AWS Certified Cloud Practitioner Foundational Crash Course (CLF-C02)

Chad Smith

Principal Cloud Architect

Pearson

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**
Partial Credit	**0**
Penalty for guessing	**0**

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

Pearson

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

Pearson

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

Recommended AWS Knowledge

AWS Cloud concepts

Pearson

Recommended AWS Knowledge

Security and compliance within the AWS Cloud

Recommended AWS Knowledge

Understanding of the core AWS services

Recommended AWS Knowledge

Understanding of the economics of the AWS Cloud

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	24

Question Domain 1 Task Statements

Define the benefits of the AWS Cloud

Identify design principles of the AWS Cloud

Understand the benefits of and strategies for migration to the AWS Cloud

Understand concepts of cloud economics

Exam Guide Exam Content

Question Domains	%
Cloud Concepts	24
Security and Compliance	30

Question Domain 2 Task Statements

Understand the AWS shared responsibility model

Understand AWS Cloud security, governance, and compliance concepts

Identify AWS access management capabilities

Identify components and resources for security

Exam Guide Exam Content

Question Domains	%
Cloud Concepts	24
Security and Compliance	30
Cloud Technology and Services	34

Question Domain 3 Task Statements

- Define methods of deploying and operating in the AWS Cloud
- Define the AWS global infrastructure
- Identify AWS compute services
- Identify AWS database services
- Identify AWS network services
- Identify AWS storage services
- Identify AWS artificial intelligence and machine learning (AI/ML) services, and analytics services
- Identify services from other in-scope AWS service categories

Exam Guide Exam Content

Question Domains	%
Cloud Concepts	24
Security and Compliance	30
Cloud Technology and Services	34
Billing, Pricing, and Support	12

Question Domain 4 Points

Compare AWS pricing models

Understand resources for billing, budget, and cost management

Identify AWS technical resources and AWS Support options

AWS Certification Strategies

Question Format

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

All questions are multiple-choice

A. 4
B. Answer
C. Choices
D. Total

Question Format

Question details are RELEVANT

No mixing of question domains

No trick questions

A. Answers are reasonable
B. Many are functional solutions
C. Every word counts

Pearson

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 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!

Pearson

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**.

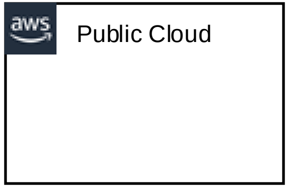
You can do these in ways not possible using on-premises data centers!

Question Domain 1: Cloud Concepts

Cloud Basics

Cloud Deployment Models

Public Cloud

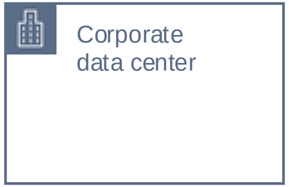


Public Cloud

- All infrastructure hosted by the provider
- Subscription model
- Shared tenancy model

Cloud Deployment Models

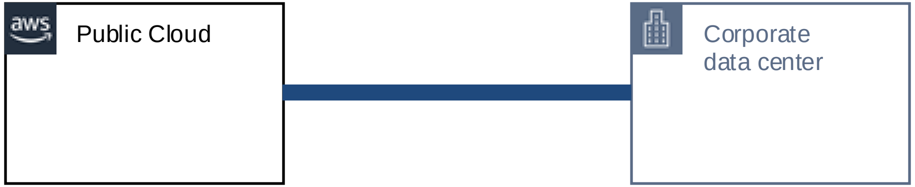
Private Cloud



- All infrastructure hosted by the customer
- All applications hosted by the customer
- Bare metal hardware
- On-premises infrastructure

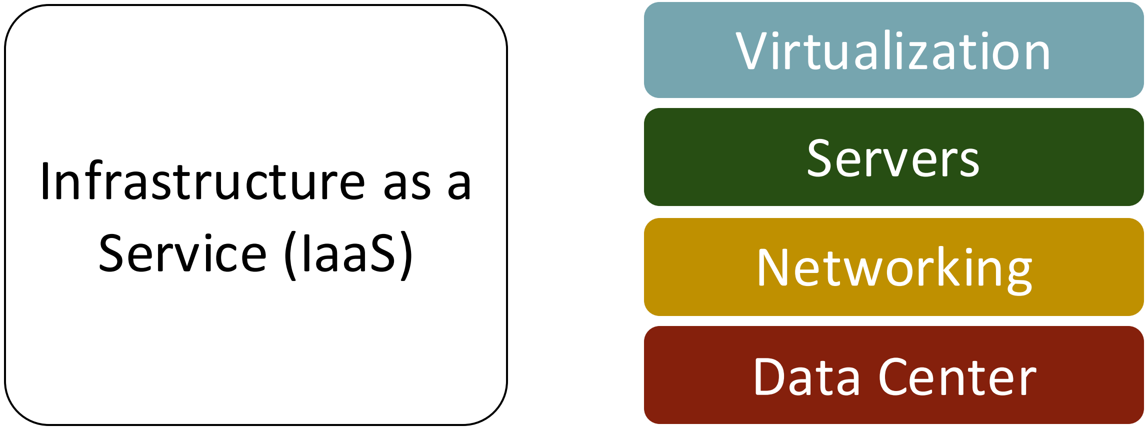
Cloud Deployment Models

Hybrid Cloud



- Combination of any 2 of public or private cloud deployments
- Often requires private networking infrastructure between the individual deployments

Cloud Service Models



Infrastructure as a Service (IaaS)

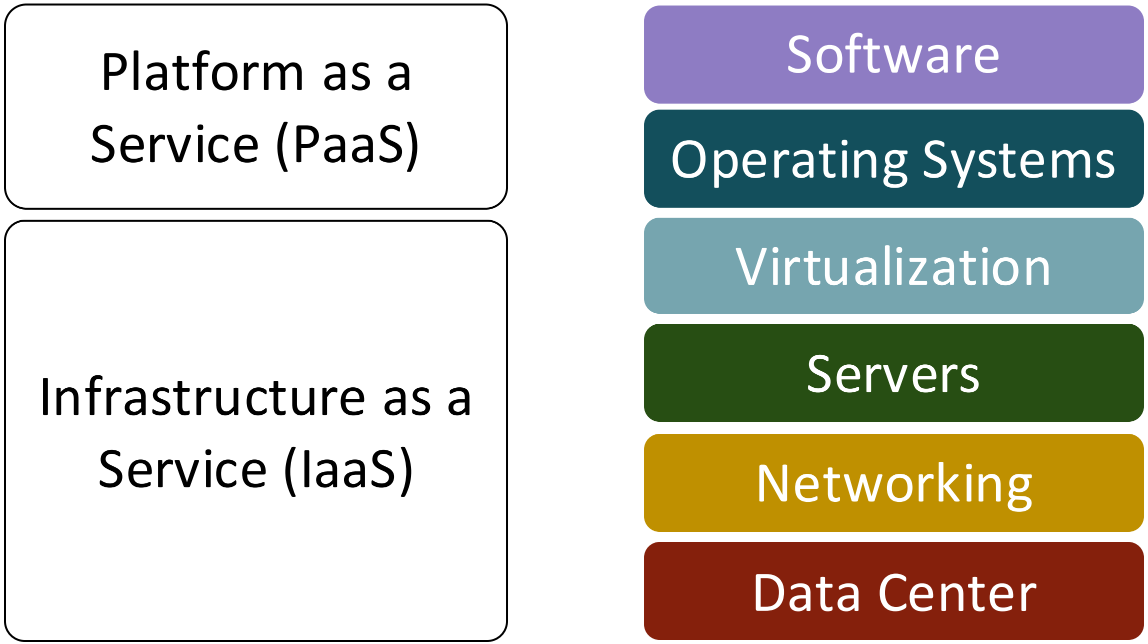
Virtualization

Servers

Networking

Data Center

Cloud Service Models



Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Software

Operating Systems

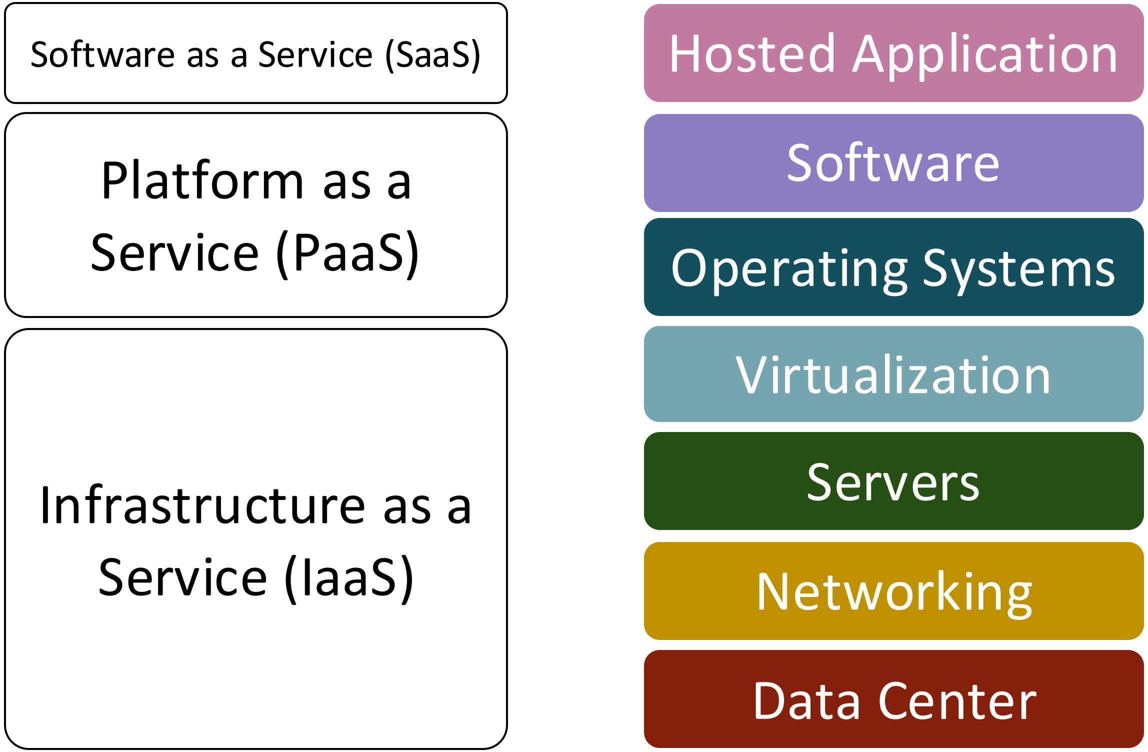
Virtualization

Servers

Networking

Data Center

Cloud Service Models



Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Hosted Application

Software

Operating Systems

Virtualization

Servers

Networking

Data Center

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

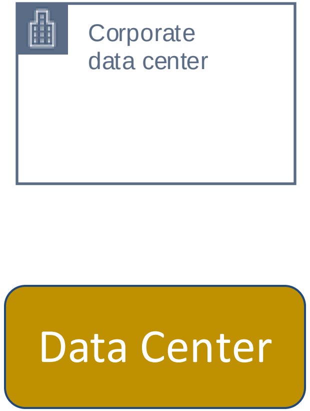
What is CapEx?

- 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

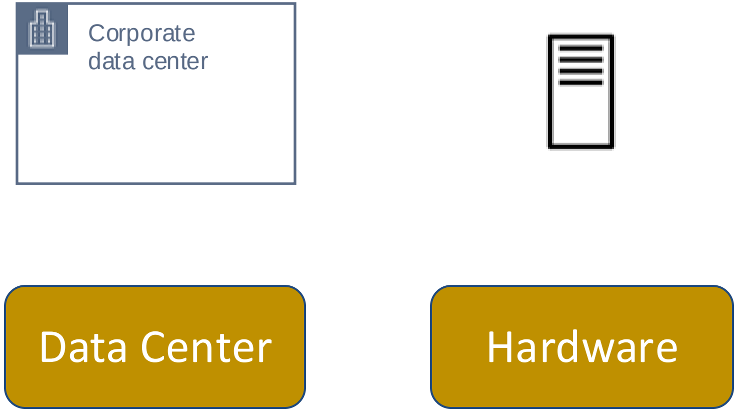
TCO - Total Cost of Ownership



Corporate data center

Data Center

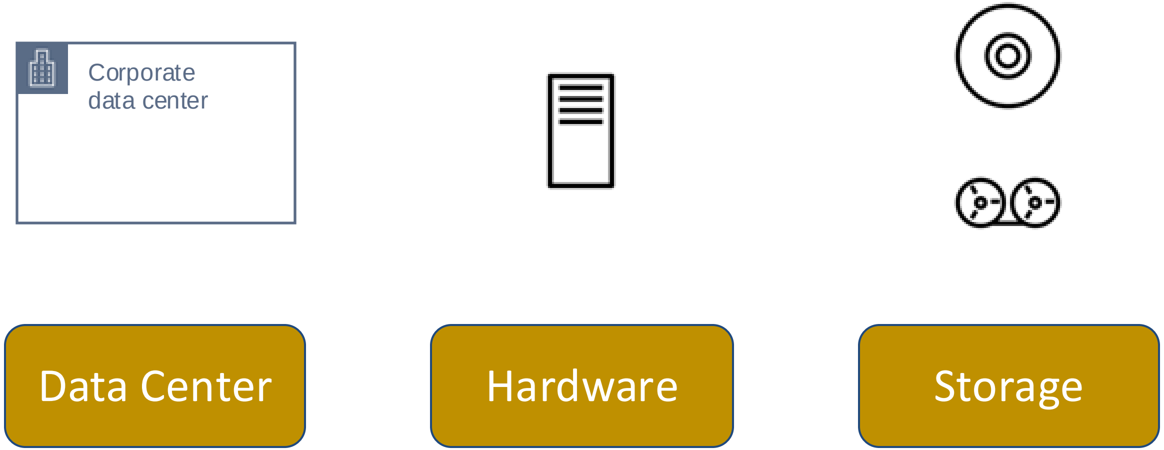
TCO - Total Cost of Ownership



Data Center

Hardware

TCO - Total Cost of Ownership

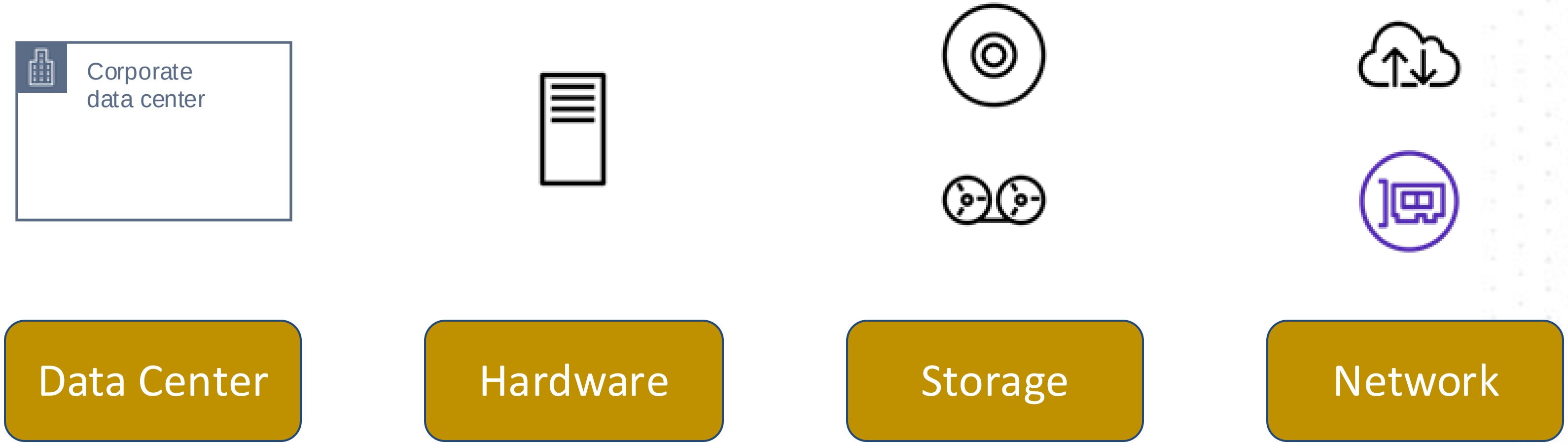


Data Center

Hardware

Storage

TCO - Total Cost of Ownership



Data Center

Hardware

Storage

Network

TCO - Total Cost of Ownership

Corporate
data center

Data Center

Hardware

Storage

Network

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

What is missing from this list?

KTLO - Keep The Lights On

- Switch primary to secondary power source
- Identify temperature anomalies
- Rack and stack new servers
- Switch backup tapes

Any zero-sum game operation

KTLO - Keep The Lights On

- User account management
- OS updates
- Disk space management
- Troubleshooting memory or disk errors

More OS-based resources = more operations

KTLO - Keep The Lights On

- Constant cycle of OS upgrades
- Constant cycle of firmware updates
- Configuration drift causes instability

Prevents corporate agility

KTLO - Keep The Lights On

- Inventory efforts
- OS upgrades
- Configuration management
- Hardware retirement
- Broken hardware replacement

Does not scale

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

Stop guessing your capacity needs

Scale horizontally using automation based on metrics

Design Principles

Stop guessing your capacity needs

Test systems at production scale

Deploy using IAC and test full-size environments in a cost effective way

Design Principles

Stop guessing your capacity needs

Test systems at production scale

Automate to make architectural experimentation easier

Replicate workloads at low cost and test impact of changes

Design Principles

Stop guessing your capacity needs

Test systems at production scale

Automate to make architectural experimentation easier

Allow for evolutionary architectures

Decouple infrastructures so technology replacement is easily accomplished

Pearson

Design Principles

Stop guessing your capacity needs

Test systems at production scale

Automate to make architectural experimentation easier

Allow for evolutionary architectures

Drive architectures using data

Establish performance baselines and explore data-driven improvement possibilities

Design Principles

- Stop guessing your capacity needs
- Test systems at production scale
- Automate to make architectural experimentation easier
- Allow for evolutionary architectures
- Drive architectures using data
- Improve through game days

Validate playbooks on test (or actual) environments frequently

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.

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.

Performance Efficiency

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

Security

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

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.

Cost Optimization

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

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.

Cloud Adoption Framework (CAF) Definition

The AWS Cloud Adoption Framework leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Best practices - you need to learn the Well-Architected Framework!

Cloud Adoption Framework (CAF) Definition

The AWS Cloud Adoption Framework leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Business outcomes - more than just reducing technology spend!

Cloud Adoption Framework (CAF) Definition

The AWS Cloud Adoption Framework leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Innovative - you can't rely on legacy strategies to succeed!

Cloud Adoption Framework (CAF) Definition

The AWS Cloud Adoption Framework leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Iteratively evolve - requires a philosophical change for architecture

CAF Perspectives

Business

People

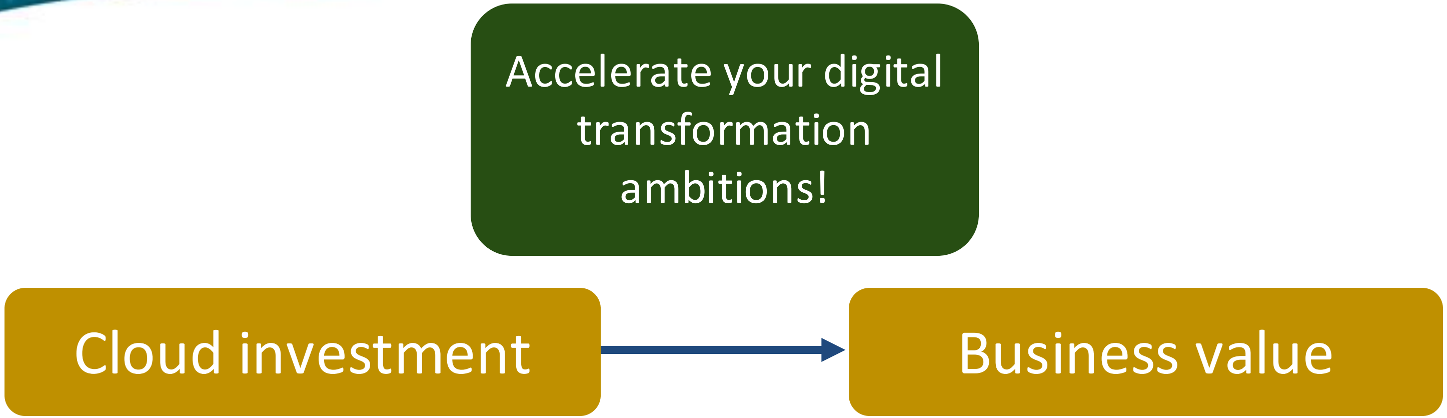
Governance

Platform

Security

Operations

Business Perspective



Accelerate your digital transformation ambitions!

Cloud investment

Business value

People Perspective

Bridge between technology and business

This requires a big philosophical change in the organization

Change becomes business as normal

Governance Perspective

Maximize organization benefits

Orchestrate and execute initiatives with transparency

Minimize transformation-related risks

Pearson

Platform Perspective

Enterprise-grade, scalable, hybrid cloud platform

Democratized advanced technologies at work!

Platform Perspective

Enterprise-grade, scalable, hybrid cloud platform

Modernize existing workloads

Utilize current, reliable, performant managed services

Platform Perspective

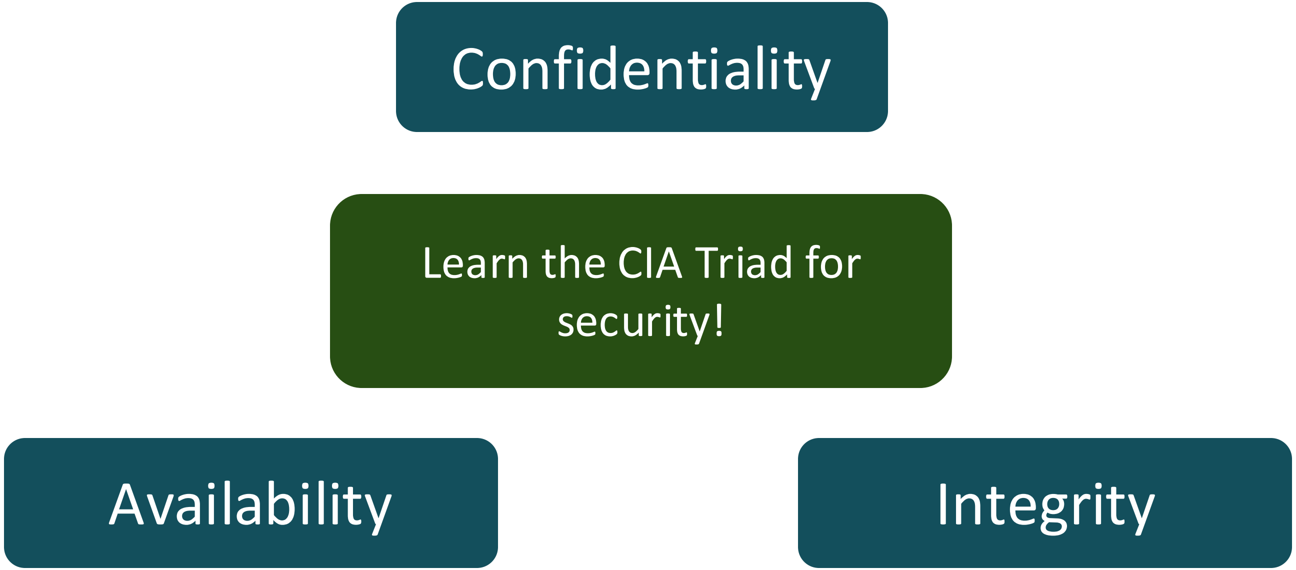
Enterprise-grade, scalable, hybrid cloud platform

Modernize existing workloads

Implement new cloud-native solutions

Use AWS building blocks to meet your requirements without compromise!

Security Perspective



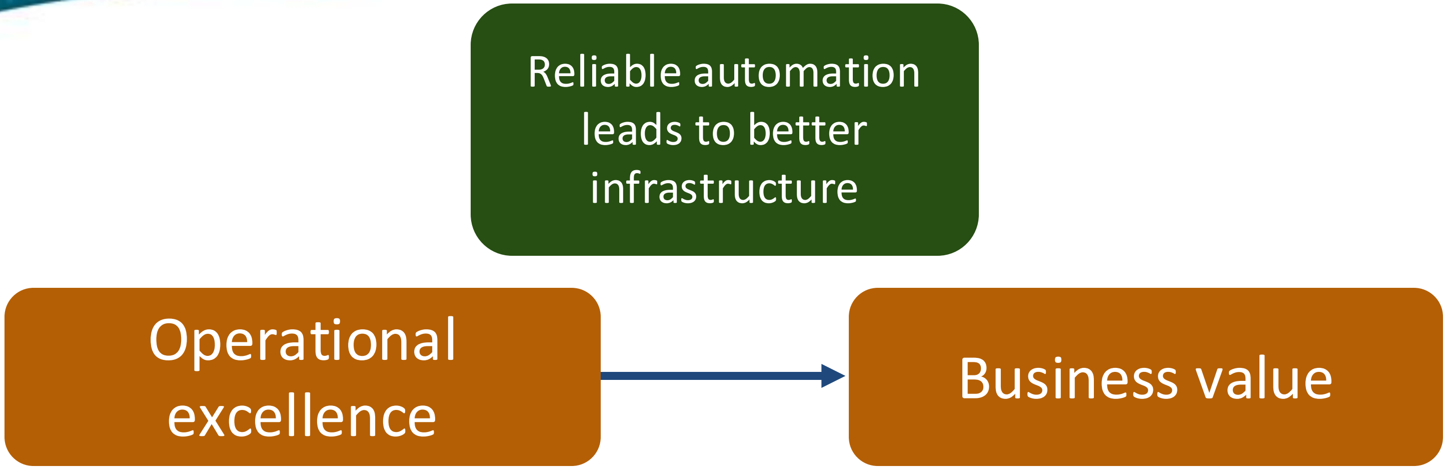
Confidentiality

Learn the CIA Triad for security!

Availability

Integrity

Operations Perspective



Reliable automation leads to better infrastructure

Operational excellence

Business value

CAF Benefits

Reduced business risk

The shared responsibility model means AWS owns many controls

CAF Benefits

Reduced business risk

Improved environmental, social and governance (ESG) performance

Use more efficient infrastructure with managed services

CAF Benefits

Reduced business risk

Improved environmental, social and governance (ESG) performance

Increased revenue

With AWS, you can deploy more reliable, performant workloads

CAF Benefits

Reduced business risk

Improved environmental, social and governance (ESG) performance

Increased revenue

Increased operational efficiency

Reduced Total Cost of Ownership (TCO) with AWS services

6 Rs of Cloud Migration

Rehost

Lift and shift, migrate to VMs in the CSP with few changes

6 Rs of Cloud Migration

Rehost

Replatform

Migrate from VM to PaaS to reduce overhead, still few changes

6 Rs of Cloud Migration

Rehost

Replatform

Repurchase

Often combined with retiring, requires switching to new software, usually SaaS

6 Rs of Cloud Migration

Rehost

Replatform

Repurchase

Re-architect to be cloud native

Refactor

6 Rs of Cloud Migration

Rehost

Replatform

Repurchase

Refactor

Retire

Stop using the app entirely rather than migrate it

6 Rs of Cloud Migration

Rehost

Replatform

Repurchase

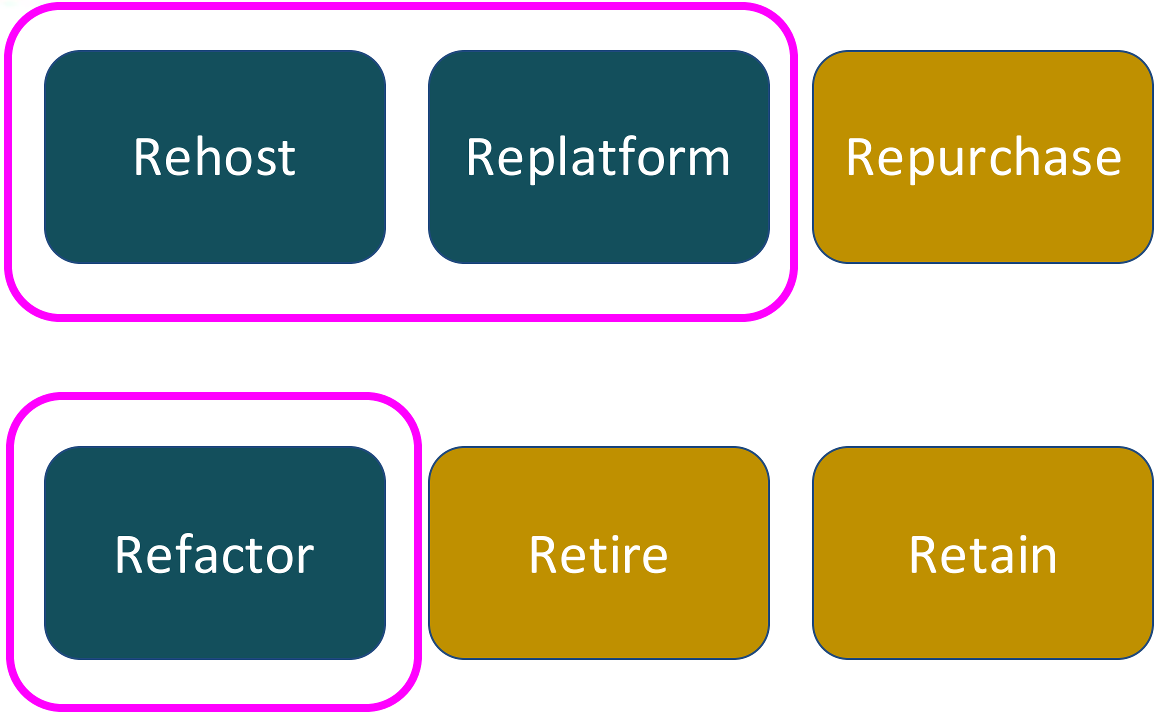
Refactor

Retire

Retain

Maintain the app on-premises rather than migrate

6 Rs of Cloud Migration



Rehost

Replatform

Repurchase

Refactor

Retire

Retain

These are in-scope for cloud migrations

Question Breakdown

Pearson

Question and Answer Choices

An architect is planning a migration from an on-premises infrastructure to a public cloud. There is a requirement to keep the migration as easy as possible while reducing operational overhead if possible.

Which cloud migration strategy should the architect recommend?

