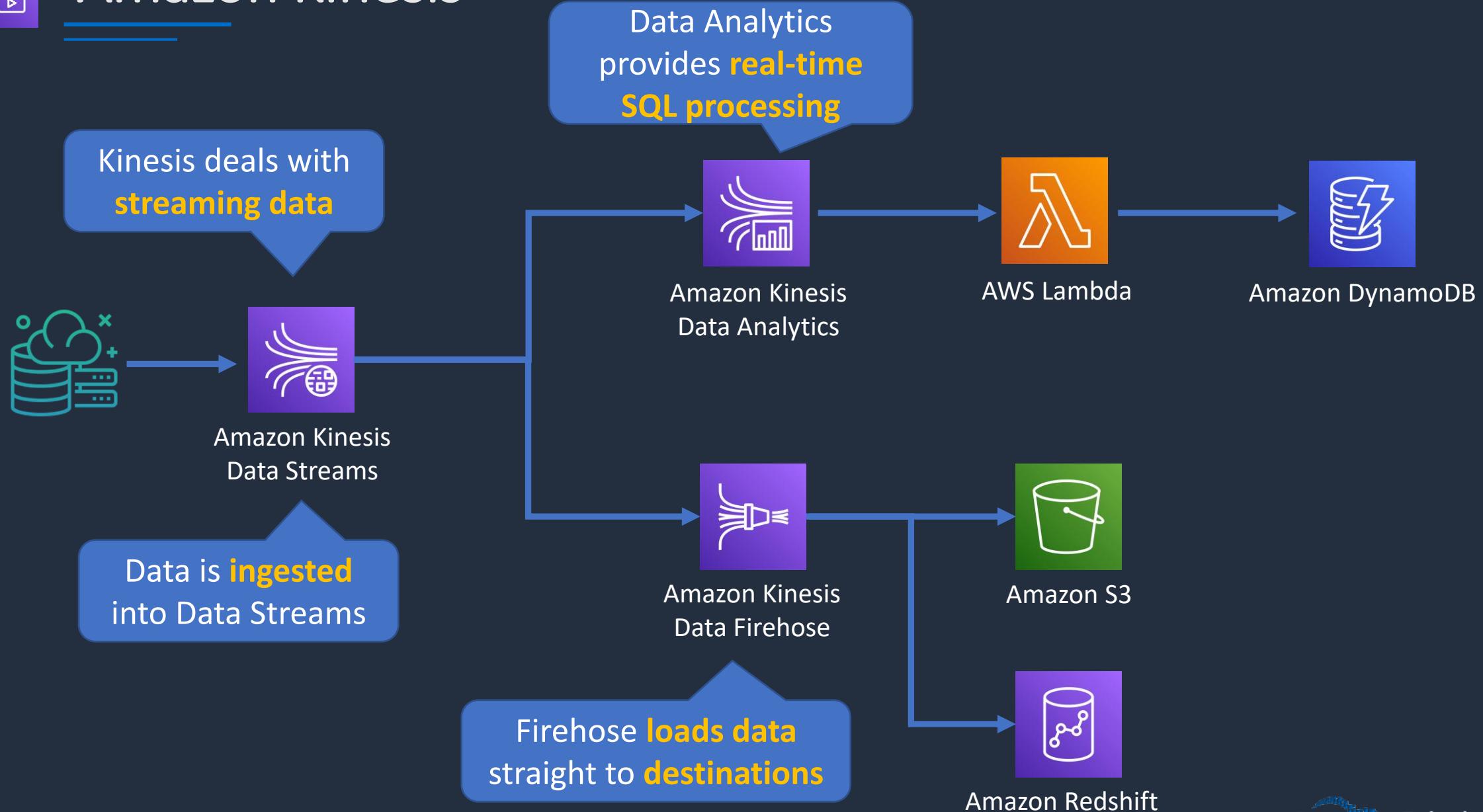
- Fully managed extract, transform and load (ETL) service
- Used for preparing data for analytics
- AWS Glue runs the ETL jobs on a fully managed, scale-out Apache Spark environment
- Works with data lakes (e.g. data on S3), data warehouses (including RedShift), and data stores (including RDS or EC2 databases)

Amazon Kinesis





Amazon Kinesis





Amazon Kinesis

Examples of streaming data use cases include:

- Purchases from online stores
- Stock prices
- Game data (statistics and results as the gamer plays)
- Social network data
- Geospatial data (think uber.com)
- IoT sensor data



Amazon Kinesis

Kinesis Data Streams

- Producers send data which is stored in shards for up to 7 days
- Consumers process the data and save to another service

Amazon Kinesis Data Firehose

- No shards, completely automated and elastically scalable
- Saves data directly to another service such as S3, Splunk, RedShift, or Elasticsearch

Amazon Kinesis Data Analytics

- Provides real-time SQL processing for streaming data

Amazon OpenSearch Service (Elasticsearch)





Amazon OpenSearch Service



Successor to **Amazon Elasticsearch Service**

Search, visualize, and analyze **text and unstructured data**

Amazon OpenSearch Service

Deploy **nodes** and **replicas** across AZs



Fully Managed



Petabyte Scale



Secure



Highly Available



Scalable

Deploy to **Amazon VPC** and integrates with **IAM**



DigitalCloud
TRAINING



Amazon OpenSearch Service

- Distributed search and analytics suite
- Based on the popular open source Elasticsearch
- Supports queries using SQL syntax
- Integrates with open-source tools
- Scale by adding or removing instances
- Availability in up to three Availability Zones
- Backup using snapshots
- Encryption at-rest and in-transit

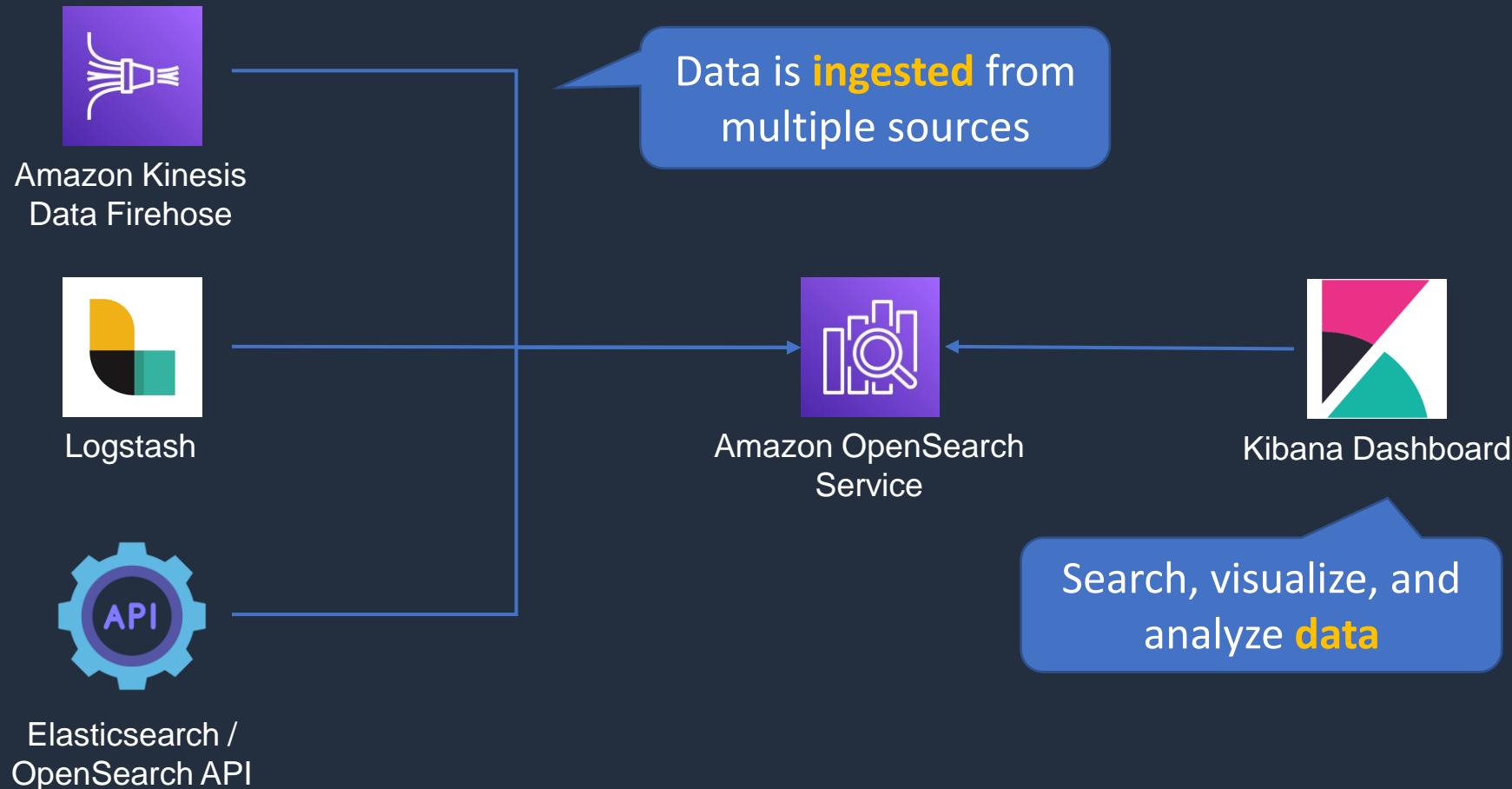


OpenSearch Service Deployment

- Clusters are created (Management Console, API, or CLI)
- Clusters are also known as OpenSearch Service domains
- You specify the number of instances and instance types
- Storage options include UltraWarm or Cold storage



Ingesting Data into OpenSearch Service Domains





OpenSearch in an Amazon VPC

- Clusters can be deployed in a VPC for secure intra-VPC communications
- VPN or proxy required to connect from the internet (public domains are directly accessible)
- Cannot use IP-based access policies



OpenSearch in an Amazon VPC

- Limitations of VPC deployments:
 - You can't switch from VPC to a public endpoint. The reverse is also true
 - You can't launch your domain within a VPC that uses dedicated tenancy
 - After you place a domain within a VPC, you can't move it to a different VPC, but you can change the subnets and security group settings



The ELK Stack

- ELK stands for Elasticsearch, Logstash, and Kibana



Logstash



Amazon OpenSearch
Service



Kibana Dashboard

- This is a popular combination of projects
- Aggregate logs from systems and applications, analyze these logs, and create visualizations
- Use cases include:
 - Visualizing application and infrastructure monitoring data
 - Troubleshooting
 - Security analytics



OpenSearch Access Control

- **Resource-based policies** – often called a domain access policy
- **Identity-based policies** – attached to users or roles (principals)
- **IP-based policies** – Restrict access to one or more IP addresses or CIDR blocks
- **Fine-grained access control** – Provides:
 - Role-based access control
 - Security at the index, document, and field level
 - OpenSearch Dashboards multi-tenancy
 - HTTP basic authentication for OpenSearch and OpenSearch Dashboards



OpenSearch Access Control

- Authentication options include:
 - Federation using SAML to on-premises directories
 - Amazon Cognito and social identity providers



OpenSearch Best Practices

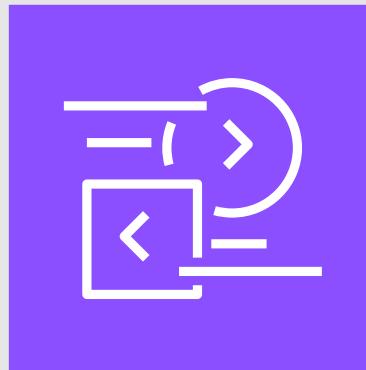
- Deploy OpenSearch data instances across three Availability Zones (AZs) for the best availability
- Provision instances in multiples of three for equal distribution across AZs
- If three AZs are not available use two AZs with equal numbers of instances



OpenSearch Best Practices

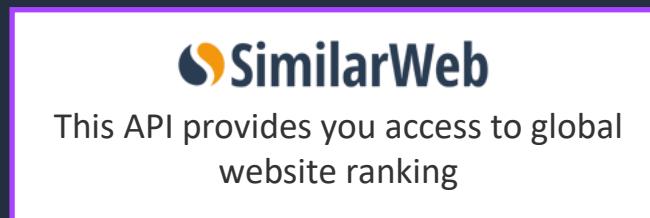
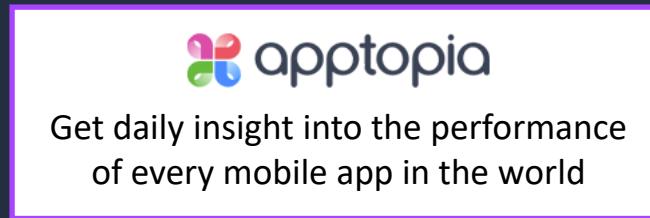
- Use three dedicated master nodes
- Configure at least one replica for each index
- Apply restrictive resource-based access policies to the domain (or use fine-grained access control)
- Create the domain within an Amazon VPC
- For sensitive data enable node-to-node encryption and encryption at rest

AWS Data Exchange

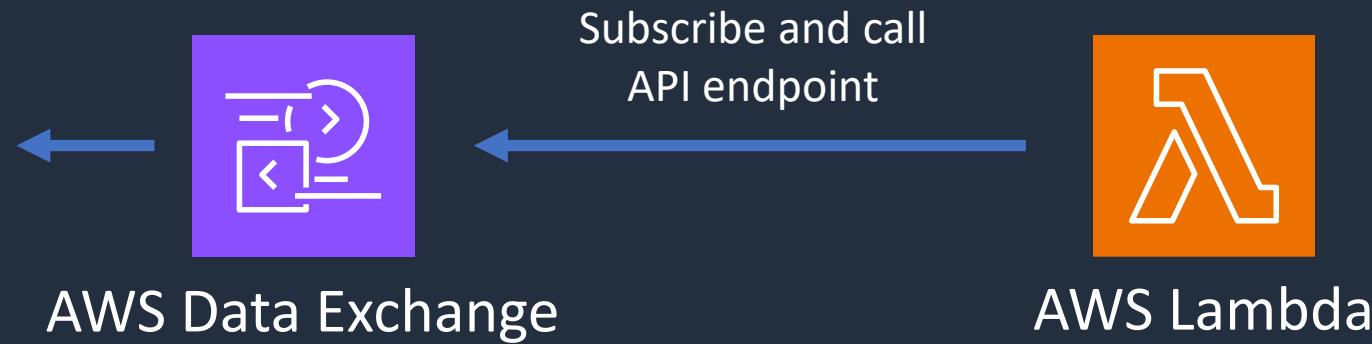




AWS Data Exchange



Example Data Sets



- **Publish Products** – Create data sets, publish products, and get subscriptions
- **Dynamically update products** – Create revisions, upload assets, and publish services
- **Receive Reports** – Receive daily, weekly, and monthly reports on subscription activity



AWS Data Exchange

AWS Data Exchange is a platform that facilitates the secure exchange and use of data products, including third-party data

- **Extensive Data Sets** – 3,500+ data sets from 300+ providers
- **Providers and Subscribers** – Data providers publish data products to AWS Data Exchange, and subscribers can then find and subscribe to these data products
- **Data Sets** – Data products are composed of one or more data sets, which are collections of data that are related to each other

Use Cases:

- **Business Intelligence** – AWS Data Exchange can be used to enhance business intelligence and analytics solutions
- **Machine Learning** – Data from AWS Data Exchange can be used to create more effective machine learning models



AWS Data Exchange

- **AWS Data Exchange for Amazon S3** – data subscribers can find, subscribe to, and use third-party files directly from data providers' S3 buckets
- **AWS Data Exchange for AWS Lake Formation** – Access to live, ready-to-use structured tables through Lake Formation
- **Data APIs** – Use AWS IAM credentials and AWS SDKs to call data APIs from hundreds of data providers
- **Data Files** – Automatically export new or updated data to your Amazon S3 buckets
- **Data Tables** – Find and subscribe to third-party data in AWS Data Exchange and directly query the data in minutes in Amazon Redshift

Amazon MSK





Amazon Managed Streaming for Apache Kafka (MSK)

- Amazon MSK is a fully managed service that enables you to build and run applications that use Apache Kafka to process streaming data
- Amazon MSK is used for ingesting and processing streaming data in real-time
- Amazon MSK provides the control-plane operations, such as those for creating, updating, and deleting clusters
- It lets you use Apache Kafka data-plane operations, such as those for producing and consuming data



Amazon Managed Streaming for Apache Kafka (MSK)

Components include:

- **Kafka Clusters** – Kafka clusters are at the core of MSK, which consists of a set of Kafka brokers coordinated by Zookeeper nodes
- **Broker nodes** — These are Kafka servers that store data and serve clients. Clusters typically contain multiple brokers to ensure data reliability and availability
- **ZooKeeper nodes** — Apache Zookeeper manages and coordinates the Kafka brokers. MSK automatically sets up a highly available Zookeeper ensemble for every Kafka cluster
- **Producers** — Kafka clients that publish data to Kafka topics
- **Consumers** — Kafka clients that read data from Kafka topics
- **Topics** – Topics are data streams where producers publish data. They are an essential part of Kafka that enables the organization of data in a way that can be consumed by different clients

Other Databases and Analytics Services





Other Databases and Analytics Services

AWS Data Pipeline

- Processes and moves data between different AWS compute and storage services
- Save results to services including S3, RDS, DynamoDB, and EMR

Amazon QuickSight

- Business intelligence (BI) service
- Create and publish interactive BI dashboards for Machine Learning-powered insights

Amazon Neptune

- Fully managed graph database service



Other Databases and Analytics Services

Amazon DocumentDB

- Fully managed document database service (non-relational)
- Supports MongoDB workloads
- Queries and indexes JSON data

Amazon QLDB

- Fully managed ledger database for immutable change history
- Provides cryptographically verifiable transaction logging

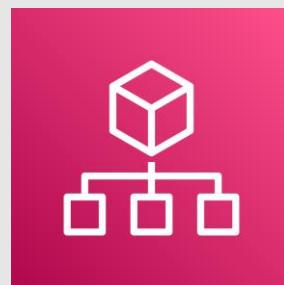
Amazon Managed Blockchain

- Fully managed service for joining public and private networks using Hyperledger Fabric and Ethereum

SECTION 12

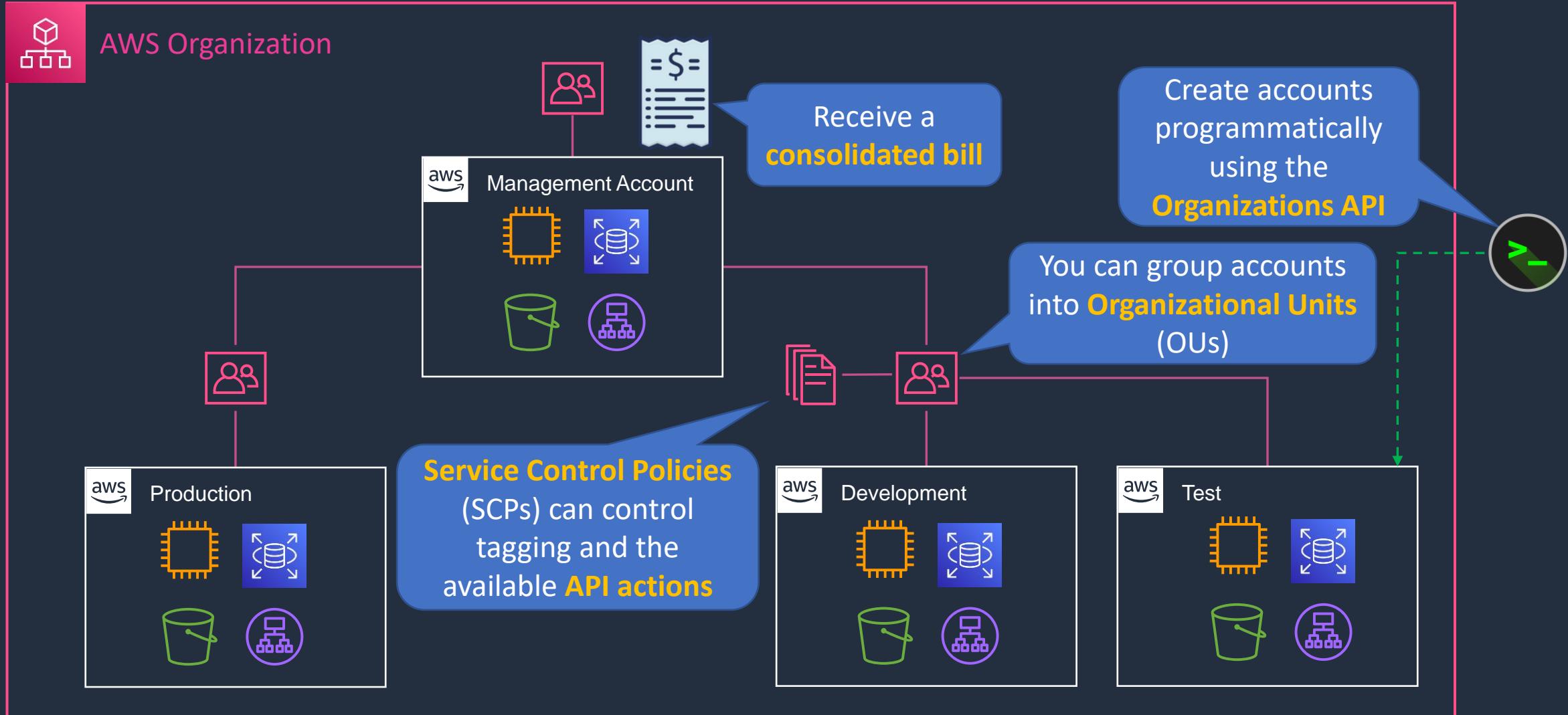
Management and Governance

AWS Organizations





AWS Organizations





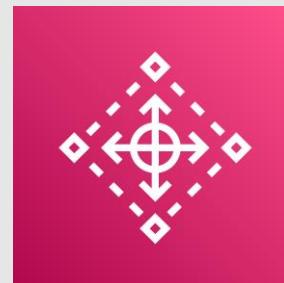
AWS Organizations

- AWS organizations allows you to consolidate multiple AWS accounts into an organization that you create and centrally manage
- Available in two feature sets:
 - **Consolidated Billing**
 - **All features**
- Includes root accounts and organizational units
- Policies are applied to root accounts or OUs
- Consolidated billing includes:
 - **Paying Account** – independent and cannot access resources of other accounts
 - **Linked Accounts** – all linked accounts are independent

