
aws
training and
certification

AWS Certified Solutions Architect - Associate

Week 3 Content Review

September 2023 Accelerator

aws training and certification

Week 3 Training Summary

aws training and certification

Week 3 Digital Training Curriculum

Core Trainings

Course
AWS Database Offerings
Amazon DynamoDB for Serverless Architectures
Migrating from MySQL to Amazon RDS
Amazon ElastiCache Service Introduction
Introduction to AWS Auto Scaling
Understanding Placement Groups
Introduction to Elastic Load Balancer - Applications

Optional Hands-On

AWS Builder Labs

Lab
Introduction to S3
Using Encryption to Protect Sensitive Data in S3

aws training and certification

About the Exam

aws training and certification

AWS Certified Solutions Architect - Associate

About the Exam

- 130 minutes
- 65 Questions
  - *50 questions count to your score*
  - Scored 100 to 1000 (720+ pass)
- $150/voucher
- Multiple Response & Individual response questions
- In-Person & Remote proctoring available

AWS Certified Solutions Architect - Associate

Key Exam Topics

Domains Covered:	% of Exam
Domain 1: Design Secure Architectures	30%
Domain 2: Design Resilient Architectures	26%
Domain 3: Design High-Performing Architectures	24%
Domain 4: Design Cost-Optimized Architectures	20%
Total:	**100%**

AWS Certified Solutions Architect - Associate

Helpful Resources

Training

- AWS Partner Accreditation: Technical
- AWS Solutions Architect – Accelerator Learning plan

White Papers

- Overview of Amazon Web Services
- AWS Well-Architected Framework
- Management and Governance Lens
- AWS Global Infrastructure
- Shared Responsibility Model
- How AWS Pricing Works
- AWS Architecture Center
- Secure Content Delivery with Amazon CloudFront
- IPv6 on AWS
- Overview of Deployment options on AWS
- Organizing your AWS Environment using multiple accounts

Exam Preparation

- Twitch Power Hours
- Sample Questions
- Schedule an Exam

Looking for more ***Practice Exams***?

*Check out our **Skill Builder Subscription** (information on the next slide)*

aws training and certification

OPTIONAL AWS Skill Builder Subscription

The Skill Builder subscription provides access to official AWS Certification practice exams, self-paced digital training content including open-ended challenges, self-paced labs, and game-based learning.
Please note, the Skill Builder subscription is not required for this Accelerator program.

Free digital training

LINK HERE

Special features include:

- 500+ digital courses
- Learning plans
- 10 Practice Question Sets
- *AWS Cloud Quest*

Individual subscription

LINK HERE

Everything in free digital training, plus:

- AWS Cloud Quest (3 additional roles)
- AWS Certification Official Practice Exams
- Exam prep courses
- 100+ AWS Builder Labs
- AWS Jam Journey (lab-based challenges)

Access ***65*** Solutions Architect - Associate Practice Exam Questions with feedback on your answer choices

Individual subscriptions are priced at $29 USD per month (*Flexibility to cancel anytime*) or $299 USD per year.

Get AWS Certified: Associate Challenge

WHO is the challenge for?

Individuals who want to earn one of the three AWS Associate Certifications:

WHEN is the challenge?

June 6 – September 29, 2023

The last day to join and receive the 50% discount voucher is September 29, 2023.

Complete the exam by October 31, 2023 to leverage the voucher.

WHERE do I get started?

Sign up for the Get AWS Certified: Associate Challenge today!

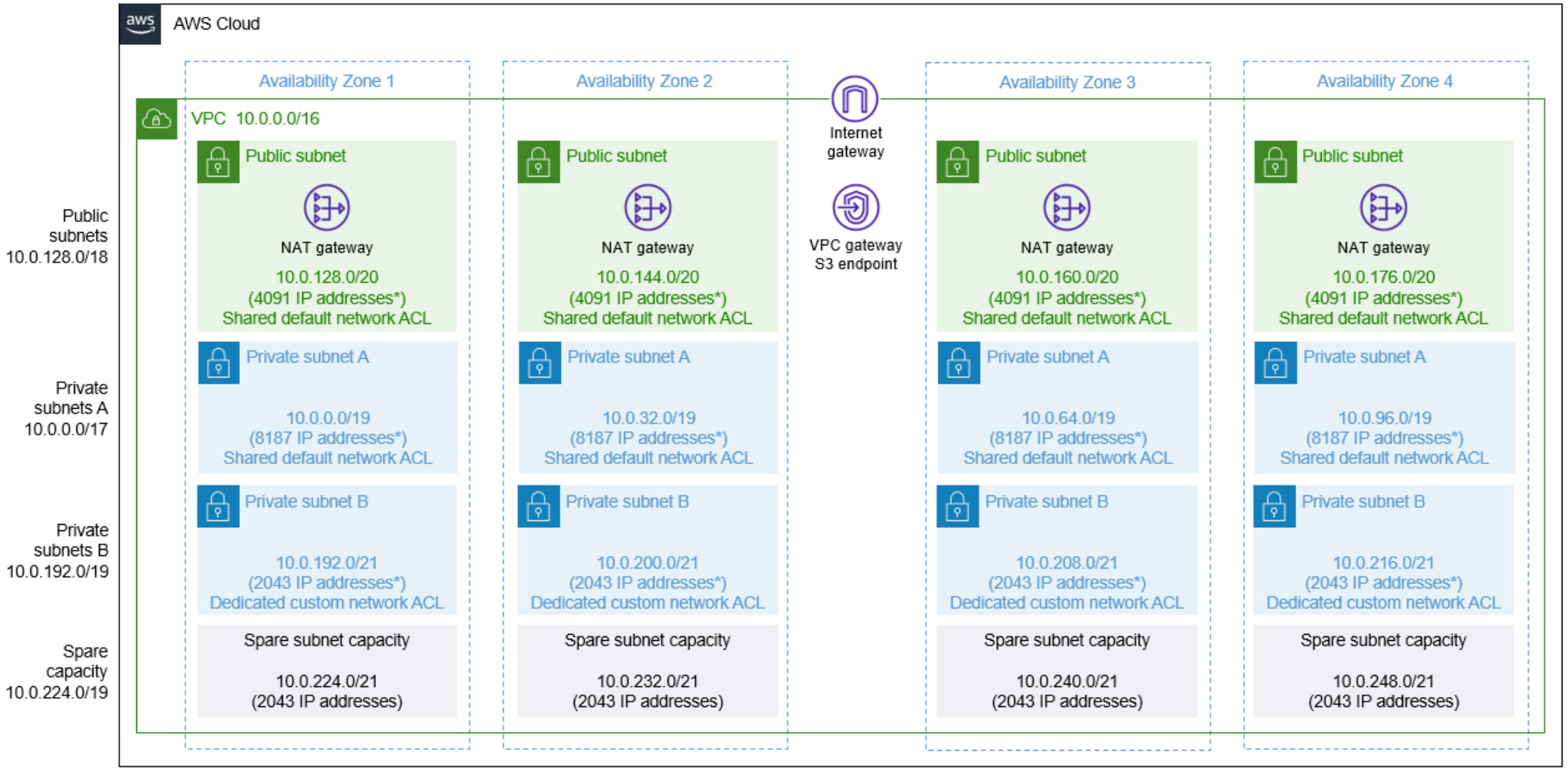
*Terms and conditions apply. A 50% discount exam voucher is available for participants who want to earn an AWS Certified Associate - level Certification

[1] Enterprise Strategy Group, AWS Training and Certification Help Learners Thrive in an Increasingly Cloud-first World, 2022

Week 3 Homework Assignment

aws training and certification

Week 2 Homework – Solution Key



*Five IP addresses in each subnet CIDR block are reserved and unavailable for use.

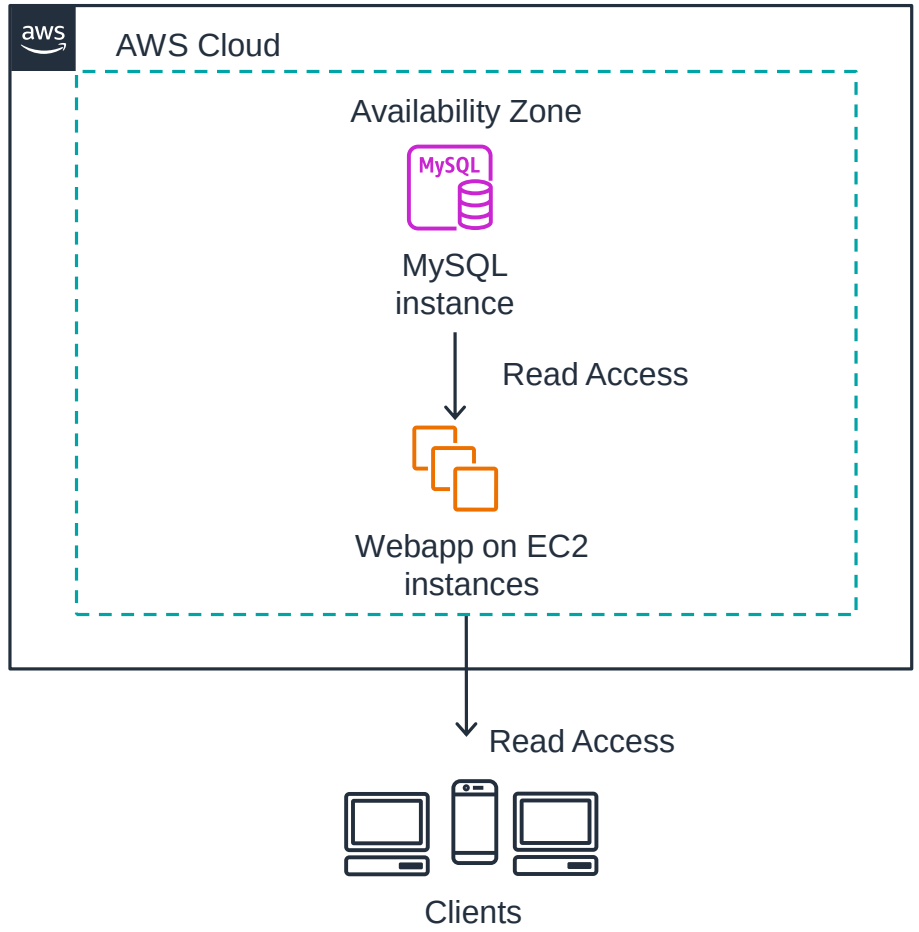
Week 3 Homework – Optimizing your DB Deployment

Solution Requirements:

1. **Amazon RDS w/ MySQL Database**
2. **Decrease latency for frequently accessed data**
3. **Ensure the database is resilient to an Availability Zone outage**

<u>Your Task:</u>

Design an architecture diagram meeting these requirements.