A. **Rehost**
B. **Replatform**
C. **Repurchase**
D. **Refactor**
E. **Retire**

Correct Answer

Replatform

A. Rehost
B. Replatform
C. Repurchase
D. Refactor
E. Retire

Question Domain 2: Security and Compliance

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

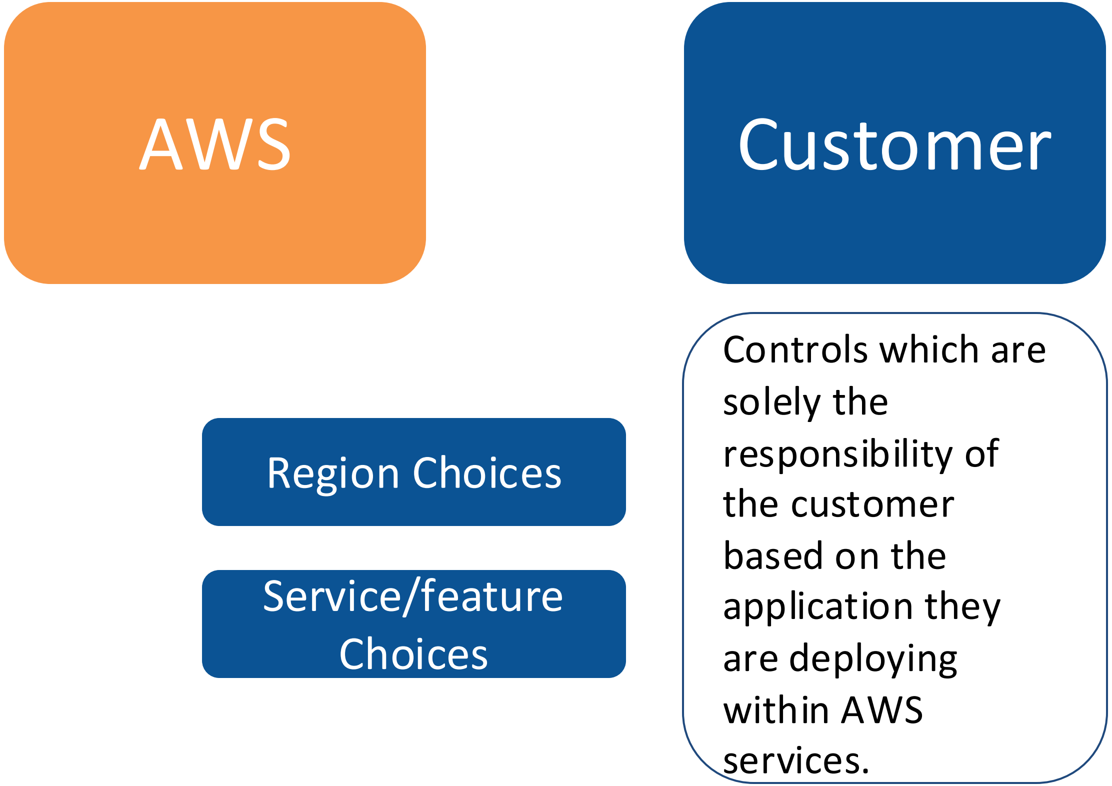
AWS

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

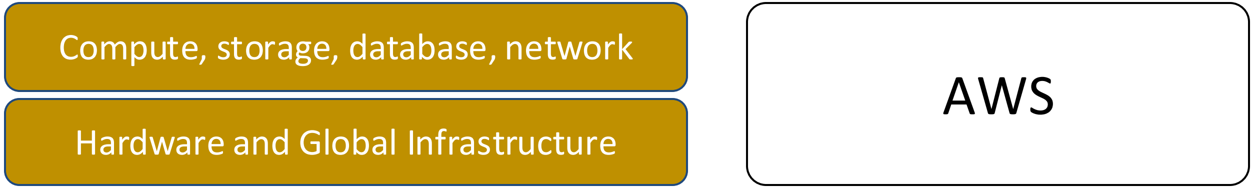
Region Choices

Service/feature Choices

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

Pearson

Shared Responsibility Model - IaaS

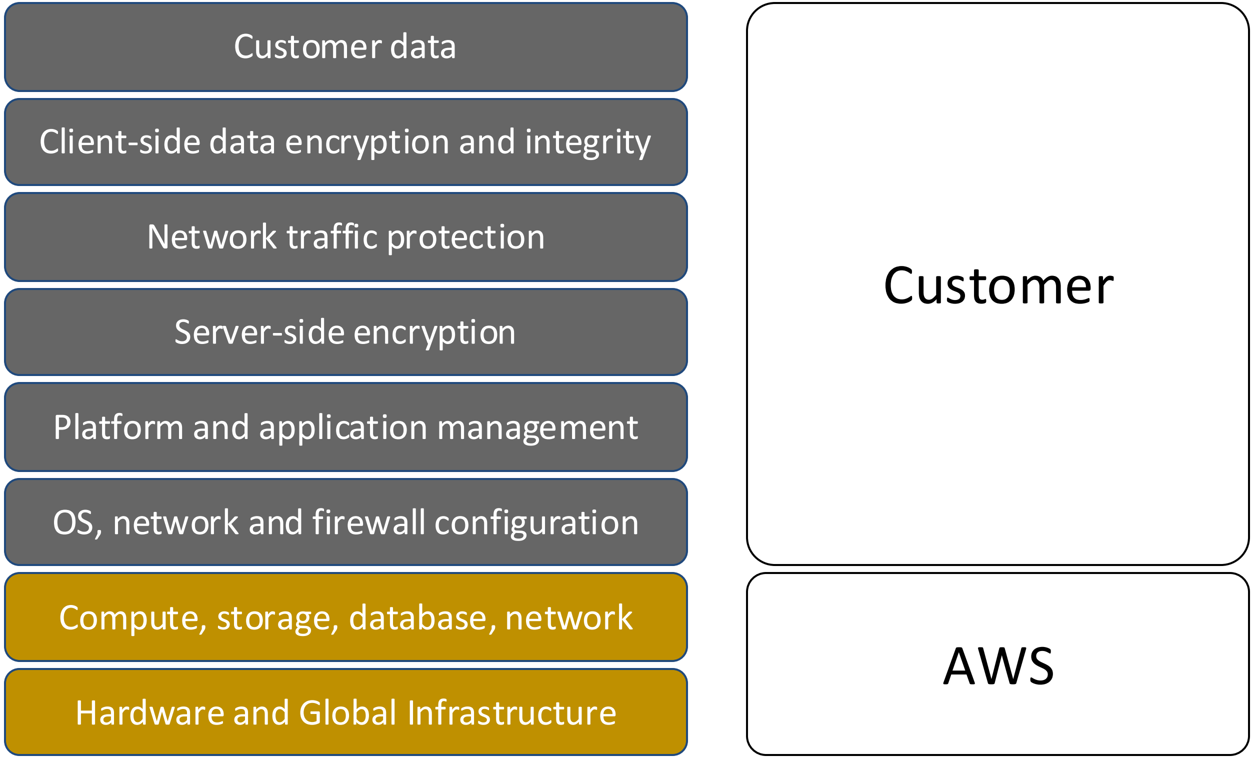


Compute, storage, database, network

Hardware and Global Infrastructure

AWS

Shared Responsibility Model - IaaS



Customer data

Client-side data encryption and integrity

Network traffic protection

Server-side encryption

Platform and application management

OS, network and firewall configuration

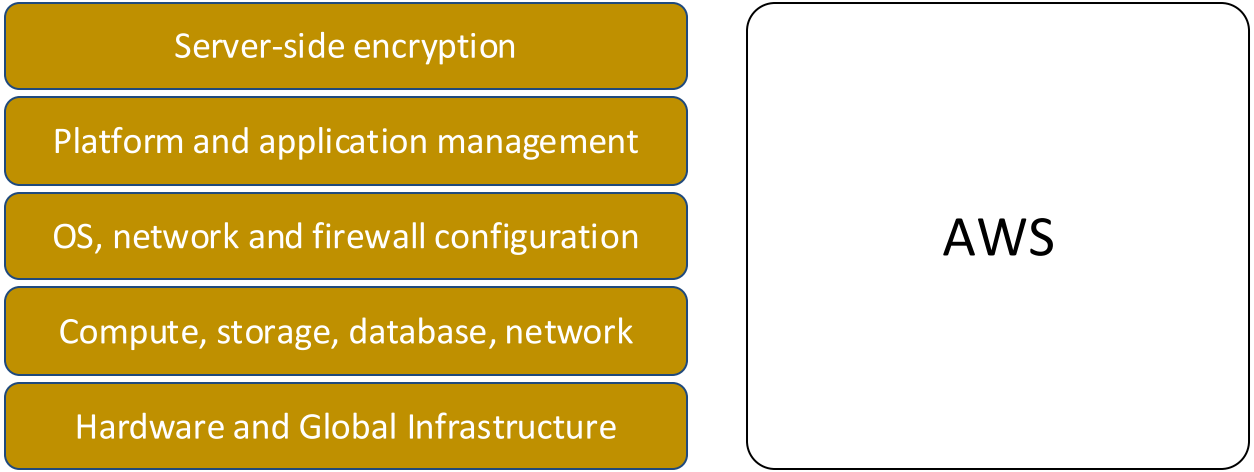
Compute, storage, database, network

Hardware and Global Infrastructure

Customer

AWS

Shared Responsibility Model - PaaS



Server-side encryption

Platform and application management

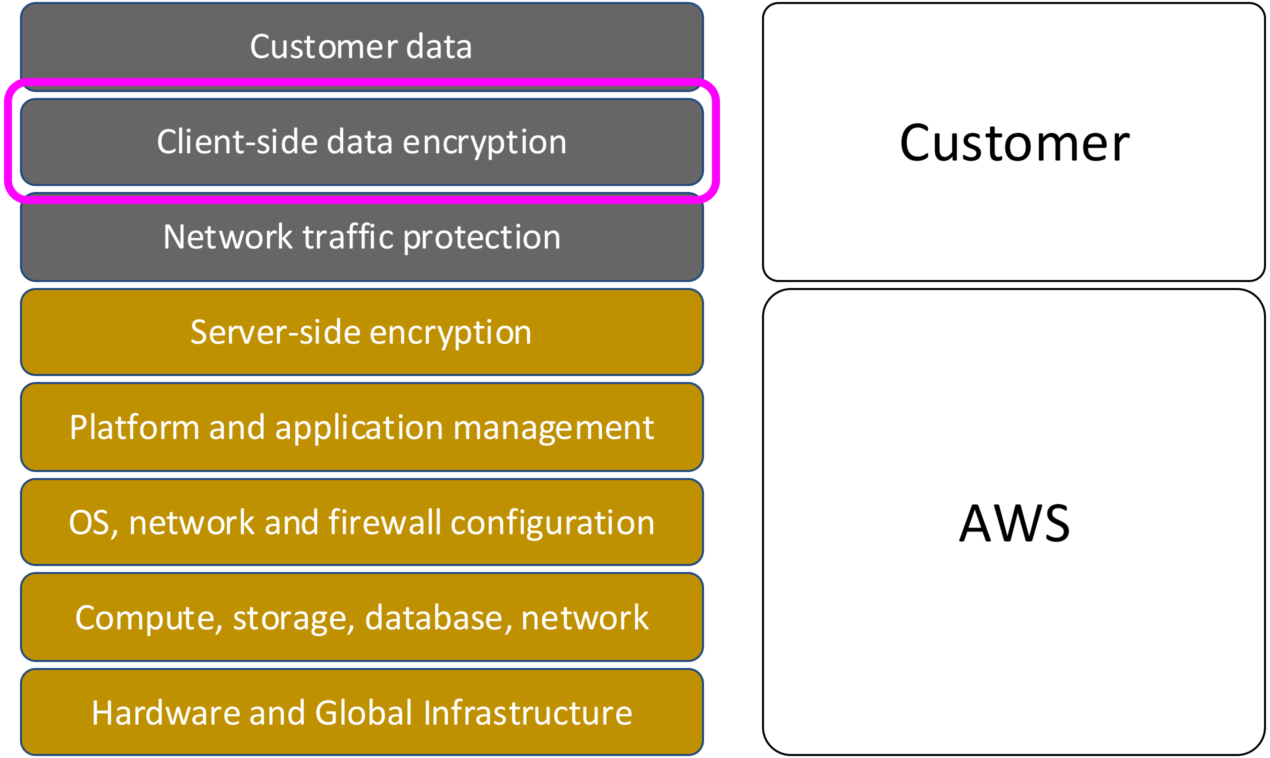
OS, network and firewall configuration

Compute, storage, database, network

Hardware and Global Infrastructure

AWS

Shared Responsibility Model - PaaS



Customer data

Client-side data encryption

Network traffic protection

Server-side encryption

Platform and application management

OS, network and firewall configuration

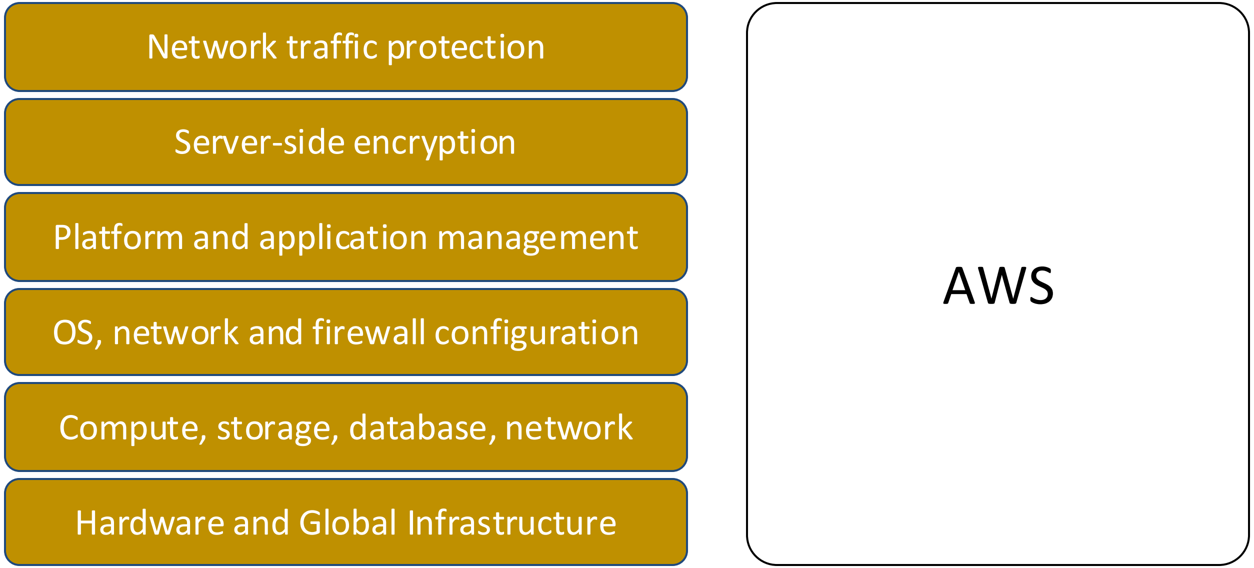
Compute, storage, database, network

Hardware and Global Infrastructure

Customer

AWS

Shared Responsibility Model - SaaS



Network traffic protection

Server-side encryption

Platform and application management

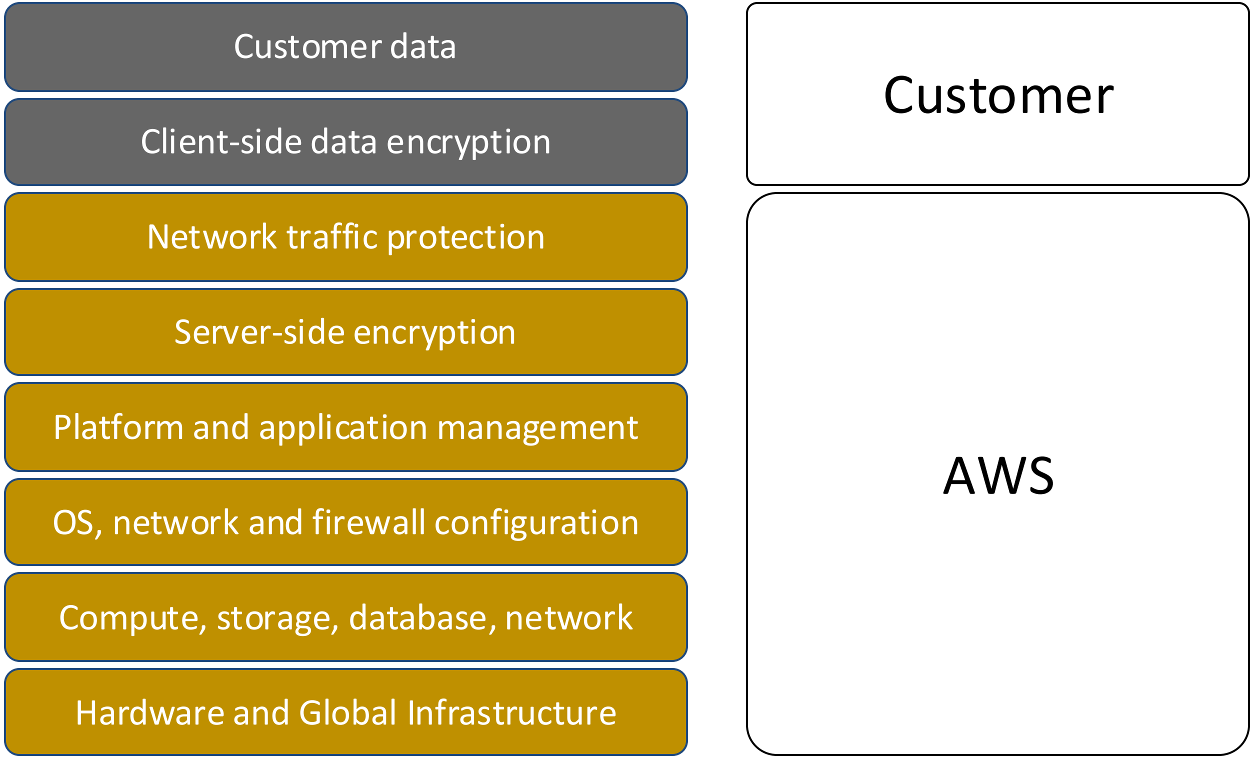
OS, network and firewall configuration

Compute, storage, database, network

Hardware and Global Infrastructure

AWS

Shared Responsibility Model - SaaS



Customer data

Client-side data encryption

Network traffic protection

Server-side encryption

Platform and application management

OS, network and firewall configuration

Compute, storage, database, network

Hardware and Global Infrastructure

Customer

AWS

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

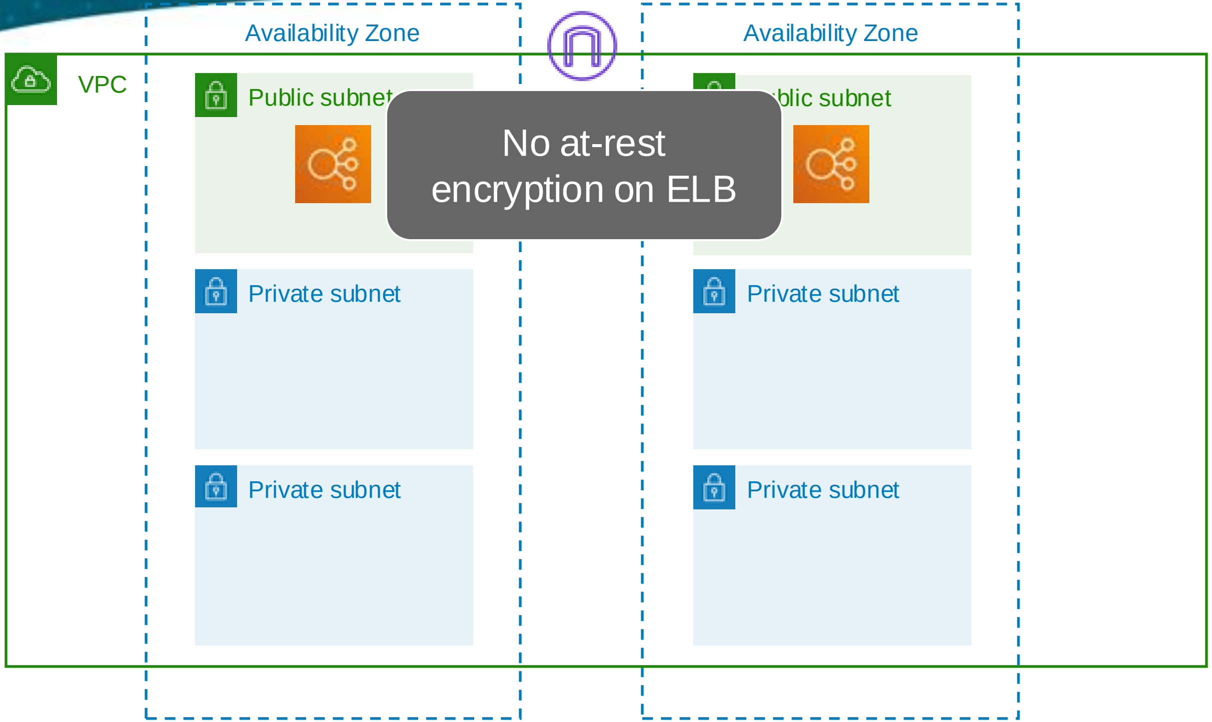
Service availability doesn't imply all features are available in the region

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

Service compliance doesn't imply all features are compliant

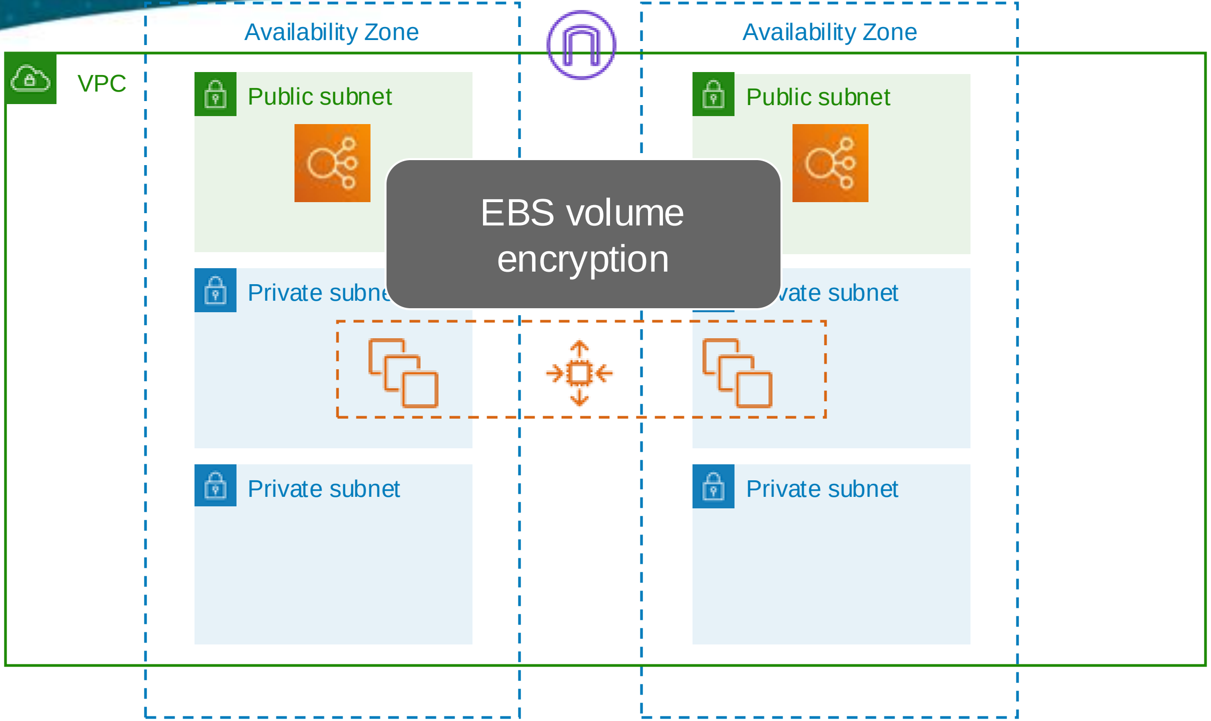
When in doubt, ask support!

At-rest Encryption On AWS

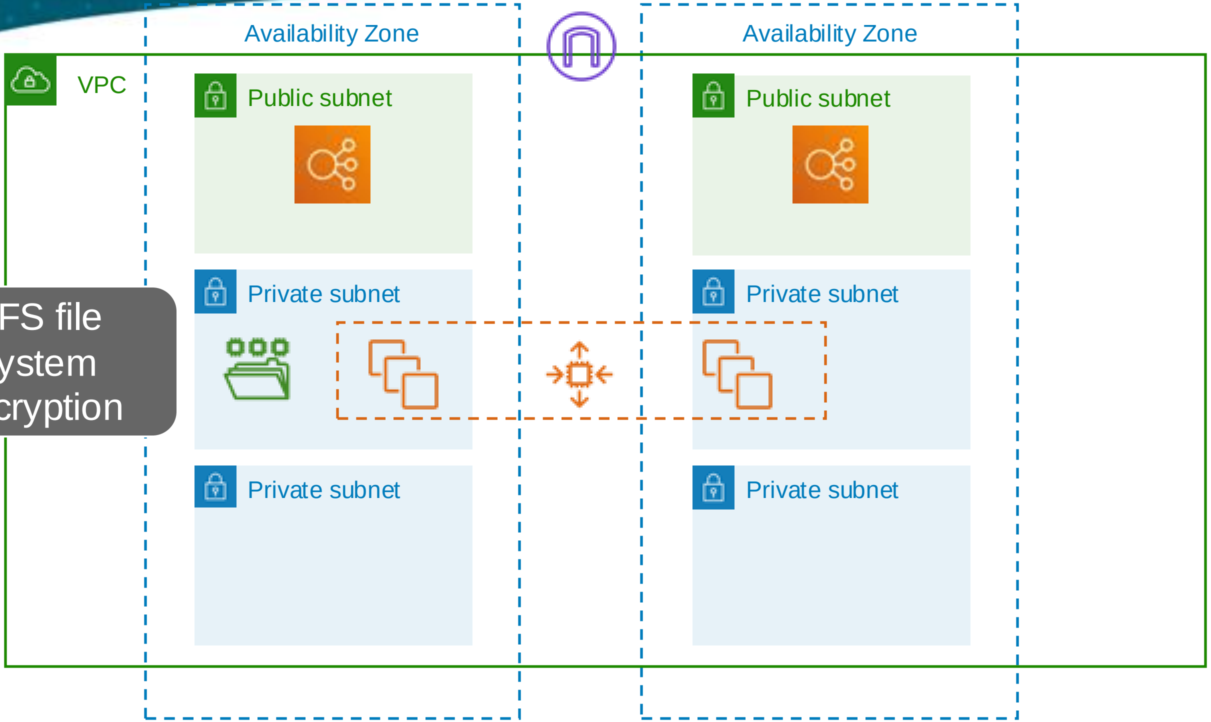


No at-rest encryption on ELB

At-rest Encryption On AWS

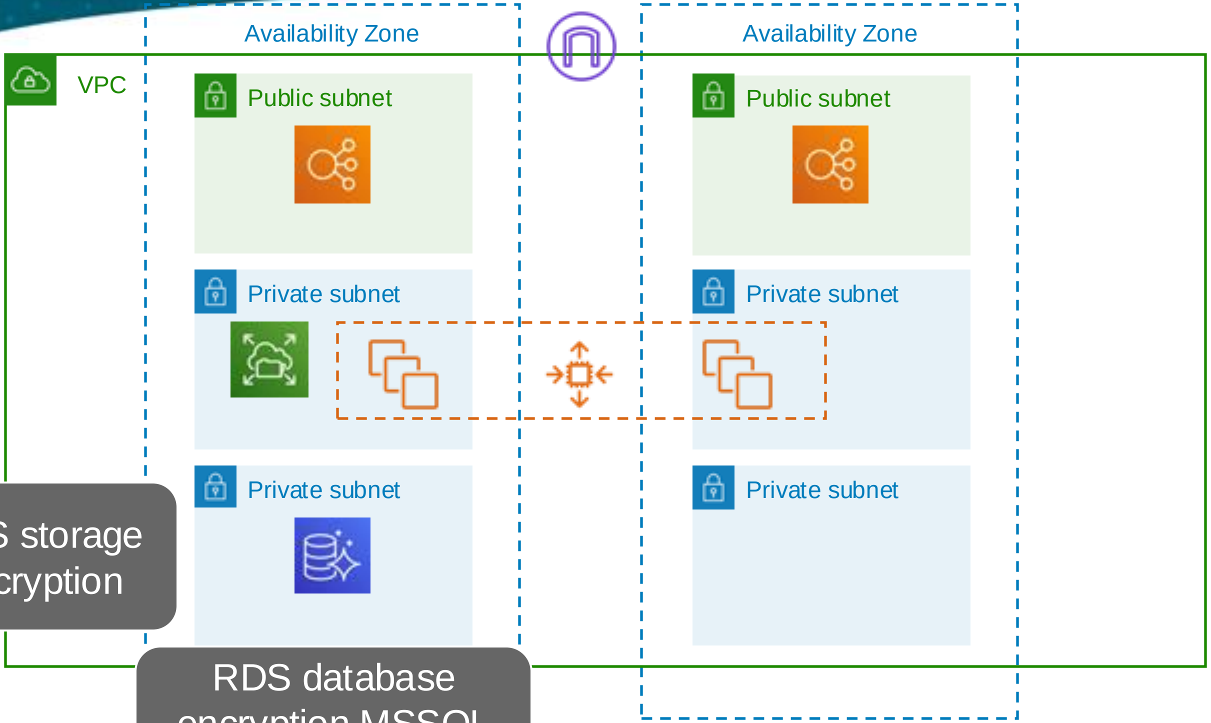


At-rest Encryption On AWS



EFS file system encryption

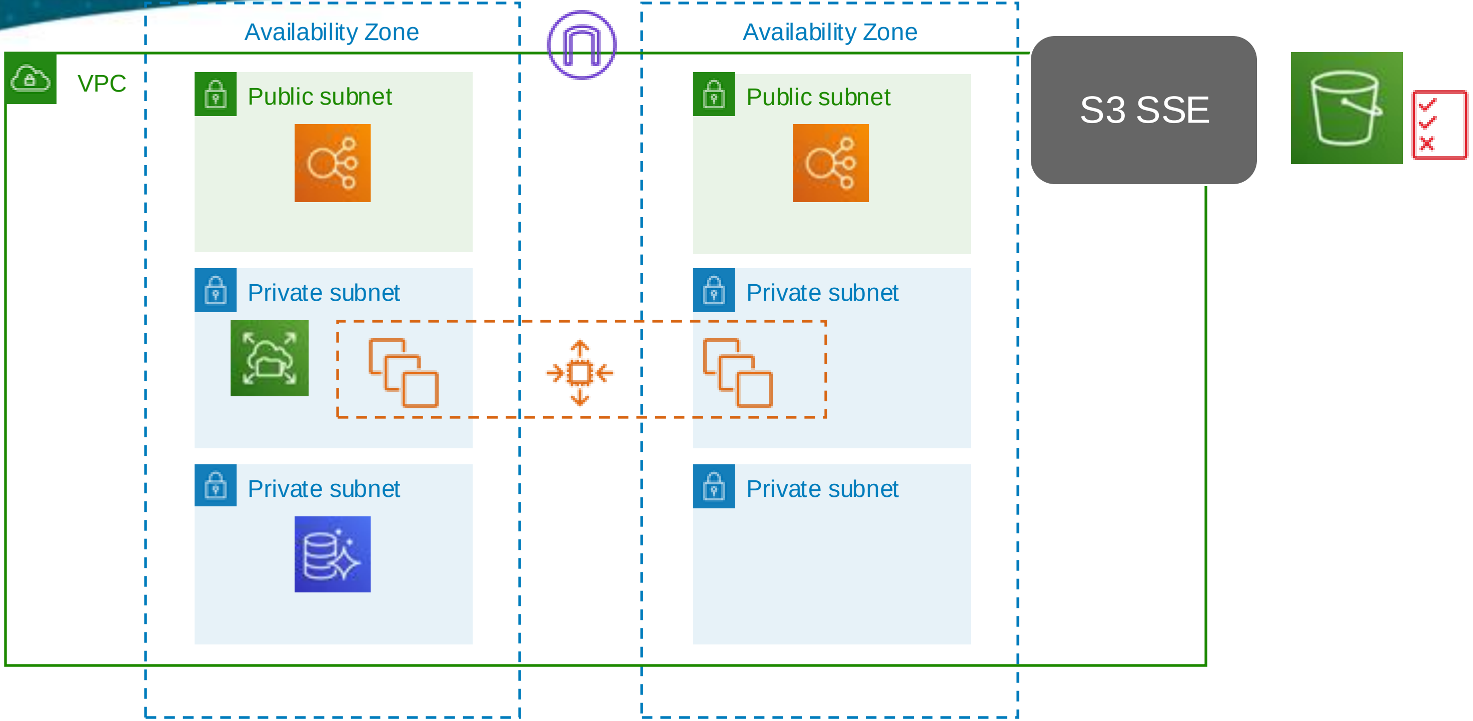
At-rest Encryption On AWS



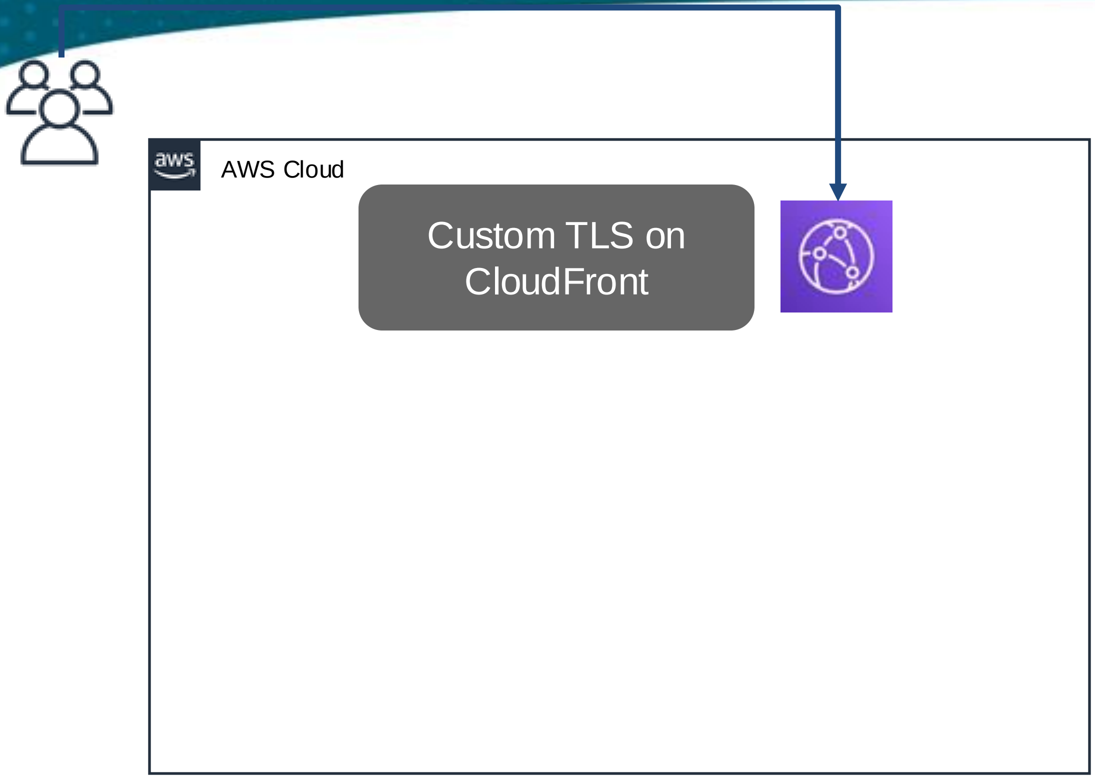
RDS storage encryption

RDS database encryption MSSQL and Oracle

At-rest Encryption On AWS

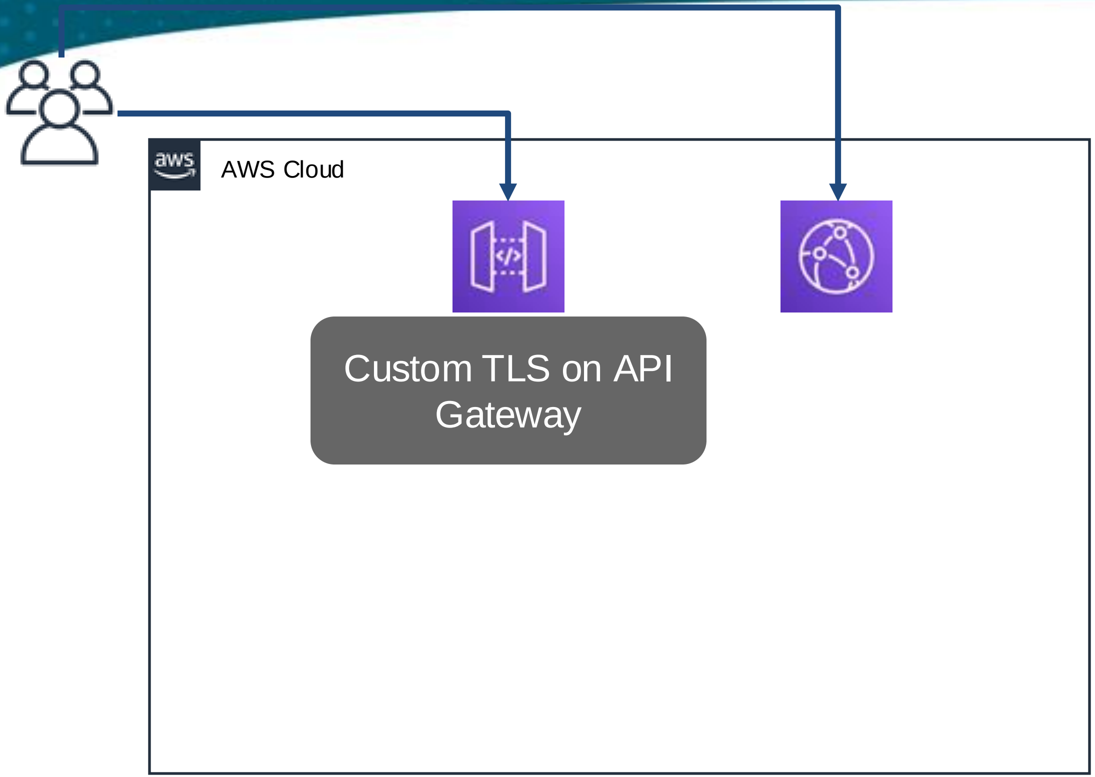


In-Transit Encryption On AWS



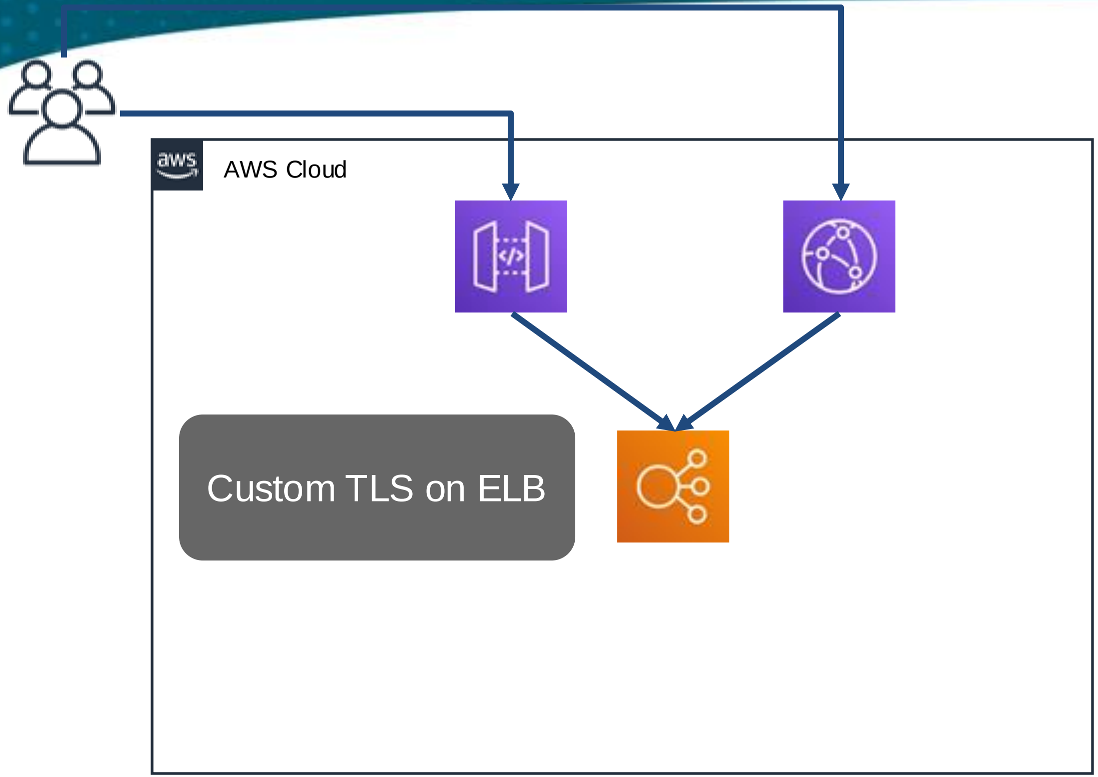
The CloudFront distribution must have the DNS CNAME records listed in the configuration for TLS

In-Transit Encryption On AWS



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

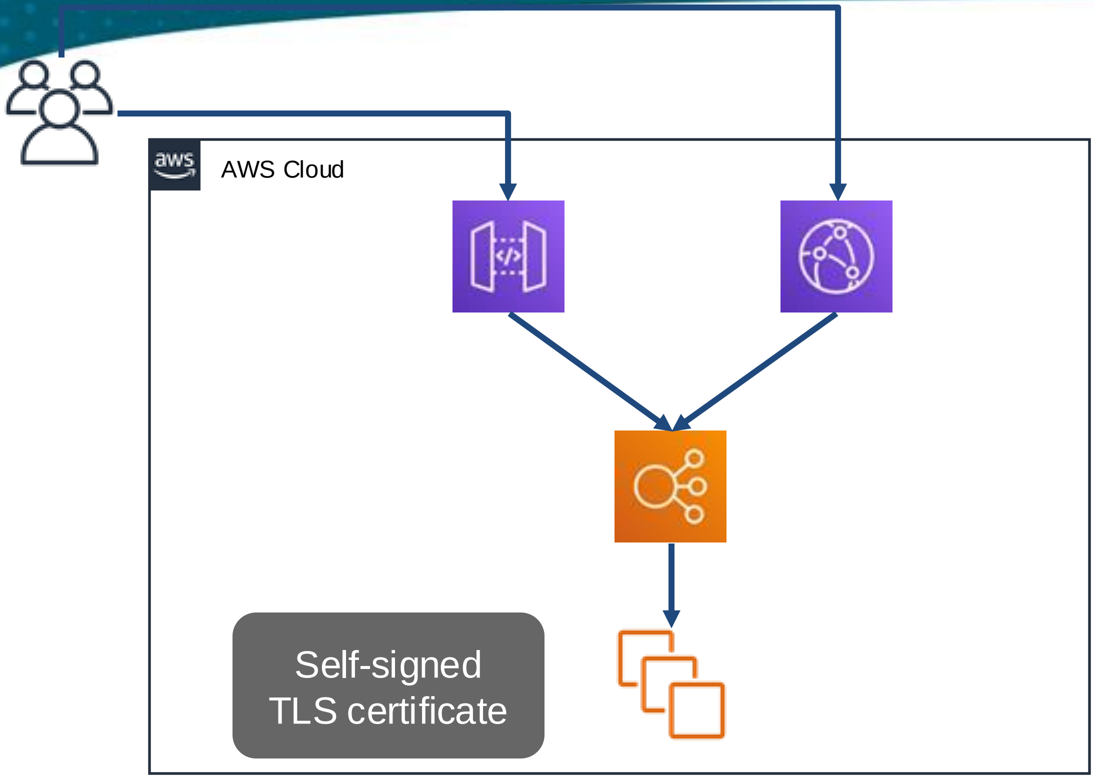
In-Transit Encryption On AWS



Custom TLS on ELB

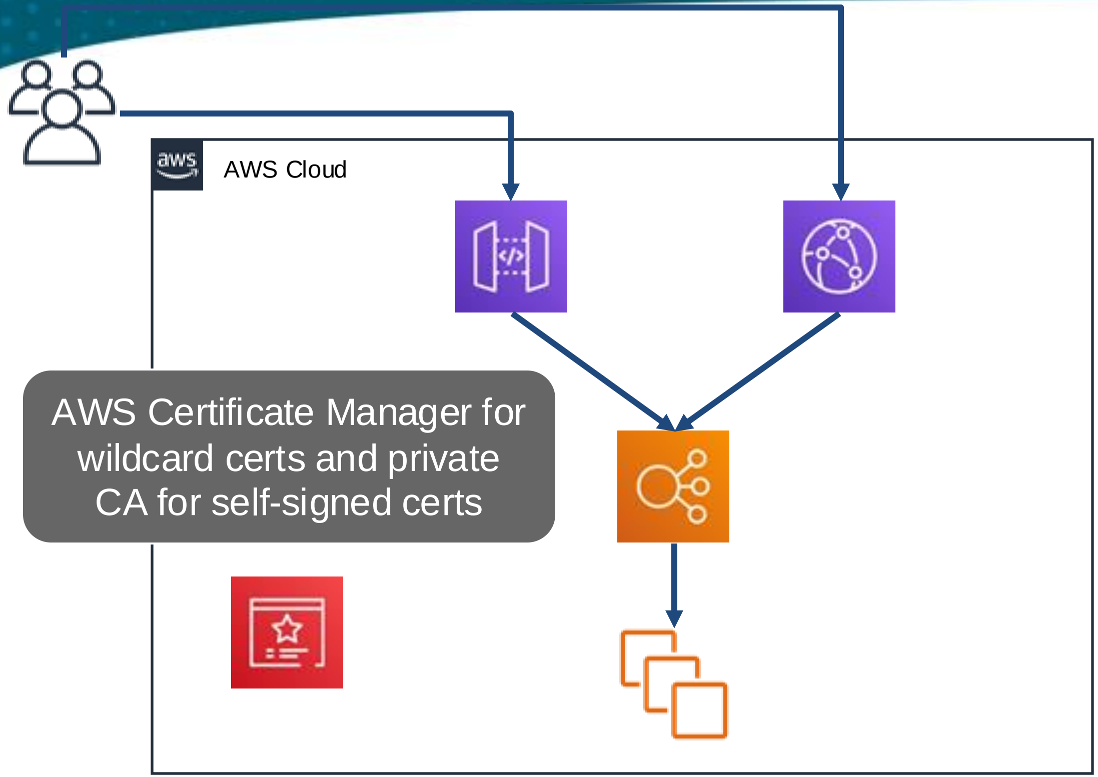
Network load balancers and Application load balancers support 25 certs concurrently

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



AWS Certificate Manager for wildcard certs and private CA for self-signed certs

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

- AWS resource monitoring service
- Collect and track metrics
- Traditional + cloud-native features

Auditing and Reporting - CloudWatch Logs

- Log delivery and monitoring service
- Fault tolerant
- Durable

Pearson

Auditing and Reporting - CloudTrail

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

Auditing and Reporting - CloudTrail

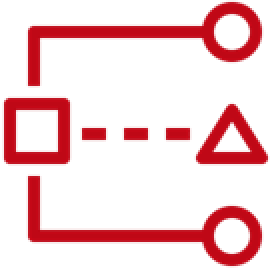
- Transferred to S3 for long-term storage
- Searchable history
- Insights event reporting

Security Service Deployment

AWS IAM Access Analyzer

Identify cross-account shared resources and recommend policy updates according to best practices

IAM Access Analyzer



- Supports Organizations
- Discover cross-account access permissions
- Supports both identity and resource permissions

Security Service Deployment

AWS IAM Access Analyzer

AWS Config

Inventory resources and identify non-compliant configurations, supports automated mitigation

AWS Config

- Supports Organizations
- Identifies resource associations
- Visualize resource changes as timeline
- Create rules to identify non-compliant resources
- Supports proactive and reactive mitigation

Security Service Deployment

AWS IAM Access Analyzer

AWS Config

Amazon Macie

Identify and classify S3 data at scale, alert upon S3 configuration changes

Amazon Macie

- Supports Organizations
- Classify data
- Identify sensitive data according to data privacy frameworks
- Analyze data access permissions
- Generate findings and organize by severity or bucket

Security Service Deployment

AWS IAM Access Analyzer

AWS Config

Amazon Macie

Amazon GuardDuty

Managed account protection using ML with detective controls on several services and features

Amazon GuardDuty

- Supports Organizations
- Protect AWS workloads, credentials and data
- Ingests from several event and data sources

Security Service Deployment

AWS IAM Access Analyzer

AWS Config

Amazon Macie

Amazon GuardDuty

Amazon Inspector

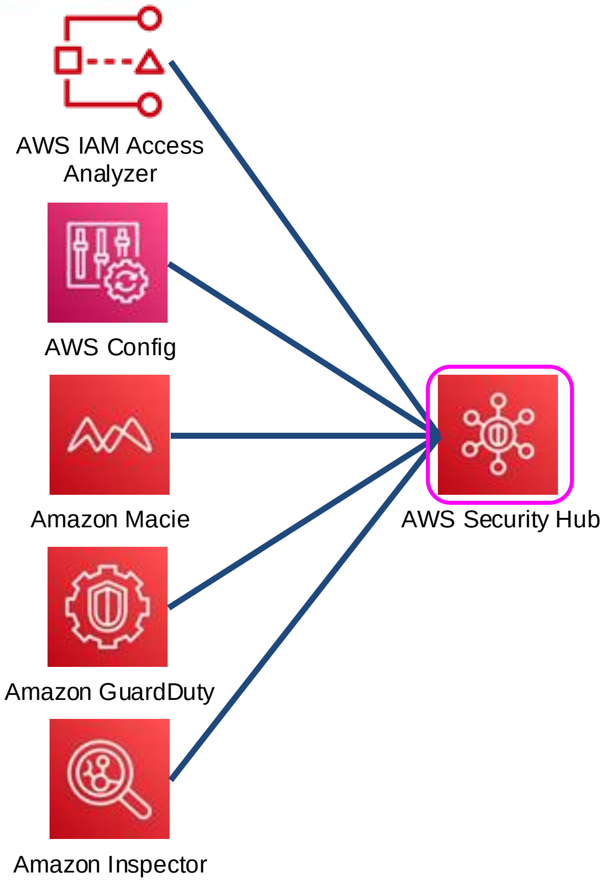
Automated software vulnerability management for EC2, ECR, and Lambda

Amazon Inspector

- Supports Organizations
- Discover and scan AWS workloads for software vulnerabilities
- Also scans for unintended network exposure

Pearson

Security Service Deployment

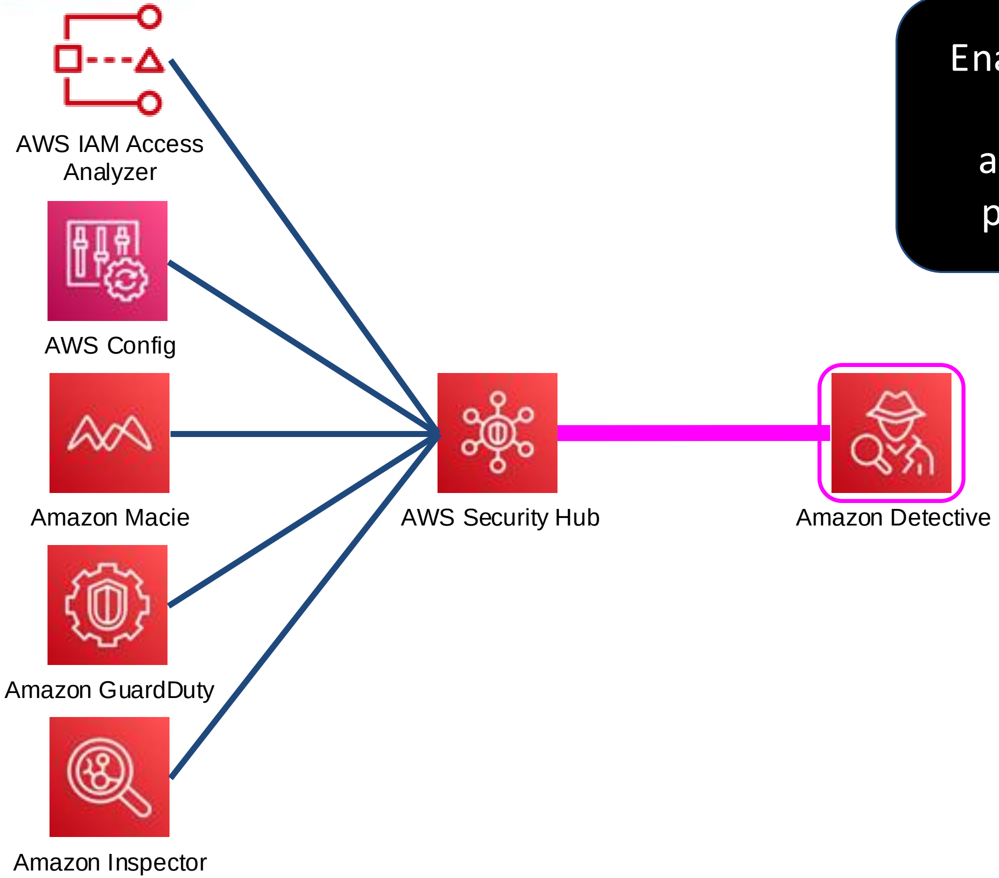


View centralized security dashboards and implement controls in various security standards

AWS Security Hub

- Supports Organizations
- Automate security checks, centralize alerts and findings
- Ingest findings from third-party sources
- Implement checks from several security standards