AWS Organizations



AWS Control Tower





AWS Control Tower

- Simplifies the process of creating multi-account environments
- Sets up governance, compliance, and security guardrails for you
- Integrates with other services and features to setup the environment for you including:
 - AWS Organizations, SCPs, OUs, AWS Config, AWS CloudTrail, Amazon S3, Amazon SNS, AWS CloudFormation, AWS Service Catalog, AWS Single Sign-On (SSO)



AWS Control Tower

Examples of guardrails AWS Control Tower can configure for you include:

- Disallowing public write access to Amazon Simple Storage Service (Amazon S3) buckets
- Disallowing access as a root user without multi-factor authentication
- Enabling encryption for Amazon EBS volumes attached to Amazon EC2 instances

AWS Systems Manager





AWS Systems Manager

- Manages many AWS resources including Amazon EC2, Amazon S3, Amazon RDS etc.
- Systems Manager Components:
 - **Automation**
 - **Run Command**
 - **Inventory**
 - **Patch Manager**
 - **Session Manager**
 - **Parameter Store**

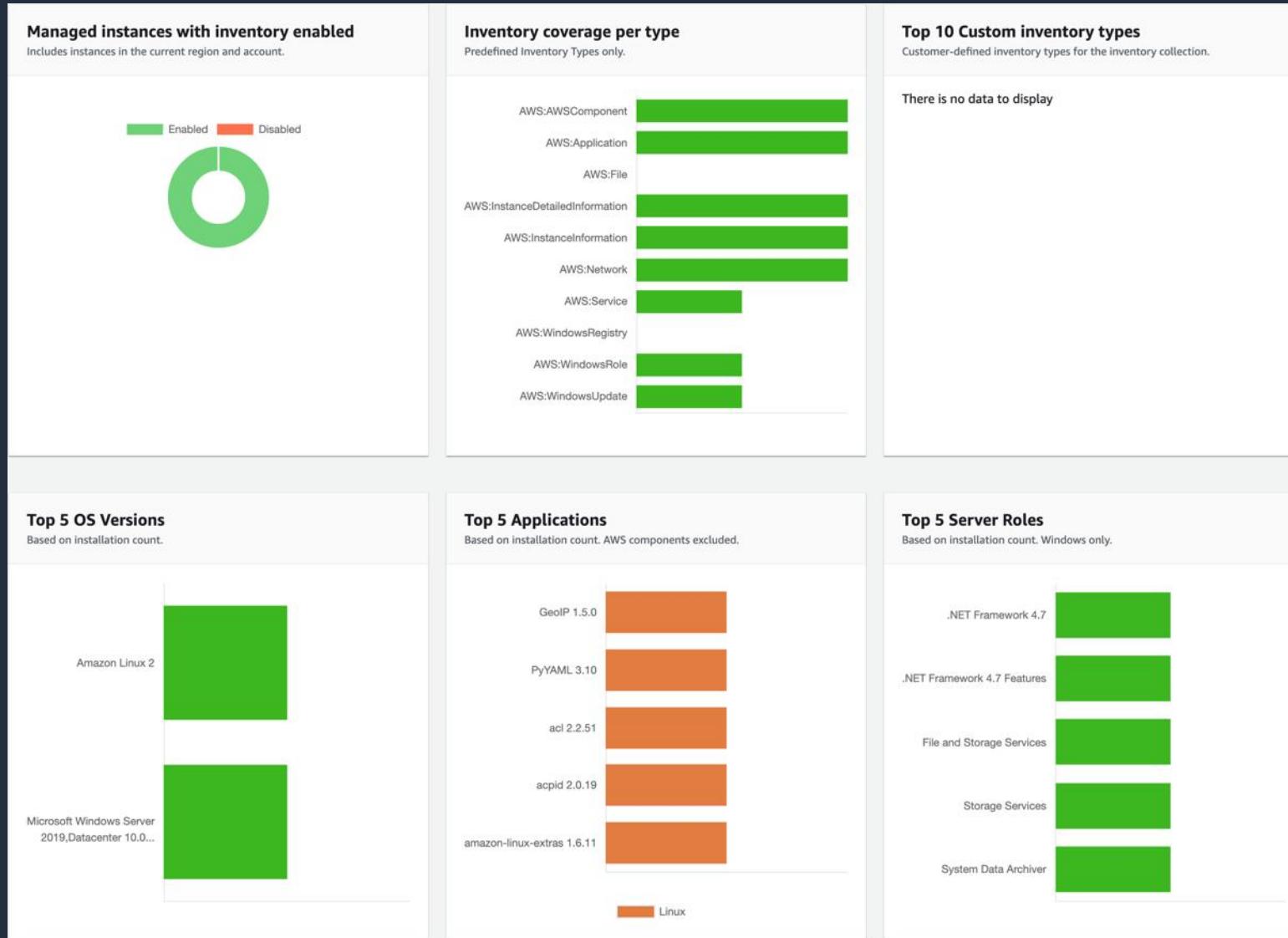


AWS Systems Manager





AWS Systems Manager



Inventory



AWS Systems Manager

Patch Manager

- Deploy operating system and software patches automatically across large groups of Amazon EC2 or on-premises instances

Compliance

- Scan managed instances for patch compliance and configuration inconsistencies



AWS Systems Manager

Session Manager

- Secure remote management of your instances at scale without logging into your servers
- Replaces the need for bastion hosts, SSH, or remote PowerShell

Parameter Store

- Parameter Store provides secure, hierarchical storage for configuration data management and secrets management

AWS Service Catalog



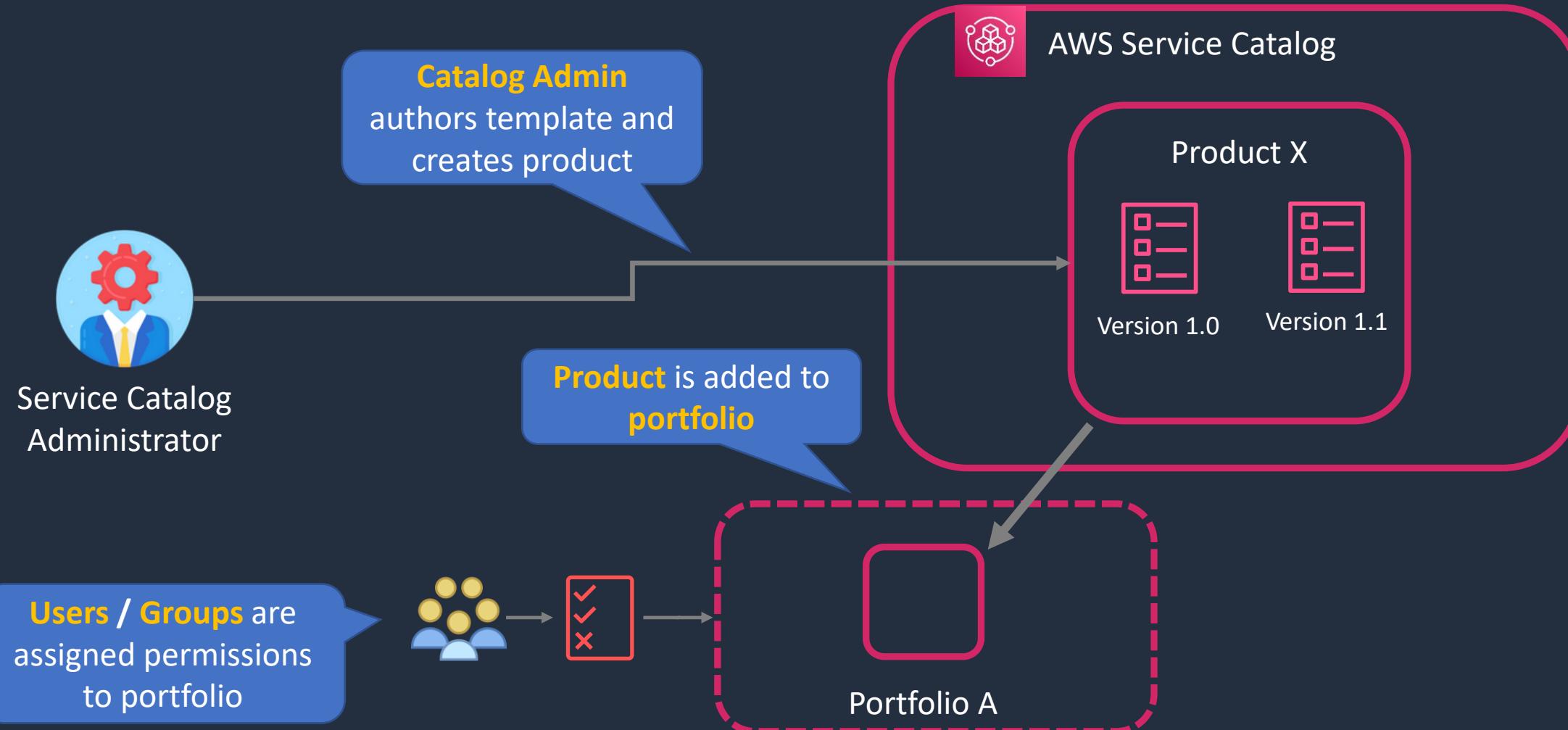


AWS Service Catalog

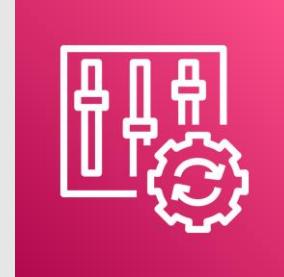
- AWS Service Catalog allows organizations to create and manage **catalogs of IT services** that are approved for use on AWS
- AWS Service Catalog allows you to **centrally manage** commonly deployed IT services
- IT services can include virtual machine images, servers, software, and databases and multi-tier application architectures
- Enables users to quickly deploy only the approved IT services they need



AWS Service Catalog



AWS Config

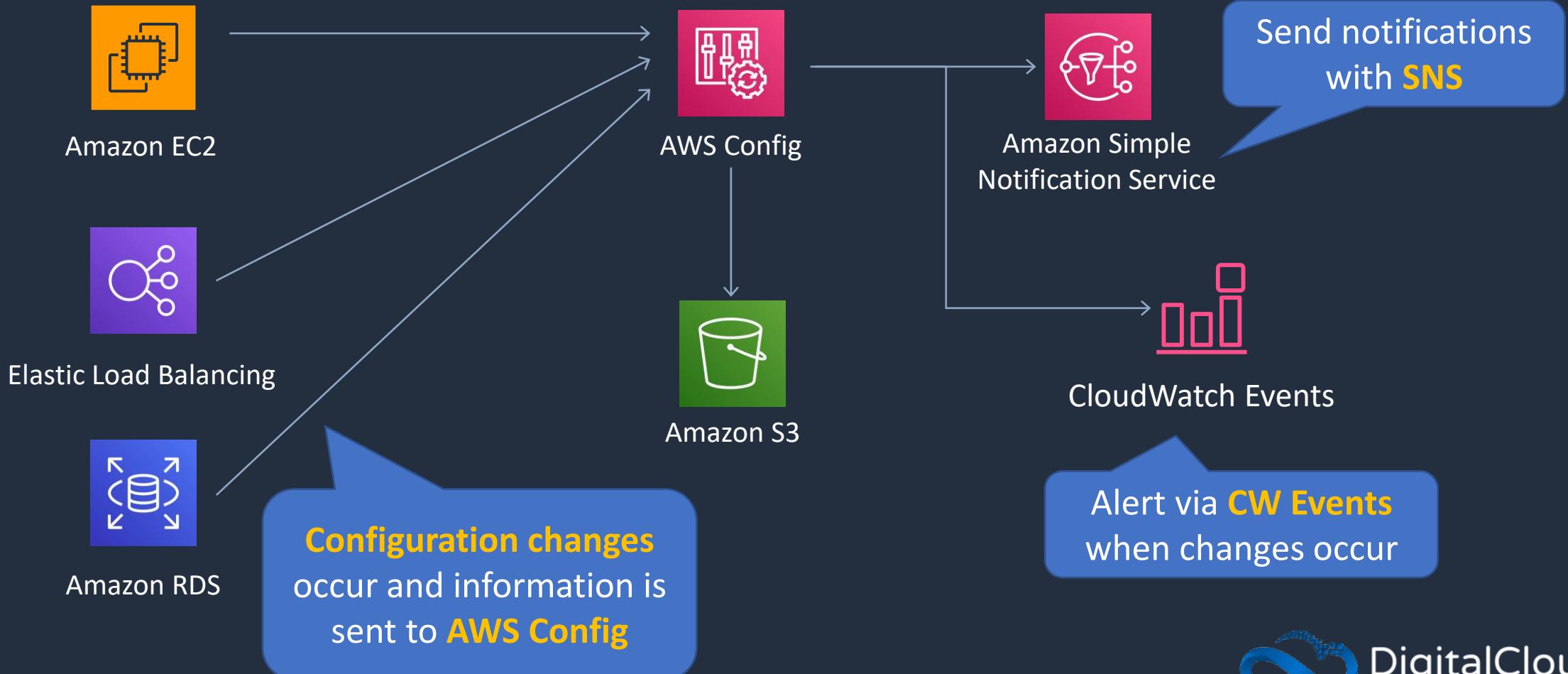




AWS Config

AWS Config evaluates the **configuration** against desired configurations

Example Services:

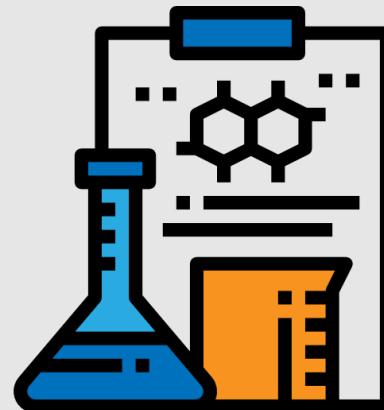




AWS Config

Example Rule	Description
s3-bucket-server-side-encryption-enabled	Checks that your Amazon S3 bucket either has S3 default encryption enabled or that the S3 bucket policy explicitly denies put-object requests without server side encryption
restricted-ssh	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic
rds-instance-public-access-check	Checks whether the Amazon Relational Database Service (RDS) instances are not publicly accessible
cloudtrail-enabled	Checks whether AWS CloudTrail is enabled in your AWS account

Configuration Compliance with AWS Config



AWS Trusted Advisor





AWS Trusted Advisor

- Trusted Advisor is an online resource that helps to reduce cost, increase performance and improve security by optimizing your AWS environment
- Trusted Advisor provides real time guidance to help you provision your resources following best practices
- Advisor will advise you on **Cost Optimization**, **Performance**, **Security**, and **Fault Tolerance**

AWS Health API and Dashboards





AWS Personal Health Dashboard

- AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may **impact you**
- Personal Health Dashboard gives you a **personalized** view into the performance and availability of the AWS services underlying your AWS resources
- Also provides proactive notification to help you plan for scheduled activities



AWS Service Health Dashboard

Not personalized information so may not be relevant to you

No proactive notification of scheduled activities

Current Status - Jun 7, 2020 PDT

Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

North America	South America	Europe	Africa	Asia Pacific	Middle East	Contact Us
Recent Events	Details				RSS	
No recent events.						
Remaining Services		Details			RSS	
Alexa for Business (N. Virginia)		Service is operating normally				
Amazon API Gateway (Montreal)		Service is operating normally				
Amazon API Gateway (N. California)		Service is operating normally				
Amazon API Gateway (N. Virginia)		Service is operating normally				
Amazon API Gateway (Ohio)		Service is operating normally				
Amazon API Gateway (Oregon)		Service is operating normally				
Amazon AppStream 2.0 (N. Virginia)		Service is operating normally				
Amazon AppStream 2.0 (Oregon)		Service is operating normally				
Amazon Athena (Montreal)		Service is operating normally				
Amazon Athena (N. Virginia)		Service is operating normally				
Amazon Athena (Ohio)		Service is operating normally				
Amazon Athena (Oregon)		Service is operating normally				

Shows current status information on service availability

AWS Compute Optimizer





AWS Compute Optimizer

- Recommends optimal AWS resources for your workloads to reduce costs and improve performance
- Uses machine learning to analyze historical utilization metrics
- Offers optimization guidance for:
 - Amazon EC2 instances
 - Amazon EBS volumes
 - AWS Lambda functions
- Results can be viewed in the console or via the CLI



AWS Compute Optimizer

AWS Compute Optimizer > Dashboard

Dashboard Info

Findings per AWS resource

090765505187 ▾

Filter by one or more Regions

Region: US East (N. Virginia)

EC2 instances (13) Info

30.77% Under-provisioned 7.... 61.54% Over-provisioned

Findings

- Under-provisioned: 4 instances
- Optimized: 1 instance
- Over-provisioned: 8 instances

[View recommendations for EC2 instances](#)

Auto Scaling groups (1) Info

100% Not optimized

Findings

- Not optimized: 1 group
- Optimized: 0 groups

[View recommendations for Auto Scaling groups](#)



AWS Compute Optimizer

AWS Compute Optimizer > Dashboard > Recommendations for EC2 instances

Recommendations for EC2 instances (8) Info

Recommendations for modifying current resources for better cost and performance.

Action ▾

View detail

Filter by one or more Regions

090765505187 ▾

Over-provisioned ▾

< 1 >

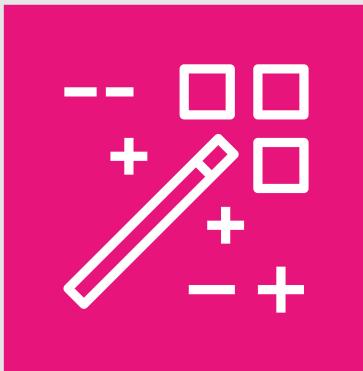


Region: US East (N. Virginia) X

Clear filters

Instance ID ▾	Instance name ▾	Finding ▾	Current Instance type ▾	Current On-Demand price ▾	Recommended Instance type ▾	Recommended On-Demand price
i-0fb9323080785de1e	-	Over-provisioned	c5.xlarge	\$0.17 per hour	t3.large	\$0.0832 per hour
i-0f4f4c06ad8afe81a	-	Over-provisioned	m5.2xlarge	\$0.384 per hour	r5.xlarge	\$0.252 per hour
i-0f277818dfef522e9	-	Over-provisioned	c5.xlarge	\$0.17 per hour	t3.large	\$0.0832 per hour
i-0ceb95ed248026d24	-	Over-provisioned	m5.xlarge	\$0.192 per hour	r5.large	\$0.126 per hour
i-0af9322ff627d7e8f	-	Over-provisioned	m5.xlarge	\$0.192 per hour	r5.large	\$0.126 per hour
i-07084b94d1bcf391b	-	Over-provisioned	c5.xlarge	\$0.17 per hour	t3.large	\$0.0832 per hour
i-069f6e837890db127	-	Over-provisioned	c5.xlarge	\$0.17 per hour	t3.large	\$0.0832 per hour
i-0218a45abd8b53658	-	Over-provisioned	m5.xlarge	\$0.192 per hour	r5.large	\$0.126 per hour

AWS Launch Wizard





AWS Launch Wizard

- AWS Launch Wizard offers a guided way of sizing, configuring, and deploying AWS resources for third party applications
- Focuses on the deployment of enterprise applications like SQL Server Always On, SAP, and Active Directory
- Automatically identifies and deploys the most cost-effective and optimal resources for your application based on your input and requirements
- Why Choose AWS Launch Wizard?
 - **Simplified Deployments:** Offers a straightforward solution to deploy complex applications, removing the traditional complexities involved
 - **Resource Optimization:** Ensures that you get the best utilization of AWS resources tailored to your application needs
 - **Quick Start:** Facilitates a quick start to application deployment, helping businesses to get their applications up and running in a shorter timeframe

SECTION 13

AWS Cloud Security and Identity

Identity Providers and Federation

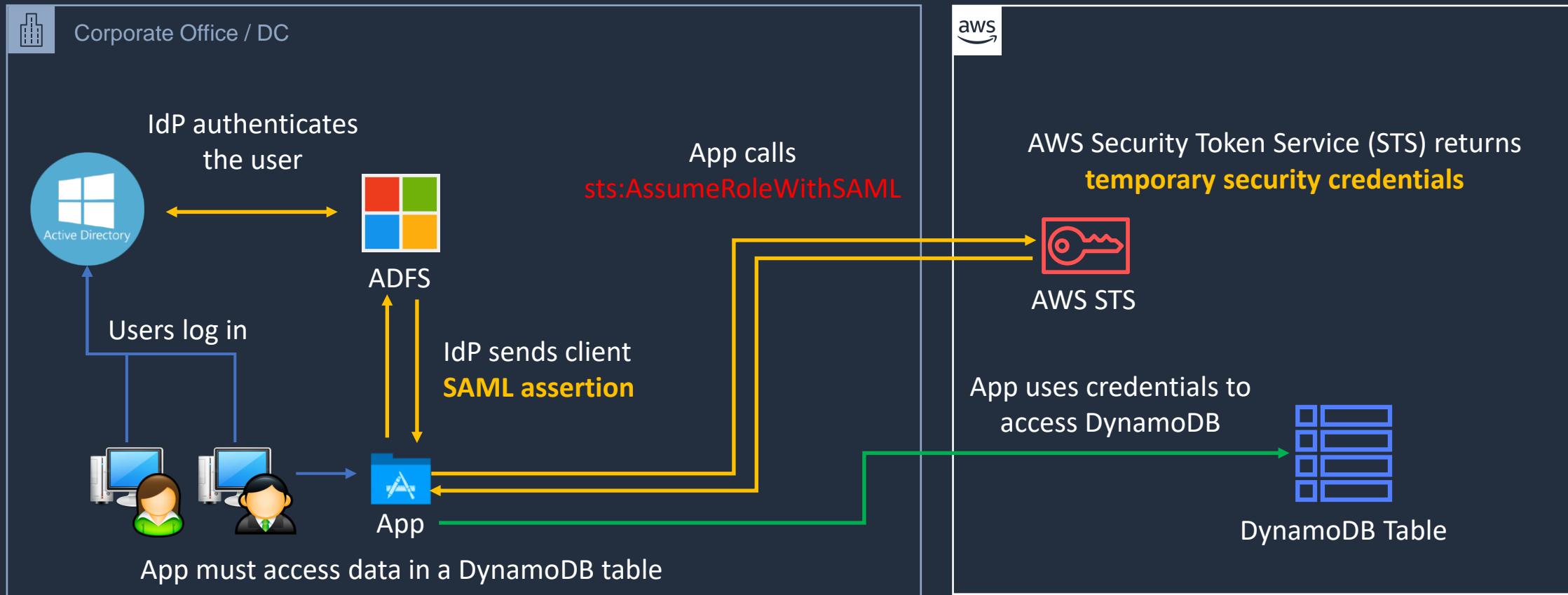




IAM – SAML 2.0 Identity Federation

Active Directory is an
LDAP **Identity Store**

Active Directory Federation Services
is an **Identity Provider** (IdP)





