# AWS Certified Cloud Practitioner Foundational Crash Course

**Chad Smith**
Principal Cloud Architect

Pearson

# Introduction to AWS Certifications

# Cloud Practitioner Exam Details

# Exam Logistics - By the Numbers

| | |
|---|---|
| Number of questions: | **65** |
| Time for exam | **90 minutes** |
| Answer choices | **4-6** |
| Score required | **700/1000** |
| Number of unscored questions | **15** |
| Penalty for guessing | **0** |

# Exam Guide Layout

- Introduction
- Target Candidate Description
- Exam Content

# Exam Guide Introduction

Validates a candidate's ability to:

Explain the value of the AWS Cloud

# Exam Guide Introduction

Validates a candidate's ability to:

Understand and explain the AWS shared responsibility model

# Exam Guide Introduction

Validates a candidate's ability to:

Understand security best practices

# Exam Guide Introduction

Validates a candidate's ability to:

Understand AWS Cloud costs, economics, and billing practices

# Exam Guide Introduction

Validates a candidate's ability to:

Describe and position the core AWS services, including compute, network, databases, and storage

# Exam Guide Introduction

Validates a candidate's ability to:

Identify AWS services for common use cases

# Exam Guide Target Candidate Description

- 6 months engagement
- Exposure to:
  - Design
  - Implementation
  - Operations
- Understanding of well-designed AWS cloud solutions

# Exam Guide Out of Scope

- Coding
- Designing cloud architecture
- Troubleshooting
- Implementation
- Migration
- Load and performance testing
- Business applications

# Exam Guide Exam Content

| Question Domains | % |
| --- | --- |
| Cloud Concepts | 26 |
| Security and Compliance | 25 |
| Technology | 33 |
| Billing and Pricing | 16 |

# Exam Guide Exam Content

- Outline for each domain
- Terminology
- Service names
- Feature names

# AWS Certification Strategies

# Question Format

All questions are fact-based. None of them will involve more than a single topic

Multiple response questions are clearly marked. (SELECT two or three)

A. Answer
B. Choices
C. Up
D. To
E. Six
F. Options

# Question Format

**Question details are RELEVANT**

**No mixing of question domains**

**No trick questions**

A. **Answers are reasonable**
B. **Many are functional solutions**
C. **Very few obvious wrong answers**
D. **Every word counts**

# Strategy Tips

## Tip #1

It is more important to know why a wrong answer is wrong than to know why the right answer is right

# Strategy Tips

## Tip #2

Read the documentation, as the question words and phrases will follow the same patterns

# Strategy Tips

## Tip #3

Don't spin your wheels, flag questions and come back later

# Strategy Tips

## Tip #4

Don't memorize numbers: the exam will not have number-based questions

# Strategy Tips

## Tip #5 (Optional)

Read the answer choices BEFORE the question

# Question Domain 1: Cloud Concepts

# Question Domain Points

Define the AWS Cloud and its value proposition

Identify aspects of AWS Cloud economics

Explain the different cloud architecture design principles

## Question Domain 1: Cloud Concepts

# AWS Cloud Definition

# AWS Official Definition

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

# Definition Drill-Down

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted **cloud** platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

Cloud?
*On-demand
*Pay as you go
*Network-accessible

# Definition Drill-Down

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering **over 200 fully featured services** from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

There is a service for almost everything, and you'll need to specialize!

# Definition Drill-Down

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from **data centers globally**. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

Hundreds of data centers and millions of servers around the world!

# Definition Drill-Down

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to **lower costs, become more agile, and innovate faster**.

You can do these in ways not possible using on-premises data centers!

## Question Domain 1: Cloud Concepts

# Cloud Value Proposition

# Benefits of AWS

## Security

AWS offers easy access to centralized security services and features

# Benefits of AWS

## Reliability

Reduced KTLO tasks because AWS manages the data centers

# Benefits of AWS

## High Availability

Placement options for business continuity, and built-in HA/FT for many services and features

# Benefits of AWS

## Elasticity

Scale out for performance, scale in for cost

# Benefits of AWS

## Agility

AWS democratizes advanced technologies making them easier to adopt

# Benefits of AWS

## Pay-as-you go Pricing

Allows for experimentation and testing, even at full scale

# Benefits of AWS

## Scalability

Scale out to much greater capacity than would be possible on-premises

# Benefits of AWS

## Global Reach

Provision resources close to customers or to maintain compliance

# Benefits of AWS

## Economy of scale

AWS Pricing is competitive because of the overall size of infrastructure

# Question Breakdown

# Question and Answer Choices

**Which of the following benefits of the cloud value proposition would be defined by the ability to add or remove resources to meet demand?**

A. Reliability
B. Scalability
C. Elasticity
D. Economy of scale

# Correct Answer and Explanation

**Elasticity - the ability of a system to increase and decrease resources allocated (usually horizontally) to match demand, and implies automation.**

A. Reliability
B. Scalability
C. Elasticity
D. Economy of scale

## Question Domain 1: Cloud Concepts

# AWS Cloud Economics

# Pay As You Go

- Adapt to changing business needs
- Stop wasting time on forecasting
- No need to overprovision

# Save When You Commit

- Reservations
- Savings Plans
- 1- or 3-year commitments

# Pay Less By Using More

- Volume-based discounts
- Tiered pricing
- Mostly storage and network traffic

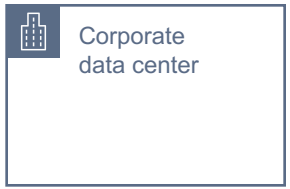
# What is CapEx?

- Up front payment
- Maintenance contracts
- Amortize value over time
- Own the product
- Predictable cost

# What is OpEx?

- Subscriptions
- Pay as you go
- Operations have their own cost
- Variable and often unpredictable

# TCO - Total Cost of Ownership



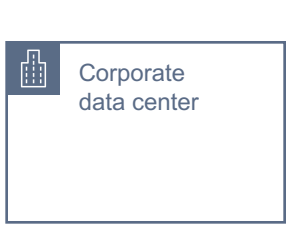

Data Center

# TCO - Total Cost of Ownership


Data Center

Hardware

# TCO - Total Cost of Ownership




Data Center

Hardware

Storage

# TCO - Total Cost of Ownership


Data Center | Hardware | Storage | Network

What do many organizations consider to be Total Cost of Ownership?

What is missing from this list?

# KTLO - Keeping The Lights On

- Any zero-sum game operation
- Proportional to unmanaged resources
- More OS-based resources = more operations

# Cloud Software Licensing

- More complex than on-premises licensing
- Must account for temporary resources
- Bring Your Own - sometimes

# Question Breakdown

# Question and Answer Choices

**Which of the following is not part of AWS cloud economics?**

A. Pay as you go
B. Save when you commit
C. Pay less by using more
D. Pay for everything up front

# Correct Answer and Explanation

**The AWS pricing model does not support CapEx methods, and is much more oriented toward dynamic, operational expenses.**

A. Pay as you go
B. Save when you commit
C. Pay less by using more
D. Pay for everything up front

## Question Domain 1: Cloud Concepts

# Cloud Architecture Design Principles

# Design Principles

- Design for failure
- Decouple components
- Implement elasticity
- Think parallel

# Well-Architected Framework

Learn how to design, use, and manage workloads in the cloud.

Learn how to translate requirements into architecture and operations while following best practices.

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization
- Sustainability

# Operational Excellence


The ability to support development and run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value.

# Operational Excellence

- Perform operations as code
- Annotated documentation
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

# Performance Efficiency


The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.

# Performance Efficiency

- Democratize advanced technologies
- Go global in minutes
- Use serverless architectures
- Experiment more often
- Mechanical sympathy

# Security


The ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.

# 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


The ability of a workload to 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.

# Reliability

- Test recovery procedures
- Automatically recover from failure
- Scale horizontally to increase aggregate system availability
- Stop guessing capacity
- Manage change in automation

# Cost Optimization


The ability to run systems to deliver business value at the lowest price point.

# Cost Optimization

- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on data center operations
- Analyze and attribute expenditure
- Use managed services to reduce cost of ownership

# Sustainability


Ability to focus on environmental impacts, especially energy consumption and efficiency, since they are important levers for architects to inform direct action to reduce resource usage.

# Sustainability

- Understand your impact
- Establish sustainability goals
- Maximize utilization
- Anticipate and adopt new, more efficient hardware and software offerings
- Use managed services
- Reduce the downstream impact of your cloud workloads

# Question Breakdown

# Question and Answer Choices

**Which of the pillars of the Well-Architected Framework contains the principle "stop guessing capacity"?**

A. Performance efficiency
B. Operational excellence
C. Reliability
D. Sustainability

# Correct Answer and Explanation

**The Reliability pillar has some overlap with Performance Efficiency, but the maximum capacity values belong in Reliability.**

A. Performance efficiency
B. Operational excellence
C. Reliability
D. Sustainability

# Question Domain 2: Security and Compliance

# Question Domain Points

- Define the AWS shared responsibility model
- Define AWS Cloud security and compliance concepts
- Identify AWS access management capabilities
- Identify resources for security support

## Question Domain 2: Security and Compliance

# AWS Shared Responsibility Model

# Who Shares Responsibility?

?

?

# AWS Responsibility

AWS

"Security of the Cloud"

Responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

# Customer Responsibility

Customer

"Security in the Cloud"

Responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

# Who Owns IT Controls?

AWS

Customer

# Inherited Controls

AWS

Customer

Physical Controls

Environmental Controls

Controls which a customer fully inherits from AWS.

# Shared Controls

AWS

Customer

Patch Management

Configuration Management

Awareness & Training

Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives.

# Customer-Specific Controls

AWS

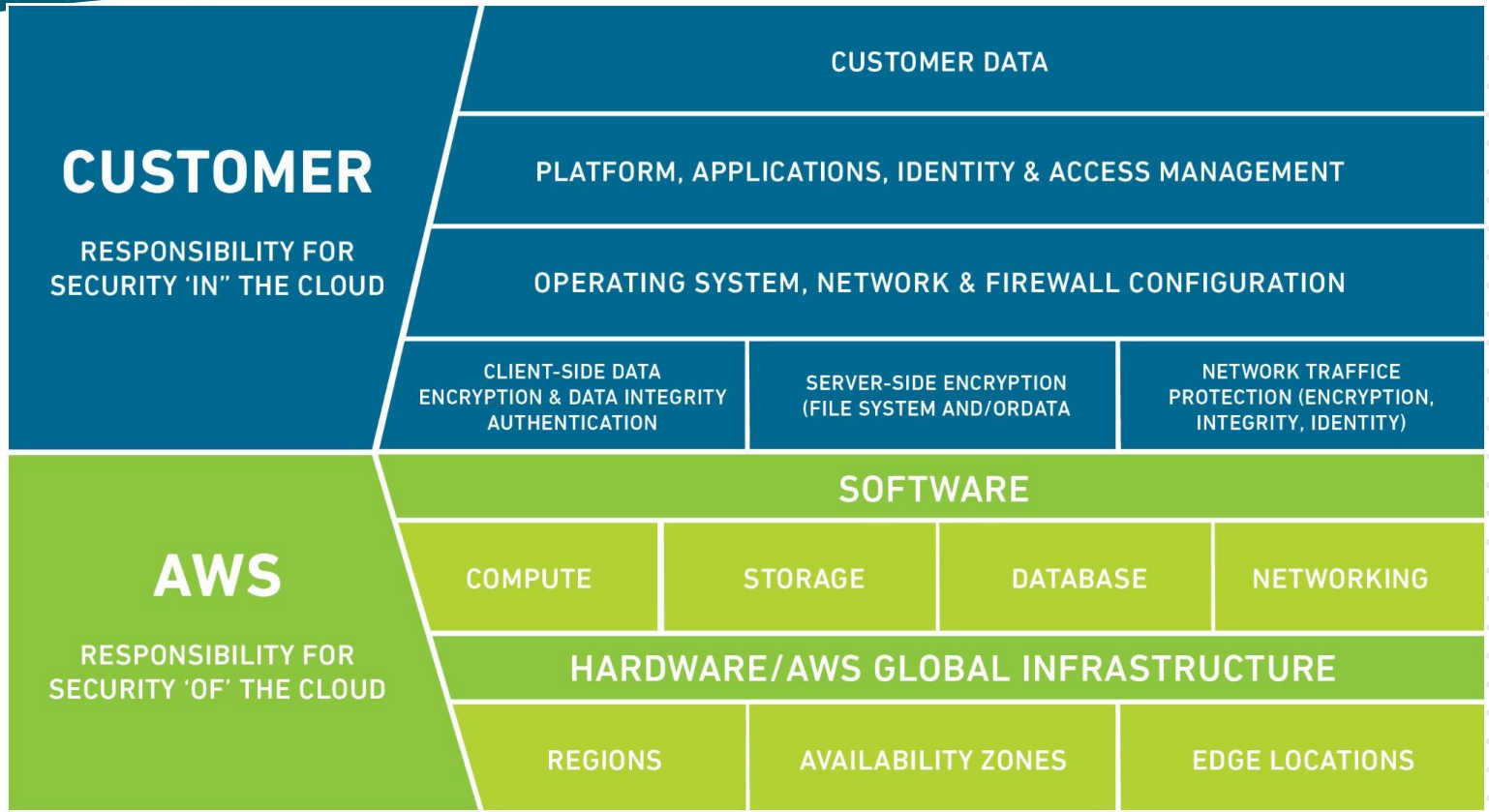
Customer

Region Choices

Service/feature Choices

Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services.

# Shared Responsibility Big Picture



# Question Breakdown

# Question and Answer Choices

**Which of the following responsibilities would the customer manage directly, according to the AWS shared responsibility model?**

**(pick two)**

A. Applying security patches to the hypervisor for virtual machines
B. Enforcing DDoS protection for service API endpoints
C. User account management on virtual machine guest operating systems
D. Selecting the encryption key to use for protecting data at-rest
E. In-transit encryption of cross-region network traffic

# Correct Answer and Explanation

**All guest OS operations are the responsibility of the customer, as is the choice of encryption keys for any at-rest encryption.**

A. Applying security patches to the hypervisor for virtual machines
B. Enforcing DDoS protection for service API endpoints
C. User account management on virtual machine guest operating systems
D. Selecting the encryption key to use for protecting data at-rest
E. In-transit encryption of cross-region network traffic

## Question Domain 2: Security and Compliance

# Security and Compliance Concepts

# AWS Compliance Locations

## Portals

https://aws.amazon.com/compliance/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compliance-validation.html

# AWS Compliance Locations

## Portals

https://aws.amazon.com/compliance/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compliance-validation.html

## Whitepapers

Amazon Web Services: Risk and Compliance

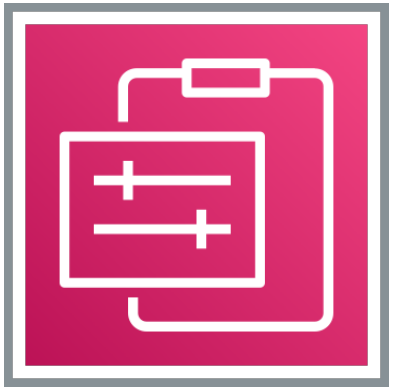
Navigating GDPR Compliance on AWS

# AWS Compliance Programs

## Compliance Programs

- SOC
- PCI
- FedRAMP
- HIPAA
- FINMA
- and others!
- Compliance varies per service

# Service Compliance Considerations



Service availability doesn't imply all features are available in the region

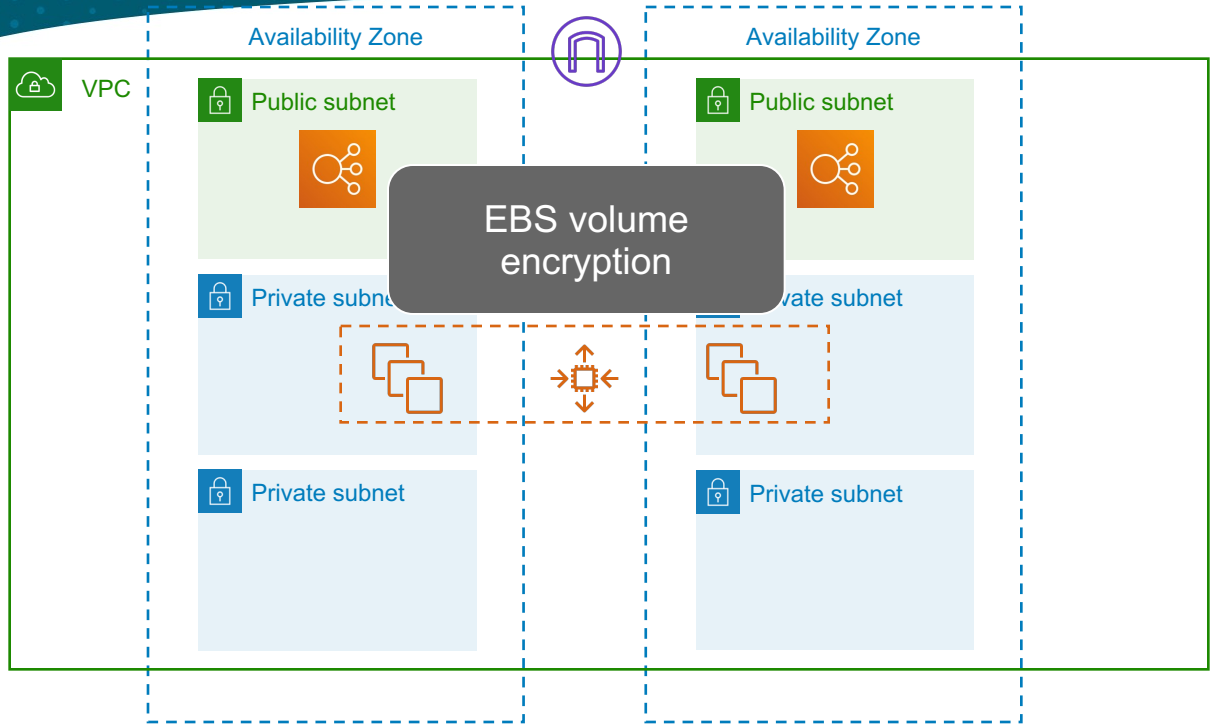
Check for service compliance by program (PCI, SOC, GDPR, etc.)

Service compliance doesn't imply all features are compliant

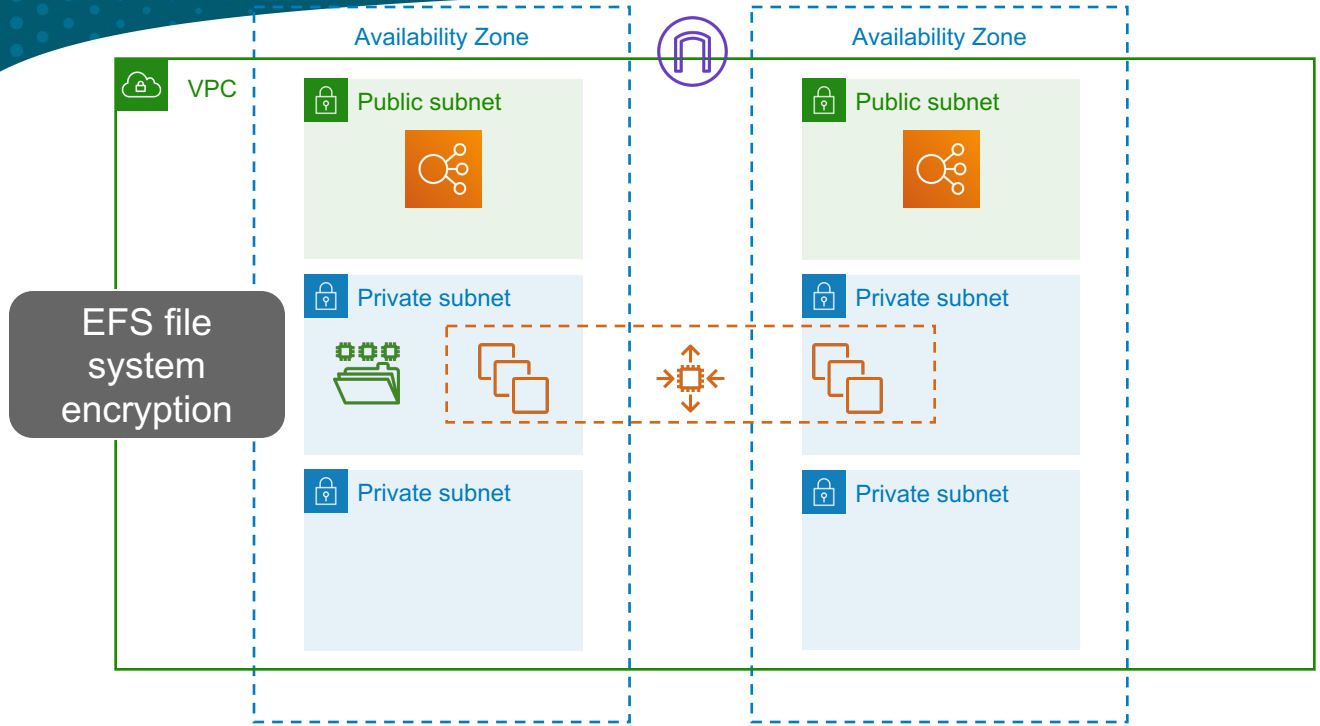
When in doubt, ask support!

# At-rest Encryption On AWS

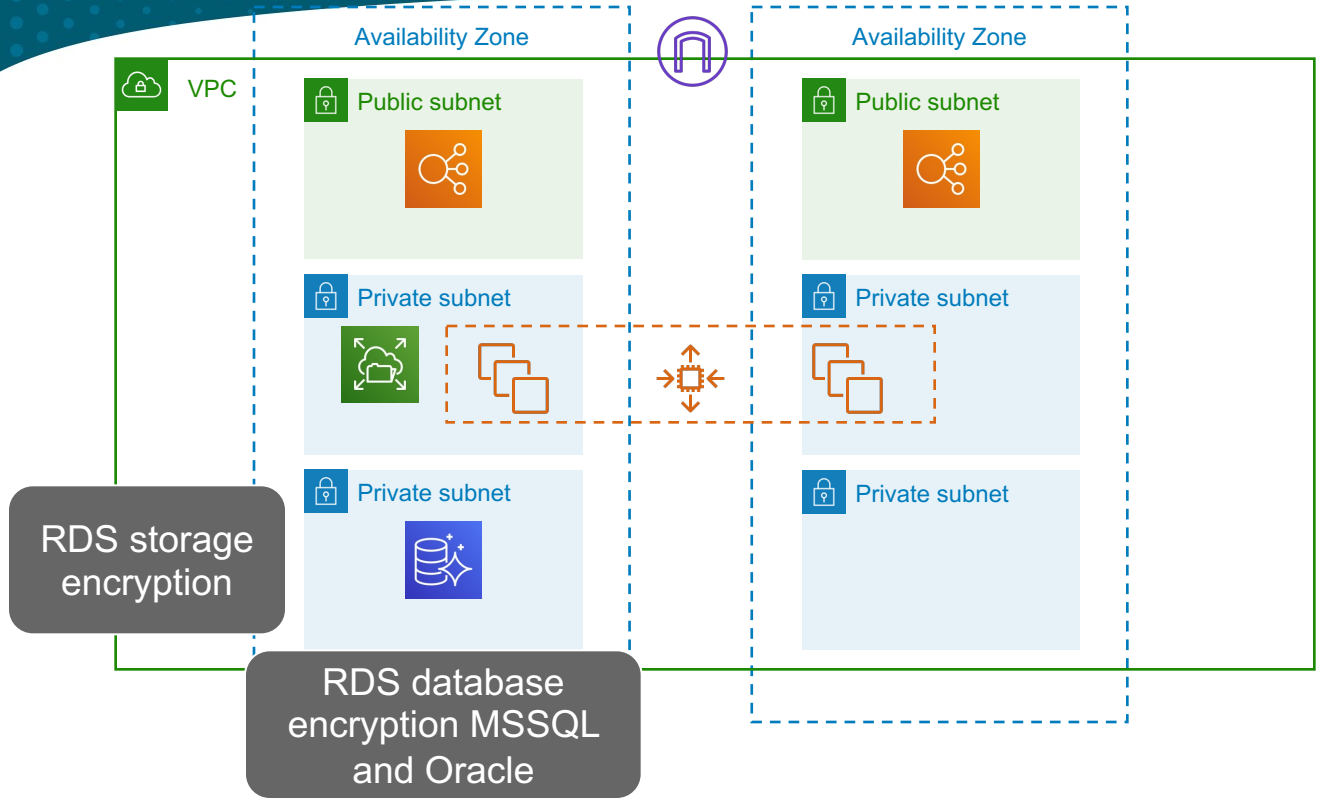
# At-rest Encryption On AWS



# At-rest Encryption On AWS

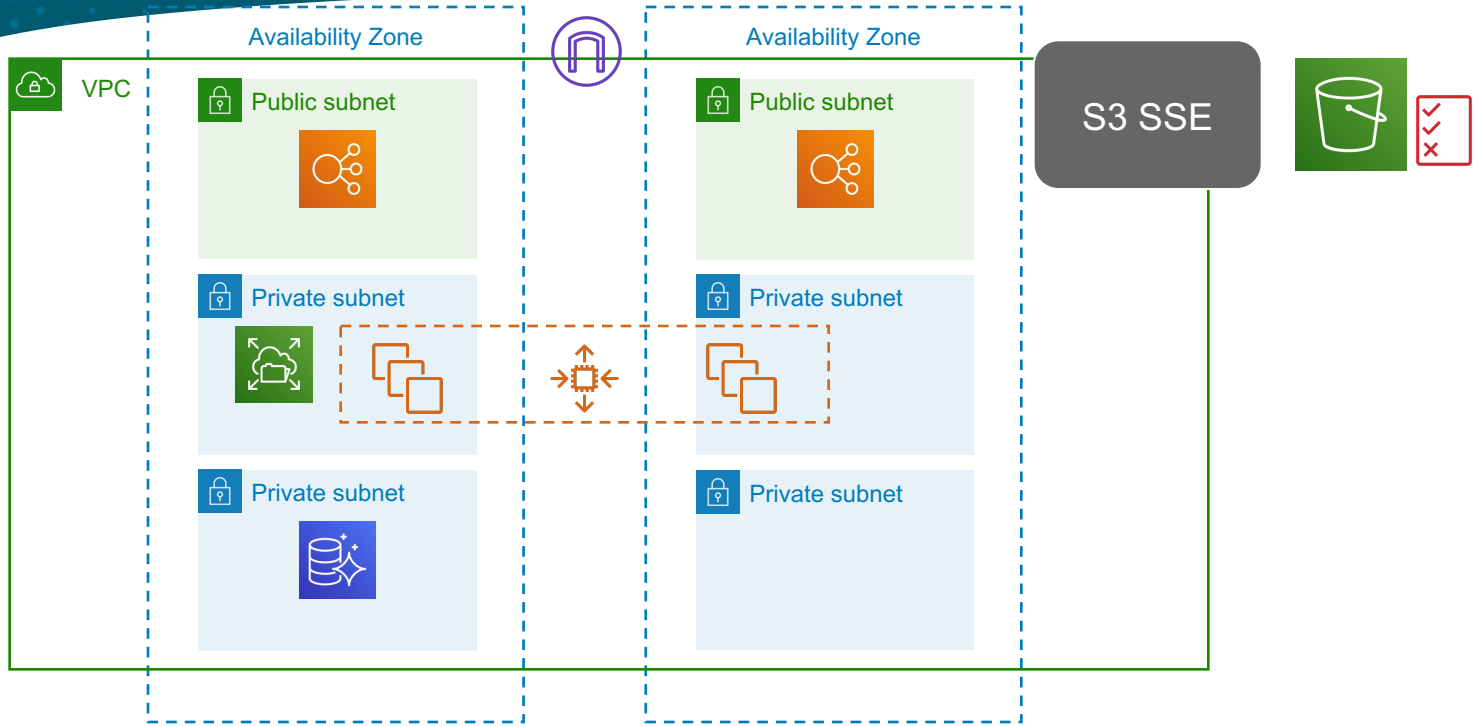


# At-rest Encryption On AWS

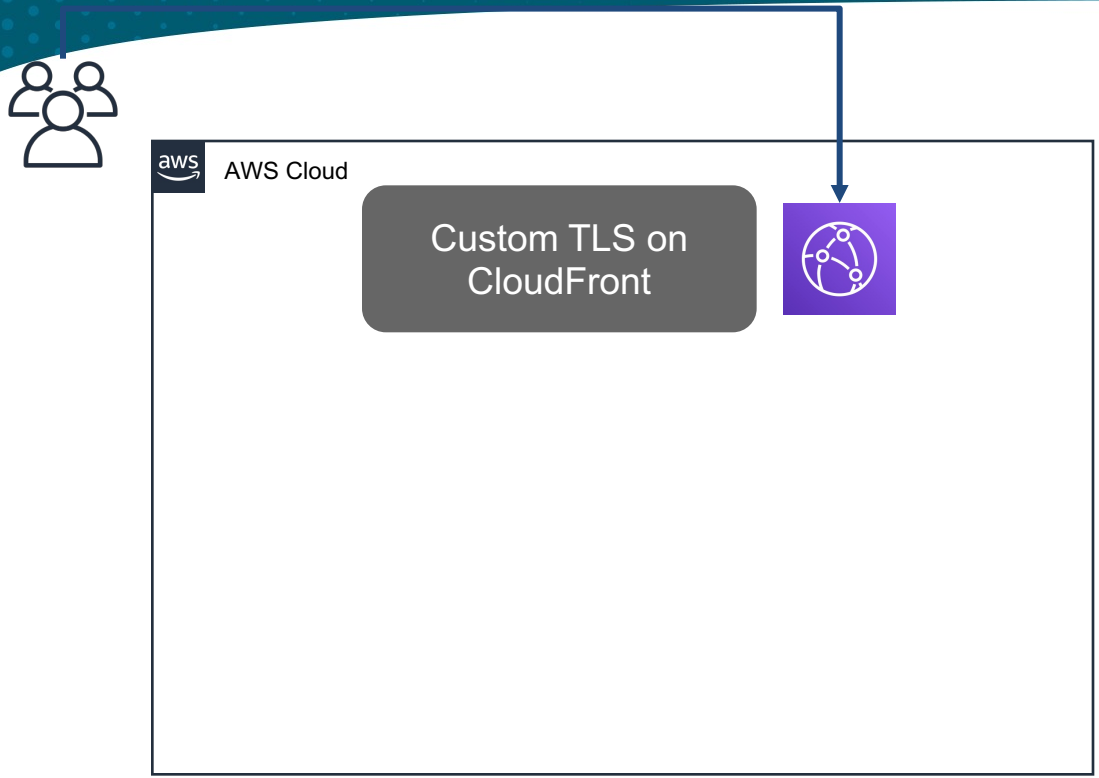



Pearson

# At-rest Encryption On AWS

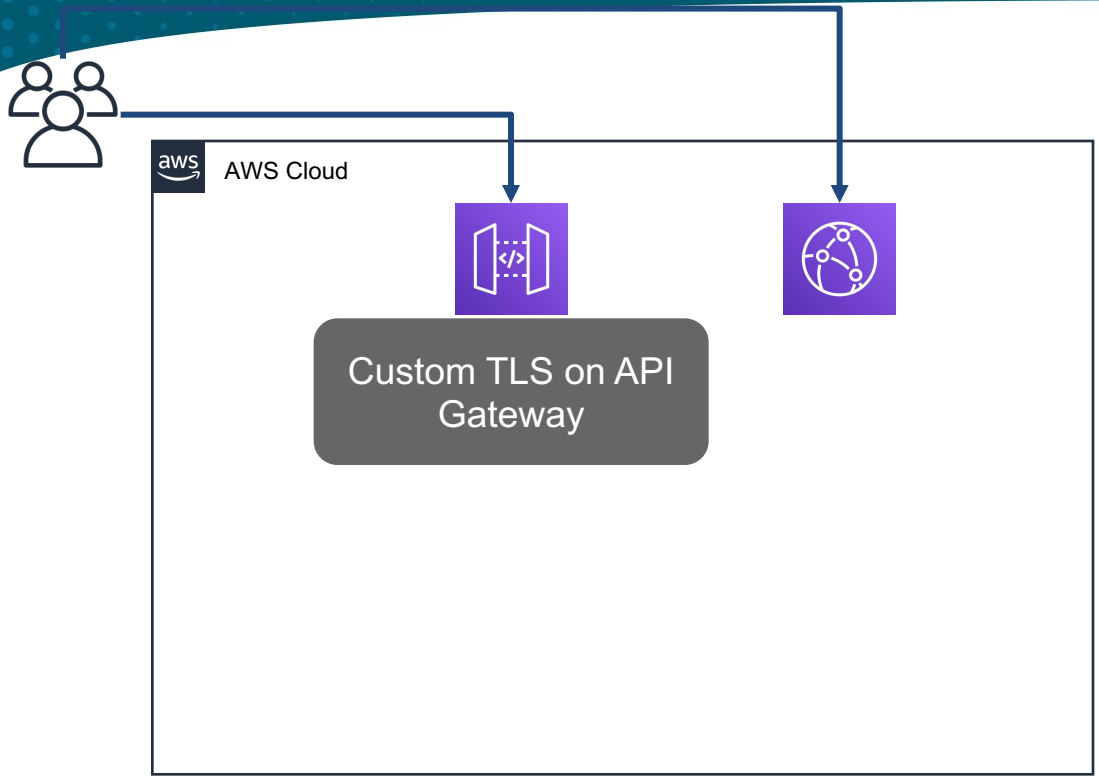


# In-Transit Encryption On AWS



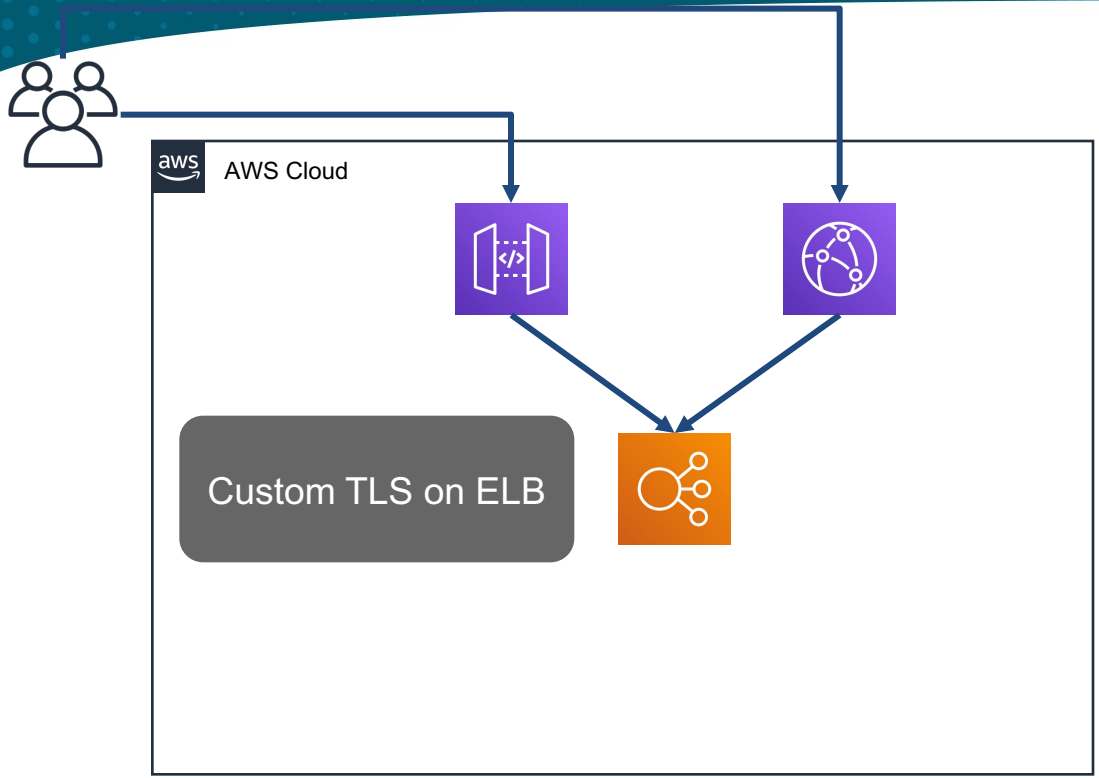

The CloudFront distribution must have the DNS CNAME records listed in the configuration for TLS