Security Service Deployment

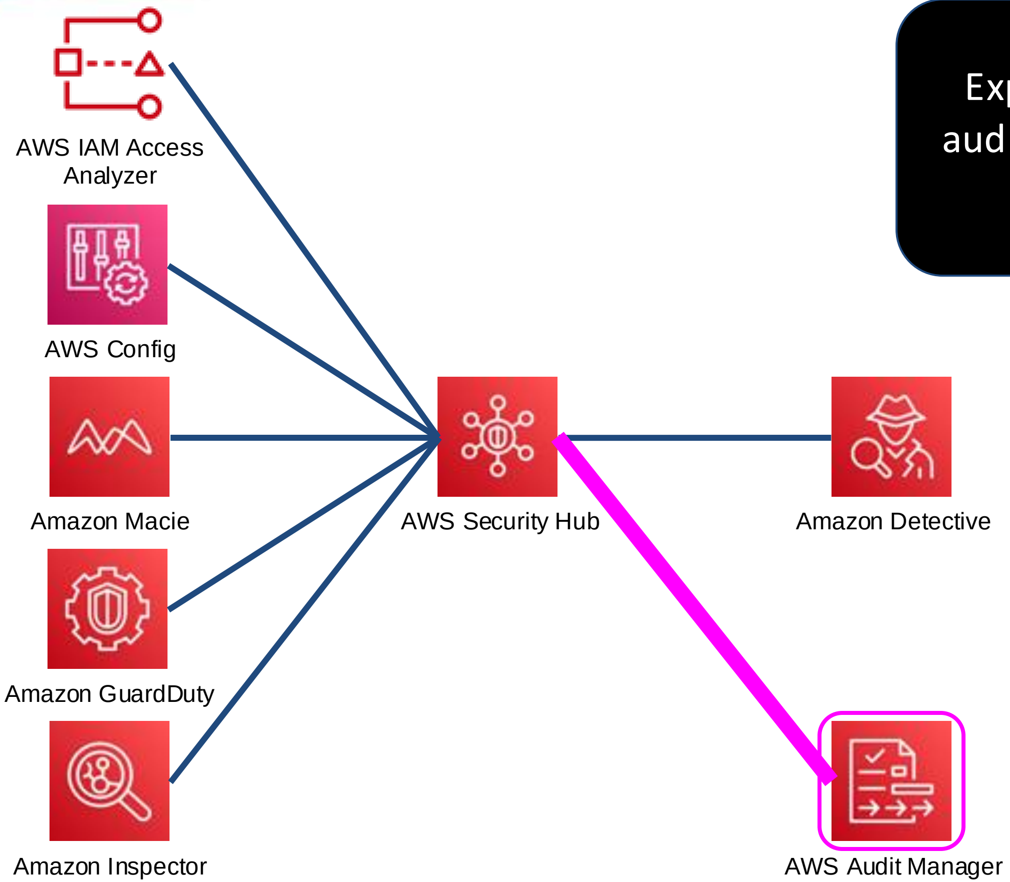


Enable GuardDuty as a data input to Detective for analyzing and visualizing potential security issues

Amazon Detective

- Supports Organizations
- Integrates with Security Hub
- Organizes security data into a graph model
- Use interactive visualizations to identify security event root causes

Security Service Deployment

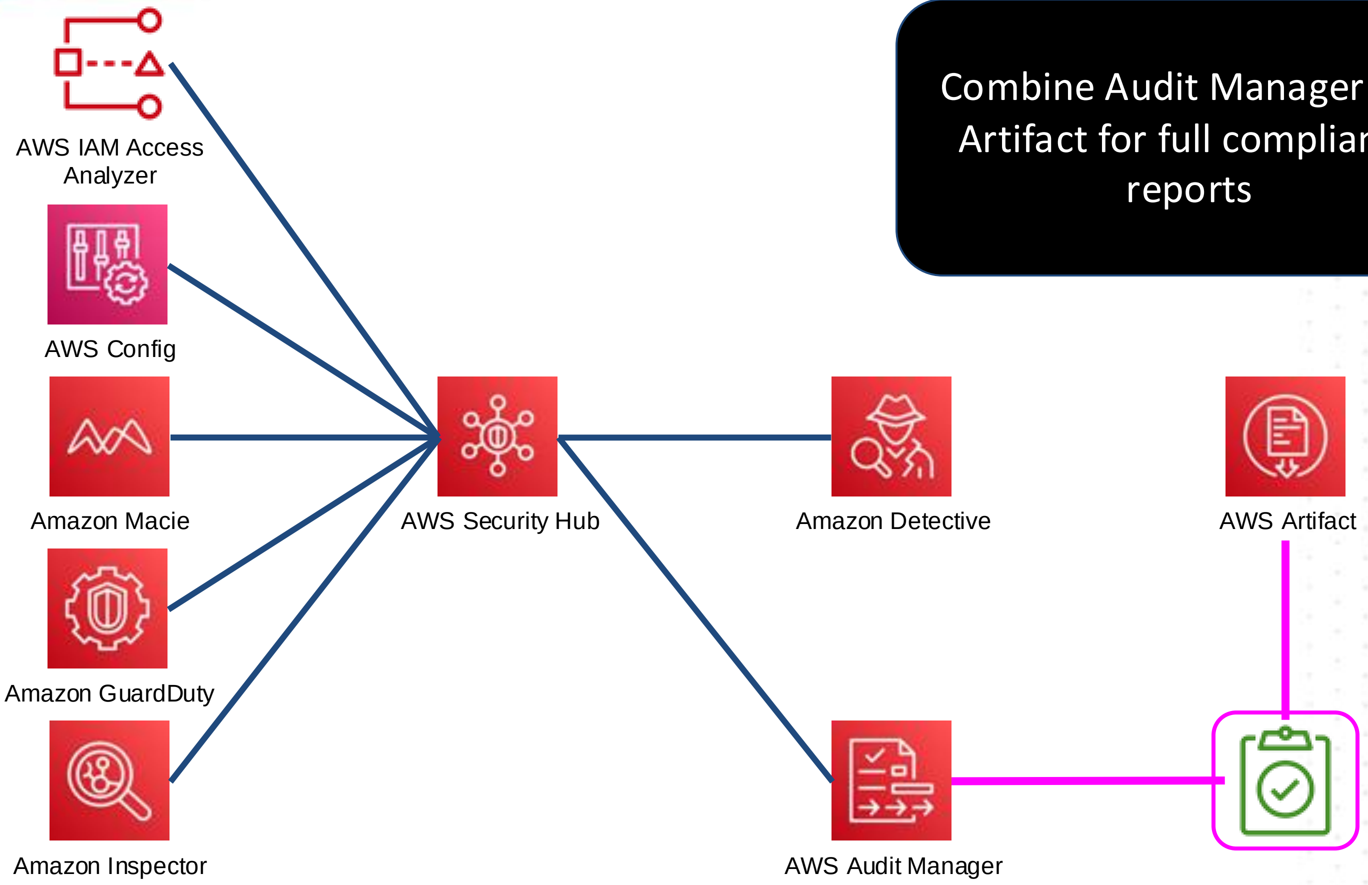


Export evidence and build audit reports for compliance programs

AWS Audit Manager

- Integrates with Security Hub
- Organizes findings and evidence
- Create reports for specific compliance frameworks

Security Service Deployment



Combine Audit Manager and Artifact for full compliance reports

AWS Artifact

- Enabled by default per account
- Auditor issued reports on AWS security and compliance
- Certifications, attestations, accreditations in one location

Question Breakdown

Question and Answer Choices

Who maintains responsibility for the retention of CloudTrail logs in AWS?

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

Correct Answer and Explanation

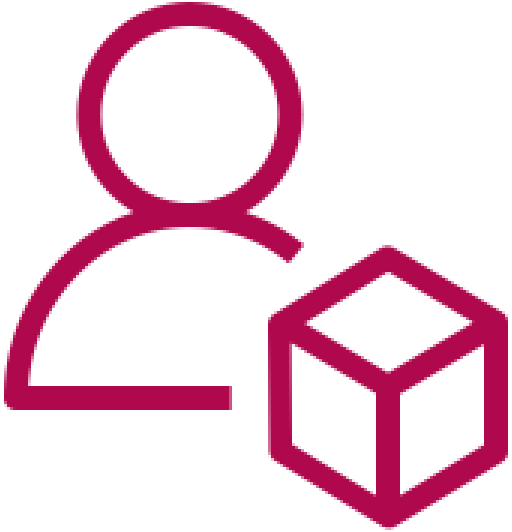
The customer is 100% responsible for enabling and retaining log features in AWS.

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



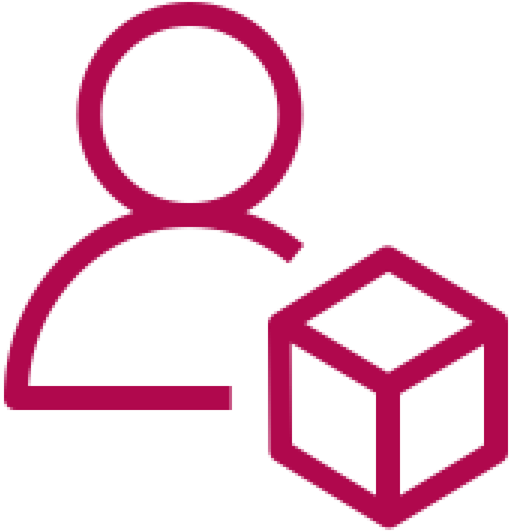
Container for AWS resources

Account Definition

Unit of:

- Organization
- Billing
- Access

Account Definition



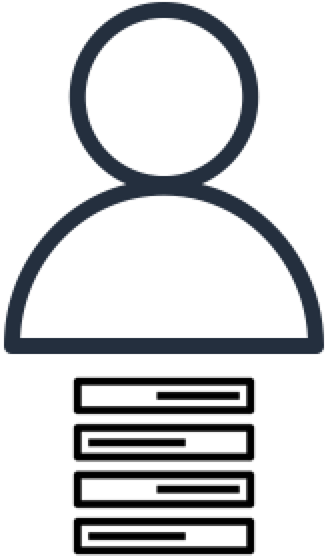
1 Root User

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***

Authenticating to AWS

Static identity

Includes IAM users

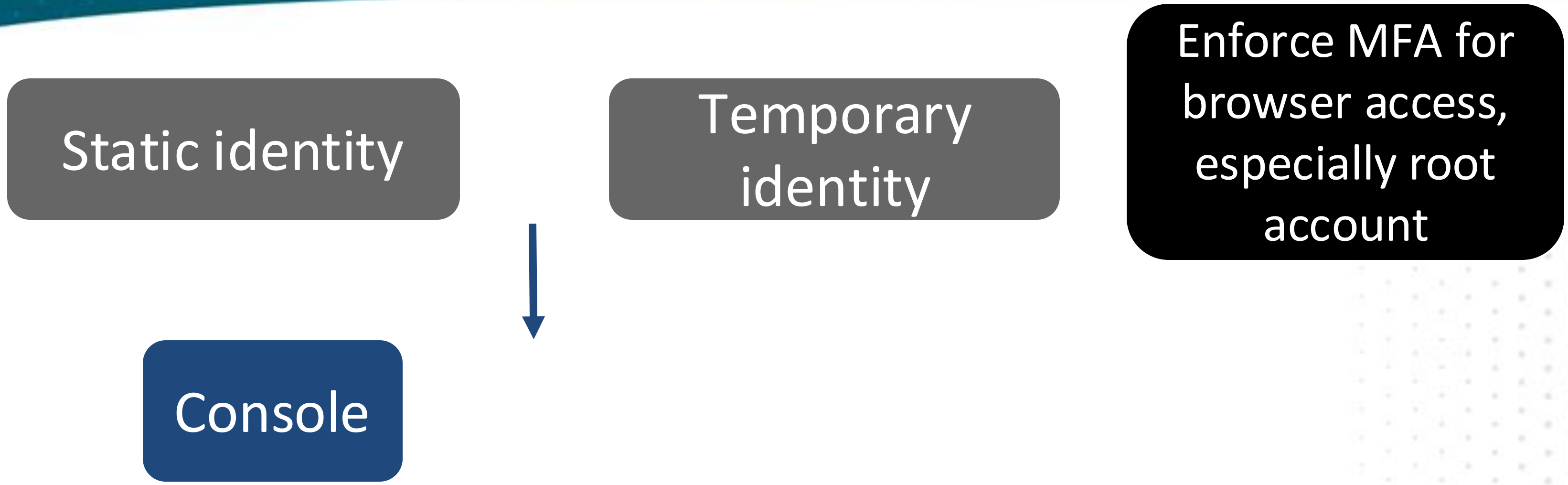
Authenticating to AWS

Static identity

Temporary identity

Federation and IAM roles

Authenticating to AWS



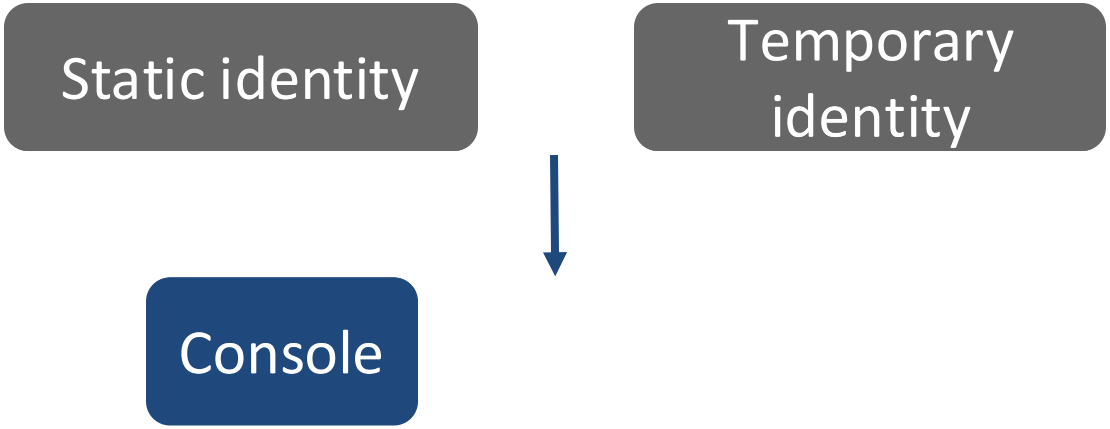
Static identity

Temporary identity

Console

Enforce MFA for browser access, especially root account

Authenticating to AWS


Static identity

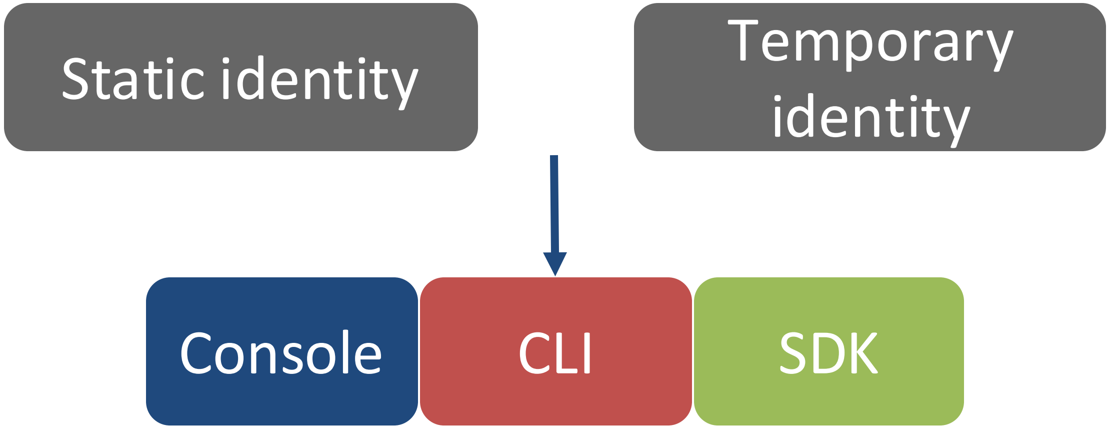
Temporary identity

Console

Enforce MFA for browser access, especially root account

Apply password complexity policy per AWS account

Authenticating to AWS



Static identity

Temporary identity

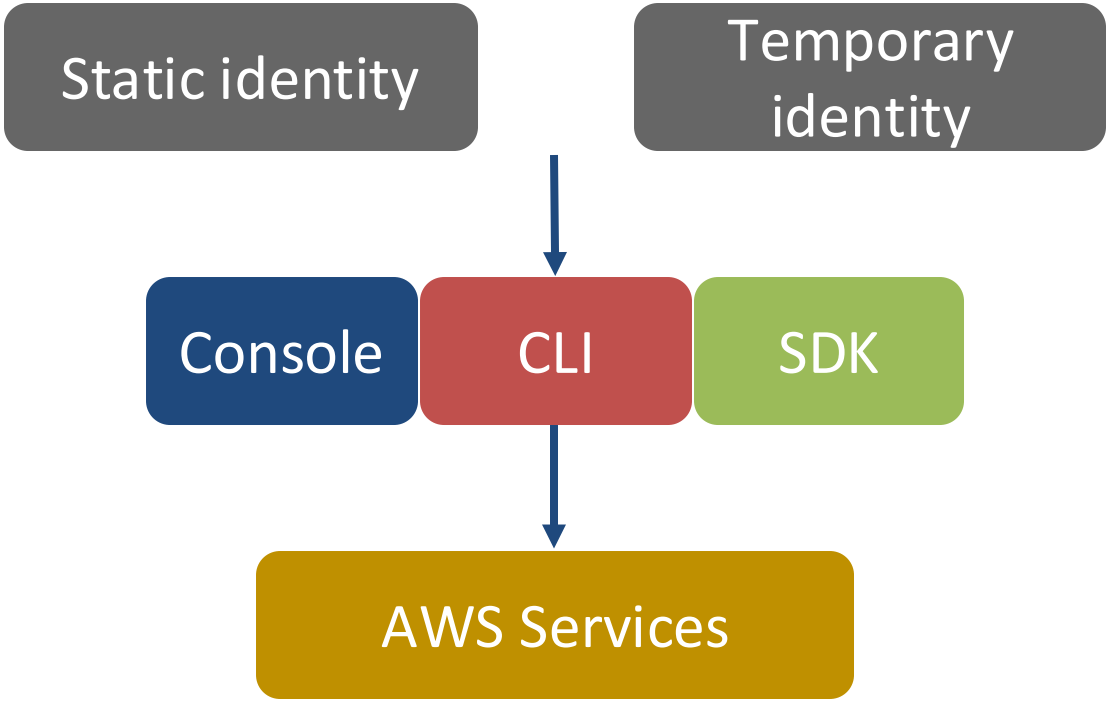
Console

CLI

SDK

CLI and SDK require access keys and signed requests

Authenticating to AWS



Static identity

Temporary identity

Console

CLI

SDK

AWS Services

All services are API-driven via HTTP or HTTPS

Identity and Access Management (IAM)

- Authentication
- Authorization
- Identity-based access control

IAM Password Policy Options

- Minimum length
- Strength
- Expiration days
- Expiration = admin reset
- Self reset
- No password reuse

What is an IAM User?

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

Pearson

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

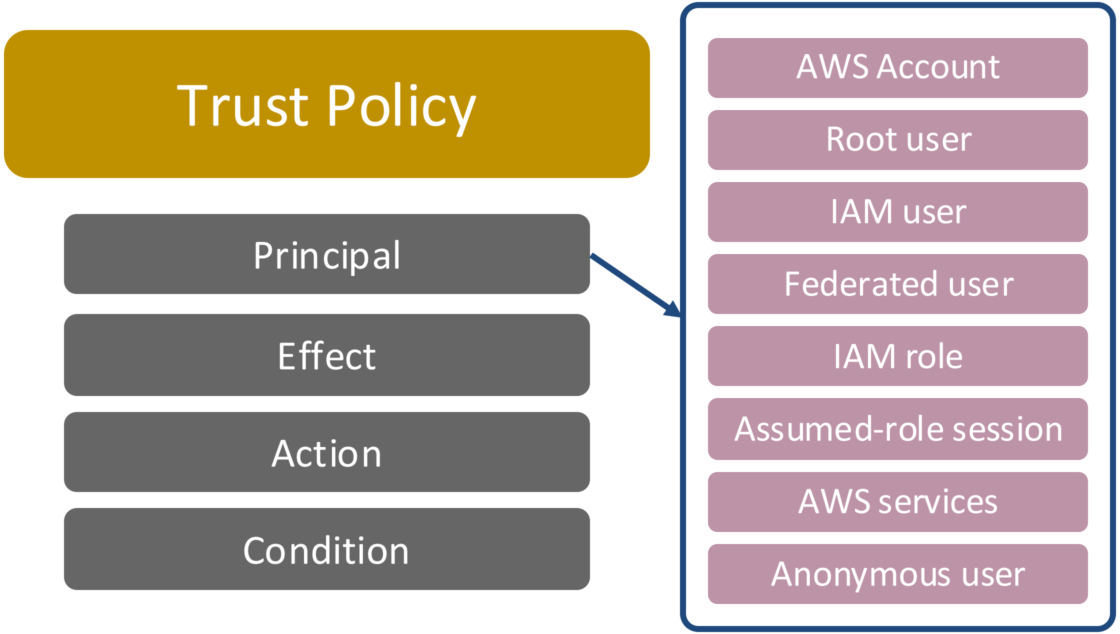
Inline Policy

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

What is an IAM Role?

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

Role Trust Policy



Trust Policy

- Principal
- Effect
- Action
- Condition

Principal:

- AWS Account
- Root user
- IAM user
- Federated user
- IAM role
- Assumed-role session
- AWS services
- Anonymous user

The principal is the entity allowed to assume the role

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

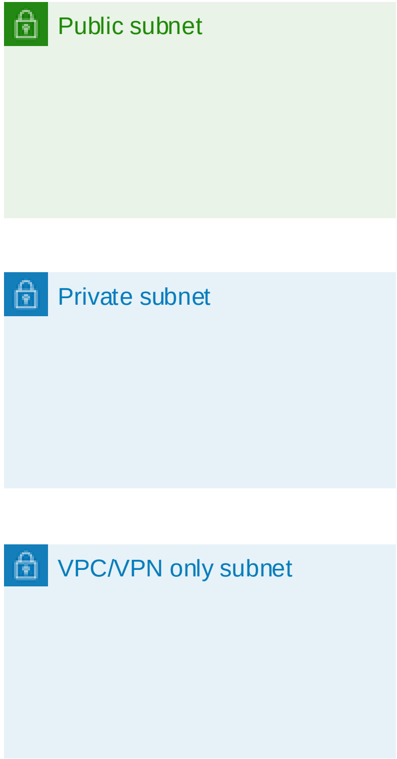
VPC Network Security Options

Each subnet can only exist in one AZ

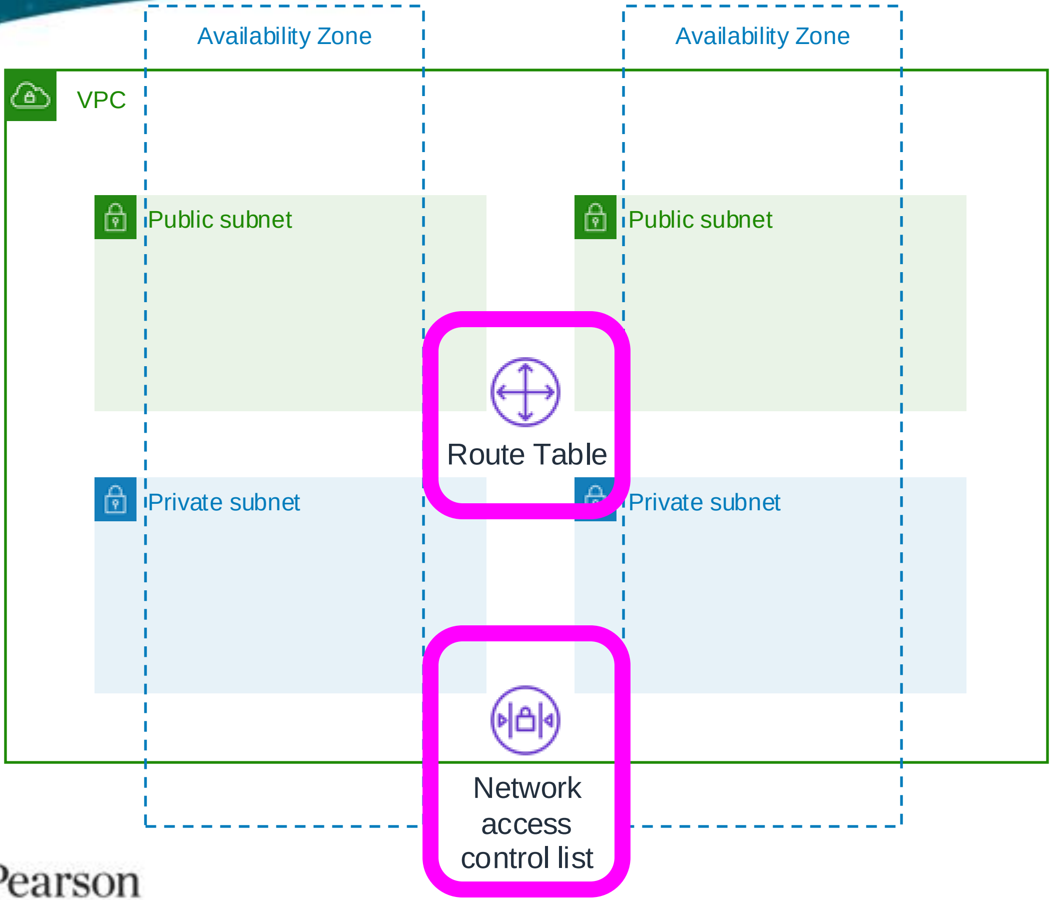
Bidirectional Internet access via IGW

Outbound Internet access via proxy (NAT GW)

No Internet access, or only via VPN/DX



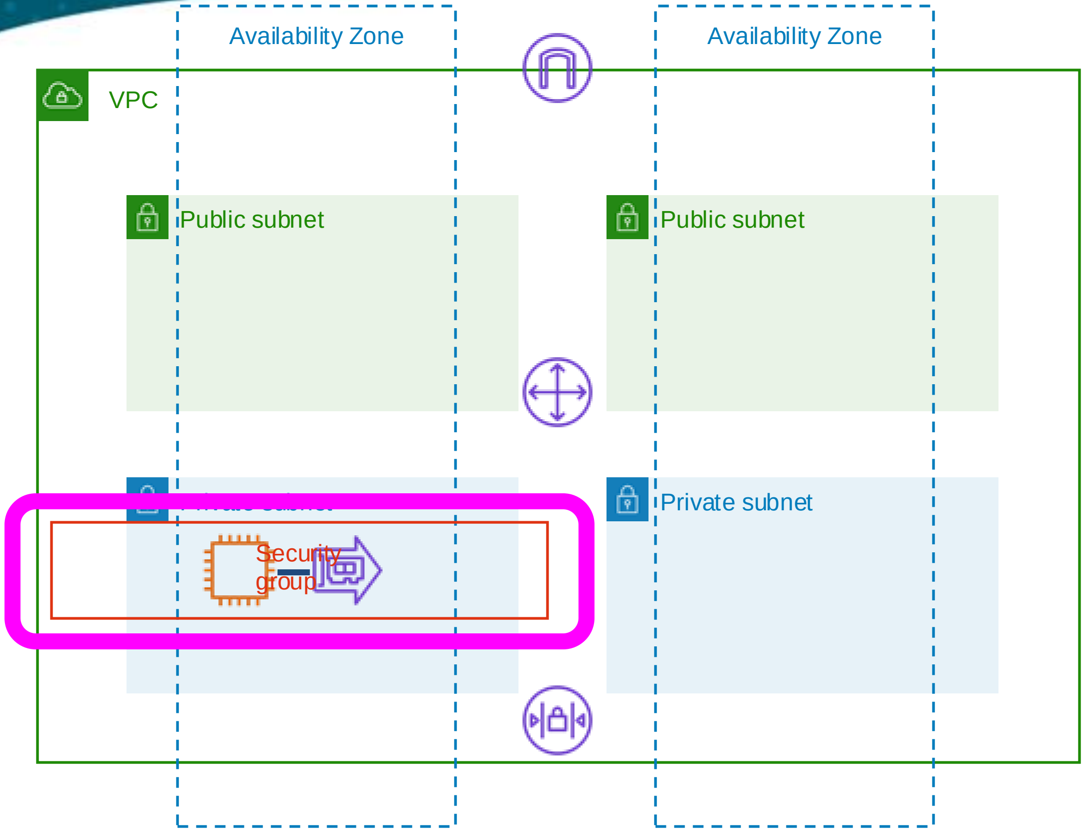
VPC Network Security Options



Route tables operate on traffic leaving a subnet and for another subnet or network

NACLs operate on traffic entering and leaving a subnet

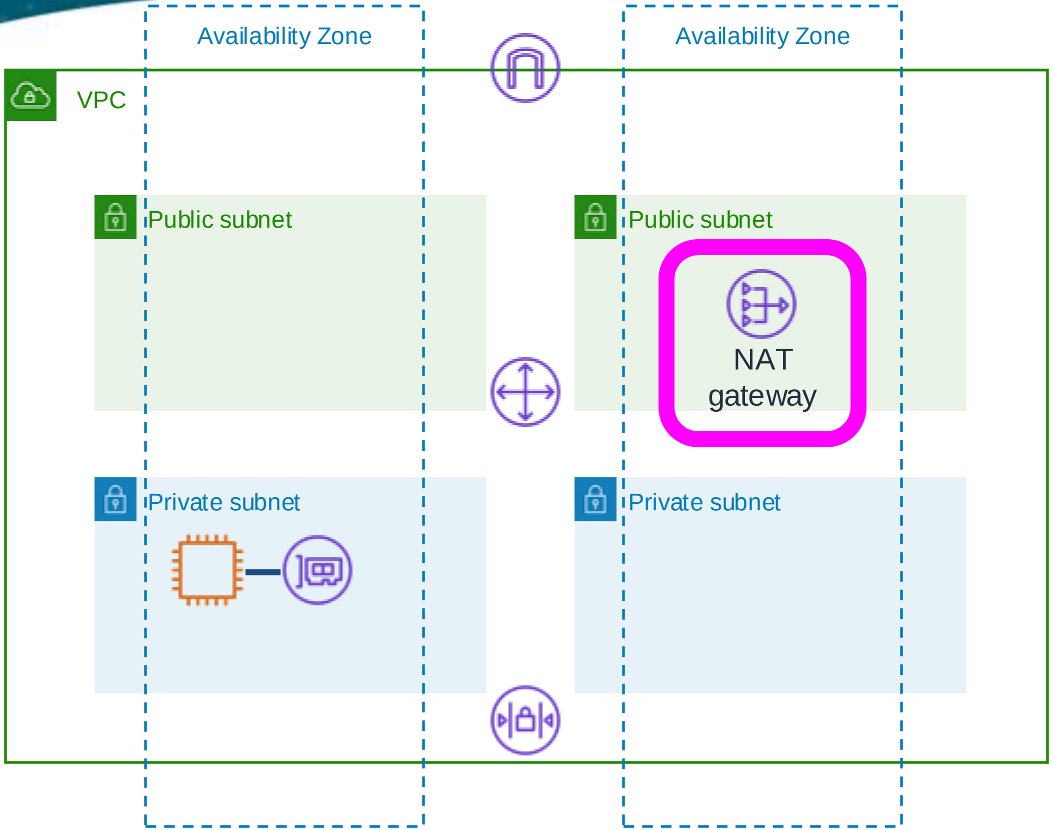
VPC Network Security Options



Security group ingress rules only operate on inbound-initiated traffic

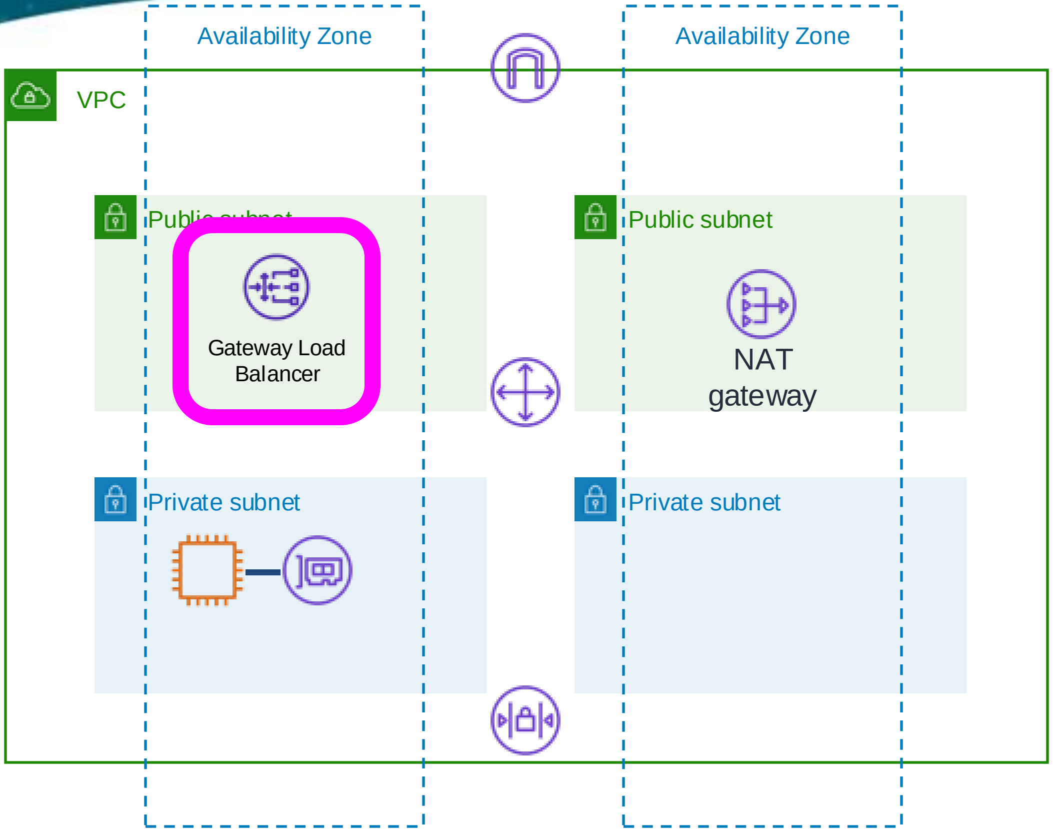
Security group egress rules only operate on outbound-initiated traffic

VPC Network Security Options



NAT Gateways are used to proxy outbound traffic to public or private destinations

VPC Network Security Options



Gateway Load Balancers (GWLB) provide scaling for outbound proxy, router, NAT or other security applications

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.

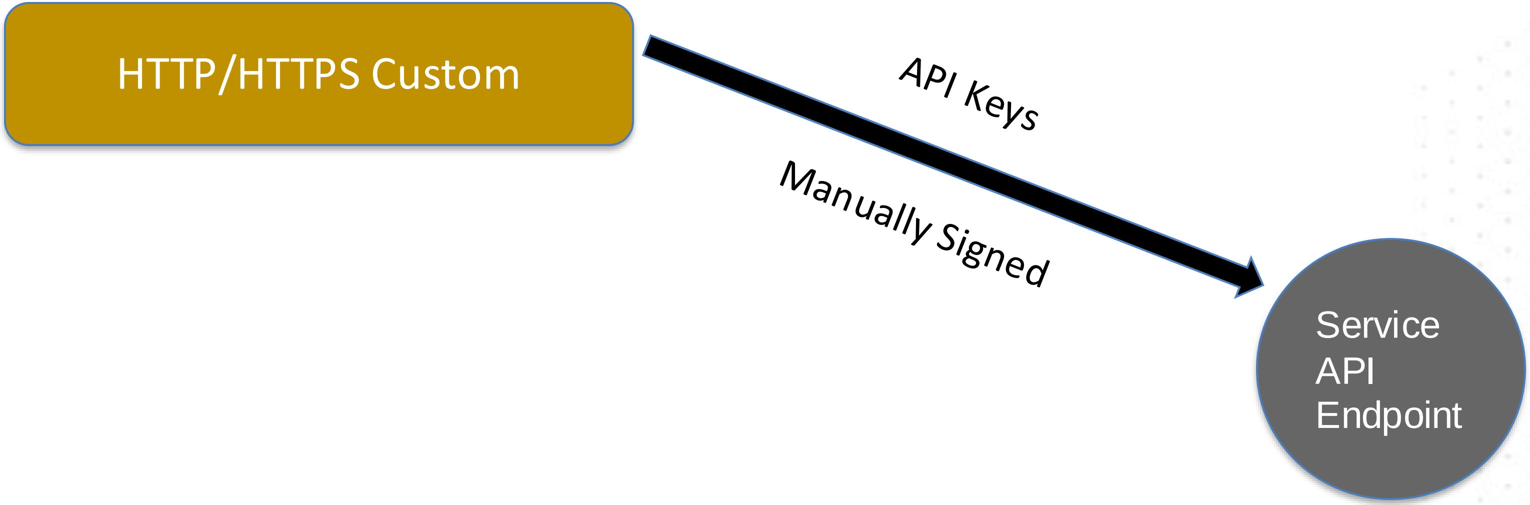
A. Network ACL
B. Security Group
C. Firewall Manager
D. AWS Network Firewall

Question Domain 3: Technology

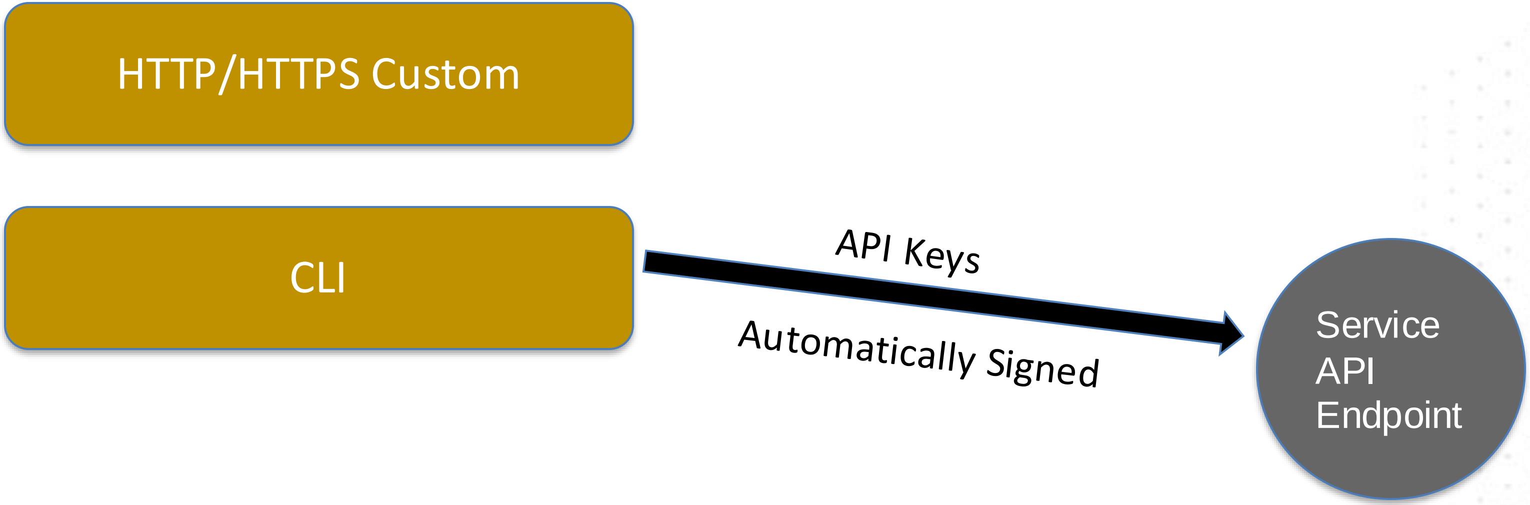
Question Domain 3: Technology

AWS Deployments and Operations

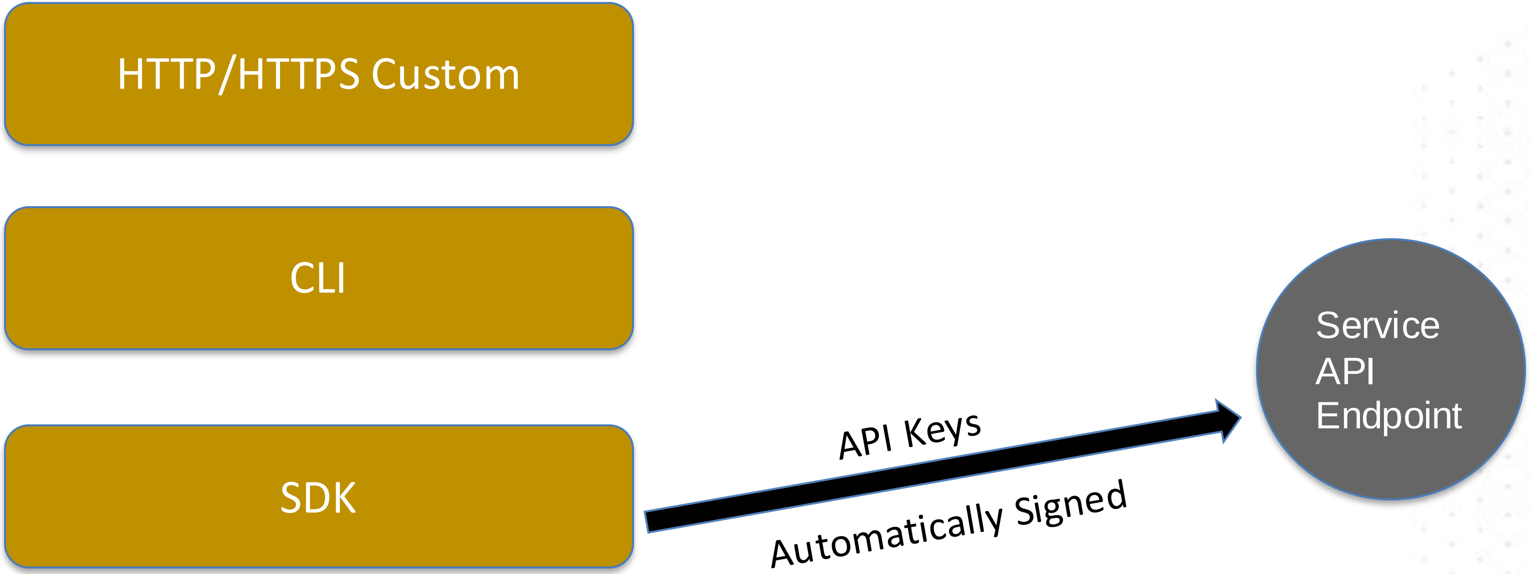
How To Access AWS - Direct Credentials



How To Access AWS - Direct Credentials



How To Access AWS - Direct Credentials



HTTP/HTTPS Custom

CLI

SDK

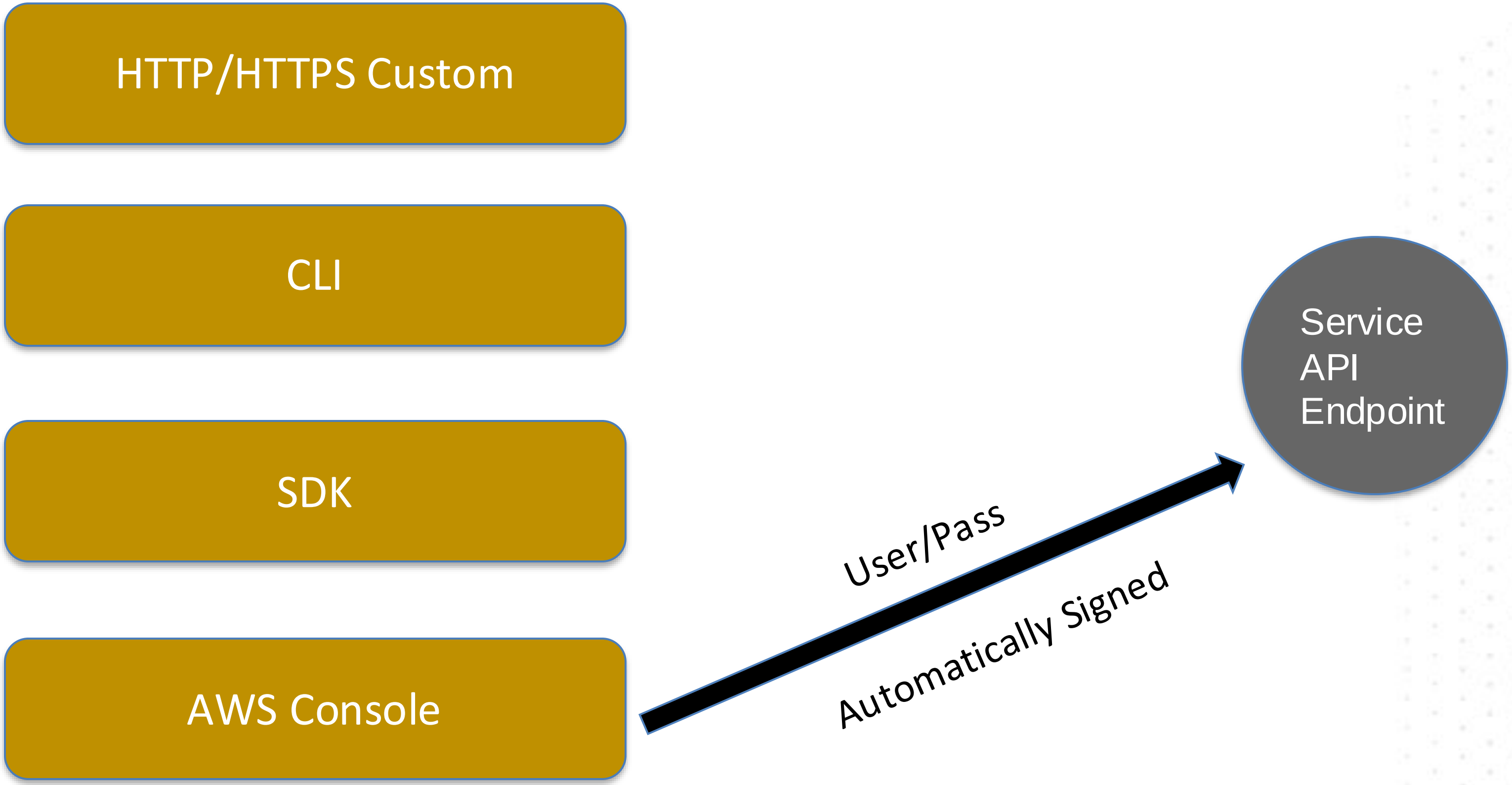
API Keys

Automatically Signed

Service API Endpoint

Pearson

How To Access AWS - Direct Credentials



HTTP/HTTPS Custom

CLI

SDK

AWS Console

User/Pass

Automatically Signed

Service API Endpoint

AWS Unified CLI Basics

`aws`

All operations are unified under a single "aws" command

AWS Unified CLI Basics

`aws` `[options]`

General options include region and output format, as well as more specific query and filter choices

AWS Unified CLI Basics

`aws` `[options]` `<command>`

The command corresponds to a service API endpoint (EC2, S3, RDS, and others)

AWS Unified CLI Basics

`aws` `[options]` `<command>` `<subcommand>`

The subcommand is the action being taken, such as launching an EC2 instance or uploading to S3

AWS Unified CLI Basics

```
aws [options] <command> <subcommand> [parameters]
```

Parameters are the specific options corresponding to the subcommand

Infrastructure as Code (IaC) Basics

- Use automation to deploy virtual infrastructure
- Uses DevOps principles
- All changes are performed using code

Infrastructure as Code (IaC) Benefits

- Faster deployments
- Faster infrastructure changes
- Faster recovery with possibility of rollback
- Less configuration drift
- Code reusability
- Version control
- Self-documenting infrastructure

Infrastructure As Code Services and Tools

- CloudFormation
- AWS Cloud Development Kit (CDK)
- 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?