IAM – Web Identity Federation

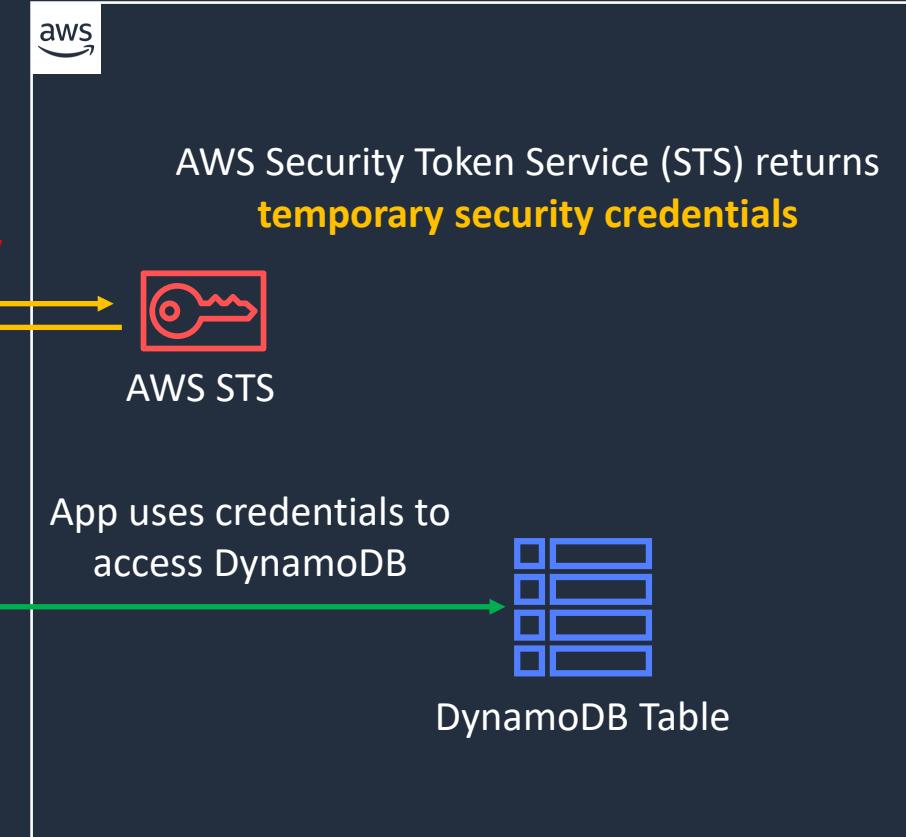
Any **Open ID Connect (OIDC)**
compatible IdP supported

Social identity providers (IdPs)



Mobile App

App calls
`sts:AssumeRoleWithWebIdentity`



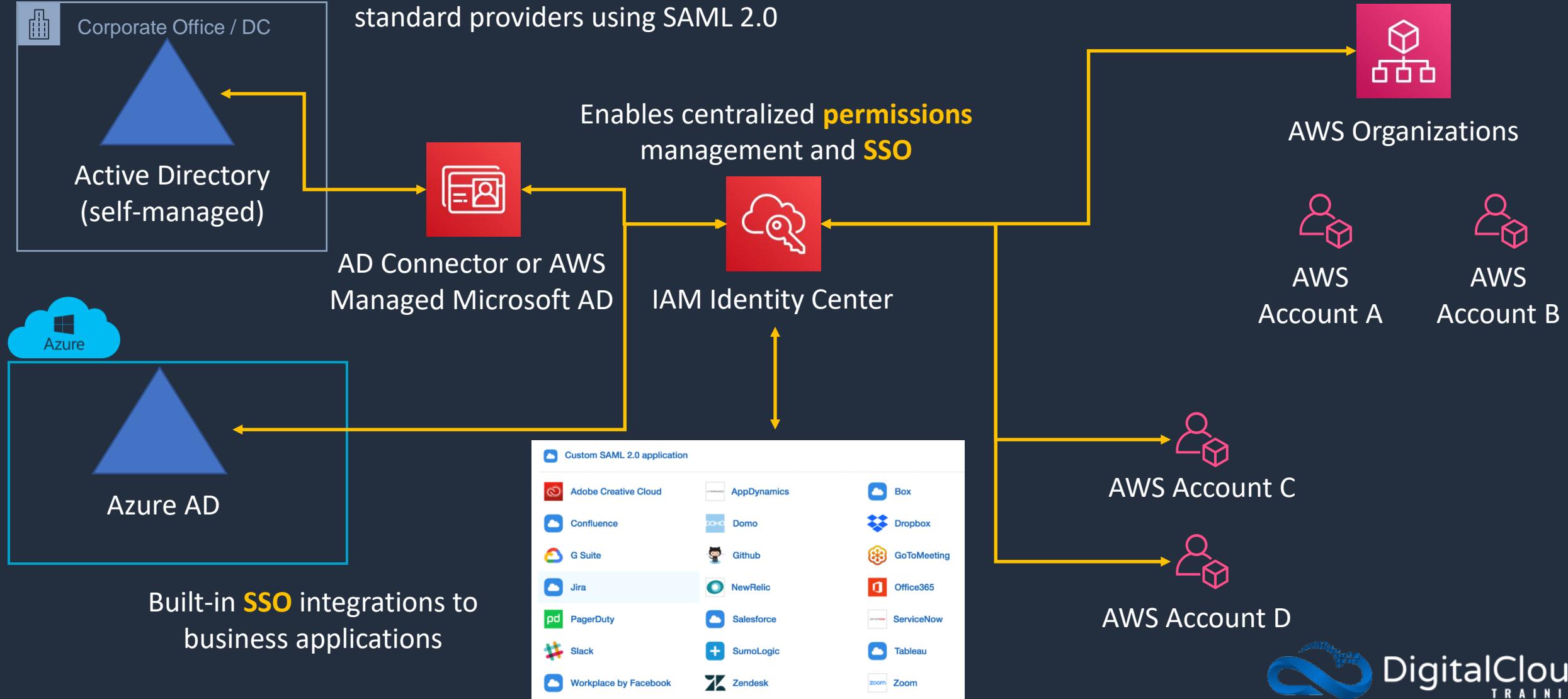
AWS recommend to use **Cognito** for **web identity federation** in most cases



IAM Identity Center

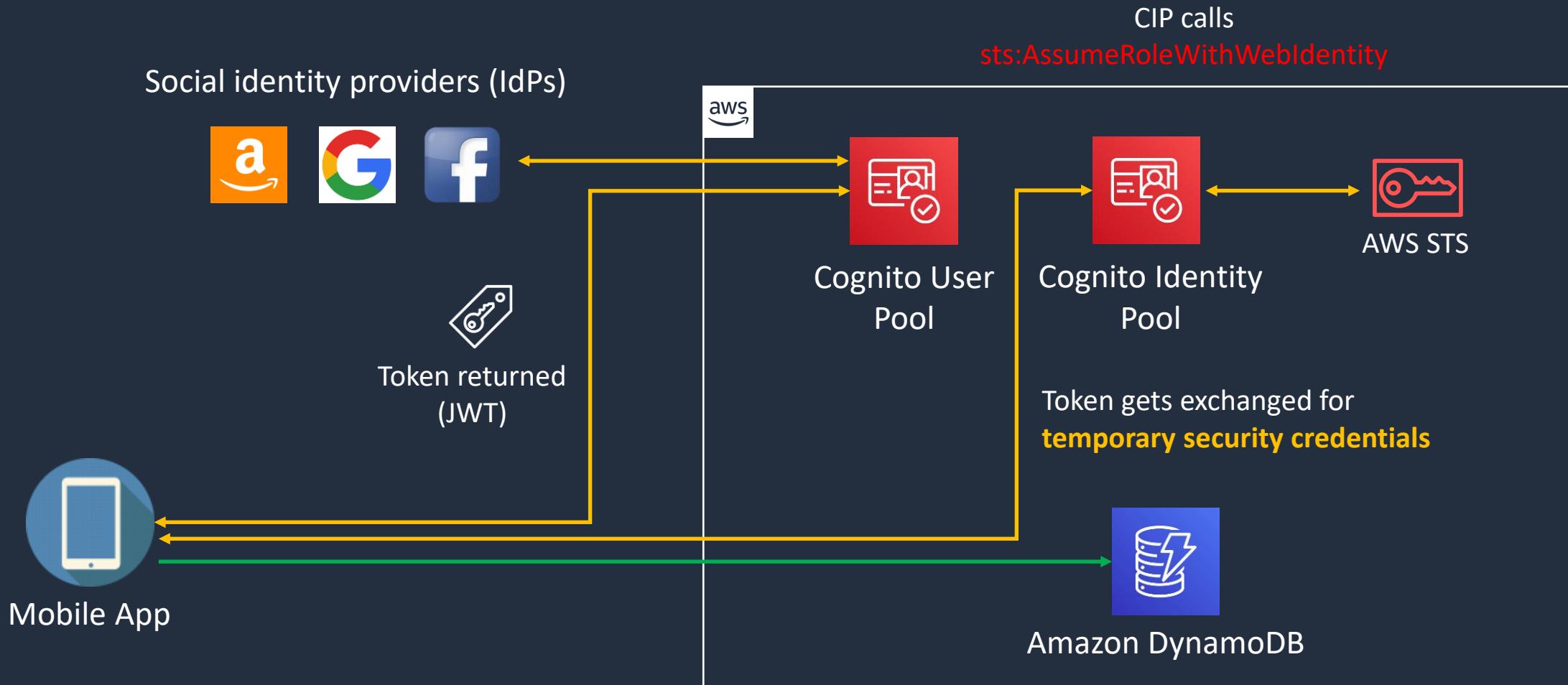
Identity sources can be Identity Center directory, Active Directory and standard providers using SAML 2.0

IAM Identity Center is the successor to **AWS Single Sign-On (SSO)**

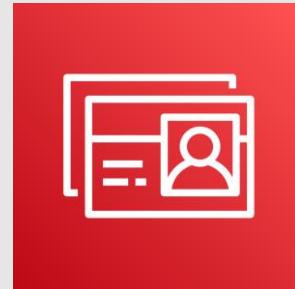




Amazon Cognito



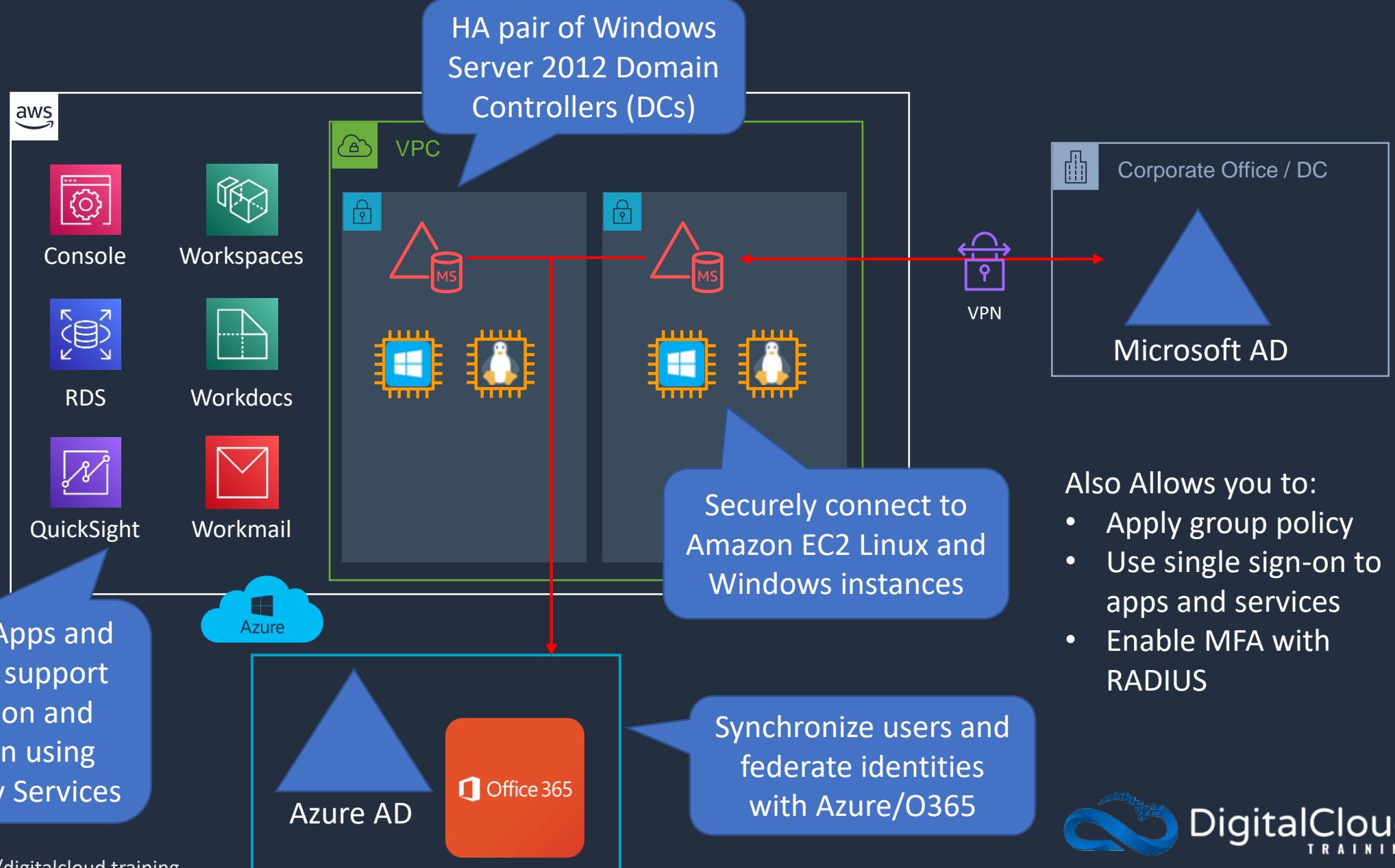
AWS Directory Service





AWS Managed Microsoft Active Directory

Managed implementation of Microsoft Active Directory running on Windows Server 2012 R2



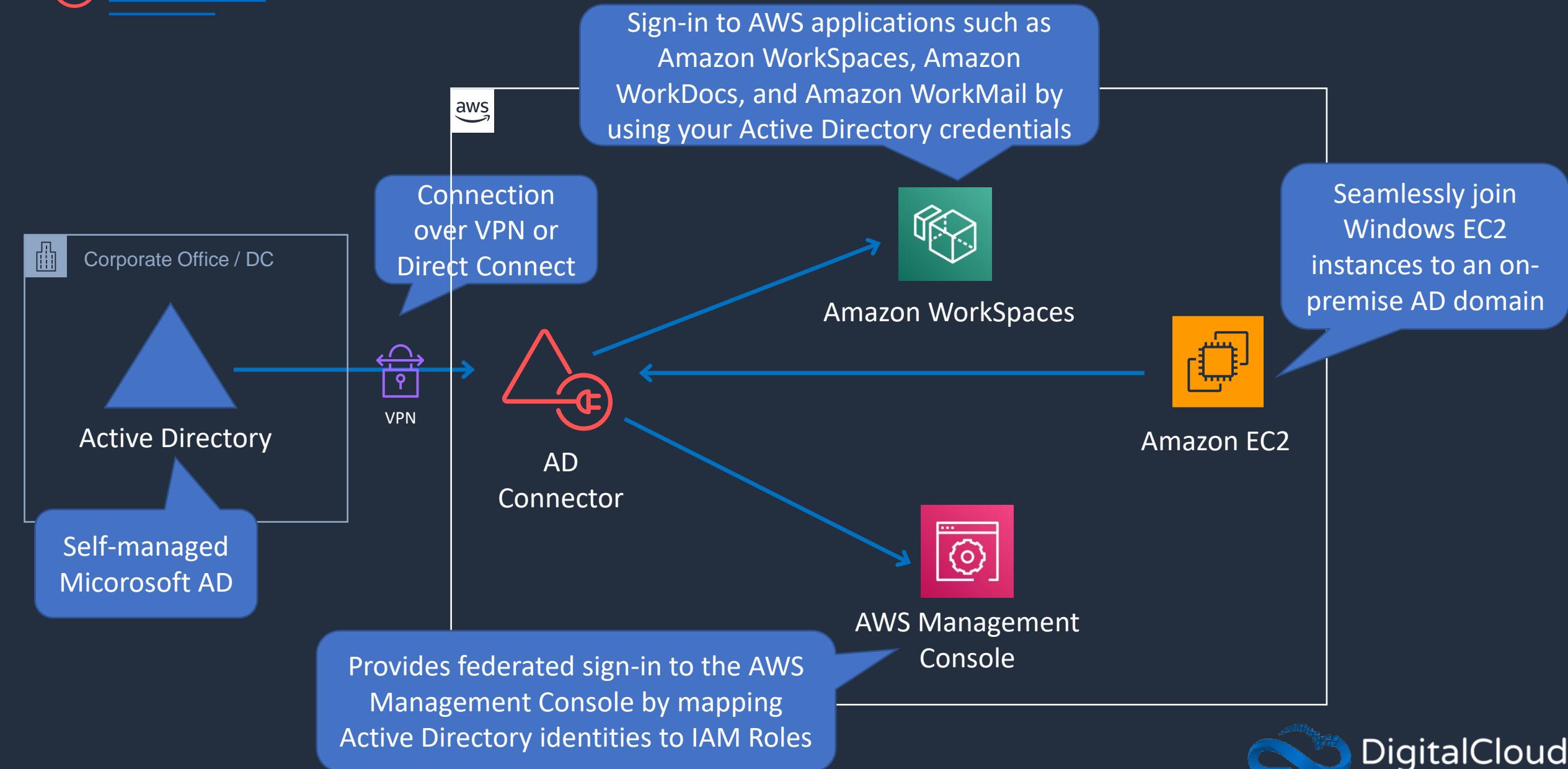


AWS Managed Microsoft Active Directory

- Fully managed AWS services on AWS infrastructure
- Best choice if you have more than 5000 users and/or need a trust relationship set up
- You can setup trust relationships to extend authentication from on-premises Active Directories into the AWS cloud
- On-premise users and groups can access resources in either domain using SSO
- Can be used as a standalone AD in the AWS cloud



AD Connector





AD Connector

- AD Connector is a directory gateway for redirecting directory requests to your on-premise Active Directory.
- AD Connector eliminates the need for directory synchronization and the cost and complexity of hosting a federation infrastructure
- Connects your existing on-premise AD to AWS
- Best choice when you want to use an existing Active Directory with AWS services.



AWS Directory Services Options

Directory Service	Service Description	Use Case
AWS Directory Service for Microsoft Active Directory	AWS-managed full Microsoft AD running on Windows Server 2012 R2	Enterprises that want hosted Microsoft Active Directory
AD Connector	Allows on-premises users to log into AWS services with their existing AD credentials	Single sign-on for on-premises employees
Simple AD	Low scale, low cost, AD implementation based on Samba	Simple user directory, or you need LDAP compatibility

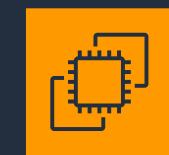
Protecting Secrets





Systems Manager Parameter Store

- Provides secure, hierarchical storage for configuration data management and secrets management
- It is highly scalable, available, and durable
- You can store data such as passwords, database strings, and license codes as parameter values
- You can store values as plaintext (unencrypted data) or ciphertext (encrypted data)
- You can then reference values by using the unique name that you specified when you created the parameter



Amazon EC2



Parameter
Store



Amazon RDS

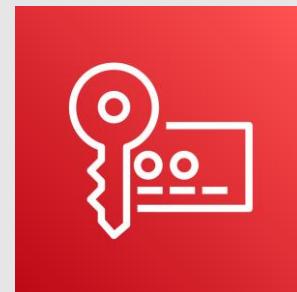
Retrieve database
connection string



AWS Secrets Manager

- Similar to Parameter Store
- Allows native and automatic rotation of keys
- Fine-grained permissions
- Central auditing for secret rotation

Encryption





Encryption In Transit vs At Rest



User

Encryption In Transit

HTTPS Connection

Data is protected by
SSL/TLS in transit



ALB

Encryption At Rest

Amazon S3 **encrypts** the object as it is **written** to the bucket it



Unencrypted
Object



Data encryption key



Encryption process

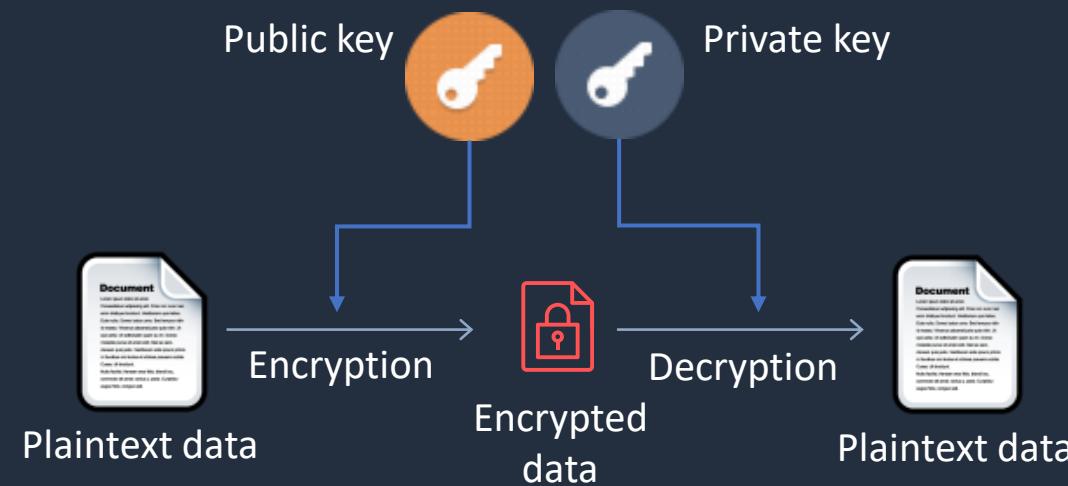


Encrypted
bucket



Asymmetric Encryption

- Asymmetric encryption is also known as public key cryptography
- Messages encrypted with the public key can only be decrypted with the private key
- Messages encrypted with the private key can be decrypted with the public key
- Examples include SSL/TLS and SSH