# In-Transit Encryption On AWS



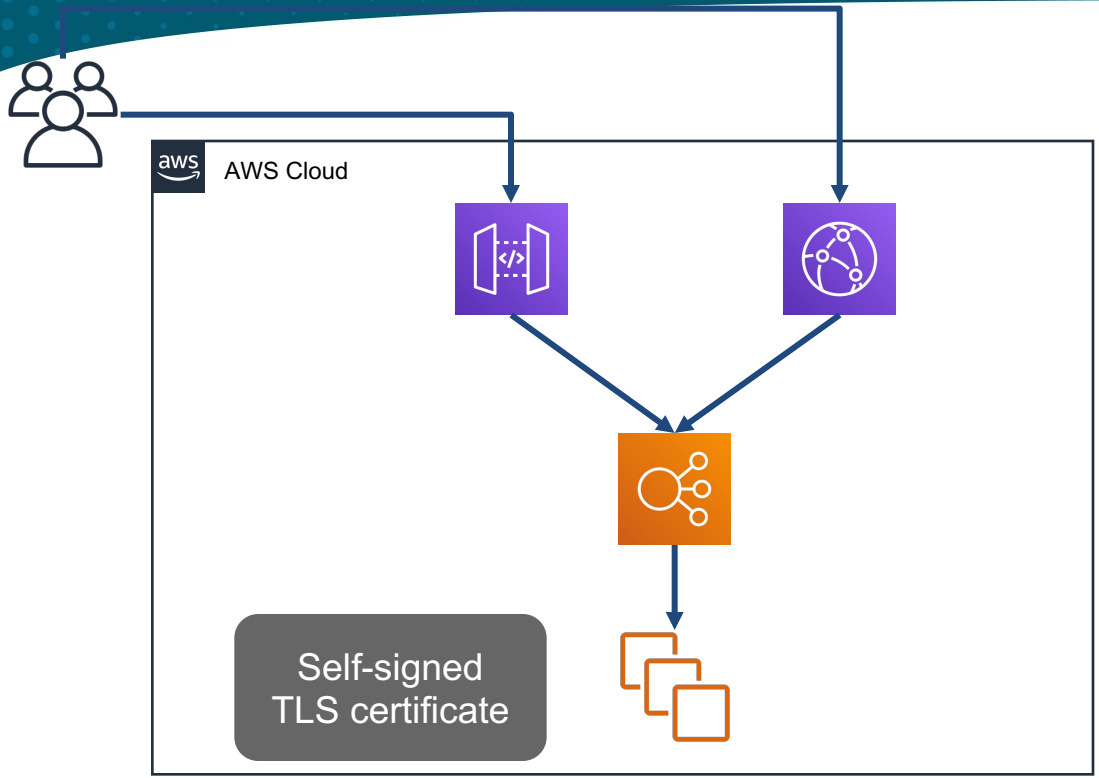

The API Gateway must also have the DNS CNAME records listed in the configuration for TLS

# In-Transit Encryption On AWS



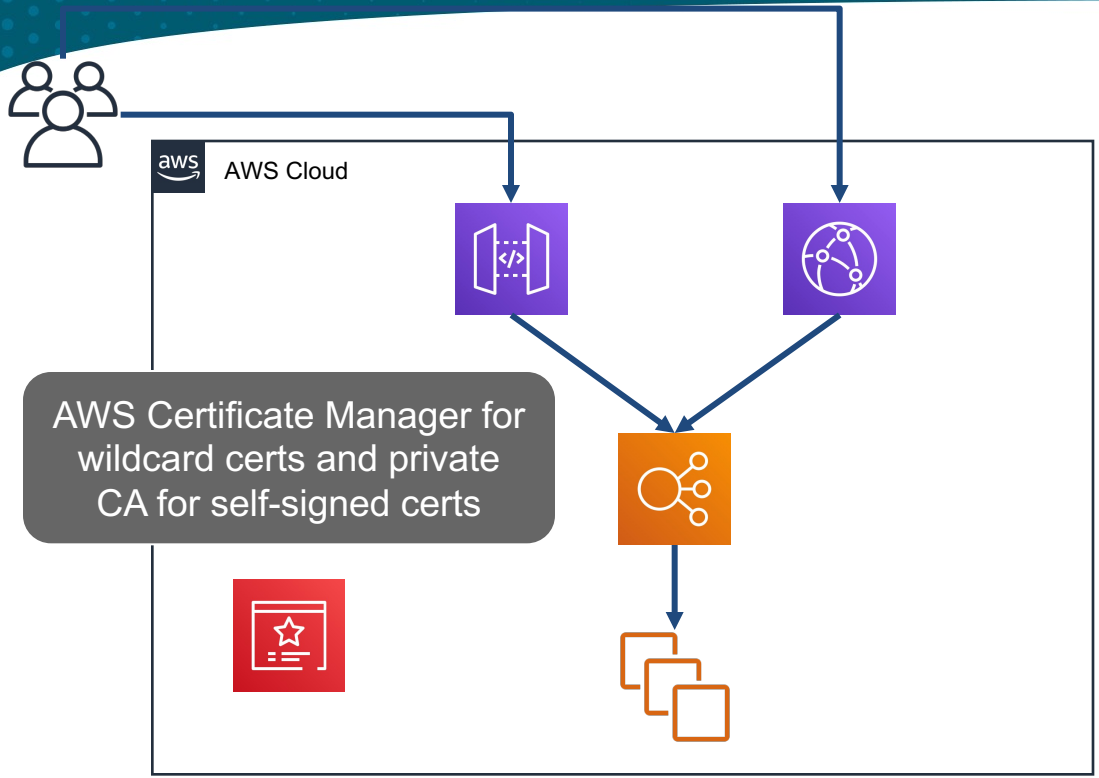

Classic and Network load balancers support 1 TLS cert, Application load balancers support 25

# In-Transit Encryption On AWS




This cert does not require matching DNS or can even be expired as the ELB does not validate TLS

# In-Transit Encryption On AWS




ACM certs must be provisioned in us-east-1 for CloudFront, otherwise in the same region as the resource

# Encryption Questions

- What keys are involved?
- Who owns the keys?
- Where is the encryption performed?
- How is key access control implemented?
- Who enables encryption?

# Question Breakdown

# Question and Answer Choices

**When a customer chooses server side data encryption in an AWS service, who owns the Data Encryption Key (DEK)?**

A. A third party, usually the owner of the root CA
B. AWS only
C. The customer only
D. AWS or the customer, depending on the service

# Correct Answer and Explanation

**When choosing server side encryption in AWS, the customer can choose to own the master encryption key and the DEK, or can delegate ownership of those to AWS for some services.**

A. A third party, usually the owner of the root CA
B. AWS only
C. The customer only
D. AWS or the customer, depending on the service

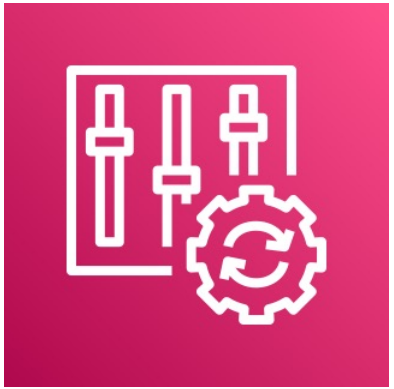
# Auditing and Reporting - CloudWatch

- Region scope
- AWS resource monitoring service
- Collect and track metrics

# Auditing and Reporting - CloudWatch Logs

- Region scope
- Fault tolerant
- Durable
- Push, not pull

# Auditing and Reporting - Config



- Region scope
- Config streams
- Capture changes and configuration
- Snapshots
- Rules

# Auditing and Reporting - CloudTrail

- Region scope
- Audit trail of AWS API actions in your account
- Log successes and failures
- Multi-region trail support
- Organization trail support

# Auditing and Reporting - CloudTrail

- Transferred to S3 for long-term storage
- Searchable history
- Insights event reporting

# Least Privilege - RBAC and ABAC

## Role-Based Access Control

- Coarse read-only access
- Group membership
- Instance profiles
- Static policies

## Access based on identity

# Least Privilege - RBAC and ABAC

## Attribute-Based Access Control

Access based on properties

- Policy conditions
- Principal tags
- Resource tags
- Dynamic policies

# Question Breakdown

# Question and Answer Choices

**Who maintains responsibility for the retention of security audit logs in AWS?**

A. AWS
B. The customer
C. Both AWS and the customer
D. Neither AWS or the customer

# Correct Answer and Explanation

**The customer is 100% responsible for enabling and retaining log features in AWS.**

A. AWS
B. The customer
C. Both AWS and the customer
D. Neither AWS or the customer

## Question Domain 2: Security and Compliance

# AWS Access Management

# Account Definition

Container for AWS resources

# Account Definition

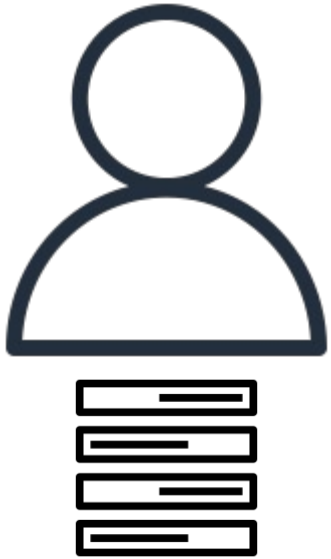
**Unit of:**

- Organization
- Billing
- Access

# Account Definition

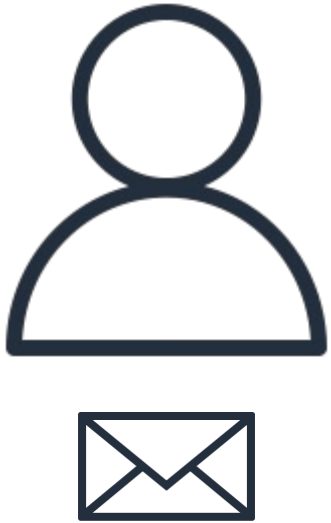
- 1 Root User
- Unique Email
- Billing Info
- Contact Info

# Root User Characteristics



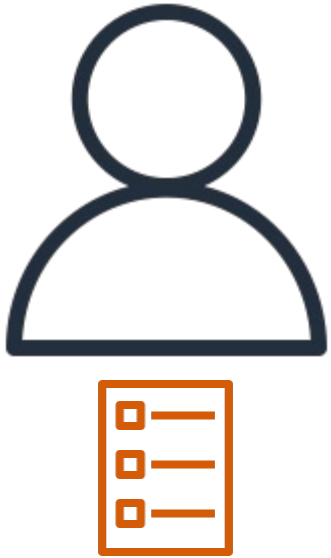
- Email address as username
- Generic login URL
- Access to unique tasks

# Root Account Email



- Use a distribution list
- Use an alias
- Root account properties can only be changed by the root user

# Root Account Unique Tasks



- Change account settings
- Change AWS support plan
- Activate access to the Billing and Cost Management Console
- View billing tax invoices
- Restore IAM User permissions for only IAM administrator
- Configure S3 bucket for MFA delete
- Edit/Delete S3 bucket policy with invalid VPC ID or VPC Endpoint ID
- Sign up for GovCloud
- ***Close the account***

# Identity and Access Management (IAM)

- Authentication
- Authorization
- Identity-based access control

# What is an IAM User?

- A principal identity
- Associated with permissions - group, inline, managed
- Associated with a permission boundary
- Container for credentials

# IAM User Credentials

- Sign-in Credentials
- Access Keys
- You must have at least one of the above to access AWS resources

# User Examples

Username: csmith
Sign-in credentials
Uses MFA
Profile: Billing Admin

Username: hsimpson
Sign-in credentials
API keys
Uses MFA
Profile: DevOps

Username: myapp1
API keys only
Profile: App runtime

# What is an IAM Group?

- Collection of IAM Users
- Associated with permissions - inline, managed
- Cannot be nested

# IAM Identity Policy Types

## Managed Policy

- Standalone resource
- Associate with 1+ IAM Users, Groups, Roles
- Versioned up to 5 revisions
- AWS- or Customer-managed

# IAM Identity Policy Types

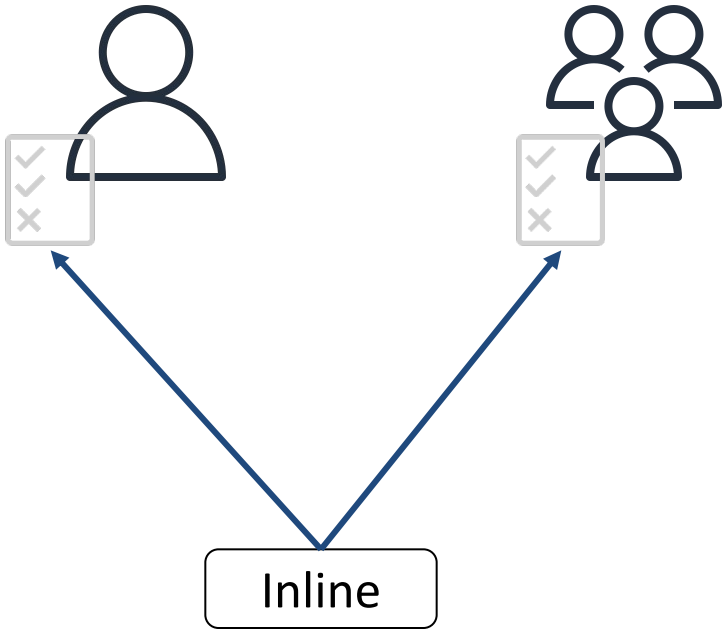
## Managed Policy

- Standalone resource
- Associate with 1+ IAM Users, Groups, Roles
- Versioned up to 5 revisions
- AWS- or Customer-managed

## Inline Policy

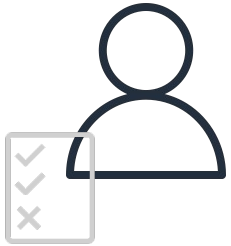
- Embedded with IAM User, Group or Role
- No versioning available

# Identity Policy Attachment




Inline policies are a parameter of the User or Group, not a separate resource

# Identity Policy Attachment

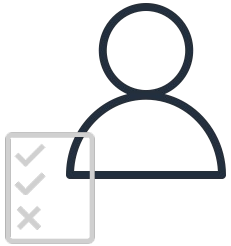


Managed policies are standalone resources

Customer-managed

AWS-managed

# Identity Policy Attachment



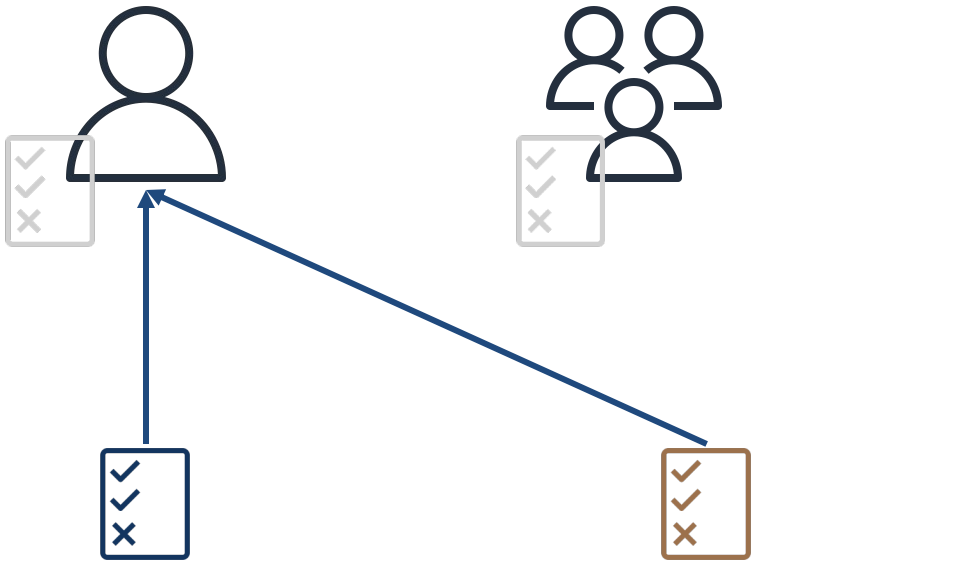
Customer-managed

AWS-managed

Customer managed policies can be edited

AWS managed policies cannot be edited

# Identity Policy Attachment

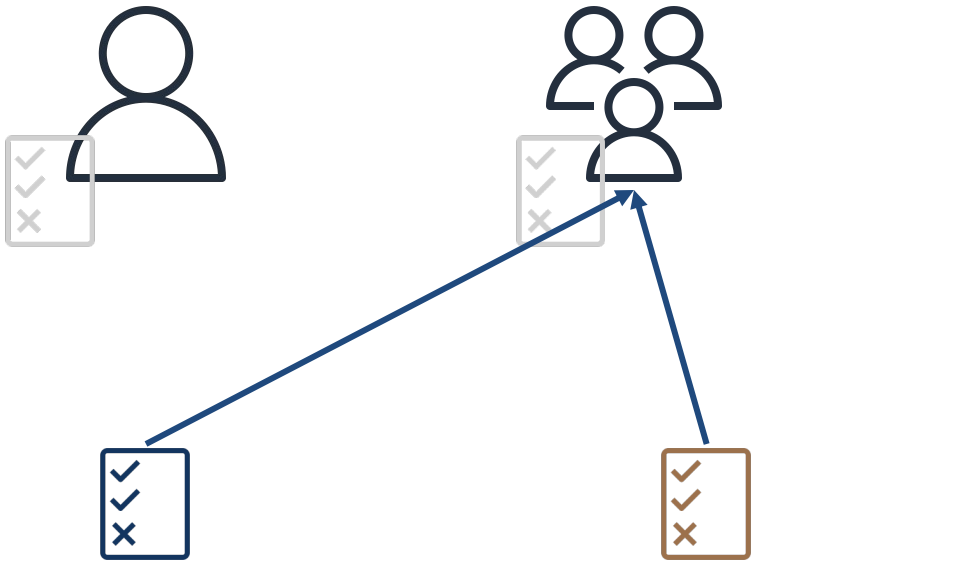


Customer-managed

AWS-managed

Both managed policy types can be associated with an IAM User

# Identity Policy Attachment

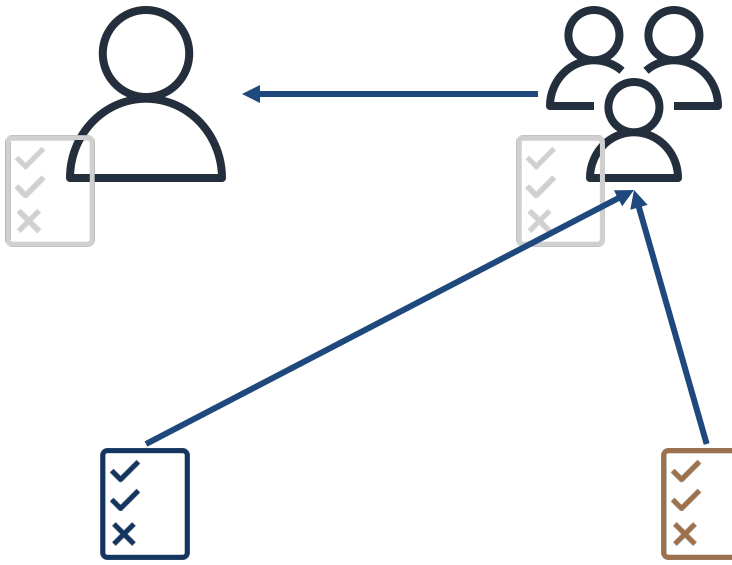


Customer-managed

AWS-managed

Both managed policy types can be associated with an IAM Group

# Identity Policy Attachment



Customer-managed

AWS-managed

Associate permissions with user through group membership

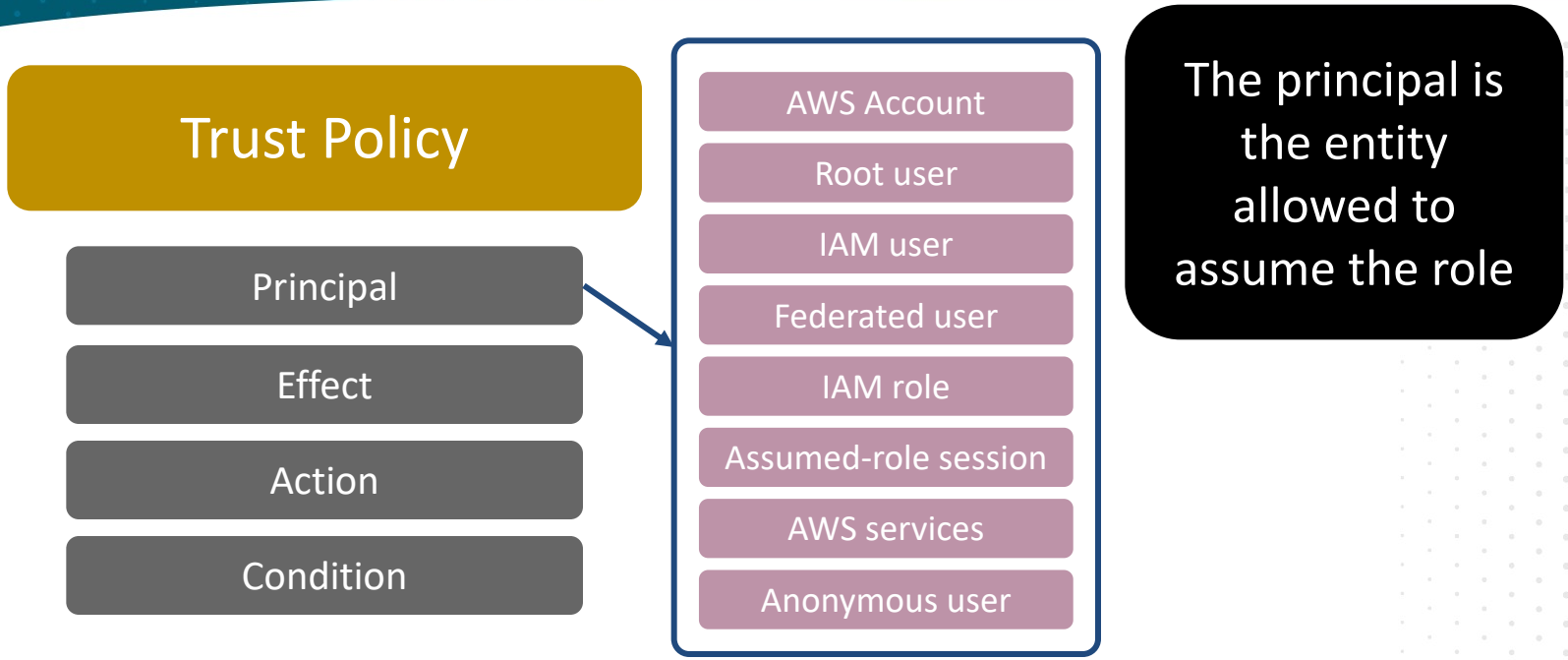
# What is a Session Policy?

- Parameter passed during creation of temporary session
- Use with IAM Role
- Use with federated users

# What is an IAM Role?

- IAM Identity
- Associated with permissions - inline, managed
- Assumed by other principals

# Role Trust Policy



# Amazon Resource Name (ARN)

Globally Unique Identifier

arn:

# Amazon Resource Name (ARN)

Globally Unique Identifier

arn:partition

- aws
- aws-cn
- aws-us-gov

# Amazon Resource Name (ARN)

Globally Unique Identifier

arn:partition:service

ec2
s3
iam

# Amazon Resource Name (ARN)

Globally Unique Identifier

arn:partition:service:region

us-east-1
eu-west-1
ap-south-1

# Amazon Resource Name (ARN)

Globally Unique Identifier

arn:partition:service:region:account-id

0123456789012

# Amazon Resource Name (ARN)

Globally Unique Identifier

arn:partition:service:region:account-id:resource-id

User/Chad
instance/i-XXXXXX
volume/vol-XXXXX

# Question Breakdown

# Question and Answer Choices

**Which AWS IAM resource would be used for granting temporary permissions for cross-account access?**

A. IAM User
B. IAM Group
C. IAM Role
D. IAM Policy

# Correct Answer and Explanation

**IAM Roles can be used with session policies to grant temporary access to AWS resources, and are good candidates for cross-account permissions.**

A. IAM User
B. IAM Group
C. IAM Role
D. IAM Policy

## Question Domain 2: Security and Compliance

# Security Support Resources

# VPC Network Security Options

- Private network
- Network ACL
- Security Group
- NAT Gateway
- Third party Marketplace options

# Other Network Security Options

- DNS Firewall
- Firewall manager
- WAF
- GuardDuty

# Security Documentation Resources

- Knowledge Center
- Security Center
- Whitepapers
- Security blog

# Trusted Advisor Checks

- Online tool, not a service
- Cost optimization checks
- Security checks
- Fault tolerance checks
- Performance checks
- Service limit checks

# Question Breakdown

# Question and Answer Choices

**Which VPC security feature acts as a stateful firewall for network interfaces?**

A. Network ACL
B. Security Group
C. Firewall Manager
D. AWS Network Firewall

# Correct Answer and Explanation

**Security groups are stateful firewall resources attached to network interfaces in a VPC, supporting both inbound and outbound rules.**

A. Network ACL
B. Security Group
C. Firewall Manager
D. AWS Network Firewall

# Question Domain 3: Technology

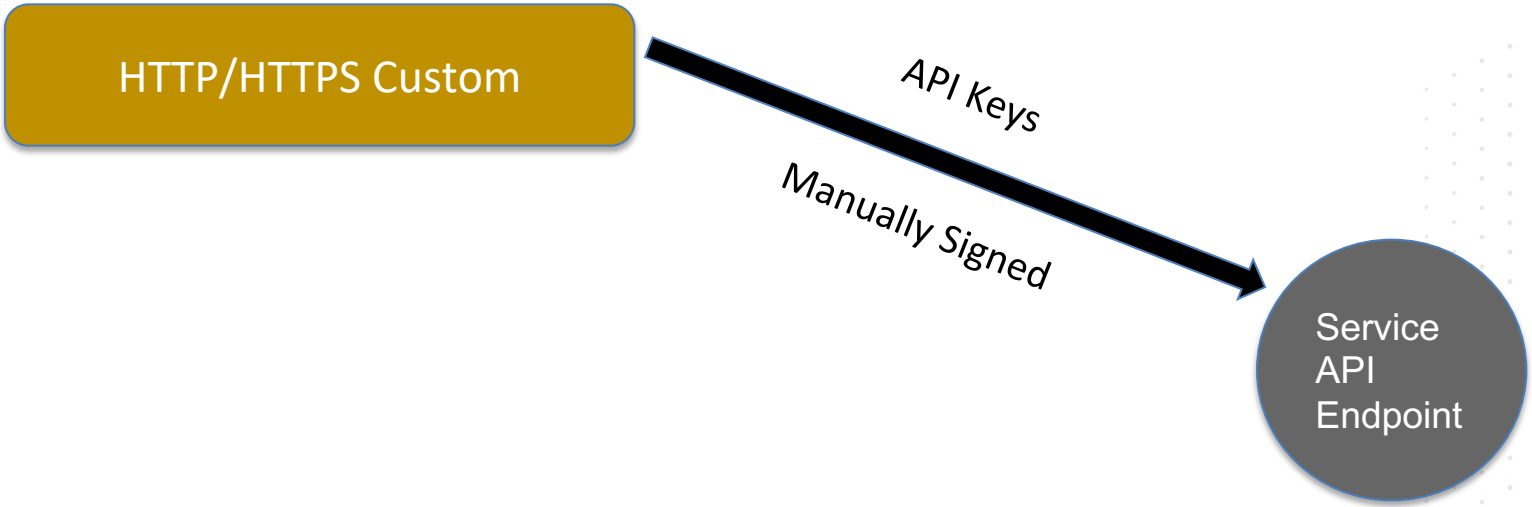
# Question Domain Points

- Define methods of deploying and operating in the AWS Cloud
- Define the AWS global infrastructure
- Identify the core AWS services
- Identify resources for technology support

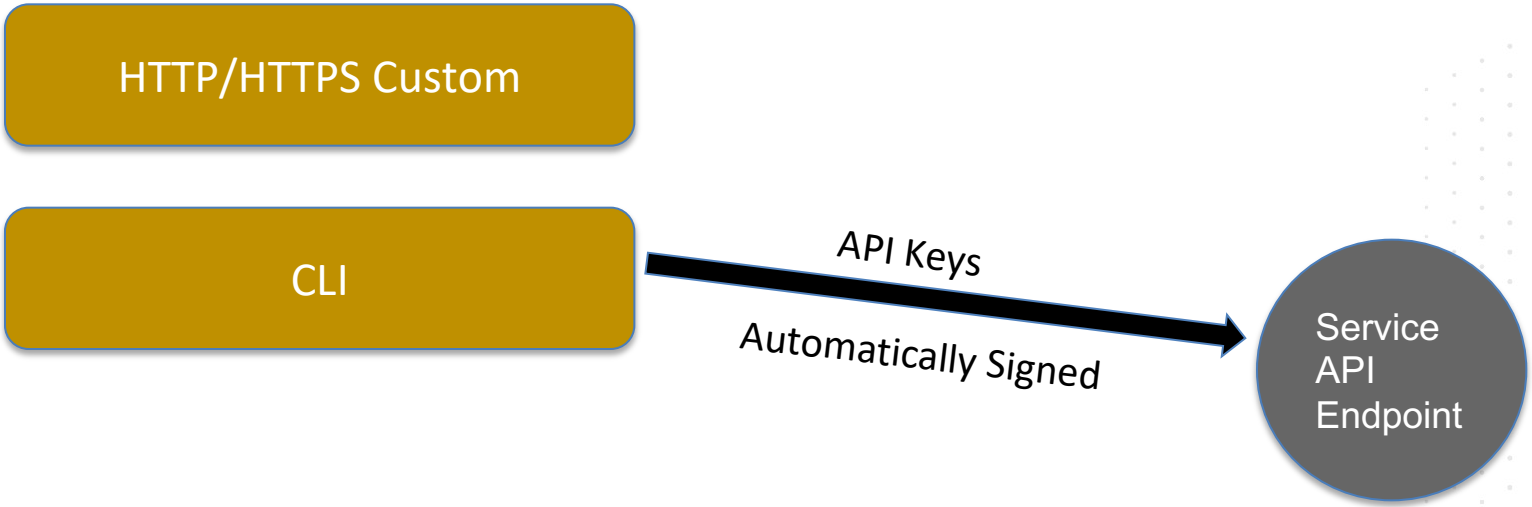
## Question Domain 3: Technology

# AWS Deployments and Operations

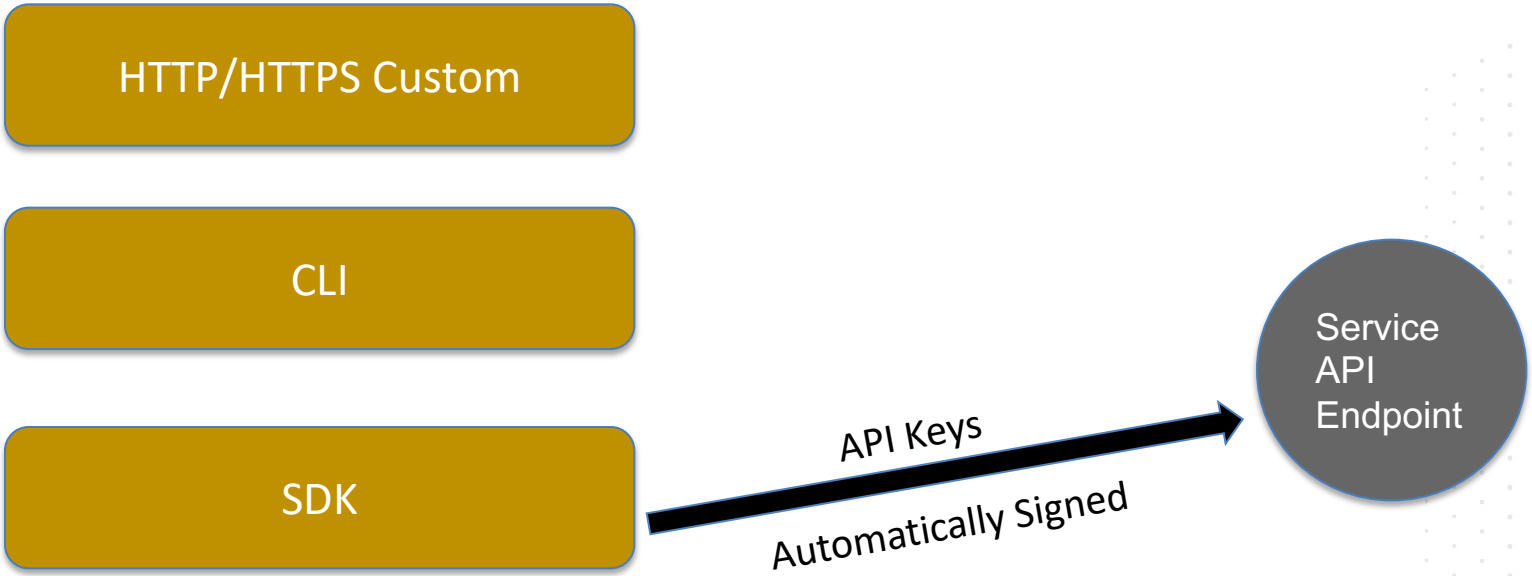
# How To Access AWS - Direct Credentials