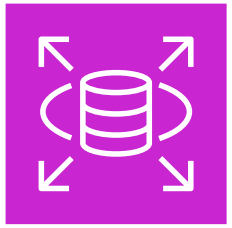


Week 3 Homework – Bonus Points!

Your Task:

Update your solution based on the following constraints:

- **Minimal changes to application code**
- **Database queries to the application are not consistent**



Amazon Relational Database Service (Amazon RDS)

Week 3 Homework – Show and Tell!

Share us your architecture, answers, and explanation on LinkedIn!

#AWSpartners

#AWSaccelerator

Tag us so we don't miss it!

Kevin, Sam, Brady

Please do not share confidential or proprietary information on social media.

aws training and certification

AWS Caching & File Servers

aws training and certification

Amazon ElastiCache

A fully managed, in-memory caching service

Overview

A fully managed, in-memory caching service (database) that can support flexible, real time use cases.

Provides managed Redis or MemcacheD as a service and is best used for read heavy workloads with low latency requirements.

Using ElastiCache can assist with reducing database workloads (expensive) and be used to store session data (stateless servers).

ElastiCache DOES require application code changes!

Amazon ElastiCache – Redis vs. Memcached

A fully managed, in-memory caching service

What's the difference?

Memcached is a distributed memory caching system designed for ease of use and simplicity. It is well-suited as a cache or a session store.

Redis is an in-memory data structure store that offers a rich set of features. It is useful as a cache, database, message broker, and queue.

	ElastiCache for Memcached	ElastiCache for Redis
Sub-millisecond latency	✓	✓
Data partitioning	✓	✓
Advanced Data structures	✗	✓
Multi-threaded architecture	✓	✗
Snapshots	✗	✓
Replication	✗	✓
Transactions	✗	✓
Pub/Sub	✗	✓

Amazon Elastic File System (EFS)

Simple, Serverless, set-and-forget file system

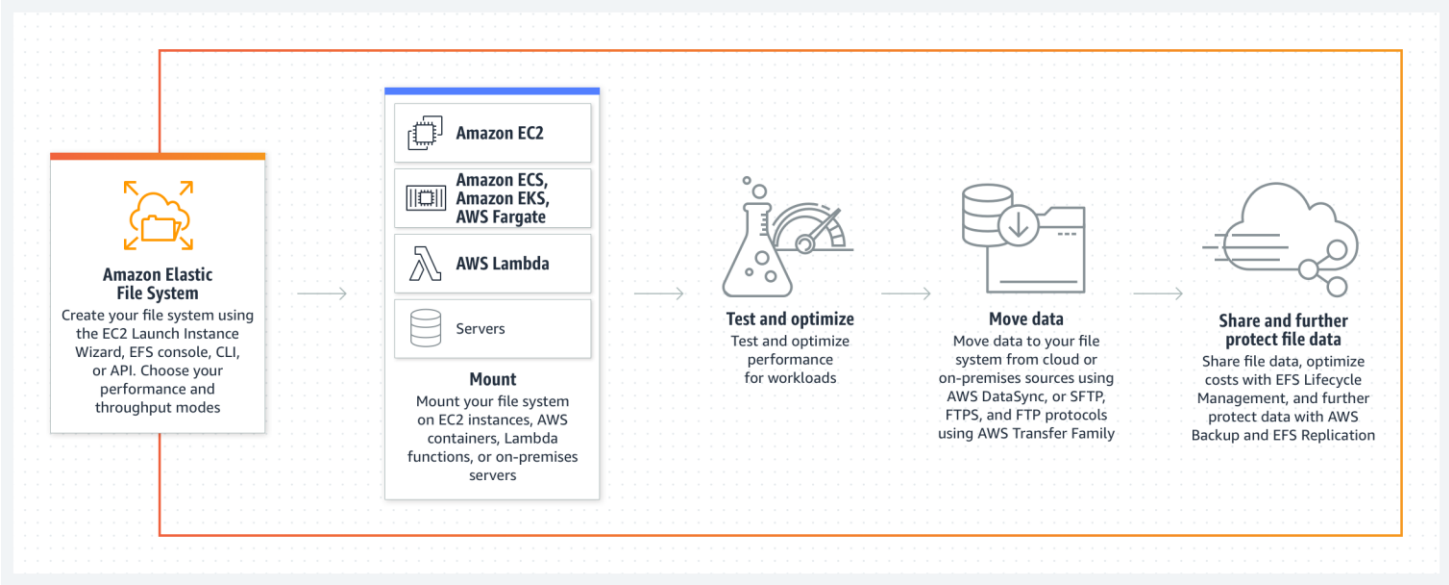
What is it?

Amazon EFS is a shared file system within AWS based on the Network File System (NFS).

- Can be shared between many EC2 instances
- Private service, via mount targets, inside a VPC

How can I use it?

EFS can be mounted on Linux EC2 instances, or even on-premises servers so long as private networking has been set up and configured between the network and AWS.



aws training and certification

Amazon FSx for Windows File Server

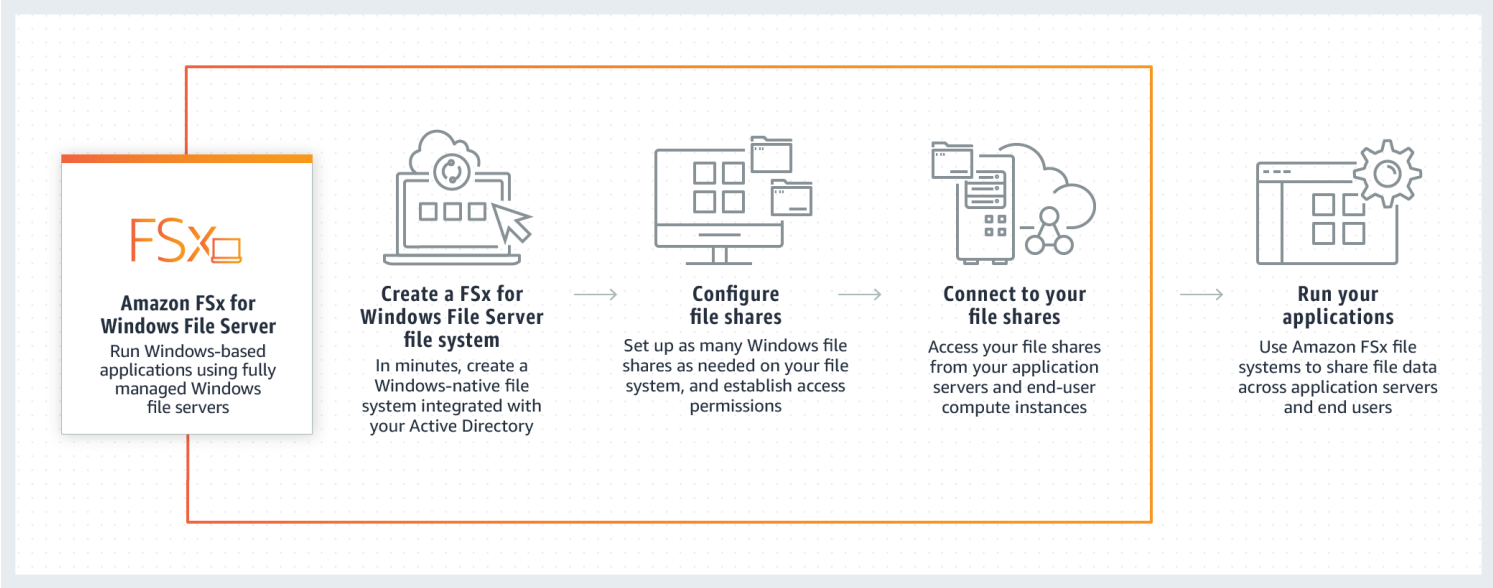
Fully Managed file storage built on Windows Server

How It Works

Amazon FSx for Windows File Server provides fully managed shared storage built on Windows Server. It delivers a wide range of data access, data management, and admin capabilities.

Exam Tip

Questions related to migration of files from Windows servers to AWS, accelerating the adoption of migrations through the use of hybrid file systems with low latency.



AWS Database Offerings

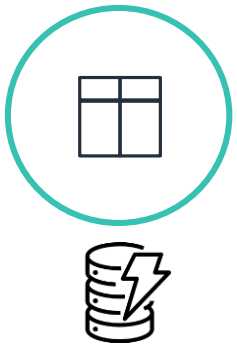
aws training and certification

AWS Purpose-built Database Offerings

Relational

Aurora RDS

Key - Value

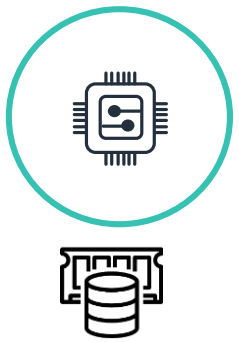


DynamoDB

Document

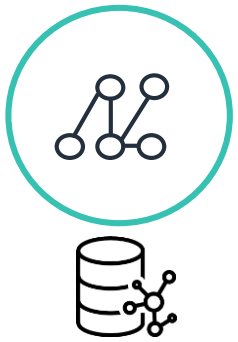
DocumentDB

In Memory



ElastiCache

Graph



Neptune

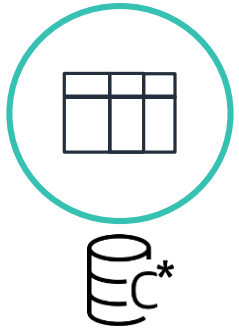
Time Series

Timestream

Ledger

QLDB

Wide Column



Keyspaces

Move to fully managed databases

Migrate on-premises or self-managed databases to fully managed services

Relational databases

ORACLE
MySQL
Microsoft SQL Server
PostgreSQL
MariaDB

Non-relational databases

mongoDB
Cassandra
redis
memcached

aws training and certification

Amazon RDS (Relational Database Service)

Set up, operate, and scale a fully managed RDS with just a few clicks

Amazon Aurora PostgreSQL-Compatible Edition

Amazon Aurora MySQL-Compatible Edition

MySQL

PostgreSQL

MariaDB

Microsoft SQL Server

ORACLE

Easy to administer

Easily deploy and maintain hardware, OS, and DB software, with built-in monitoring

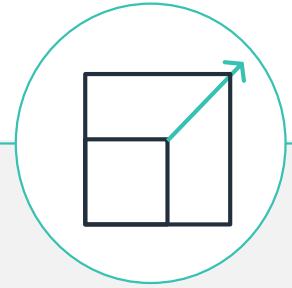
Secure and compliant

Data encryption at rest and in transit, with industry compliance and assurance programs

Available and durable

Automatic Multi-AZ data replication, with automated backup, snapshots, and failover

Performant and scalable



Scale compute and storage with a few clicks, plus minimal downtime for your application

Amazon Aurora

MySQL and PostgreSQL compatible relational database – built for the cloud

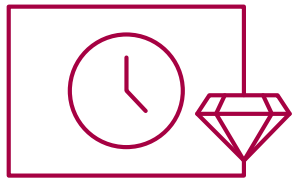
Aurora Resiliency

Aurora maintains six copies of data, two copies in each Availability Zone (3 AZ's). This protects against AZ +1 failures.