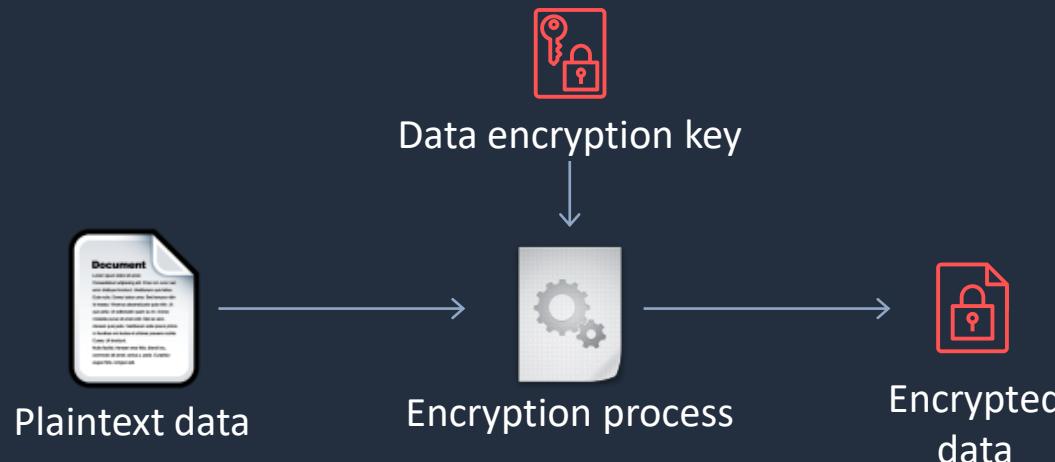
AWS Certificate Manager (ACM)

- Create, store and renew SSL/TLS X.509 certificates
- Single domains, multiple domain names and wildcards
- Integrates with several AWS services including:
 - **Elastic Load Balancing**
 - **Amazon CloudFront**
 - **AWS Elastic Beanstalk**
 - **AWS Nitro Enclaves**
 - **AWS CloudFormation**

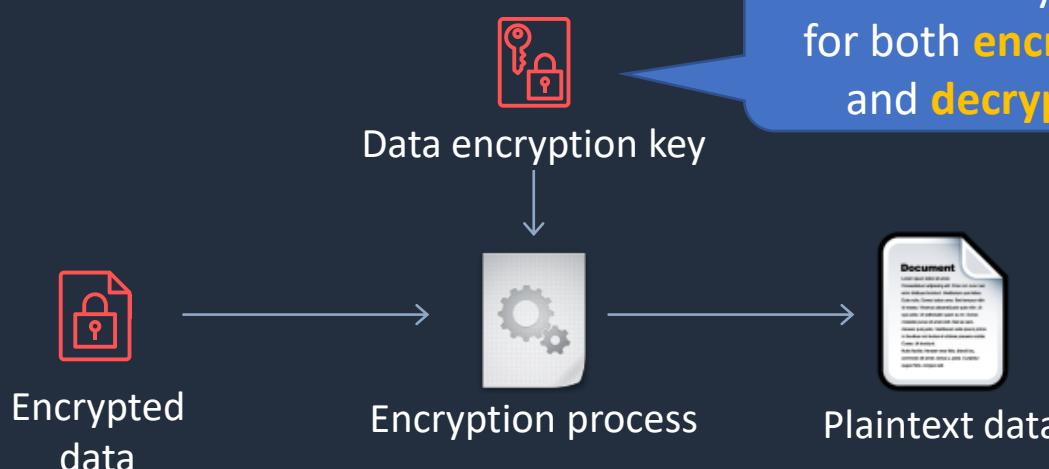


Symmetric Encryption

Encryption



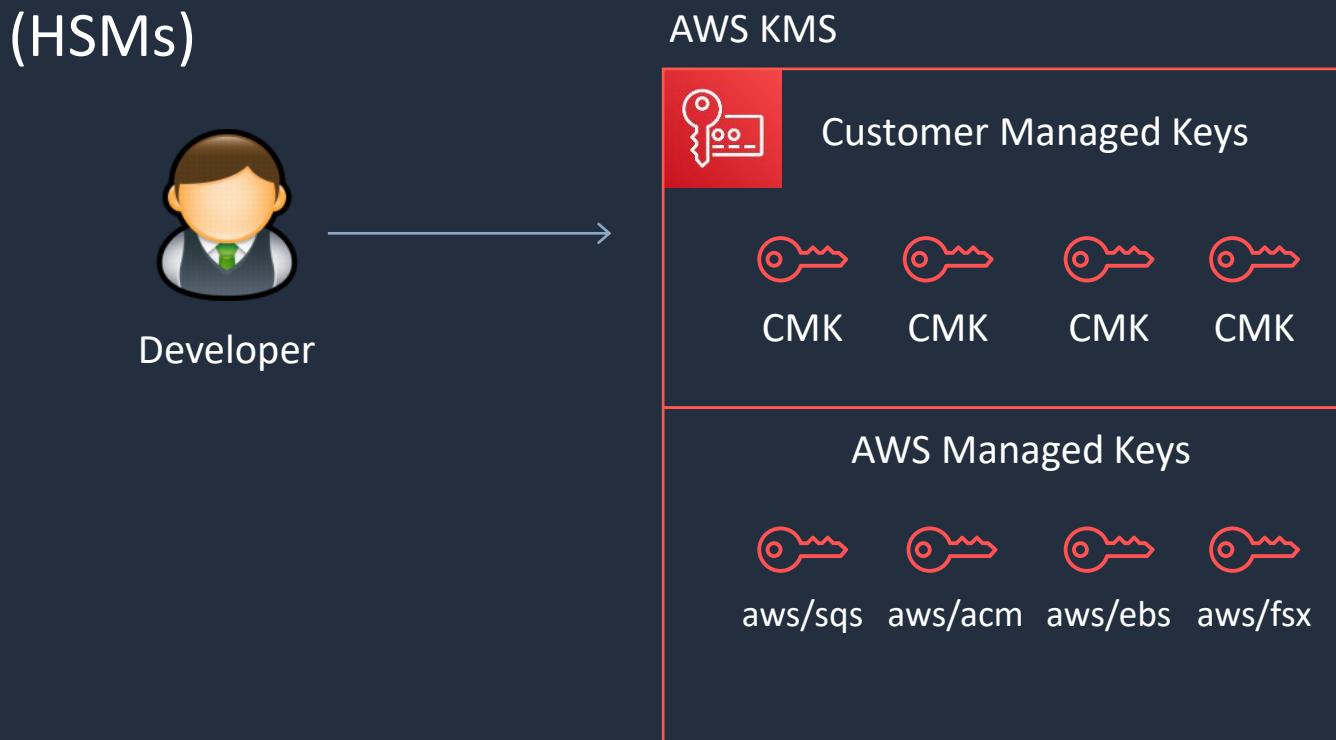
Decryption





AWS Key Management Service (KMS)

- Create and managed **symmetric** and **asymmetric** encryption keys
- The **customer master keys** (CMKs) are protected by hardware security modules (HSMs)





AWS CloudHSM

- AWS CloudHSM is a cloud-based hardware security module (HSM)
- Generate and use your own encryption keys on the AWS Cloud
- Manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs
- CloudHSM runs in your VPC

	CloudHSM	AWS KMS
Tenancy	Single-tenant HSM	Multi-tenant AWS service
Availability	Customer-managed durability and available	Highly available and durable key storage and management
Root of Trust	Customer managed root of trust	AWS managed root of trust
FIPS 140-2	Level 3	Level 2 / Level 3 in some areas
3 rd Party Support	Broad 3 rd Party Support	Broad AWS service support

Encryption on AWS



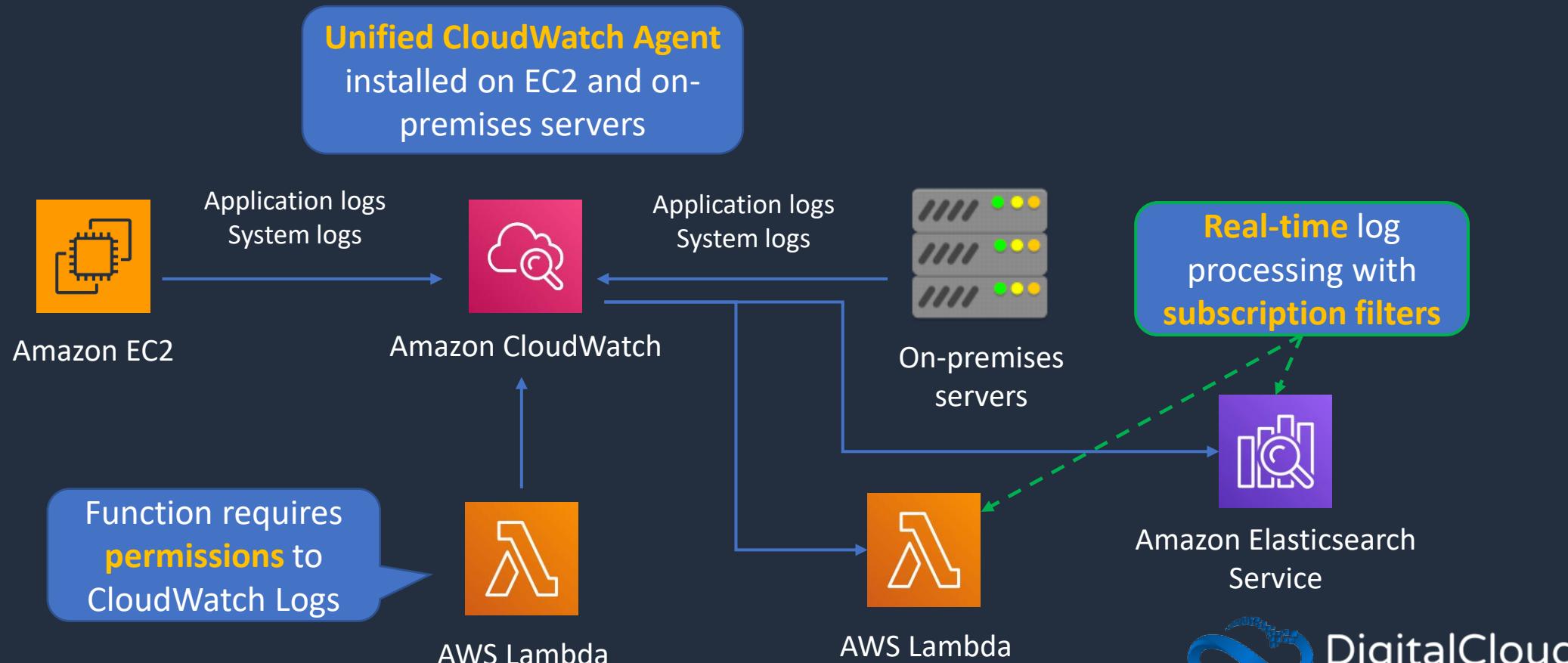
Logging and Auditing





Amazon CloudWatch Logs

- Gather application and system logs in CloudWatch
- Defined expiration policies and KMS encryption





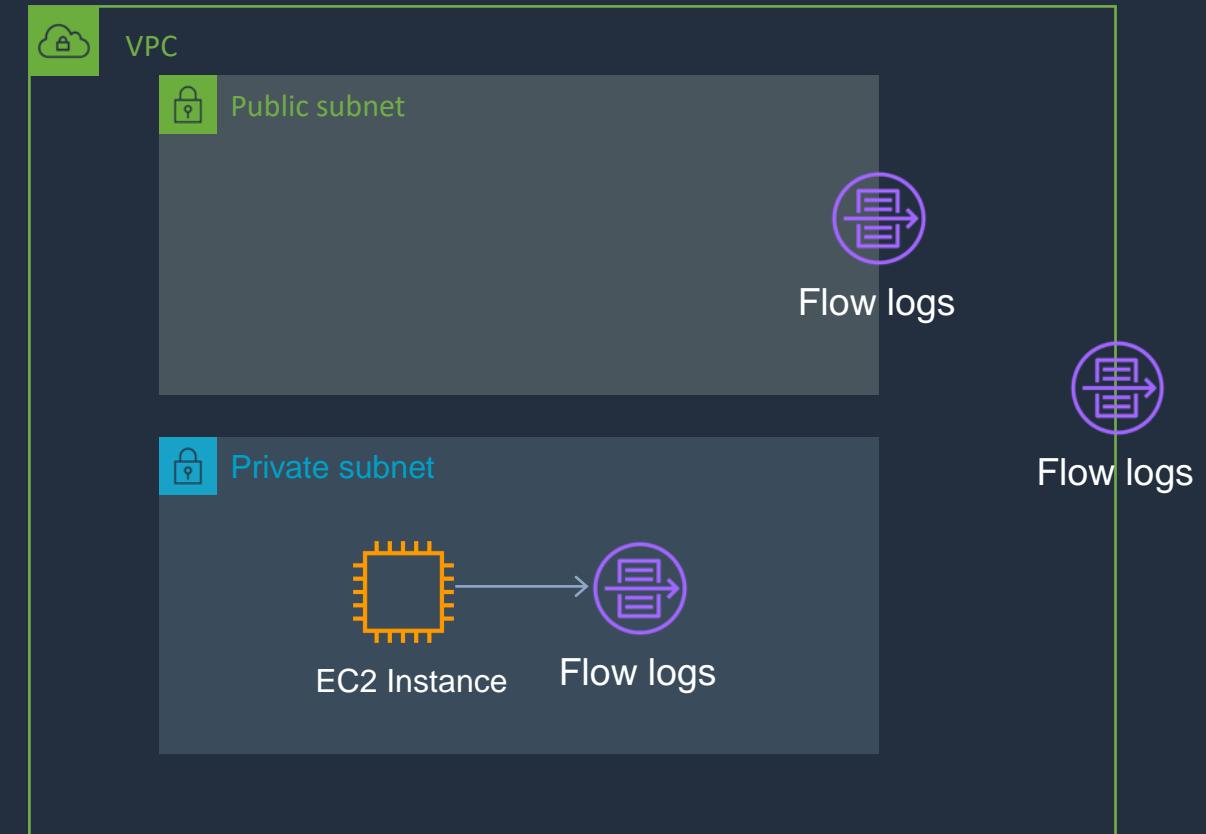
AWS CloudTrail

- CloudTrail logs **API activity** for auditing
- By default, management events are logged and retained for 90 days
- A **CloudTrail Trail** logs any events to S3 for indefinite retention
- Trail can be within Region or all Regions
- CloudWatch Events can be triggered based on API calls in CloudTrail
- Events can be streamed to CloudWatch Logs



VPC Flow Logs

- Flow Logs capture information about the IP traffic going to and from network interfaces in a VPC
- Flow log data is stored using Amazon CloudWatch Logs
- Flow logs can be created at the following levels:
 - VPC
 - Subnet
 - Network interface





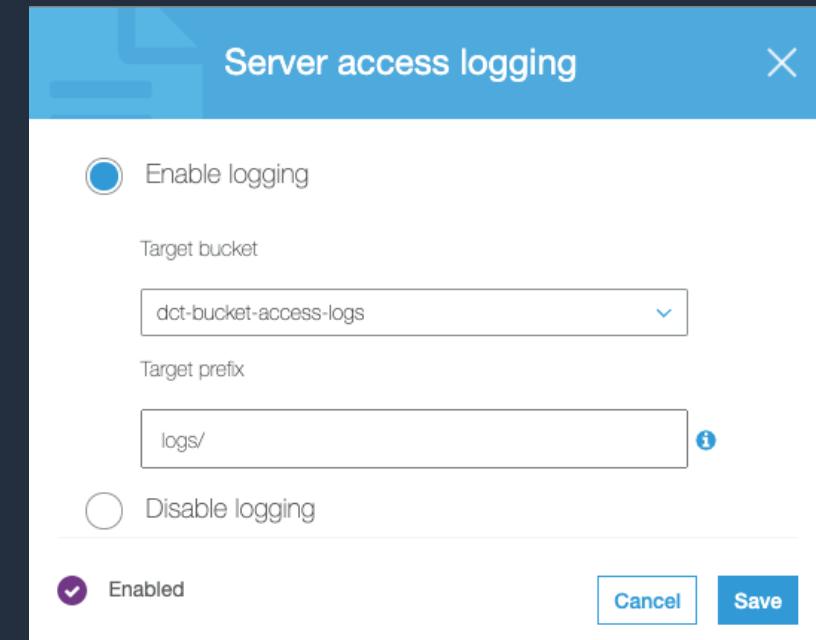
Access Logs

Elastic Load Balancing Access Logs

- capture detailed information about requests sent to the load balancer
- Use to analyze traffic patterns and troubleshoot issues
- Can identify requester, IP, request type etc.
- Can be optionally stored and retained in S3.

S3 Access Logs

- Provides detailed records for the requests that are made to a bucket
- Details include the requester, bucket name, request time, request action, response status, and error code (if applicable)
- Disabled by default



AWS CloudTrail



Detect and Respond





Amazon Detective

- Analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities
- Automatically collects data from AWS resources
- Uses machine learning, statistical analysis, and graph theory
- Creates a unified, interactive view of resources, users and interactions between them
- Data sources include VPC Flow Logs, CloudTrail, and GuardDuty



AWS GuardDuty

- Intelligent threat detection service
- Detects account compromise, instance compromise, malicious reconnaissance, and bucket compromise
- Continuous monitoring for events across:
 - **AWS CloudTrail Management Events**
 - **AWS CloudTrail S3 Data Events**
 - **Amazon VPC Flow Logs**
 - **DNS Logs**

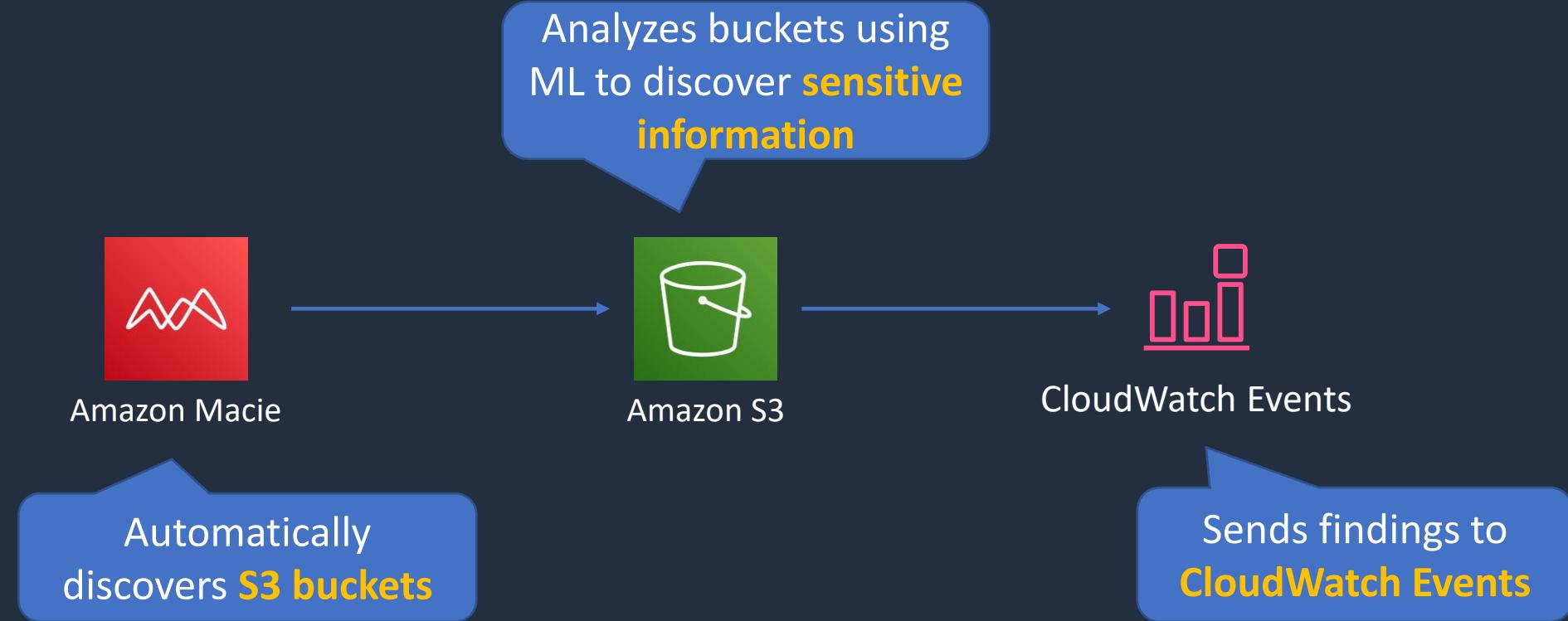


Amazon Macie

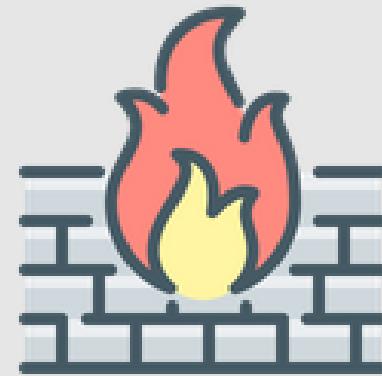
- Macie is a fully managed data security and data privacy service
- Uses machine learning and pattern matching to discover, monitor, and help you protect your sensitive data on Amazon S3
- Macie enables security compliance and preventive security
- Can Identify a variety of data types, including PII, Protected Health Information (PHI), regulatory documents, API keys, and secret keys