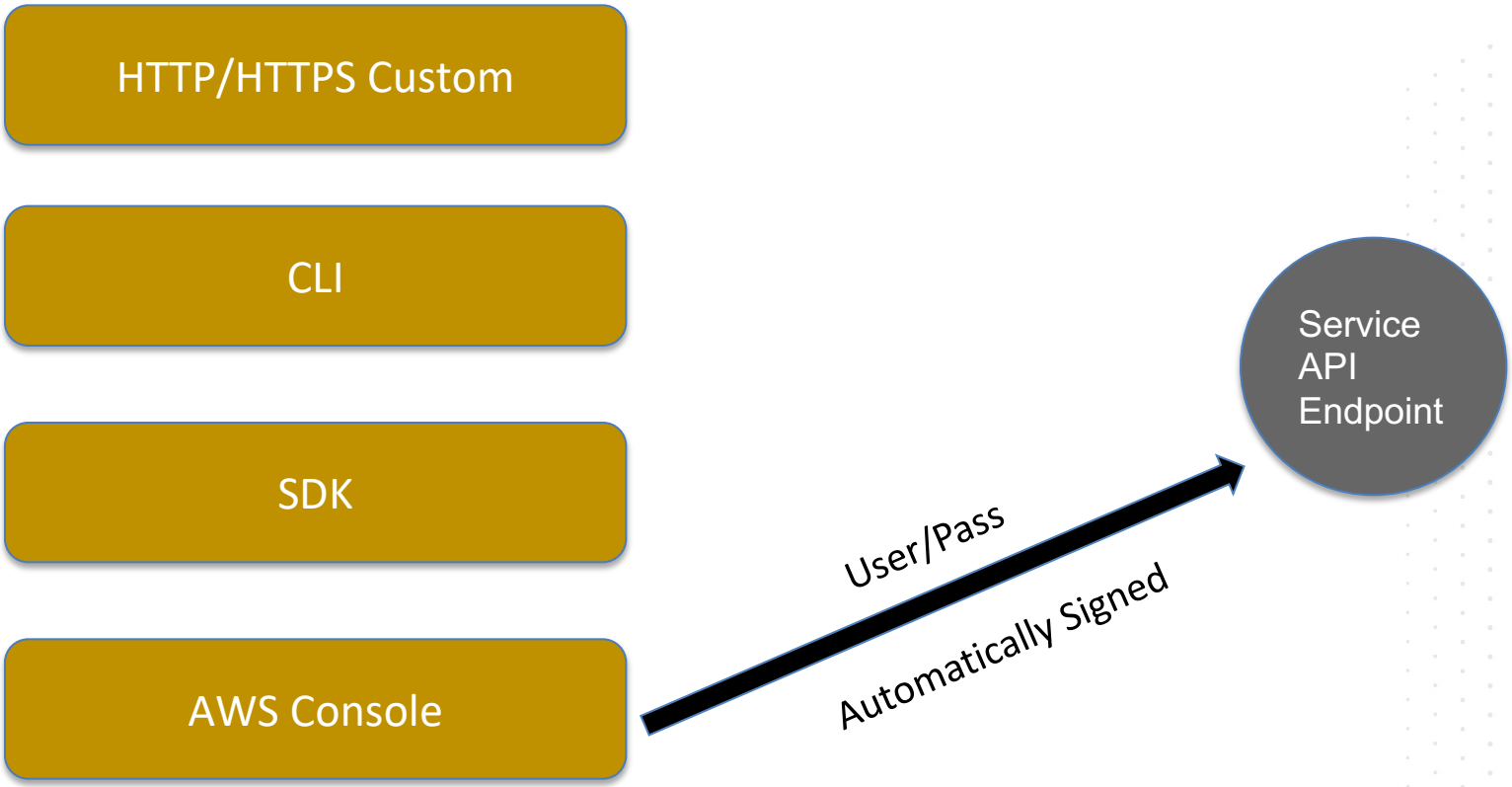
# How To Access AWS - Direct Credentials



# How To Access AWS - Direct Credentials



# How To Access AWS - Direct Credentials



# Infrastructure As Code (IAC)

- Use SDLC best practices for infrastructure
- CloudFormation
- OpsWorks
- Third-party tools

# Question Breakdown

# Question and Answer Choices

**When planning for programmatic interaction with AWS services, which method would ensure access to the complete suite of actions?**

A. HTTP/HTTPS
B. AWS Command Line Interface
C. AWS Software Development Kits (SDKs)
D. AWS Console

# Correct Answer and Explanation

**Accessing the service API endpoints directly using clients such as curl or postman is the only way to utilize all API actions, as each of the other methods have some missing functions.**

A. **HTTP/HTTPS**
B. **AWS Command Line Interface**
C. **AWS Software Development Kits (SDKs)**
D. **AWS Console**

# Cloud Deployment Models

## Cloud Native


- All infrastructure in the cloud
- All applications in the cloud
  - Created new
  - Migrated from on-premises

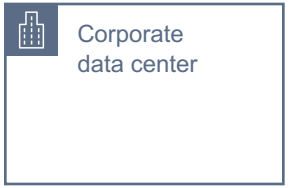
# Cloud Deployment Models

## Hybrid Cloud


- Cloud-native resources
- On-premises resources
- Connect cloud resources to internal systems

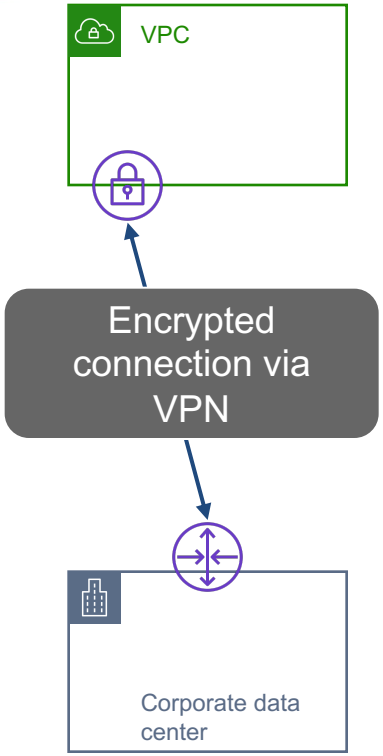
# Cloud Deployment Models

## On-premises

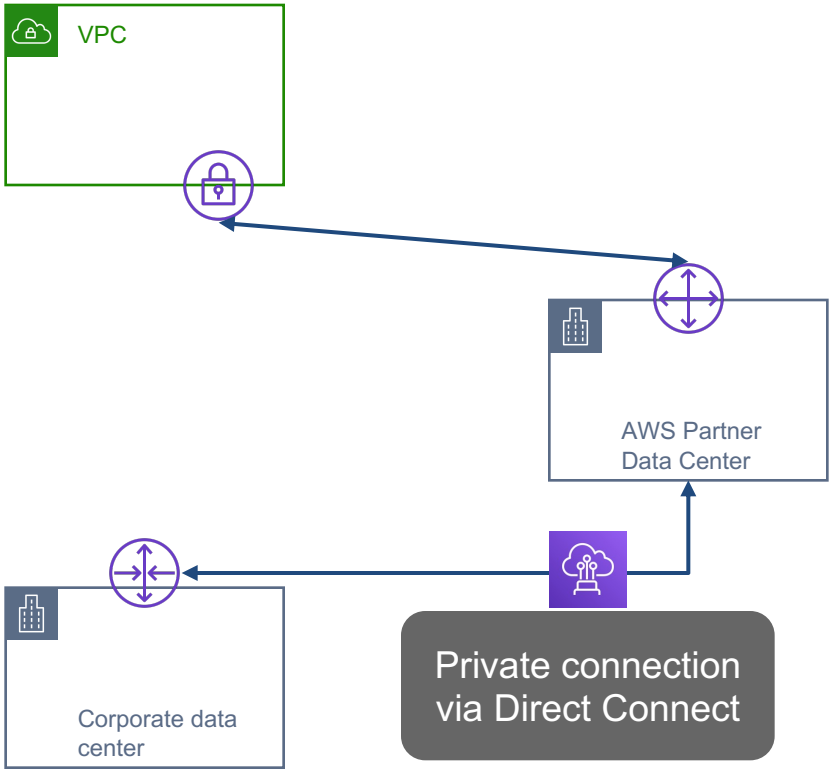



- All infrastructure external to the cloud
- All applications external to the cloud
- Bare metal hardware
- Private cloud infrastructure

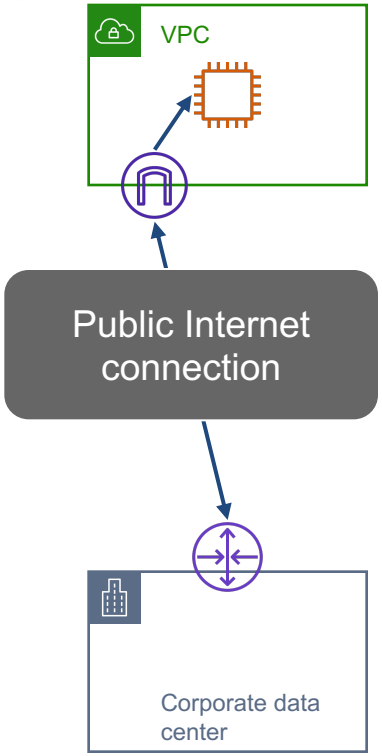
# Hybrid Connectivity Options



# Hybrid Connectivity Options



# Hybrid Connectivity Options



# Question Breakdown

# Question and Answer Choices

**When planning for programmatic interaction with AWS services, which method would ensure access to the complete suite of actions?**

A. HTTP/HTTPS
B. AWS Command Line Interface
C. AWS Software Development Kits (SDKs)
D. AWS Console

# Correct Answer and Explanation

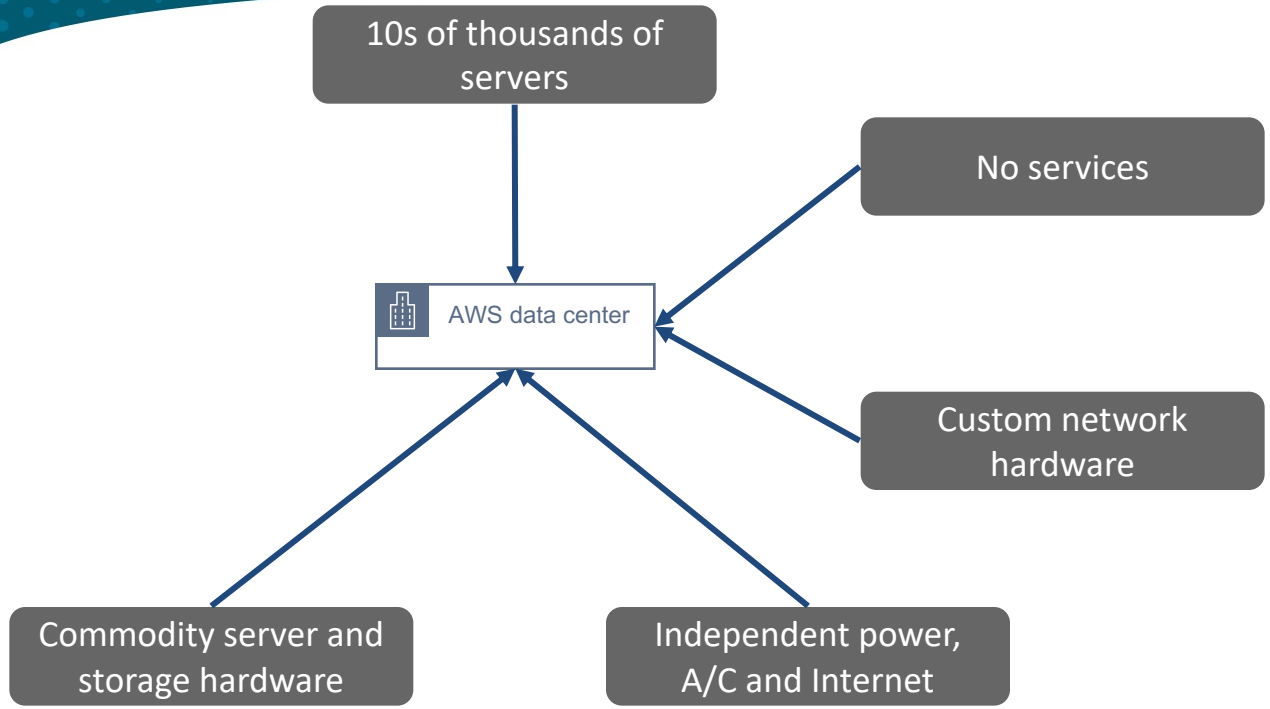
**Accessing the service API endpoints directly using clients such as curl or postman is the only way to utilize all API actions, as each of the other methods have some missing functions.**

A. **HTTP/HTTPS**
B. **AWS Command Line Interface**
C. **AWS Software Development Kits (SDKs)**
D. **AWS Console**

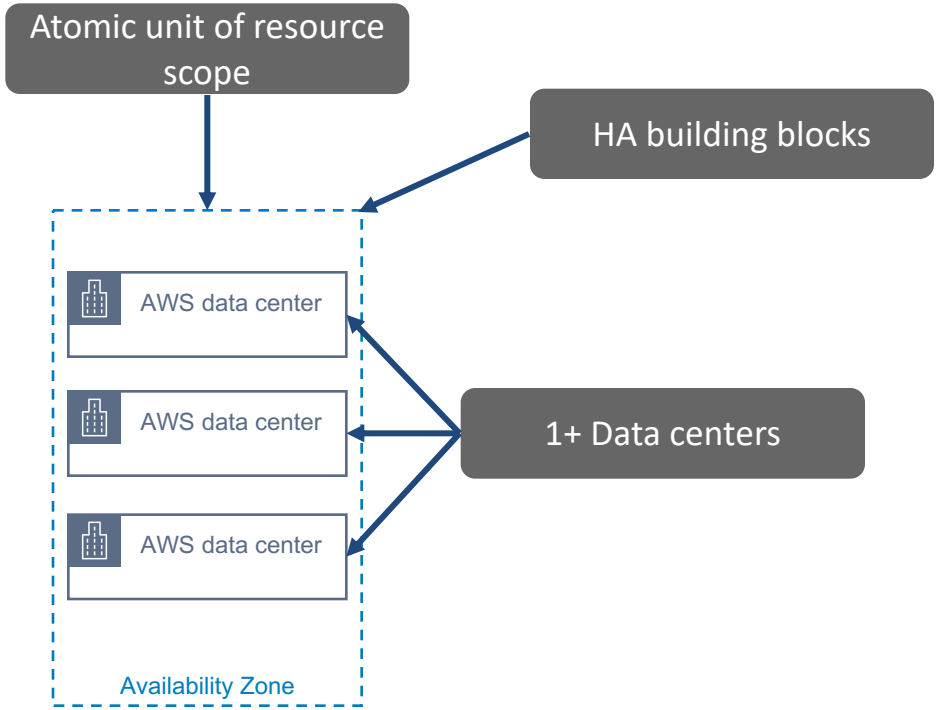
## Question Domain 3: Technology

# AWS Global Infrastructure

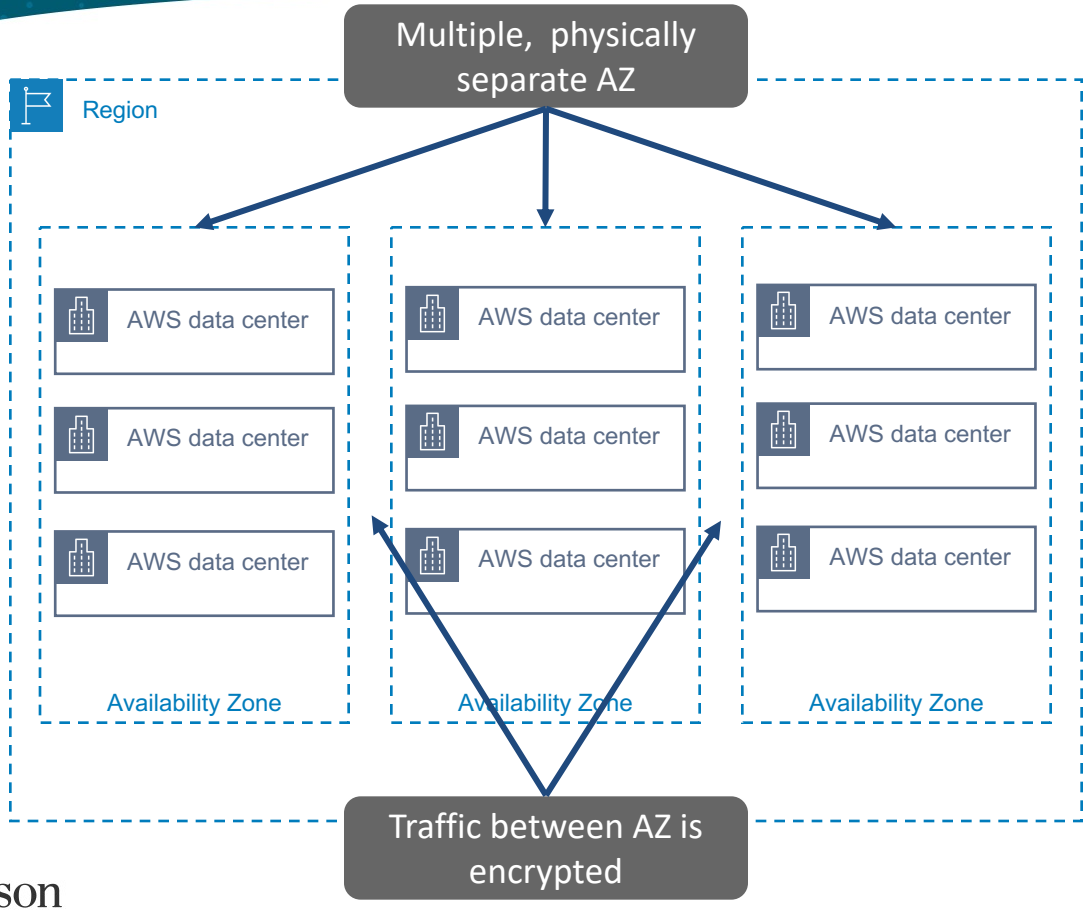
# AWS Data Center



# AWS Availability Zone



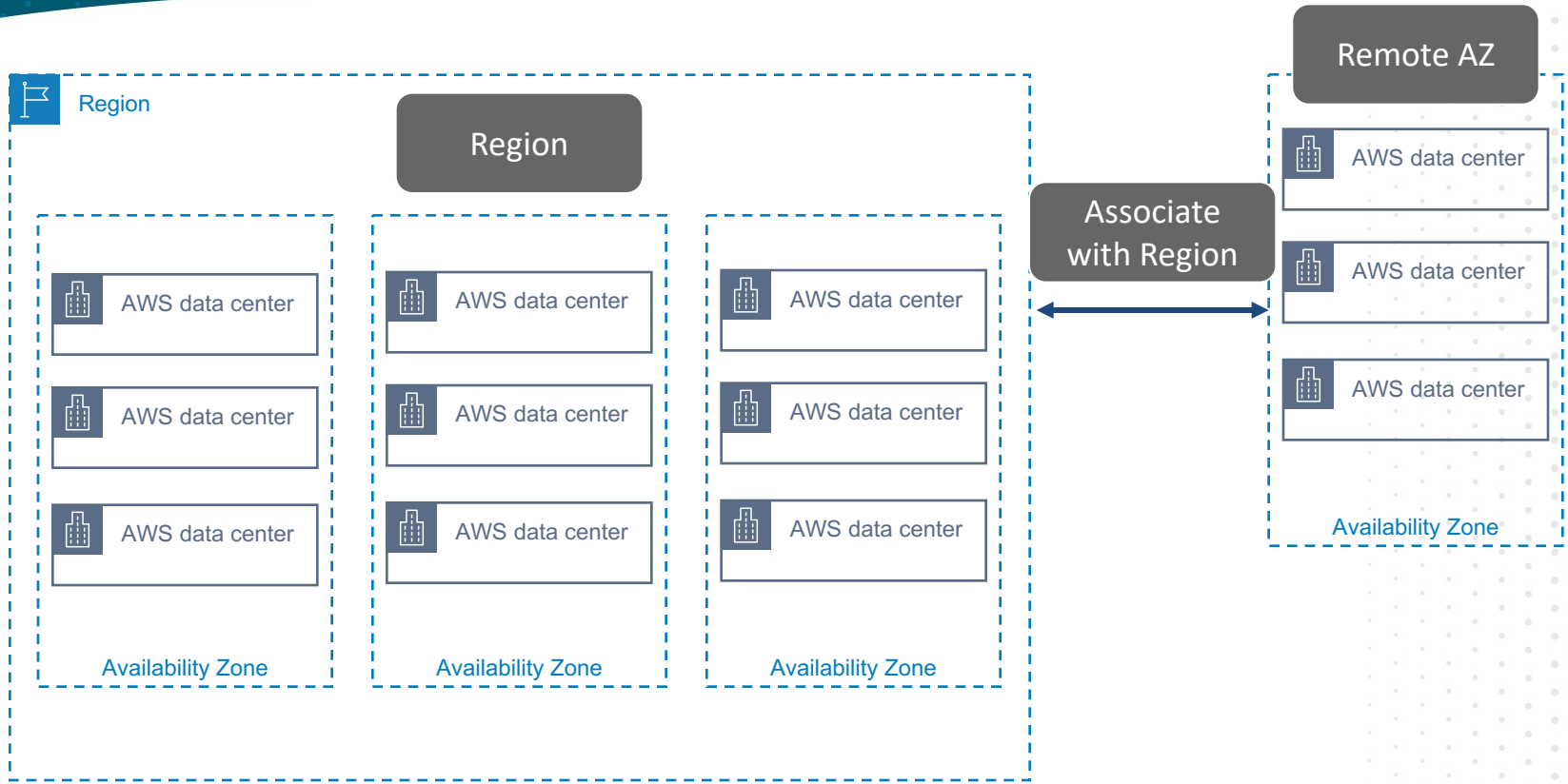
# AWS Region



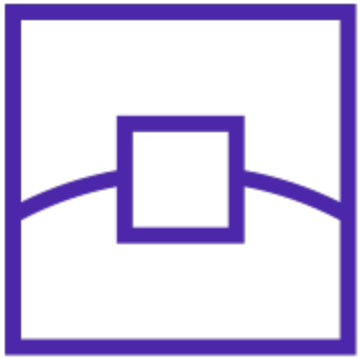

Service API Endpoints hosted here

Common unit of resource scope

# AWS Local Zone



# Single Edge Location



- Separate infrastructure from regions
- Connected to Region networks
- Scope for Global services
- Used for caching