Primary and replicas all point to the same underlying storage

Exam Tip

Questions that speak to migrations of MySQL / PostgreSQL databases to the cloud that require high availability, resiliency, or multiple AZ's → Aurora should be your first thought!

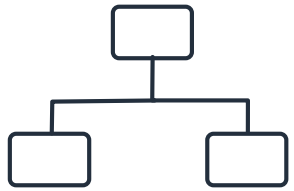


Availability and durability

Fault-tolerant, self-healing storage; six copies of data across three Availability Zones; continuous backup to Amazon S3

Performance and scalability

5x throughput of standard MySQL and 3x of standard PostgreSQL; scale-out up to 15 read replicas



Fully managed

Managed by RDS: no server provisioning, software patching, setup, configuration, or backups

Amazon Aurora Global Databases

Amazon Aurora global databases span multiple AWS Regions

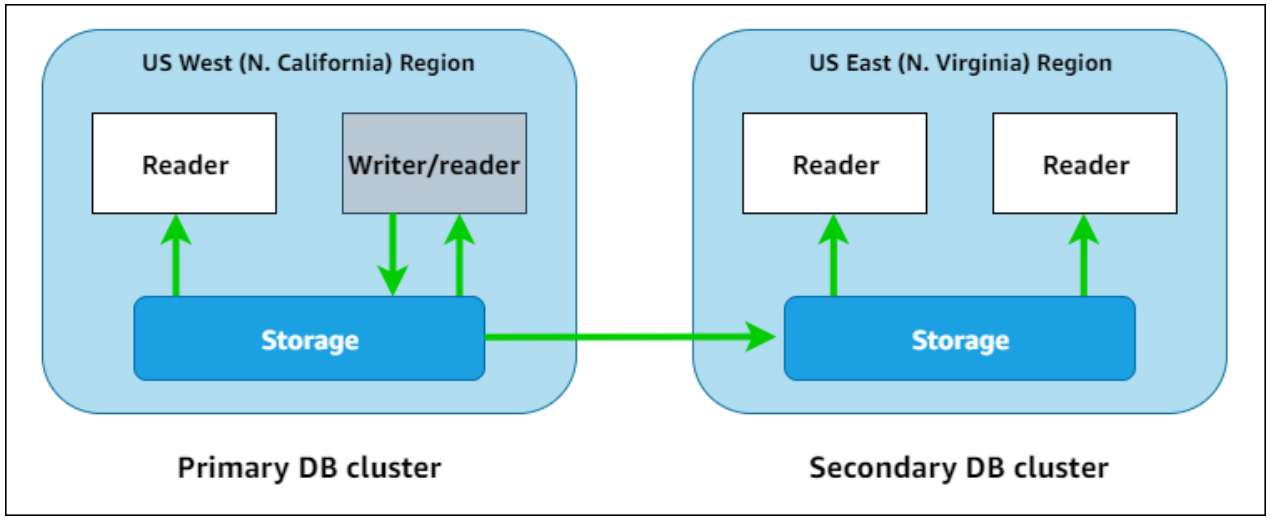
Aurora includes some high availability features that apply to data in your DB cluster

Overview

By using an Amazon Aurora global database, you can run your globally distributed applications using a single Aurora database that spans multiple AWS Regions.

Advantages

- Global reads with local latency
- Scalable secondary Aurora DB clusters
- Fast replication from primary to secondary Aurora DB clusters
- Recovery from Region-wide outages



Amazon DynamoDB

Fast and Flexible **Key-Value** database service for any scale

DynamoDB

A fully managed – multiple master, multiple region database solution for high performance, globally distributed applications

Disaster proof solution with multi-region redundancy

Exam Tip

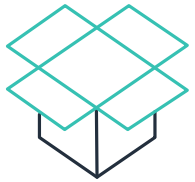
Key-Value is the dead giveaway for DynamoDB. Any question that references this on the exam is cluing you towards a solution that is built around DynamoDB

Serverless architecture

No hardware provisioning, software patching, or upgrades; scales up or down automatically; continuously backs up your data

Enterprise security

Encrypts all data by default and fully integrates with AWS Identity and Access Management for robust security

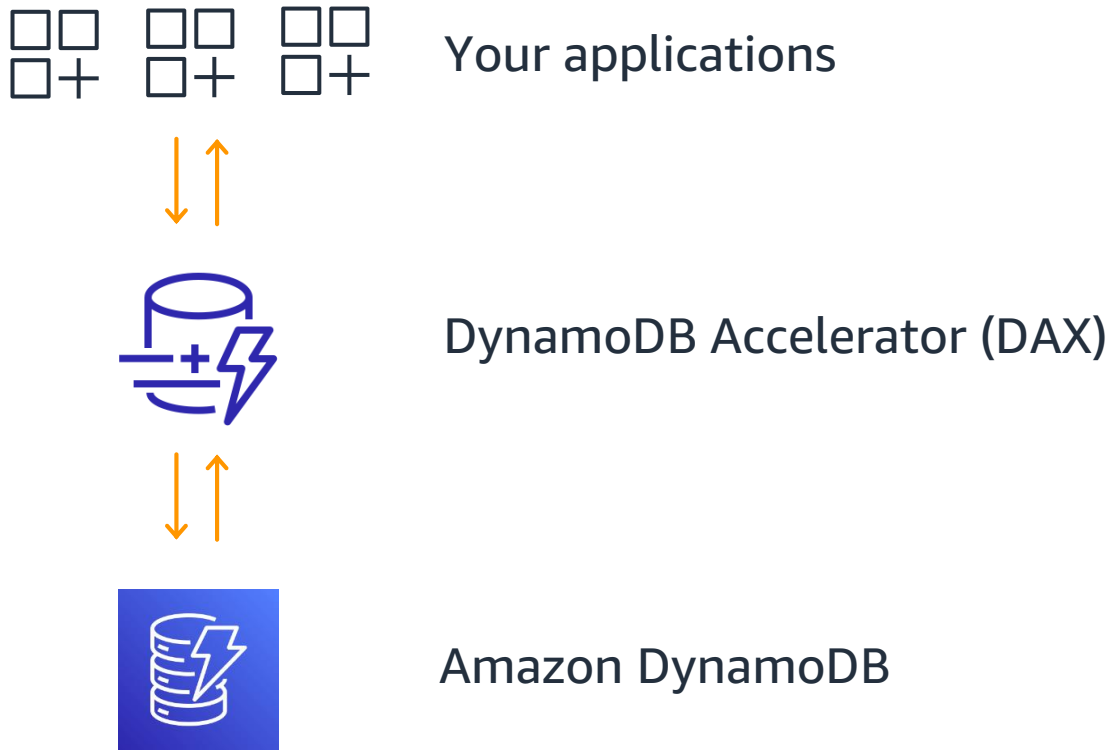


Global replication

Build global applications with fast access to local data by easily replicating tables across multiple AWS Regions

DynamoDB Accelerator (DAX)

In-memory cache for DynamoDB w/ up to 10x performance improvement



- Fully managed, highly available cache for DynamoDB
- Even faster—microsecond latency
- Scales to millions of requests per second
- API compatible

AWS Elastic Compute Cloud (EC2)

aws training and certification

Amazon EC2

Provides secure, resizable compute capacity in the AWS Cloud, enabling servers to be spun up in minutes without the need for physical hardware.

Reliable and Scalable Infrastructure

Increase or decrease capacity within minutes and provide 99.99% availability for each Amazon EC2 region.

Easy Migration

Get started quickly through AWS Migration Tools, AWS Managed Services, or Amazon Lightsail with the help from AWS Professional Services, AWS Support and APN Partners.

Secure Your Applications

Provide various security standards and features, reduce the risk of human error and eliminate the attack surface.

Flexible Pricing

Offer five pricing models to pay for Amazon EC2 instances: On-Demand, Savings Plans, Dedicated Hosts, Spot Instances and Per Second Billing.

Amazon EC2 Auto Scaling

Add or remove compute capacity to meet changes in demand

Use with EC2 fleet to improve fault tolerance, application availability, and lower costs.