Amazon Macie



Firewalls and DDoS Protection



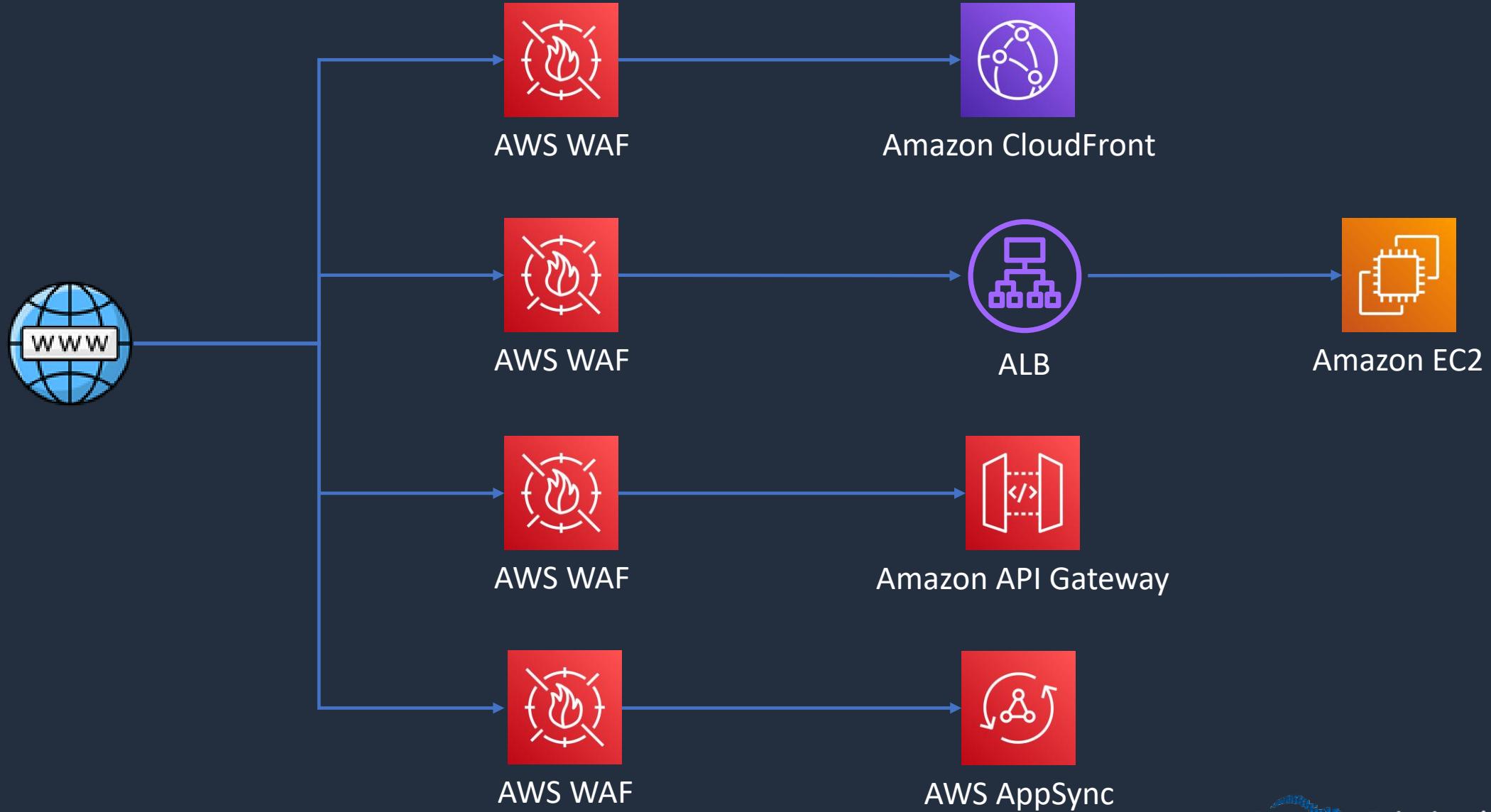


AWS Web Application Firewall (WAF)

- AWS WAF is a **web application firewall**
- WAF lets you create rules to filter web traffic based on conditions that include IP addresses, HTTP headers and body, or custom URIs
- WAF makes it easy to create rules that block common web exploits like **SQL injection** and **cross site scripting**
- The rules are known as Web ACLs



AWS Web Application Firewall (WAF)

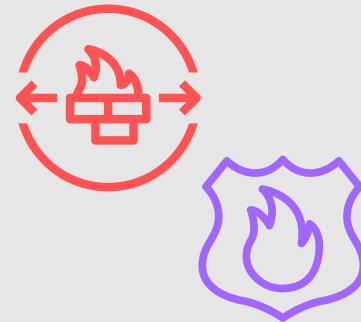




AWS Shield

- AWS Shield is a managed **Distributed Denial of Service** (DDoS) protection service
- Safeguards web application running on AWS with always-on detection and automatic inline mitigations
- Helps to minimize application downtime and latency
- Two tiers –
 - **Standard** – no cost
 - **Advanced** - \$3k USD per month and 1 year commitment
- Integrated with Amazon CloudFront (standard included by default)

Network Firewall and DNS Firewall

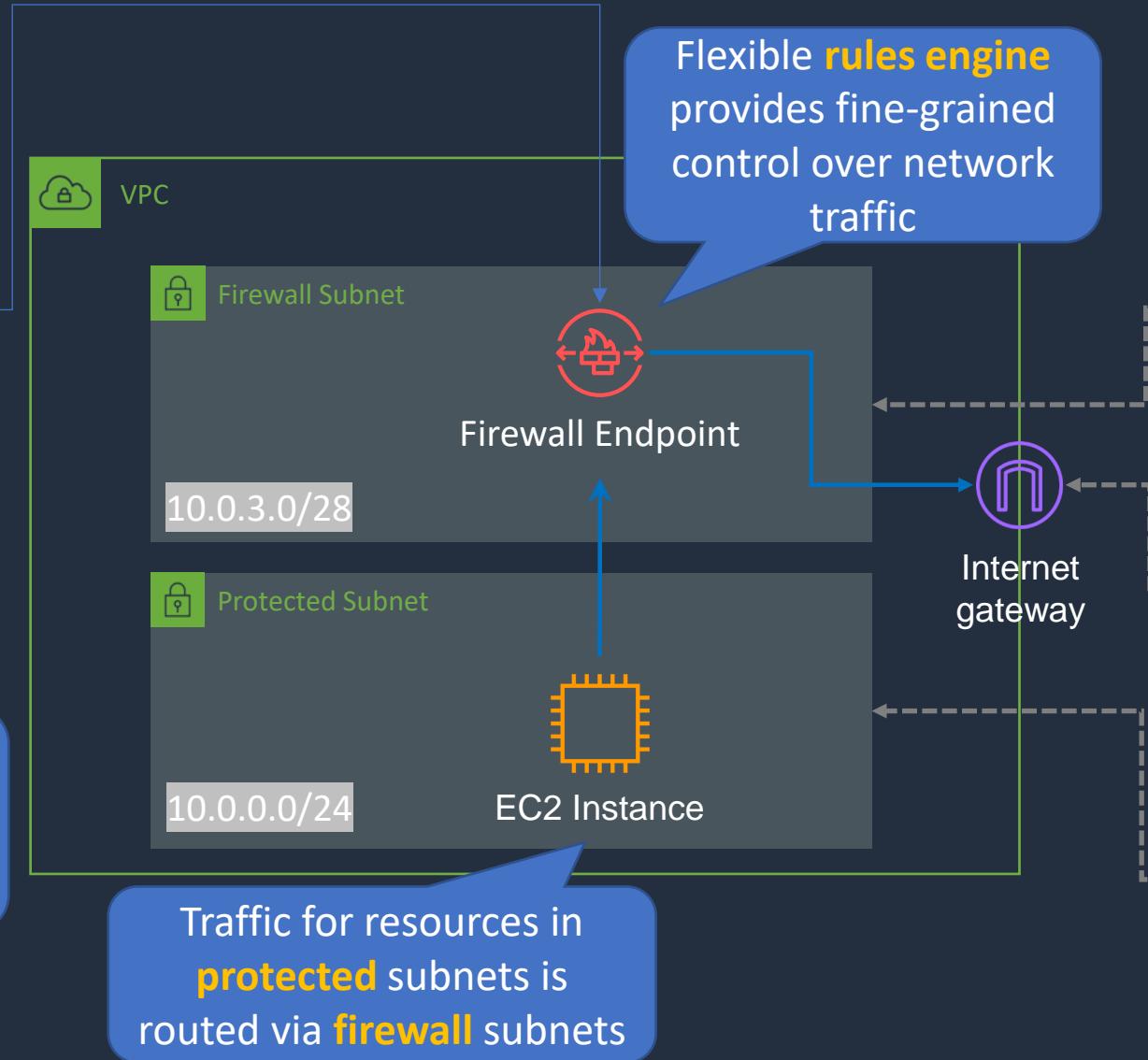




AWS Network Firewall



Manage multiple AWS Network Firewall deployments



Firewall Subnet RT	
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

IGW Ingress RT	
Destination	Target
10.0.0.0/16	Local
10.0.0.0/24	vpce-id-az-a

Protected Subnet RT	
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	vpce-id-az-a



AWS Network Firewall

- Managed service for **VPC network protection**
- **Includes:**
 - Stateful & Stateless firewall
 - Intrusion Prevention System (IPS)
 - Web filtering
- Works with **AWS Network Firewall** manager for centrally applying policies across VPCs / accounts
- Uses a **VPC endpoint** and **Gateway Load Balancer**
- Do not deploy resources in the firewall subnet
- For HA, allocate a subnet per AZ



Route 53 Resolver DNS Firewall

- Filter and regulate outbound **DNS traffic for VPCs**
- Requests route through Route 53 Resolver for DNS
- Helps prevent DNS exfiltration of data
- Monitor and control the domains applications can query
- Can use AWS Firewall Manager to centrally configure and manage DNS Firewall
- Central management can span VPCs and accounts in AWS Organizations

AWS Resource Access Manager (RAM)





AWS RAM

- Shares resources:
 - Across AWS accounts
 - Within AWS Organizations or OUs
 - IAM roles and IAM users
- Resource shares are created with:
 - The AWS RAM Console
 - AWS RAM APIs
 - AWS CLI
 - AWS SDKs



AWS RAM

RAM can be used to share:

- 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
- Amazon S3 on Outposts
- AWS Resource Groups
- Amazon Route 53
- AWS Systems Manager Incident Manager
- Amazon VPC

Compliance Services





AWS Artifact

- AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements
- Reports available in AWS Artifact include:
 - Service Organization Control (SOC) reports
 - Payment Card Industry (PCI) reports
- Provides certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of **AWS security controls**
- Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA)

Security Management and Support





AWS Security Hub

- Provides a comprehensive view of security alerts and security posture **across AWS accounts**
- Aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services
- Continuously monitors your environment using automated security checks
- Configure security standards to validate against
 - AWS Foundational Security Best Practices v1.0.0
 - CIS AWS Foundations Benchmark v1.2.0
 - PCI DSS v3.2.1



AWS Security Bulletins

- Security and privacy events affecting AWS services are published (also has an RSS feed)

▼ Content Type

Important
 Informational

▼ Year

2021
 2020
 2019
 2018
 2017
 2016
 2015
 2014

Sudo Security Issue (CVE-2021-3156) AWS-2021-001, 01/27/2021
Xen Security Advisory (XSA-286) AWS-2020-005, 10/23/2020
Container Networking Security Issue (CVE-2020-8558) AWS-2020-002v2, 07/09/2020
Minimum Version of TLS 1.2 Required for FIPS Endpoints by March 31, 2021 AWS-2020-001, 03/31/2020
Kubernetes Security Issue (CVE-2019-11249) AWS-2019-007, 08/15/2019
Kubernetes Security Issue (CVE-2019-11246) AWS-2019-006, 07/02/2019
Linux Kernel TCP SACK Denial of Service Issues AWS-2019-005, 06/17/2019



AWS Trust & Safety Team

- Contact the **AWS Trust & Safety** team if AWS resources are being used for:
 - Spam
 - Port scanning
 - Denial-of-service attacks
 - Intrusion attempts
 - Hosting of objectionable or copyrighted content
 - Distributing malware
- Email address is: abuse@amazonaws.com

Penetration testing





Penetration Testing

- Penetration testing is the practice of testing one's own application's security for vulnerabilities by simulating an attack

AWS Customer Support Policy for Penetration Testing

AWS customers are welcome to carry out security assessments or penetration tests of their AWS infrastructure without prior approval for the services listed in the next section under "Permitted Services." Additionally, AWS permits customers to host their security assessment tooling within the AWS IP space or other cloud provider for on-prem, in AWS, or third party contracted testing. All security testing that includes Command and Control (C2) requires prior approval.

Please ensure that these activities are aligned with the policy set out below. Note: Customers are not permitted to conduct any security assessments of AWS infrastructure or the AWS services themselves. If you discover a security issue within any of the AWS services observed in your security assessment, please [contact AWS Security](#) immediately.

If AWS receives an abuse report for activities related to your security testing, we will forward it to you. When responding, please provide us with approved language detailing your use case, including a point of contact that we can share with any third party reporters. Learn more [here](#).

Resellers of AWS services are responsible for their customers' security testing activity.



Penetration Testing

Permitted services

- Amazon EC2 instances, WAF, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS AppSync
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments
- Amazon Elastic Container Service
- AWS Fargate
- Amazon Elasticsearch
- Amazon FSx
- Amazon Transit Gateway
- S3 hosted applications (targeting S3 buckets is strictly prohibited)

Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- DNS hijacking via Route 53
- DNS Pharming via Route 53
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS (These are subject to the DDoS Simulation Testing policy)
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

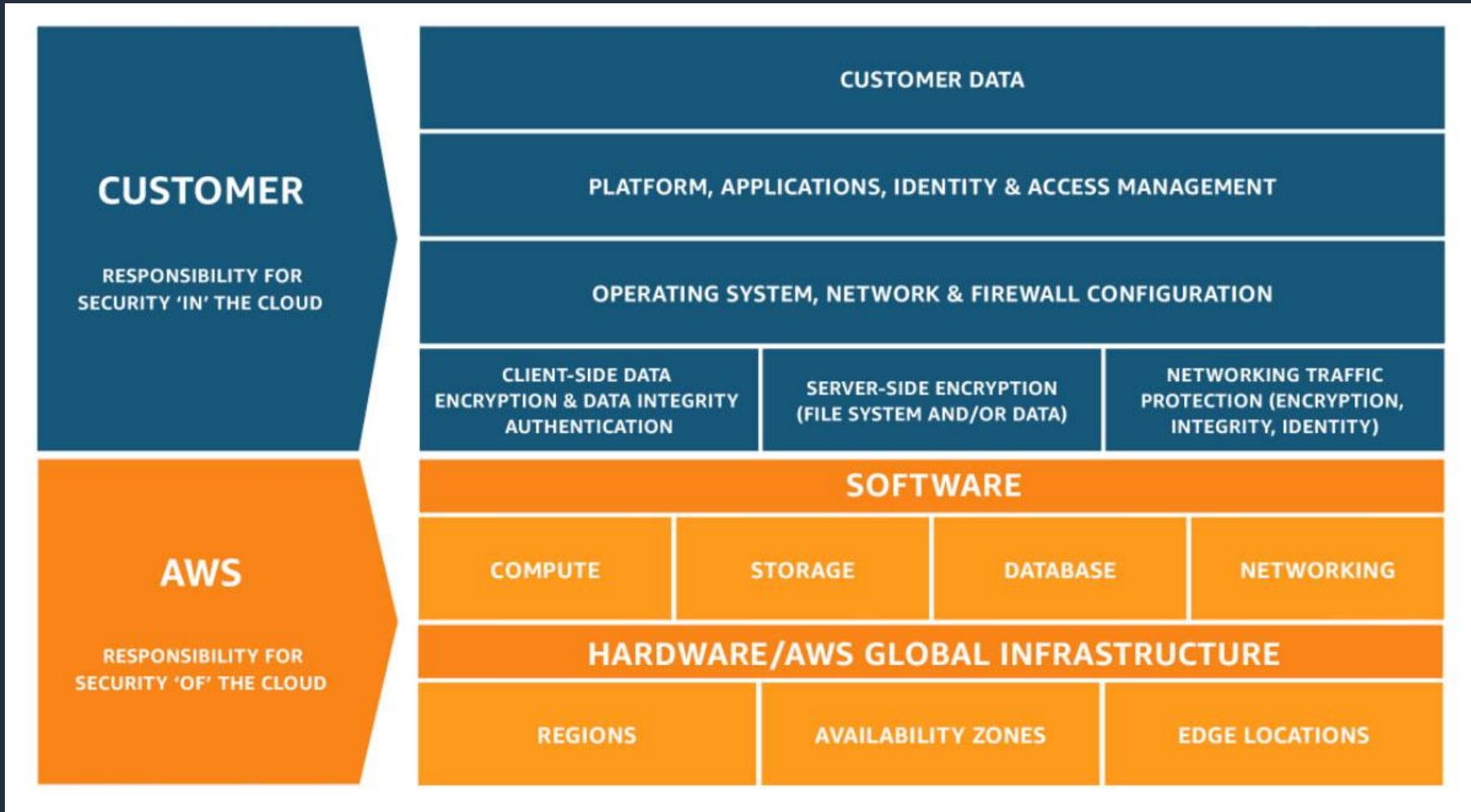
<https://aws.amazon.com/security/penetration-testing/>

Shared Responsibility Model Review





The AWS Shared Responsibility Model





The AWS Shared Responsibility Model

CUSTOMER RESPONSIBILITY



Bucket with objects



Role



Multi-Factor Authentication



Security Group



Patch management



Staff training



Data encryption



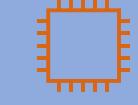
IAM User



Network ACL



SSL encryption



EC2 Instance



Auto Scaling



Elastic load balancer

AWS RESPONSIBILITY



Data center



Data center security



Network router



Network switch



Server



Storage



Database Server



Disk drive

SECTION 14

Architecting for the Cloud

AWS Well-Architected





AWS Well-Architected

- AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads
- Based on 6 pillars:
 - **Operational Excellence**
 - **Security**
 - **Reliability**
 - **Performance Efficiency**
 - **Cost Optimization**
 - **Sustainability**



AWS Well-Architected

Consists of:

- AWS Well-Architected Pillars
- AWS Well-Architected Guidance
- AWS Well-Architected Tool
- AWS Well-Architected Lenses
- AWS Architecture Center
- Partners

<https://aws.amazon.com/architecture/well-architected/>

AWS Well-Architected Framework





AWS Well-Architected Framework

- Helps you understand the pros and cons of decisions you make while building systems on AWS
- Based on 6 pillars:

Operational Excellence Pillar

- Support development and run workloads effectively
- Gain insight into workload operations
- Continuously improve processes and procedures to deliver business value



AWS Well-Architected

- Best practices for operational excellence:
 - Perform operations as code
 - Make frequent, small, reversible changes
 - Refine operations procedures frequently
 - Anticipate failure
 - Learn from all operational failures



Security Pillar

- Protect data, systems, and assets to take advantage of cloud technologies to improve your security
- Best practices for security:
 - Implement a strong identity foundation
 - Enable traceability
 - Apply security at all layers
 - Automate security best practices
 - Protect data in transit and at rest
 - Keep people away from data
 - Prepare for security events



Reliability Pillar

- Ensuring a workload can perform its intended function correctly and consistently when it's expected to
- This includes the ability to operate and test the workload through its total lifecycle
- Best practices for reliability:
 - Automatically recover from failure
 - Test recovery procedures
 - Scale horizontally to increase aggregate workload availability
 - Stop guessing capacity
 - Manage change in automation



Performance Efficiency Pillar

- The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve
- Best practices for performance efficiency:
 - Democratize advanced technologies
 - Go global in minutes
 - Use serverless architectures
 - Experiment more often
 - Consider mechanical sympathy



Cost Optimization Pillar

- The ability to run systems to deliver business value at the lowest price point
- Best practices for cost optimization:
 - Implement Cloud Financial Management
 - Adopt a consumption model
 - Measure overall efficiency
 - Stop spending money on undifferentiated heavy lifting
 - Analyze and attribute expenditure



Sustainability Pillar

- Environmental sustainability is a shared responsibility between customers and AWS
 - AWS is responsible for optimizing the sustainability of the cloud – delivering efficient, shared infrastructure, water stewardship, and sourcing renewable power
 - Customers are responsible for sustainability in the cloud – optimizing workloads and resource utilization, and minimizing the total resources required to be deployed for your workloads

AWS Cloud Adoption Framework





AWS Cloud Adoption Framework

- Helps organizations understand how adopting cloud transforms the way they will function
- Leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS
- AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations



AWS Cloud Adoption Framework

AWS CAF groups its capabilities in six perspectives:

- Business
- People
- Governance
- Platform
- Security
- Operations



AWS Cloud Adoption Framework

AWS CAF groups its capabilities in six perspectives:

- **Business Perspective** – helps ensure that your cloud investments accelerate your digital transformation ambitions and business outcomes
- **People Perspective** – serves as a bridge between technology and business, accelerating the cloud journey to help organizations more rapidly evolve to a culture of continuous growth and learning
- **Governance Perspective** – helps you orchestrate your cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks



AWS Cloud Adoption Framework

AWS CAF groups its capabilities in six perspectives:

- **Platform Perspective** – helps you build an enterprise-grade, scalable, hybrid cloud platform; modernize existing workloads; and implement new cloud native solutions
- **Security Perspective** – helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads
- **Operations Perspective** – helps ensure that your cloud services are delivered at a level that meets the needs of your business



AWS Cloud Adoption Framework



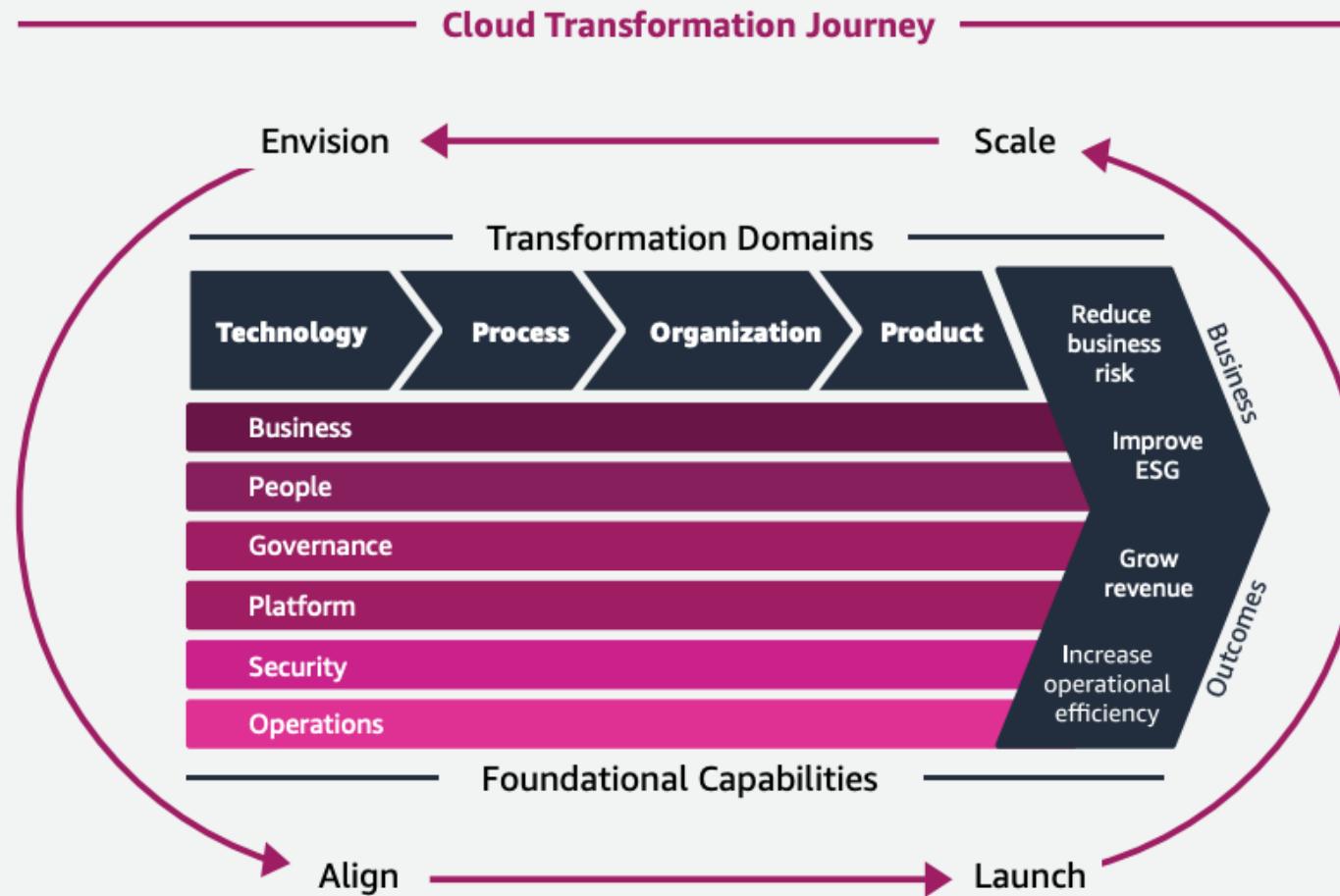


AWS Cloud Adoption Framework





AWS Cloud Adoption Framework



SECTION 15

Accounts, Billing and Support

Amazon EC2 Pricing Options





Amazon EC2 Pricing Options

On-Demand

Standard rate - no discount; no commitments; dev/test, short-term, or unpredictable workloads