# Global Edge Location Presence


Pearson

# Region Selection Criteria


Service availability

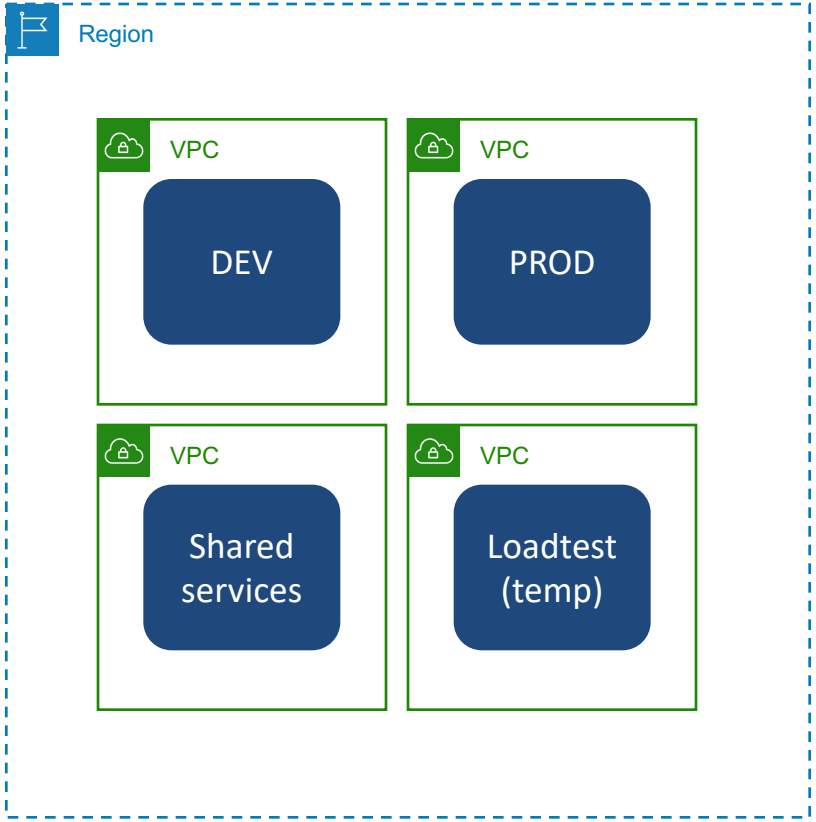
Co-locate with users

Co-locate with infra

Data residency

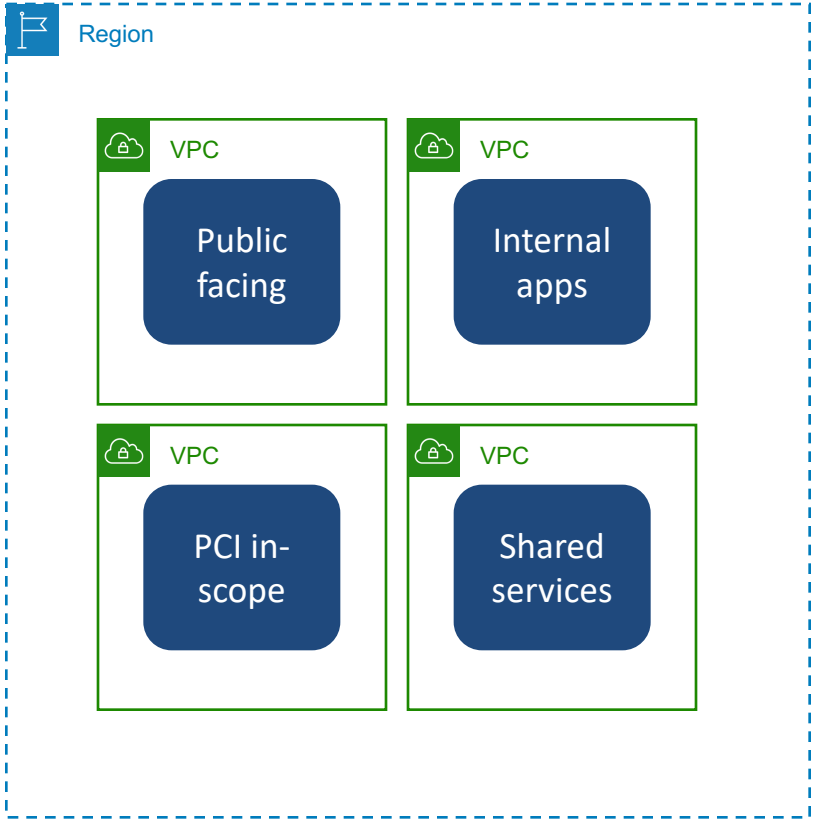
Multi-region DR

# VPC Workload Isolation Strategies



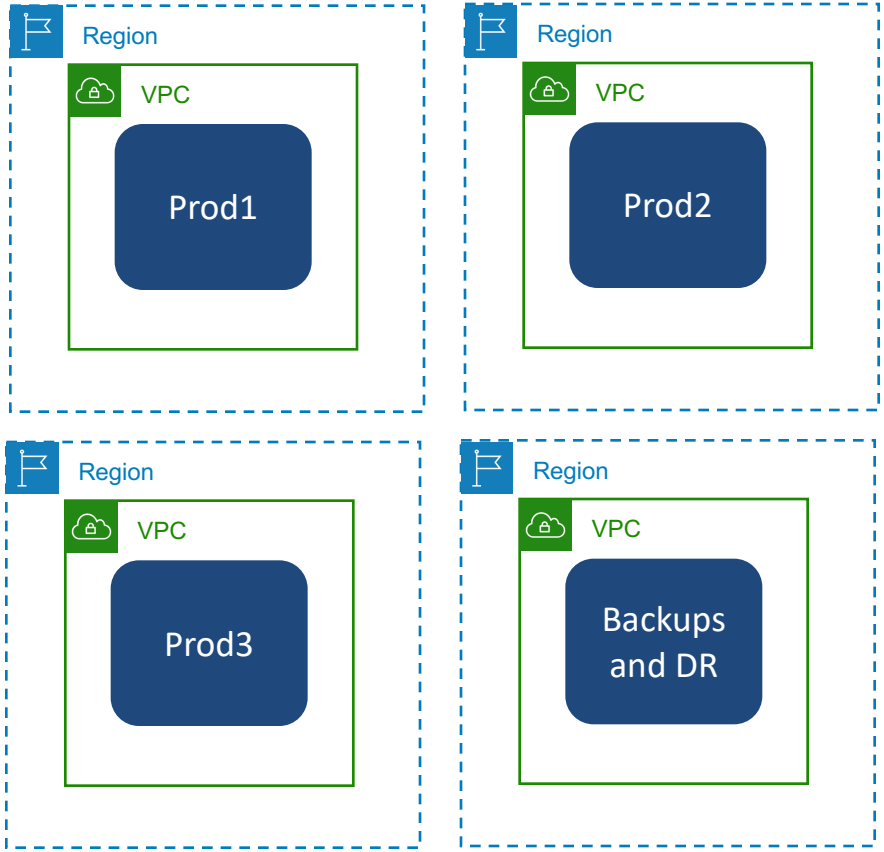

Organize by environment

# VPC Workload Isolation Strategies



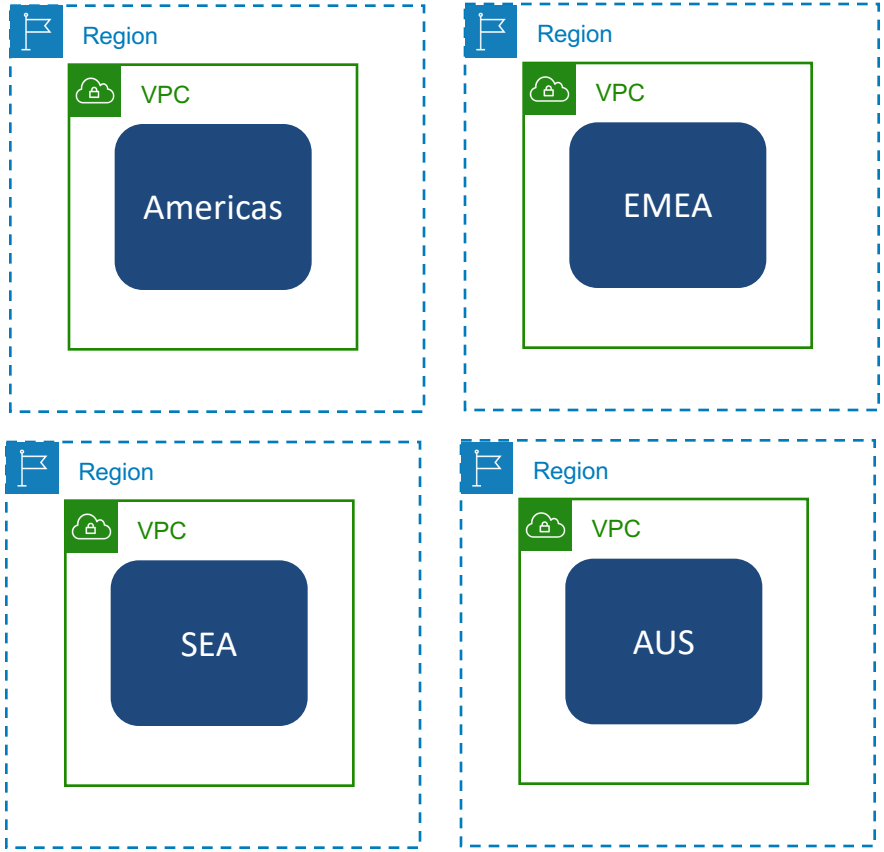

Organize by workload compliance

# VPC Workload Isolation Strategies



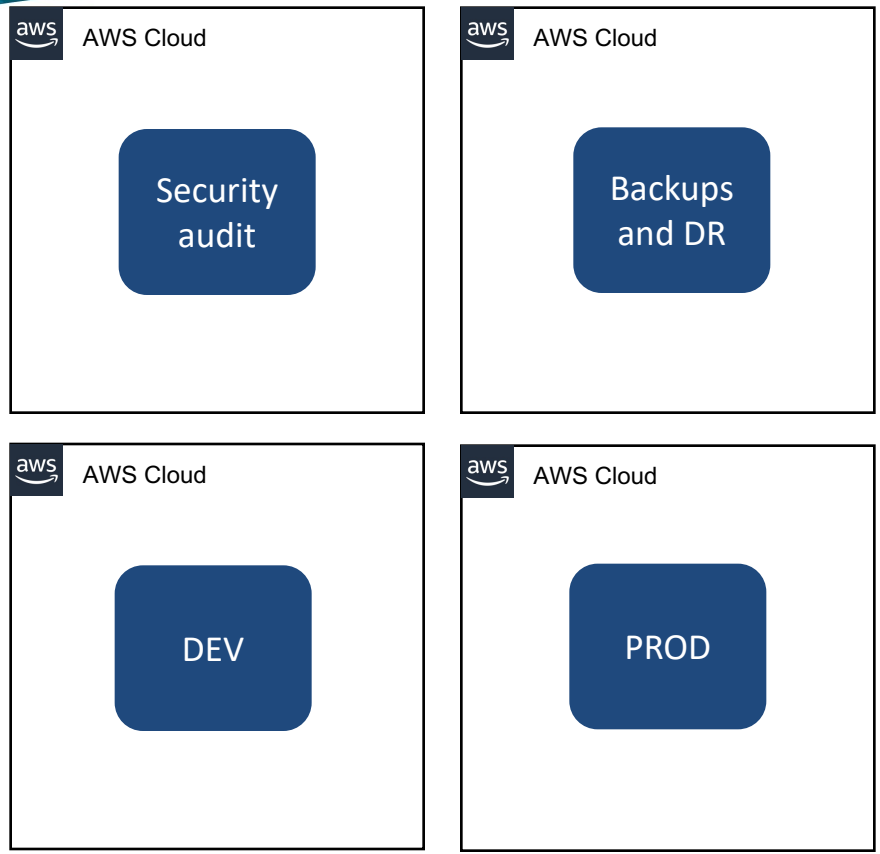

Organize by business continuity

# VPC Workload Isolation Strategies



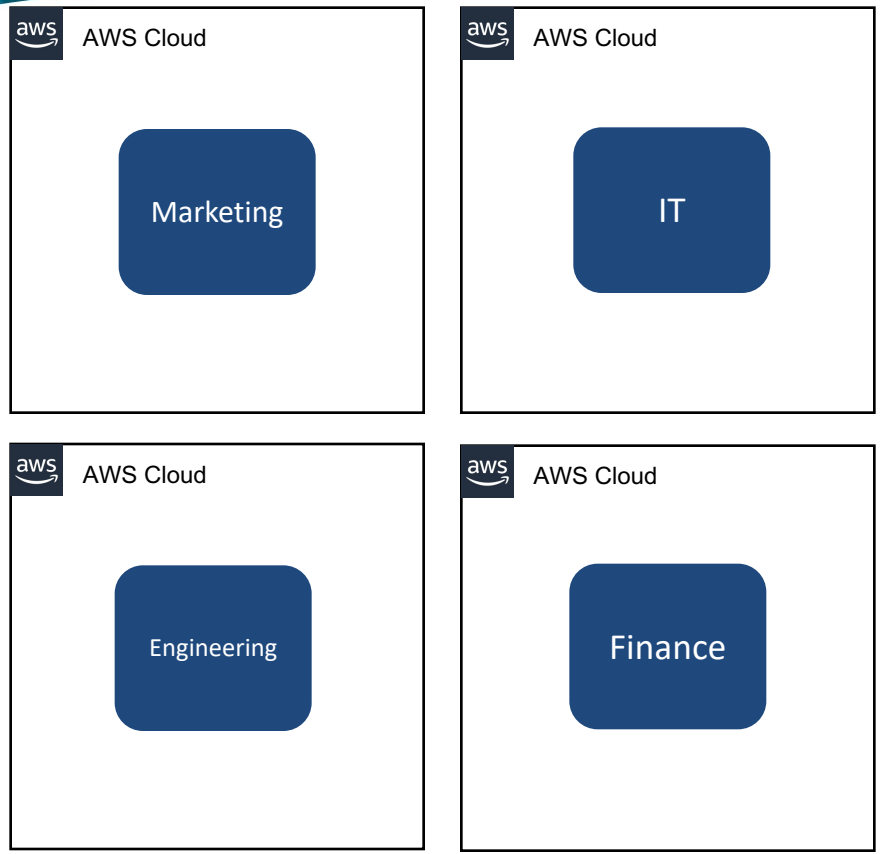

Organize by data sovereignty

# Workload Isolation Strategies




Organize by security requirements

# Workload Isolation Strategies




Organize to match company hierarchy

# Question Breakdown

# Question and Answer Choices

**Which of these is a reason to isolate workloads into separate AWS regions?**

A. Decreased latency
B. Data sovereignty compliance
C. Business Continuity (DR)
D. All of these

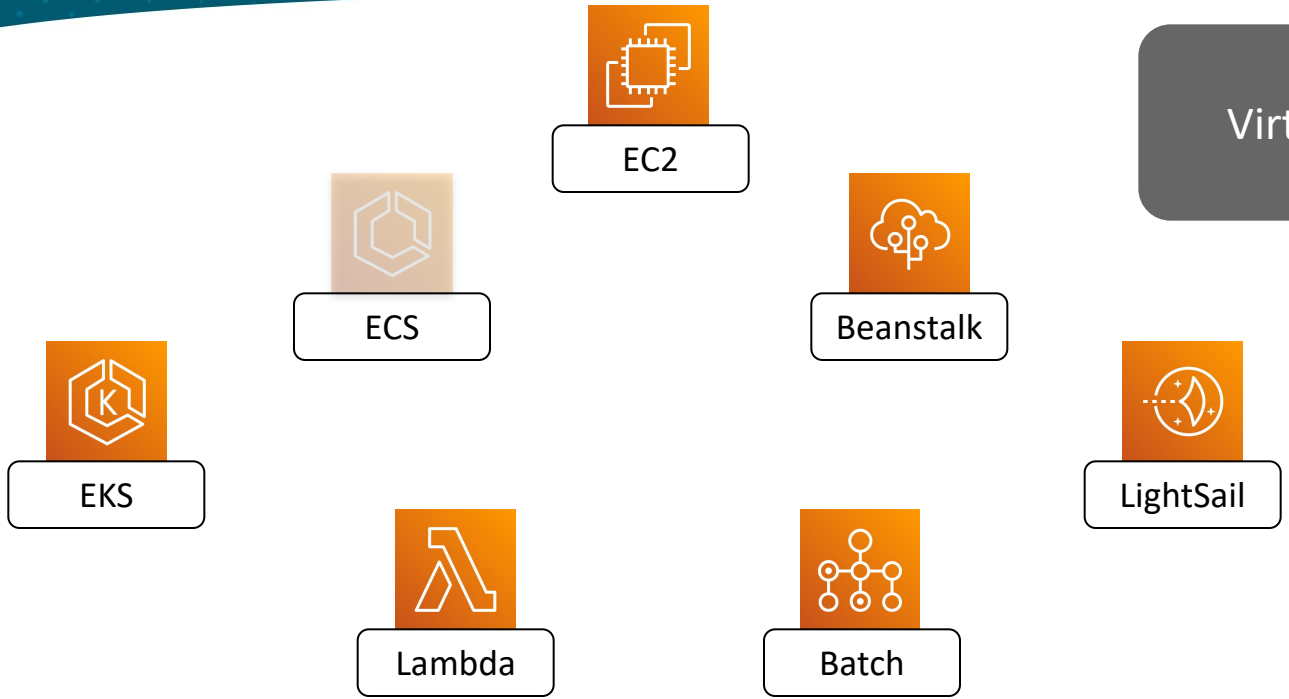
# Correct Answer and Explanation

**There are many valid reasons for separating workloads into accounts or regions, and all of these are legitimate.**

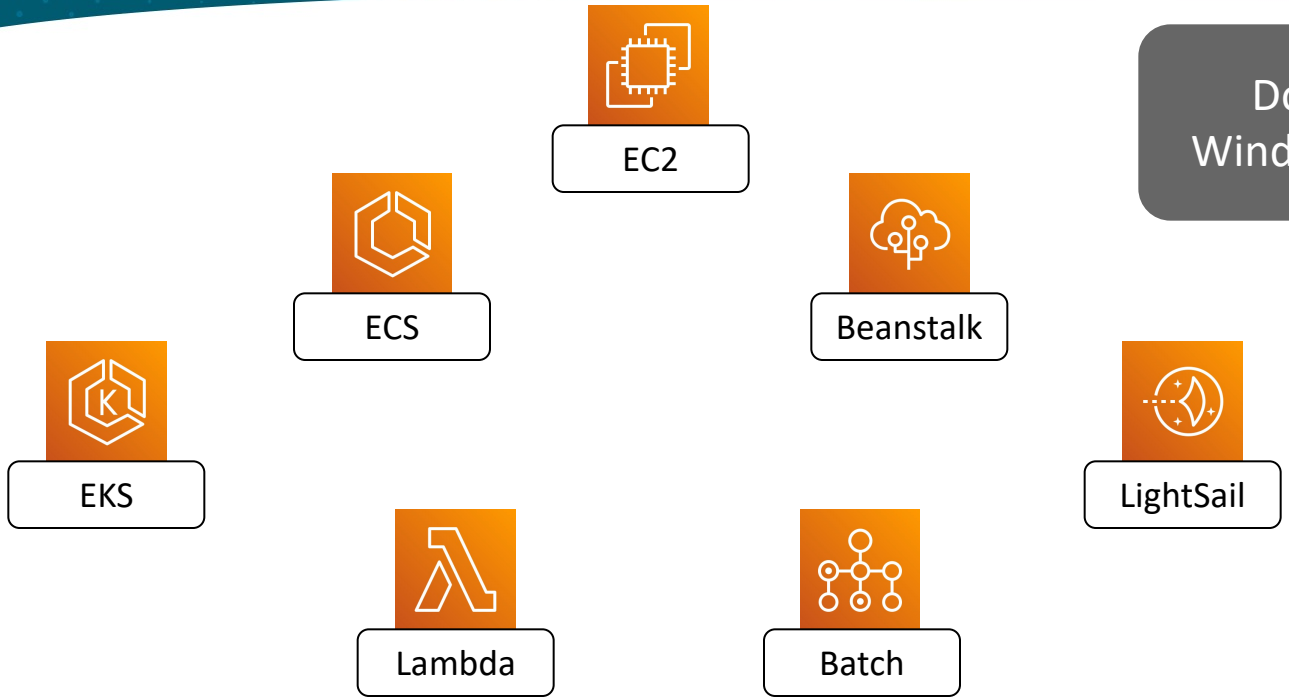
A. Decreased latency
B. Data sovereignty compliance
C. Business Continuity (DR)
D. All of these

# Core AWS Services

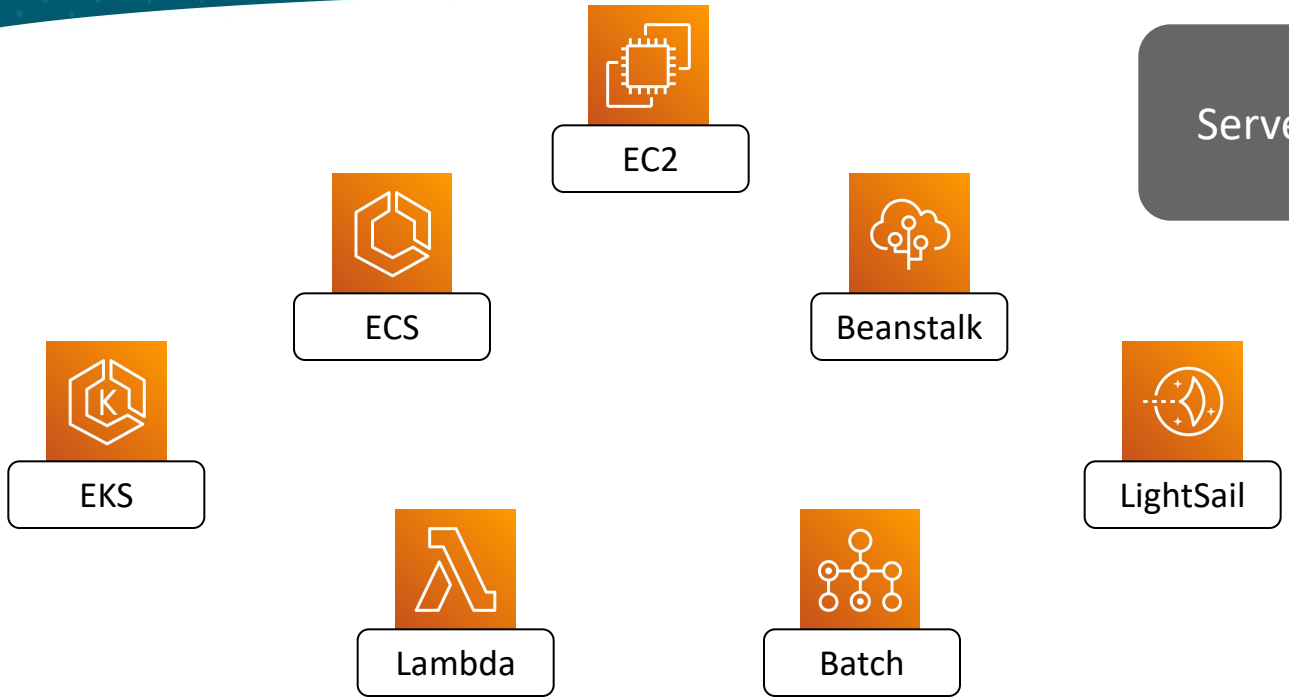
# AWS Compute Services



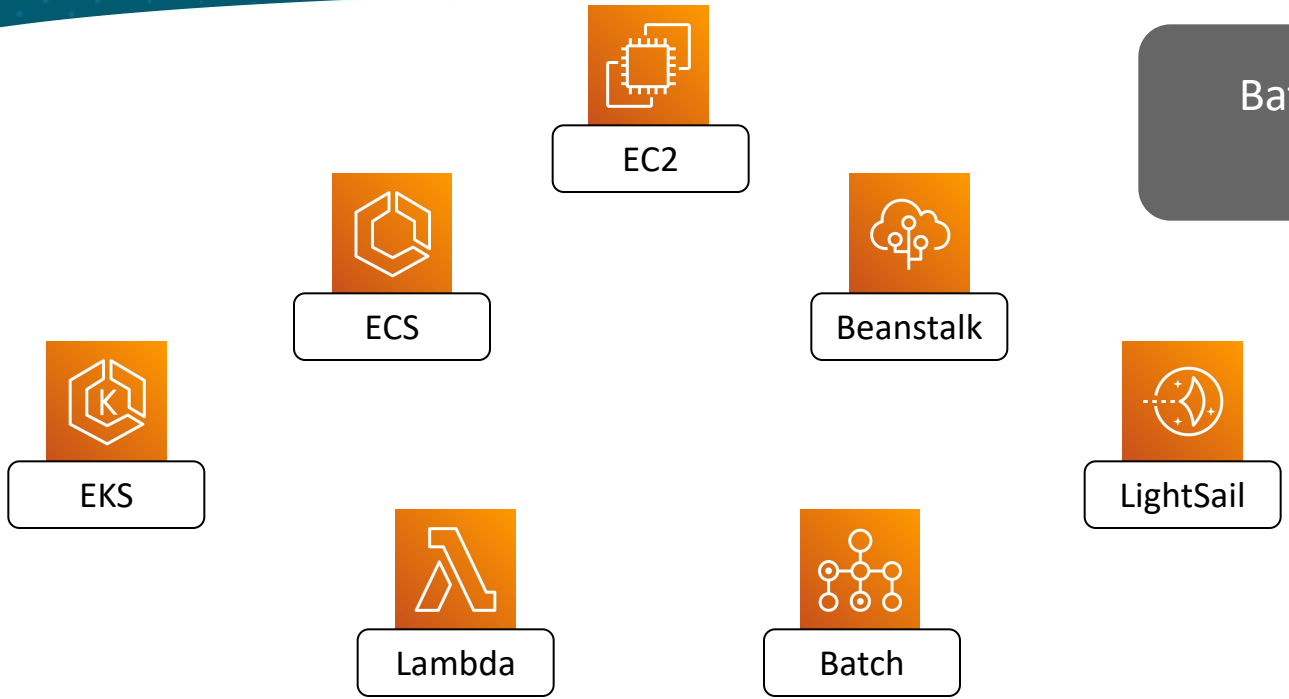
# AWS Compute Services



# AWS Compute Services

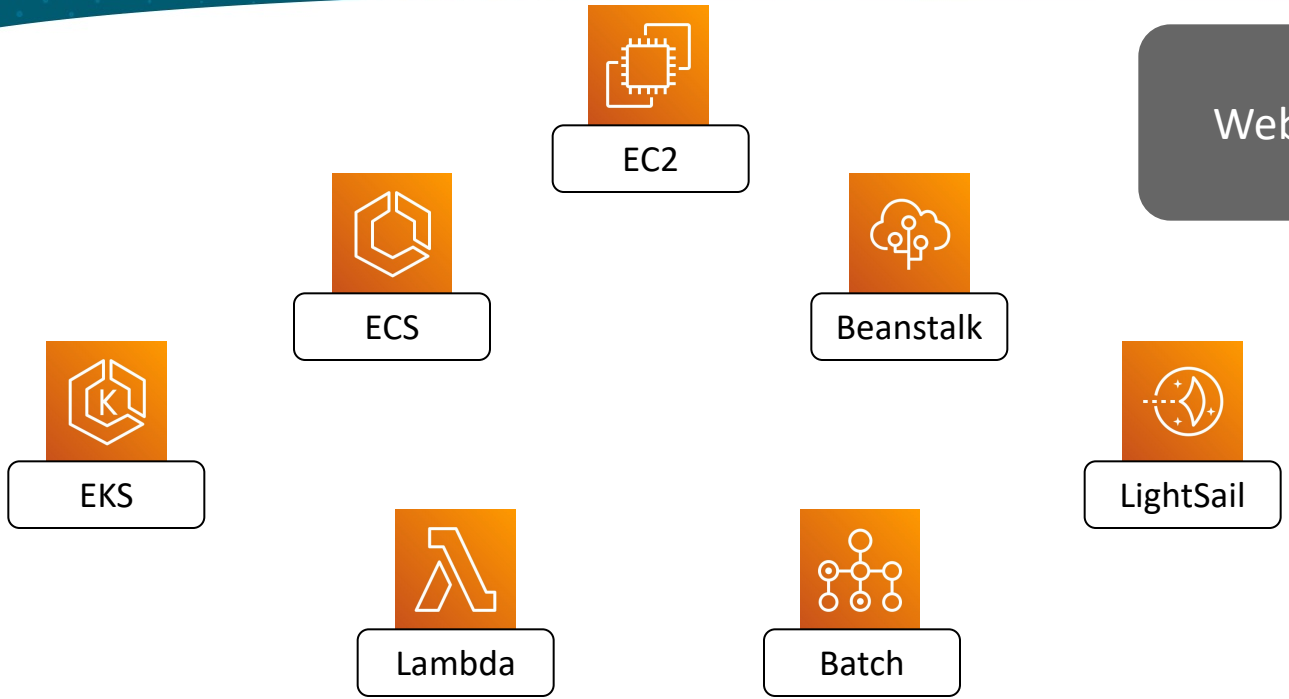


# AWS Compute Services

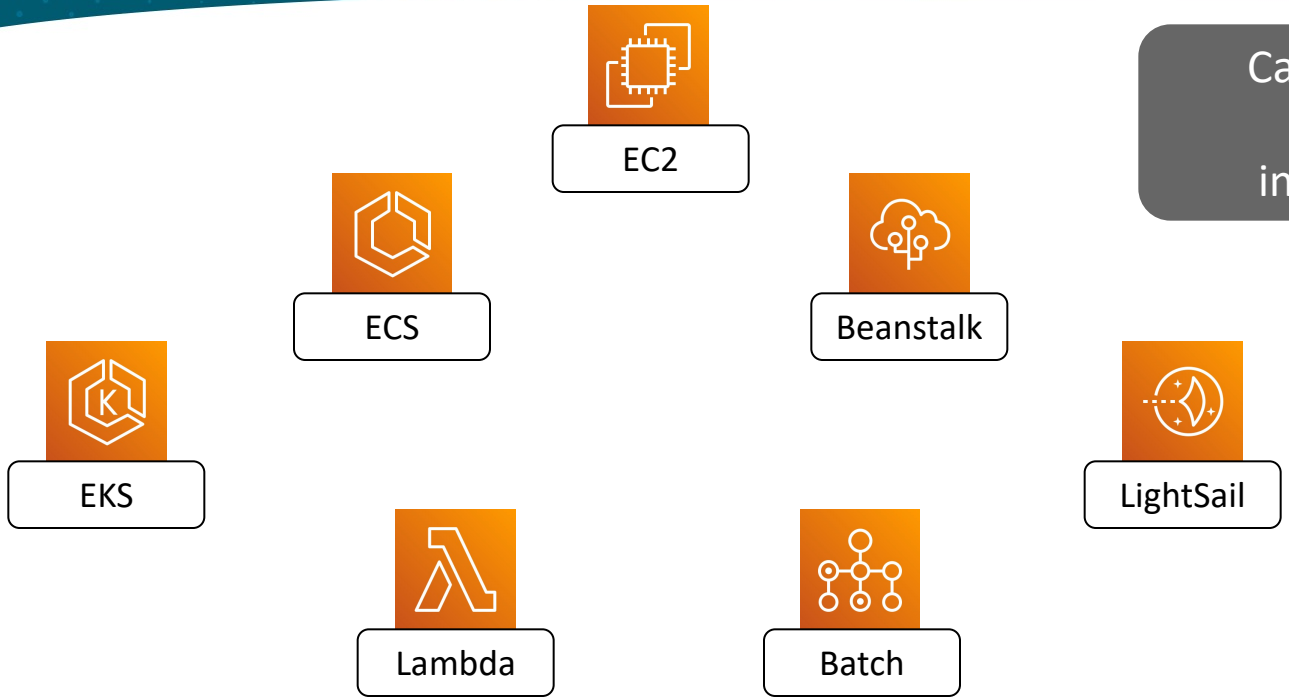



Batch container processes

# AWS Compute Services

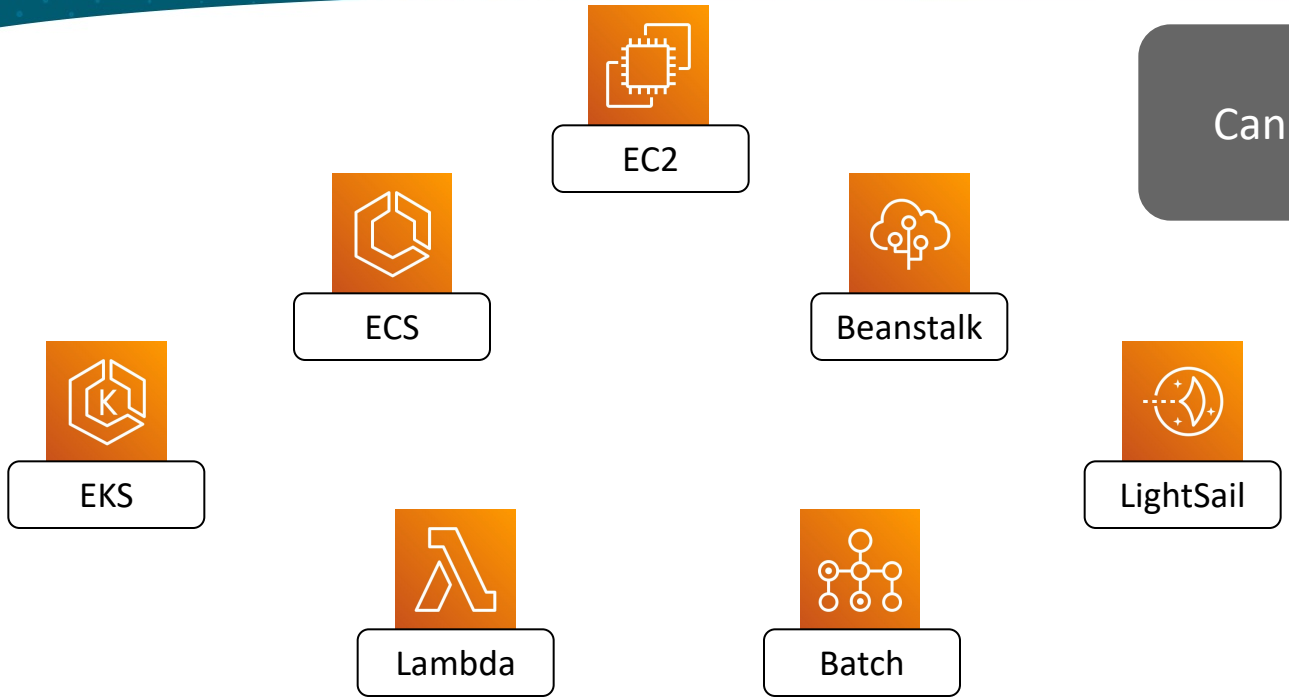


# AWS Compute Services



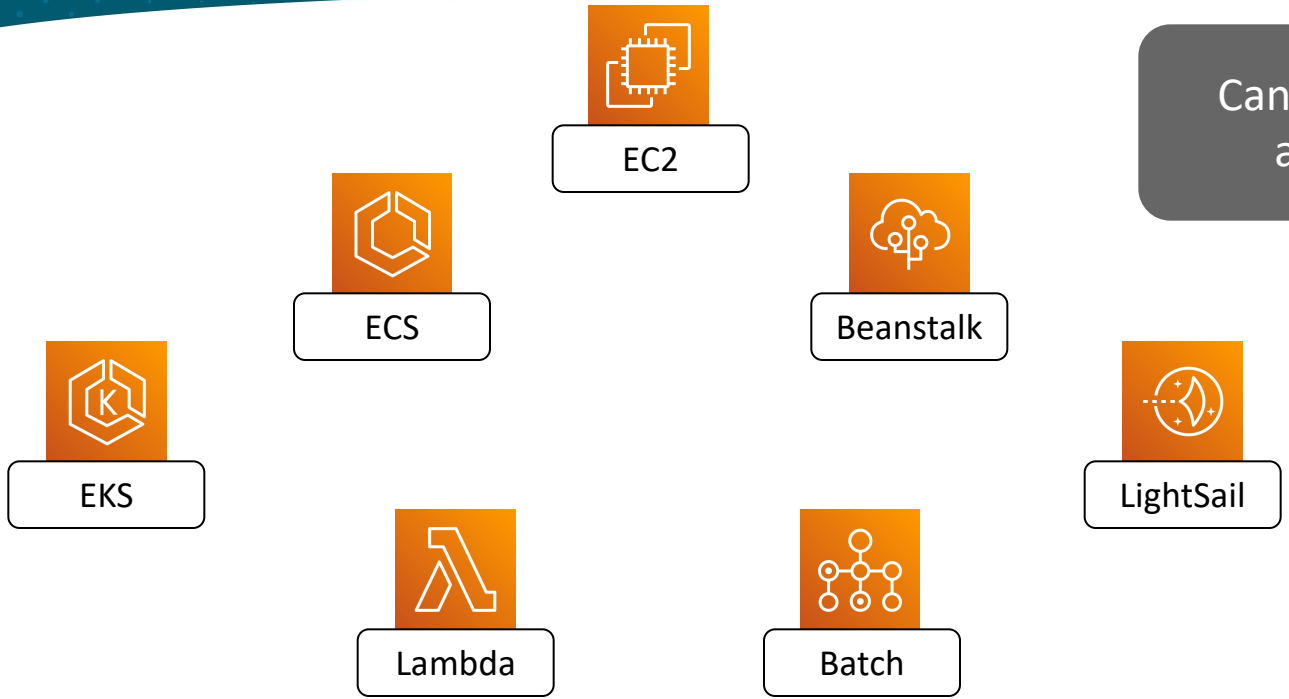

Can use EC2 as underlying infrastructure

# AWS Compute Services



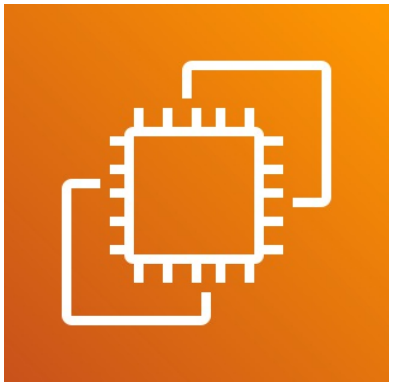

Can run serverless

# AWS Compute Services



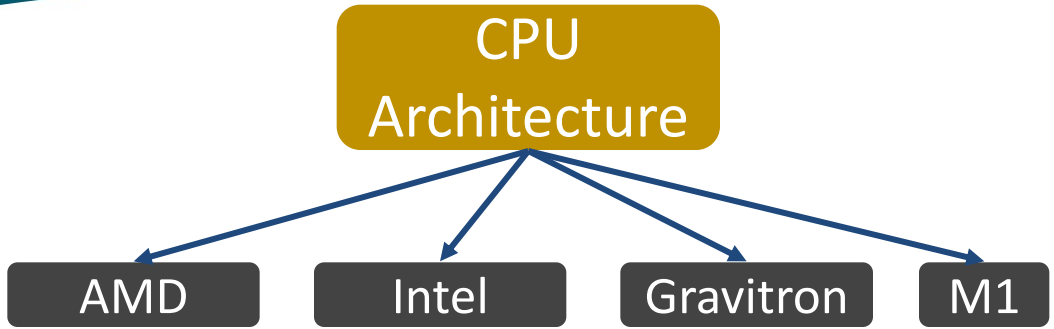

Can run container applications

# EC2 Basics



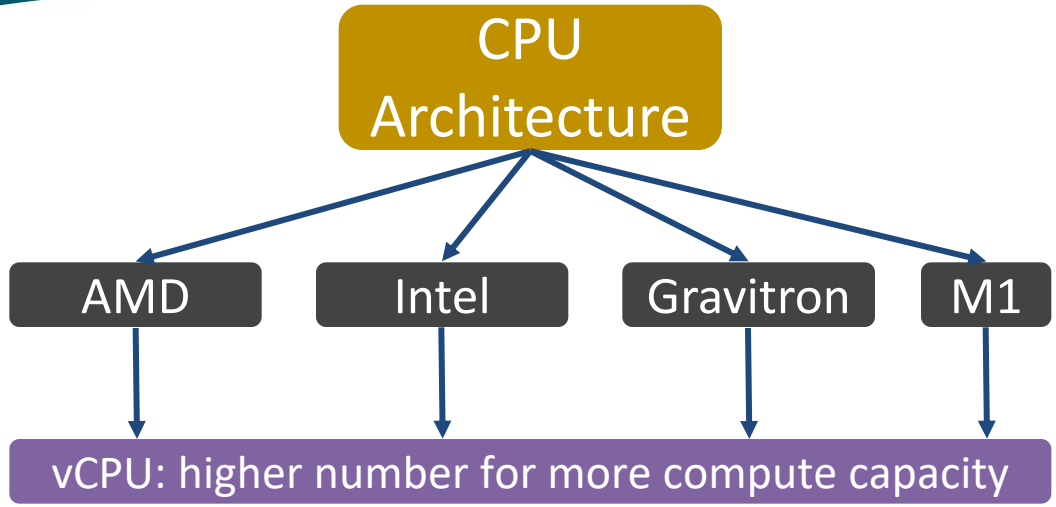
- AZ scope
- Virtual machines
- Flexible resources
- Flexible OS