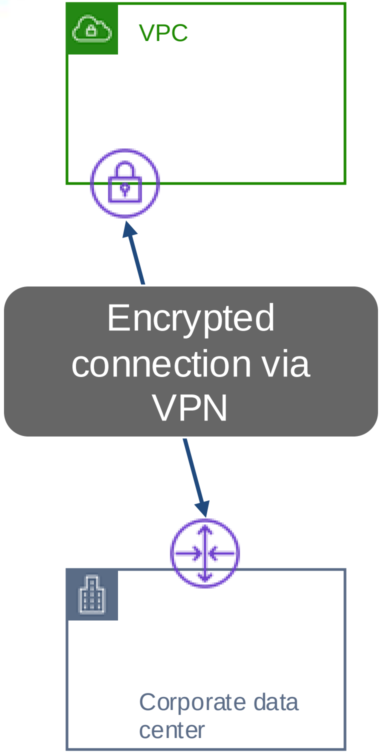
A. **HTTP/HTTPS**
B. **AWS Command Line Interface**
C. **AWS Software Development Kits (SDKs)**
D. **AWS Console**

Correct Answer and Explanation

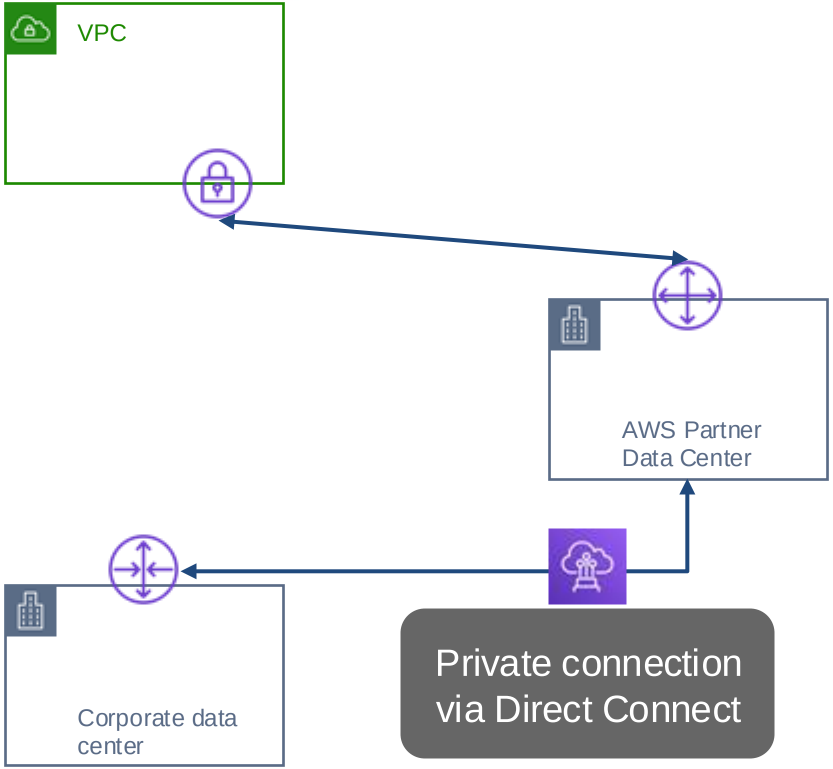
Accessing the service API endpoints directly using clients such as curl or postman is the only way to utilize all API actions, as each of the other methods have some missing functions.

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

Hybrid Connectivity Options

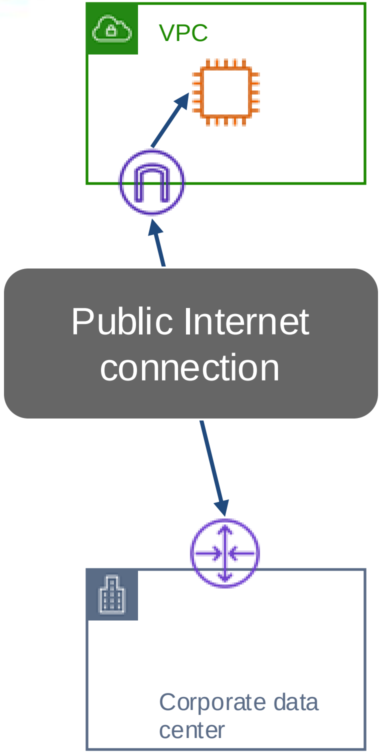


Hybrid Connectivity Options



Private connection via Direct Connect

Hybrid Connectivity Options



Question Breakdown

Question and Answer Choices

Your company wants to establish network connectivity between your data center and an AWS VPC network. There are requirements for high bandwidth and low latency. Which connectivity option would meet the requirements?

A. VPN using a Virtual Private Gateway
B. Use the on-premises Internet connection and an Internet gateway in a VPC
C. Configure Direct Connect from the on-premises data center to the VPC network
D. There are no high bandwidth/low latency options for hybrid network connectivity

Correct Answer

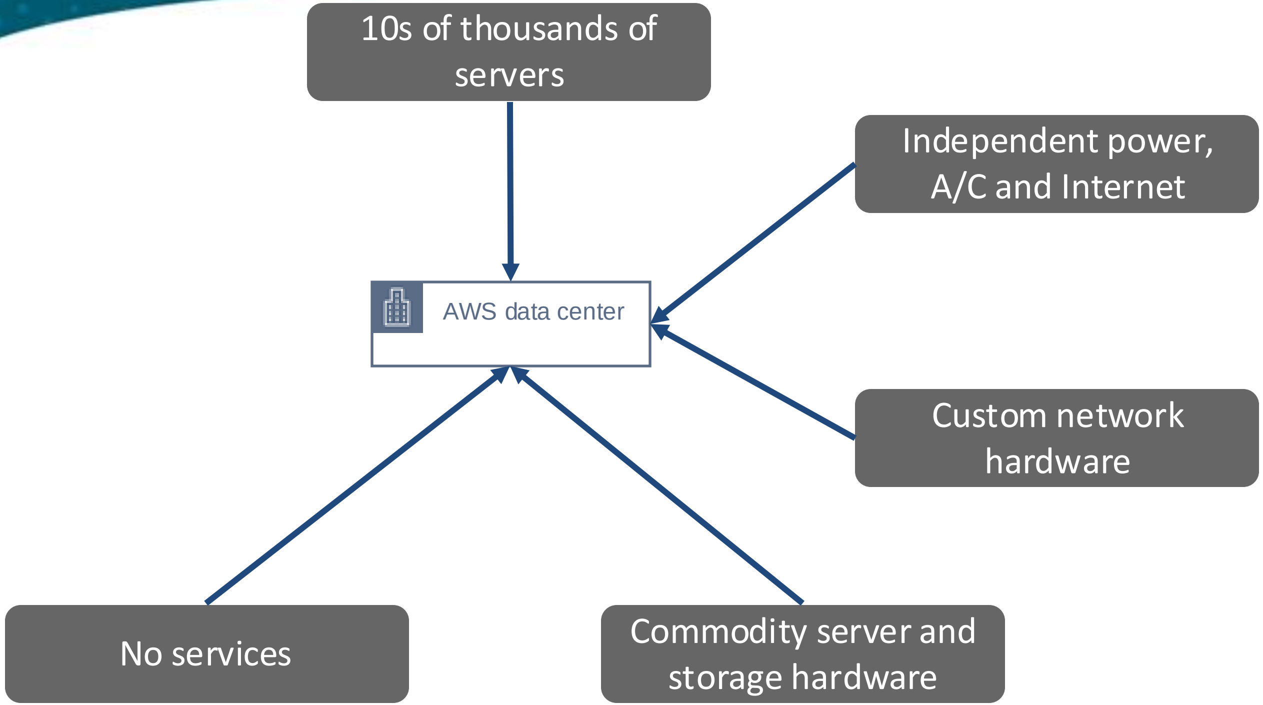
Configure Direct Connect from the on-premises data center to the VPC network

A. VPN using a Virtual Private Gateway
B. Use the on-premises Internet connection and an Internet gateway in a VPC
C. Configure Direct Connect from the on-premises data center to the VPC network
D. There are no high bandwidth/low latency options for hybrid network connectivity

Question Domain 3: Technology

AWS Global Infrastructure

AWS Data Center



10s of thousands of servers

Independent power, A/C and Internet

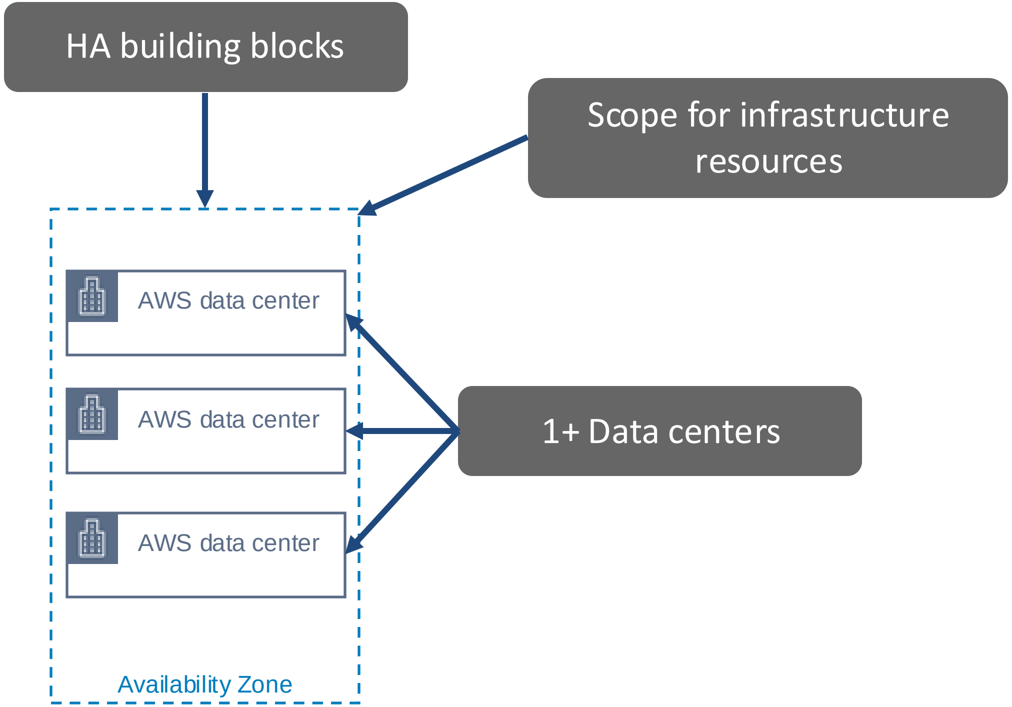
AWS data center

Custom network hardware

No services

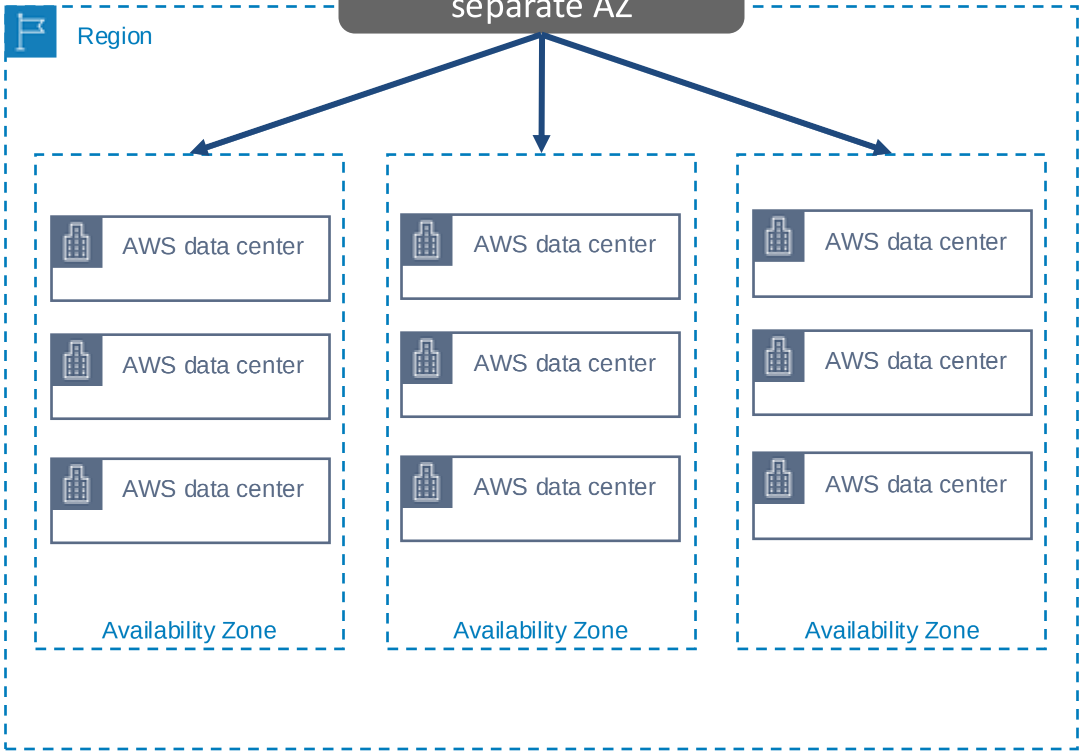
Commodity server and storage hardware

AWS Availability Zone



AWS Region

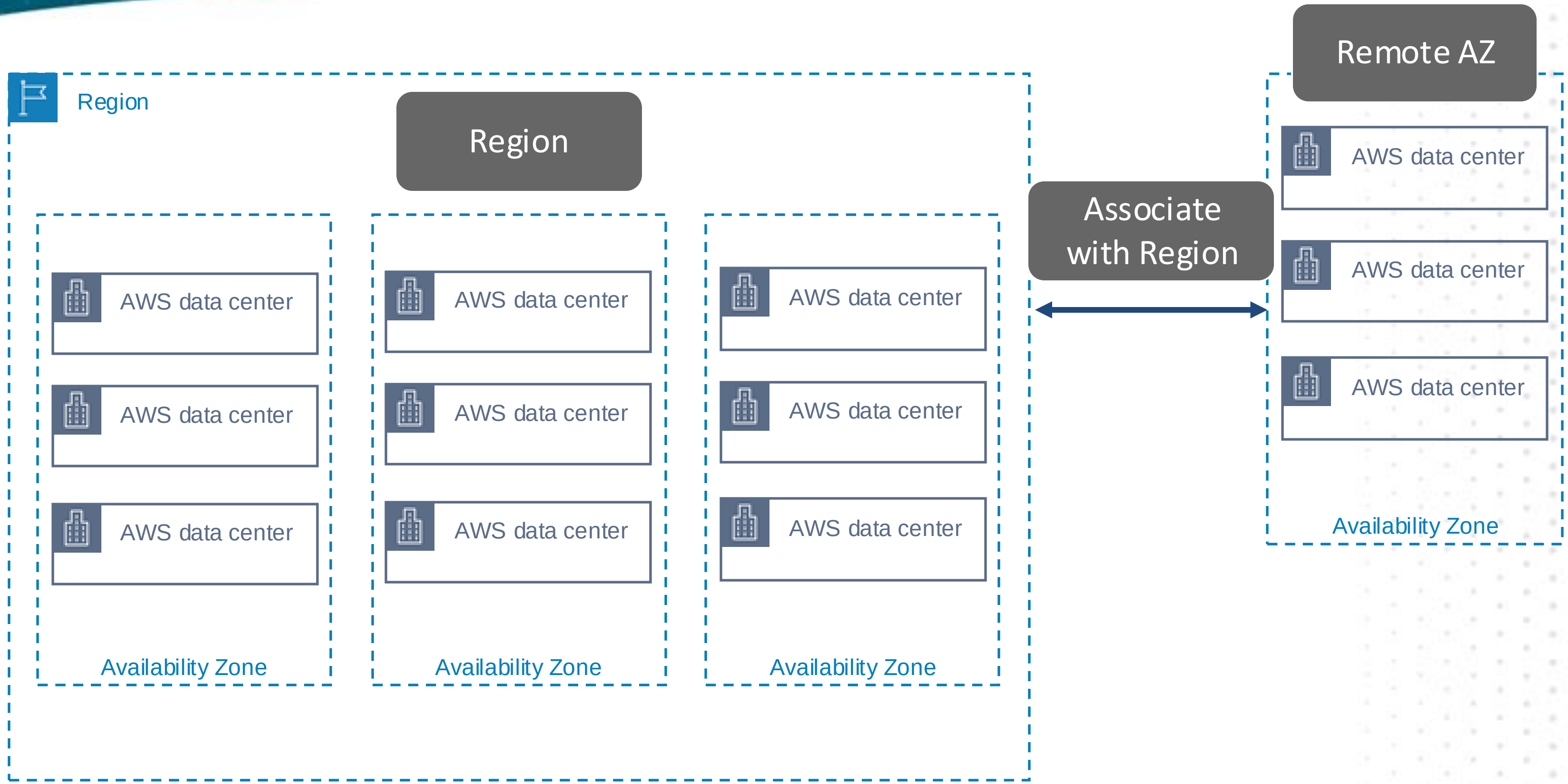
Multiple, physically separate AZ



Service API Endpoints hosted here

Common unit of resource scope

AWS Local Zone



Region Selection Criteria

Service availability

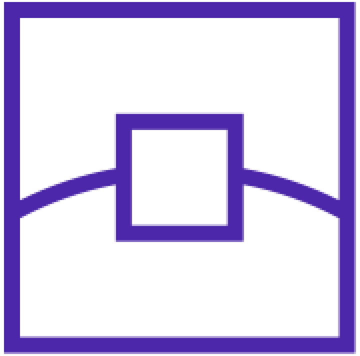
Co-locate with users

Co-locate with infra

Data residency

Multi-region DR

Single Edge Location



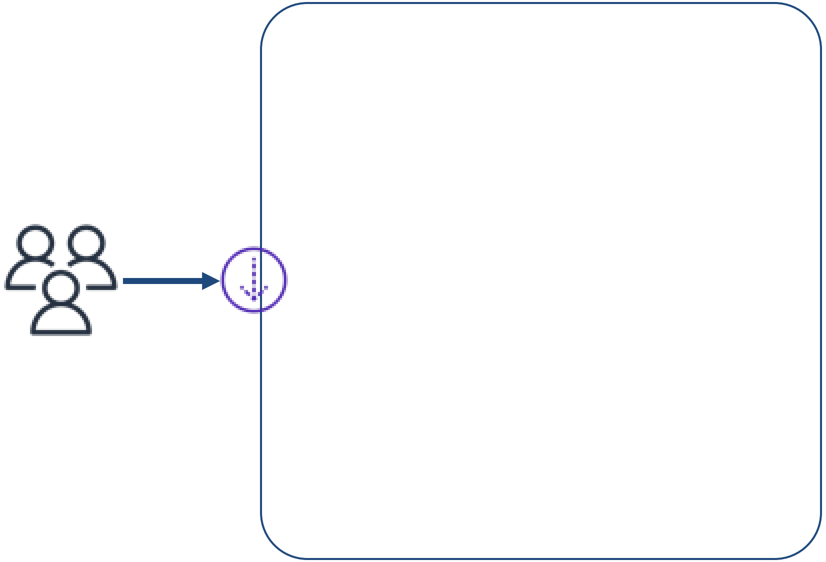
Separate infrastructure from regions

Connected to Region networks

Scope for Global services

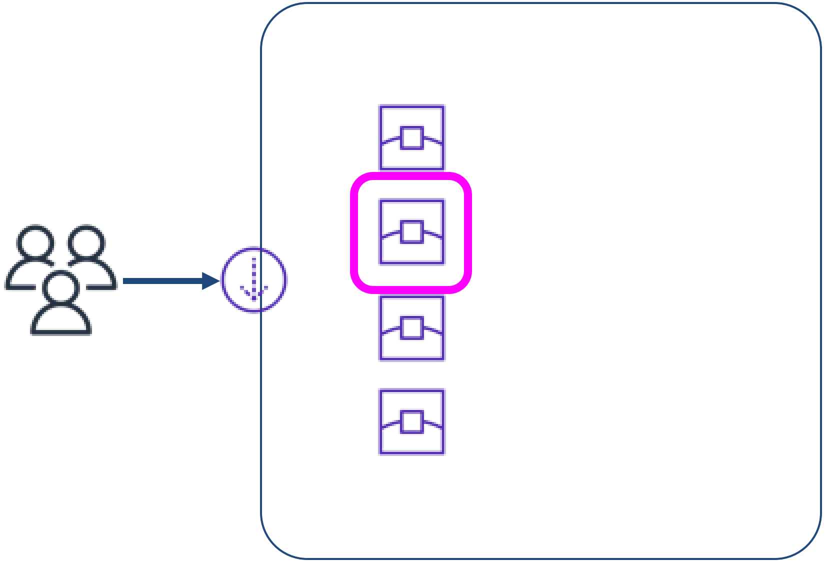
Used for caching

CloudFront Caching Architecture



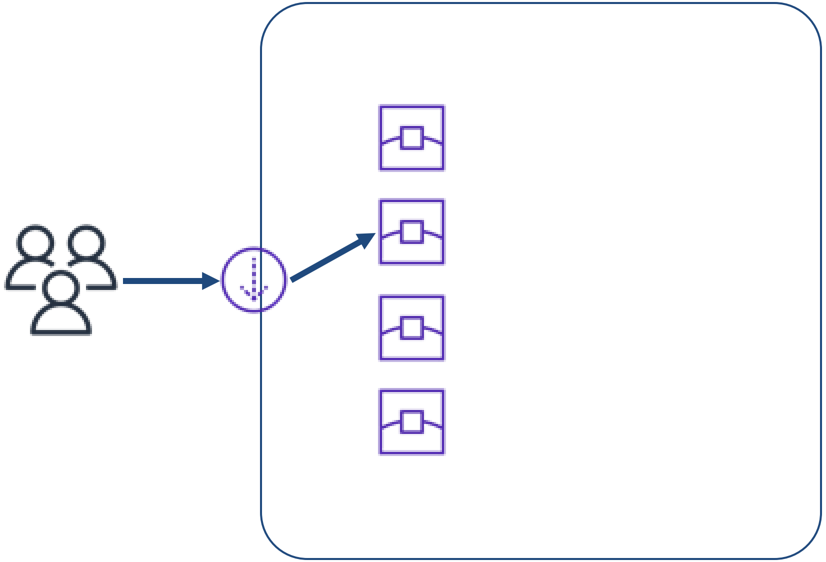
User makes request from CloudFront distribution

CloudFront Caching Architecture



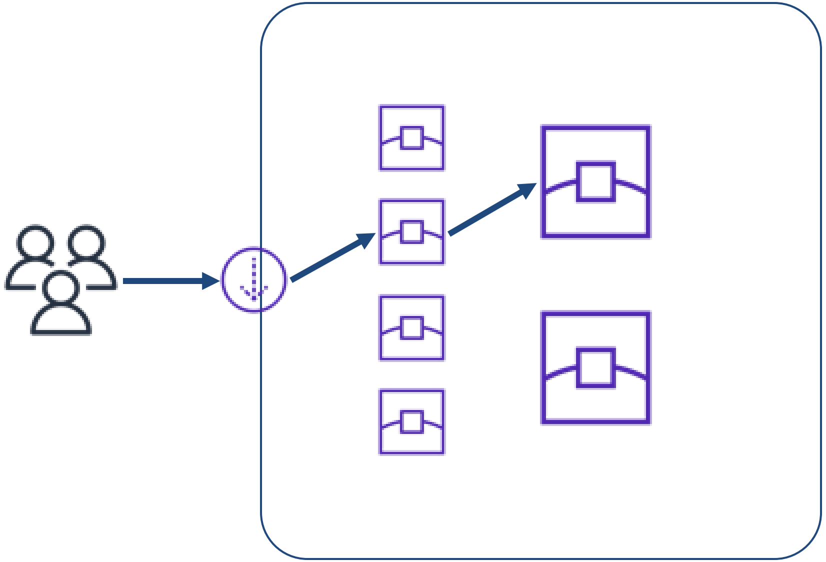
Identify which of 600+ edge locations is nearest

CloudFront Caching Architecture



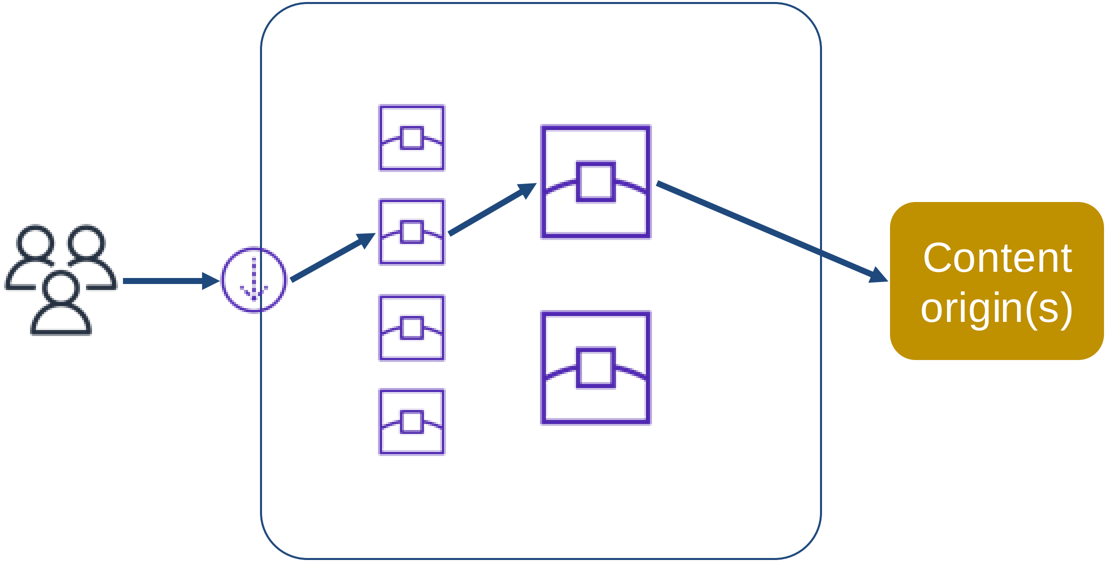
Test for asset in cache and serve to client