Spot Instances

Get discounts of up to 90% for unused capacity. Can be terminated at any time

Dedicated Hosts

Physical server dedicated for your use; Socket/core visibility, host affinity; pay per host; workloads with server-bound software licenses

Reserved

1 or 3-year commitment; up to 75% discount; steady-state, predictable workloads and reserved capacity

Dedicated Instances

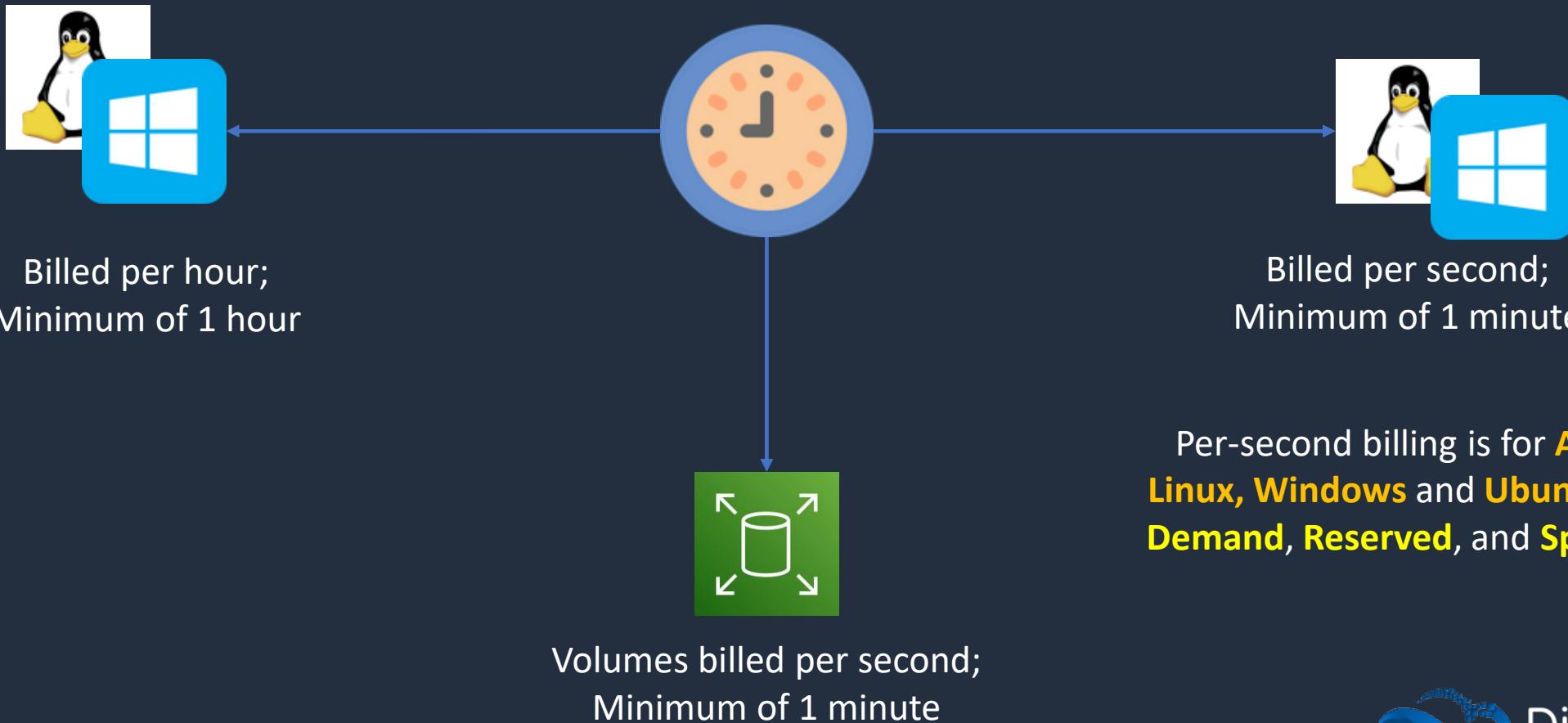
Physical isolation at the host hardware level from instances belonging to other customers; pay per instance

Savings Plans

Commitment to a consistent amount of usage (EC2 + Fargate + Lambda); Pay by \$/hour; 1 or 3-year commitment

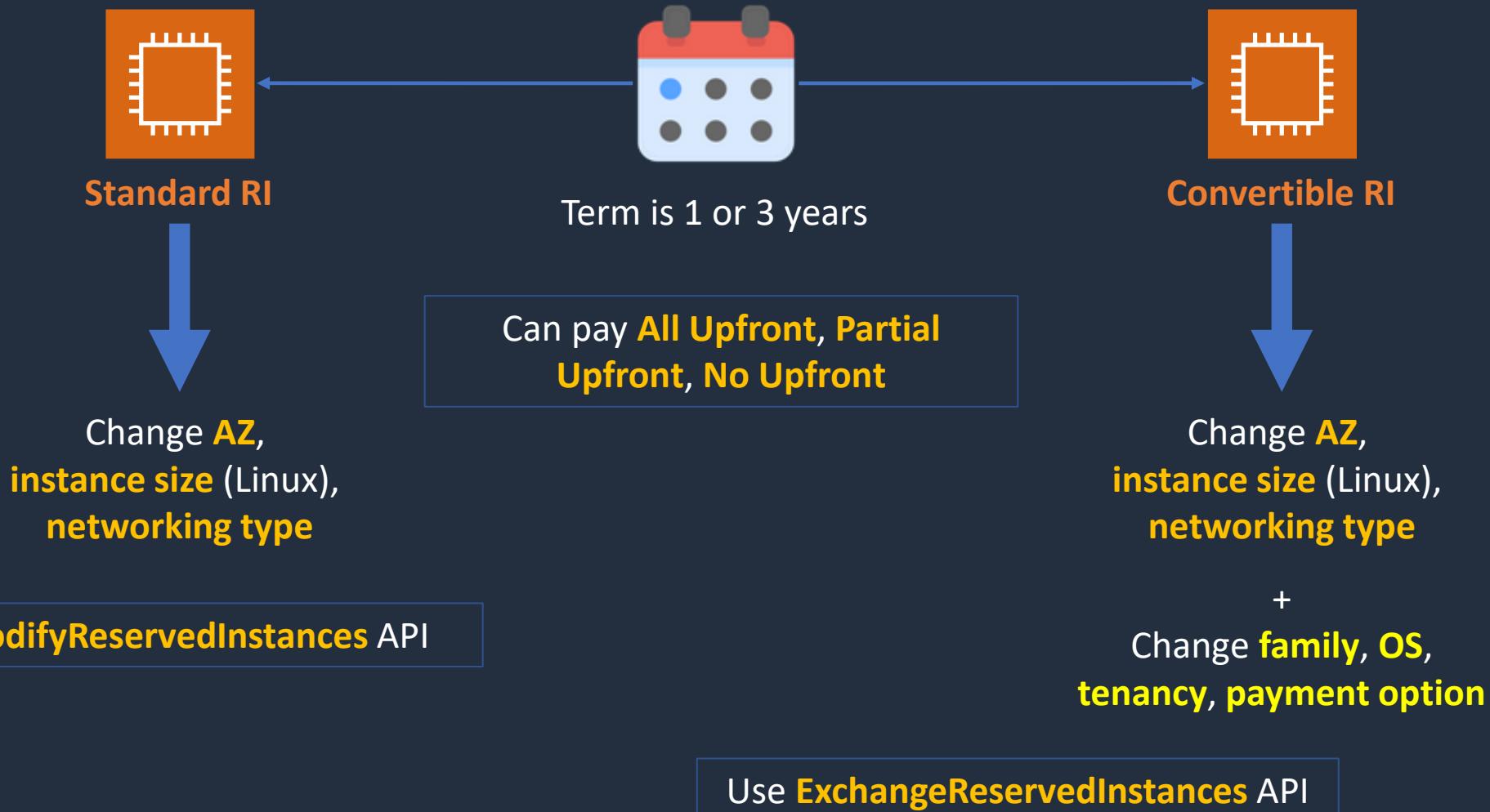
\$ Amazon EC2 Billing

Commercial Linux distros such as **Red Hat EL** and **SUSE ES** use **hourly** pricing



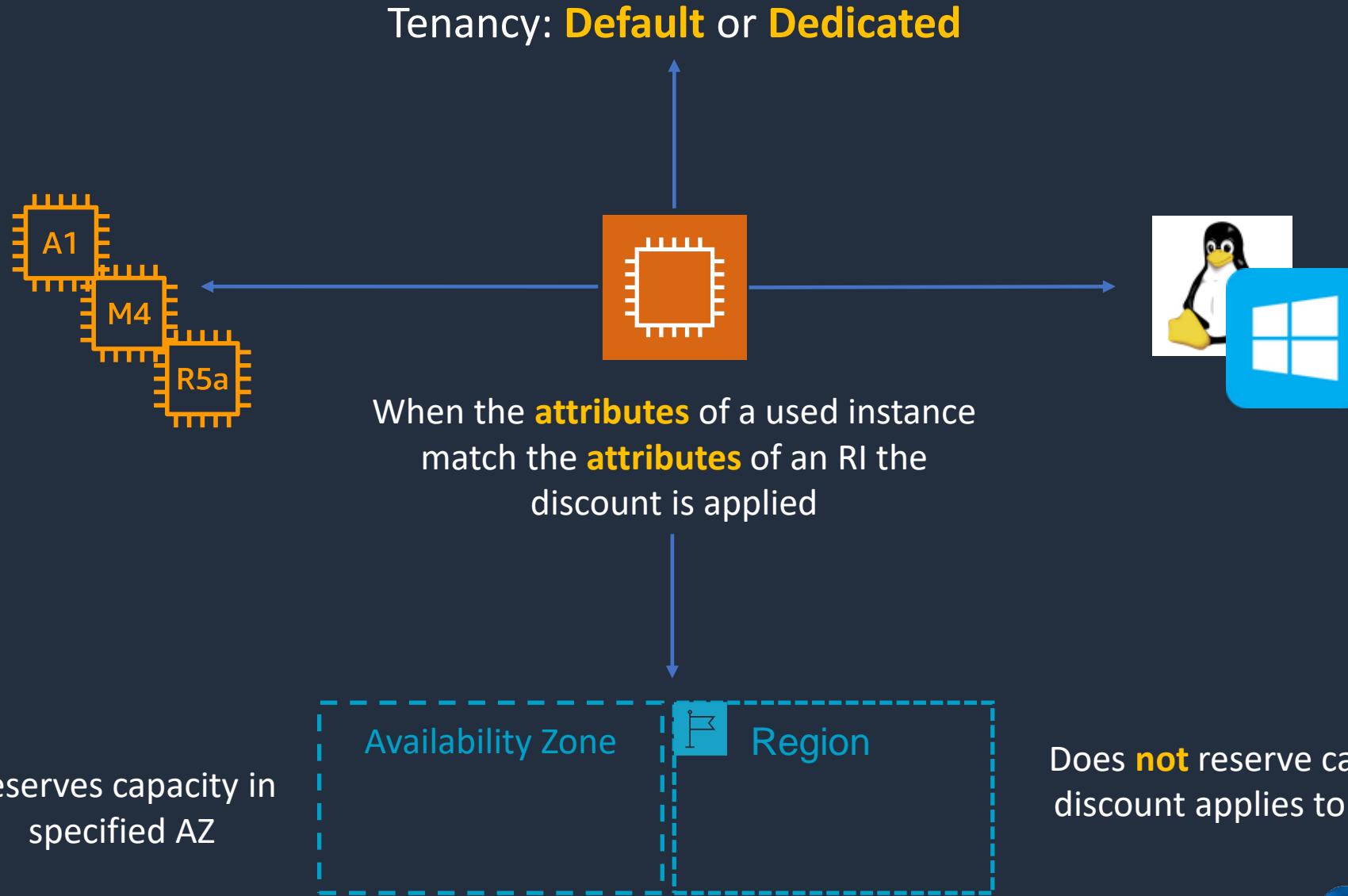


Amazon EC2 Reserved Instances (RIs)





Amazon EC2 Reserved Instances (RIs)





Amazon EC2 On-Demand Capacity Reservations

- Reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone
- Any duration can be specified
- Mitigates against the risk of being unable to get On-Demand capacity
- Does not require any term commitments and can be cancelled at any time
- When you create a Capacity Reservation, you specify:
 - The **Availability Zone** in which to reserve the capacity
 - The **number of instances** for which to reserve capacity
 - The **instance attributes**, including the instance type, tenancy, and platform/OS

\$ AWS Savings Plans



Compute Savings Plan



1 or 3-year; hourly commitment to usage of **Fargate**, **Lambda**, and **EC2**; Any Region, family, size, tenancy, and OS



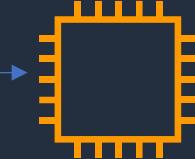
EC2 Savings Plan



1 or 3-year; hourly commitment to usage of **EC2** within a **selected Region** and **Instance Family**; Any size, tenancy and OS



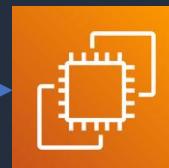
Amazon EC2 Spot Instances



Spot Instance: One or more EC2 instances



Spot Fleet: launches and maintains the number of Spot / On-Demand instances to meet specified target capacity



EC2 Fleet: launches and maintains specified number of Spot / On-Demand / Reserved instances in a **single API call**



2-minute warning if AWS need to reclaim capacity – available via **instance metadata** and **CloudWatch Events**

Can define separate OD/Spot **capacity targets**, **Spot price**, **instance types**, and **AZs**



Spot Block



Requirement:
Uninterrupted for
1-6 hours

Pricing is **30% - 45%** less
than On-Demand

Solution: **Spot Block**

```
$ aws ec2 request-spot-instances \
  --block-duration-minutes 360 \
  --instance-count 5 \
  --spot-price "0.25" ...
```



Dedicated Instances and Dedicated Hosts

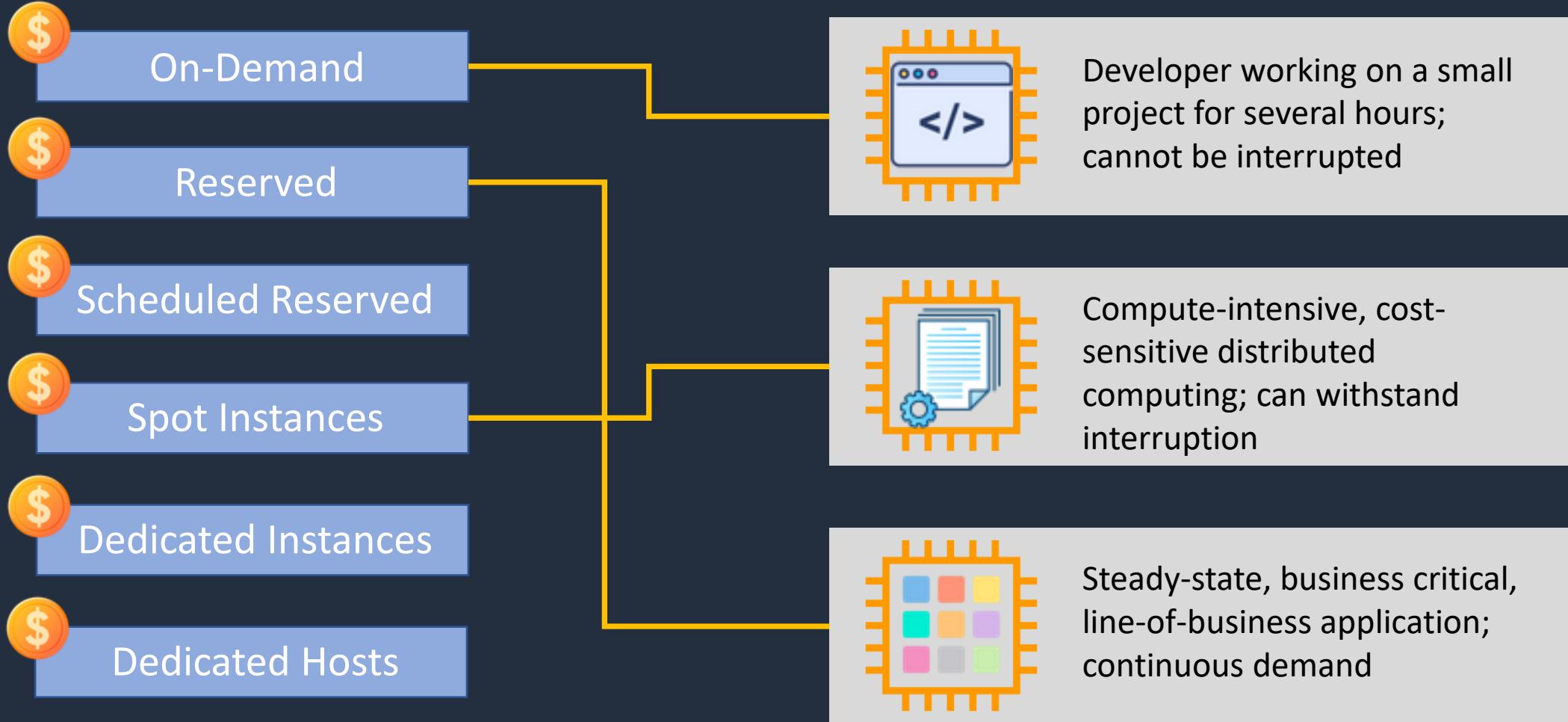
Characteristic	Dedicated Instances	Dedicated Hosts
Enables the use of dedicated physical servers	X	X
Per instance billing (subject to a \$2 per region fee)	X	
Per host billing		X
Visibility of sockets, cores, host ID		X
Affinity between a host and instance		X
Targeted instance placement		X
Automatic instance placement	X	X
Add capacity using an allocation request		X

Amazon EC2 Pricing Use Cases



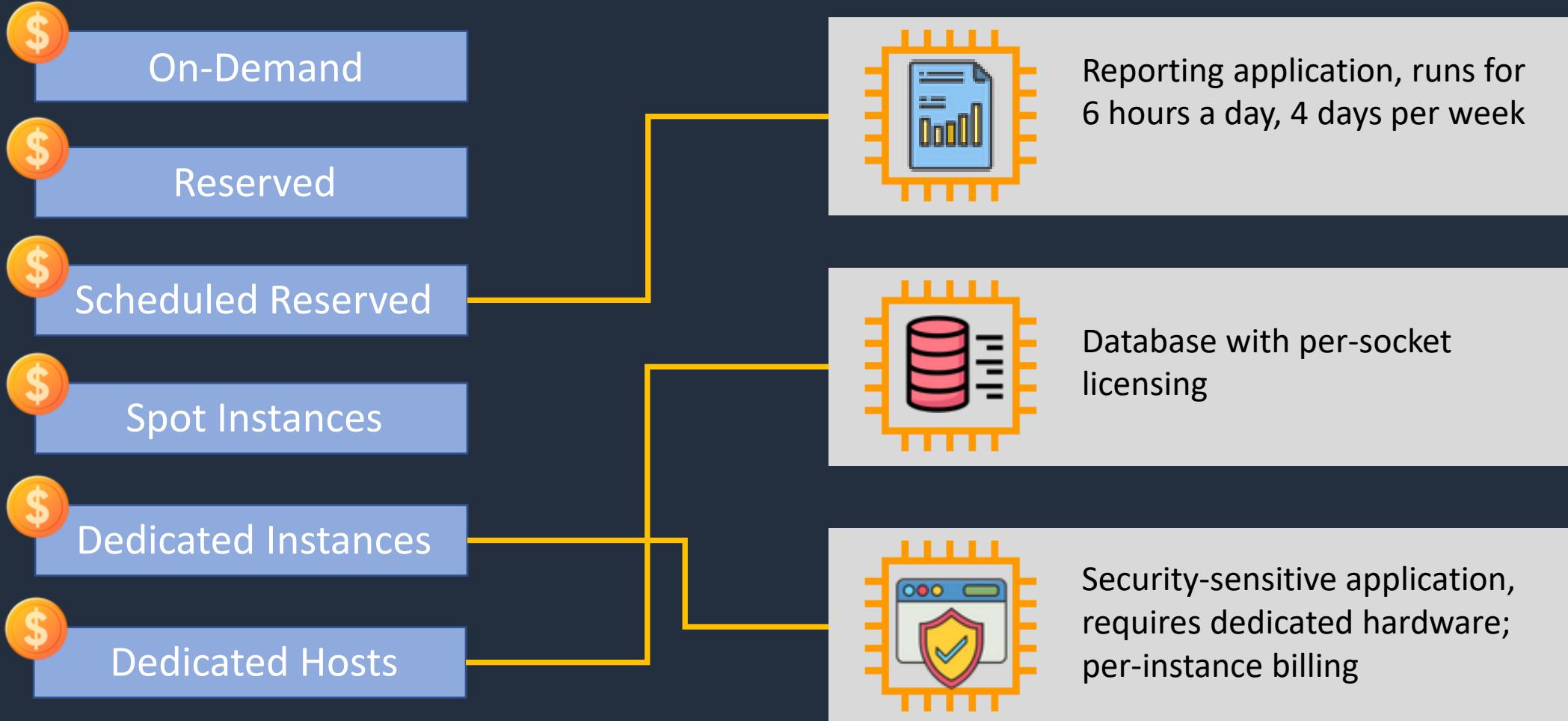


Amazon EC2 Pricing Use Cases

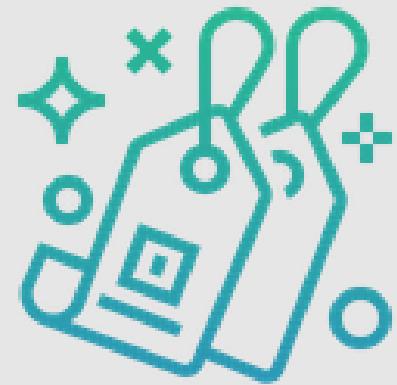




Amazon EC2 Pricing Use Cases



Pricing for other AWS Services





Amazon S3 Pricing

- **Storage class** – e.g. Standard or IA
- **Storage quantity** – data volume stored in your buckets on a per GB basis
- **Number of requests** – the number and type of requests, e.g. GET, PUT, POST, LIST, COPY
- **Lifecycle transitions requests** – moving data between storage classes
- **Data transfer** – data transferred out of an S3 region is charged
- **Retrievals / Requests** – for some storage classes