# EC2 Resources - Processor & Memory



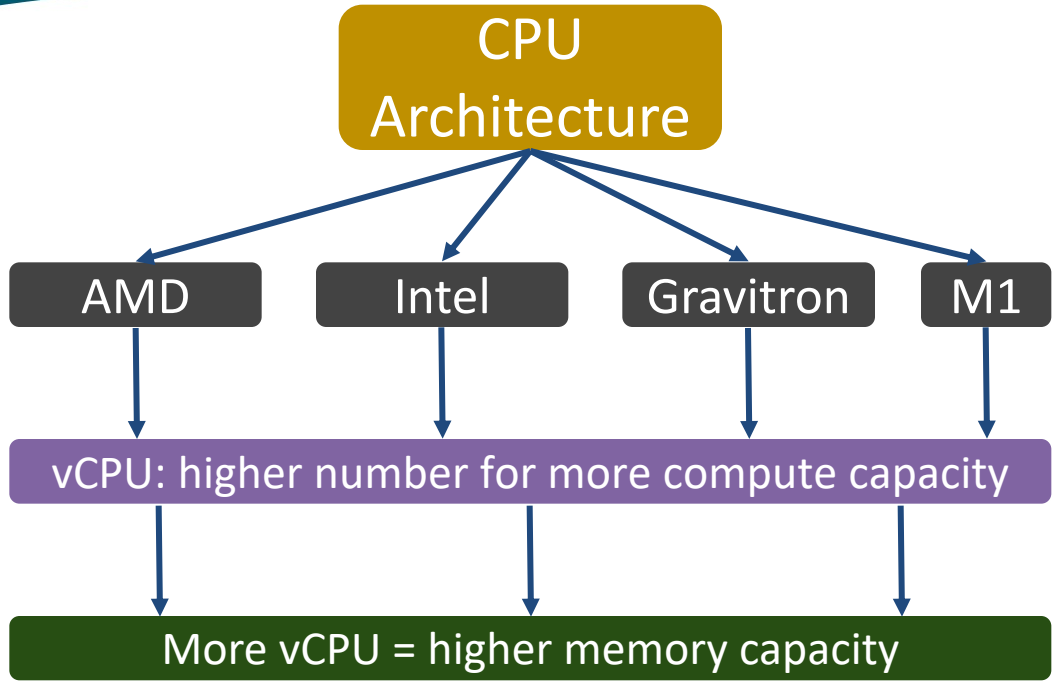

Flexible choices of processor architecture and generation

# EC2 Resources - Processor & Memory



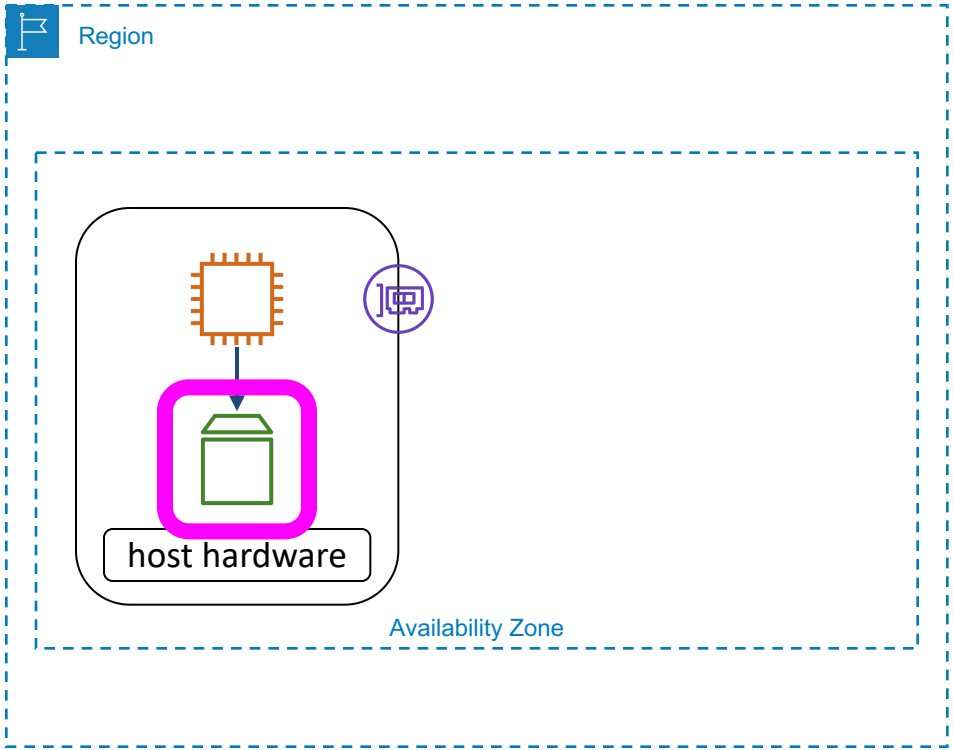

vCPU is roughly equivalent to a thread on a processor core

# EC2 Resources - Processor & Memory



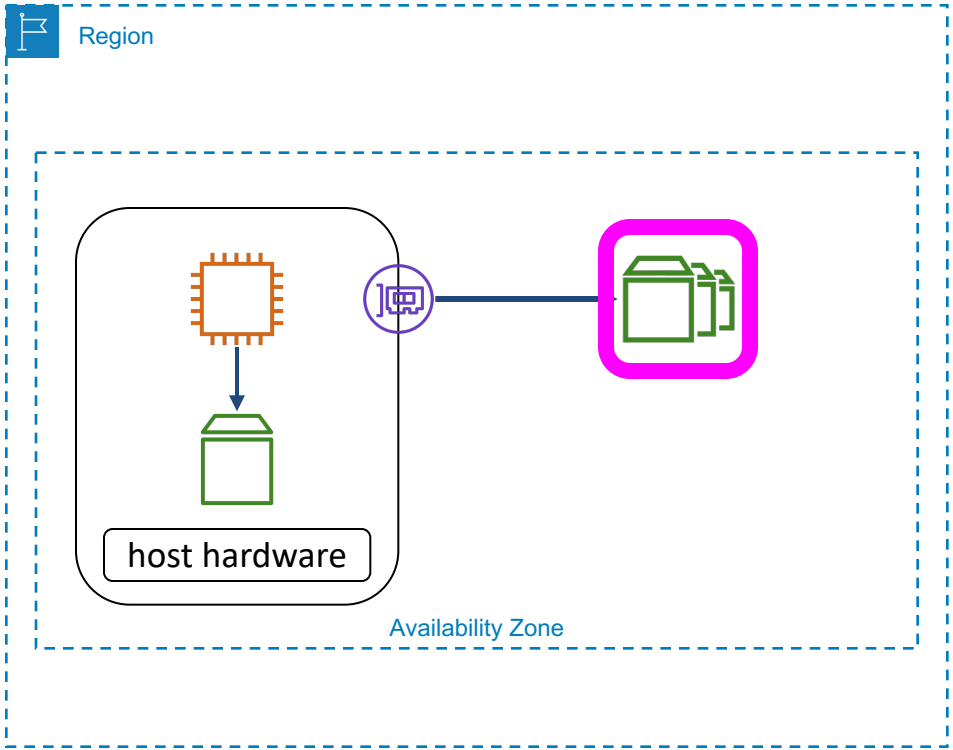

Choosing architectures with more vCPU raises the memory ceiling

# EC2 Resources - Storage



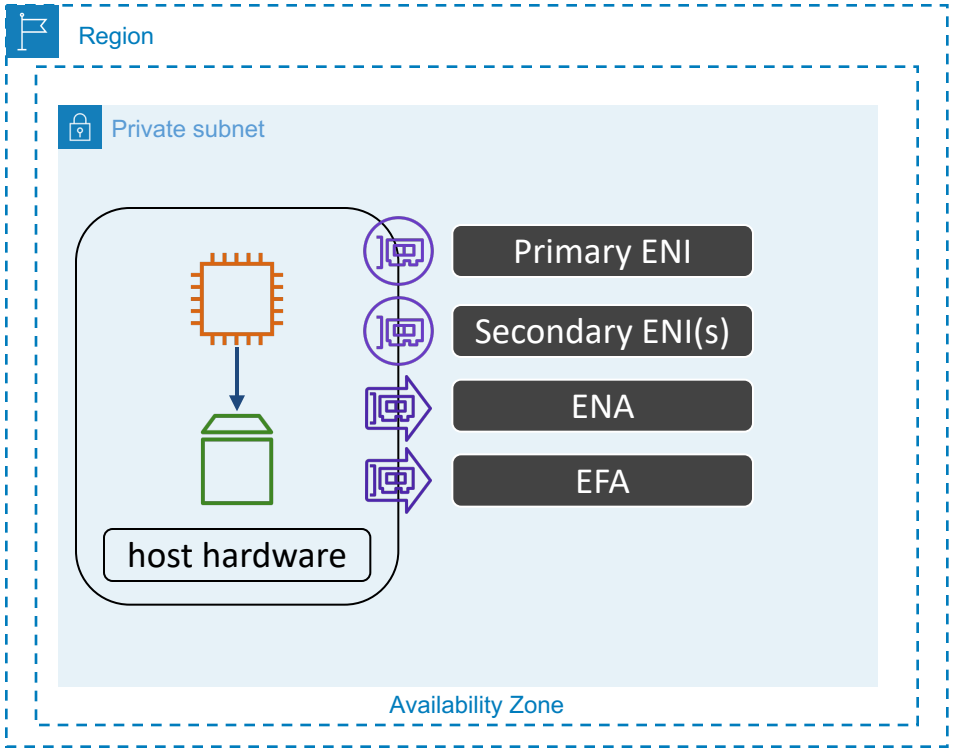

Instance storage is direct attached to the EC2 host hardware

# EC2 Resources - Storage



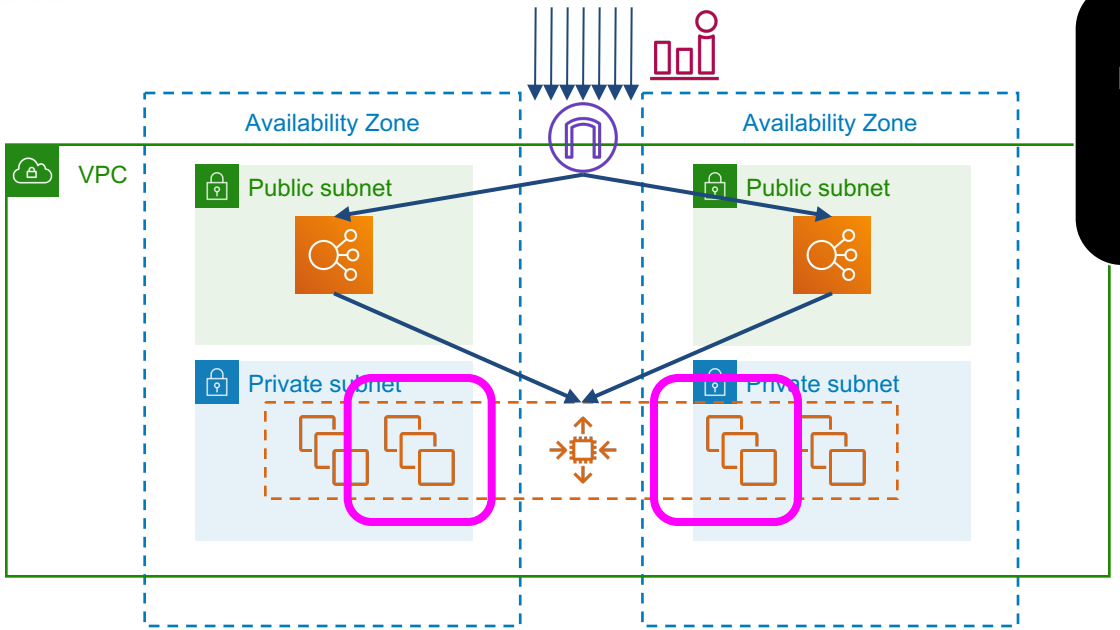

EBS storage is reached via network but presented as local block storage

# EC2 Resources - Network



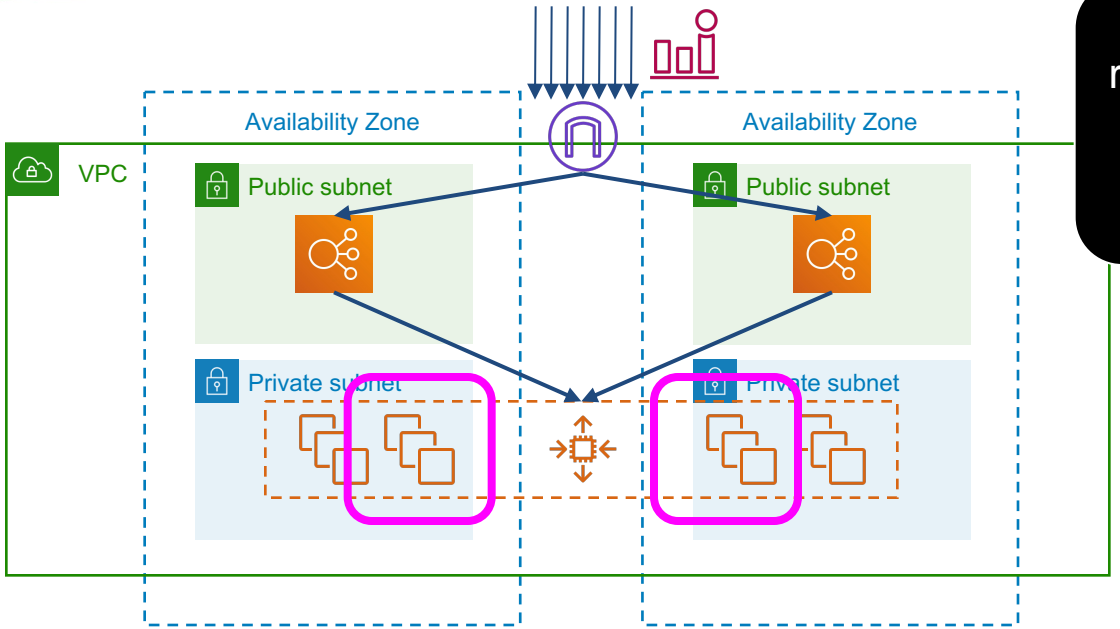

One primary network interface required, others are optional

# What Is Auto Scaling?



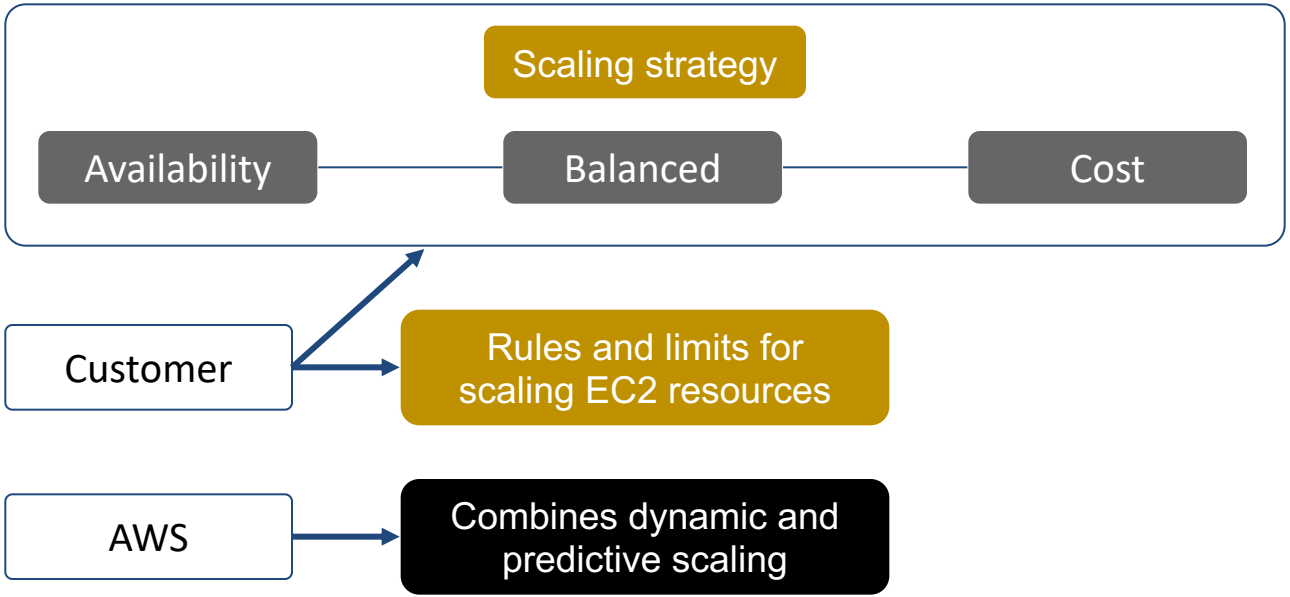

Add EC2 resources into the fleet, scaling capacity to match load

# What Is Auto Scaling?




Remove EC2 resources from the fleet, scaling capacity to match load

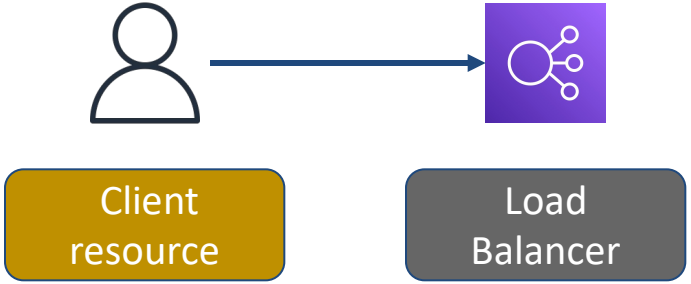
# What is an Auto Scaling plan?



# Elastic Load Balancer Basics

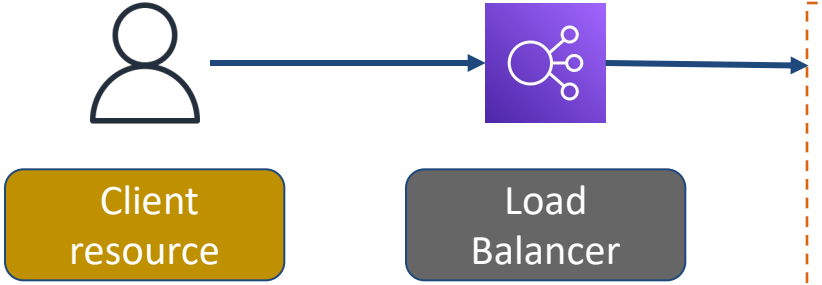
- AZ scoped
- Multi-AZ support
- Managed load balancing service
- Distribute traffic to back end

# Load Balancer Architecture



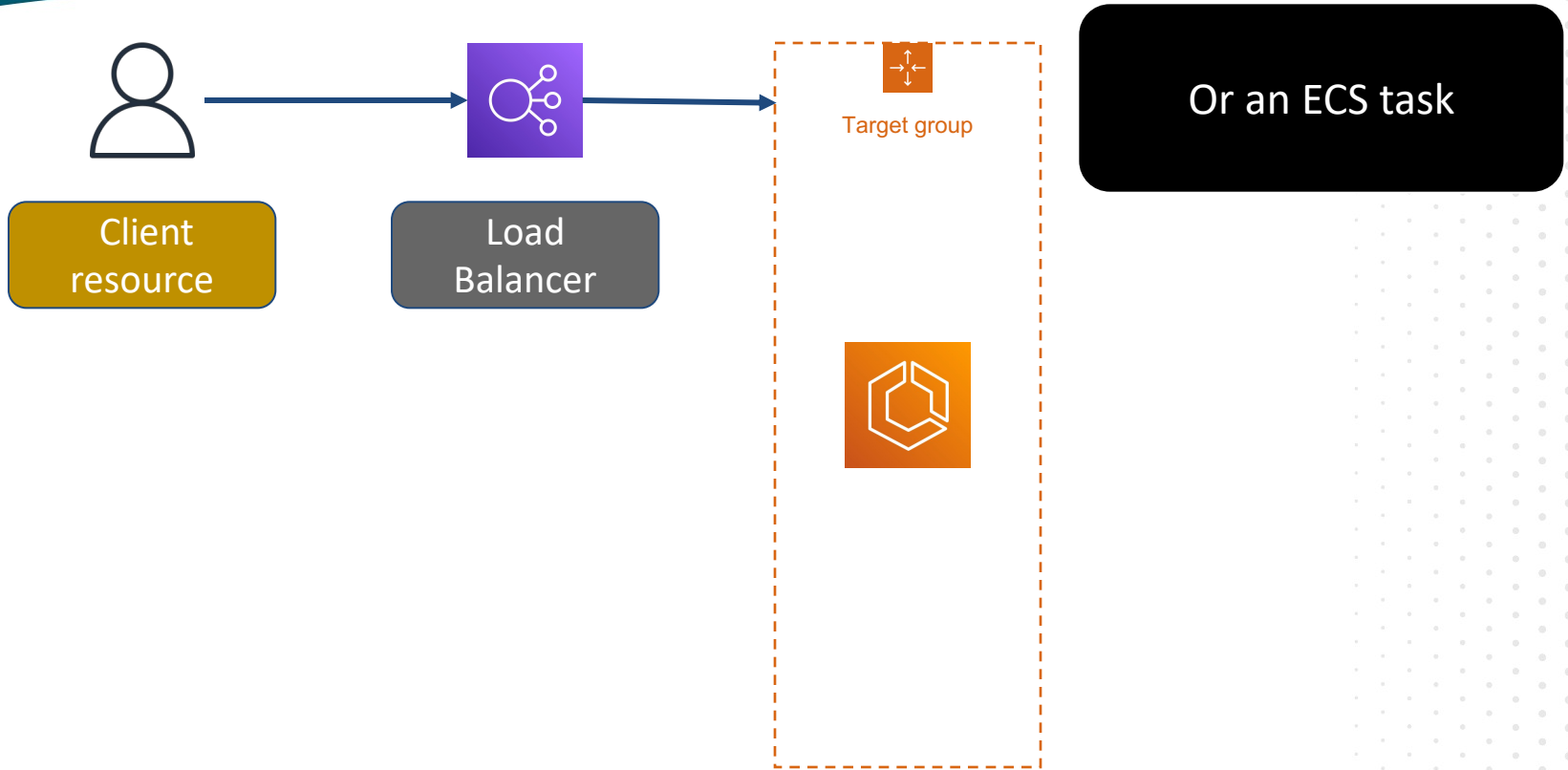

Client sends traffic at layer 4 or 7 to the ELB endpoint

# Load Balancer Architecture

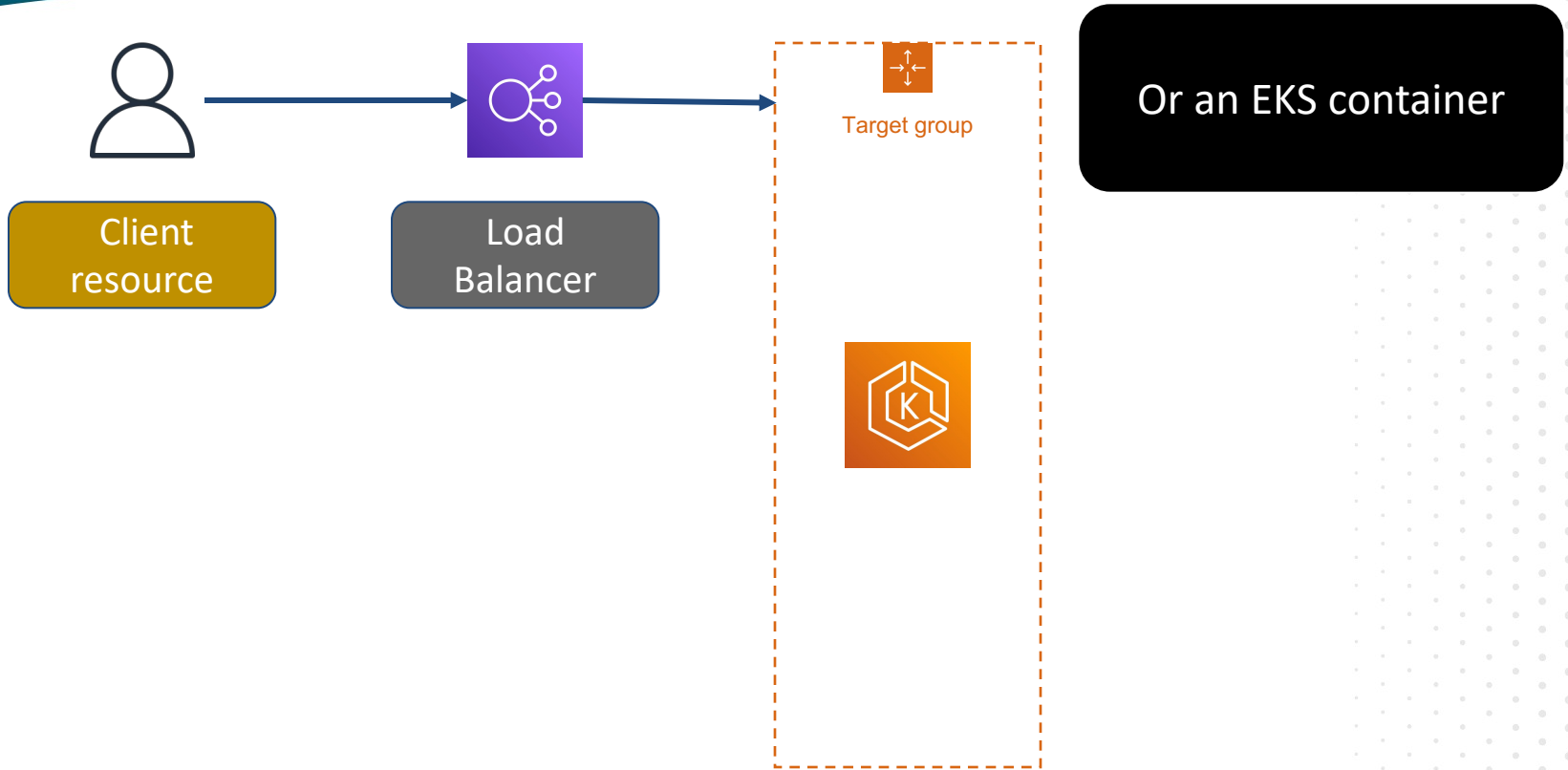



The ELB either proxies or passes traffic through to EC2

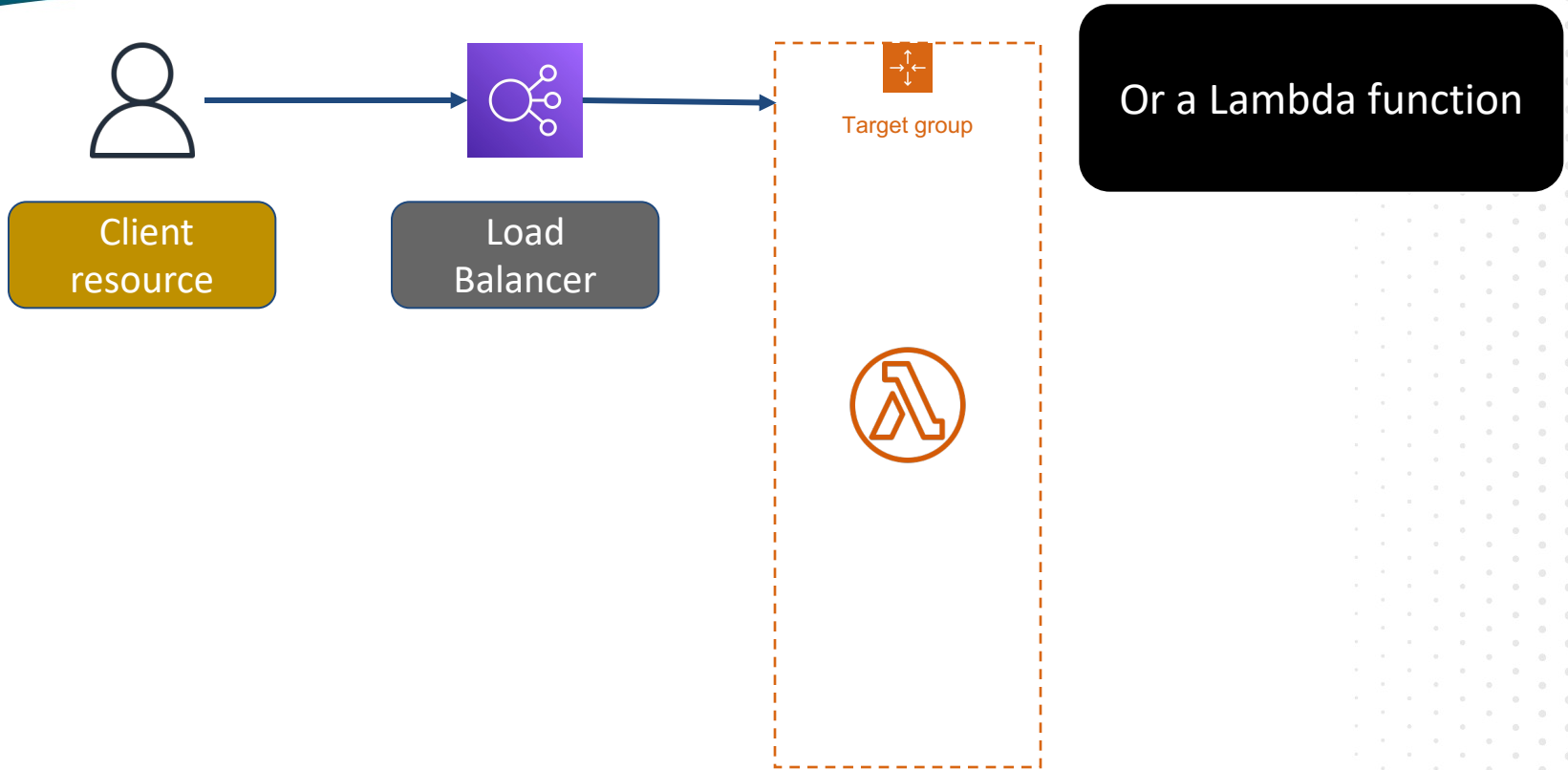
# Load Balancer Architecture



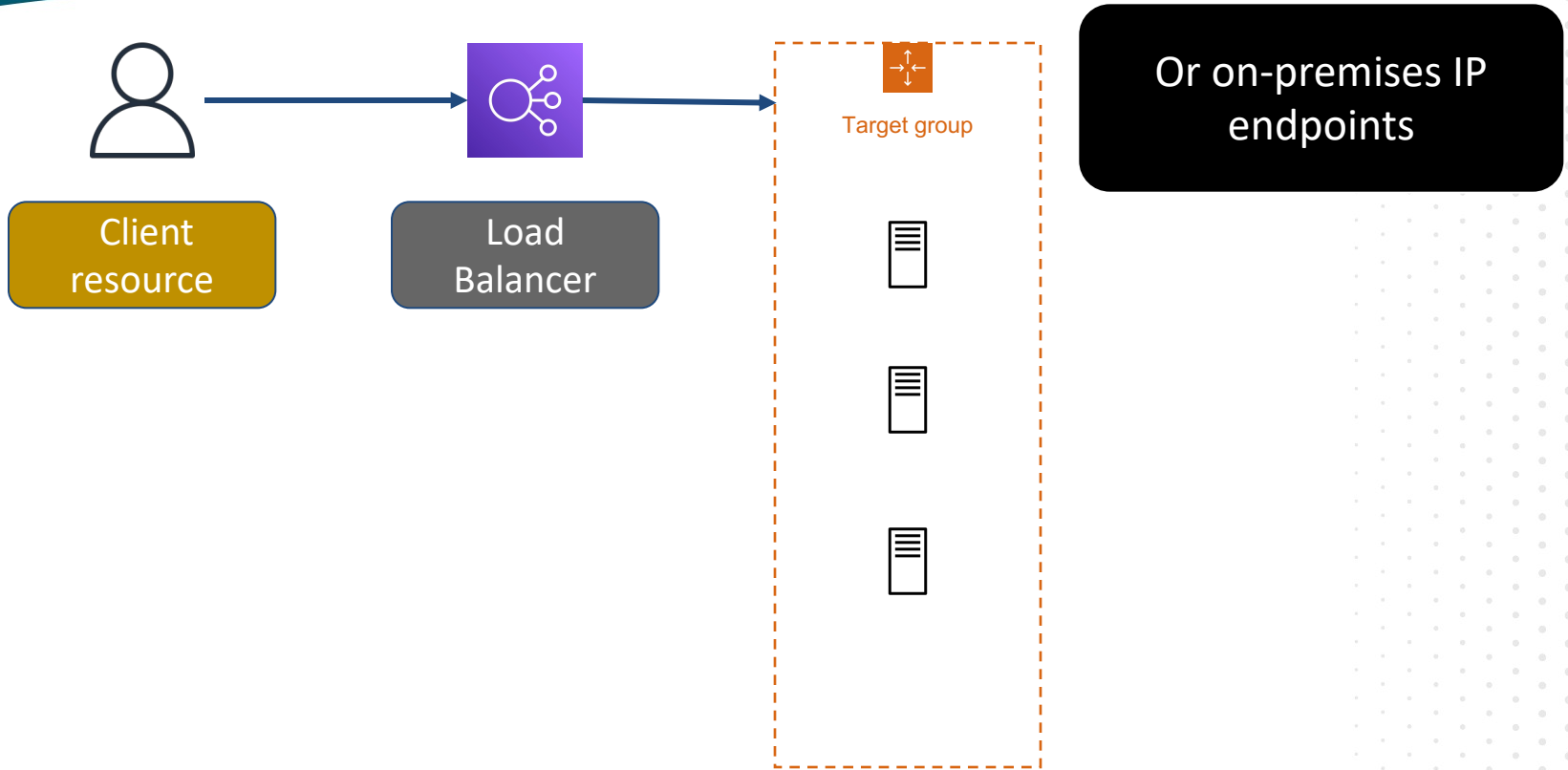
# Load Balancer Architecture



# Load Balancer Architecture



# Load Balancer Architecture



# Question Breakdown

# Question and Answer Choices

**Which AWS offering can be described as Function As A Service (FAAS)?**

A. EC2
B. Lambda
C. Elastic Beanstalk
D. ECS

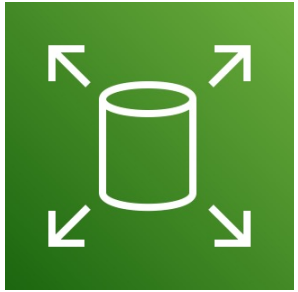
# Correct Answer and Explanation

**AWS Lambda is a region-scoped service which enables customers to deploy functions to a serverless infrastructure.**

A. EC2
B. Lambda
C. Elastic Beanstalk
D. ECS

# AWS Block Storage Services

Block storage

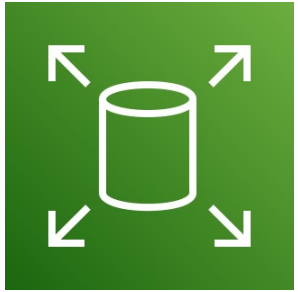


EBS is presented to EC2 instances as raw block devices and separate infrastructure from EC2

# AWS File Storage Services

Block storage

File storage

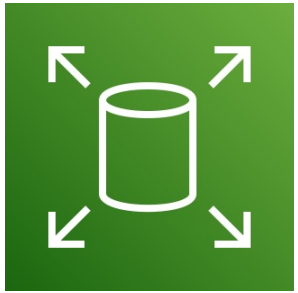


EFS is a managed NFSv4 service

# AWS File Storage Services

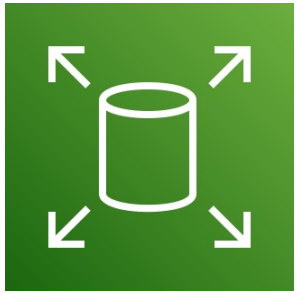
Block storage

File storage




FSx for NetAppONTAP, OpenZFS, Windows File Server, Lustre

# AWS Object Storage Services

| Block storage | File storage | Block storage |
| --- | --- | --- |
|  |  |  |
| |   |  |

S3 and Glacier are designed for object (WORM - Write Once, Read Many) storage and do not behave like filesystems

# Other Storage Services

On-premises storage

Storage Gateway and the Snow* services can be used to transfer data to and from AWS

# Other Storage Services

On-premises storage

Backups

AWS Backup is used to manage backups in many services across the AWS ecosystem

# Question Breakdown

# Question and Answer Choices

**Your company must migrate 1Pb data from an on-premises data center into AWS. Which AWS service would be appropriate for this migration?**

A. S3
B. EFS
C. Direct Connect
D. Snowball

# Correct Answer and Explanation

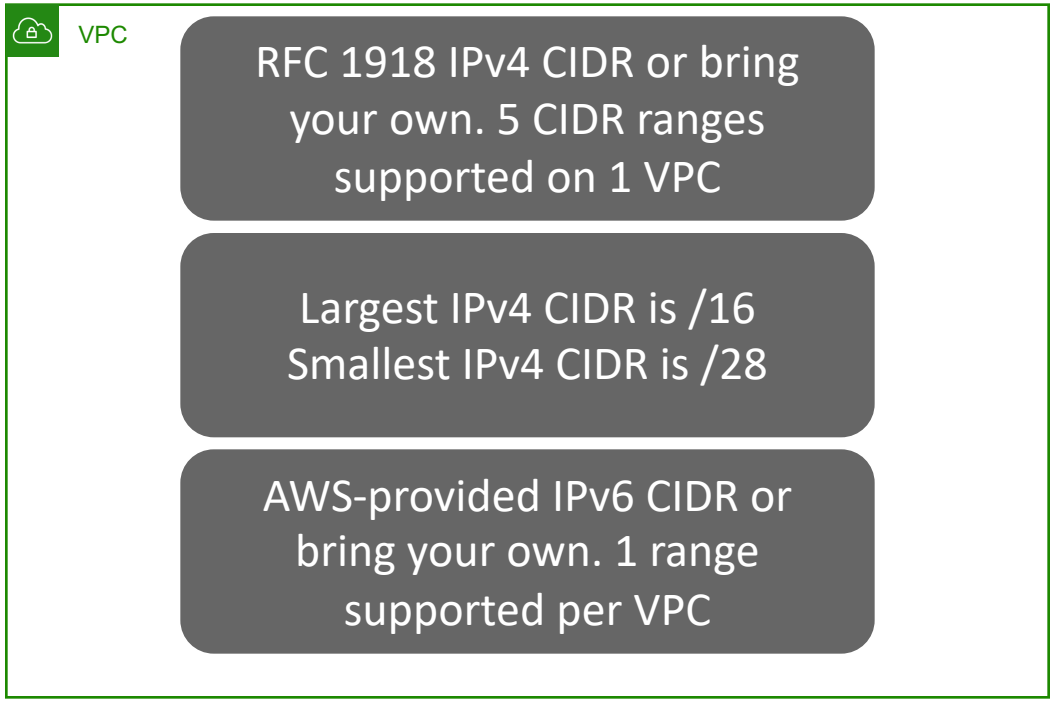
**AWS Snowball is an appliance-based offering that can be used to migrate large data sets into S3. In this case, you will need multiple appliances to achieve the migration.**

A. S3
B. EFS
C. Direct Connect
D. Snowball

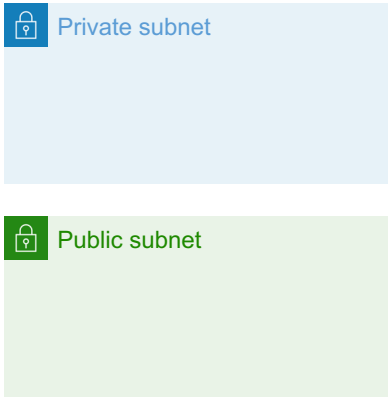
# VPC Basics


- Virtual Private Cloud
- Region scope
- Private network for many AWS resources

# VPC CIDR Addresses



# Subnet Basics




- Contiguous range of IP addresses in a VPC
- AZ scope
- Local Zone scope
- Associate with Route table and Network ACL

# Subnet Types

Bidirectional Internet access via IGW

Public subnet

Outbound Internet access via proxy (NAT GW)

Private subnet

No Internet access, or only via VPN/DX

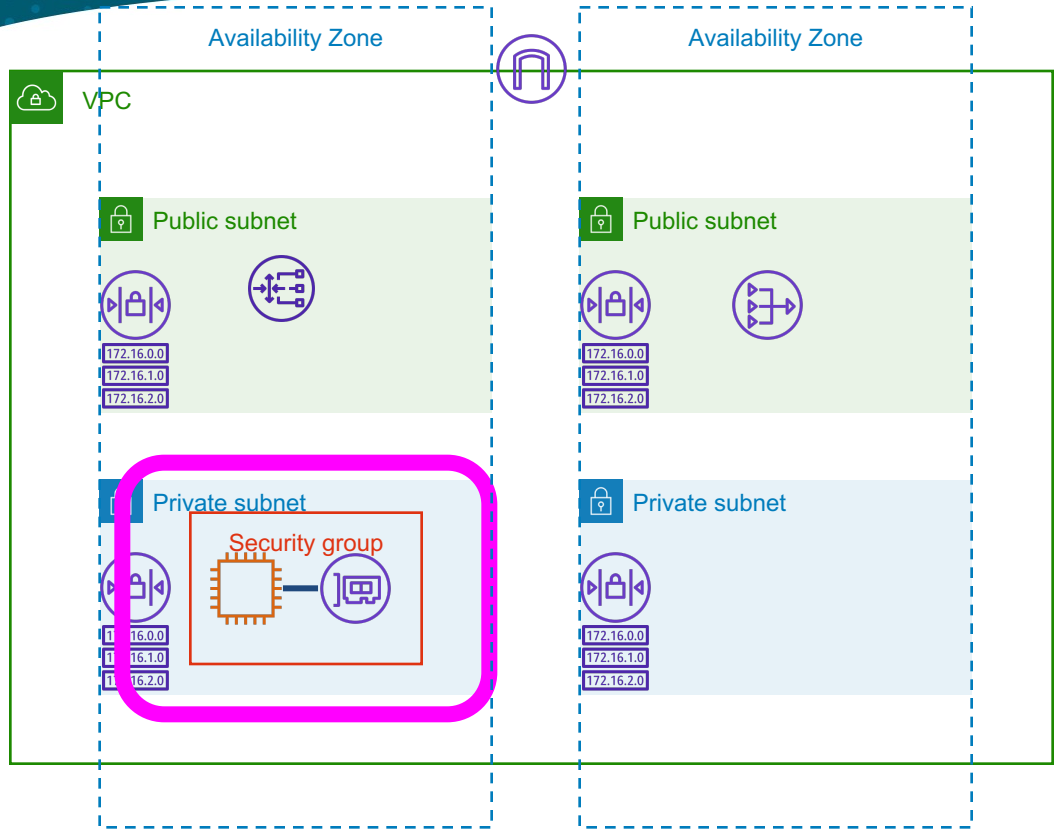
VPC/VPN only subnet

0: network
1: VPC router
2: DNS (if base VPC CIDR)
3: Reserved for future use
Last: Bcast address (not used)

# Security Group Basics


- Associate with 1+ network interfaces
- Stateful firewall resource
- Inbound/outbound rules
- Default deny
- Rules evaluated as a whole

# Security Group Strategy




Suggestion: 1 Security group per application per tier!