CloudFront Caching Architecture



If not cached, test the nearest Regional edge cache for asset

CloudFront Caching Architecture



If not cached, load from origin into both cache layers and serve to client

Question Breakdown

Question and Answer Choices

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

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

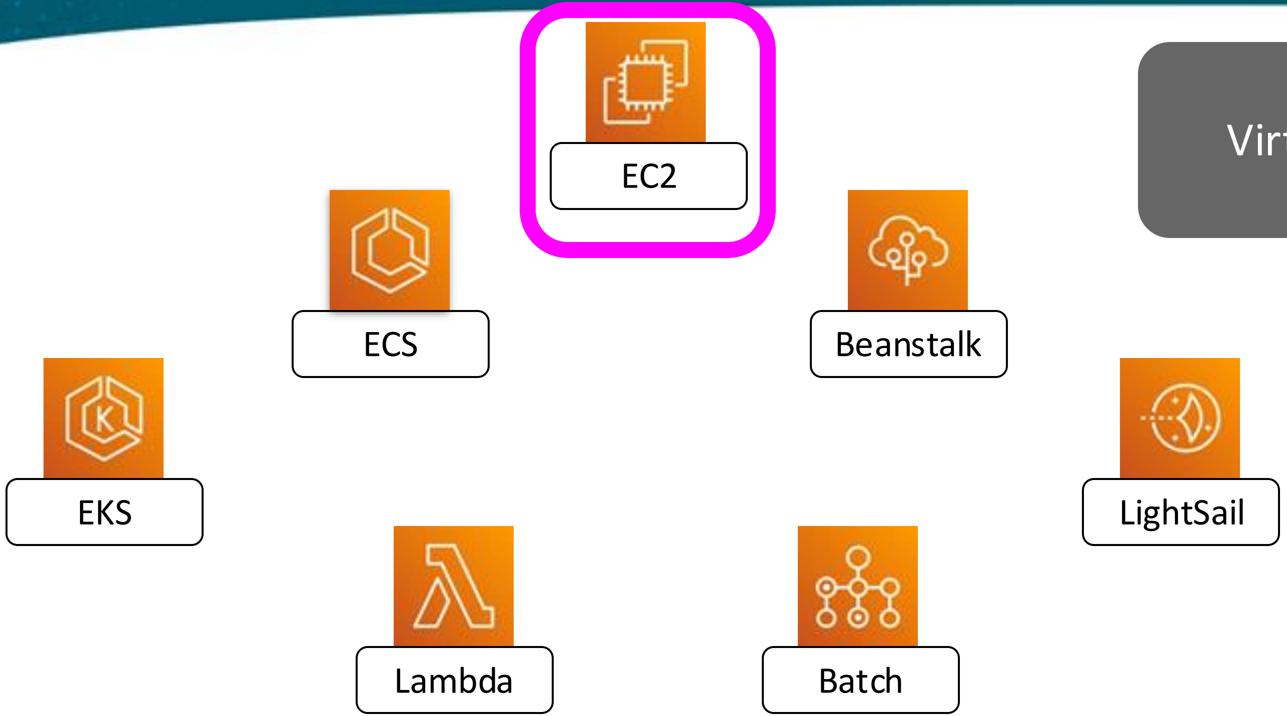
Correct Answer and Explanation

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



EC2

ECS

Beanstalk

EKS

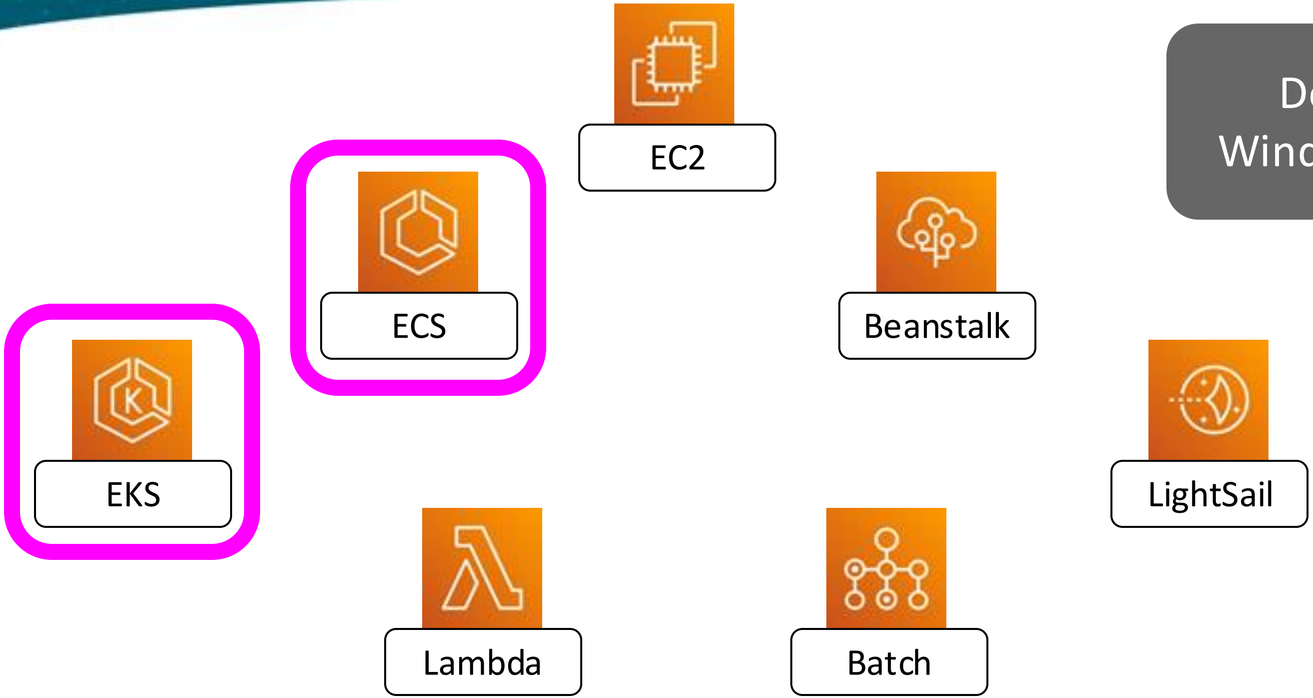
LightSail

Lambda

Batch

Virtual Machines

AWS Compute Services



EC2

ECS

EKS

Beanstalk

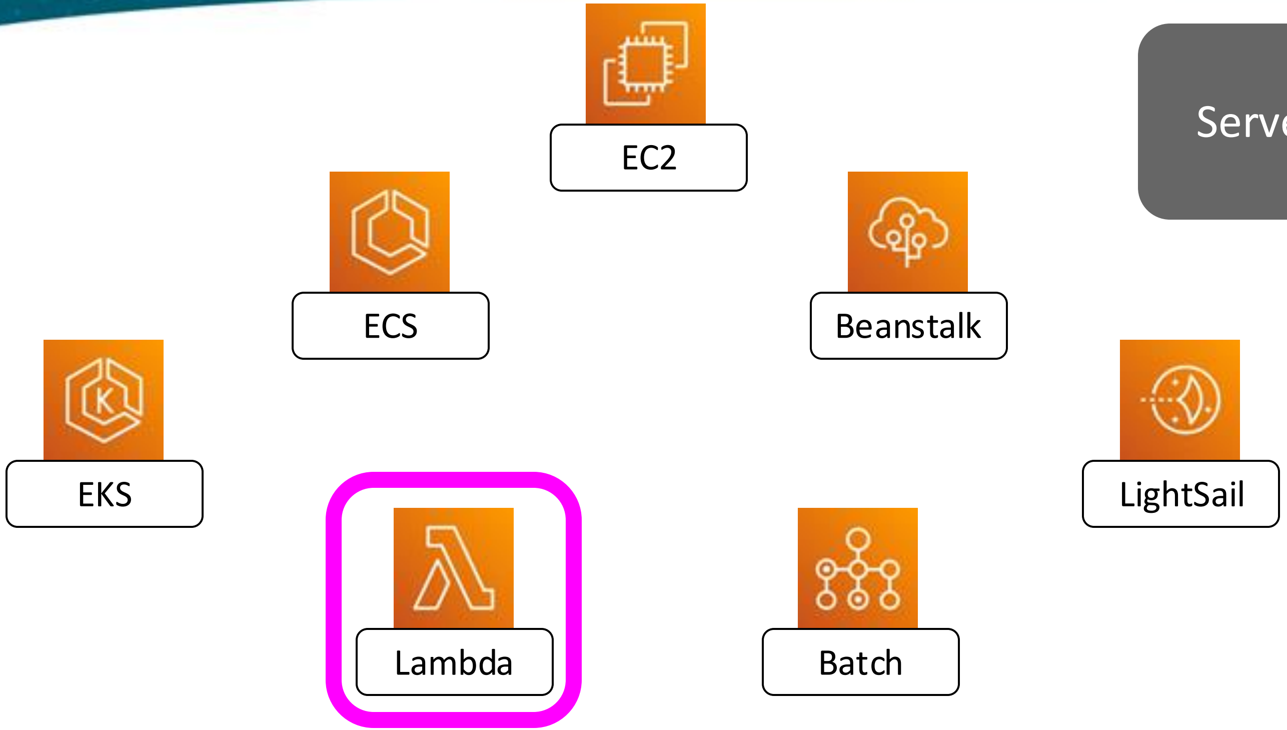
LightSail

Lambda

Batch

Docker and/or Windows Containers

AWS Compute Services



EC2

ECS

Beanstalk

EKS

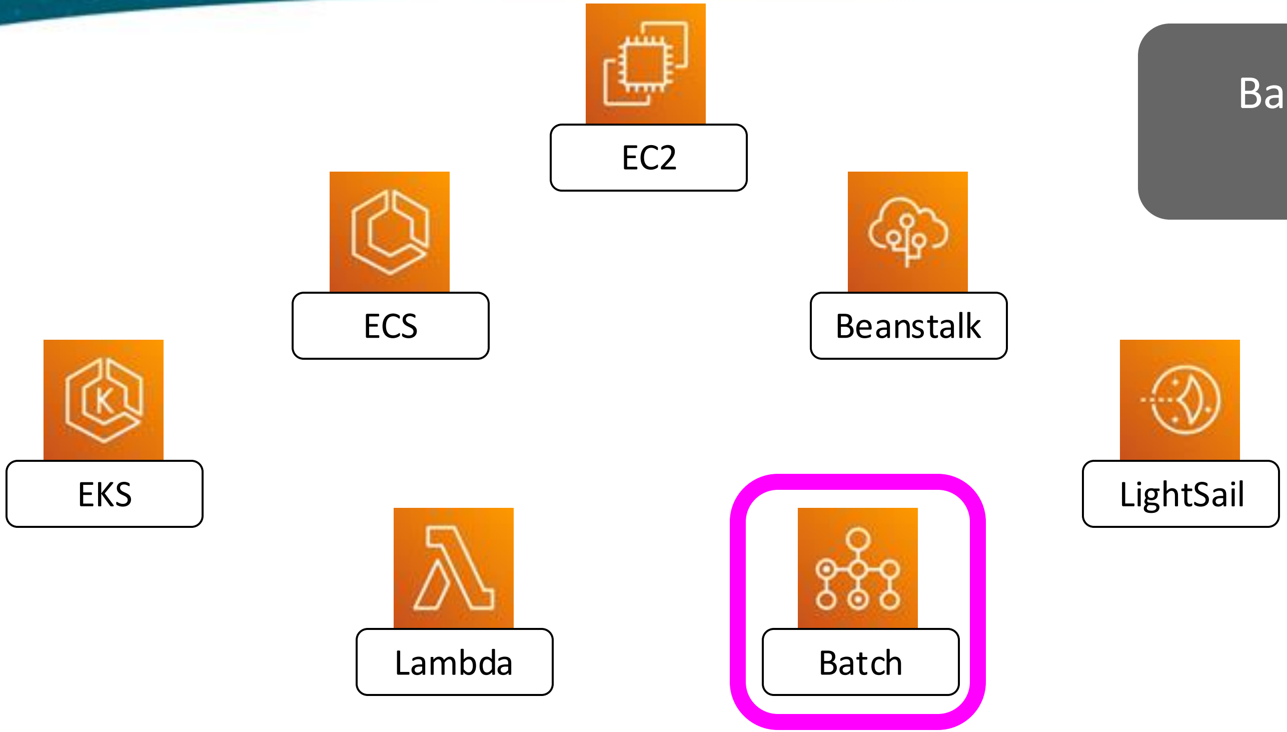
LightSail

Lambda

Batch

Serverless functions

AWS Compute Services



EC2

ECS

Beanstalk

EKS

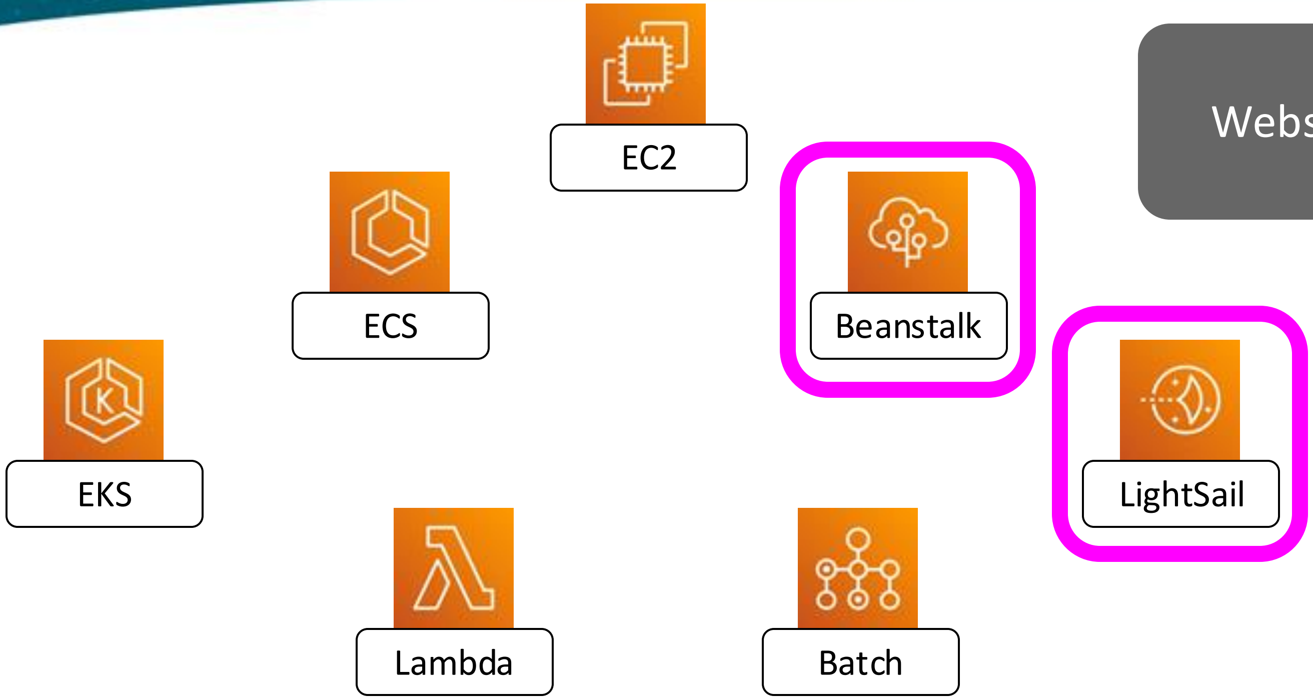
LightSail

Lambda

Batch

Batch container processes

AWS Compute Services



EC2

ECS

Beanstalk

EKS

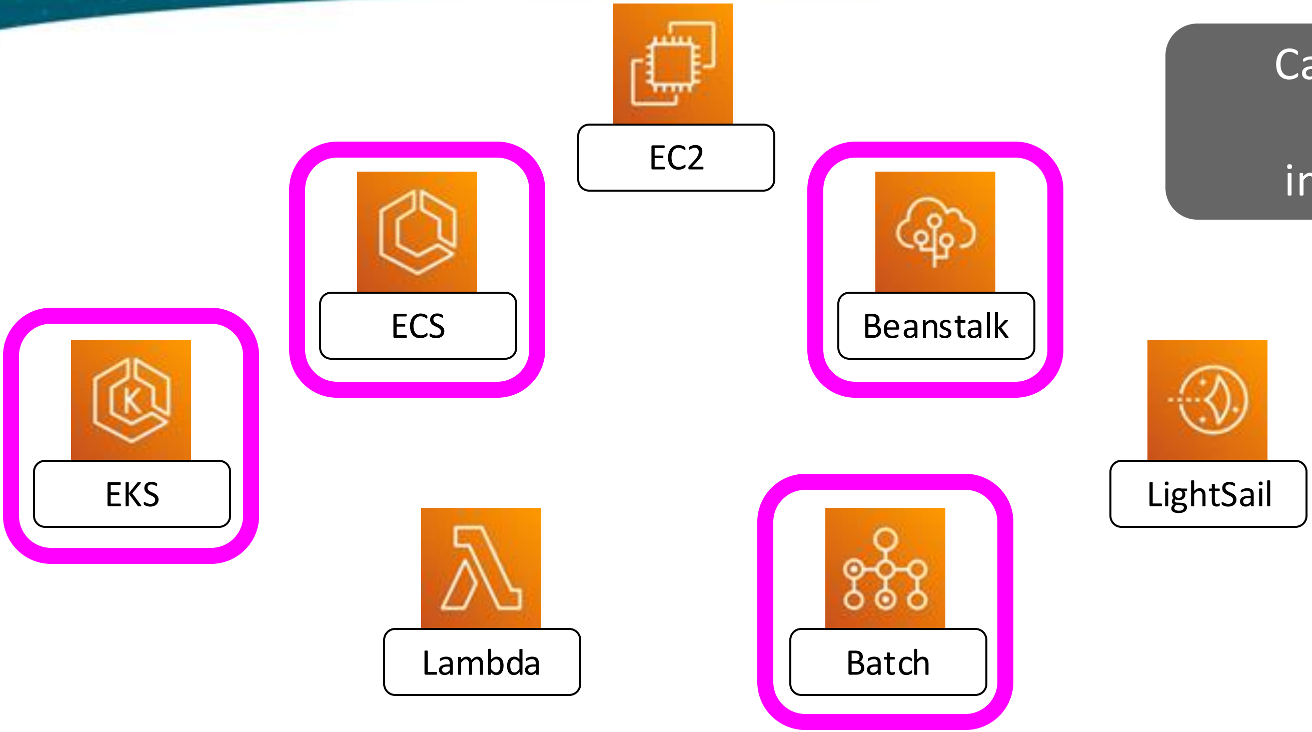
LightSail

Lambda

Batch

Website platforms

AWS Compute Services



EC2

ECS

Beanstalk

EKS

LightSail

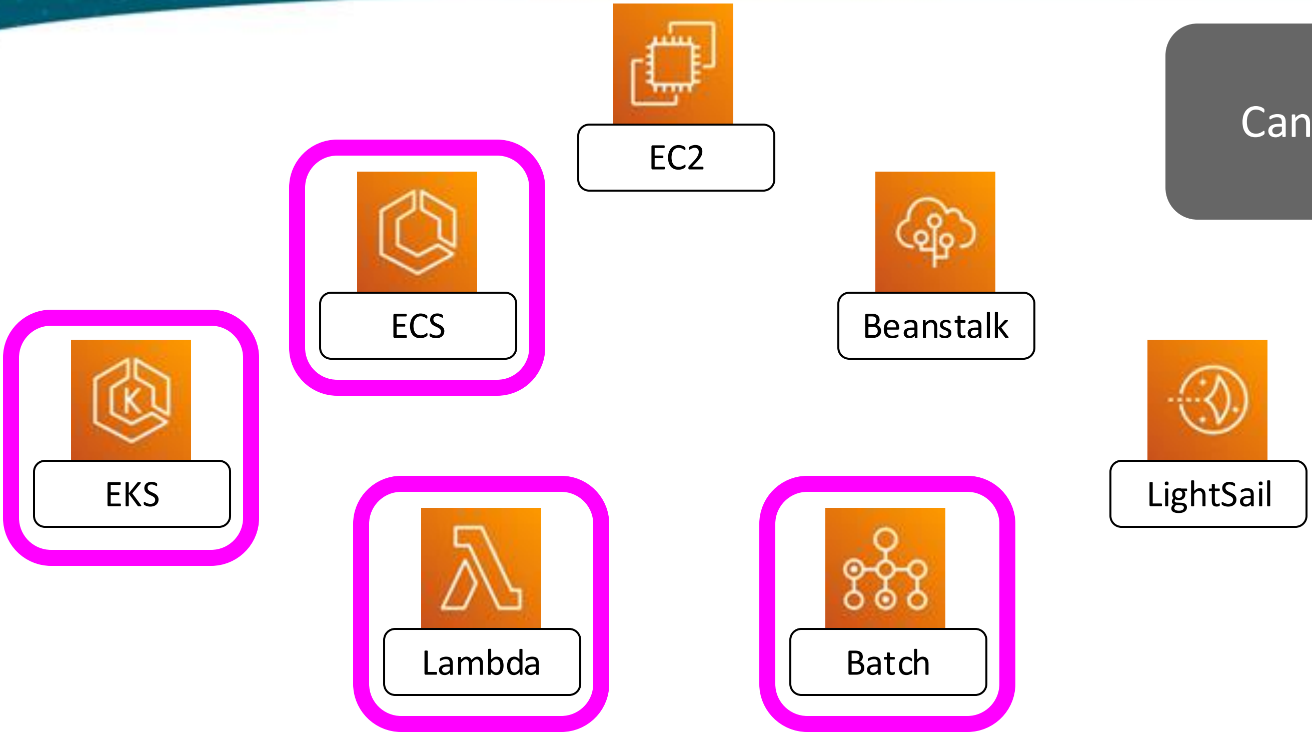
Lambda

Batch

Can use EC2 as underlying infrastructure

AWS Compute Services

Can run serverless



EC2

ECS

Beanstalk

EKS

LightSail

Lambda

Batch

AWS Compute Services

Can run container applications - ALL of these

EC2

ECS

Beanstalk

EKS

LightSail

Lambda

Batch

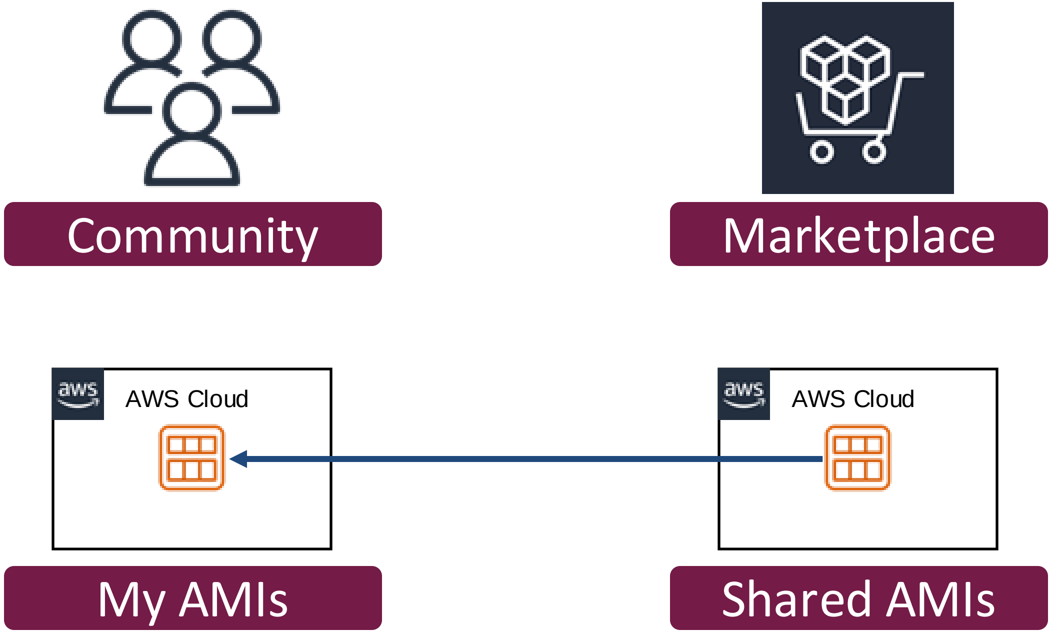
EC2 Basics

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

EC2 AMI Basics

- Amazon Machine Image
- Region scope
- Root volume snapshot
- Launch permissions
- Block device mappings for non-root volumes

EC2 AMI Sources



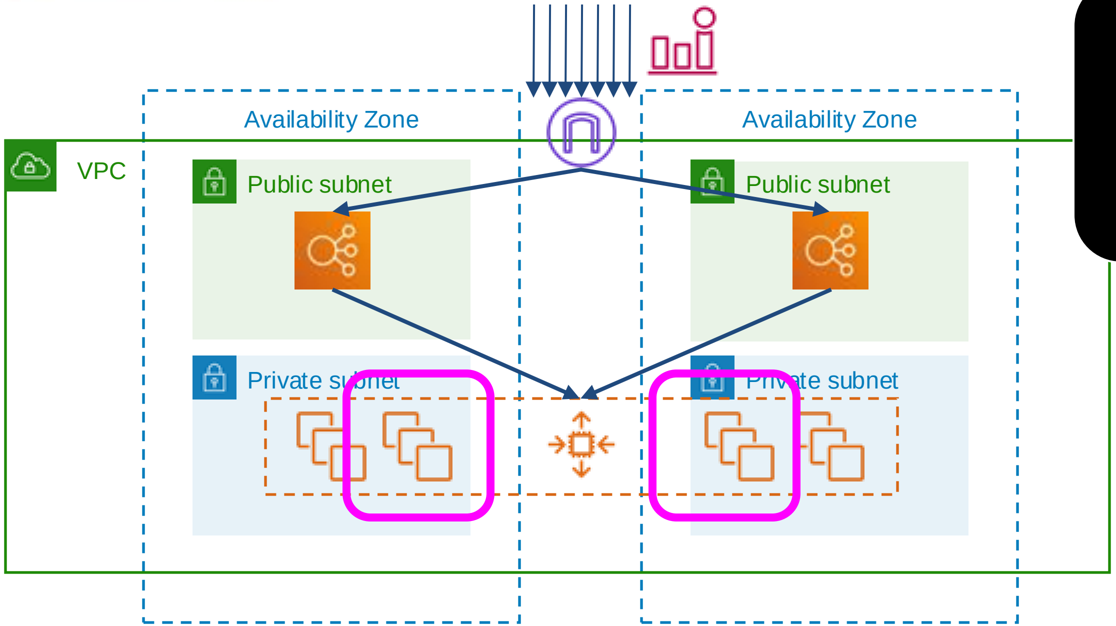
Community

Marketplace

My AMIs

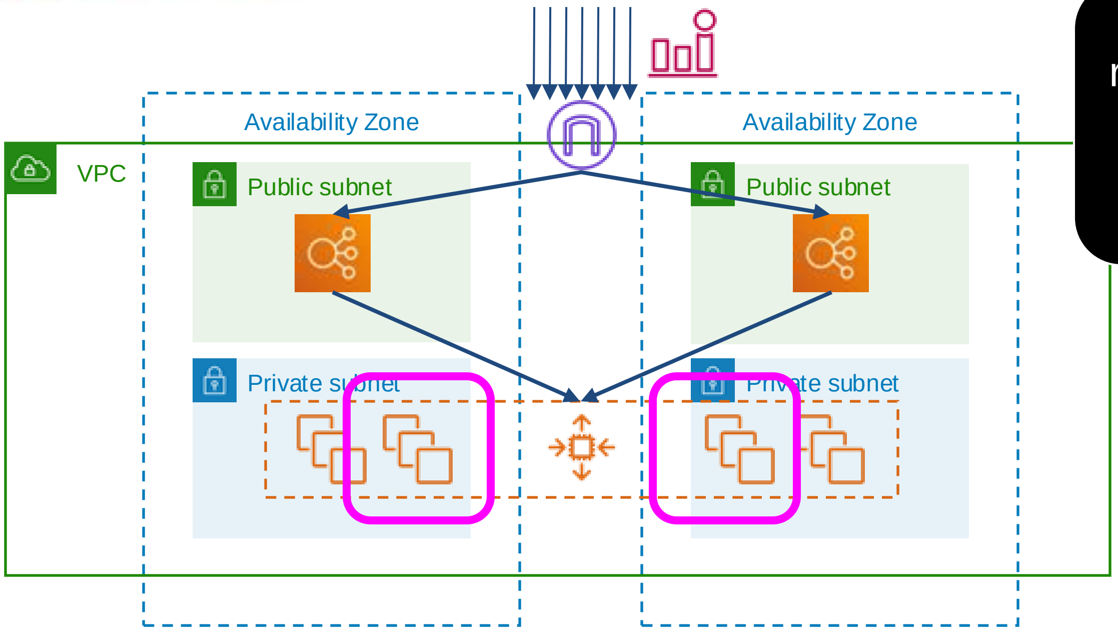
Shared AMIs

What Is Auto Scaling?



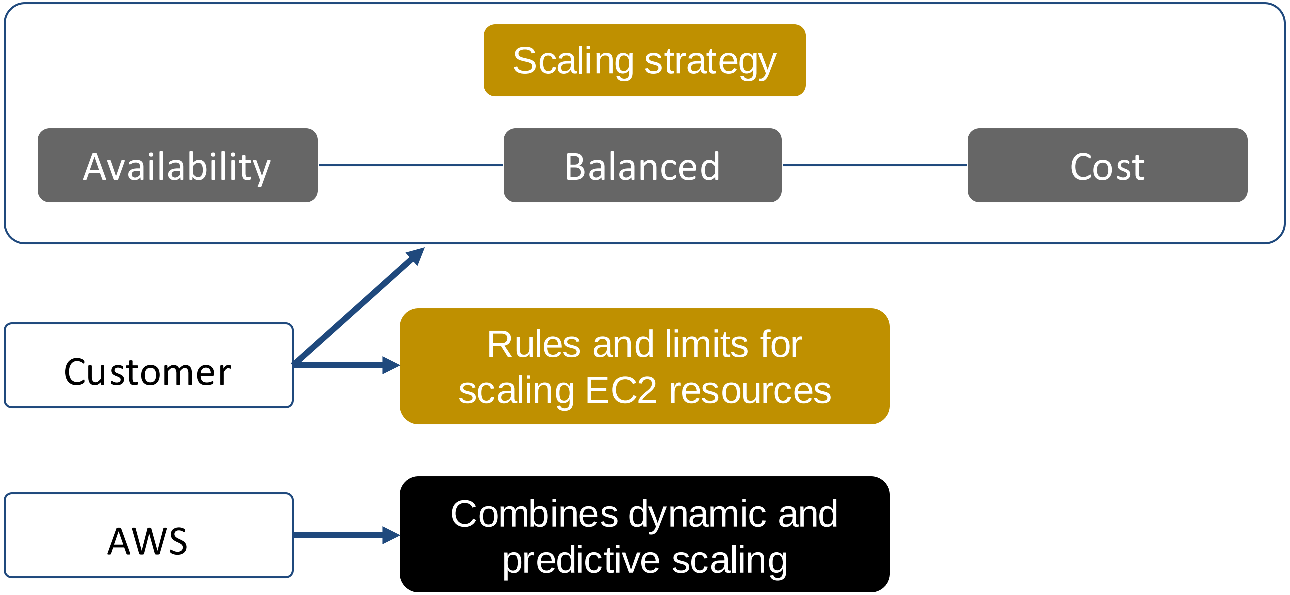
Add EC2 resources into the fleet, scaling capacity to match load

What Is Auto Scaling?



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

What is an Auto Scaling plan?



Scaling strategy

Availability

Balanced

Cost

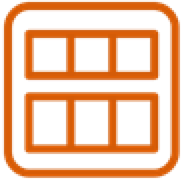
Customer

Rules and limits for scaling EC2 resources

AWS

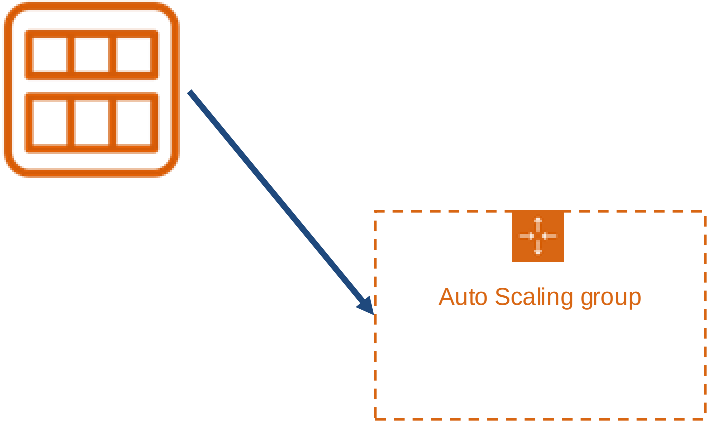
Combines dynamic and predictive scaling

Auto Scaling Architecture



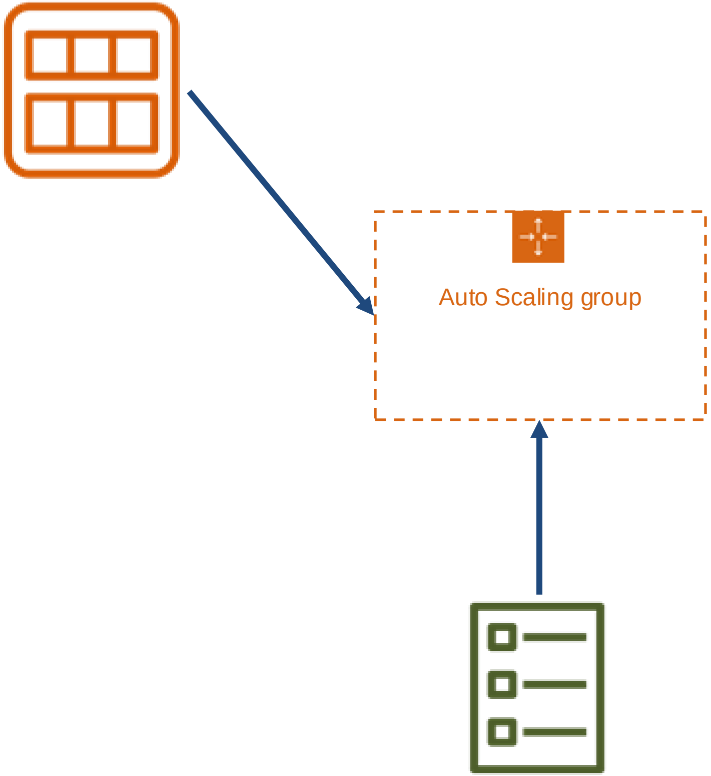
Launch Templates define WHAT to launch

Auto Scaling Architecture



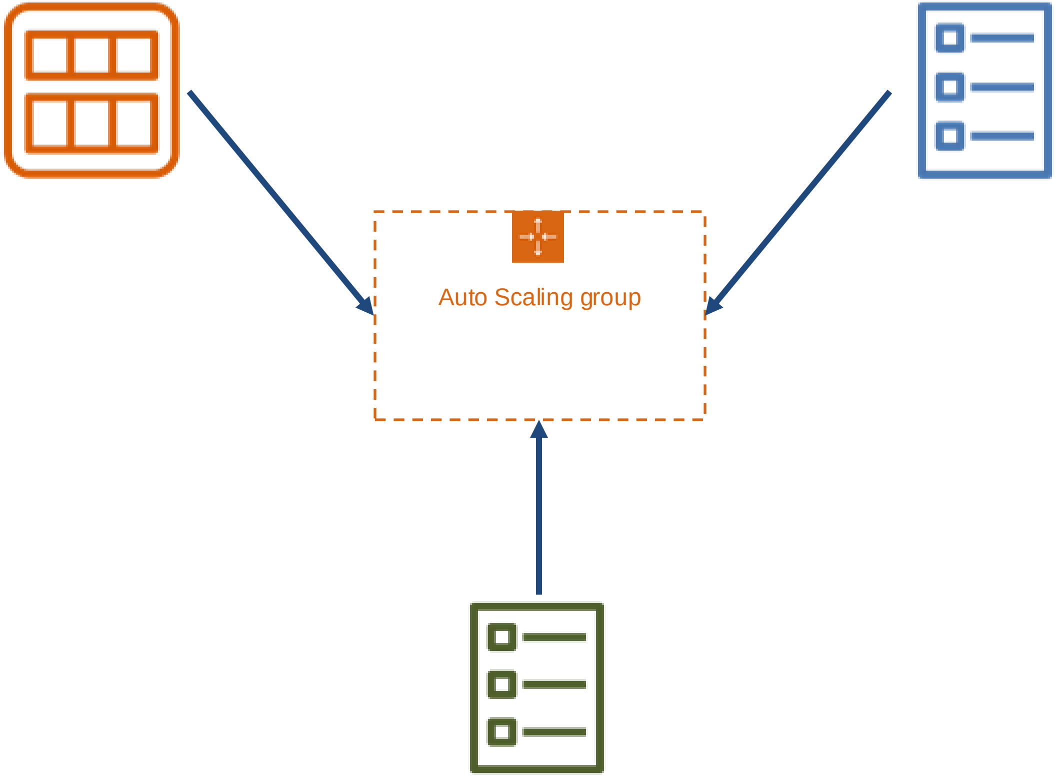
Auto Scaling Groups define LIMITS and ASSOCIATIONS

Auto Scaling Architecture



Scaling Policies define WHEN to scale according to metrics

Auto Scaling Architecture

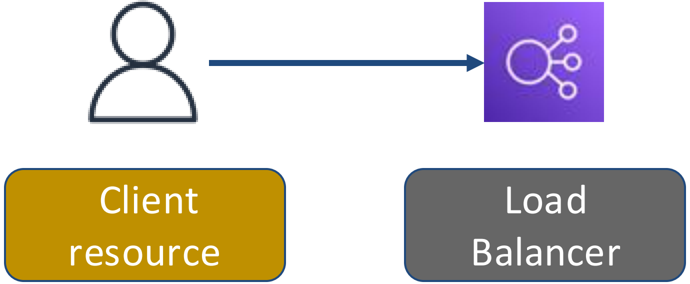


Scheduled Actions define WHEN to scale according to the clock

Elastic Load Balancer Basics

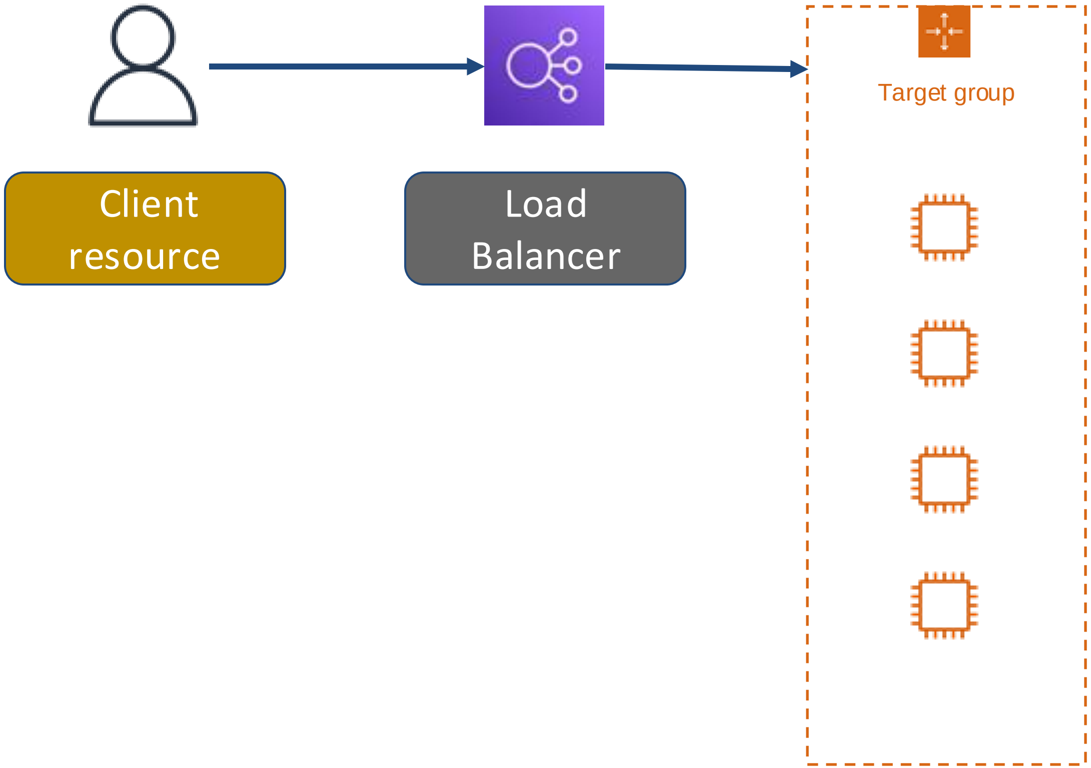
- AZ scoped
- Multi-AZ support
- Managed load balancing service
- Distribute traffic to back end

Load Balancer Architecture



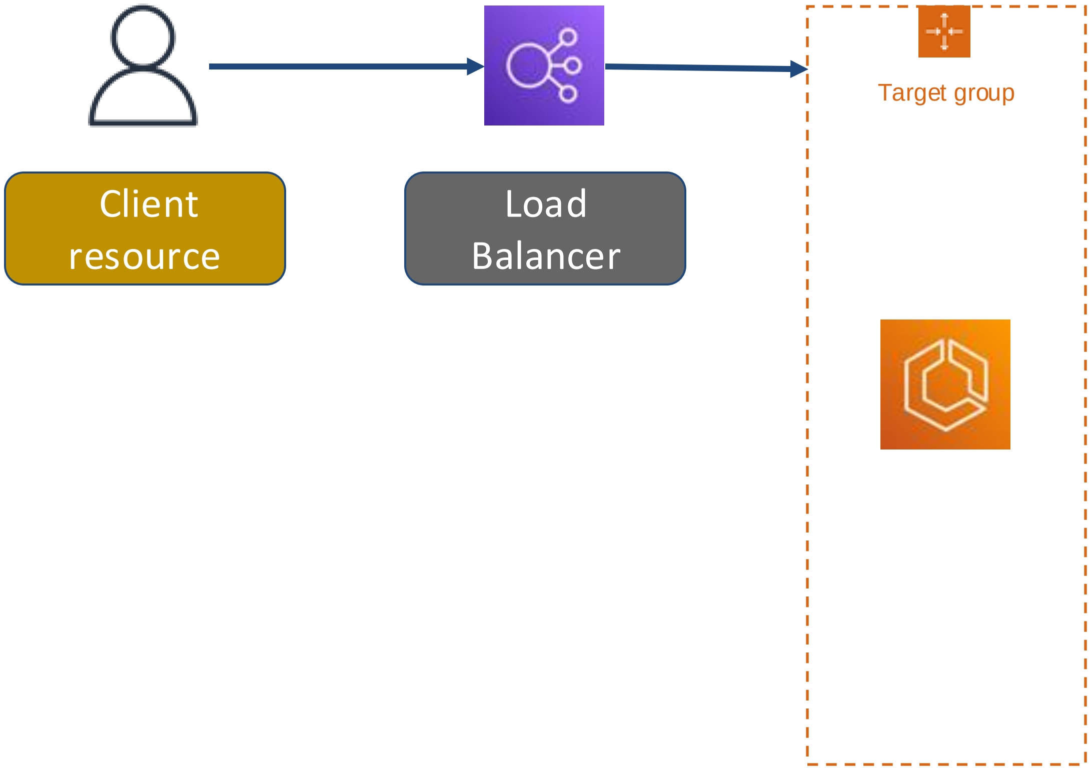
Client sends traffic at layer 4 or 7 to the ELB endpoint

Load Balancer Architecture



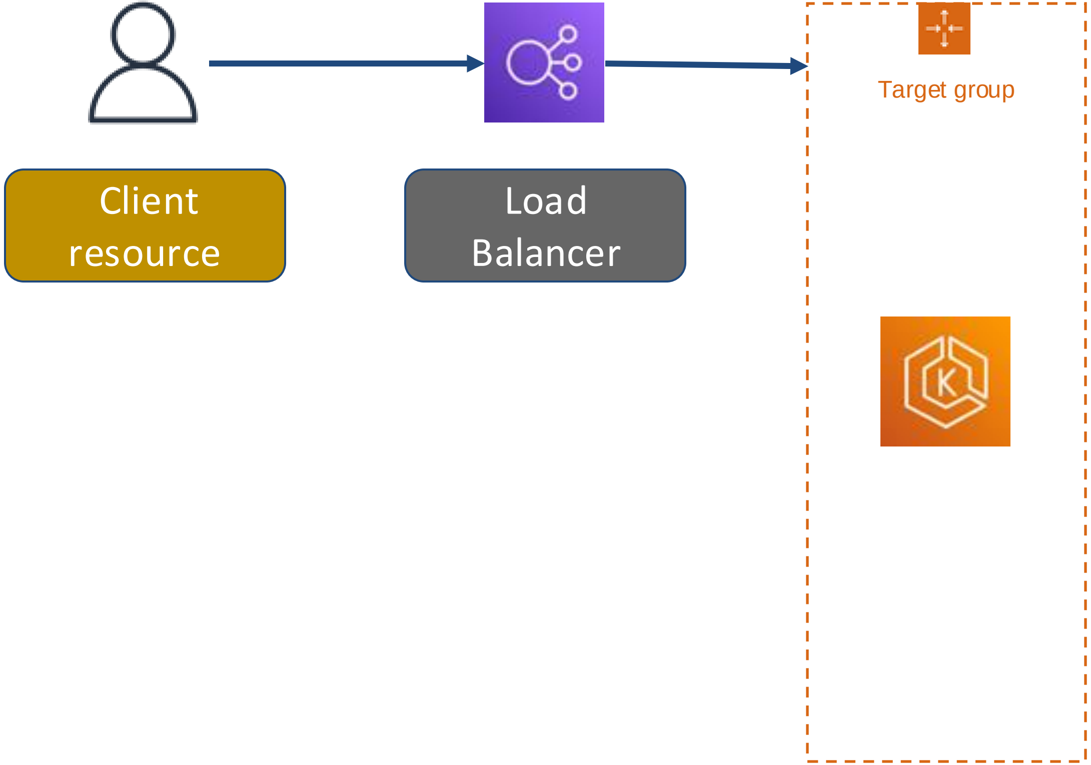
The ELB either proxies or passes traffic through to EC2

Load Balancer Architecture



Or an ECS task

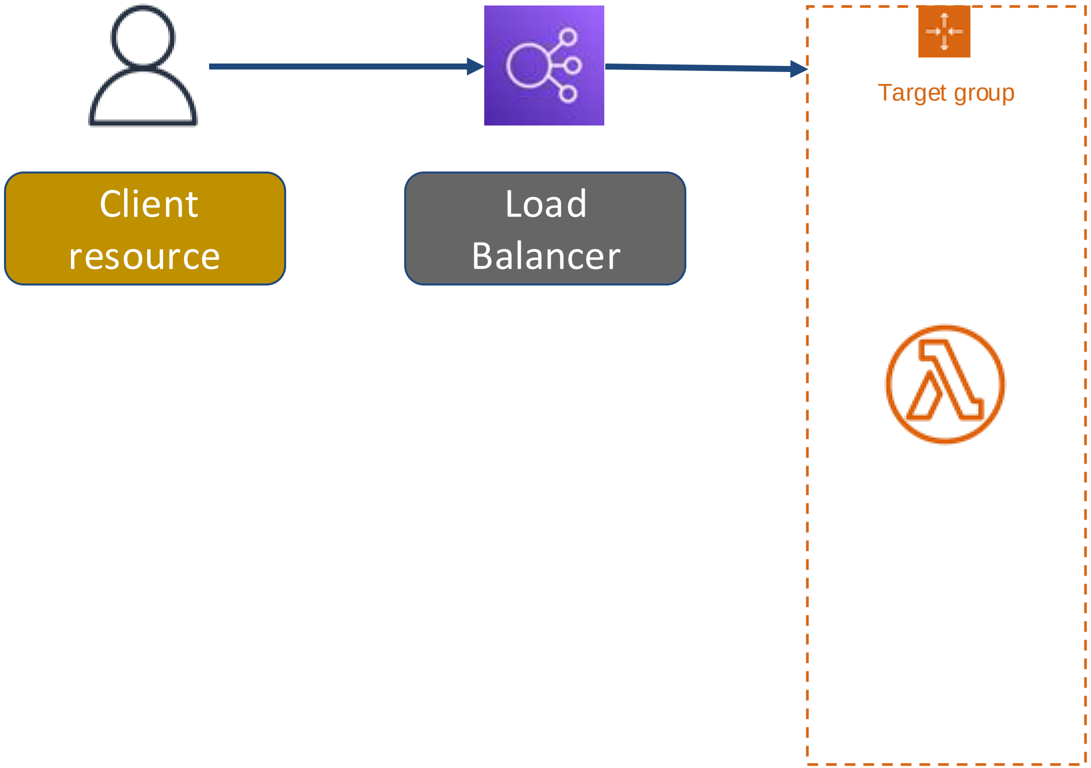
Load Balancer Architecture



Or an EKS container

Pearson

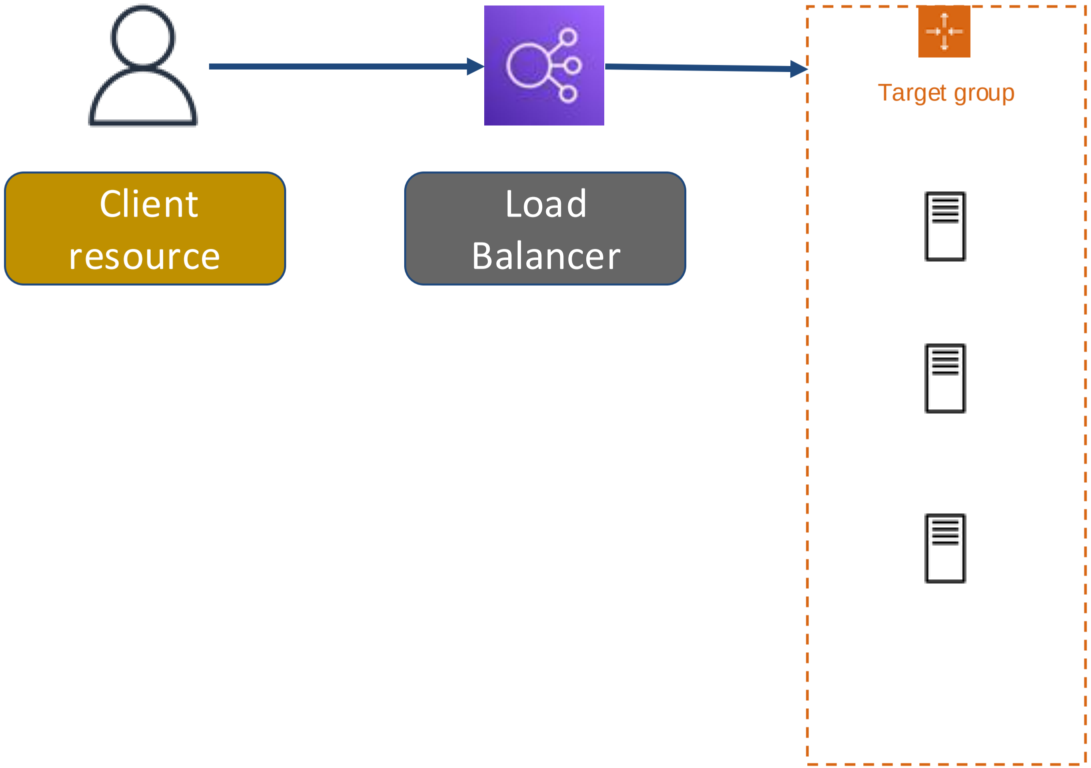
Load Balancer Architecture



Or a Lambda function

Pearson

Load Balancer Architecture



Or on-premises IP endpoints

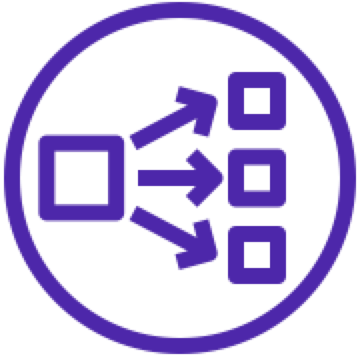
Application Load Balancer Basics

- Layer 7 only
- Internet-facing or internal only
- Multiple TLS certs
- Path-based routing
- Redirect support
- WAF support

ALB Use Cases

- Stateless web applications
- Stateful application servers
- Anything using HTTP or HTTPS

Network Load Balancer Basics



- Layer 4 only
- Internet-facing or internal only
- Multiple TLS certs
- TCP and UDP

NLB Use Cases

- TCP applications
- TCP/UDP combo listeners
- High performance
- Low latency

GateWay Load Balancer Basics

- Layer 3 only
- deploy, manage and scale virtual appliances
- Deep packet inspection

GWLB Use Cases

- Outbound web proxy
- Data Loss Prevention
- Network intrusion detection & prevention
- Deep packet inspection

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

EBS Basics

- Elastic Block Store
- AZ scope
- EC2 block storage
- HDD or SSD
- OS views as local block device