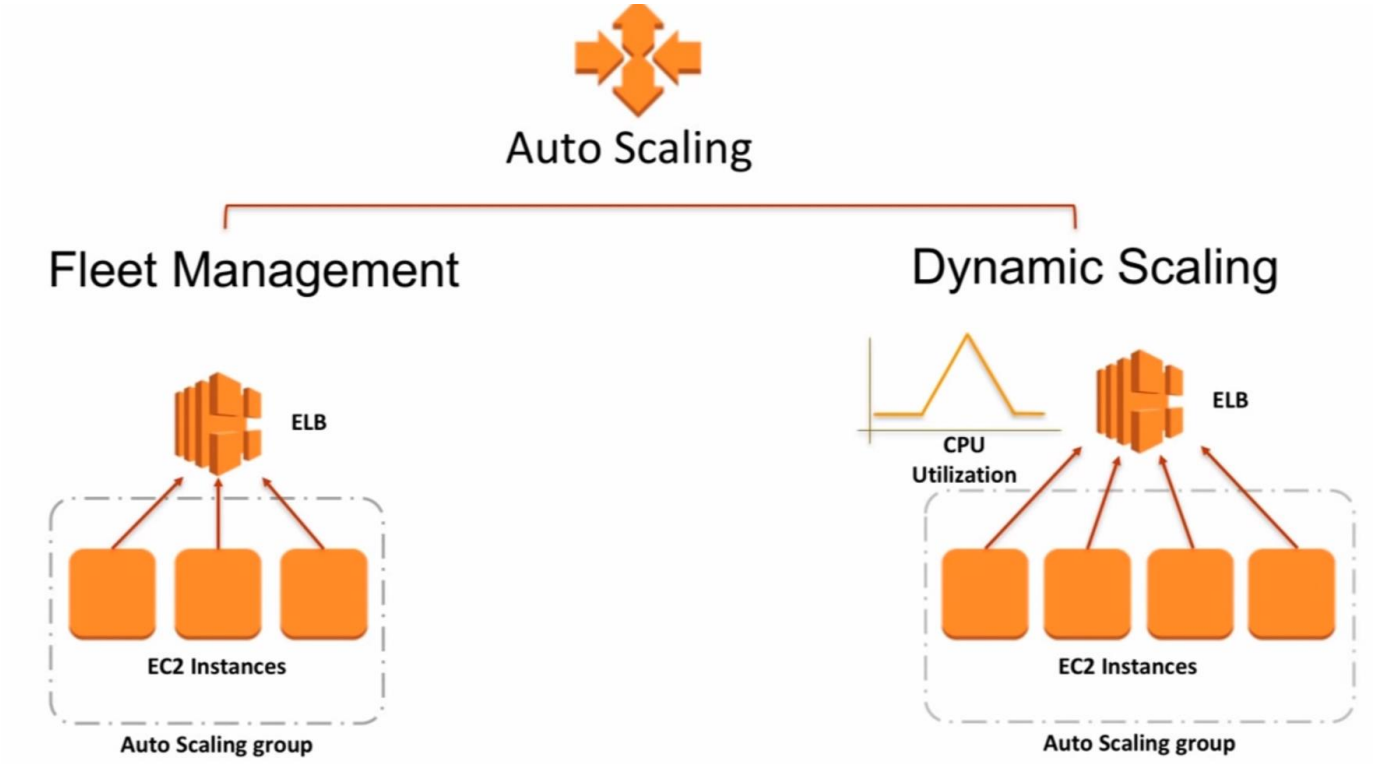
Fleet Management

Maintain health and availability of EC2 fleet. Monitor health of running instances, replace impaired instances automatically, and balance capacity across Availability Zones.

Scaling Options

Scheduled scaling allows you to scale up or down ahead of known load changes.

Dynamic scaling allows you to automatically follow the demand curve of your application usage based on load metrics.



AWS Auto Scaling

Scaling for multiple AWS services and resources

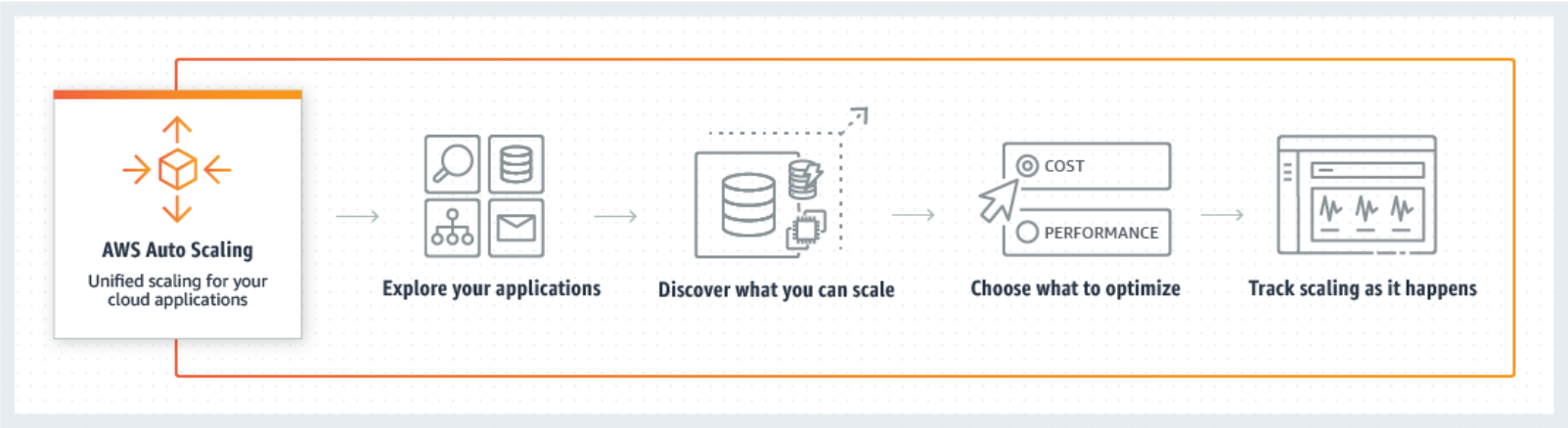
Monitor applications and automatically adjust capacity for maintain steady, predictable performance at lowest possible cost.

Scale Services

Manage Spot fleets, scale ECS tasks, DynamoDB tables, Aurora Replicas, and other resources needed for an application to effectively scale.

Predictive Scaling

Predicts future traffic, including regularly-occurring spikes, and provisions the right number of EC2 instances in advance of predicted changes.



aws training and certification

Amazon EC2 Auto Scaling Groups

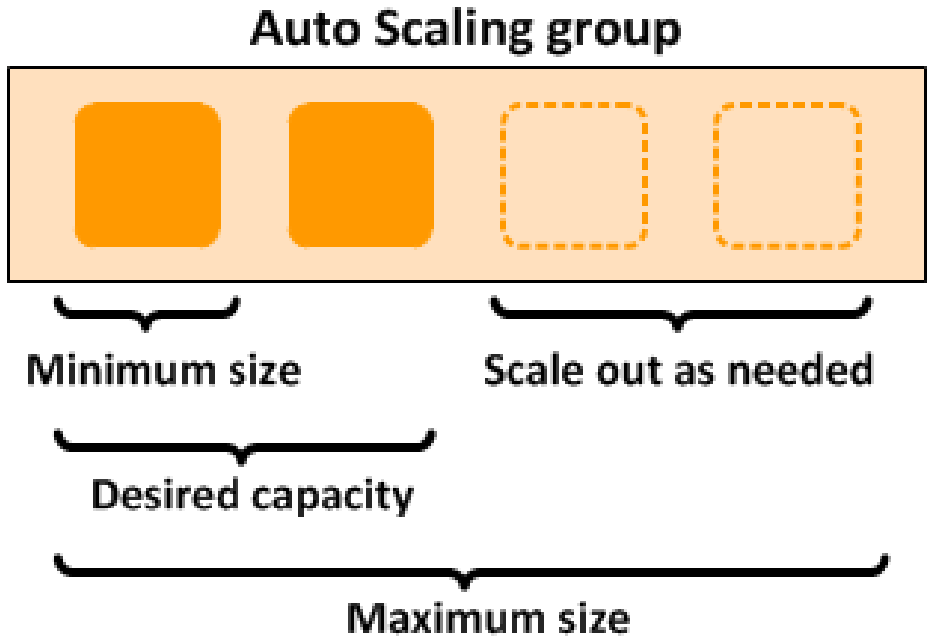
Collection of Amazon EC2 instances that are treated as a logical grouping

Utilized with Auto Scaling to define which group scales.

What it Does

Allows usage of EC2 Auto Scaling features such as health check replacements, and scaling policies. Group launches enough instances to meet desired capacity and maintains by performing periodic health checks. The Auto Scaling Group is the defined group of instances which is managed by the EC2 Auto Scaling policies.

On-Demand instances, Spot instances, or both may be launched. Templates should be defined for the groups, with consideration of multiple Availability Zones.



Elastic Load Balancing

Distribute network traffic to improve application scalability

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets and virtual appliances in one or more Availability Zones (AZs)

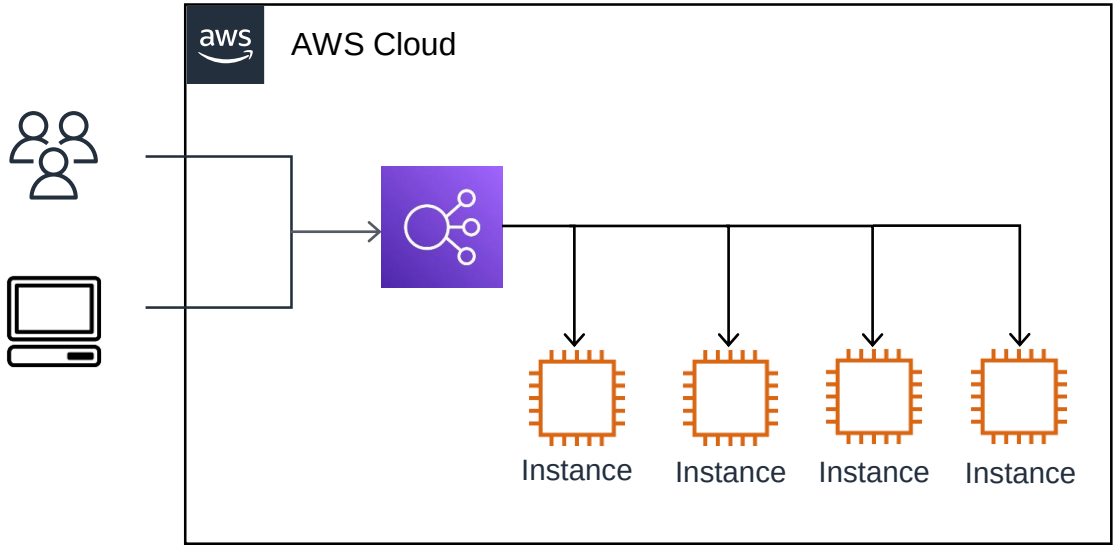
Key Capabilities

Security
Use with VPC, create and manage security groups associated with ELB for additional networking and security options. Configure as a internet or internal facing load balancer.

High Availability
Distribute traffic across single or multiple AZ's. Automatically scales its request handling capacity in response to incoming application traffic.