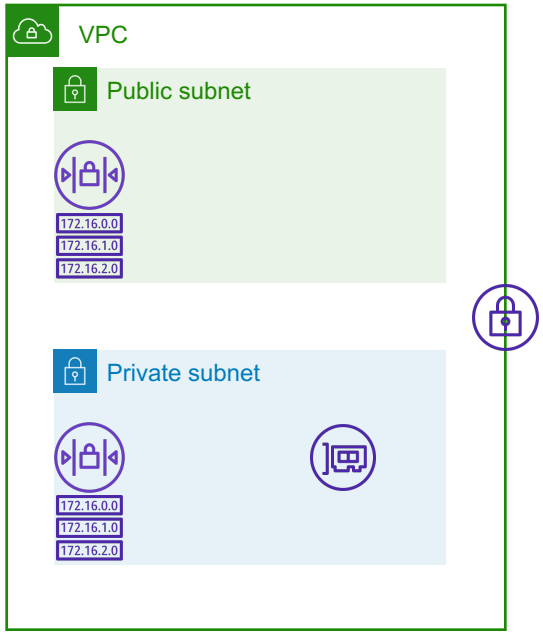
# Site-to-Site VPN Basics

- Attach to VPC
- Region scoped
- Hardware-backed
- IPSEC encryption

# Site-to-Site VPN Provisioning

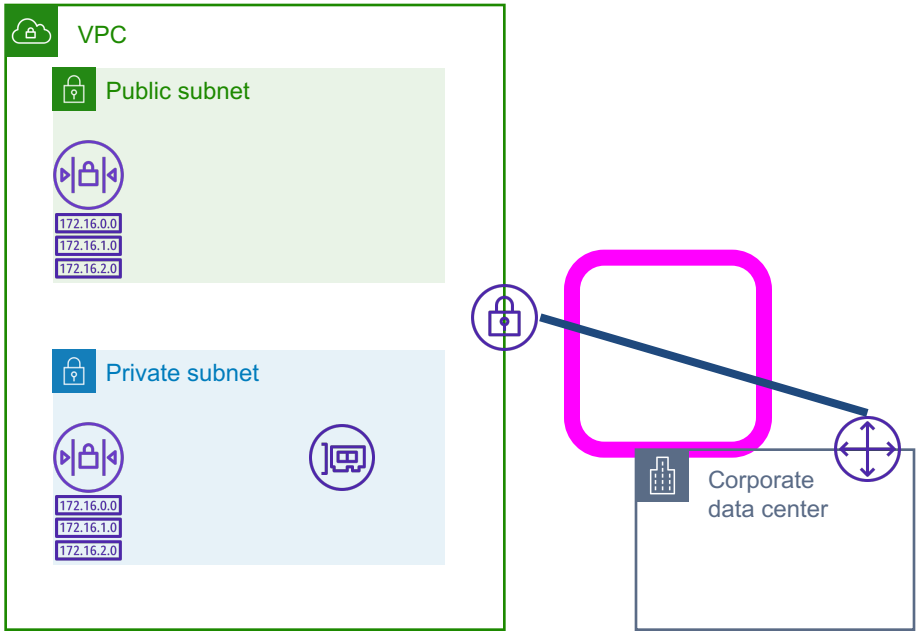
Virtual Private Gateway can be deployed as a standalone resource

# Site-to-Site VPN Provisioning



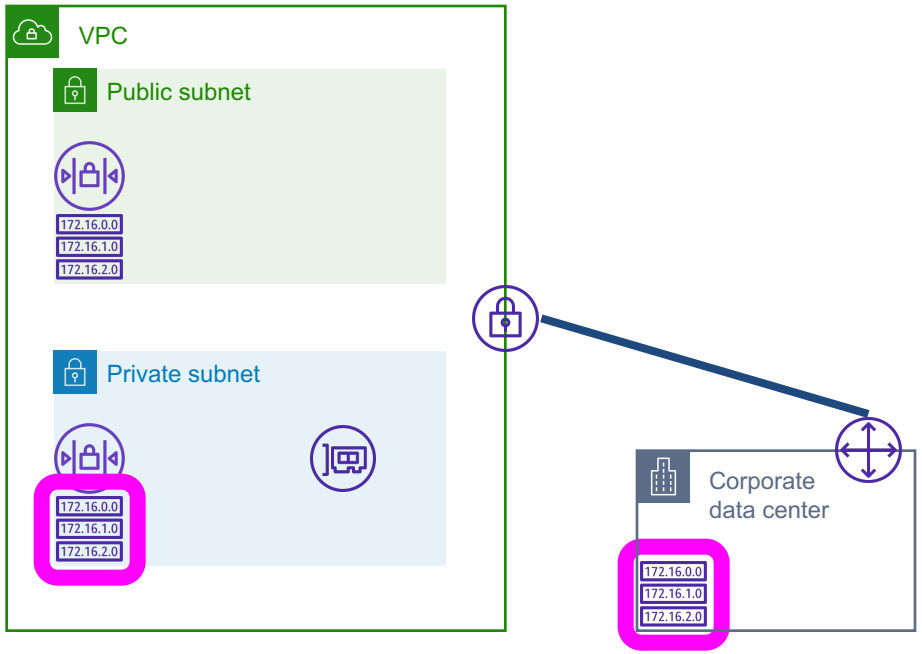

Attach the VGW to the VPC

# Site-to-Site VPN Provisioning



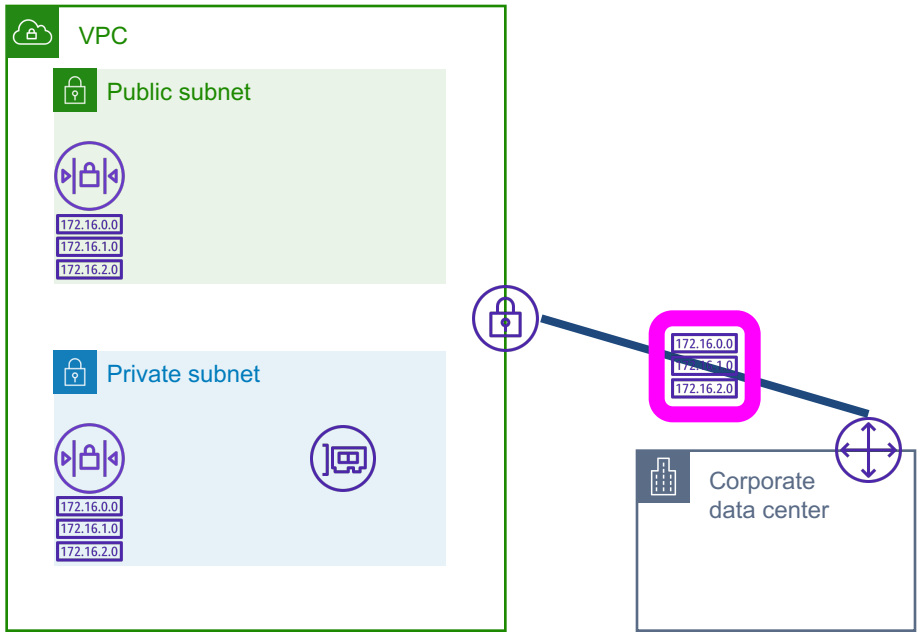

Configure the IPSEC VPN from the on-premises network

# Site-to-Site VPN Routing Options




Static VPN requires route table entries on each side

# Site-to-Site VPN Routing Options



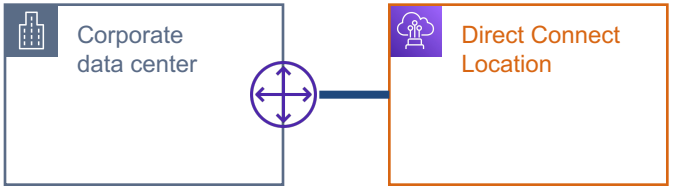

Dynamic VPN uses BGP to propagate routes

# Direct Connect Basics

- On-prem to AWS network connectivity
- Region scoped
- Multi-region supported (US only)
- Requires BGP and 802.1q VLANs

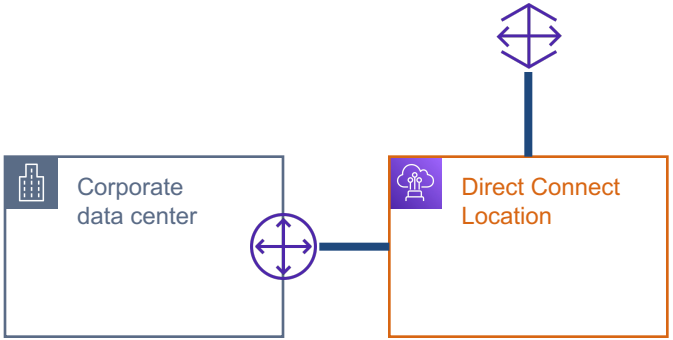
# Direct Connect Provisioning

Provision 1, 10, or 100Gb fiber to AWS partner data center



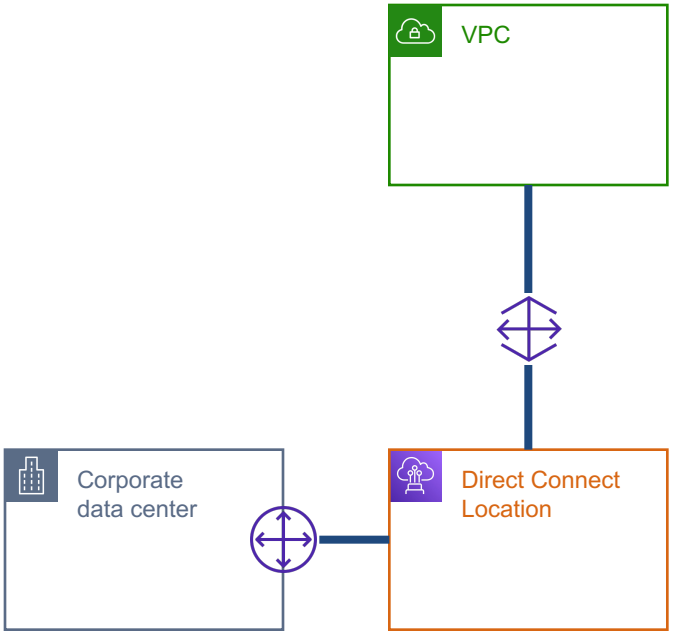
# Direct Connect Deployment Options

Partner provisions cross-connect into AWS network



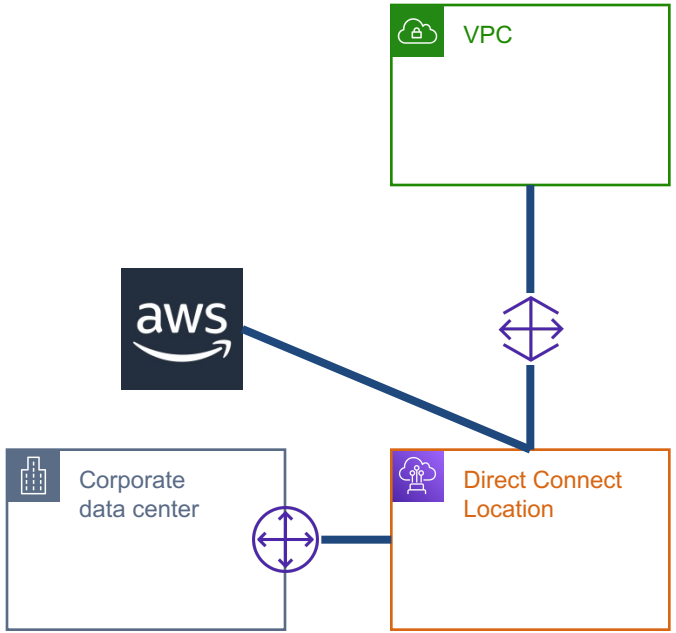
# Direct Connect Deployment Options

Configure interface to connect to VPC



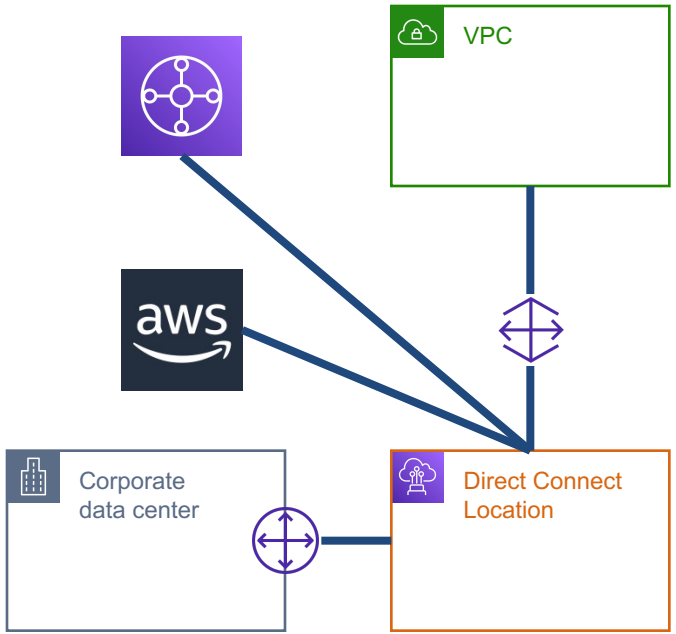
# Direct Connect Deployment Options

Configure interface to connect to AWS public network



# Direct Connect Deployment Options

Configure interface to connect to Transit Gateway



# Route 53 Basics


- Global scope
- DNS service
- Traditional DNS
- Cloud-native features

# Route 53 Basics


- DNS Registrar
- DNS Zones
- Health checks
- Resolver endpoints
- Resolver rules

# Question Breakdown

# Question and Answer Choices

**Which AWS networking feature would be appropriate for a low cost, reliable, and secure connection from an on-premises data center into a VPC network?**

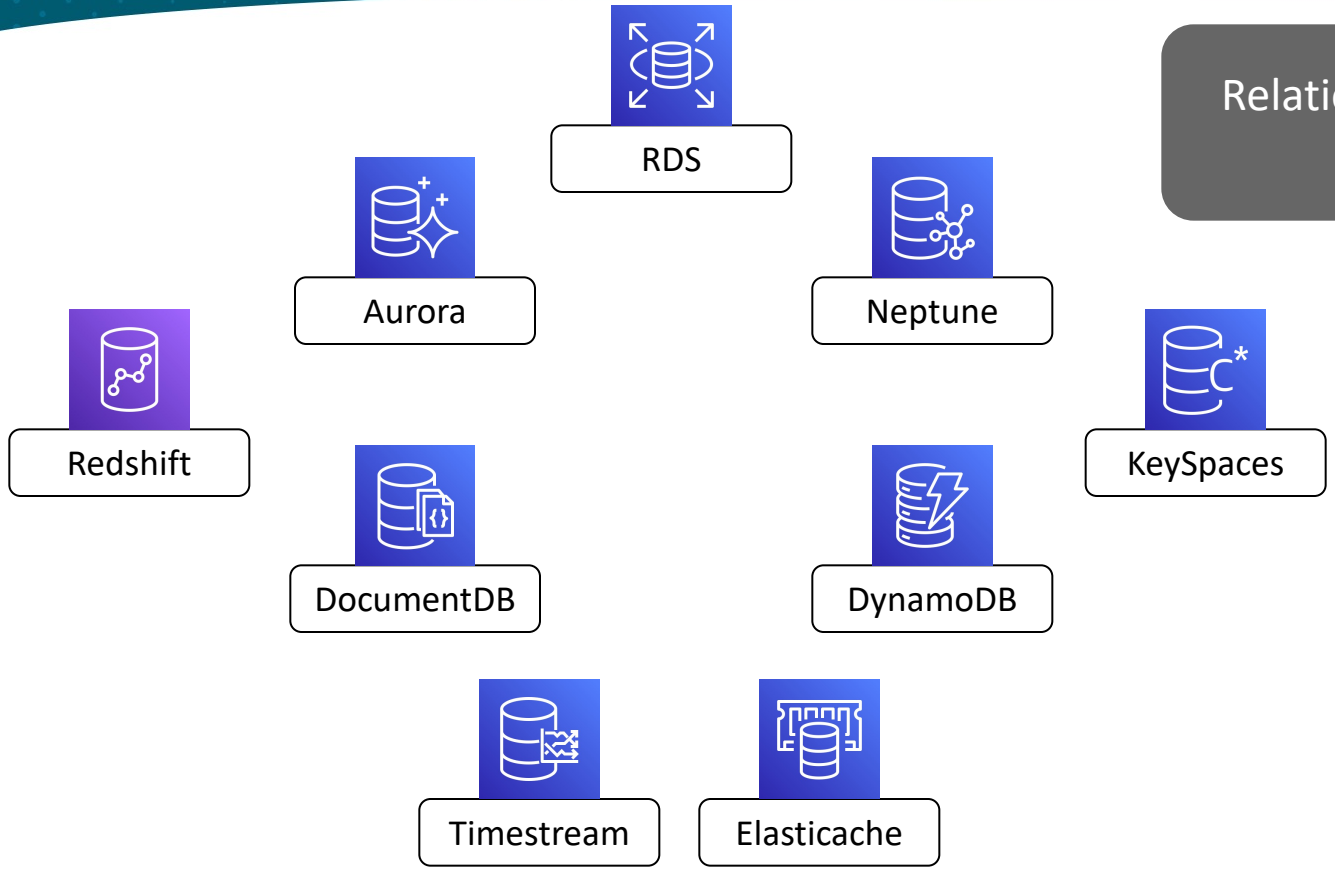
A. Site to site VPN
B. Direct Connect
C. Public Internet
D. OpenVPN client

# Correct Answer and Explanation

**The AWS Virtual Private Gateway/VPN product is easy to set up and uses secure IPSEC VPN tunnels for routing traffic from an external network to a VPC.**

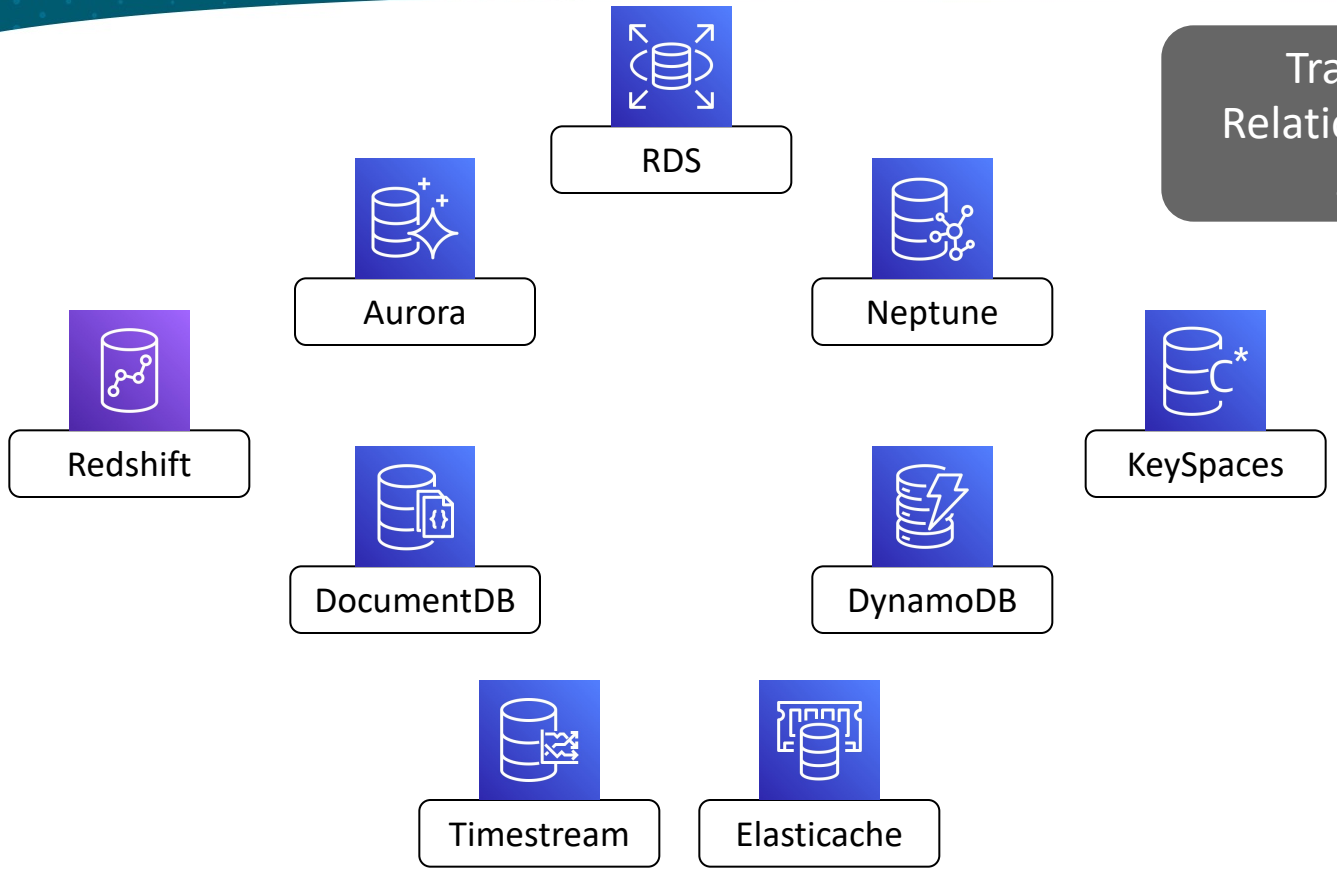
A. Site to site VPN
B. Direct Connect
C. Public Internet
D. OpenVPN client