AWS File Storage Services

Block storage

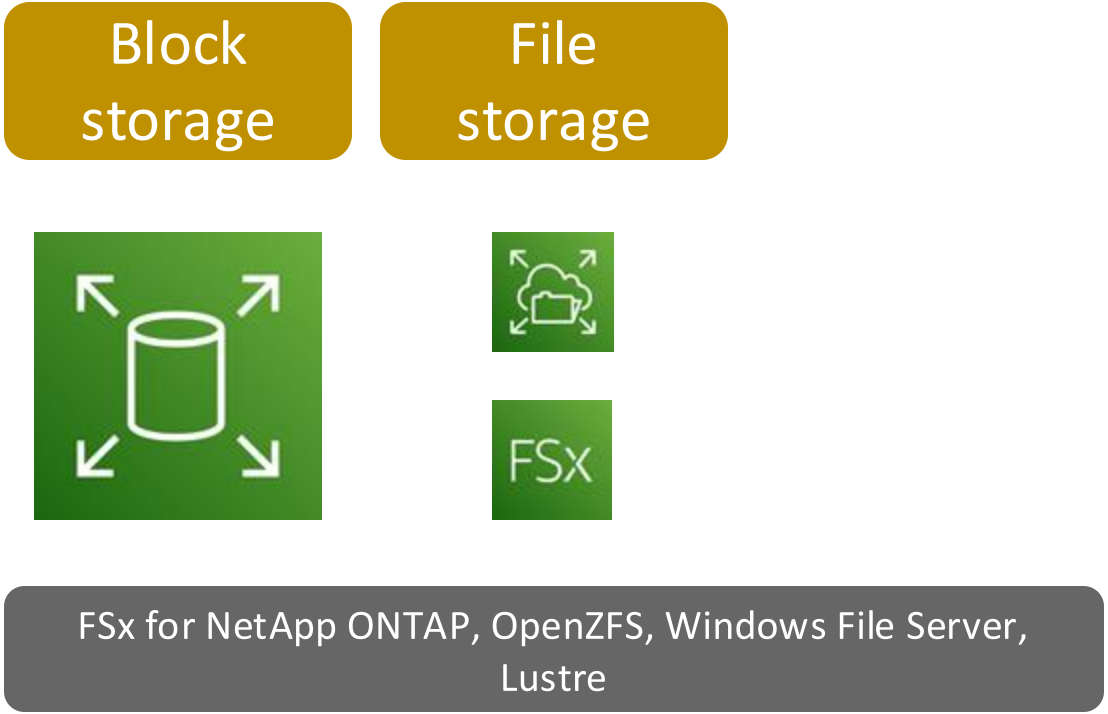
File storage

EFS is a managed NFSv4 service

EFS Basics

- Elastic File System
- Region scope file system
- AZ scope mount targets
- Managed NFSv4
- Data replicated for durability

AWS File Storage Services



Block storage

File storage

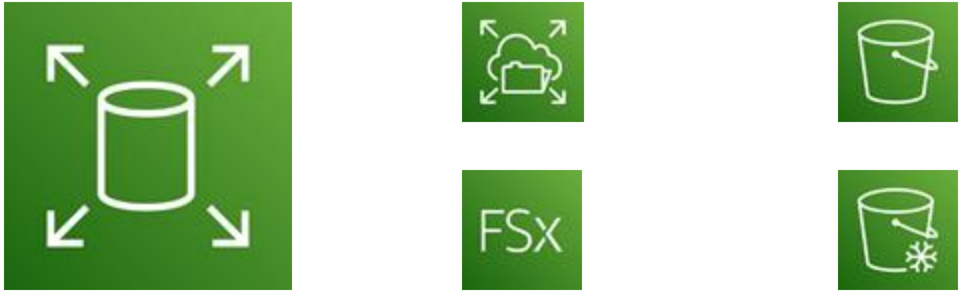
FSx for NetApp ONTAP, OpenZFS, Windows File Server, Lustre

AWS Object Storage Services

Block storage

File storage

Object storage

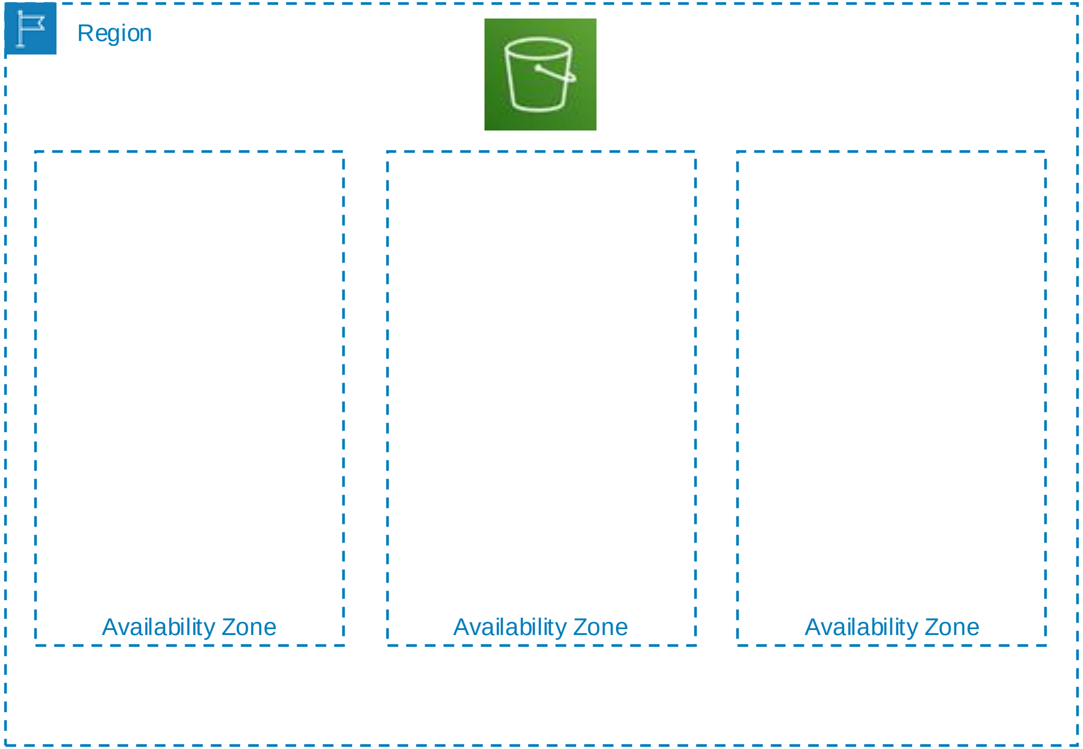


S3 and Glacier are designed for object (WORM - Write Once, Read Many) storage and do not behave like filesystems

S3 Basics

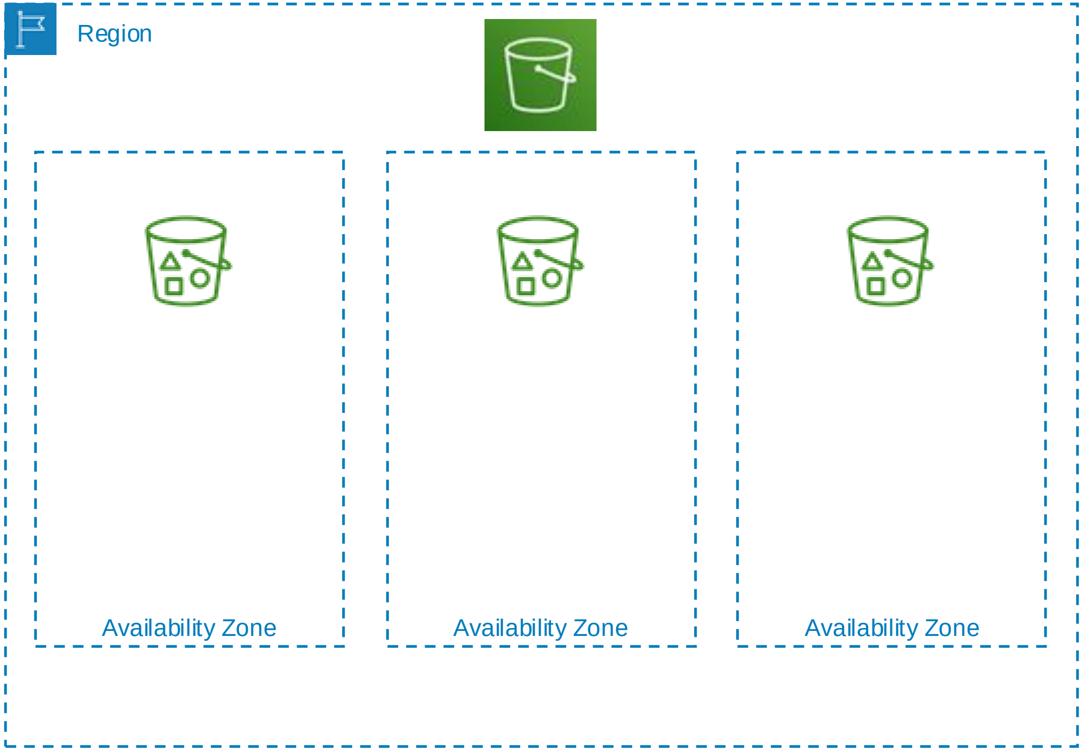
- Simple Storage Service
- Region scope
- Object storage
- Buckets and objects
- Designed for durability

S3 Storage Architecture



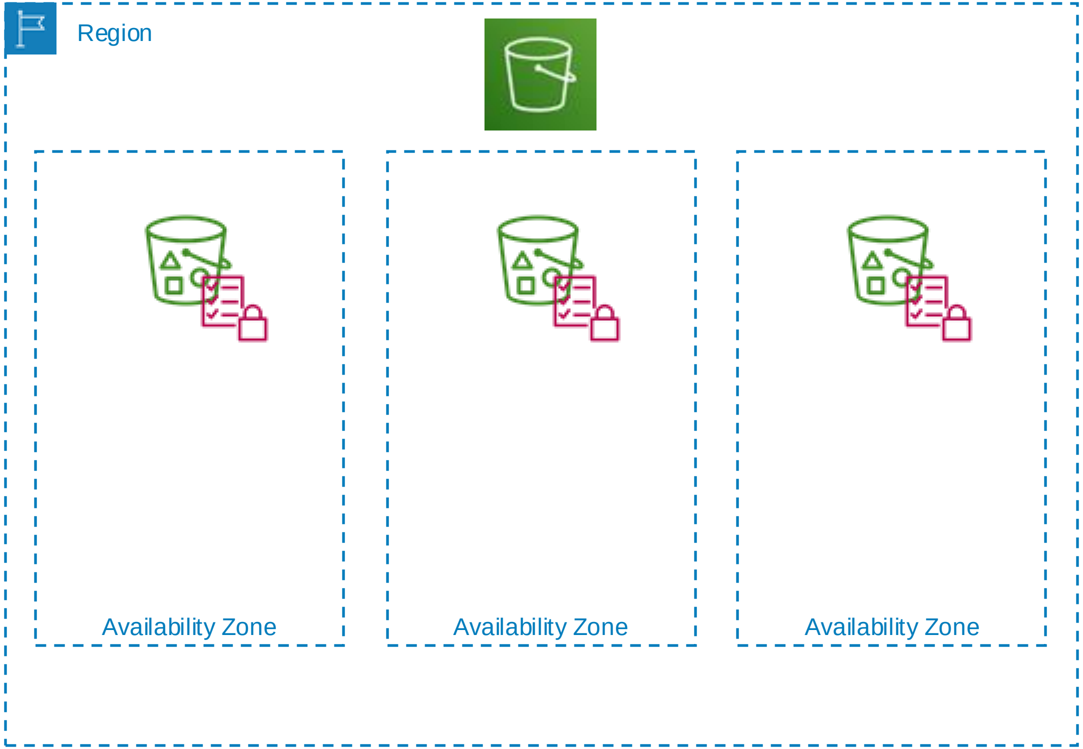
A bucket is a region-scoped logical container for configuration and permissions

S3 Storage Architecture



An object consists of data and metadata and is replicated in 3 AZs within the region

S3 Storage Architecture



Each copy of the object is validated via checksum and replaced if checksum fails to match

Other Storage Services

On-premises storage

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

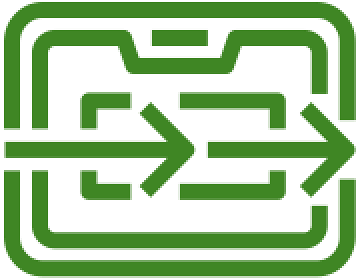
Storage Gateway Basics

- Virtual appliance
- Requires direct-attached storage (on-premises)
- Requires EBS storage (EC2)

Storage Gateway Types

- S3 File Gateway
- FSx File Gateway
- Tape Gateway
- Volume Gateway

Snowball Basics



- Hardware appliance
- Object store
- Encrypted at rest
- Up to 100 Tb capacity

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 but doesn't have any network bandwidth to spare for the migration. Which AWS service would be appropriate for this migration?

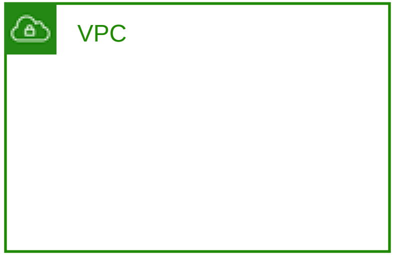
A. S3
B. EFS
C. Direct Connect
D. Snowball

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.

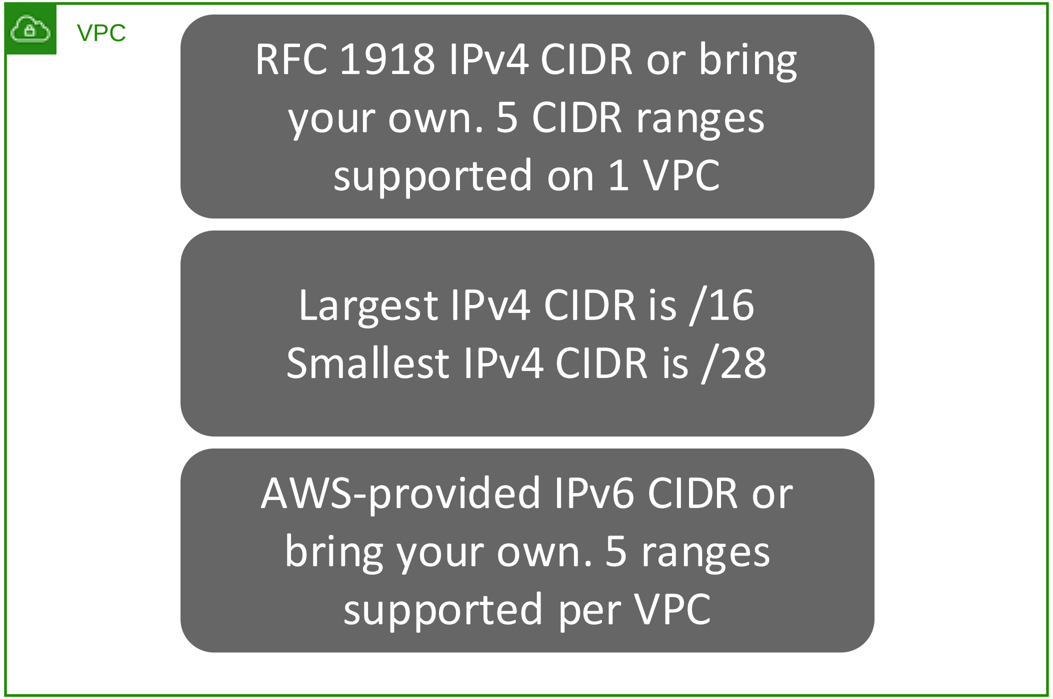
A. S3
B. EFS
C. Direct Connect
D. Snowball

VPC Basics



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

VPC CIDR Addresses



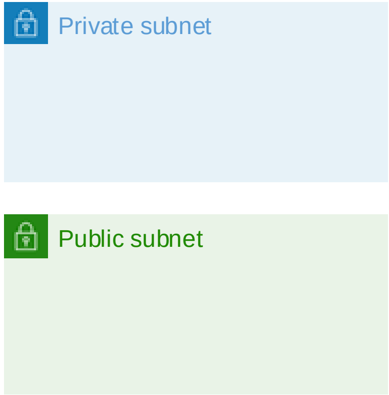
VPC

RFC 1918 IPv4 CIDR or bring your own. 5 CIDR ranges supported on 1 VPC

Largest IPv4 CIDR is /16
Smallest IPv4 CIDR is /28

AWS-provided IPv6 CIDR or bring your own. 5 ranges supported per VPC

Subnet Basics

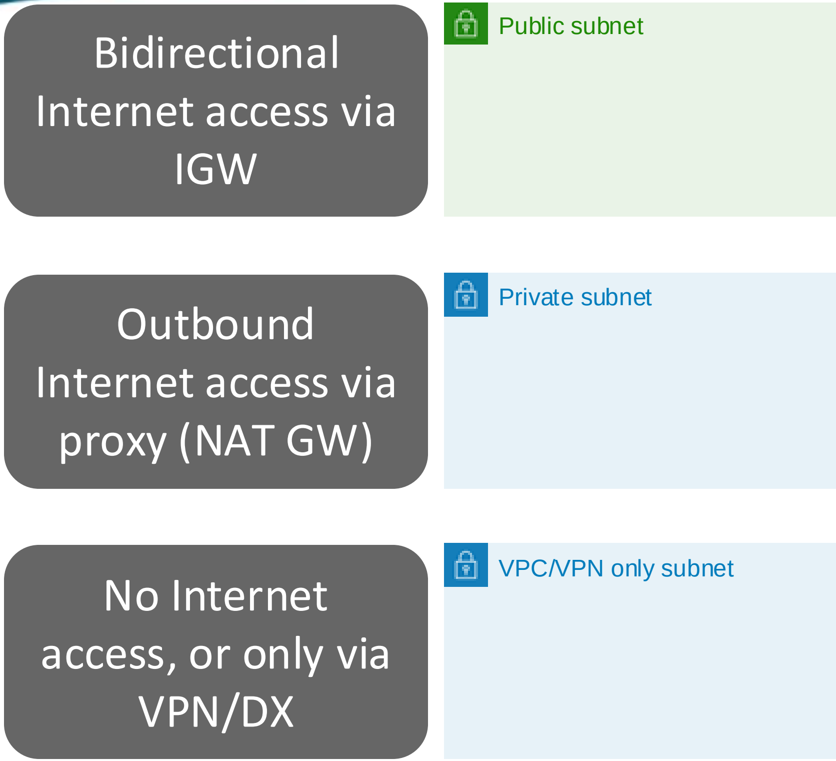


Private subnet

Public subnet

- 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

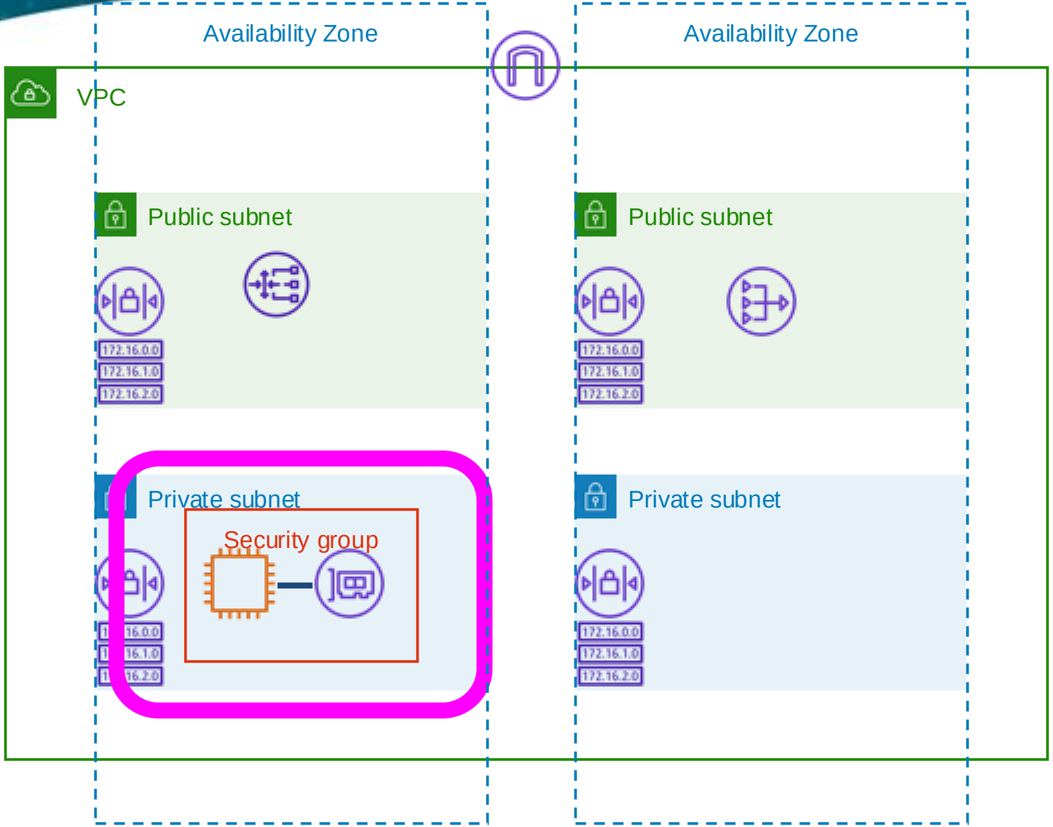
VPC/VPN only subnet

AWS reserves 5 IP addresses from each subnet for internal use

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!

Pearson

Site-to-Site VPN Basics

- Attach to VPC
- Hardware-backed
- IPSEC encryption
- Connect on-prem network to a VPC network

Direct Connect Basics

- On-prem to AWS network connectivity
- Connect to AWS services
- Connect to VPC networks
- Requires BGP and 802.1q VLANs