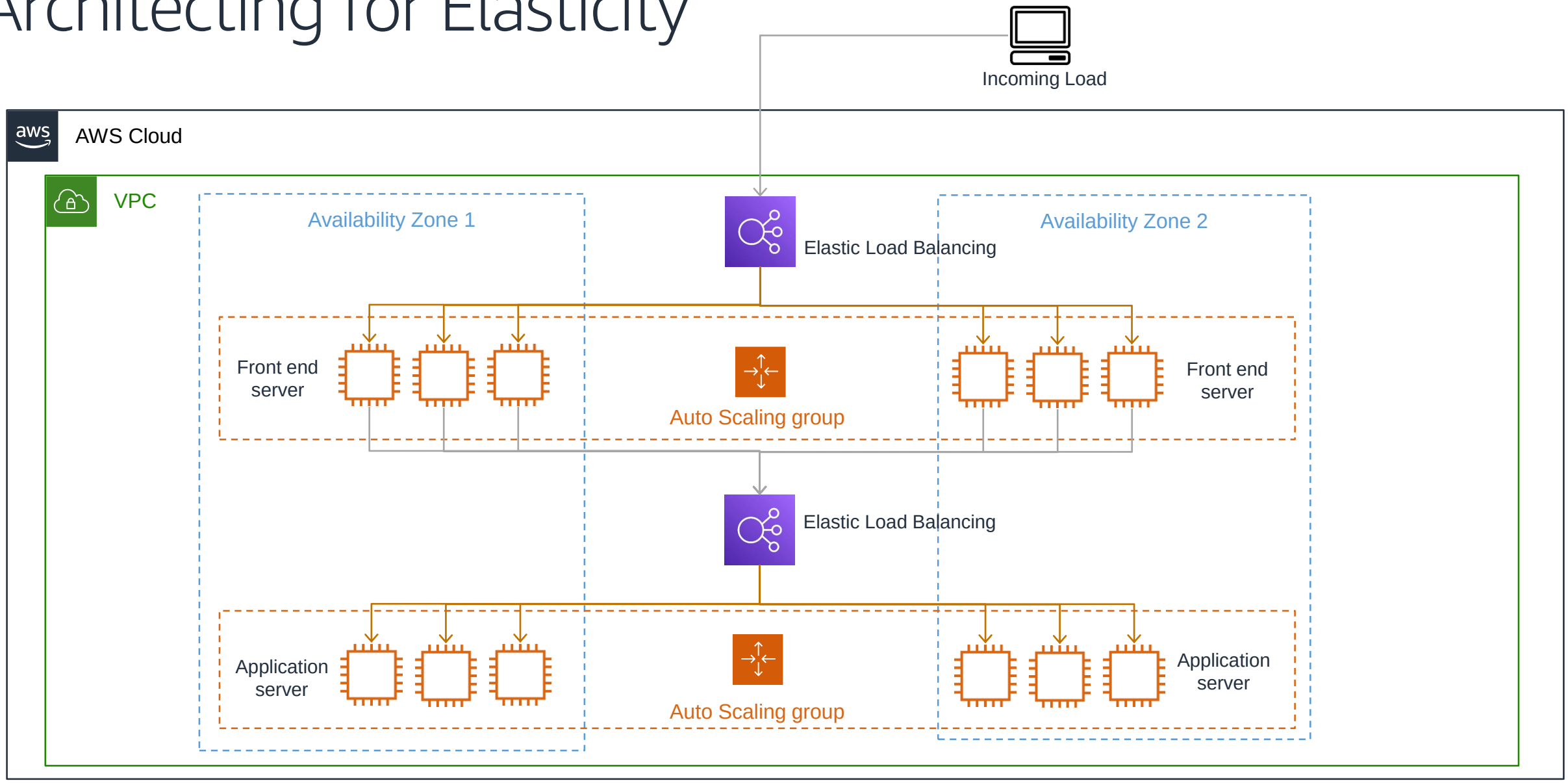
High Throughput
Handles traffic as it grows, to millions of requests/sec and sudden, volatile traffic patterns.

Health checks
Only routes traffic to healthy targets. Provides insight into ELB backed services and metrics on traffic patterns for services running on instances.



aws training and certification

Architecting for Elasticity



Amazon EC2 Billing

Provides secure, resizable compute capacity in the AWS Cloud, enabling servers to be spun up in minutes without the need for physical hardware.

Savings Plans

Lower prices on Amazon EC2 instance usage regardless of instance family, size, OS, tenancy, or AWS Region for commitments on **usage.**

Per Second Billing

On Demand

Pay for EC2 compute capacity by the second without any long-term commitments. Pay-as-you go pricing.

Spot Instances

UEC2 capacity in the AWS cloud. Spot instances can provide up to 90% savings over on-demand instance types.

Dedicated Host

Use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2

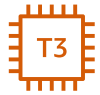
Amazon EC2 General Purpose Instances

Balance of compute, memory, and networking resources.

Mac instance

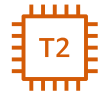
M1 Mac instance

T4g instance



T3 instance

T3a instance



T2 instance

M6g instance

M6gd instance

M6i instance

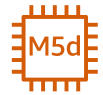
M6in instance

M6idn instance

M6a instance

M5 instance

M5a instance



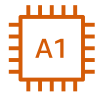
M5d instance

M5n instance

M5dn instance

M5zn instance

M4 instance



A1 instance

aws training and certification

Amazon EC2 Compute Optimized Instances

Ideal for compute bound applications that benefit from high performance processors.

Amazon EC2 Memory Optimized Instances

Designed to deliver fast performance for workloads that process large data sets in memory

R7iz instance

R6in instance

R6idn instance

R6a instance

R6g instance

R6i instance

R5 instance

R5a instance

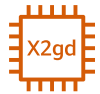
R5ad instance

R5gd instance

R5b instance

R5n instance

R4 instance



X2gd instance

X2idn instance

X2iedn instance

X2iezn instance

X1e instance

X1 instance

High Memory instance

z1d instance

Amazon EC2 Accelerated Computing Instances

Use hardware accelerators, or co-processors, to perform functions more efficiently than is possible in software running on CPUs.

Amazon EC2 Storage Optimized Instances

Designed for workloads that require high, sequential read and write access to very large data sets on local storage.

Storage-optimized instances

Im4gn instance

Is4gen instance

I4i instance

I3 instance

I3en instance

I2 instance

D2 instance

D3 instance

D3en instance

H1 instance


DB instance

HPC-optimized instances

Hpc6id instance

Hpc6a instance

aws training and certification

EC2 Placement Groups

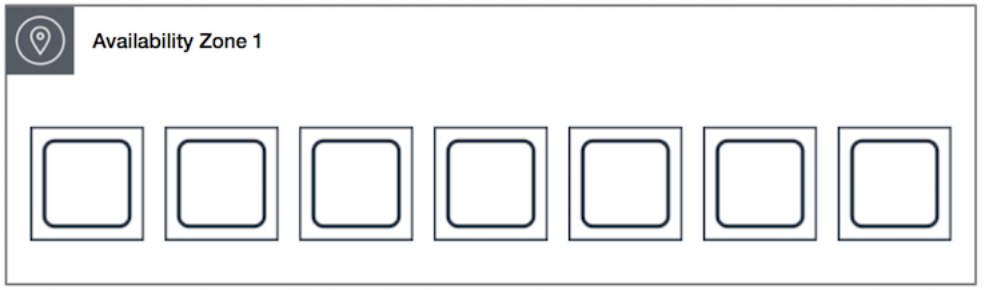
aws training and certification

EC2 Placement Groups

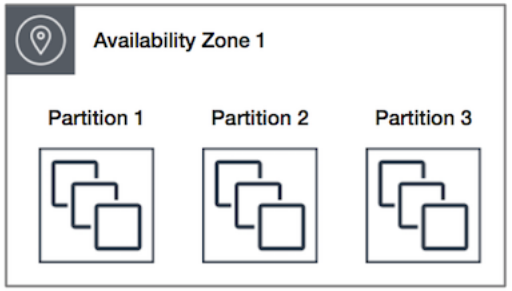
There are three types of placement groups you can use with EC2 instances. Each has their advantages and disadvantages to your proposed architecture.

Cluster

Spread



Partition



Cluster Placement Group

Placement Groups are the bread and butter of a Solutions Architect. Understanding when, and how, to deploy your resources is a critical skillset

Cluster Placement

A cluster placement group is a logical grouping of instances within a single Availability Zone. A cluster placement group can span peered VPCs in the same Region.

When to use them?

Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. They are also recommended when the majority of the network traffic is between the instances in the group.

Partition Placement Group

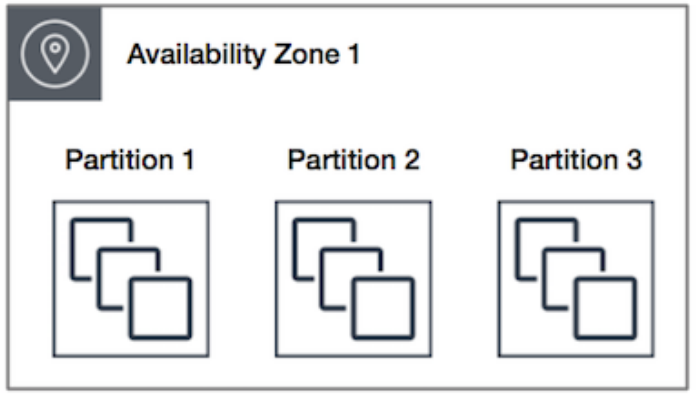
Placement Groups are the bread and butter of a Solutions Architect. Understanding when, and how, to deploy your resources is a critical skillset

Partition Placement

Partition placement groups help reduce the likelihood of correlated hardware failures for your application. When using partition placement groups, Amazon EC2 divides each group into logical segments called partitions.

When to use them?

Partition placement groups can be used to deploy large distributed and replicated workloads, such as HDFS, HBase, and Cassandra, across distinct racks.



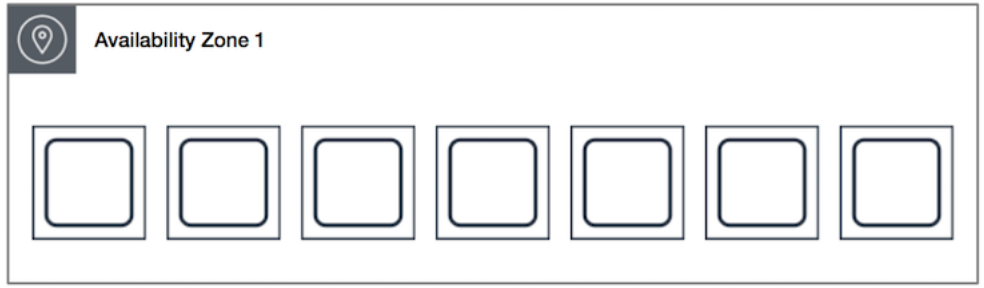
Spread Placement Group

Placement Groups are the bread and butter of a Solutions Architect. Understanding when, and how, to deploy your resources is a critical skillset

Spread Placement

A spread placement group is a group of instances that are each placed on distinct racks, with each rack having its own network and power source.