# AWS Database Services



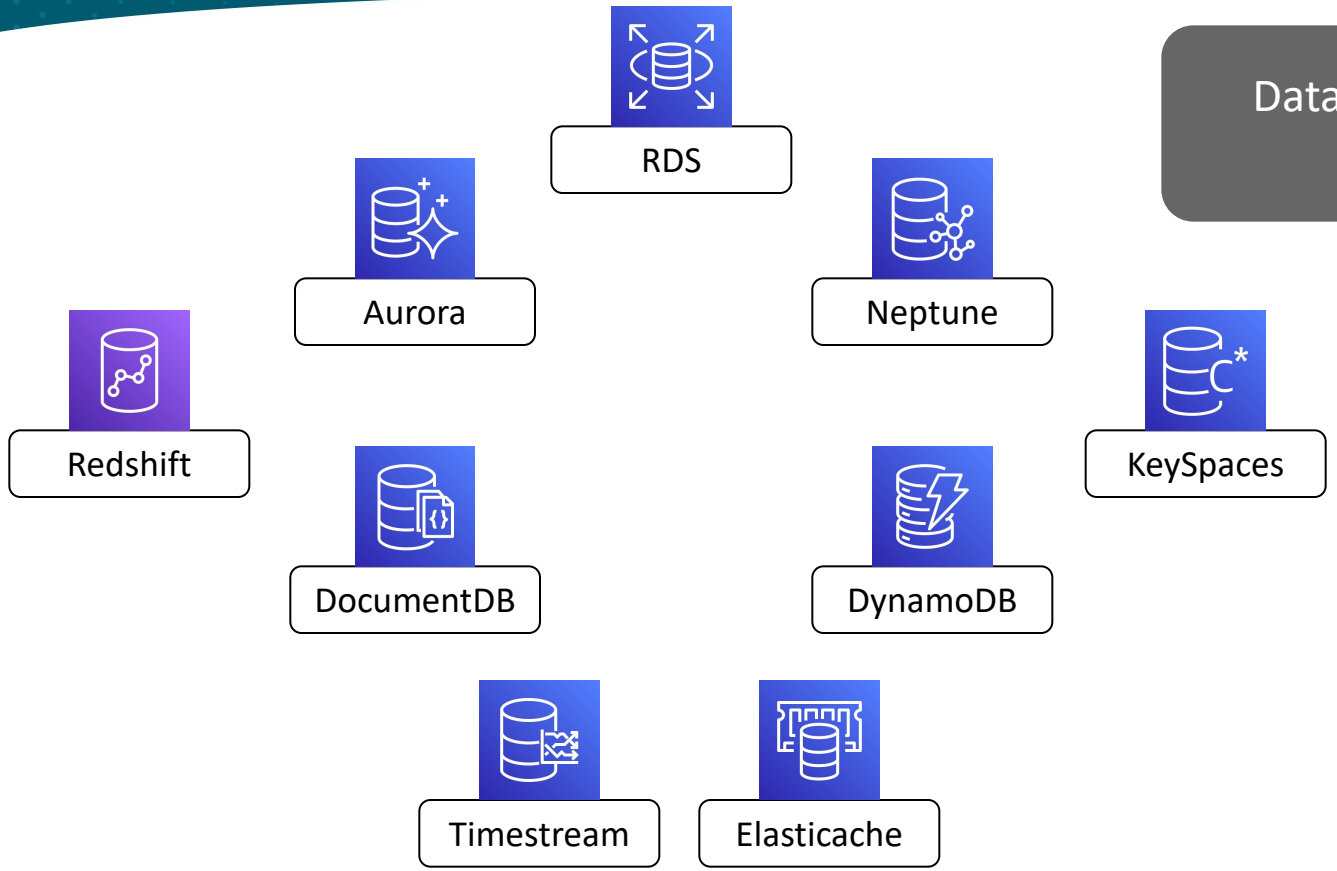

Relational Database Services

# AWS Database Services



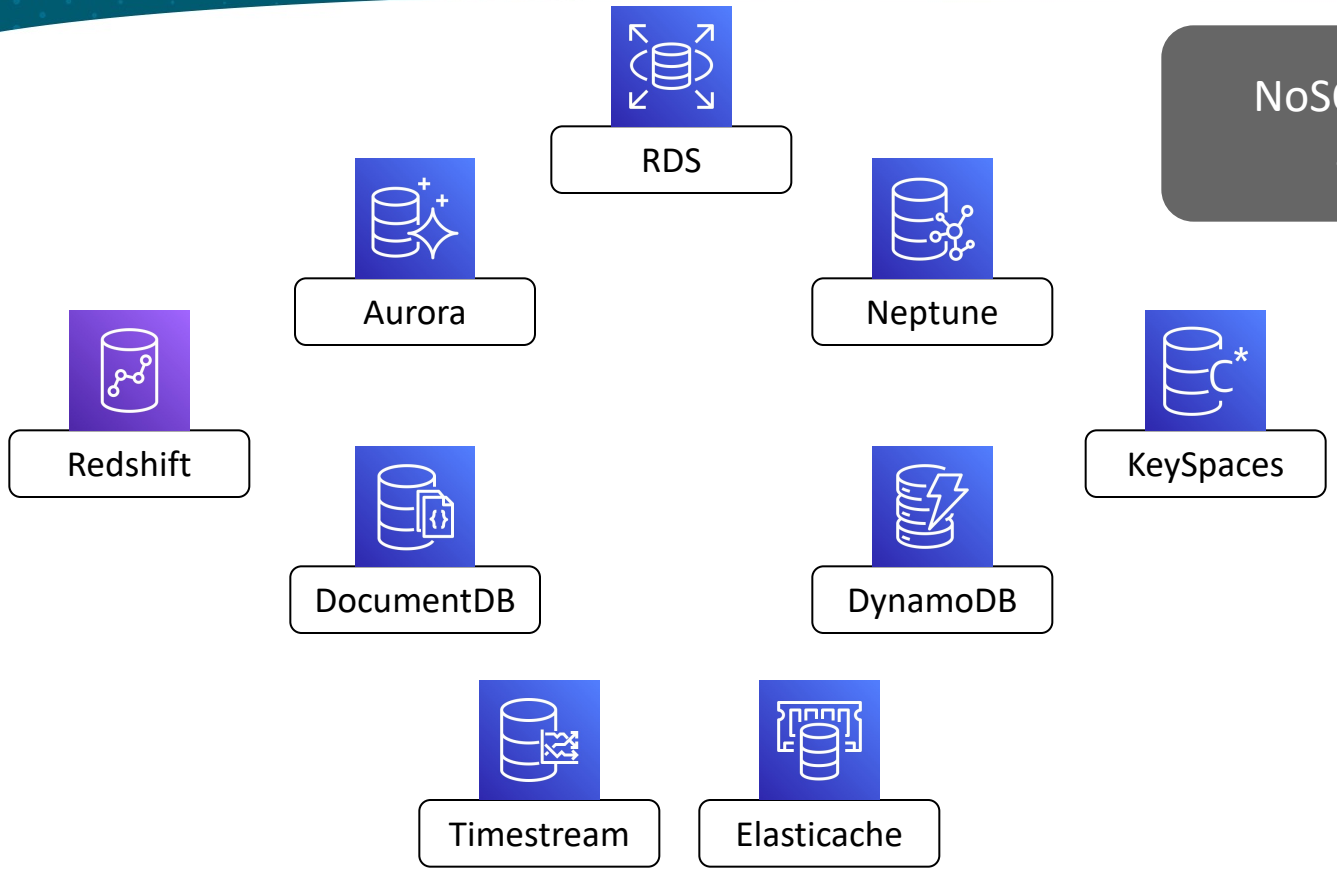

Transactional Relational Database Services

# AWS Database Services



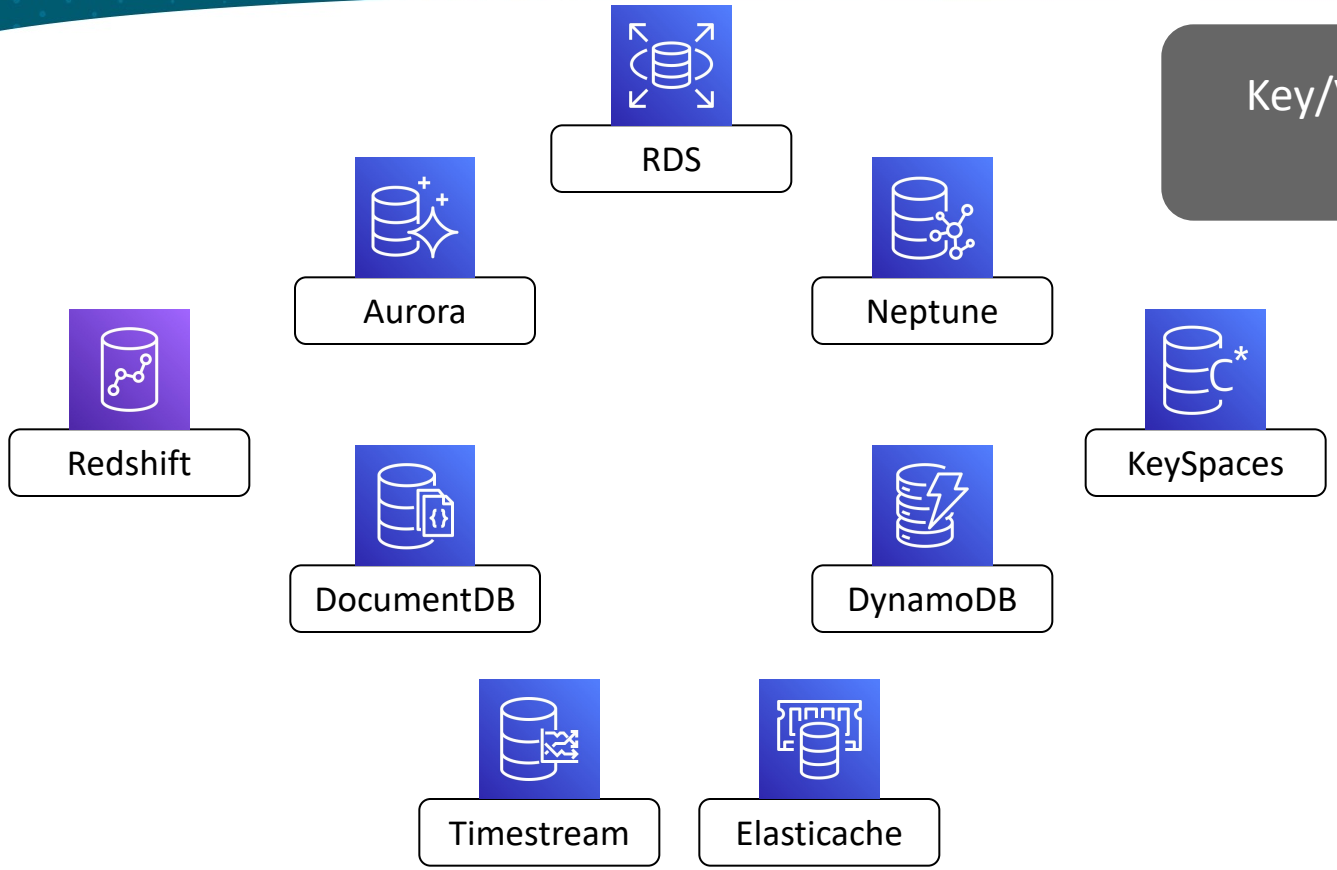

Data Warehouse Service

# AWS Database Services



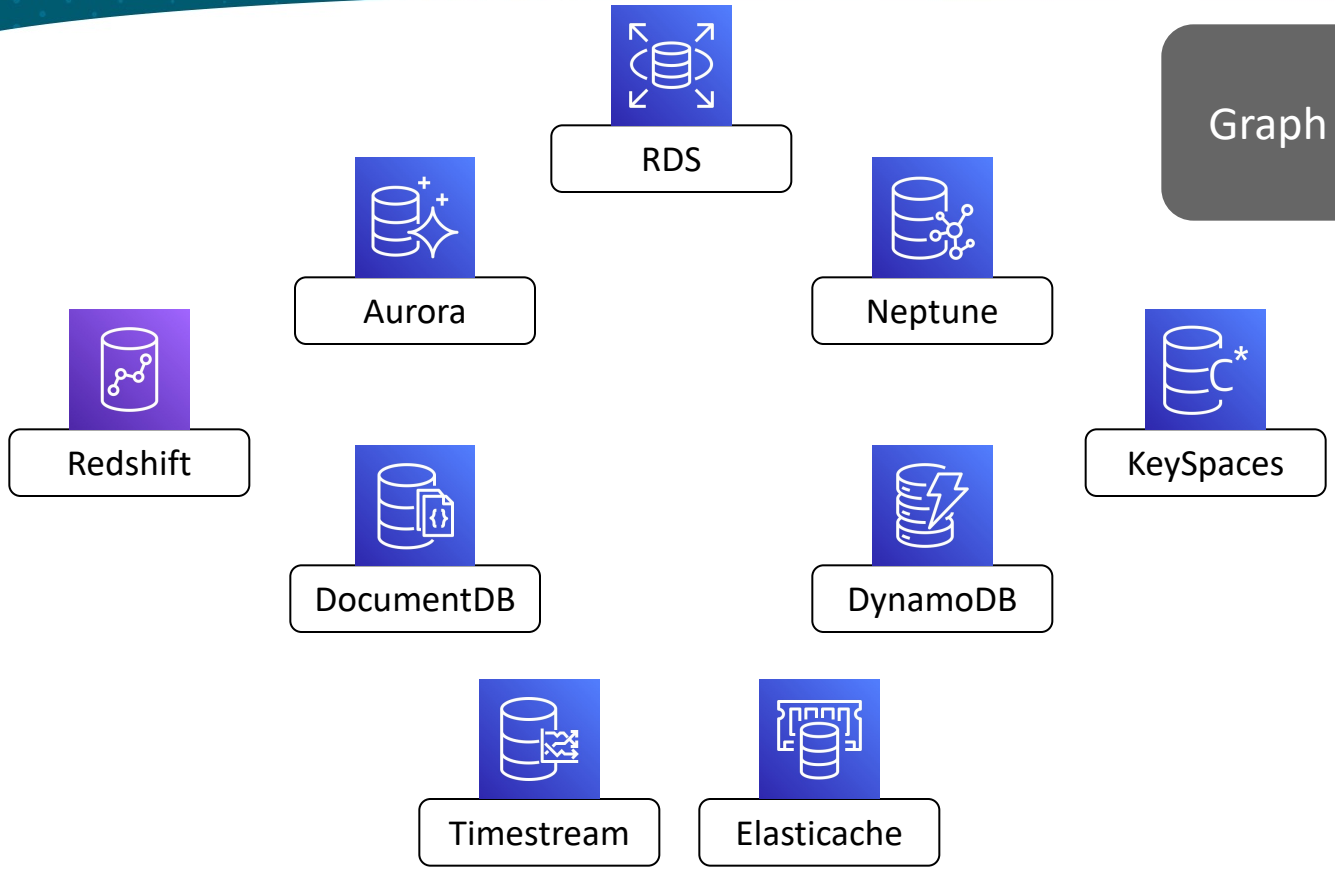

NoSQL Database Services

# AWS Database Services



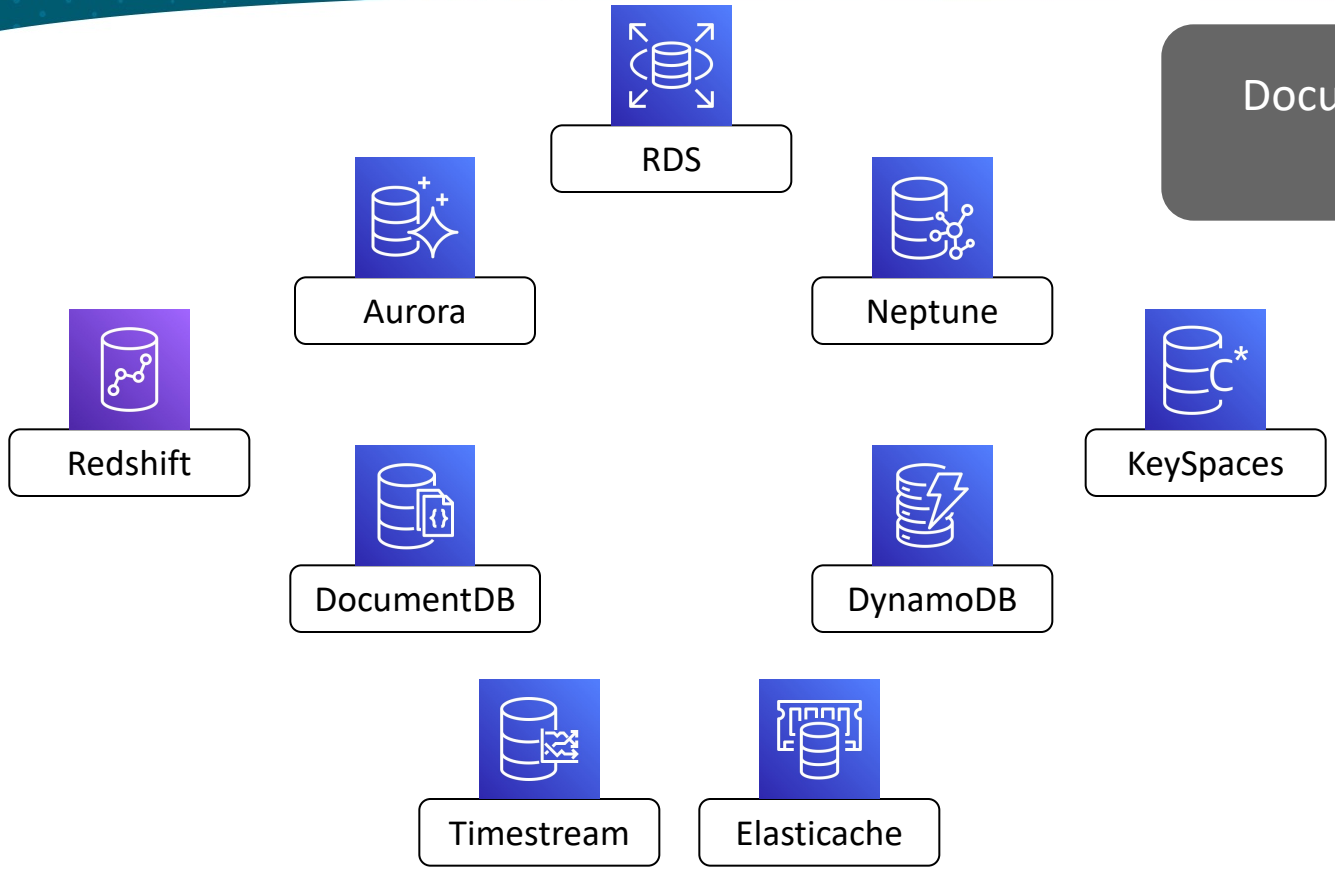

Key/Value NoSQL Service

# AWS Database Services



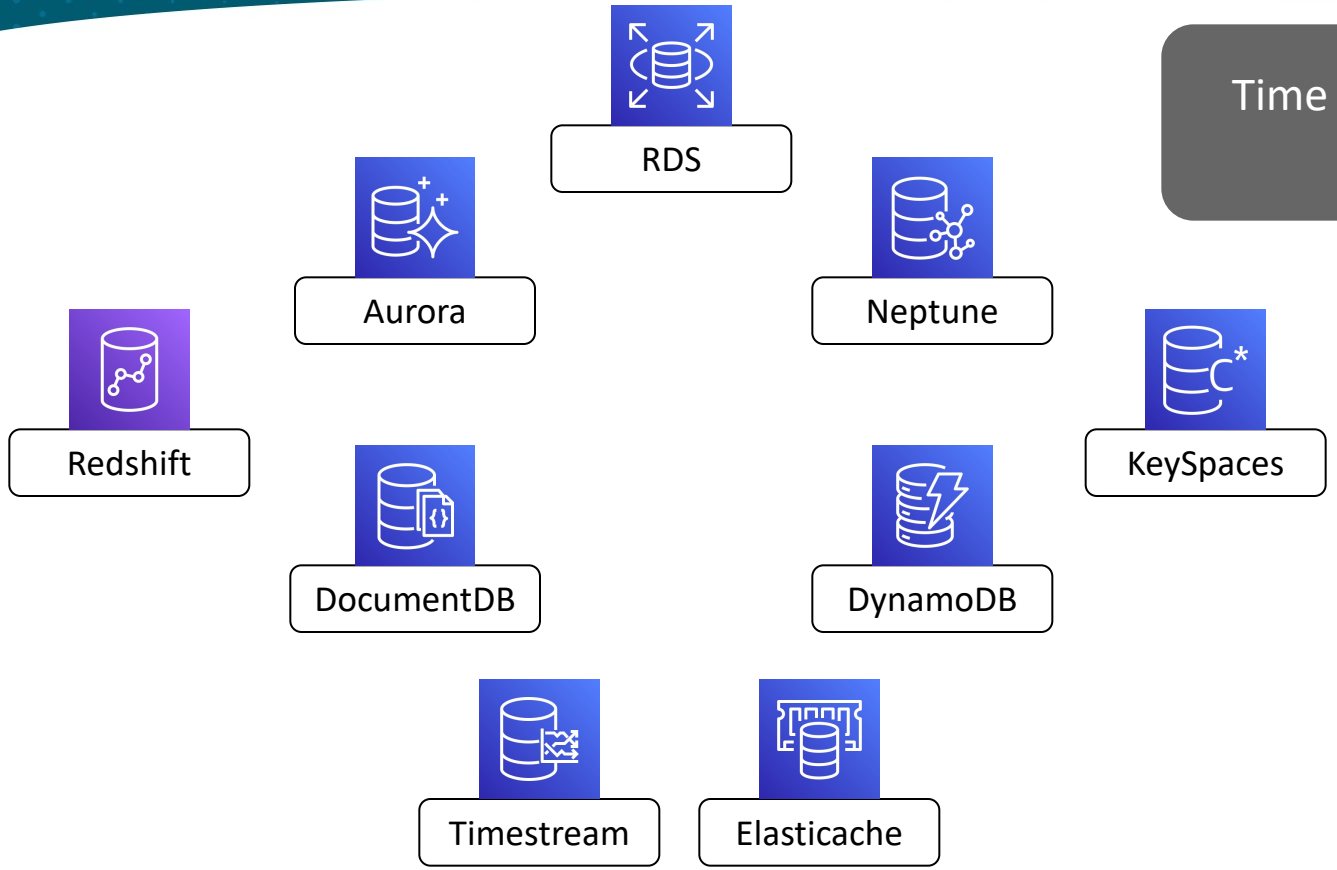

Graph NoSQL Service

# AWS Database Services



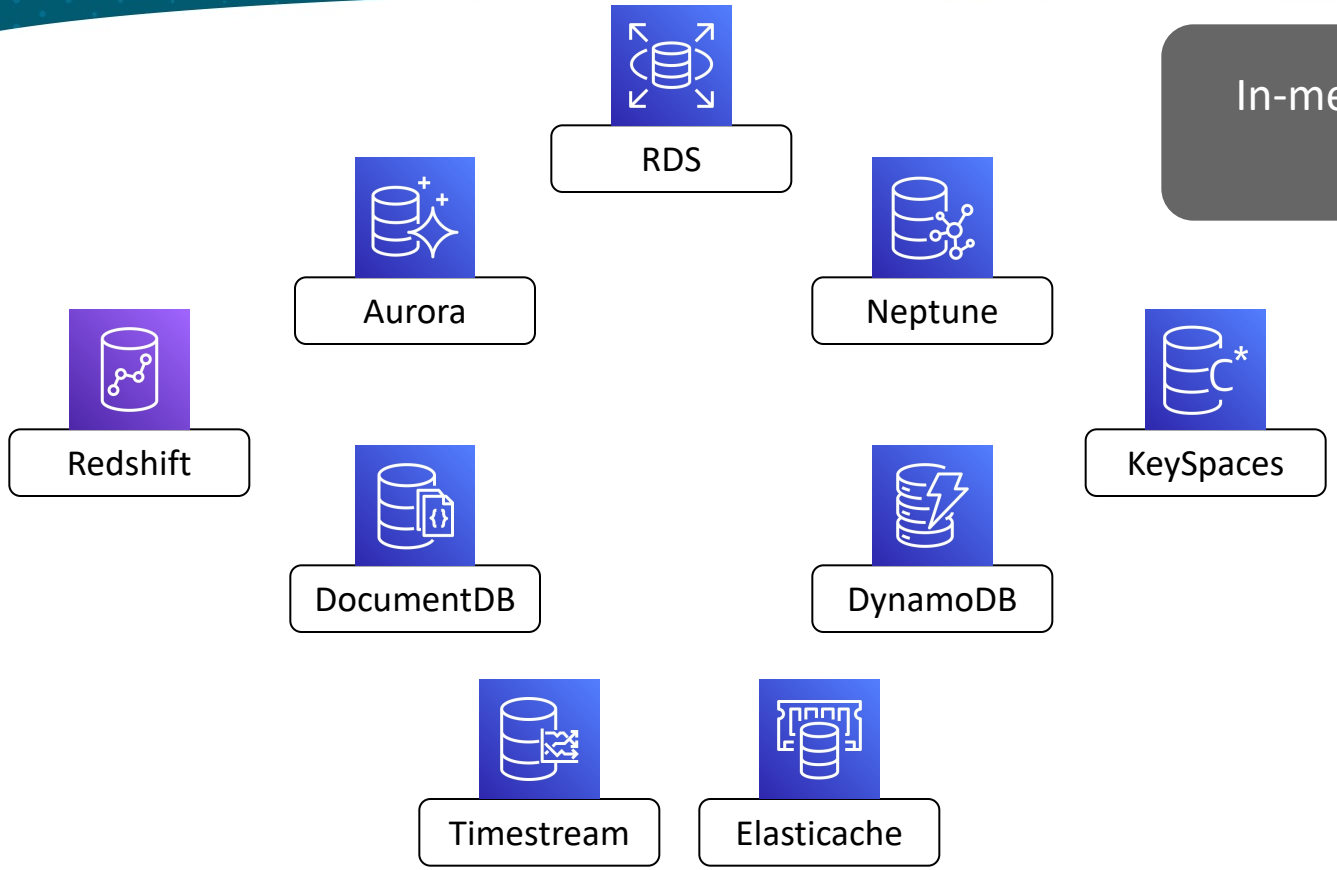

Document NoSQL Service

# AWS Database Services




Time Series NoSQL Service

# AWS Database Services




In-memory NoSQL Service

# Question Breakdown

# Question and Answer Choices

**An application has a requirement for a PostgreSQL OLTP back end, and there is a further requirement to be cloud native. Which service would be appropriate to meet this requirement?**

A. EC2
B. RDS
C. Redshift
D. No AWS services are appropriate, you must use on-premises resources

# Correct Answer and Explanation

**RDS is the managed relational database service, and supports the PostgreSQL engine.**

A. EC2
B. RDS
C. Redshift
D. No AWS services are appropriate, you must use on-premises resources

## Question Domain 3: Technology

# Technology Support Resources

# AWS Technology Documentation

- Service user guides
- Best practices*
- Whitepapers
- AWS Knowledge Center
- AWS Blogs
- AWS Support forums

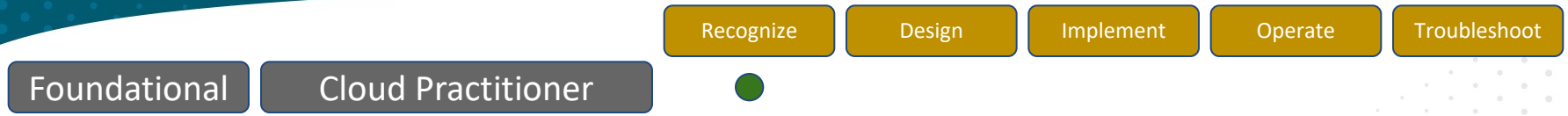
# AWS Support Scopes

- AWS Abuse
- AWS support cases
- Premium Support pages
- TAMs (Technical Account Managers)

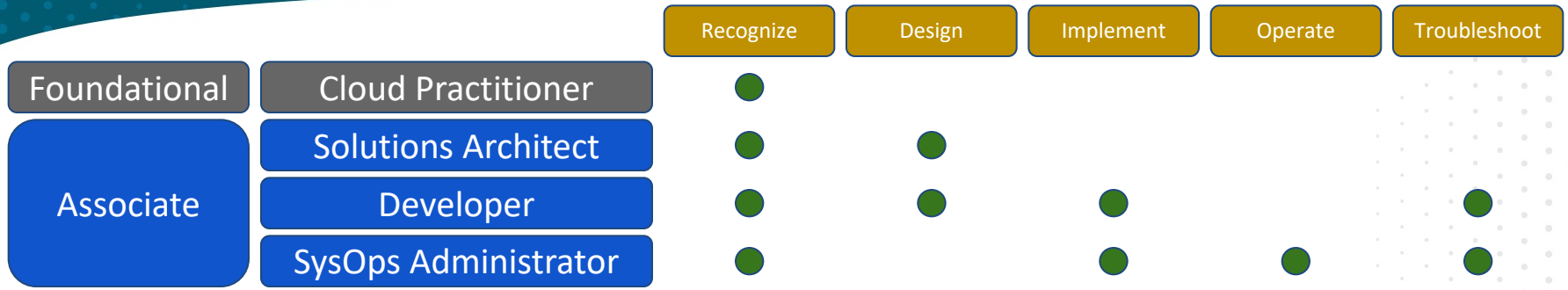
# Other Support Resources

- APN (Amazon Partner Network)
- AWS Professional Services
- AWS Trusted Advisor

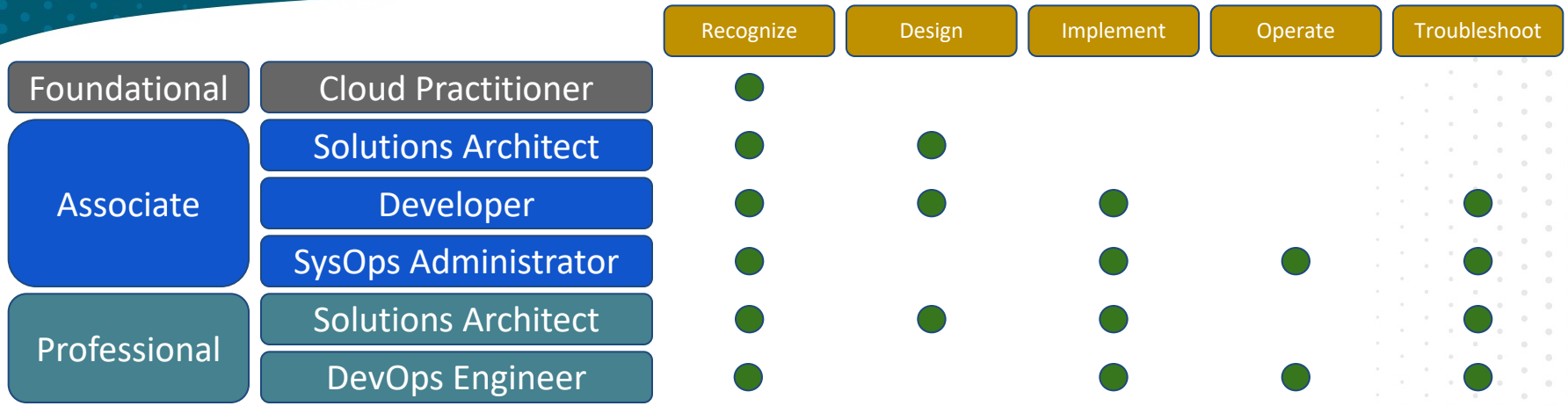
# AWS Certification Landscape



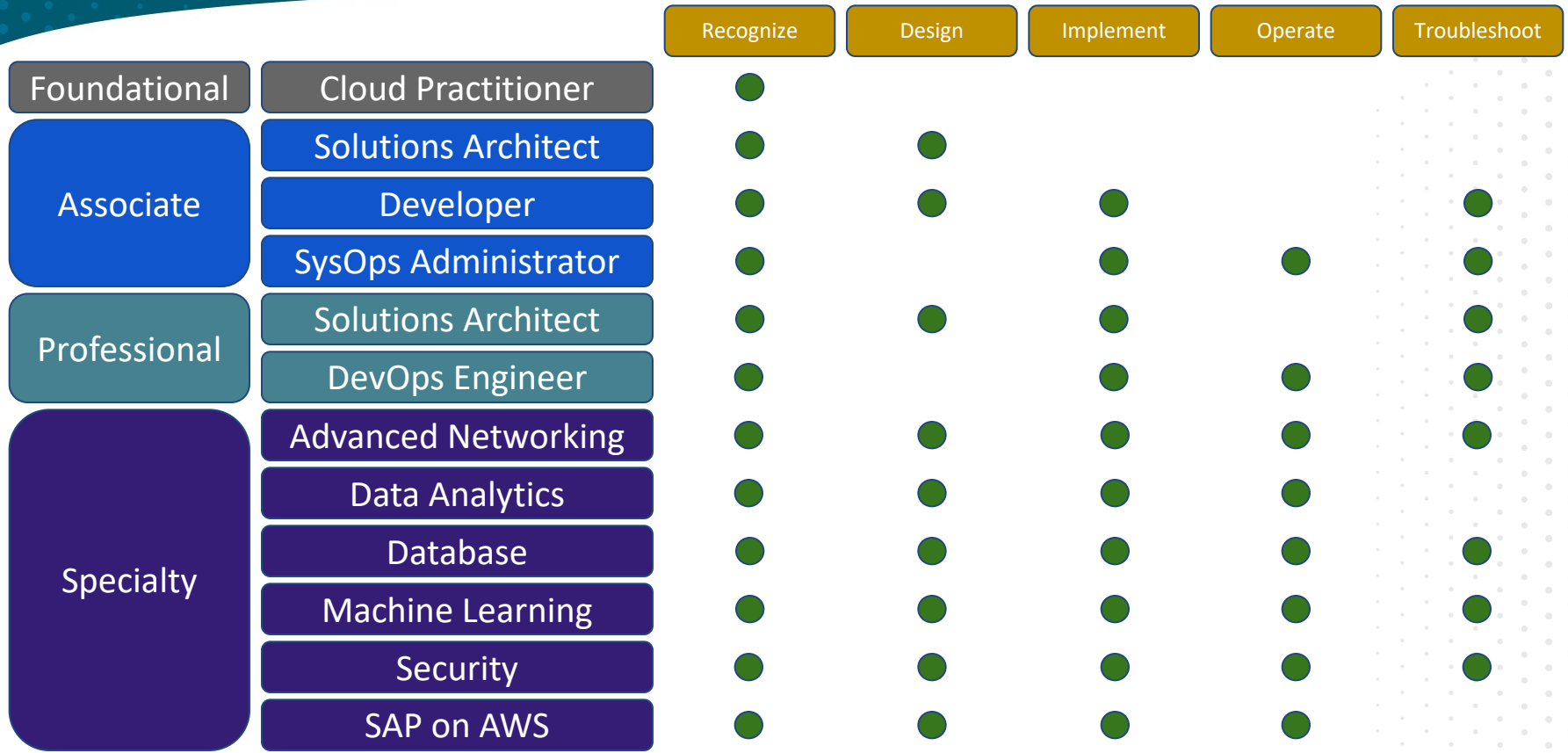
# AWS Certification Landscape



# AWS Certification Landscape



# AWS Certification Landscape




Pearson

# Question Breakdown

# Question and Answer Choices

**If your company wants to engage an AWS professional for an architecture review, what would be the available options? (pick two)**

A. AWS Well-Architected Tool
B. AWS Whitepapers
C. Amazon Partner Network
D. AWS Trusted Advisor
E. AWS Professional Services

# Correct Answer and Explanation

**Both of the correct options allow for an engagement with trained professionals. The other options are simply documentation or reports.**

A. AWS Well-Architected Tool
B. AWS Whitepapers
C. Amazon Partner Network
D. AWS Trusted Advisor
E. AWS Professional Services

# Question Domain 4: Billing and Pricing

# Question Domain Points

Compare and contrast the various pricing models for AWS

Recognize the various account structures in relation to AWS billing and pricing

Identify resources available for billing support

## Question Domain 4: Billing and Pricing

# AWS Compute Pricing Models

# AWS Free Tier Definitions

**12 Months Free**

- Small usage rate
- Specific resource types

# AWS Free Tier Definitions

| 12 Months Free | Always Free |
| --- | --- |
| ● Small usage rate<br>● Specific resource types | ● Never expire<br>● Small usage rate<br>● Think of it as a permanent discount |

# AWS Free Tier Definitions

| 12 Months Free | Always Free | Trial |
| --- | --- | --- |
| • Small usage rate<br>• Specific resource types | • Never expire<br>• Small usage rate<br>• Think of it as a permanent discount | • Short term<br>• Try before you buy<br>• Specific services |

# AWS Free Tier Definitions

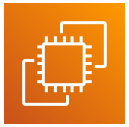
| 12 Months Free | Always Free | Trial |
| --- | --- | --- |
| • Small usage rate<br>• Specific resource types | • Never expire<br>• Small usage rate<br>• Think of it as a permanent discount | • Short term<br>• Try before you buy<br>• Specific services |

All of these can assist with learning AWS!

# AWS Free Tier Examples

12 Months Free

Amazon RDS

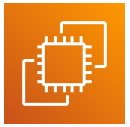


Amazon Elastic Compute Cloud (Amazon EC2)

# AWS Free Tier Examples

## 12 Months Free

Amazon RDS



Amazon Elastic Compute Cloud (Amazon EC2)

## Always Free

Amazon Simple Storage Service (Amazon S3)

AWS Lambda

# AWS Free Tier Examples

| 12 Months Free | Always Free | Trial |
| --- | --- | --- |
|  Amazon RDS |  Amazon Simple Storage Service (Amazon S3) |  Amazon Lightsail |
|  Amazon Elastic Compute Cloud (Amazon EC2) |  AWS Lambda |  Amazon GuardDuty |

# Compute Cost - EC2 Pricing

## Spot Instances

- No guaranteed pricing
- Pay for unused capacity
- Volatile
- Specify maximum bid
- +Specific duration
- +Multiple instance types
- +Multiple AZ

# Compute Cost - EC2 Pricing

## Spot Instances

- No guaranteed pricing
- Pay for unused capacity
- Volatile
- Specify maximum bid
- +Specific duration
- +Multiple instance types
- +Multiple AZ

## RIs/SPs

- Guaranteed pricing for 1-3 years
- +Capacity guarantee
- Variable up-front for more discount
- EC2 Savings Plans for more flexibility
- Compute Savings Plans for even more flexibility!

# Compute Cost - EC2 Pricing

| Spot Instances | RIs/SPs | On Demand Instances |
| --- | --- | --- |
| • No guaranteed pricing<br>• Pay for unused capacity<br>• Volatile<br>• Specify maximum bid<br>• +Specific duration<br>• +Multiple instance types<br>• +Multiple AZ | • Guaranteed pricing for 1-3 years<br>• +Capacity guarantee<br>• Variable up-front for more discount<br>• EC2 Savings Plans for more flexibility<br>• Compute Savings Plans for even more flexibility! | • Pay as you go<br>• No discount<br>• No capacity guarantee |

# Compute Cost - EC2 Pricing

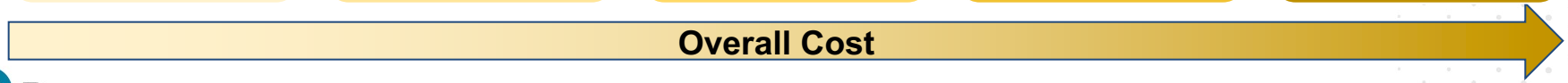
| Spot Instances | RIs/SPs | On Demand Instances | Dedicated Instances |
| --- | --- | --- | --- |
| • No guaranteed pricing<br>• Pay for unused capacity<br>• Volatile<br>• Specify maximum bid<br>• +Specific duration<br>• +Multiple instance types<br>• +Multiple AZ | • Guaranteed pricing for 1-3 years<br>• +Capacity guarantee<br>• Variable up-front for more discount<br>• EC2 Savings Plans for more flexibility<br>• Compute Savings Plans for even more flexibility! | • Pay as you go<br>• No discount<br>• No capacity guarantee | • Dedicated hardware<br>• Can share with non-dedicated VMs<br>• Per-region fee<br>• +Spot<br>• +Reservations<br>• +On Demand |

# Compute Cost - EC2 Pricing

| Spot Instances | RIs/SPs | On Demand Instances | Dedicated Instances | Dedicated Hosts |
|---|---|---|---|---|
| • No guaranteed pricing<br>• Pay for unused capacity<br>• Volatile<br>• Specify maximum bid<br>• +Specific duration<br>• +Multiple instance types<br>• +Multiple AZ | • Guaranteed pricing for 1-3 years<br>• +Capacity guarantee<br>• Variable up-front for more discount<br>• EC2 Savings Plans for more flexibility<br>• Compute Savings Plans for even more flexibility! | • Pay as you go<br>• No discount<br>• No capacity guarantee | • Dedicated hardware<br>• Can share with non-dedicated VMs<br>• Per-region fee<br>• +Spot<br>• +Reservations<br>• +On Demand | • Dedicated hardware<br>• Single instance type<br>• Pay for host capacity, not instance<br>• +Reservations<br>• +On Demand |

# Compute Cost - EC2 Pricing

| Spot Instances | RIs/SPs | On Demand Instances | Dedicated Instances | Dedicated Hosts |
|---|---|---|---|---|
| • No guaranteed pricing<br>• Pay for unused capacity<br>• Volatile<br>• Specify maximum bid<br>• +Specific duration<br>• +Multiple instance types<br>• +Multiple AZ | • Guaranteed pricing for 1-3 years<br>• +Capacity guarantee<br>• Variable up-front for more discount<br>• EC2 Savings Plans for more flexibility<br>• Compute Savings Plans for even more flexibility! | • Pay as you go<br>• No discount<br>• No capacity guarantee | • Dedicated hardware<br>• Can share with non-dedicated VMs<br>• Per-region fee<br>• +Spot<br>• +Reservations<br>• +On Demand | • Dedicated hardware<br>• Single instance type<br>• Pay for host capacity, not instance<br>• +Reservations<br>• +On Demand |



# Question Breakdown

# Question and Answer Choices

**Your performance testing team wants to execute 24 hour tests on many different instance types for an application to determine which is the most efficient. Which of the EC2 pricing models would you recommend?**

A. Spot pricing
B. Reserved instances
C. On-demand pricing
D. Dedicated instances

# Correct Answer and Explanation

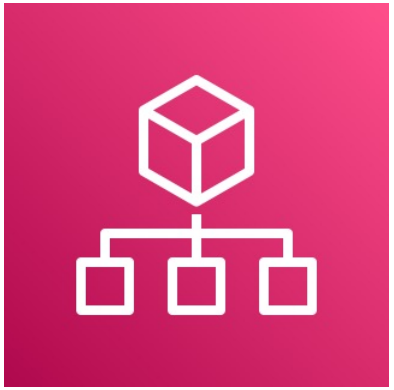
**On-demand pricing is the most flexible model and would allow for the testing of many different instance types with no commitments or contracts.**

A. Spot pricing
B. Reserved instances
C. On-demand pricing
D. Dedicated instances

## Question Domain 4: Billing and Pricing

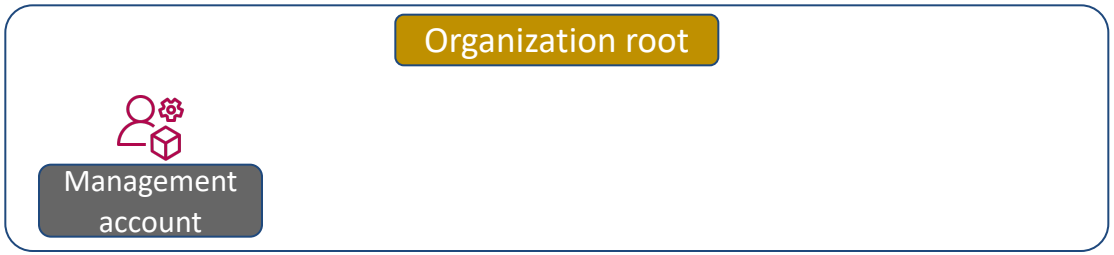
# AWS Account Structures

# AWS Organizations Basics



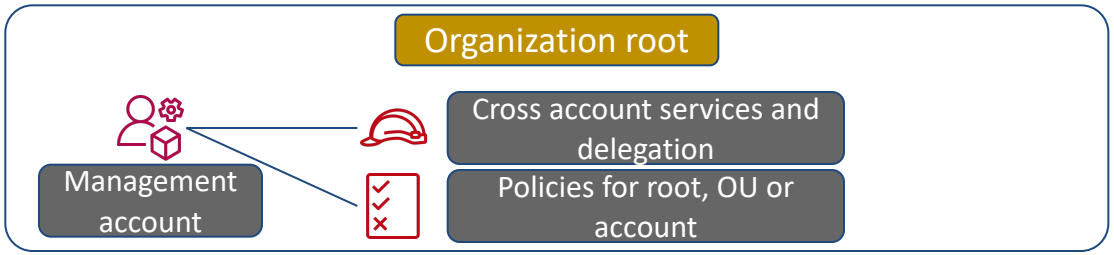
- Account scope
- Multiple account management service
- Organizational Unit (OU structure)
- Central billing
- Shared reservations
- Shared savings plans
- Central policy management

# AWS Organizations Architecture



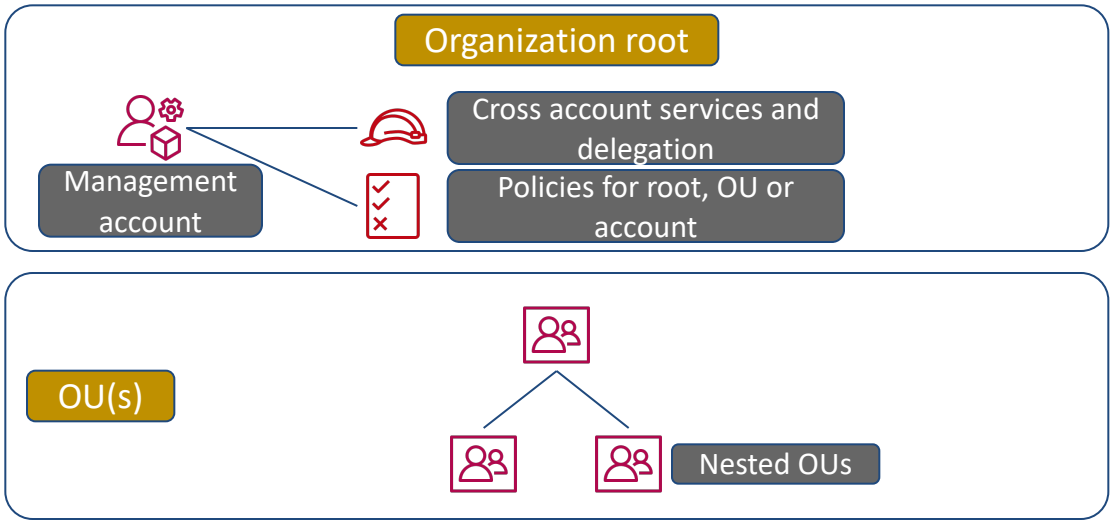

The Management account is where the Organizations service is enabled and becomes the organization root