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

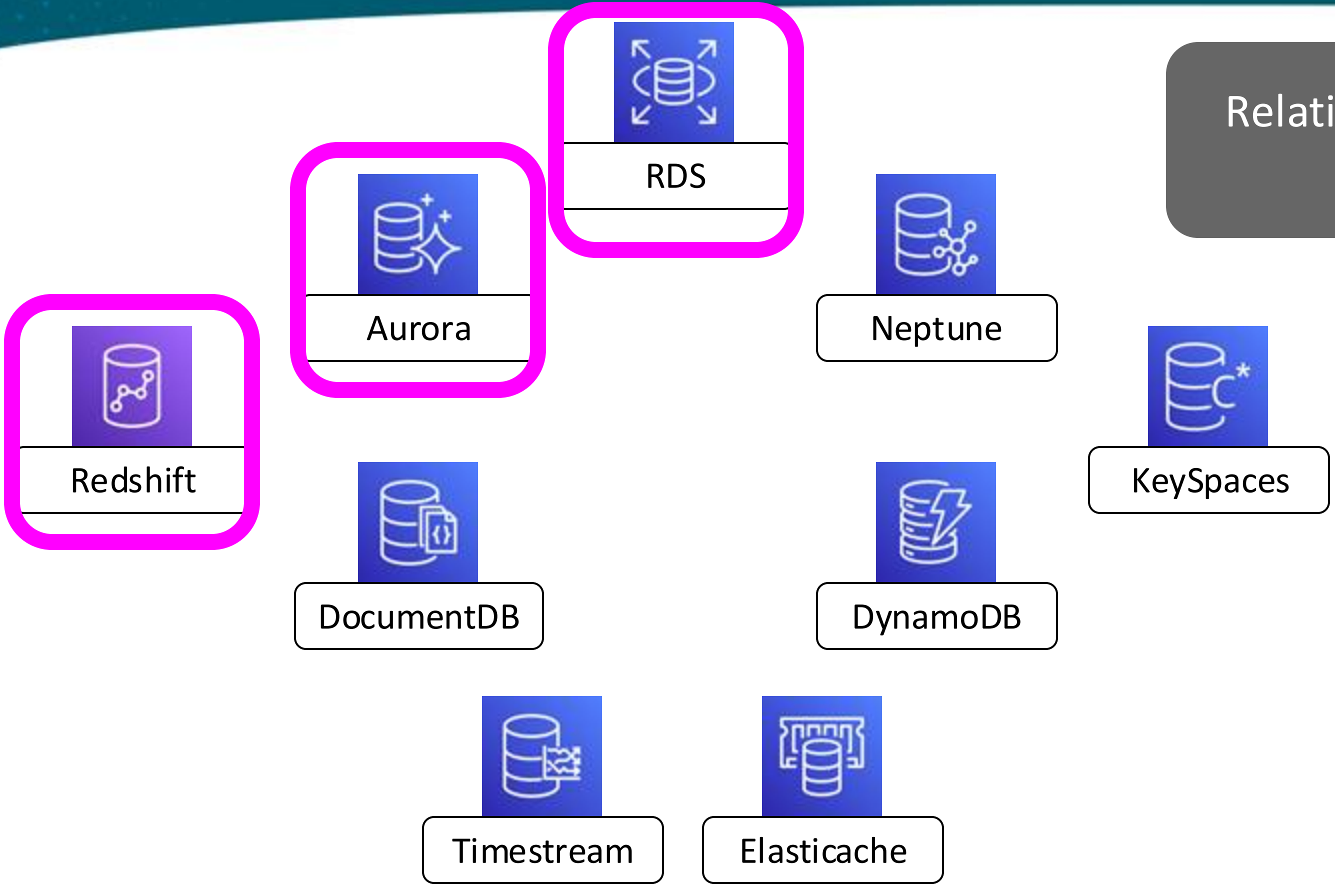
Correct Answer and Explanation

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



RDS

Aurora

Neptune

Redshift

KeySpaces

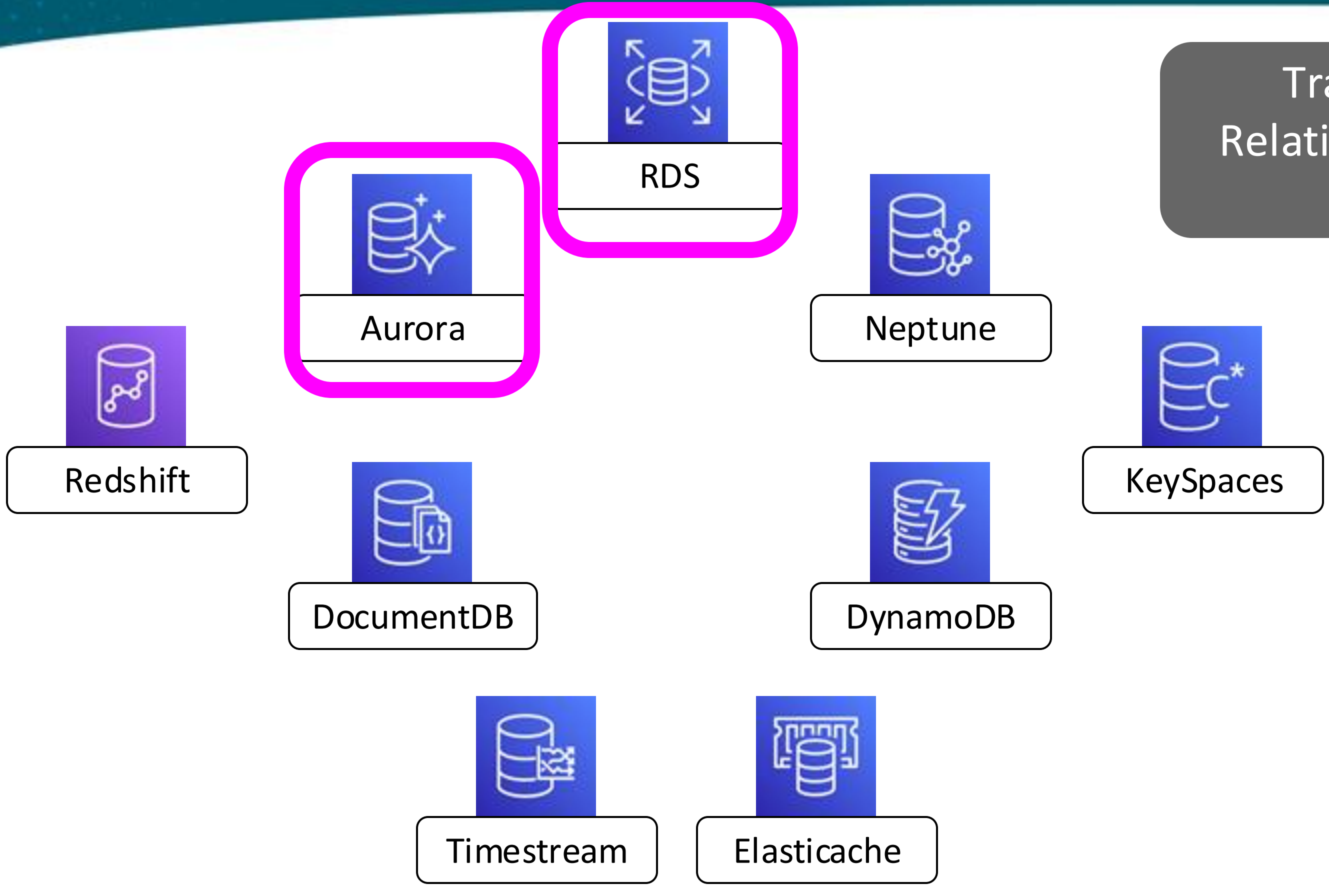
DocumentDB

DynamoDB

Timestream

Elasticache

AWS Database Services



RDS

Aurora

Neptune

Redshift

KeySpaces

DocumentDB

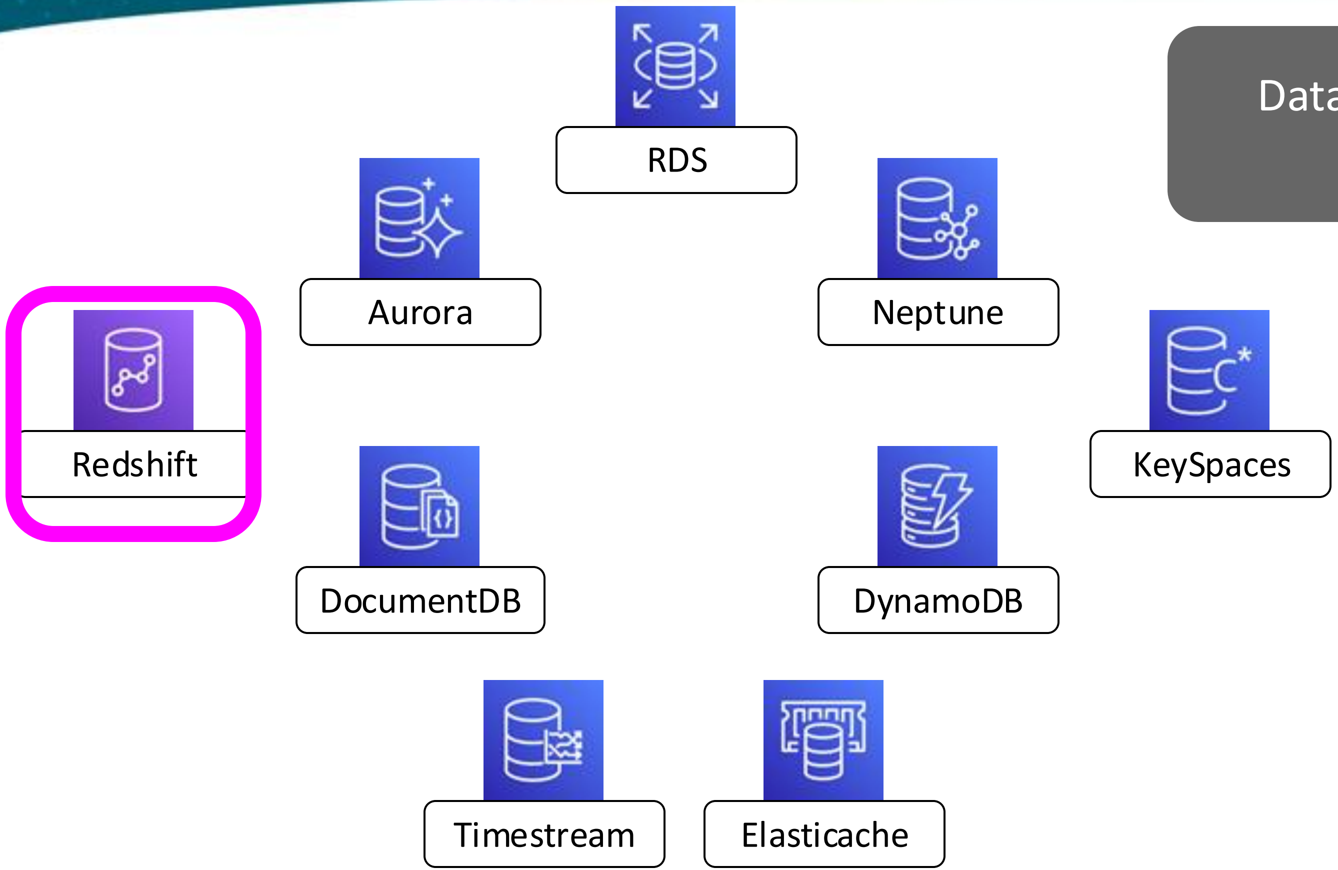
DynamoDB

Timestream

Elasticache

Transactional Relational Database Services

AWS Database Services



RDS

Aurora

Neptune

Redshift

KeySpaces

DocumentDB

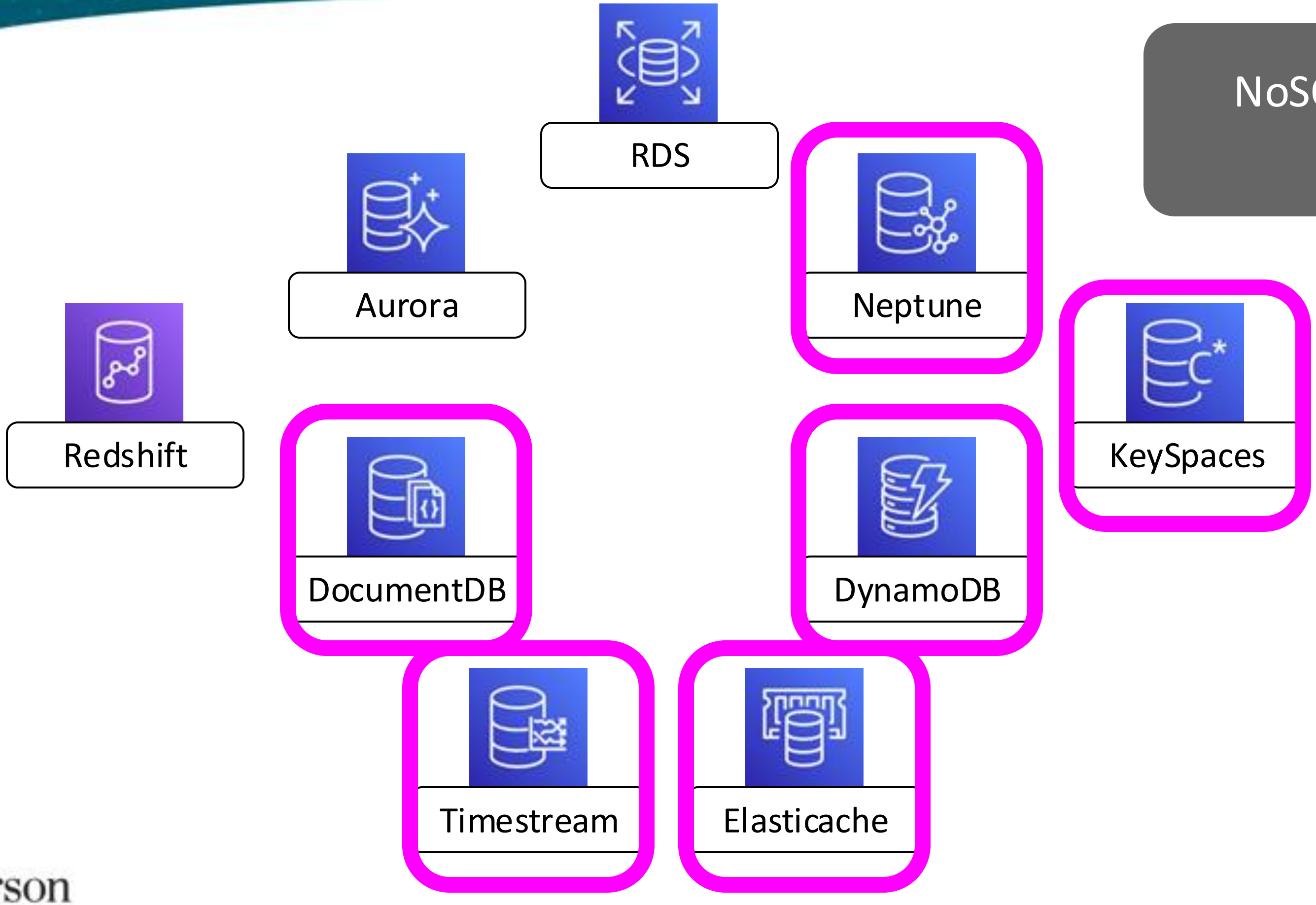
DynamoDB

Timestream

Elasticache

Data Warehouse Service

AWS Database Services



RDS

Aurora

Redshift

Neptune

KeySpaces

DocumentDB

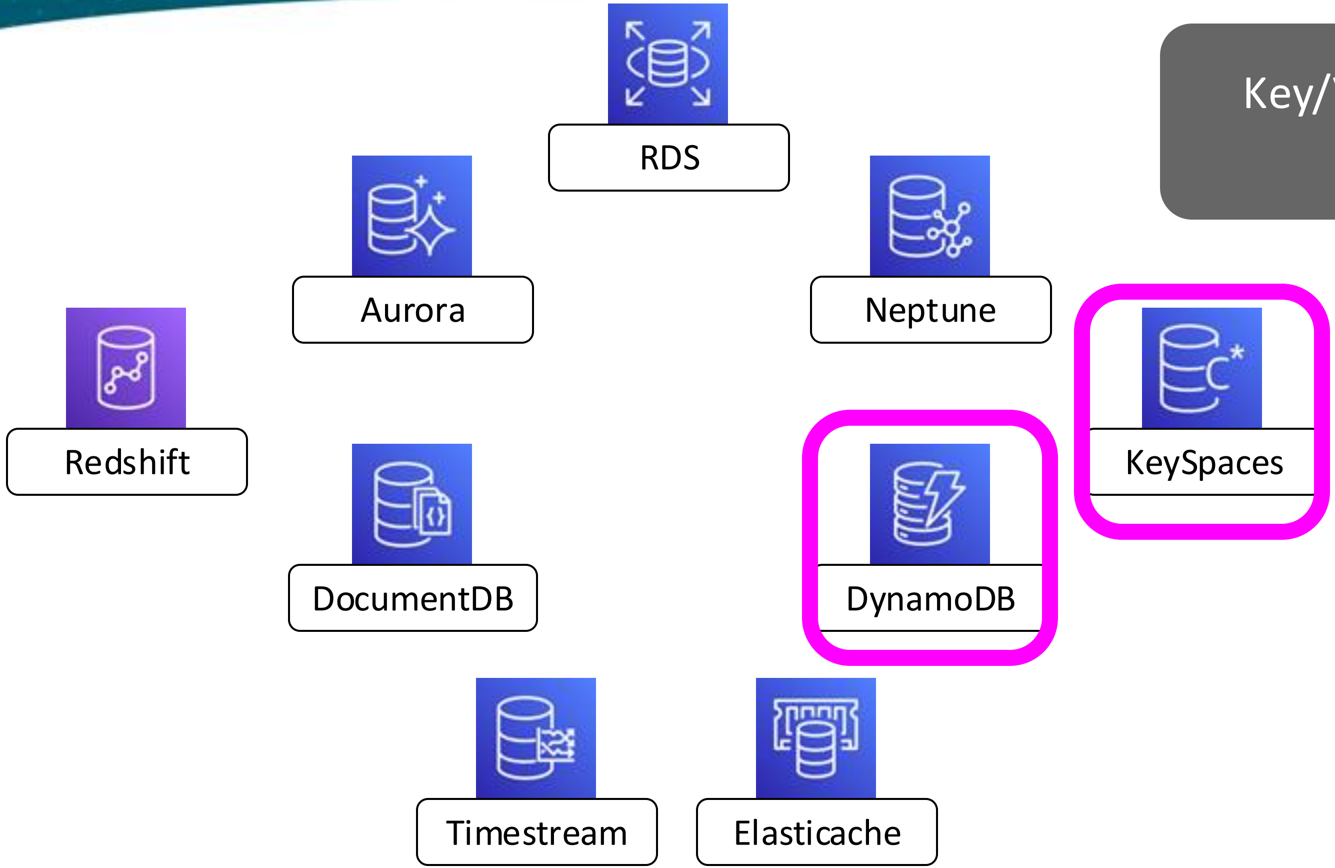
DynamoDB

Timestream

Elasticache

NoSQL Database Services

AWS Database Services



RDS

Aurora

Neptune

Redshift

KeySpaces

DocumentDB

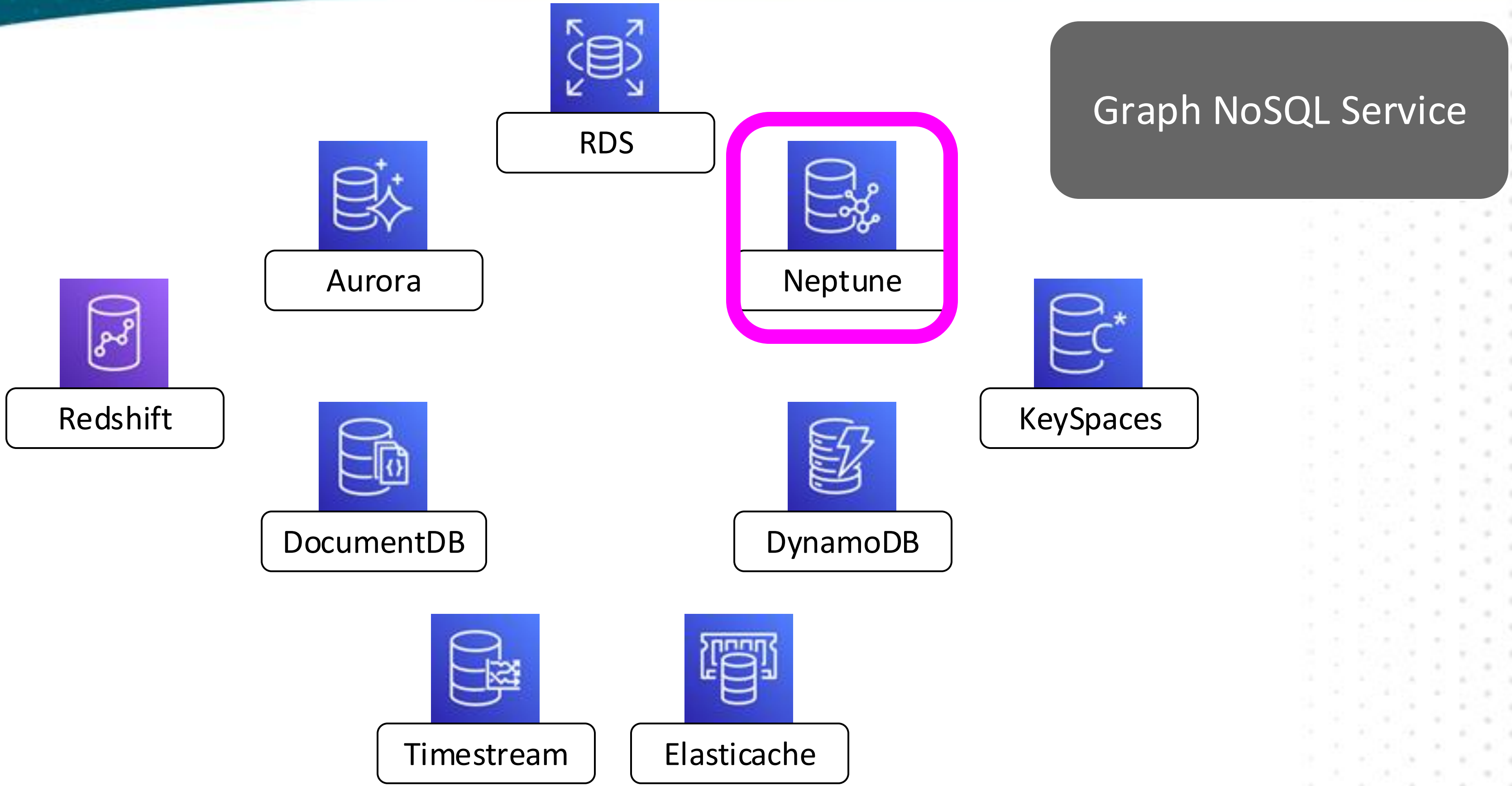
DynamoDB

Timestream

Elasticache

Key/Value NoSQL Service

AWS Database Services



RDS

Aurora

Neptune

Graph NoSQL Service

Redshift

KeySpaces

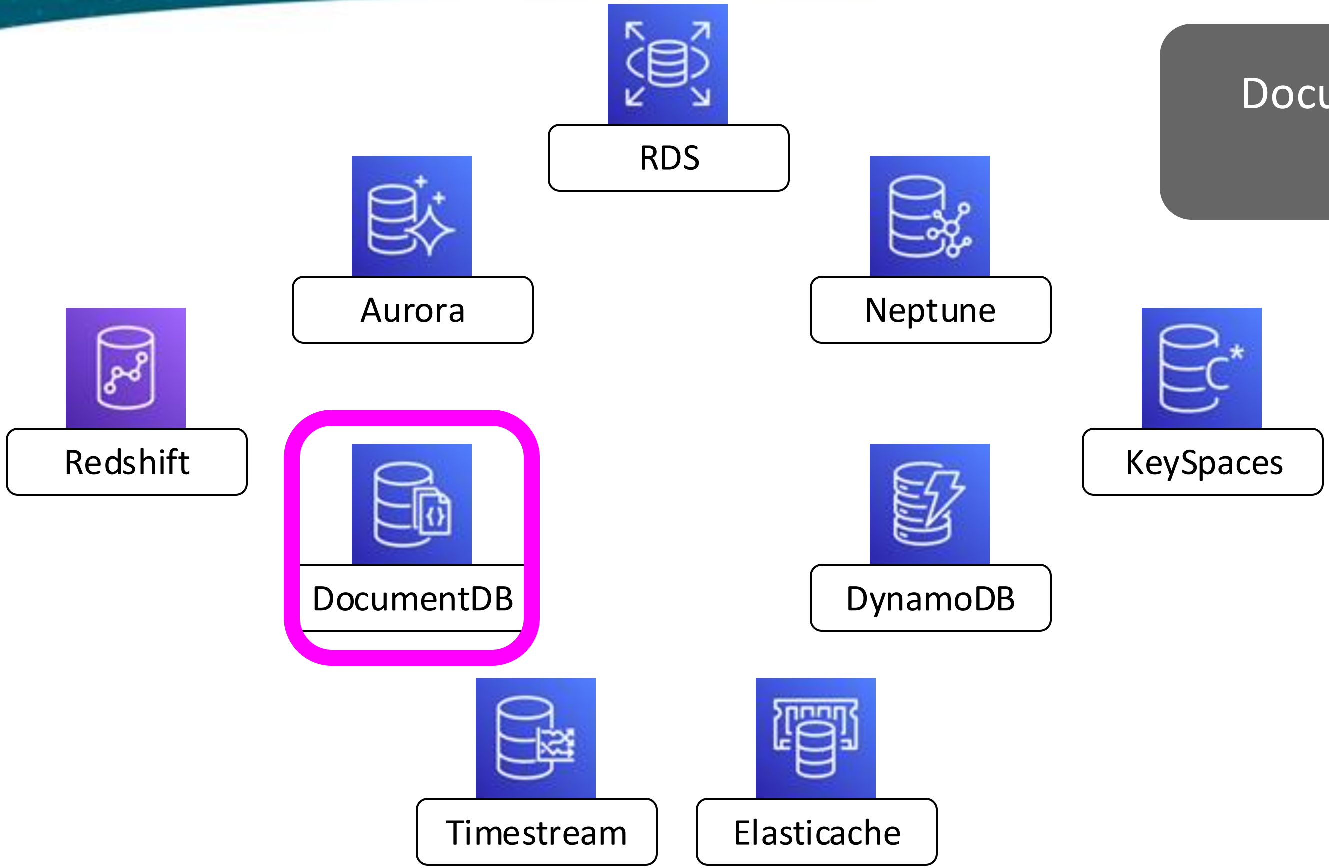
DocumentDB

DynamoDB

Timestream

Elasticache

AWS Database Services



RDS

Aurora

Neptune

Redshift

KeySpaces

DocumentDB

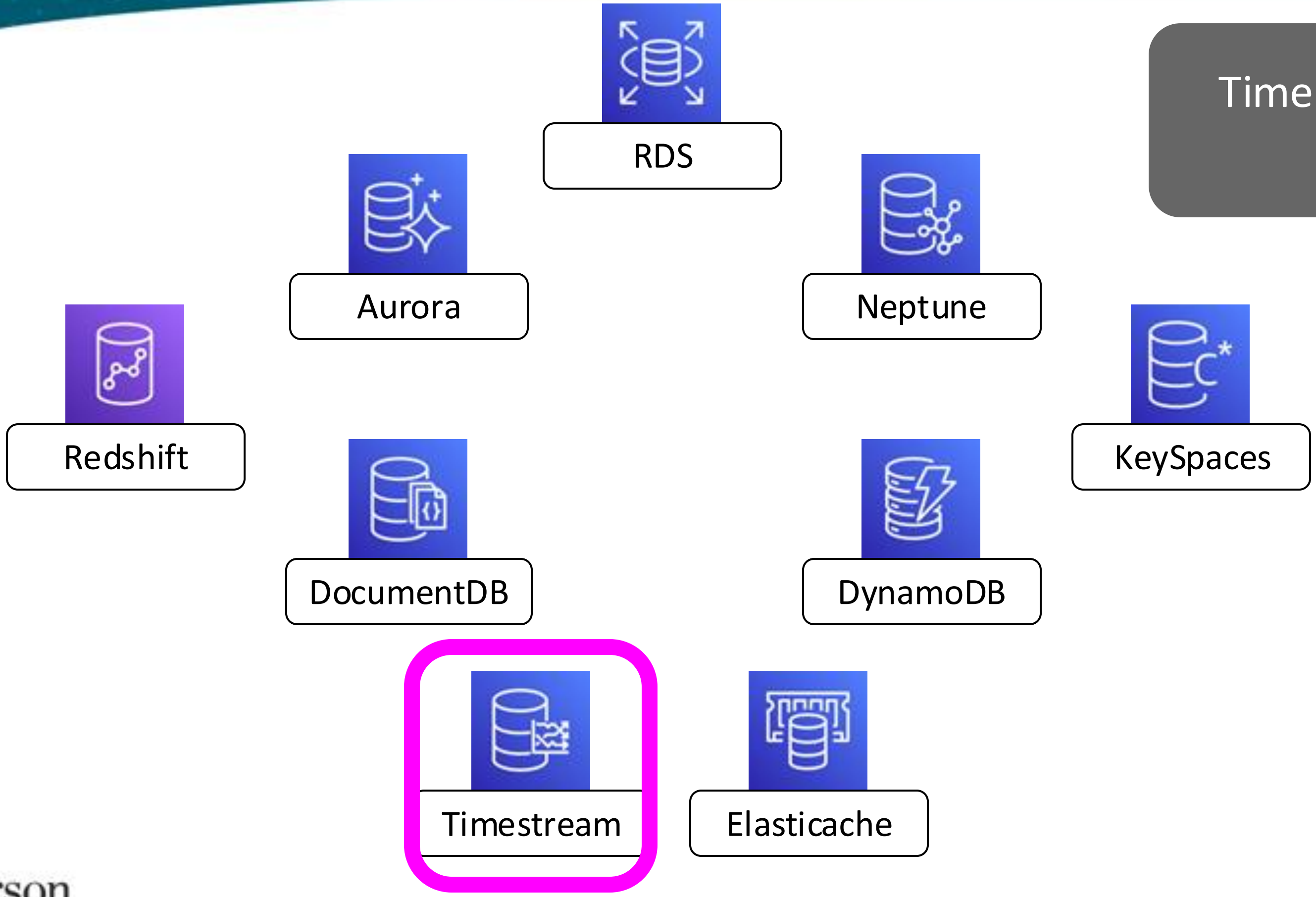
DynamoDB

Timestream

Elasticache

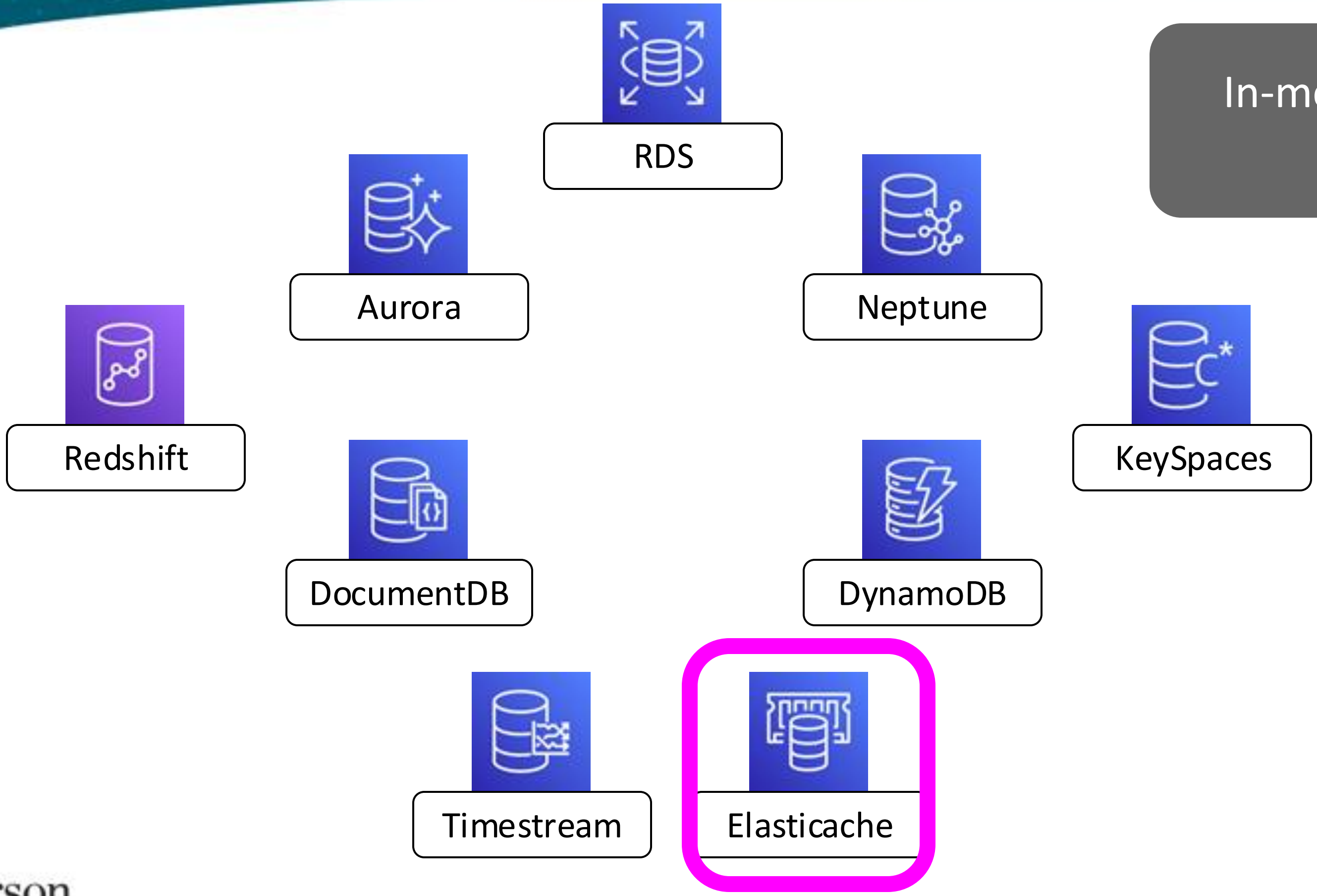
Document NoSQL Service

AWS Database Services



Time Series NoSQL Service

AWS Database Services



RDS

Aurora

Neptune

Redshift

KeySpaces

DocumentDB

DynamoDB

Timestream

Elasticache

In-memory NoSQL Service

RDS Basics

- Relational Database Service
- AZ scoped
- Third-party database engines
- Platform managed by AWS

RDS Engines

- MySQL
- Microsoft SQL Server
- Oracle DB
- Postgres
- MariaDB
- DB2
- Custom

RDS Custom Engine

- Access to underlying OS
- SQL Server
- Oracle

DynamoDB Basics

- Region scoped
- Managed NoSQL
- Key/Value data
- Serverless

Question Breakdown

Question and Answer Choices

An application has a requirement for a PostgreSQL OLTP back end, and there is a further requirement to minimize operational overhead. 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

AI, ML, and Other In-scope Services

Pearson

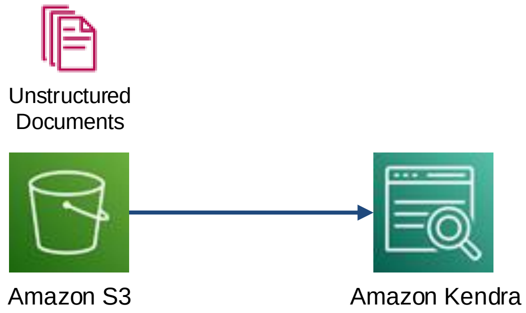
AI/ML Integrated Solution Example

Large document collection stored in S3

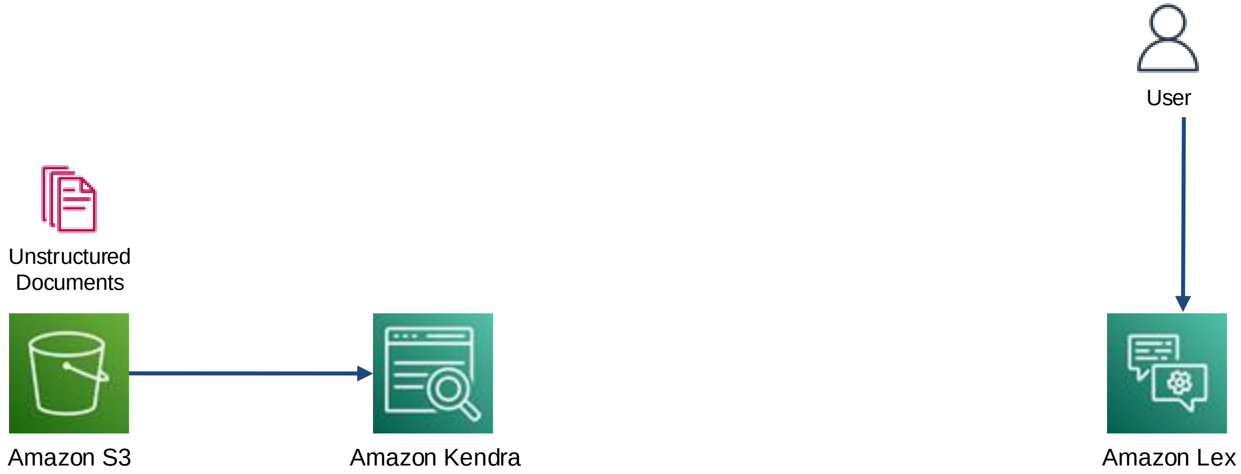
Unstructured Documents
Amazon S3

AI/ML Integrated Solution Example

Documents ingested into Kendra indexes

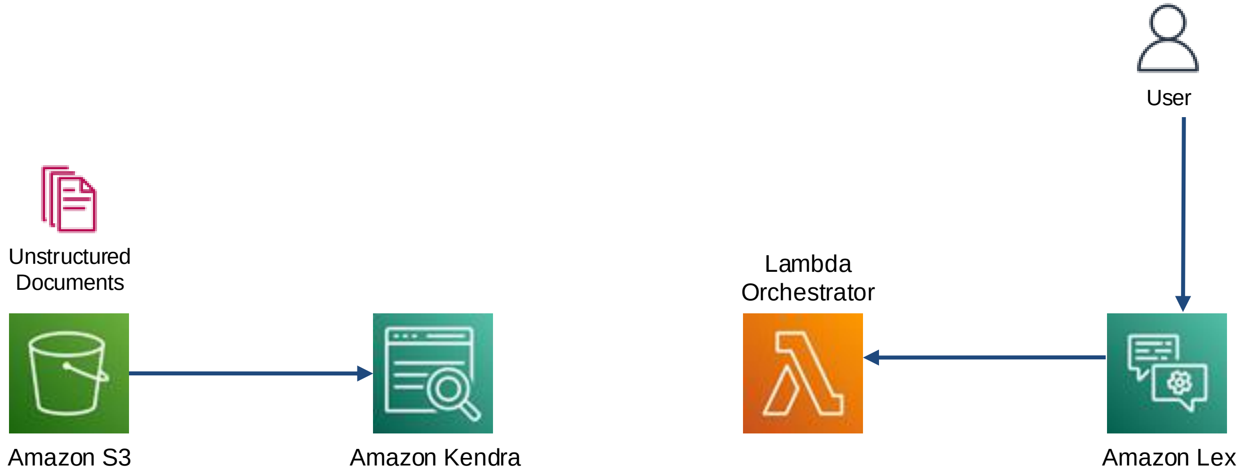


AI/ML Integrated Solution Example



User issues a prompt to the Lex chat bot

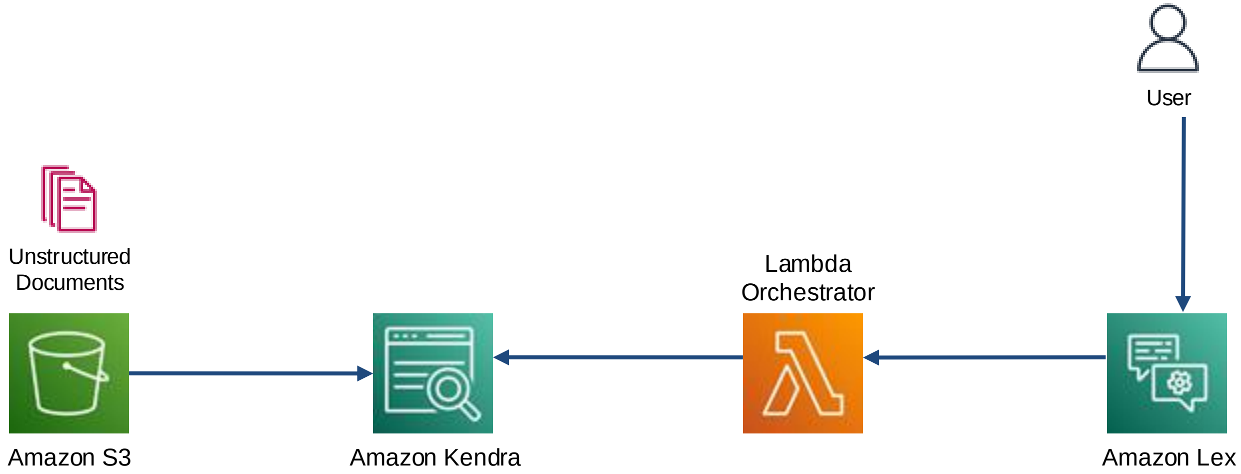
AI/ML Integrated Solution Example



The prompt is delivered to a Lambda function orchestrator

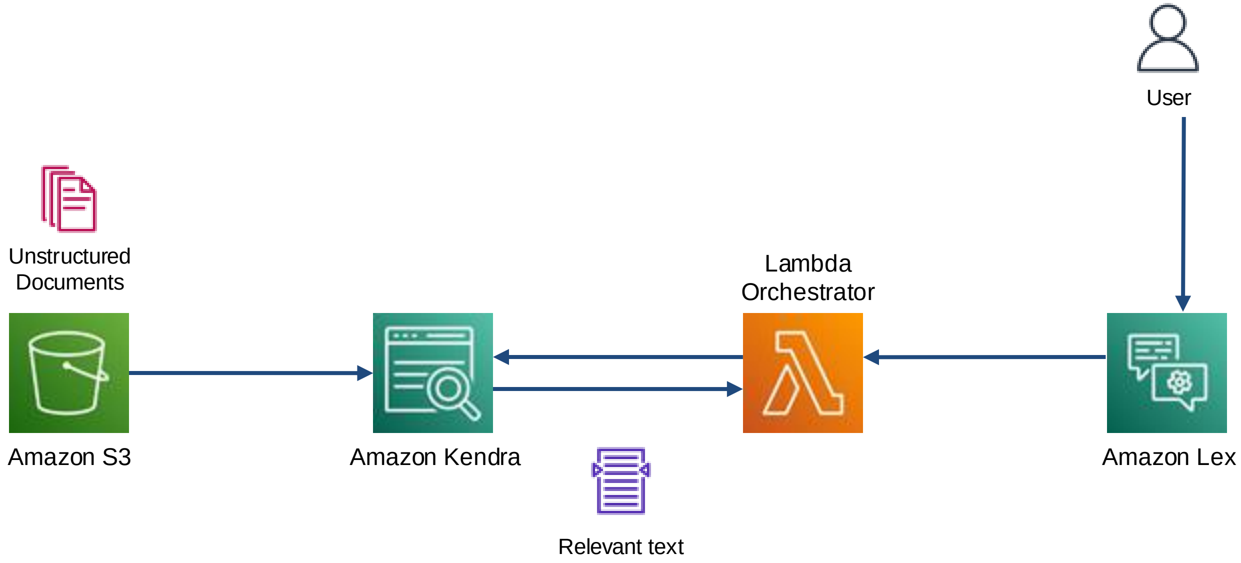
AI/ML Integrated Solution Example

Lambda issues prompt search against Kendra indexes



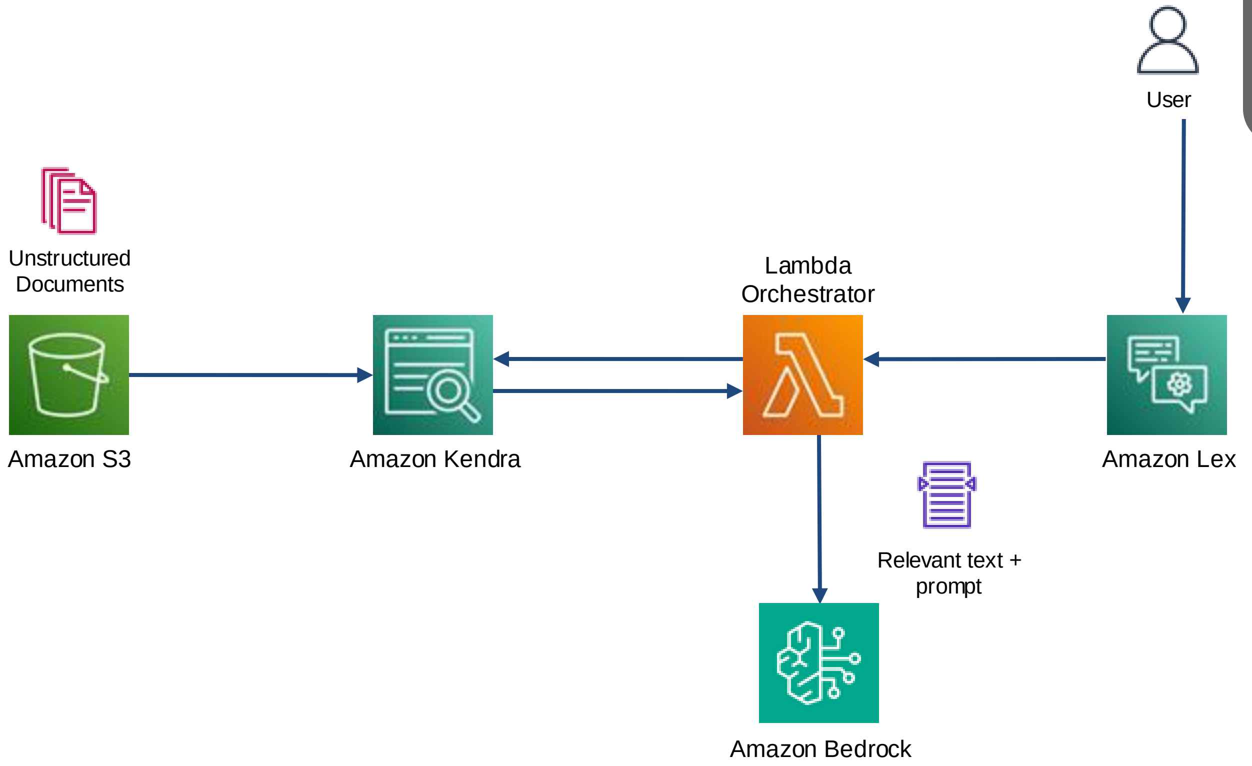
AI/ML Integrated Solution Example

The relevant text is returned to Lambda

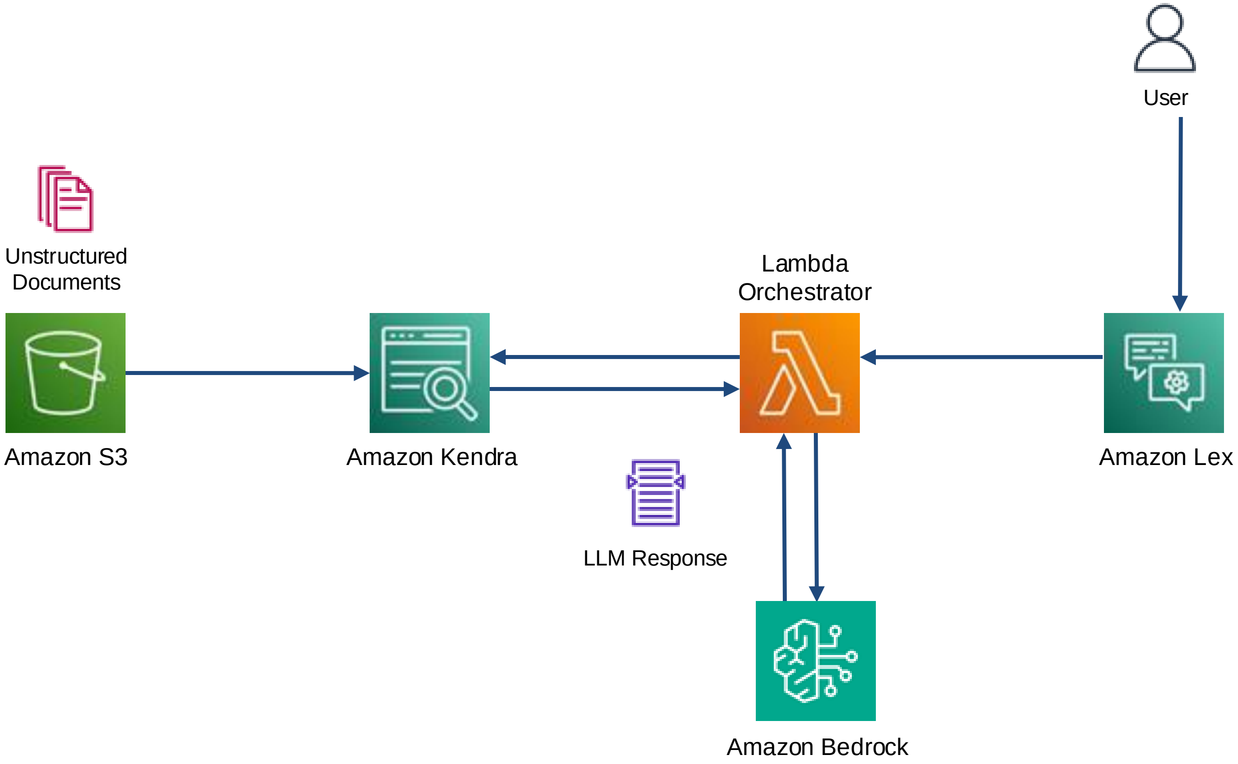


AI/ML Integrated Solution Example

Lambda delivers the prompt and the relevant document to the LLM

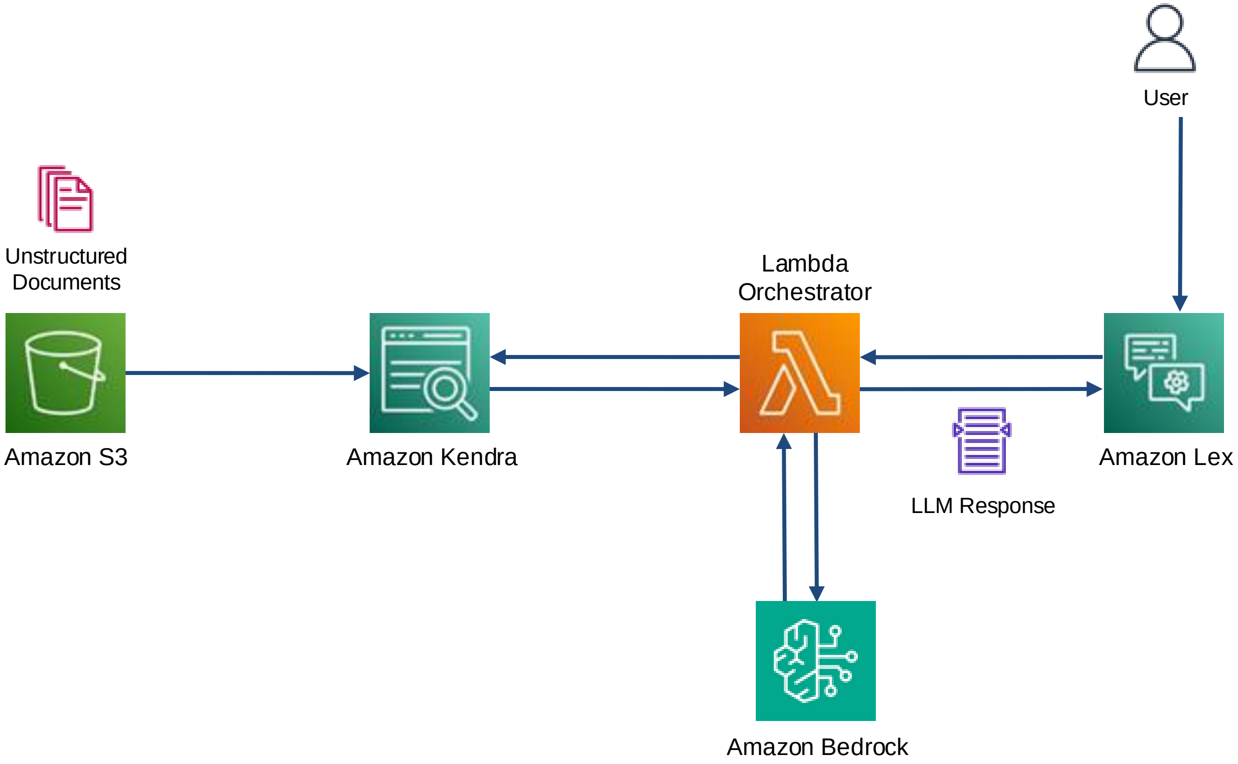


AI/ML Integrated Solution Example



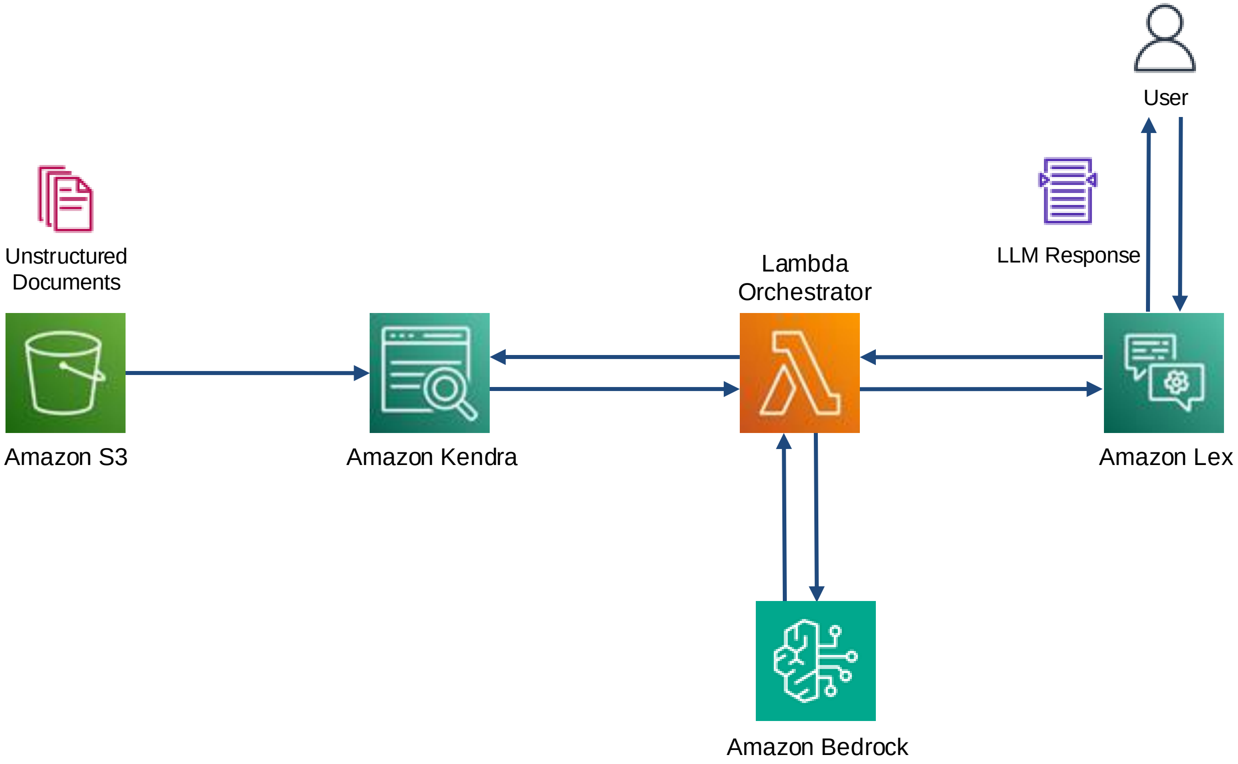
The LLM response is returned to Lambda

AI/ML Integrated Solution Example



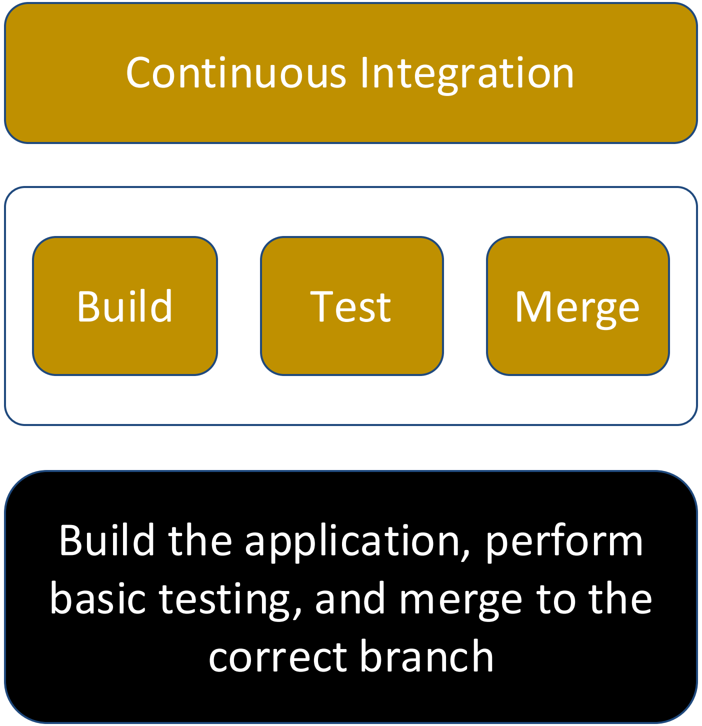
The LLM response is delivered back to the Lex chat bot

AI/ML Integrated Solution Example



Lex returns the answer back to the user

CI/CD Pipeline Example



Continuous Integration

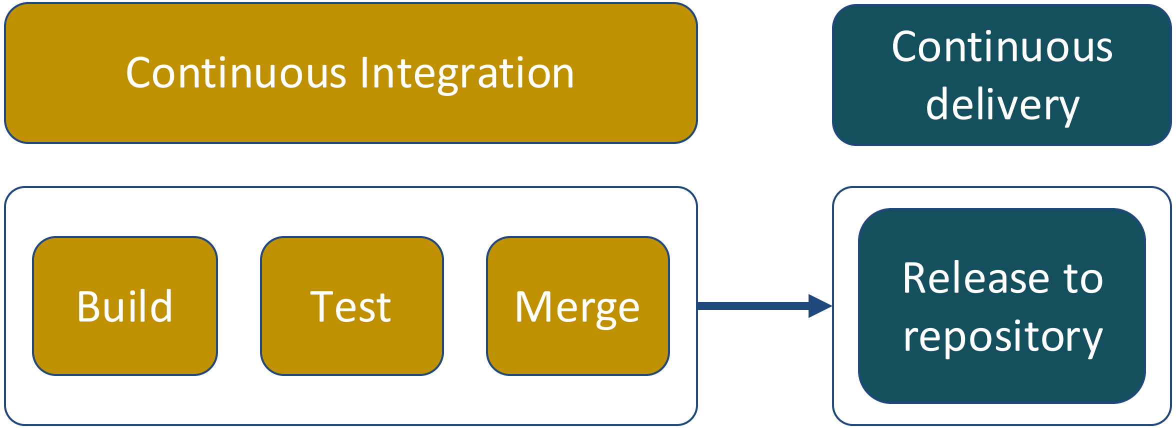
Build

Test

Merge

Build the application, perform basic testing, and merge to the correct branch

CI/CD Pipeline Example



Continuous Integration

Build

Test

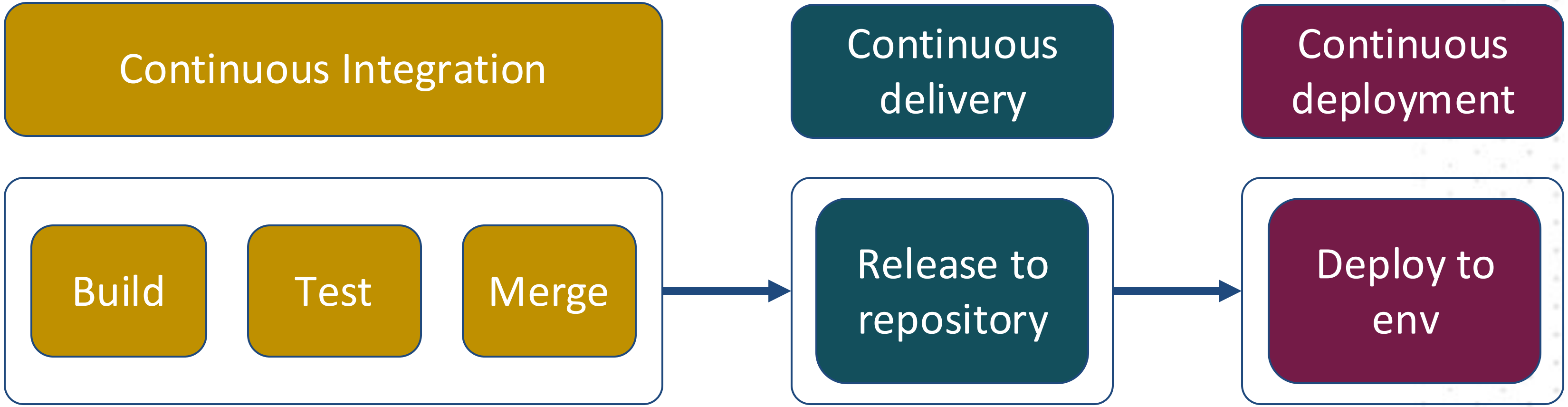
Merge

Continuous delivery

Release to repository

Push the code artifact to the appropriate repository

CI/CD Pipeline Example



Deploy the code to the appropriate environment

CI/CD Pipeline (slightly different for AWS)

AWS CodeCommit

Code repo

The versioned code is stored in CodeCommit (recently deprecated)

CI/CD Pipeline (slightly different for AWS)