The image – at right - shows seven instances in a single AZ that are placed into a spread placement group.



When to use them?

Spread placement groups are recommended for applications that have a small number of critical instances that should be kept separate from each other.

EC2 AMIs
EC2 Instance Metadata

aws training and certification

Amazon Machine Images (AMI)

An Amazon Machine Image (AMI) is a supported and maintained image provided by AWS that provides the information required to launch an instance.

Key Topics

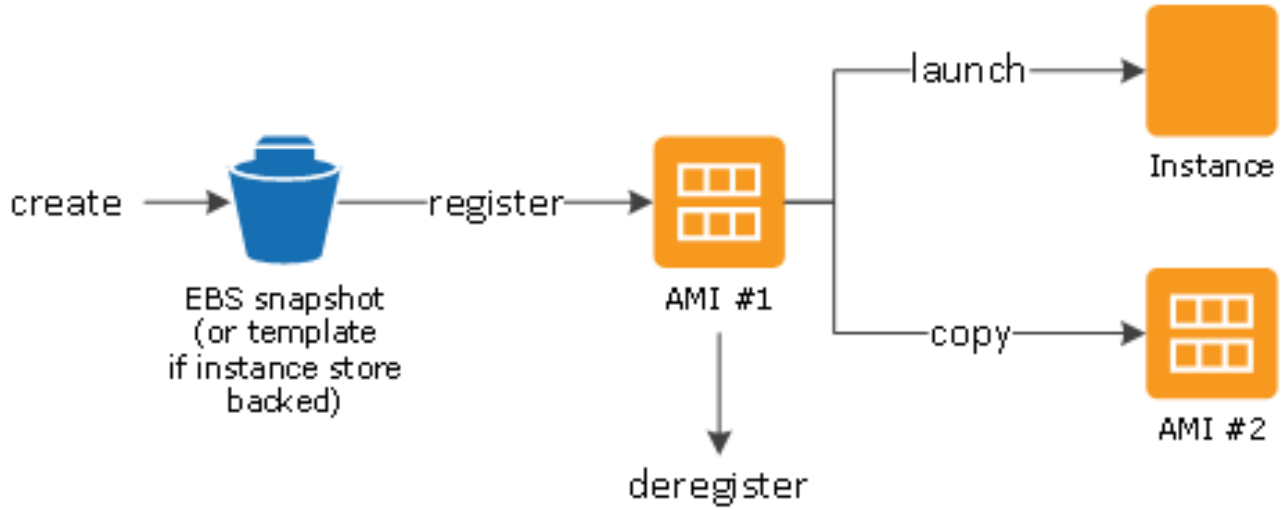
All AMIs are categorized as either *backed by Amazon EBS* or *backed by instance store*.

Amazon EBS-backed AMI – The root device for an instance launched from the AMI is an Amazon Elastic Block Store (Amazon EBS) volume created from an Amazon EBS snapshot.

Amazon instance store-backed AMI – The root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.

When to Use an AMI

You **must specify an AMI when you launch an instance**. You can launch multiple instances from a single AMI when you require multiple instances with the same configuration.



aws training and certification

EC2 Instance Metadata

Instance metadata is data about your instance that you can use to configure or manage the running instance.

How to Retrieve Instance Metadata

Because your instance metadata is available from your running instance, you do not need to use the Amazon EC2 console or the AWS CLI. This can be helpful when you're writing scripts to run from your instance. For example, you can **access the local IP** address of your instance **from instance metadata** to manage a connection to an external application.

What can you access with instance metadata?

You can also use instance metadata to access user data that you specified when launching your instance. For example, you can specify parameters for configuring your instance, or include a simple script. You can build generic AMIs and use user data to modify the configuration files supplied at launch time.

To view all categories of instance metadata from within a running instance, use the following IPv4 or IPv6 URIs.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Amazon KMS & EBS Encryption

aws training and certification

AWS Key Management Service (KMS)

AWS KMS is a managed service that makes it easy for you to create and control the cryptographic keys that are used to protect your data

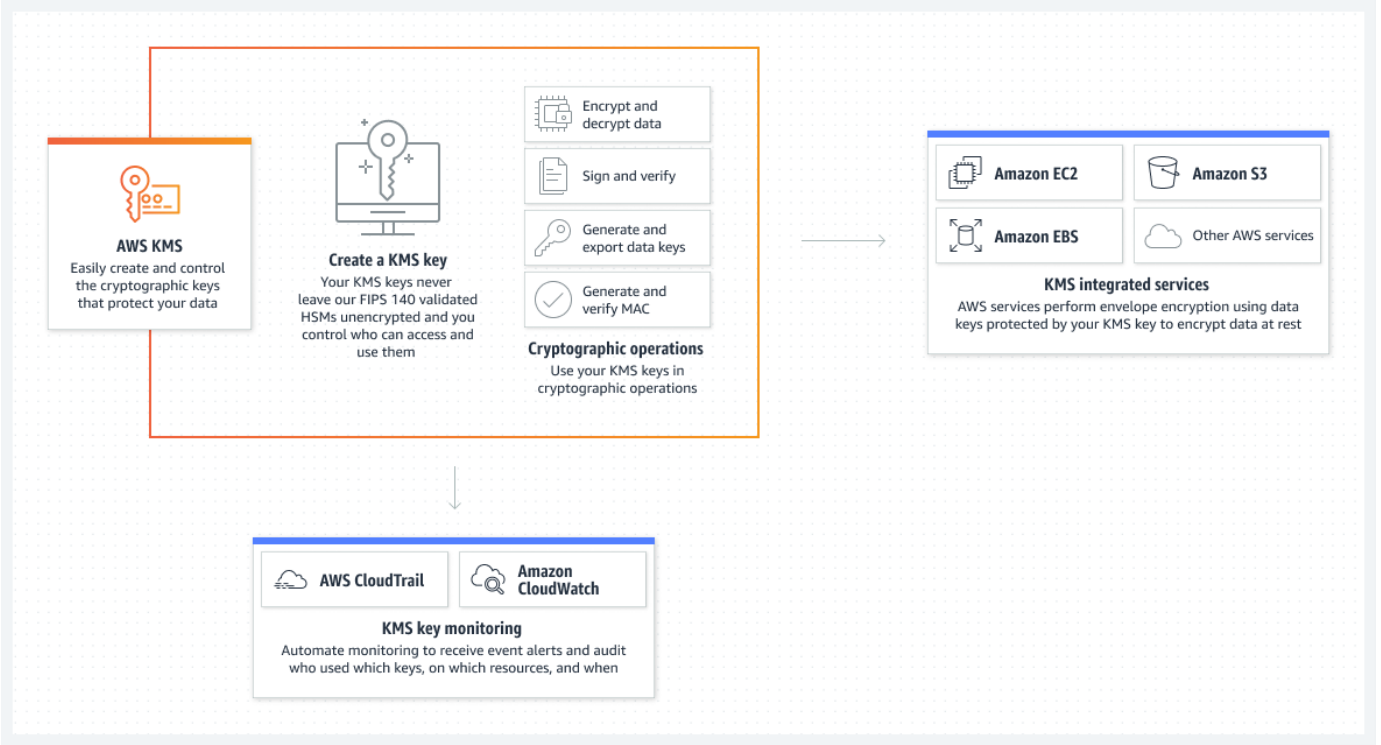
What is KMS?

AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under **FIPS 140-2**, or are in the process of being validated, to protect your keys.

What does it provide?

AWS Key Management Service (KMS) KMS keys are the primary resource in AWS KMS. You can use a KMS key to encrypt, decrypt, and re-encrypt data.

KMS provides the ability to create **symmetric** and **asymmetric** encryption keys.



AWS Key Management Service (KMS)

AWS KMS is a managed service that makes it easy for you to create and control the cryptographic keys that are used to protect your data

KMS Key Types

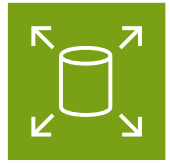
CMKs can be broken down into two general types: **AWS-managed** and **customer-managed**.

An AWS-managed CMK is created when you choose to enable server-side encryption of an AWS resource under the AWS-managed CMK for that service for the first time (e.g., SSE-KMS). An AWS-managed CMK can only be used to protect resources within the specific AWS service for which it's created. It does not provide the level of granular control that a customer-managed CMK provides.

For more control, a **best practice is to use a customer-managed CMK** in all supported AWS services and in your applications. A customer-managed CMK is created at your request and should be configured based upon your explicit use case.

	AWS-managed CMK	**Customer-managed CMK**
Creation	AWS generated on customer's behalf	Customer generated
Rotation	Once every three years automatically	Once a year automatically through opt-in or on-demand manually
Deletion	Can't be deleted	Can be deleted
Scope of use	Limited to a specific AWS service	Controlled via KMS/IAM policy
Key Access Policy	AWS managed	Customer managed
User Access Management	IAM policy	IAM policy

EBS Encryption



You can encrypt both the boot and data volumes of an EC2 instance.

Key Concepts

When you create an encrypted EBS volume and attach it to a supported instance type, the **following types of data are encrypted**:

- **Data at rest** inside the volume
- All data **moving between** the volume and the instance
- All **snapshots** created from the volume
- All **volumes** created from those snapshots

Other Considerations

Use Amazon EBS encryption as a straight-forward encryption solution for your EBS resources associated with your EC2 instances.

When you create an encrypted EBS resource, it is encrypted by your account's default KMS key for EBS encryption unless you specify a different customer managed key in the volume creation parameters or the block device mapping for the AMI or instance

Using your own KMS key gives you more flexibility, including the ability to create, rotate, and disable KMS keys.