Amazon EBS Pricing

- **Volumes** – volume storage for all EBS volumes type is charged by the amount of GB provisioned per month
- **Snapshots** – based on the amount of space consumed by snapshots in S3. Copying snapshots is charged on the amount of data copied across regions
- **Data transfer** – inbound data transfer is free, outbound data transfer charges are tiered



Amazon RDS Pricing

- **Clock hours of server uptime** – amount of time the DB instance is running
- **Database characteristics** – e.g. database engine, size and memory class
- **Database purchase type** – e.g. On-Demand, Reserved.
- **Number of database instances**
- **Provisioned storage** – backup is included up to 100% of the size of the DB
- **Additional storage** – the amount of storage in addition to the provisioned storage is charged per GB per month



Amazon RDS Pricing

- **Requests** – the number of input and output requests to the DB
- **Deployment type** – single AZ or multi-AZ
- **Reserved Instances** – RDS RIs can be purchased with No Upfront, Partial Upfront, or All Upfront terms



Amazon DynamoDB Pricing

- Charged for reading, writing, and storing data
- **On-demand capacity mode**
 - Charged for reads and writes
 - No need to specify how much capacity is required
 - Good for unpredictable workloads
- **Provisioned capacity mode**
 - Specify number of reads and writes per second
 - Can use Auto Scaling
 - Good for predictable workloads
 - Consistent traffic or gradual changes



Amazon CloudFront Pricing

- **Traffic distribution** – data transfer and request pricing, varies across regions, and is based on the edge location from which the content is served
- **Requests** – the number and type of requests (HTTP or HTTPS) and the geographic region in which they are made
- **Data transfer out** – quantity of data transferred out of CloudFront edge locations
- There are additional chargeable items such as invalidation requests, field-level encryption requests, and custom SSL certificates



AWS Lambda Pricing

- **Number of requests**
- **Duration of request** – rounded up to the nearest millisecond
- Price is dependent on the amount of memory allocated to the function

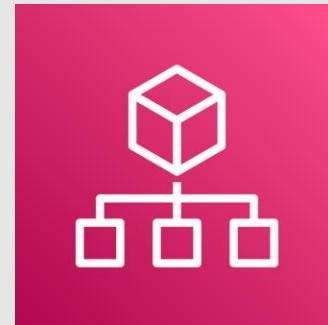
AWS Pricing Calculator



AWS Support Plans



Consolidated Billing





AWS Organizations

- Consolidated billing has the following benefits:
- One bill – You get one bill for multiple accounts
 - **Easy tracking** – You can track the charges across multiple accounts and download the combined cost and usage data
 - **Combined usage** – You can combine the usage across all accounts in the organization to share the volume pricing discounts and Reserved Instance discounts
 - **No extra fee** – Consolidated billing is offered at no additional cost



AWS Organizations

Tier Description	Price Per GB	Price Per TB
First 1 TB/month	\$0.10	\$100.00
Next 49 TB/month	\$0.08	\$80.00
Next 450 TB/month	\$0.06	\$60.00

Usage within Organization:

Account A (master) usage: 2 TB

Account B usage: 80 TB

Account C usage: 120 TB

Total: 202 TB

Calculation:

First 1 TB = \$100.00

Next 49 TB = \$3,920.00

Next 157 TB = \$9,120.00

Total cost = \$13,140.00

AWS Budgets





AWS Budgets

All budgets (1)	Cost budgets (1)	Usage budgets (0)	Reservation budgets (0)	Savings Plans budgets (0)				
Budget name	Type	Current	Budgeted	Forecasted	Current vs. budgeted	Forecasted vs. budgeted		
MyBudget	Cost	\$13.20	\$100.00	\$129.47	<div style="width: 13.2%; background-color: #0070C0;"></div> 13.2%	<div style="width: 129.47%; background-color: #E74C3C;"></div> 129.47%		

Set Custom Budgets - set custom usage and reservation budgets

Configure Alerts – receive alerts when you exceed or are forecast to exceed your alert thresholds

Integrated with other AWS services – Includes Cost Explorer Chatbot, and Service Catalog

AWS Cost Allocation Tags



AWS Cost Management Tools





AWS Cost Explorer

- The **AWS Cost Explorer** is a free tool that allows you to view charts of your costs
- You can view cost data for the past 13 months and forecast how much you are likely to spend over the next three months
- Cost Explorer can be used to discover patterns in how much you spend on AWS resources over time and to identify cost problem areas
- Cost Explorer can help you to identify service usage statistics such as:
 - Which services you use the most
 - View metrics for which AZ has the most traffic
 - Which linked account is used the most



AWS Cost & Usage Report

- Publish AWS billing reports to an Amazon S3 bucket
- Reports break down costs by:
 - Hour, day, month, product, product resource, tags
- Can update the report up to three times a day
- Create, retrieve, and delete your reports using the AWS CUR API Reference



AWS Price List API

- Query the prices of AWS services
- **Price List Service API** (AKA the Query API) – query with JSON
- **AWS Price List API** (AKA the Bulk API) – query with HTML
- Alerts via Amazon SNS when prices change

AWS Cost Explorer



SECTION 16

Migration, Machine Learning and More

AWS Migration and Transfer Services





AWS Migration Tools



Region



AWS Application
Discovery Service



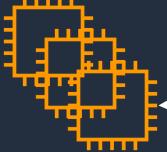
AWS Migration Hub



Amazon S3



Amazon RDS



EC2 Instances



EFS File system



AWS Application
Migration Service



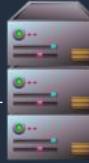
AWS Database Migration
Service



AWS DataSync



Corporate data center



Servers



Database

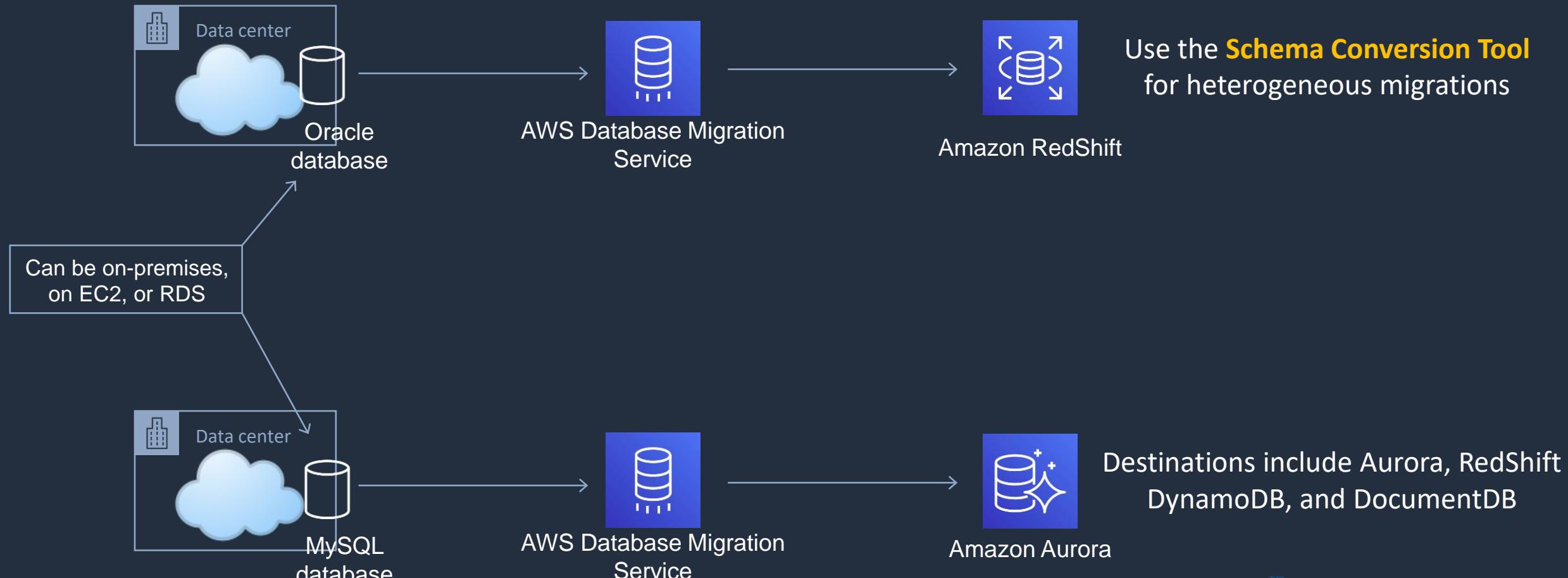


NAS / File
Server

VPN, Direct
Connect or Internet



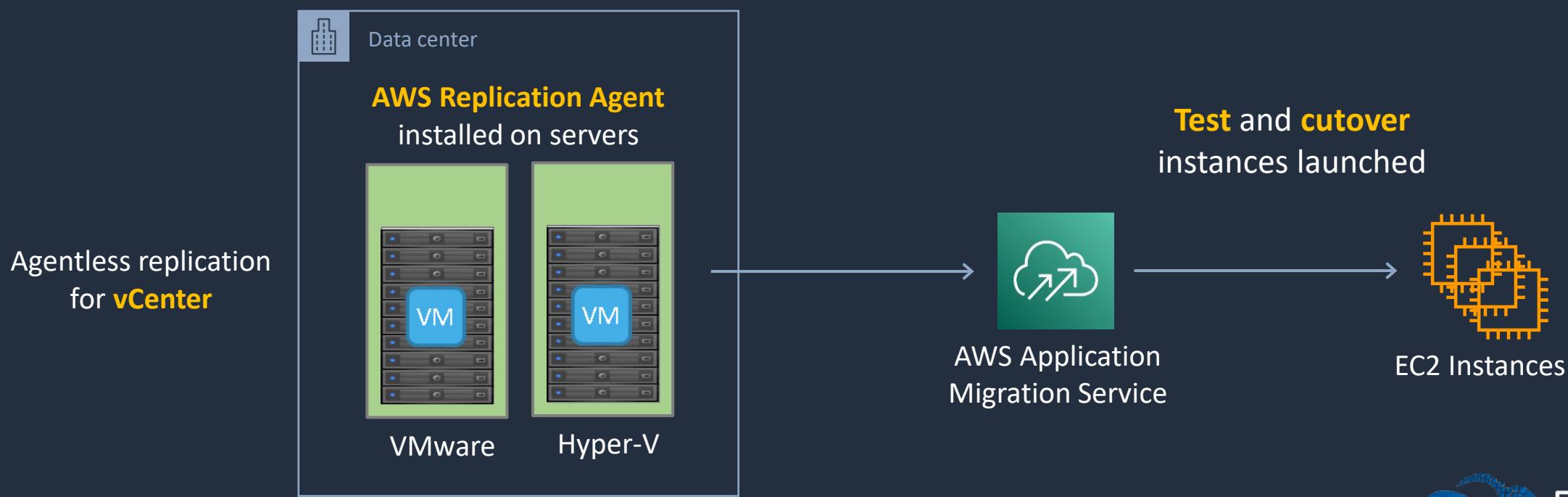
AWS Database Migration Service (DMS)





AWS Application Migration Service

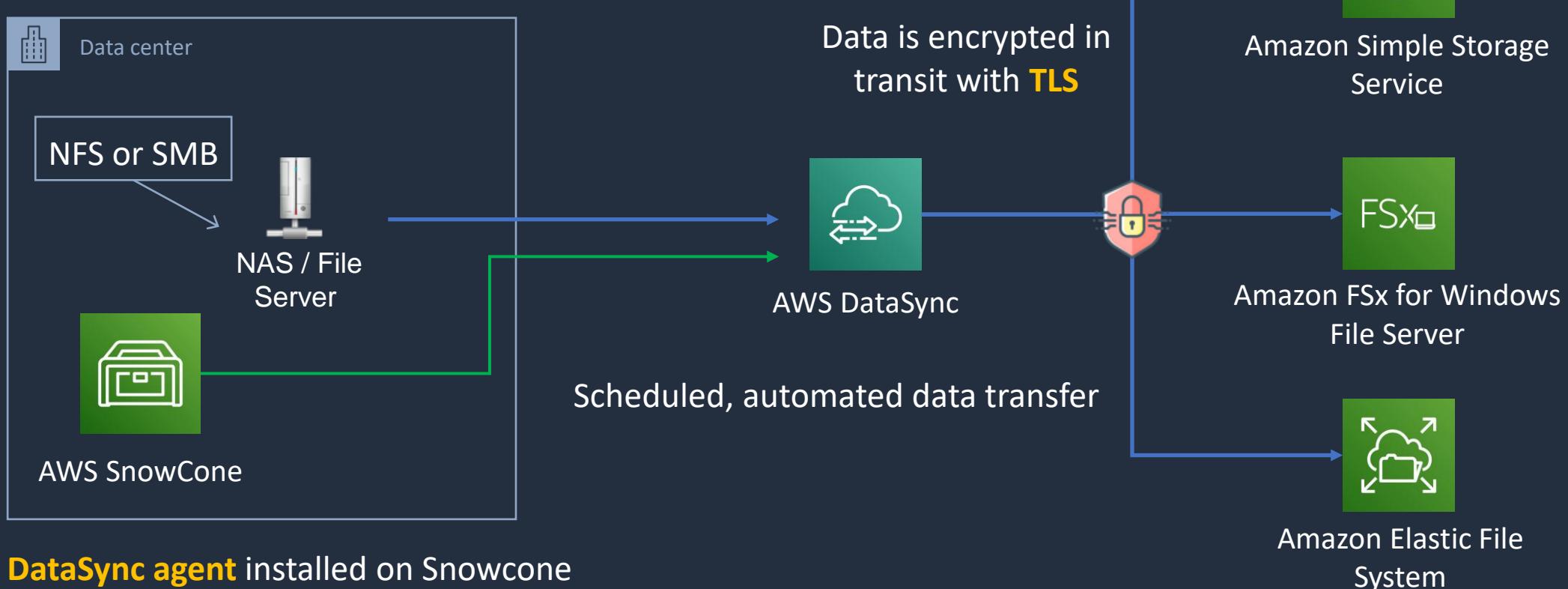
- AWS recommend the AWS Application Migration Service (AWS MGN) for lift & shift migrations
- You can also use AWS Server Migration Service (AWS SMS) and AWS VM Import / Export





AWS DataSync

AWS DataSync **software agent** connects to storage system



DataSync agent installed on Snowcone



AWS Snowball Family

- **AWS Snowball and Snowmobile** are used for migrating large volumes of data to AWS
- **Snowball Edge Compute Optimized**
 - Provides block and object storage and optional GPU
 - Use for data collection, machine learning and processing, and storage in environments with intermittent connectivity (edge use cases)
- **Snowball Edge Storage Optimized**
 - Provides block storage and Amazon S3-compatible object storage
 - Use for local storage and large-scale data transfer
- **Snowcone**
 - Small device used for edge computing, storage and data transfer
 - Can transfer data offline or online with AWS DataSync agent





AWS Snowball Family

- Uses a secure storage device for physical transportation
- Snowball Client is software that is installed on a local computer and is used to identify, compress, encrypt, and transfer data
- Uses 256-bit encryption (managed with the AWS KMS) and tamper-resistant enclosures with TPM
- **Snowball** (80TB) (50TB) “petabyte scale”
- **Snowball Edge** (100TB) “petabyte scale”
- **Snowmobile** – “exabyte scale” with up to 100PB per Snowmobile



AWS Machine Learning and AI Services





AWS Rekognition

Identify objects



Perform facial analysis



Celebrity recognition





AWS Rekognition in Event-Driven Architecture





AWS Rekognition

- Add image and video analysis to your applications
- Identify objects, people, text, scenes, and activities in images and videos
- Processes videos stored in an Amazon S3 bucket
- Publish completion status to Amazon SNS Topic



Amazon Transcribe

- Add speech to text capabilities to applications
- Recorded speech can be converted to text before it can be used in applications
- Uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately



Amazon Translate

- Neural machine translation service that delivers fast, high-quality, and affordable language translation
- Uses deep learning models to deliver more accurate and more natural sounding translation
- Localize content such as websites and applications for your diverse users



Amazon Comprehend

- Natural-language processing (NLP) service
- Uses machine learning to uncover information in unstructured data
- Can identify critical elements in data, including references to language, people, and places, and the text files can be categorized by relevant topics
- In real time, you can automatically and accurately detect customer sentiment in your content



Amazon Lex

- Conversational AI for Chatbots
- Build conversational interfaces into any application using voice and text
- Build bots to increase contact center productivity, automate simple tasks, and drive operational efficiencies across the enterprise



Amazon DevOps Guru

- Cloud operations service for improving **application operational performance and availability**
- Detect behaviors that deviate from normal operating patterns
- Benefits:
 - Automatically detect operational issues
 - Resolve issues with ML-powered insights
 - Elastically scale operational analytics
 - Uses ML to reduce alarm noise



Amazon CodeGuru Security

- Detect, track, and fix code security vulnerabilities anywhere in the development cycle using ML and automated reasoning
- Integrates with IDEs and CI/CD tools
- Automated bug tracking
- Assisted remediation through suggested code fixes
- Offers performance optimization recommendations
- Detects anomalies in application profiles

End User Computing



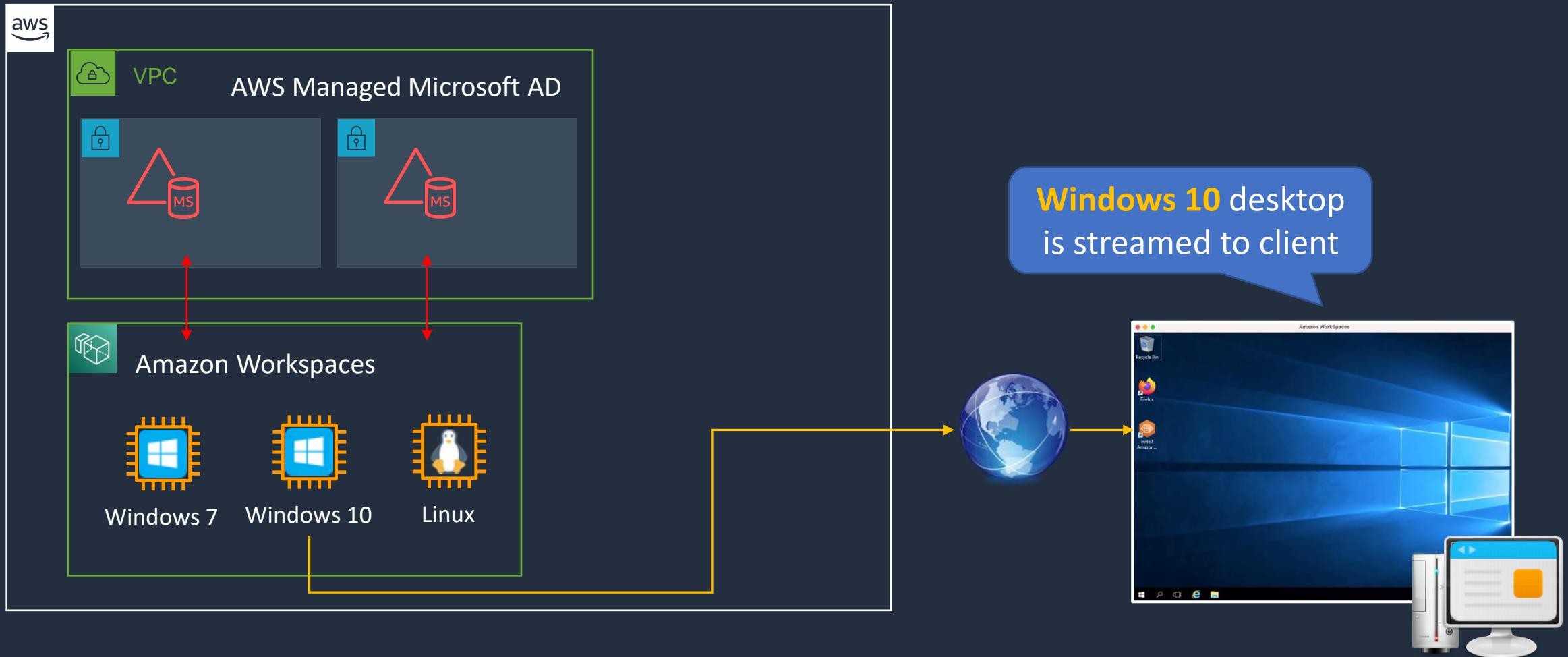


Amazon Workspaces

- Managed **Desktop-as-a-Service** (DaaS) solution
- Provision either Windows or Linux desktops
- Simplifies delivery of desktops compared to traditional virtual desktop infrastructure (VDI) deployments