# AWS Organizations Architecture



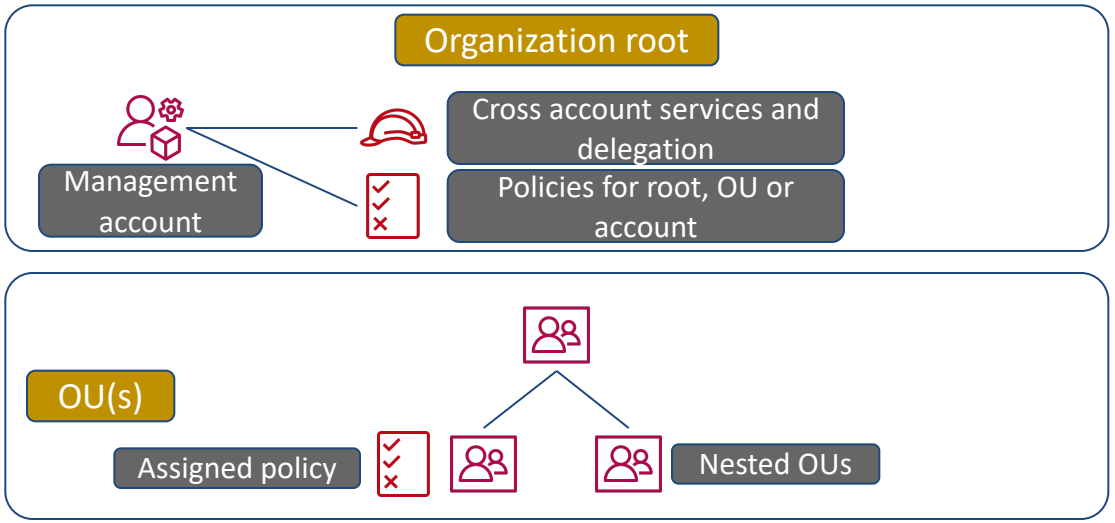

Create policies or delegate administrative rights in the management account

# AWS Organizations Architecture



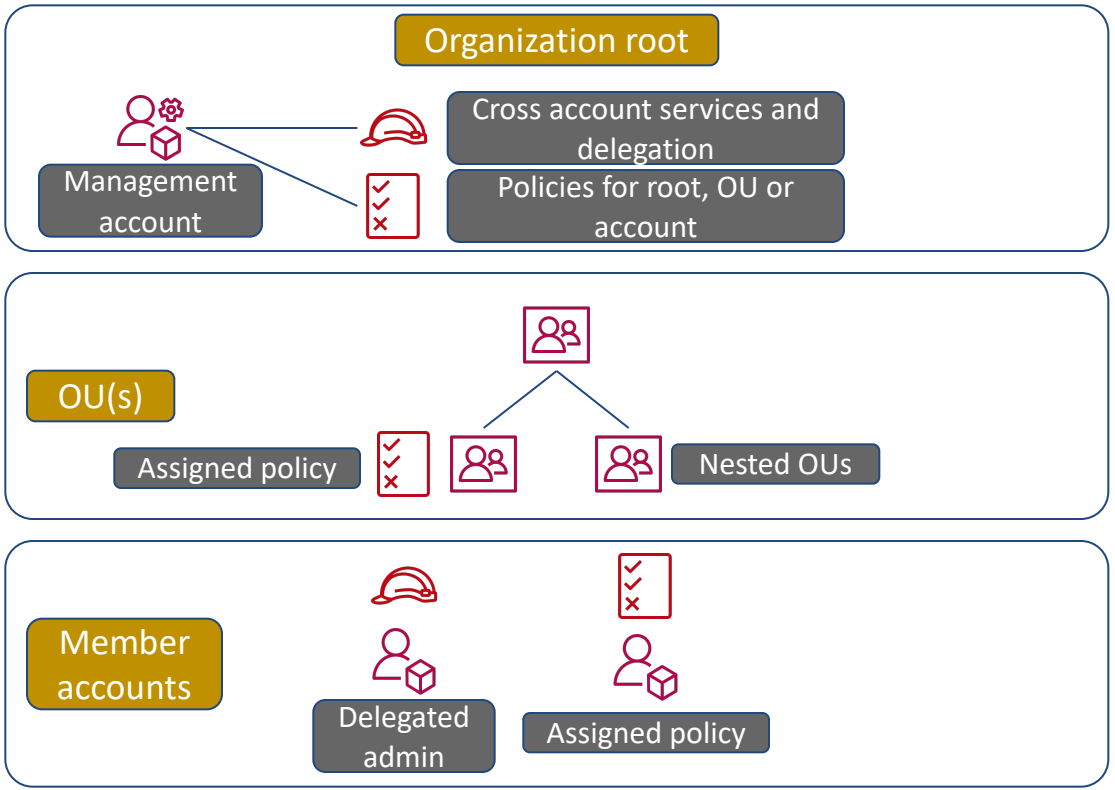

OUs can contain other OUs in a reverse tree structure from the root

# AWS Organizations Architecture



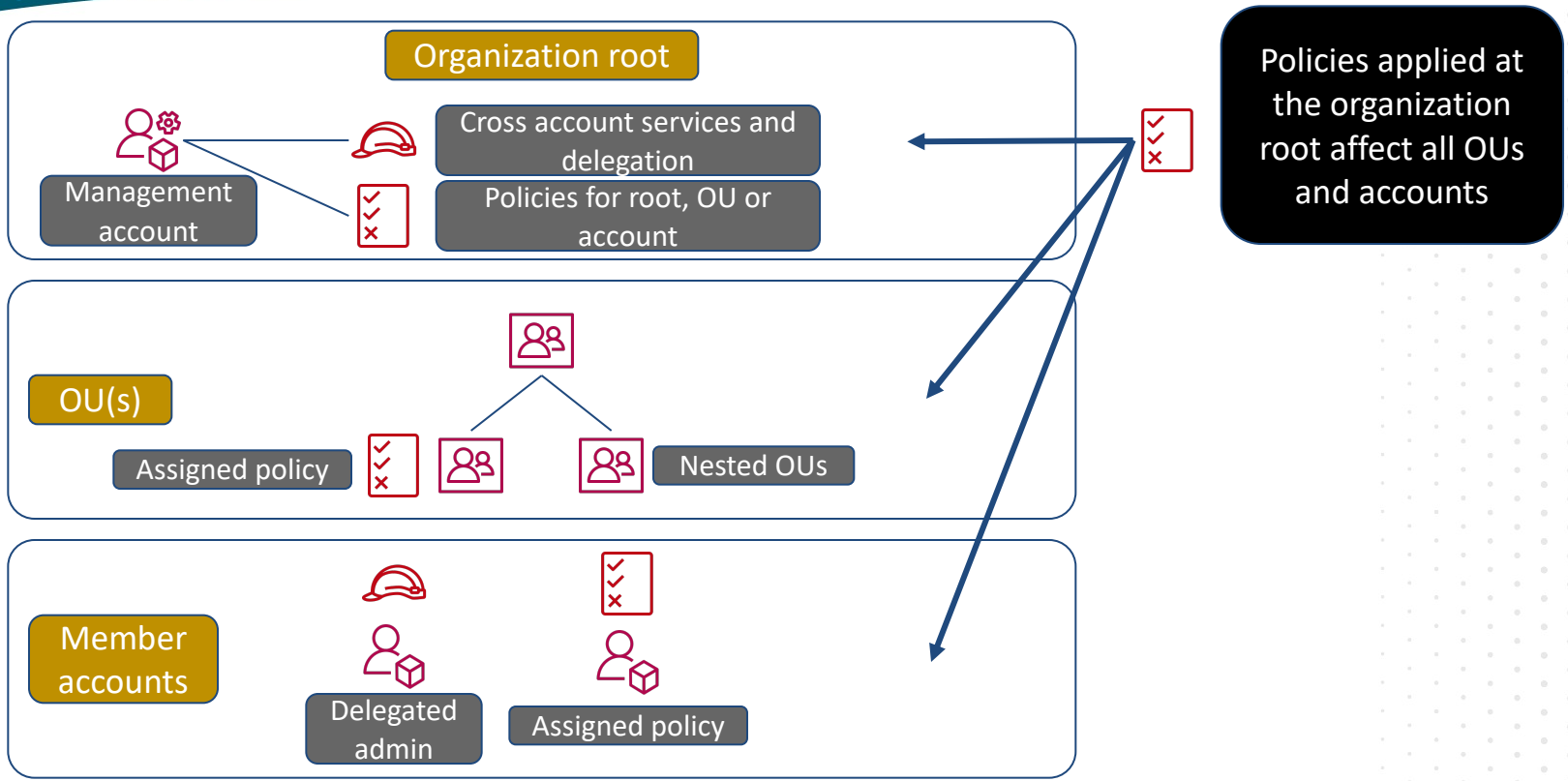

Policies can be assigned to OUs to take advantage of inheritance

# AWS Organizations Architecture




Policies can also be assigned directly to accounts instead of inherited via OU

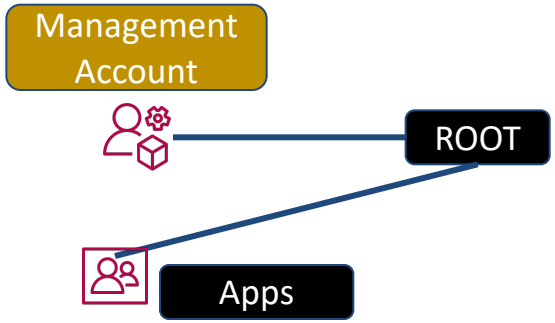
# AWS Organizations Architecture



# Multiple Accounts Using Organizations

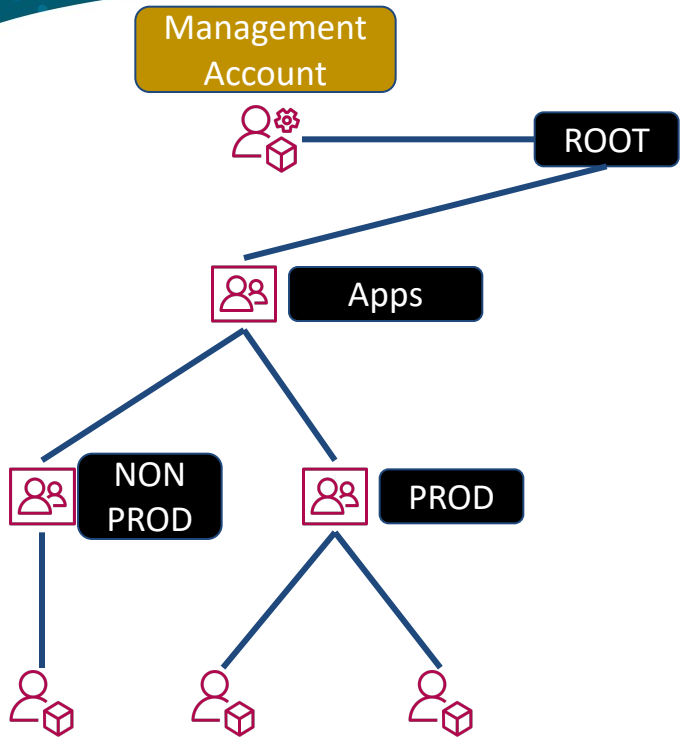

The Management account has very few resources such as SSO

# Multiple Accounts Using Organizations



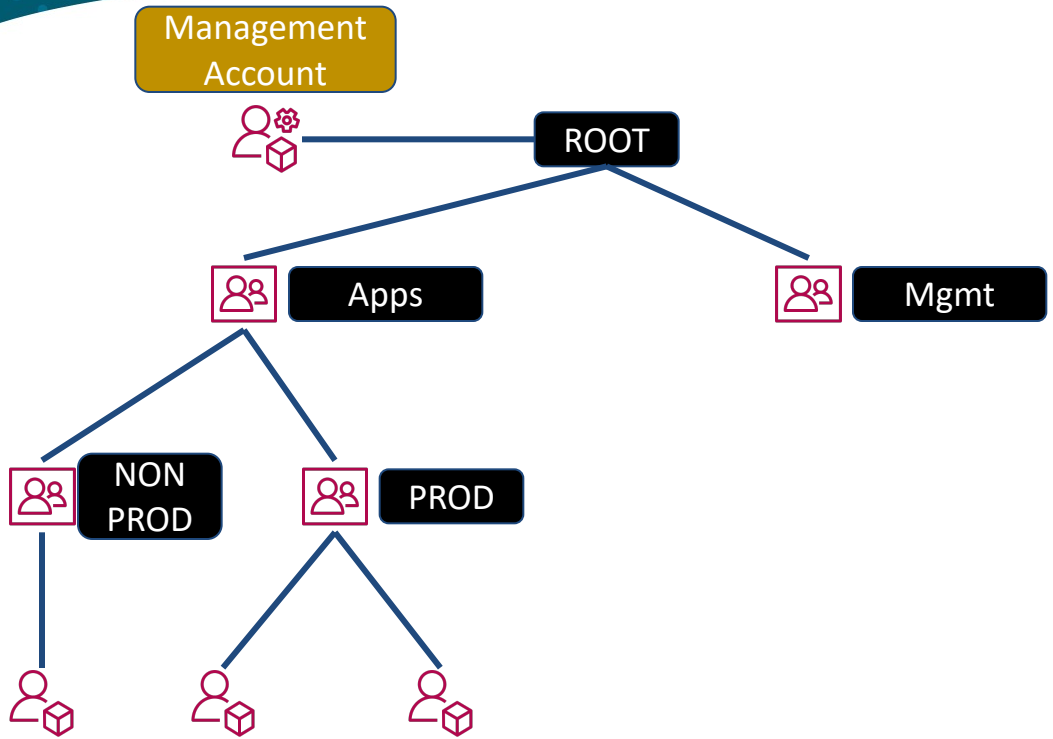

The Apps OU is for all product-related infrastructure

# Multiple Accounts Using Organizations



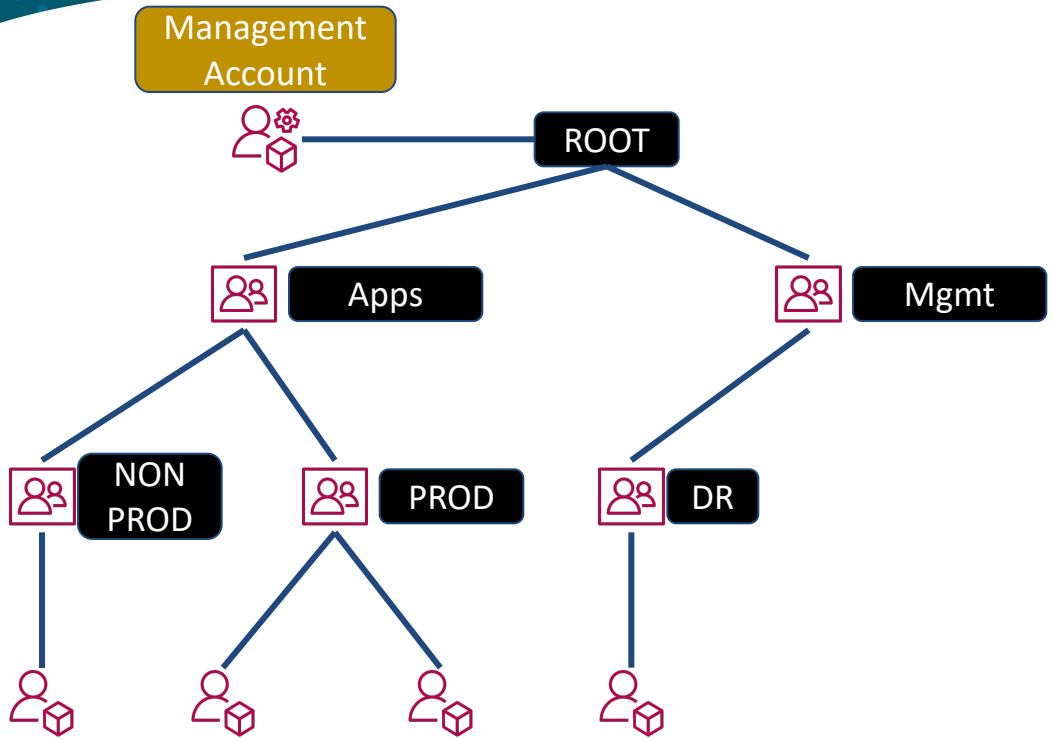

Create OUs for Non-prod and Prod environments

# Multiple Accounts Using Organizations



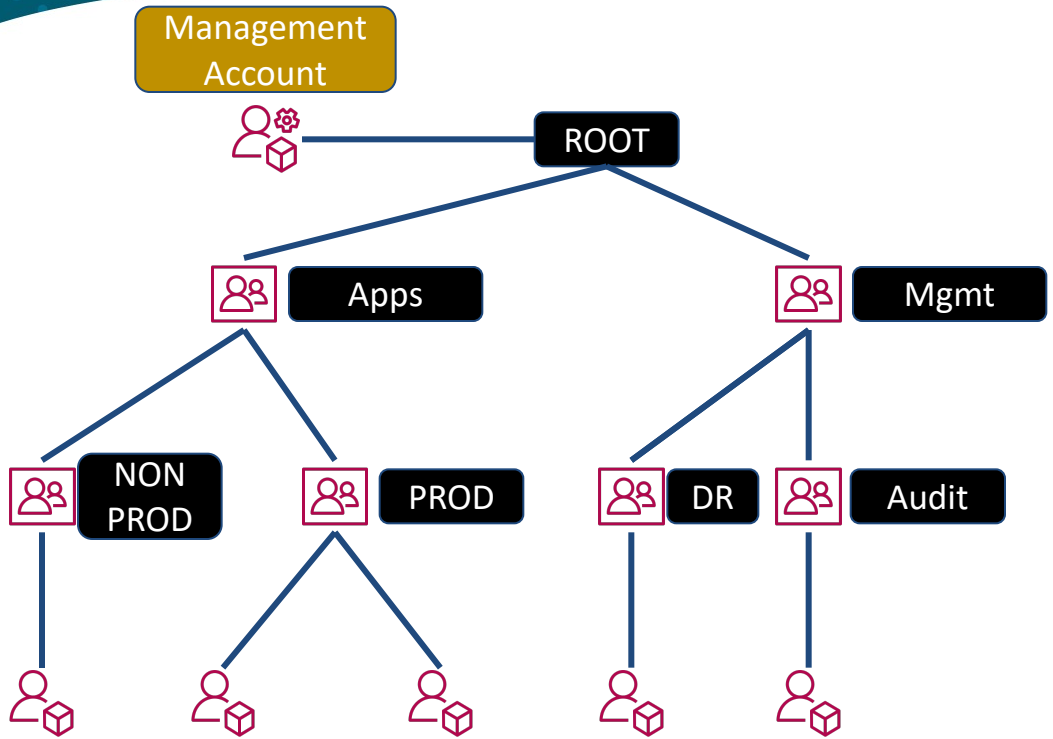

Another OU for all management activities

# Multiple Accounts Using Organizations



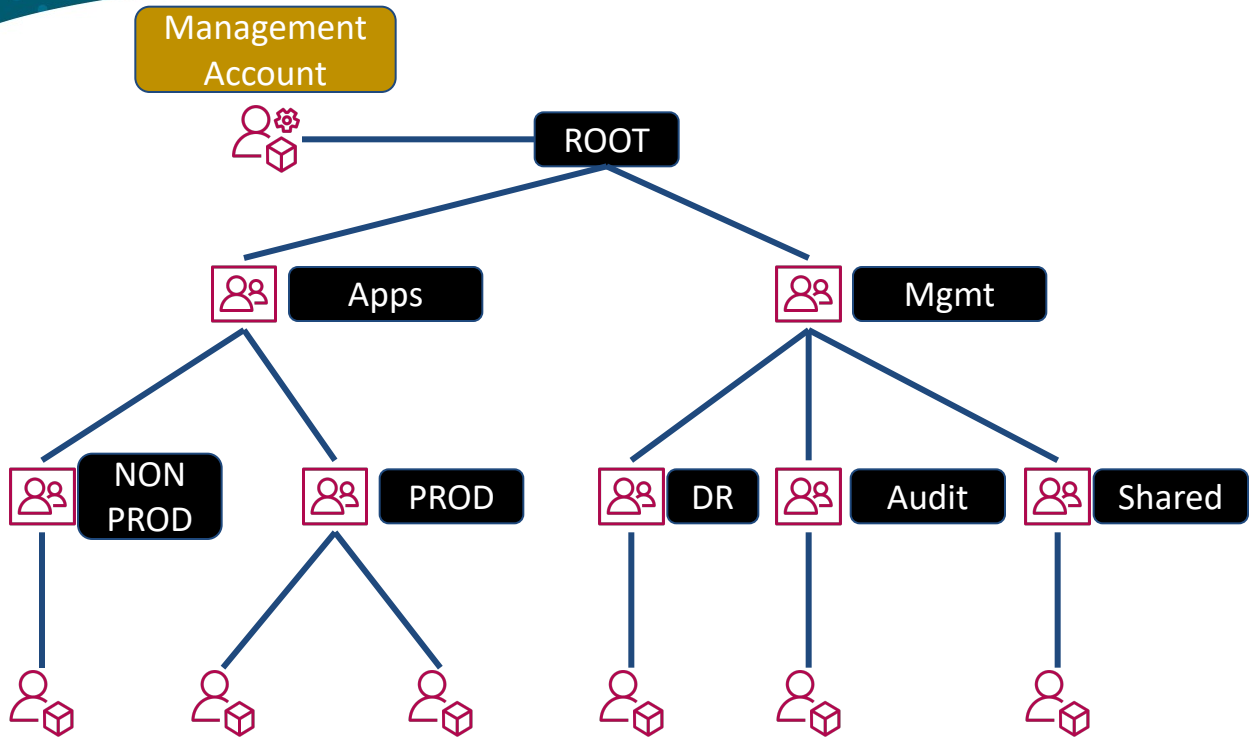

Business continuity is isolated into an OU and separate account

# Multiple Accounts Using Organizations




So is security and compliance auditing infrastructure

# Multiple Accounts Using Organizations




Finally, all shared resources can be placed in a separate OU and account

# Question Breakdown

# Question and Answer Choices

**If your company wants to engage an AWS professional for an architecture review, what would be the available options? (pick two)**

A. AWS Well-Architected Tool
B. AWS Whitepapers
C. Amazon Partner Network
D. AWS Trusted Advisor
E. AWS Professional Services

# Correct Answer and Explanation

**Both of the correct options allow for an engagement with trained professionals. The other options are simply documentation or reports.**

A. AWS Well-Architected Tool
B. AWS Whitepapers
C. Amazon Partner Network
D. AWS Trusted Advisor
E. AWS Professional Services

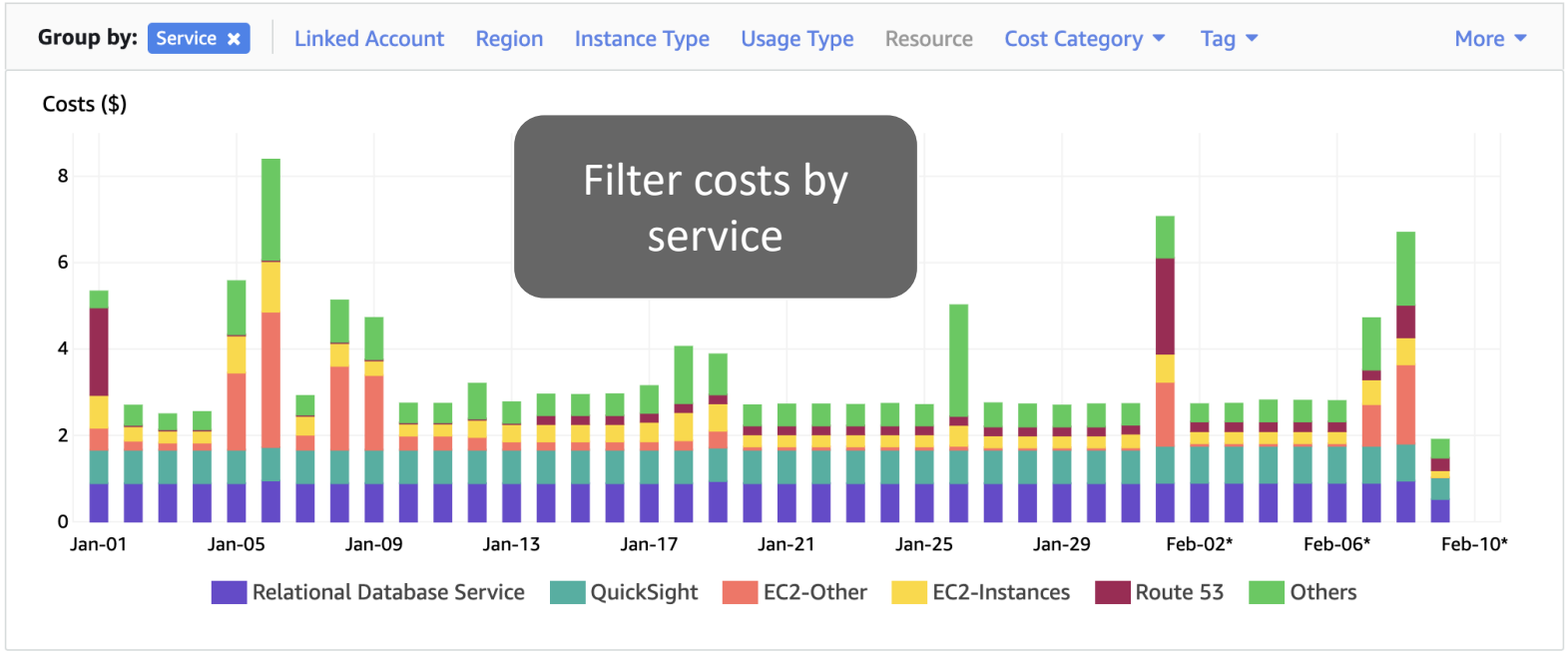
## Question Domain 4: Billing and Pricing

# Billing Support Resources

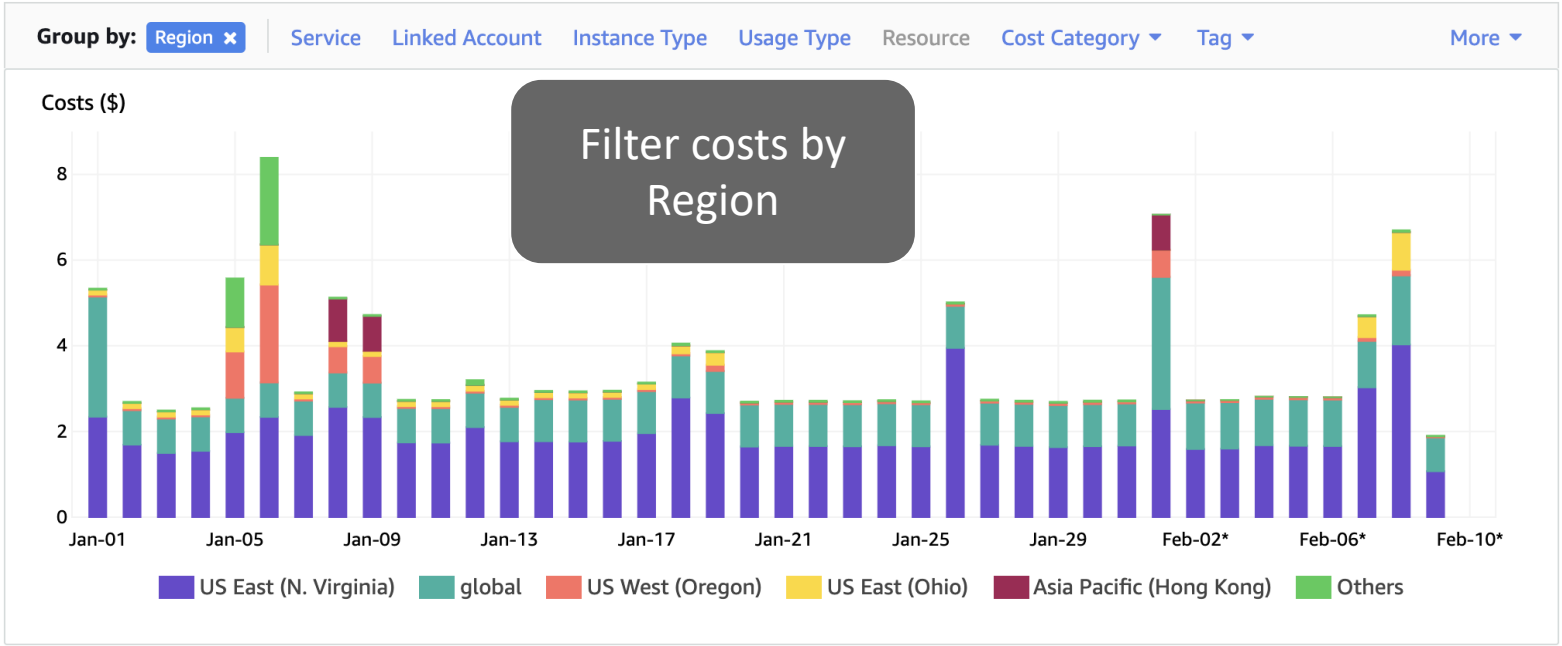
# Cost Explorer Basics

- Enable via Billing Console
- View 24 month window
- Create reports
- Filter and sort
- Cost Allocation Tag filters
- Reserved instance reports
- Rightsizing recommendations

# Cost Explorer Example

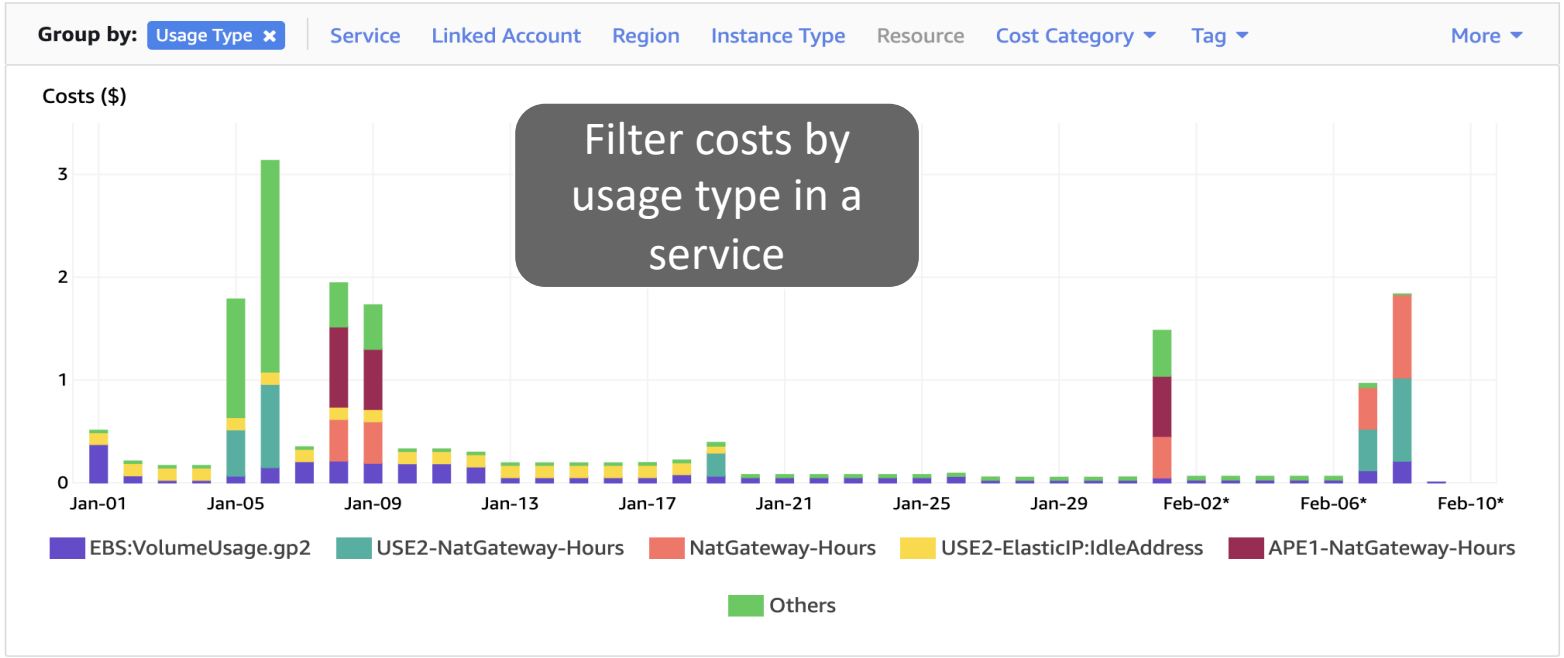


# Cost Explorer Example




Pearson

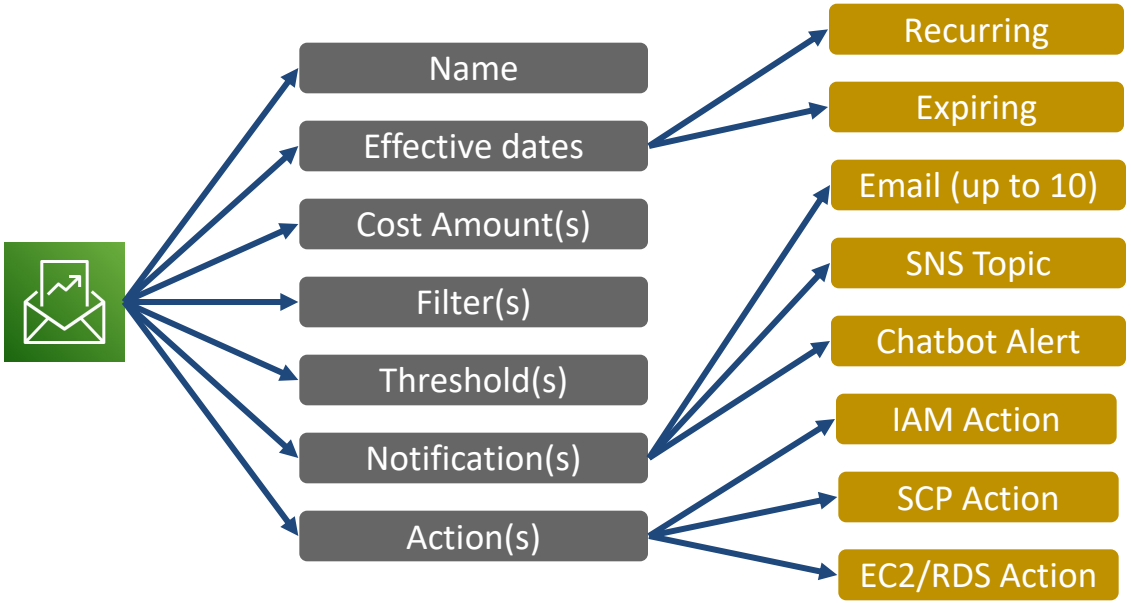
# Cost Explorer Example



# AWS Budgets Basics

- Monitor cost
- Monitor utilization
- Monitor coverage
- Passive notifications
- Active actions
- Filters same as CE

# Cost Budgets



# Cost Allocation Tag Basics

- Associate tags with billing
- Enable in AWS console
- Use in individual accounts
- Use in management accounts
- Good reason for tag strategy
- AWS-generated tags
- User-defined tags

# Question Breakdown

# Question and Answer Choices

**What AWS service/feature would you use to prevent all expenditures in an AWS account when reaching a specific threshold?**

A. AWS Billing alarm
B. AWS Budgets - cost budget
C. AWS Cost Explorer
D. AWS does not have any features to meet this requirement

# Correct Answer and Explanation

**There are no native options in AWS to prevent spend as an active guardrail.**

A. AWS Billing alarm
B. AWS Budgets - cost budget
C. AWS Cost Explorer
D. AWS does not have any features to meet this requirement

# Wrap up and Q&A