AWS Monitoring & Alerting

aws training and certification

Amazon CloudWatch

Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources

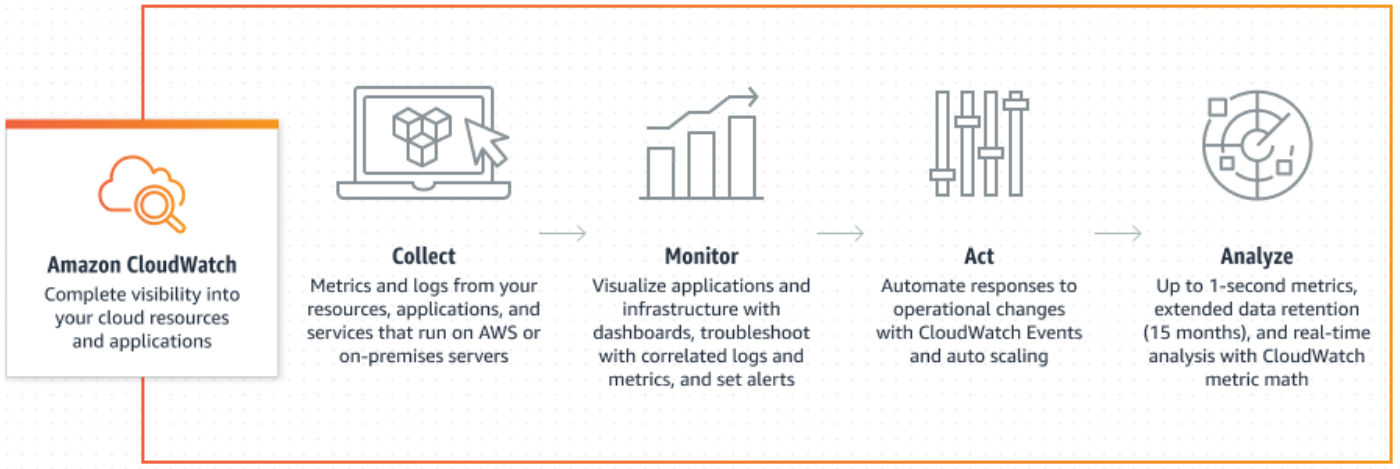
Monitoring

CloudWatch Metrics are **provided automatically** for a number of AWS products and services. You can also monitor custom metrics generated by your own applications and services.

CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files.

Key Concept

Monitor key metrics and logs, **visualize** your application and infrastructure stack, **create alarms**, and correlate data to **understand** and **resolve** the root cause of performance issues in your AWS resources.



Amazon EventBridge

Amazon EventBridge is a serverless event bus service that you can use to connect your applications with data from a variety of sources.

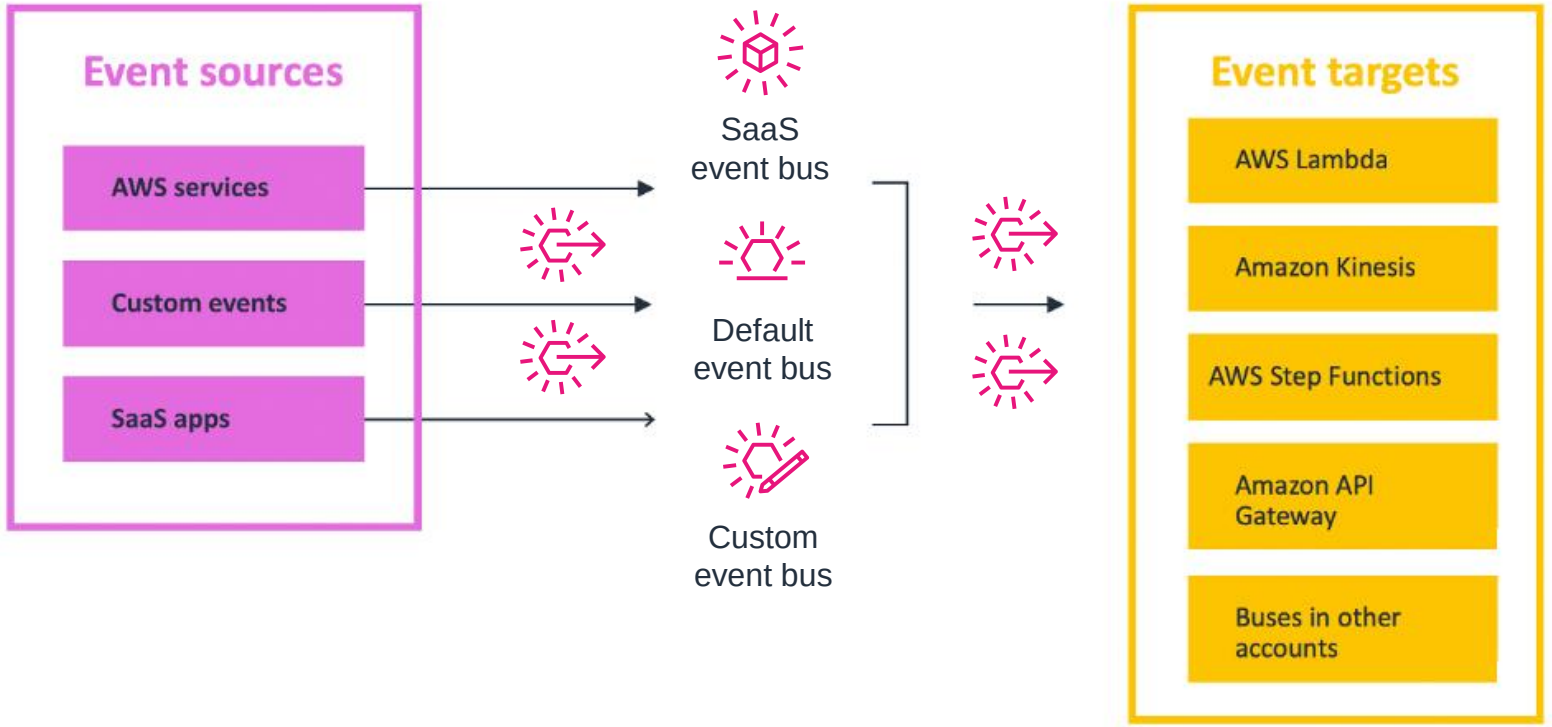
What is it?

Amazon EventBridge is a serverless event bus service that you can use to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your applications, software as a service (SaaS) applications, and AWS services to targets such as AWS Lambda functions, HTTP invocation endpoints using API destinations, or event buses in other AWS accounts.

How it works

EventBridge receives an event, an indicator of a change in environment, and applies a rule to route the event to a target. Rules match events to targets based on either the structure of the event, called an event pattern, or on a schedule.

For example, when an Amazon EC2 instance changes from pending to running, you can have a rule that sends the event to a Lambda function.



AWS Security

aws training and certification

Amazon CloudTrail

CloudTrail logs, continuously monitors, and retains **account activity** related to actions across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

Some Use Cases

Audit activity

Monitor, store, and validate activity events for authenticity. Easily generate audit reports required by internal policies and external regulations.

Identify security incidents

Detect unauthorized access using the **Who, What, and When** information in CloudTrail Events. Respond with rules-based EventBridge alerts and automated workflows.

Key Concepts

CloudTrail **records user activity and API usage across AWS services as Events**. CloudTrail Events help you answer the questions of "who did what, where, and when?"

AWS CloudTrail Event history

Always available to view / download last 90 days of events per Region within AWS Account.

CloudTrail Trail outputs

Amazon S3

Saves CloudTrail trail event as series of compressed logs in Amazon S3.

Amazon CloudWatch Logs

Saves each CloudTrail event as a log event into a CloudWatch Logs.

CloudTrail events search

Amazon Athena

Query and analyze CloudTrail logs from Amazon S3 bucket as SQL statements.

Amazon CloudWatch Insights

Search and analyze CloudTrail events from their CloudWatch Logs group.

aws training and certification

AWS WAF

AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define

Deployment Options

- On Amazon CloudFront as part of CDN
- On Application Load Balancer fronting web or origin servers running on EC2
- Amazon API Gateway for REST APIs
- AWS AppSync for GraphQL APIs

Key Concepts

AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control **bot traffic** and **block common attack patterns**, such **as SQL injection or cross-site scripting**.

Pay only for what you use, pricing based on how many rules are deployed and how many requests the application receives.

Amazon Shield

AWS Shield is a managed **Distributed Denial of Service (DDoS) protection service** that safeguards applications running on AWS.

AWS Shield

AWS Shield Standard **defends against** most common, frequently occurring network and transport layer **DDoS attacks** that target your web site or applications. AWS Shield Standard used with Amazon CloudFront and Amazon Route 53, provides comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

Managed service, provided at no additional charge.

AWS Shield Advanced

AWS Shield Advanced provides higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 resources.

Cost includes some features of AWS WAF and AWS Firewall Manager.

Amazon Firewall Manager

AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations.

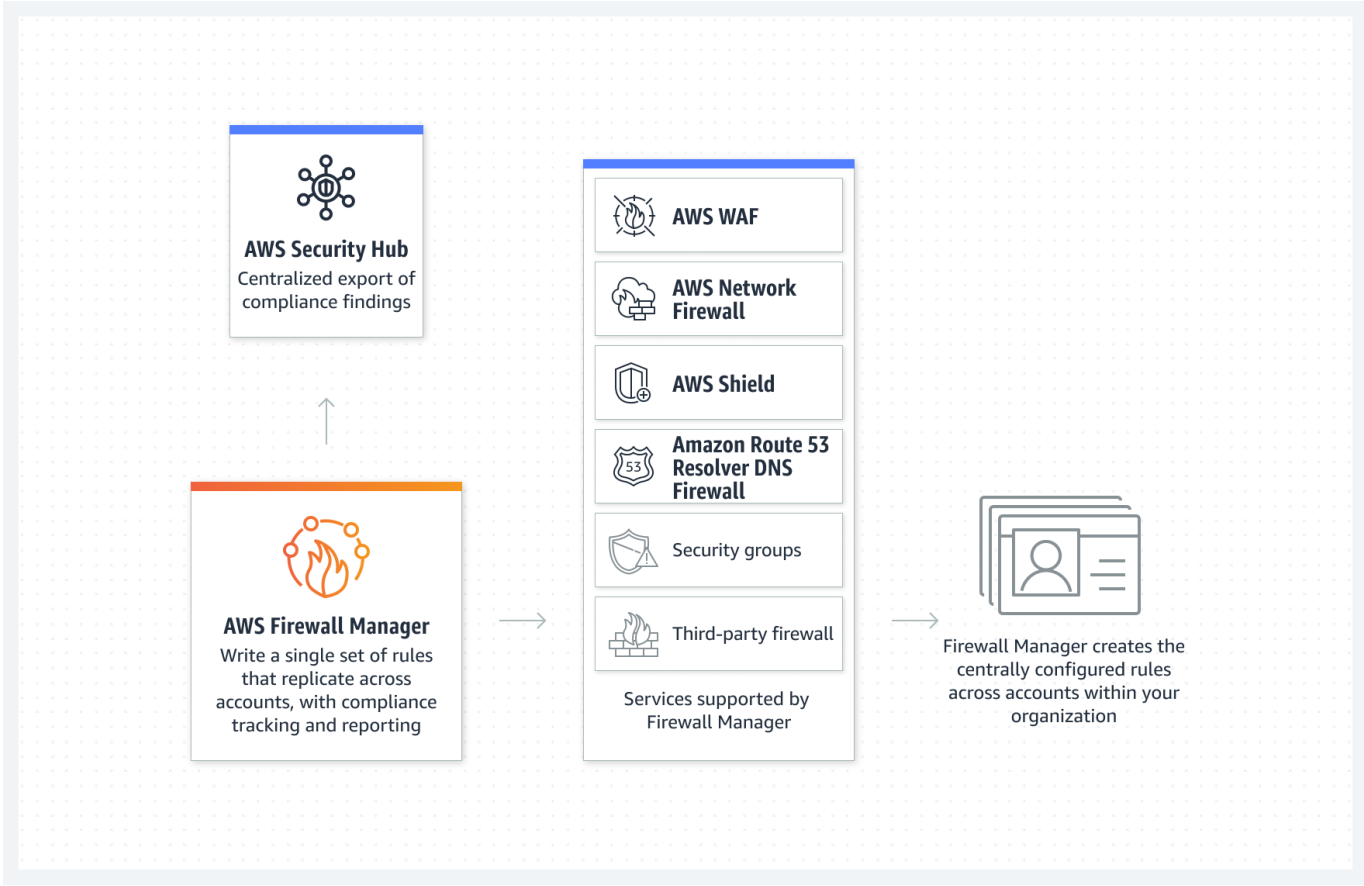
Use Cases

- Protect applications hosted on EC2 instances
- Deploy tools at scale to protect data
- Continually audit resources