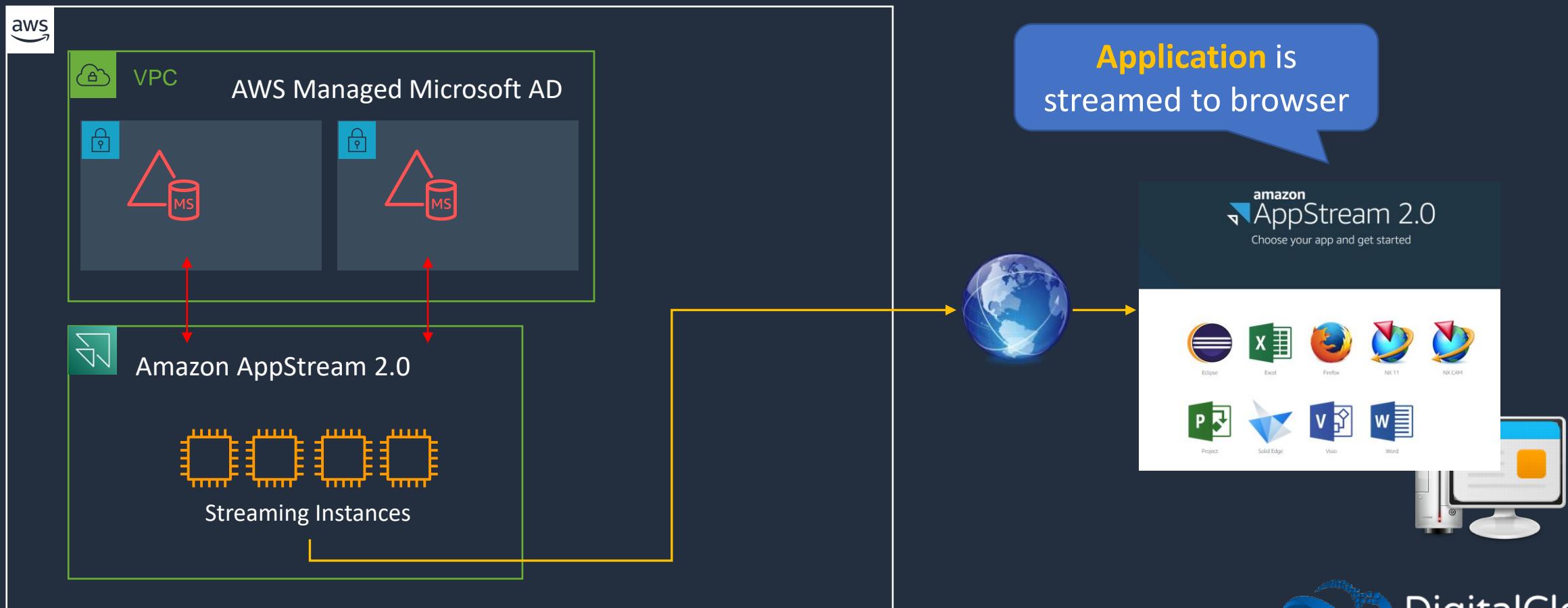
Amazon Workspaces





AWS AppStream 2.0

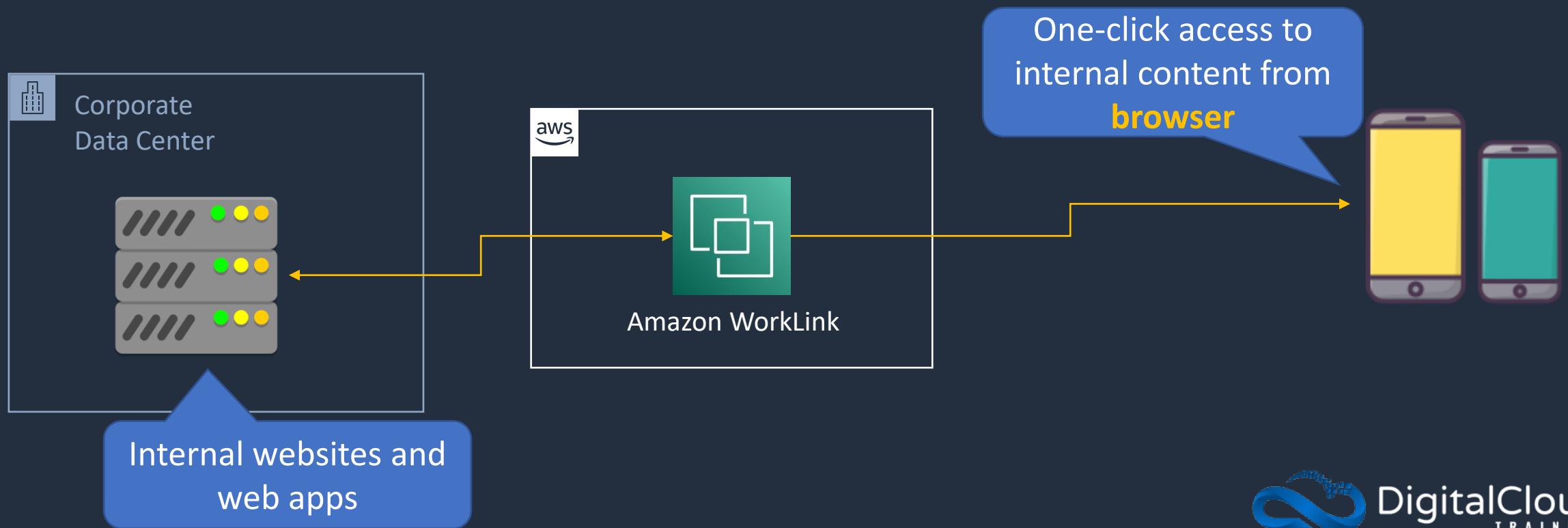
- Fully managed non-persistent application streaming service
- Alternative to popular products such as Citrix XenApp





AWS WorkLink

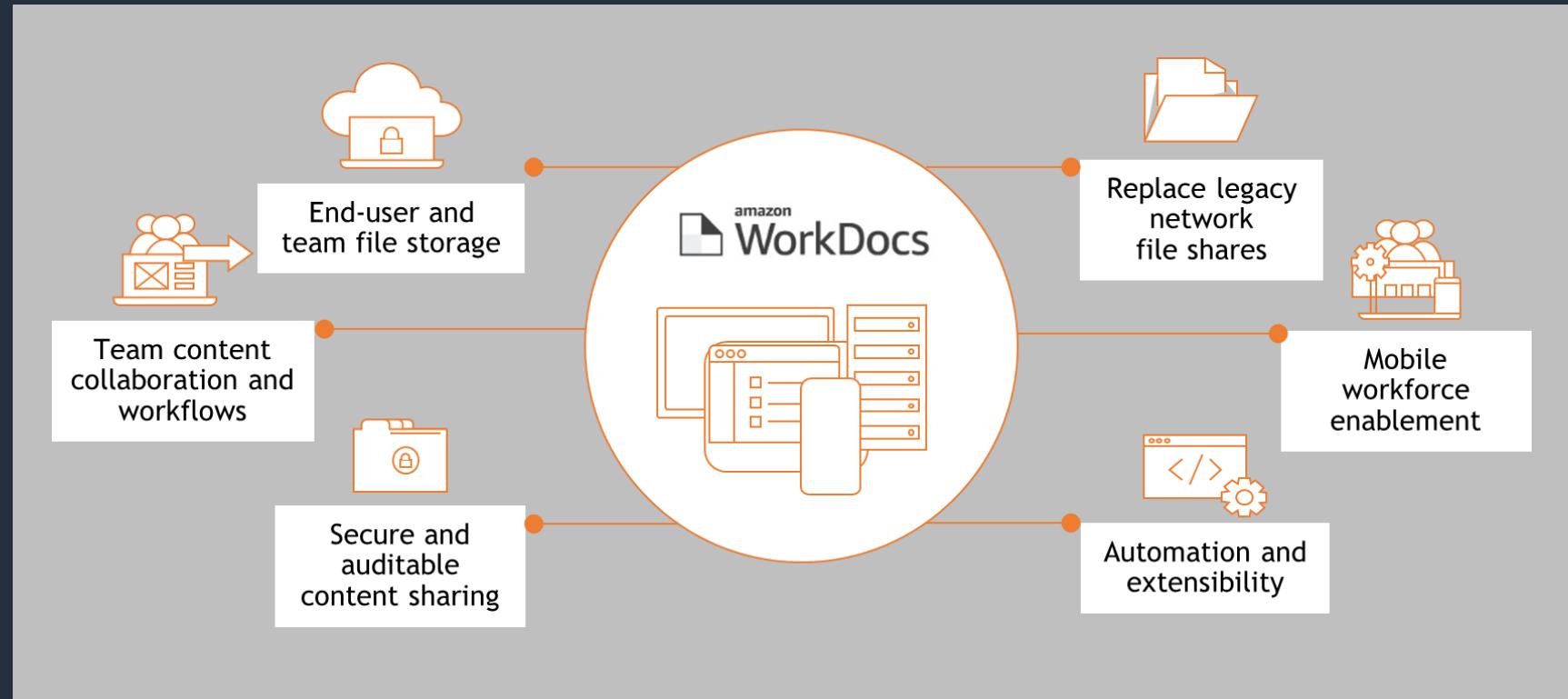
- Provides secure, one-click access to your internal websites and web apps using mobile phone browsers
- Does not require VPN client or App





AWS WorkDocs

- Fully managed, secure content creation, storage, and collaboration service
- Create, edit, and share content that's centrally stored on AWS



AWS IoT Core





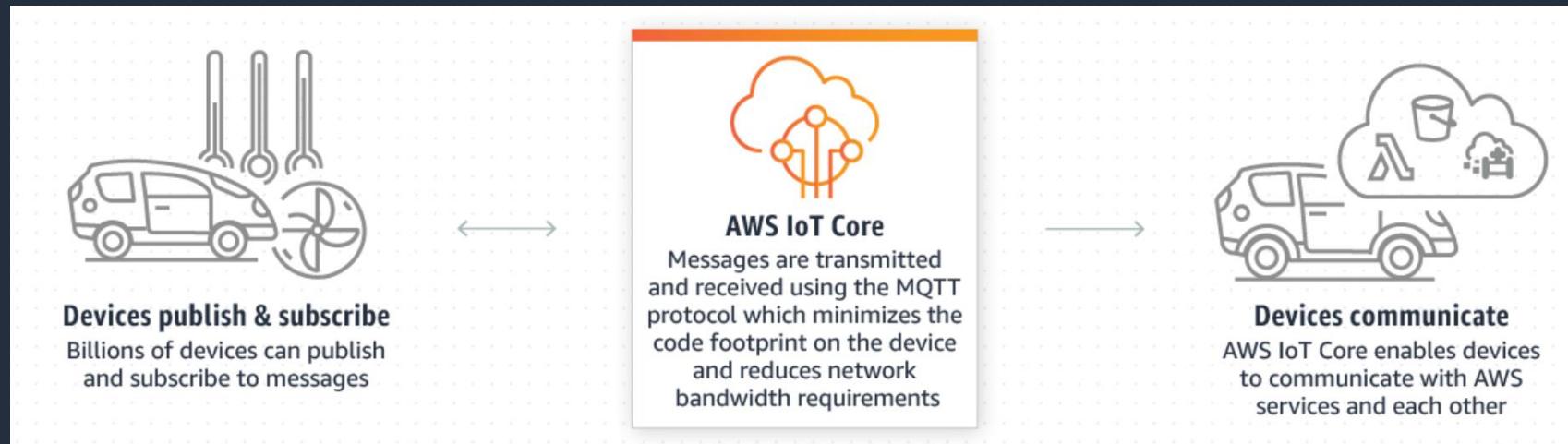
The Internet of Things (IoT)

- Describes the network of physical objects that are embedded with sensors or software
- Each IoT device can communicate and exchange data with other devices and systems
- Use cases include:
 - Smart home automation
 - Smart healthcare
 - Manufacturing
 - Agriculture



AWS IoT Core

- Lets you connect IoT devices to the AWS cloud without the need to provision or manage servers
- Can support billions of devices and trillions of messages



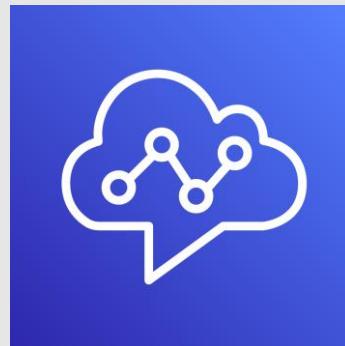
AWS Device Farm



AWS Knowledge Center



Amazon Connect

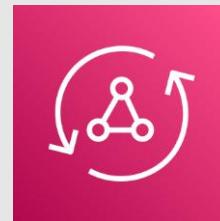




Amazon Connect

- Cloud Contact Center
- Facilitates human agents in helping customers
- Think human connection, not network connection!
- Features include telephony automation, chatbots, task management, and analytics

AWS Amplify and AppSync





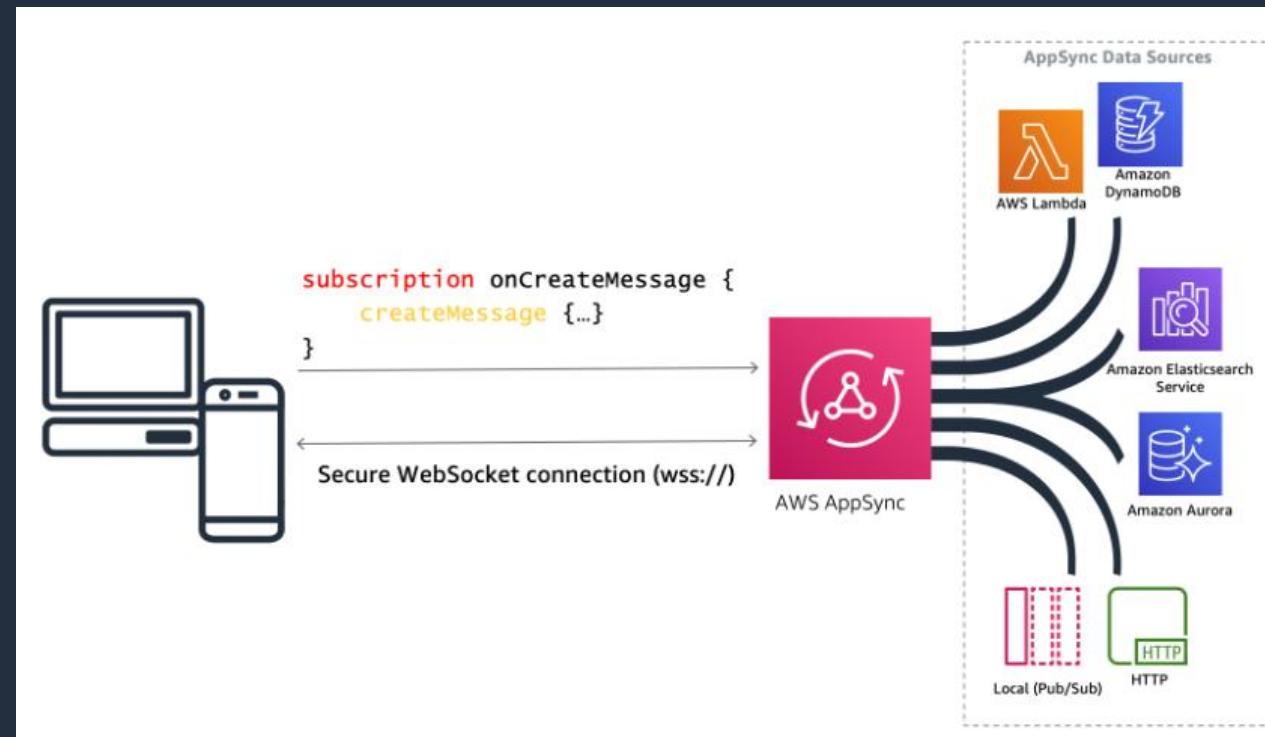
AWS Amplify

- Tools and features for building full-stack applications on AWS
- Build web and mobile backends, and web frontend UIs
- AWS Amplify Studio is a visual interface for building web and mobile apps:
 - Use the visual interface to define a data model, user authentication, and file storage without backend expertise
 - Easily add AWS services not available within Amplify Studio using the AWS Cloud Development Kit (CDK)
 - Connect mobile and web apps using Amplify Libraries for iOS, Android, Flutter, React Native, and web (JavaScript)
- AWS Amplify Hosting is a fully managed CI/CD and hosting service for fast, secure, and reliable static and server-side rendered apps



AWS AppSync

- AWS AppSync is a fully managed service that makes it easy to develop GraphQL APIs
- Applications can securely access, manipulate, and receive real-time updates from multiple data sources such as databases or APIs





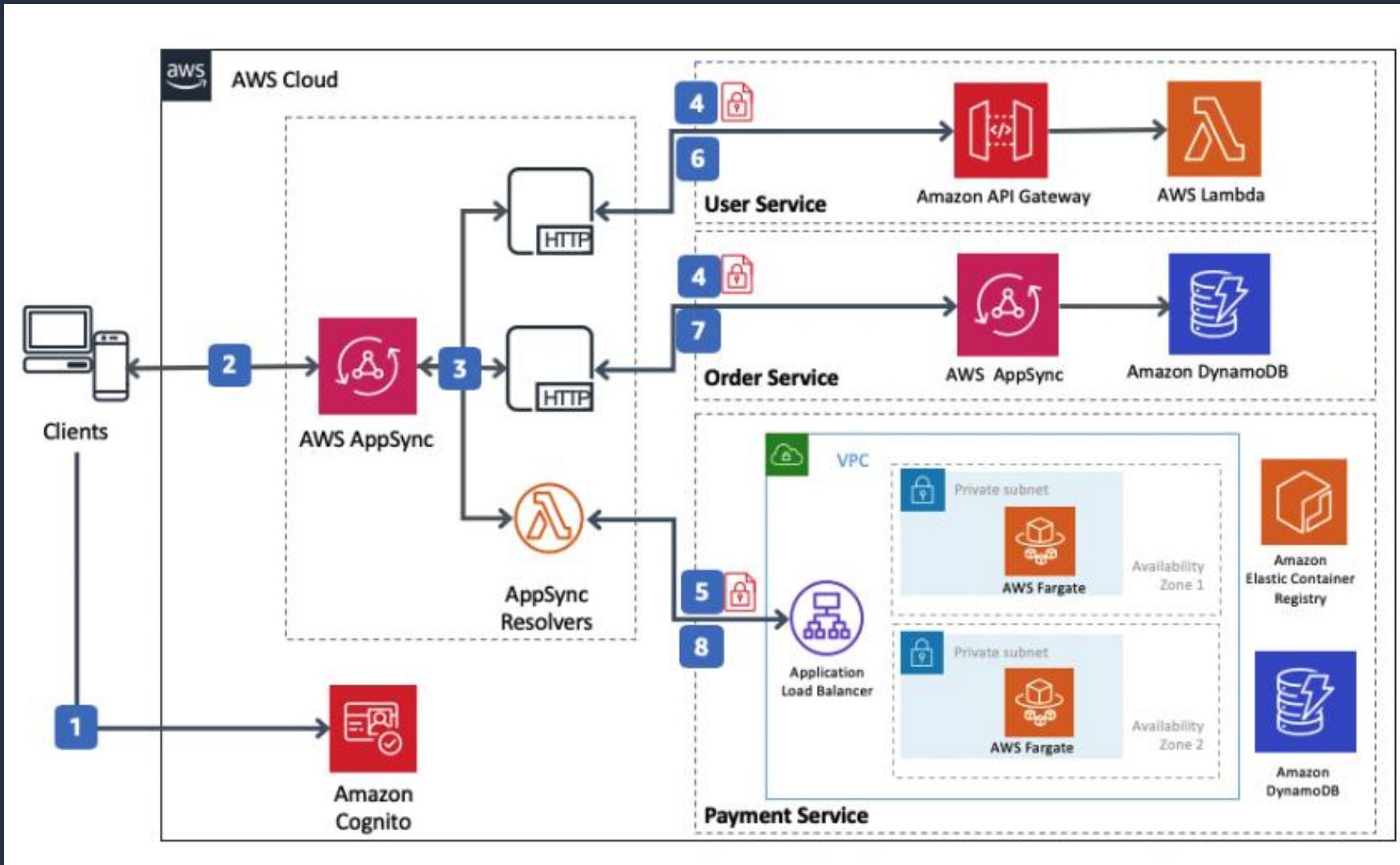
AWS AppSync

- AWS AppSync automatically scales a GraphQL API execution engine up and down to meet API request volumes
- Uses GraphQL, a data language that enables client apps to fetch, change and subscribe to data from servers
- AWS AppSync lets you specify which portions of your data should be available in a real-time manner using GraphQL Subscriptions
- AWS AppSync supports AWS Lambda, Amazon DynamoDB, and Amazon Elasticsearch
- Server-side data caching capabilities reduce the need to directly access data sources
- AppSync is fully managed and eliminates the operational overhead of managing cache clusters



AWS AppSync

Example of using **AppSync** and **Amplify** to simplify access to microservices



Amplify is used to build and host the WebStore application and create backend services

AppSync creates a unified API layer for integrating the microservices

Customer Enablement Services





- AWS IQ is a platform to help customers find, securely collaborate with, and pay AWS-certified third-party experts for on-demand project work
- AWS IQ is a marketplace where AWS customers can find and hire AWS-certified consultants and experts to help with the deployment, optimization, and management of AWS applications and services
- The platform offers secure collaboration tools, including secure messaging and project tracking, to ensure a safe and efficient collaboration environment
- AWS IQ simplifies the payment process, allowing customers to pay experts directly through their AWS account, leveraging AWS's secure payment infrastructure
- Customers have the flexibility to work with experts on a wide range of project types, whether it be a small one-time task or a larger, ongoing project



AWS Managed Services (AMS)

- AMS takes over the daily operations of AWS infrastructure, handling tasks such as patch management, backup, and incident monitoring
- Customers gain access to AWS experts for the management and operation of AWS infrastructure, leveraging industry best practices
- Speeds up the migration process to AWS, assisting businesses in quickly reaping the benefits of the cloud
- Helps in managing and reducing operational costs through optimized AWS resource management
- Ensures a secure environment that meets necessary compliance requirements, providing peace of mind
- Allows businesses to focus more on innovation and less on managing infrastructure, fostering growth and development



AWS Activate for Startups

- Empowers startups with tools and resources to help bring ideas to market
- A program designed specifically for startups, providing them with AWS credits, training, technical support, and other resources
- Facilitates growth by offering a range of tools and resources to help startups build, grow, and scale their business on AWS
- Includes training and technical support to startups, empowering them with the knowledge to leverage AWS's full potential
- Connects startups with a community of developers, mentors, and entrepreneurs, creating networking and learning opportunities

SECTION 17

Exam Preparation and Tips

Booking your Exam



Exam Preparation Tips





Exam Preparation Tips

- Dedicate regular time to learning
- Use the free study plan
- Use practice tests early and regularly
- Review knowledge areas where you score poorly
- Don't book the exam until you're ready
- Non-native English speakers can request an extension (extra 30 minutes)
- If you've taken another AWS exam before, use your 50% discount voucher

Exam Question Walkthrough