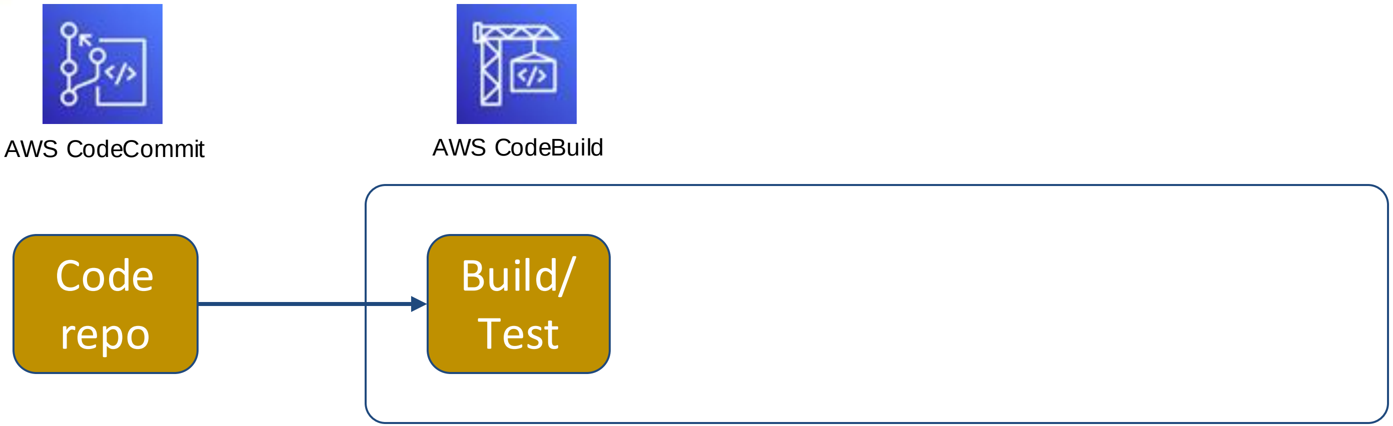
AWS CodeCommit

Code repo

CodePipeline workflows orchestrate build and deploy

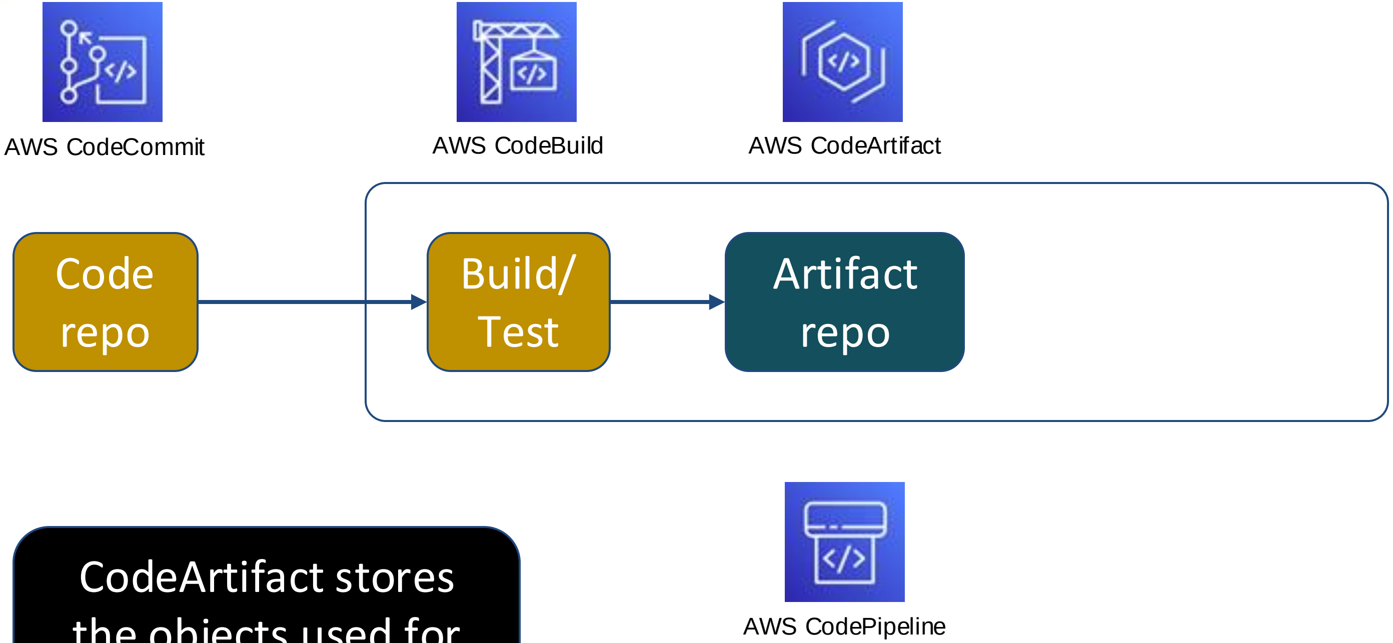
AWS CodePipeline

CI/CD Pipeline (slightly different for AWS)



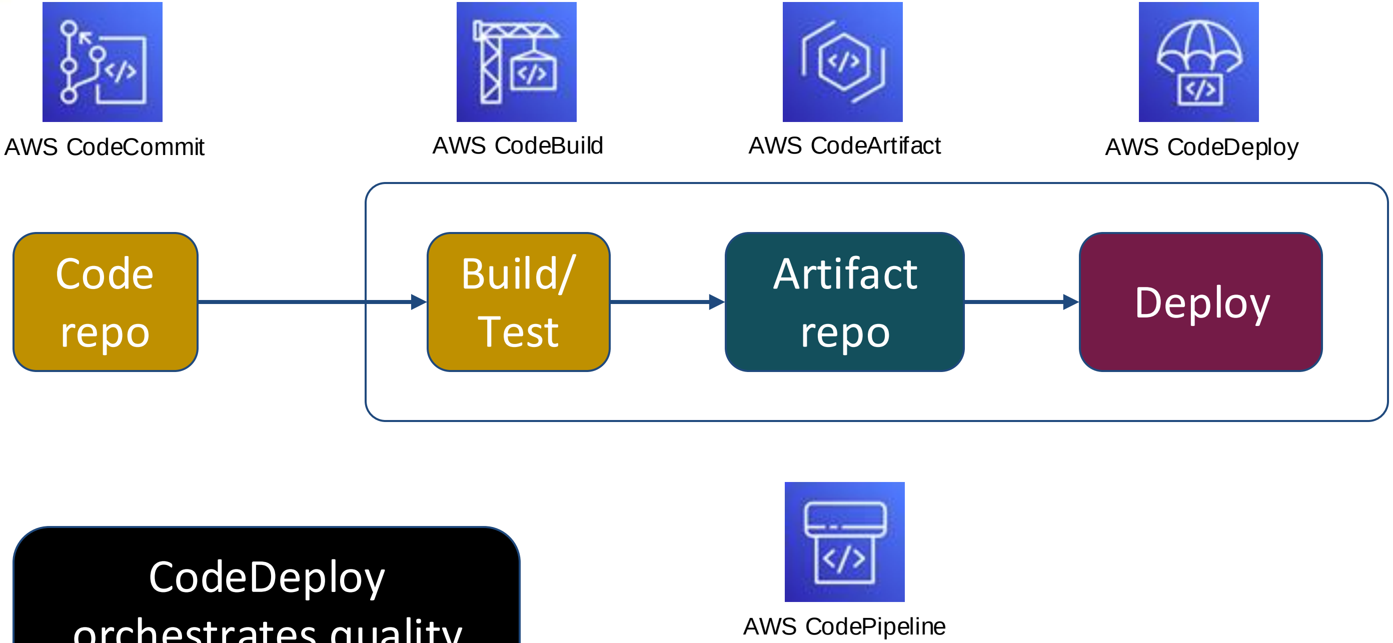
CodeBuild is used to create the code artifact

CI/CD Pipeline (slightly different for AWS)



CodeArtifact stores the objects used for deployment

CI/CD Pipeline (slightly different for AWS)



AWS CodeCommit

AWS CodeBuild

AWS CodeArtifact

AWS CodeDeploy

Code repo

Build/ Test

Artifact repo

Deploy

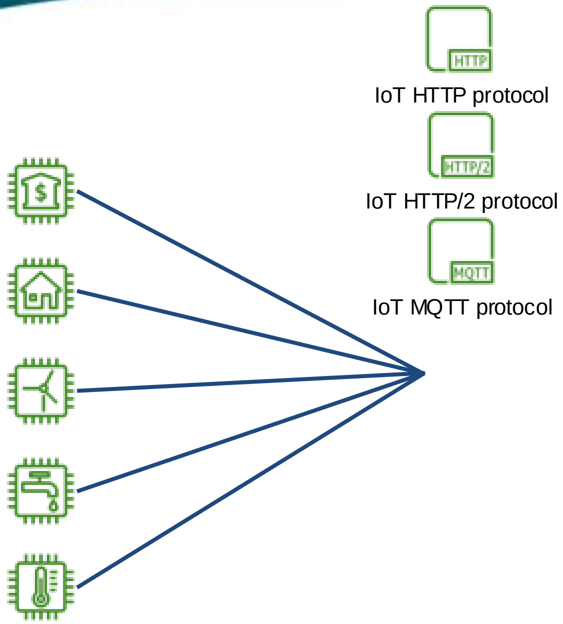
AWS CodePipeline

CodeDeploy orchestrates quality deployments

AWS IoT Core Features

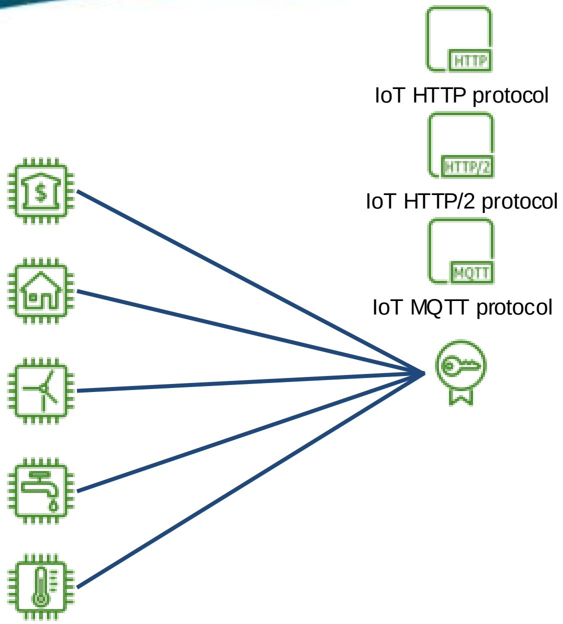
IoT devices exist in many different connected technologies

AWS IoT Core Features



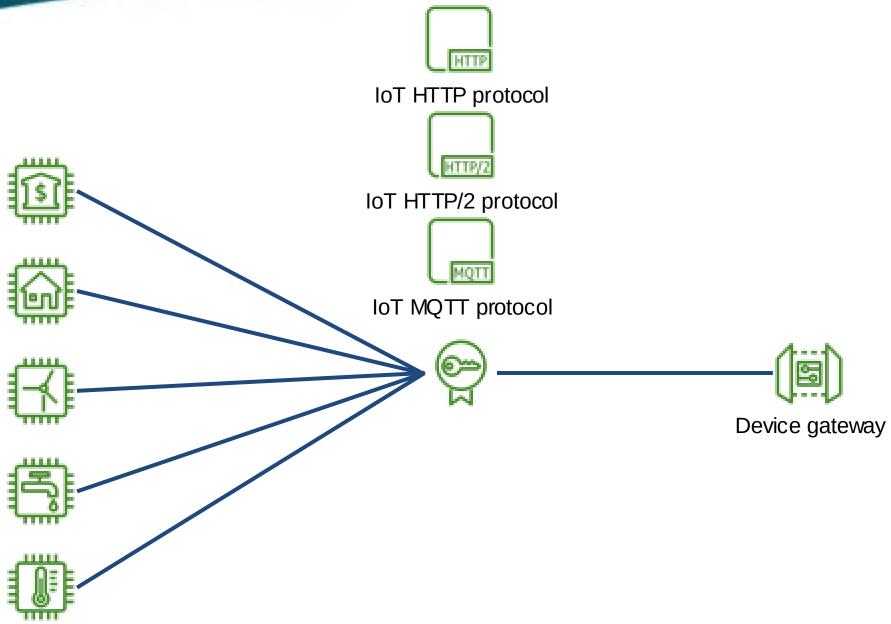
The IoT service supports several protocol choices

AWS IoT Core Features



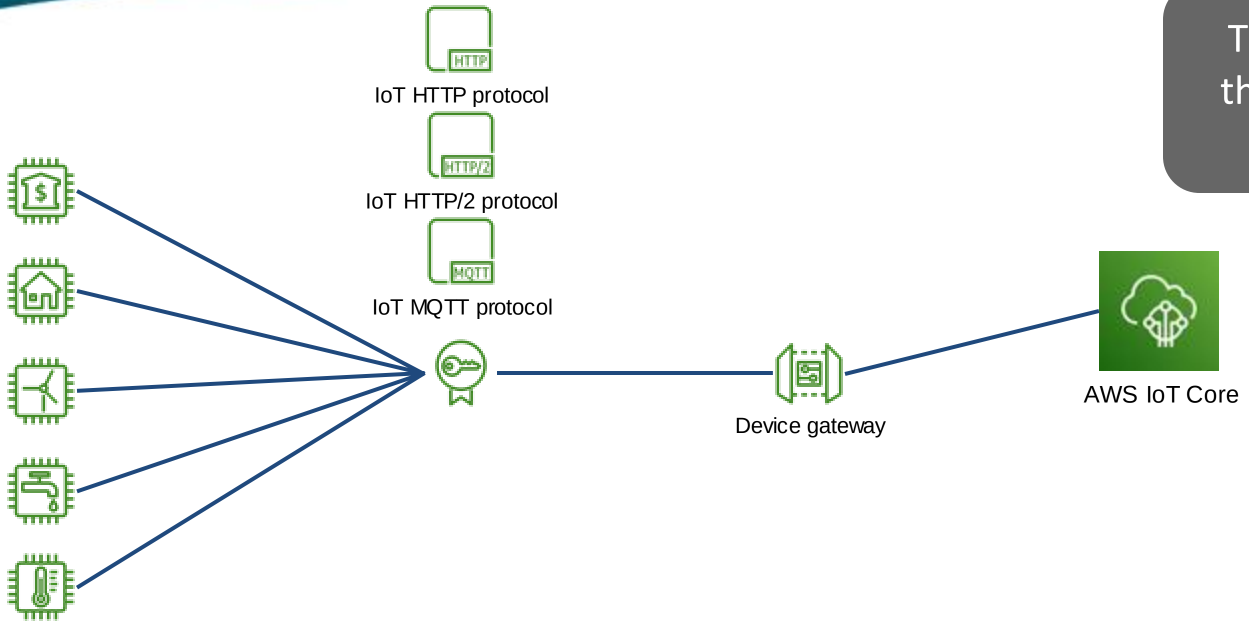
All communication uses certificate-based authentication

AWS IoT Core Features



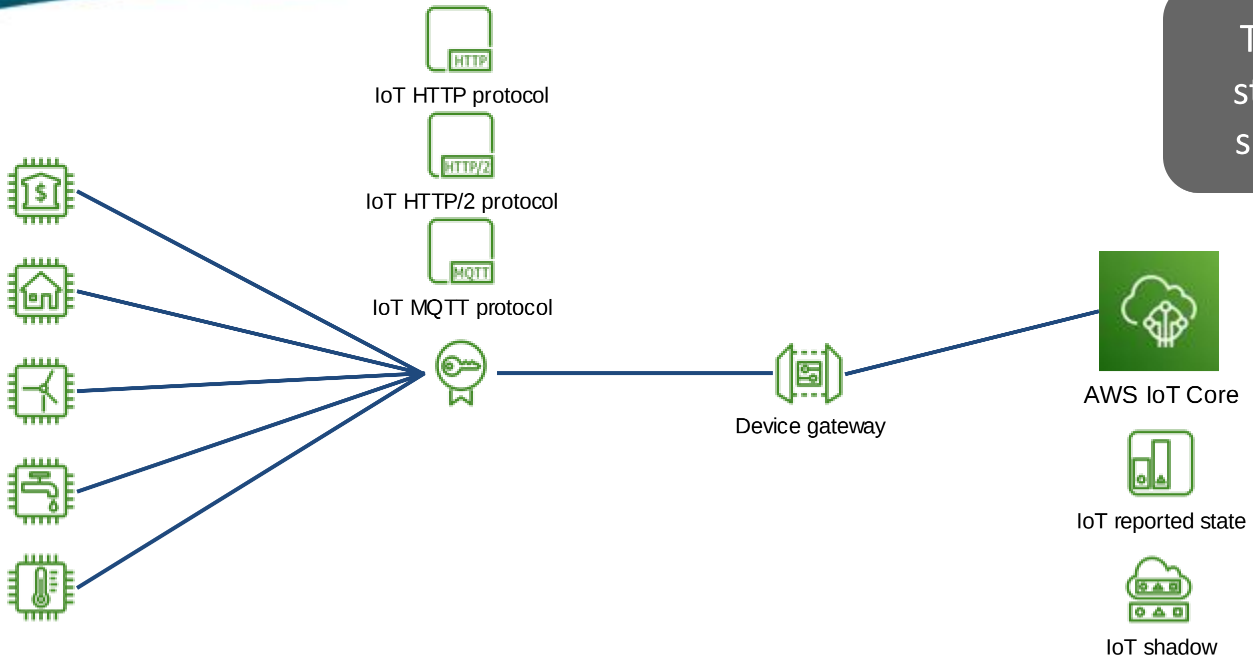
The device gateway acts as the endpoint for all communication

AWS IoT Core Features



The traffic is passed to the IoT Core service for other features

AWS IoT Core Features



The service can store state, metadata and a shadow device object

Question Domain 4: Billing, Pricing, and 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

- Small usage rate
- Specific resource types

Always Free

- Never expire
- Small usage rate
- Think of it as a permanent discount

AWS Free Tier Definitions

12 Months Free	Always Free	Trial
● Small usage rate ● Specific resource types	● Never expire ● Small usage rate ● Think of it as a permanent discount	● Short term ● Try before you buy ● Specific services

AWS Free Tier Definitions

12 Months Free

- Small usage rate
- Specific resource types

Always Free

- Never expire
- Small usage rate
- Think of it as a permanent discount

Trial

- Short term
- Try before you buy
- Specific services

All of these can assist with learning AWS!

Compute Cost - EC2 Pricing

Spot Instances

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

Compute Cost - EC2 Pricing

Spot Instances

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

RIs/SPs

- Guaranteed pricing for 1-3 years
- 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

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

RIs/SPs

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

On Demand Instances

- Pay as you go
- No discount
- No capacity guarantee

Compute Cost - EC2 Pricing

Spot Instances

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

RIs/SPs

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

On Demand Instances

- Pay as you go
- No discount
- No capacity guarantee

Dedicated Instances

- Dedicated hardware
- Can share with non-dedicated VMs
- Per-region fee
- +Spot
- +Reservations
- +On Demand

Compute Cost - EC2 Pricing

Spot Instances

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

RIs/SPs

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

On Demand Instances

- Pay as you go
- No discount
- No capacity guarantee

Dedicated Instances

- Dedicated hardware
- Can share with non-dedicated VMs
- Per-region fee
- +Spot
- +Reservations
- +On Demand

Dedicated Hosts

- Dedicated hardware
- Single instance type
- Pay for host capacity, not instance
- +Reservations
- +On Demand

Compute Cost - EC2 Pricing

Spot Instances

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

RIs/SPs

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

On Demand Instances

- Pay as you go
- No discount
- No capacity guarantee

Dedicated Instances

- Dedicated hardware
- Can share with non-dedicated VMs
- Per-region fee
- +Spot
- +Reservations
- +On Demand

Dedicated Hosts

- Dedicated hardware
- Single instance type
- Pay for host capacity, not instance
- +Reservations
- +On Demand

Overall Cost

Question Breakdown

Pearson

Question and Answer Choices

Your performance testing team wants to execute tests which last for 24 hours on many different instance types for an application to determine which is the most cost effective.

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

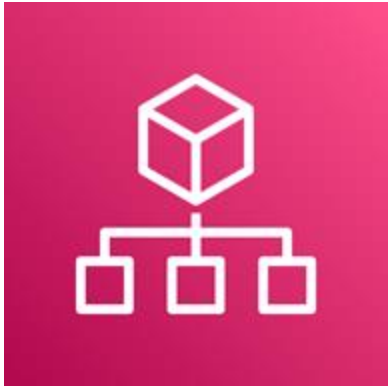
On-demand pricing is the most flexible model and would allow for the testing of many different instance types with no commitments or contracts.

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



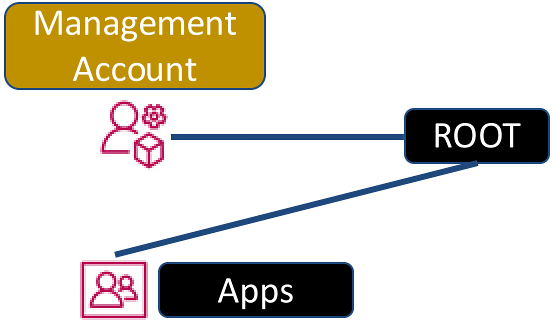
- Multiple account management service
- Central billing
- Shared reservations
- Shared savings plans
- Shared tiered pricing
- Central policy management

Multiple Accounts Using Organizations

Management Account
ROOT

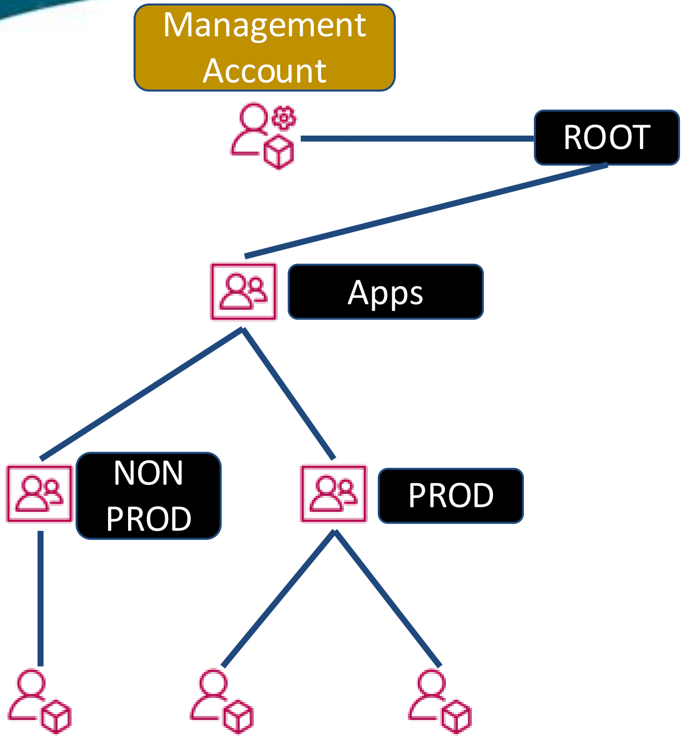
The Management account has very few resources such as SSO

Multiple Accounts Using Organizations



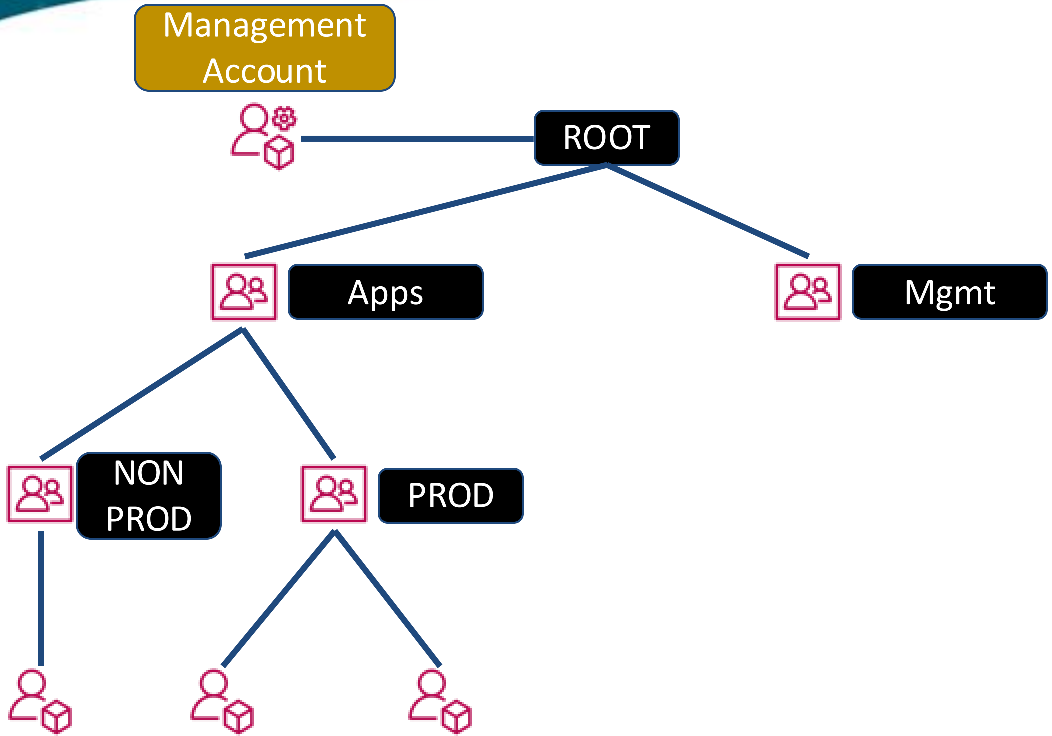
The Apps OU is for all product-related infrastructure

Multiple Accounts Using Organizations



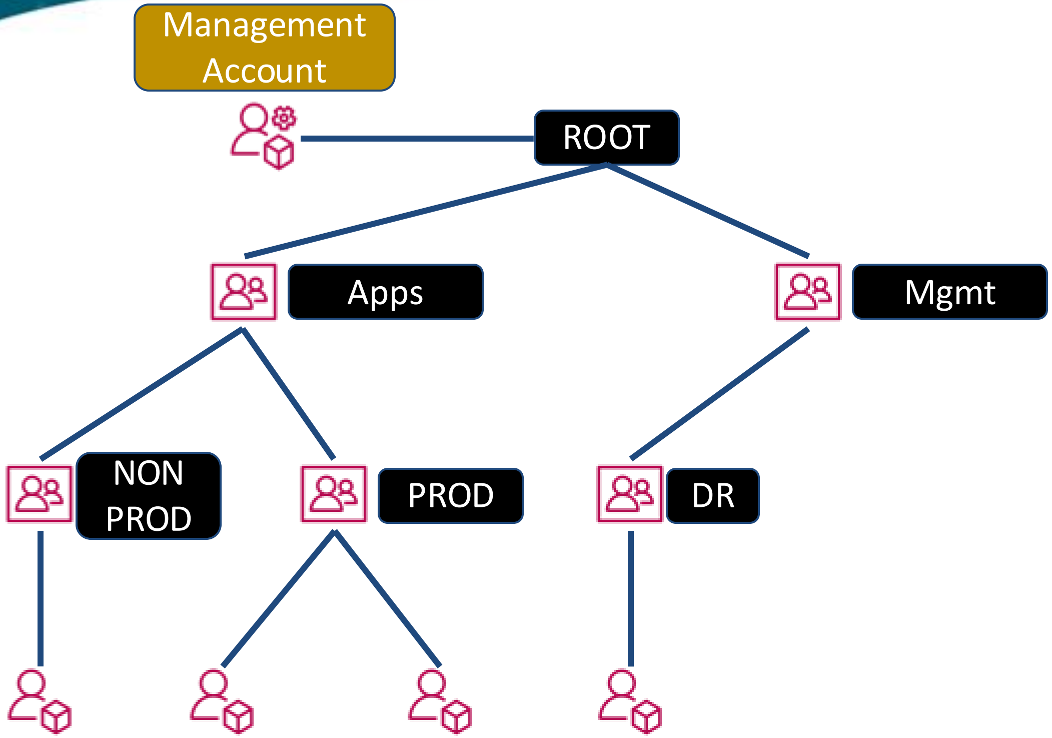
Create OUs for Non-prod and Prod environments

Multiple Accounts Using Organizations



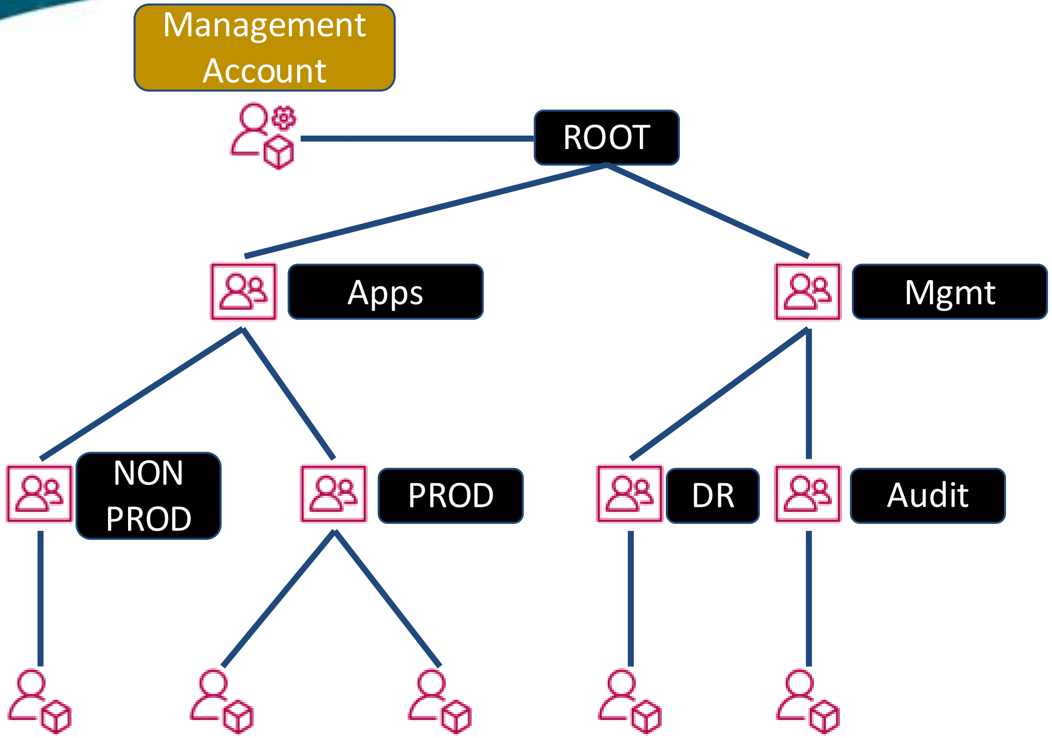
Another OU for all management activities

Multiple Accounts Using Organizations



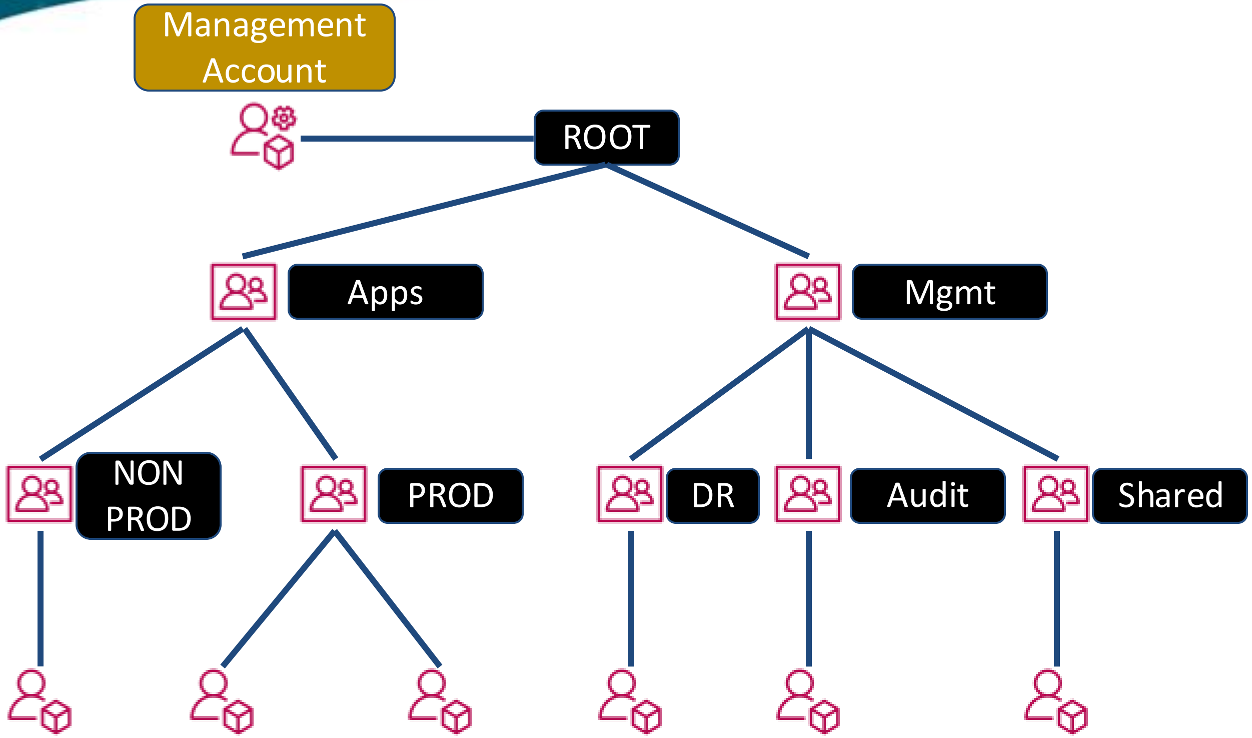
Business continuity is isolated into an OU and separate account

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 Domain 4: Billing and Pricing

Billing Support Resources

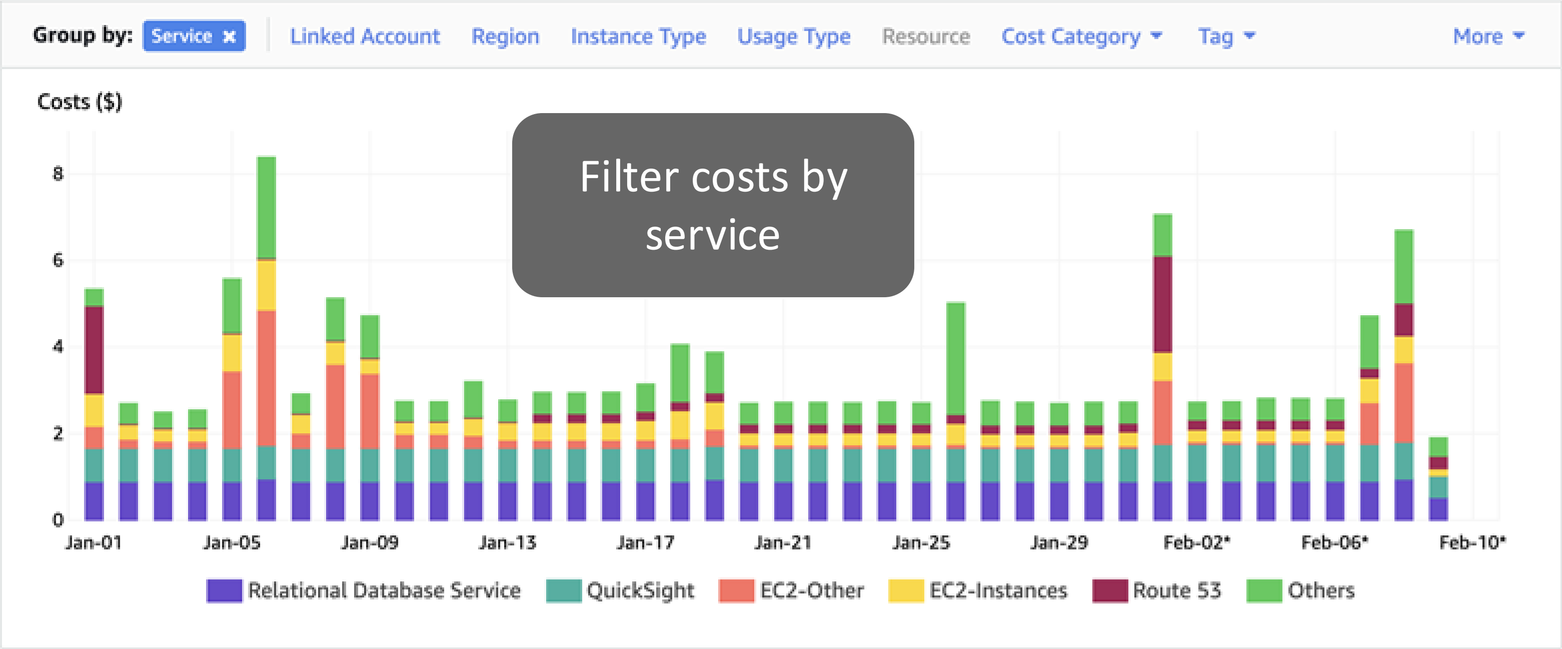
Cost Allocation Tag Basics

- 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

Cost Explorer Basics

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

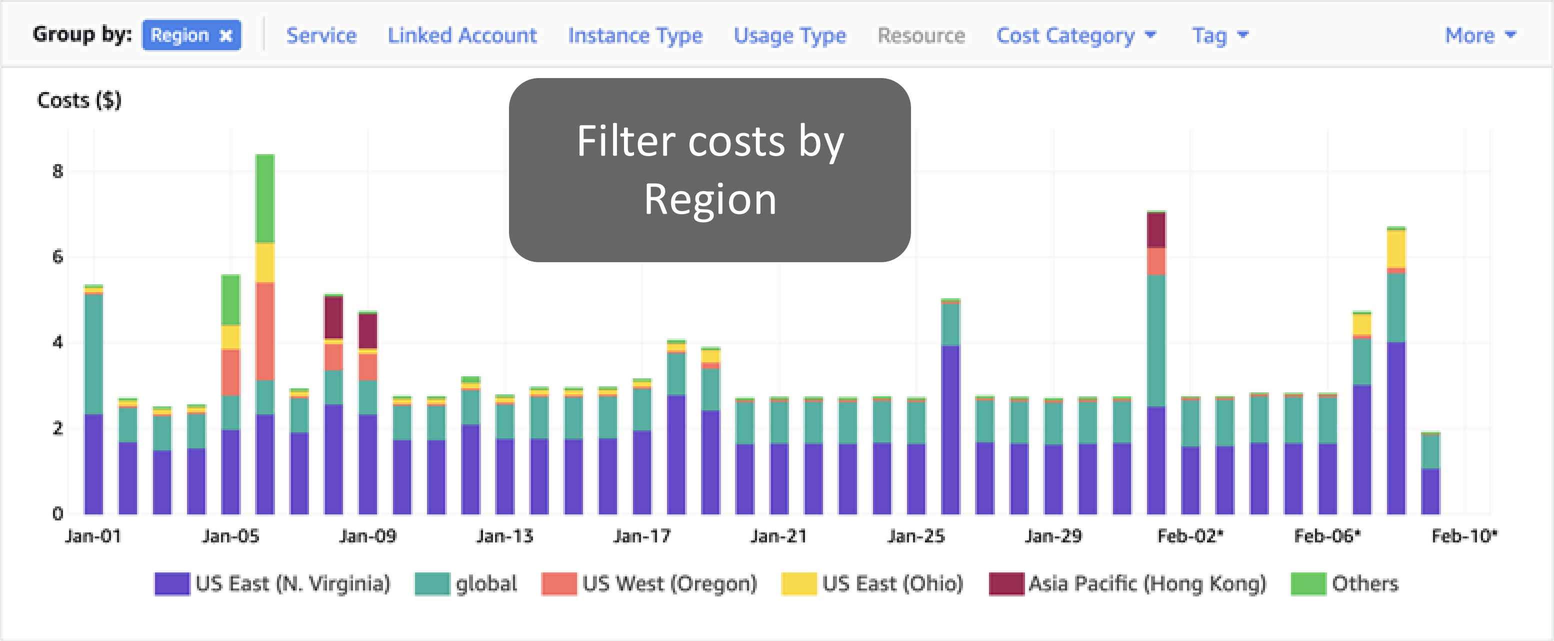
Cost Explorer Example



Group by: Service

Filter costs by service

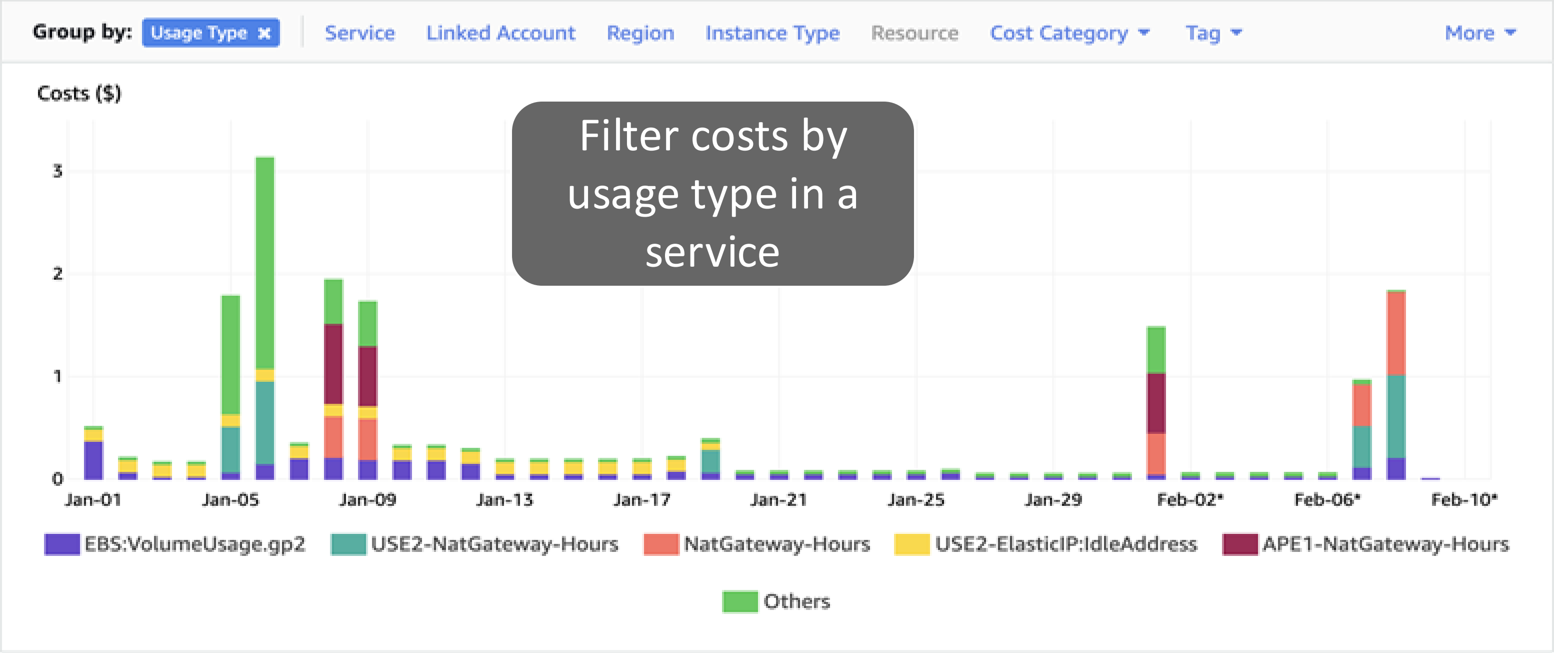
Cost Explorer Example



Group by: Region

Filter costs by Region

Cost Explorer Example



Filter costs by usage type in a service

AWS Budgets Basics

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

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

Question Domain 4: Billing, Pricing, and Support

Technology Support Resources

AWS Technology Documentation

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

AWS Abuse Notices

- Sent via email
- Respond within 24 hours (required!)
- Compromised EC2
- Compromised API keys

AWS Support Scopes

- Basic
- Developer
- Business
- Enterprise
  - TAM

APN (Amazon Partner Network)

- Global community
- Official accreditation
- Certification registry
- Specific verticals

AWS Professional Services

- AWS employees
- Subject matter experts
- Focused guidance
- Architecture reviews
- Design labs

Question Breakdown

Question and Answer Choices

If your company wants to engage an AWS-accredited 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

Wrap up and Q&A

Pearson