Key Concepts

Amazon Firewall Manager allows you to centrally deploy AWS Network Firewall across VPCs. Changes are automatically propagated across your accounts and VPCs.

Automatically deploy VPC security groups, AWS WAF rules, AWS Shield Advanced protections, AWS Network Firewall rules, and Amazon Route 53 Resolver DNS Firewall rules.



Amazon Macie

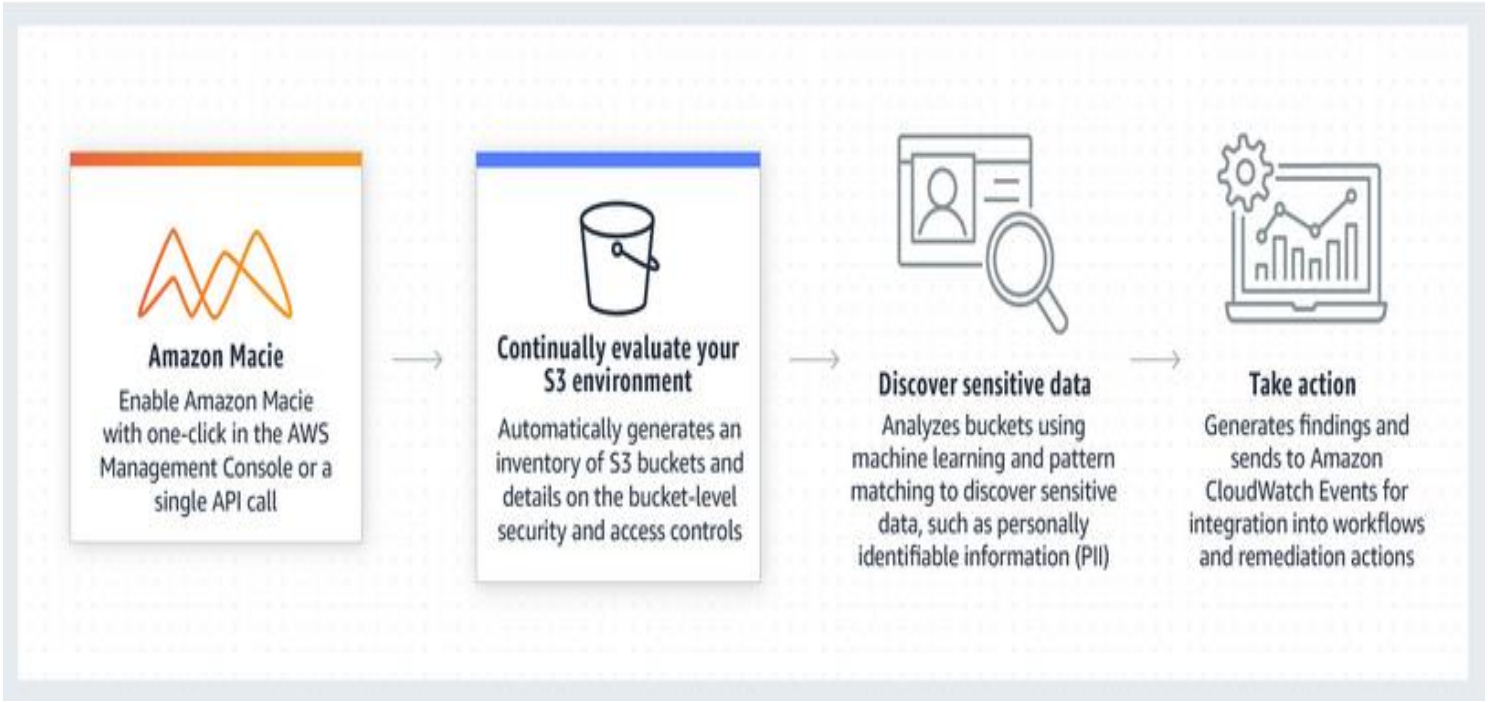
Amazon Macie continually **evaluates your Amazon S3 environment** and provides an S3 resource summary across all of your accounts.

Purpose

Amazon Macie uses machine learning and pattern matching to cost efficiently discover sensitive data at scale. Macie automatically detects a large and growing list of sensitive data types, including **personally identifiable information (PII)** such as names, addresses, and credit card numbers. It also gives you constant visibility of the data security and data privacy of **your data stored in Amazon S3.**

Easy to Deploy

With **one-click** in the AWS Management Console or a single API call, you can enable Amazon Macie in a single account. With a **few more clicks** in the console, you can enable Macie **across multiple accounts**.



Amazon GuardDuty

Monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

Key Benefits

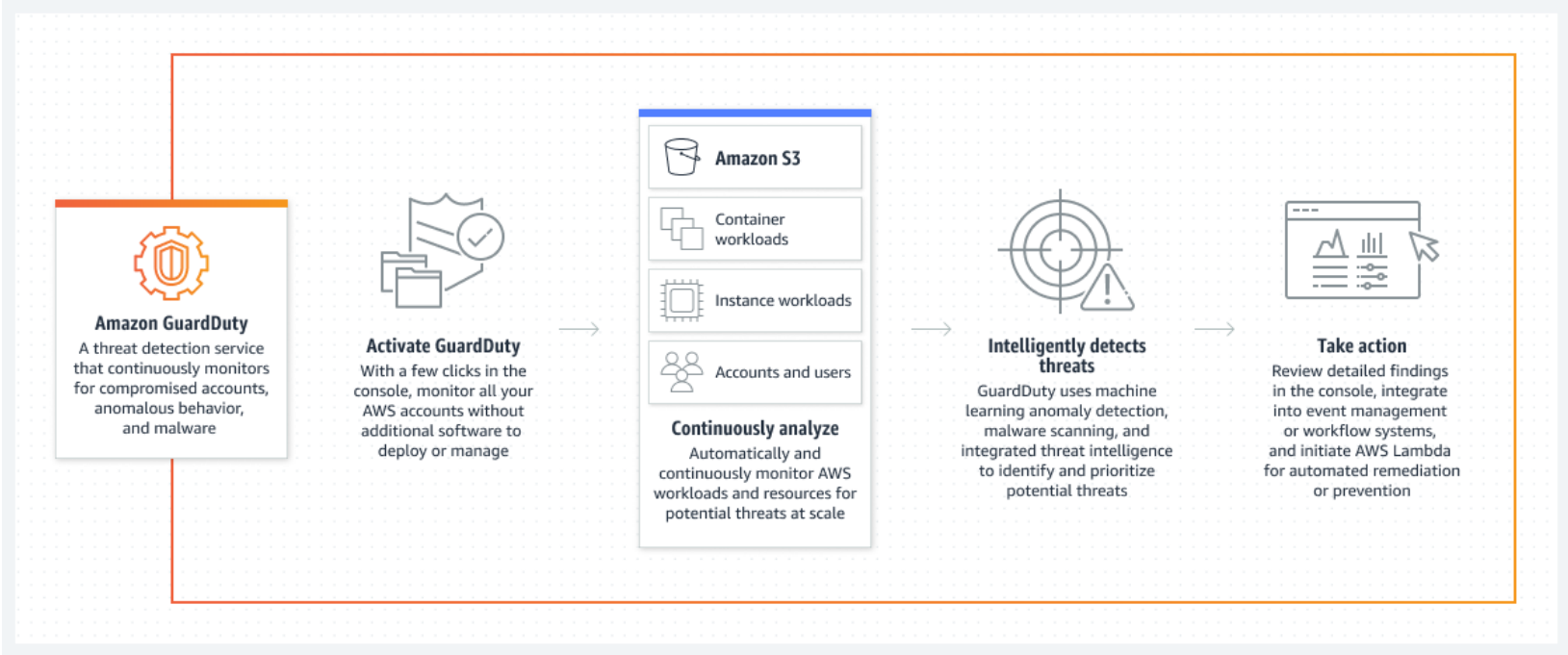
Amazon GuardDuty makes it easy for you to continuously monitor your AWS accounts, workloads, and data stored in Amazon S3.

GuardDuty operates completely independently from your resources, so there is no risk of performance or availability impacts to your workloads.

There are no upfront costs and you pay only for the events analyzed, with no additional software to deploy or threat intelligence feed subscriptions required.

Key Concept

Amazon GuardDuty analyzes **AWS CloudTrail**, **VPC Flow Logs**, and **AWS DNS logs** for malicious activity and anomalous behavior.



Amazon Inspector

An automated vulnerability management service that continually scans **Amazon Elastic Compute Cloud (EC2) and container workloads** for software vulnerabilities and unintended network exposure.

Use Cases

Use up-to-date common vulnerabilities and exposures (CVE) information combined with factors such as network accessibility to create context-based risk scores that help you prioritize and address vulnerable resources.

Support compliance requirements and best practices for NIST CSF, PCI DSS, and other regulations with Amazon Inspector scans.

Identify zero-day vulnerabilities sooner

Key Concept

Amazon Inspector is an automated vulnerability management service that continually **scans Amazon Elastic Compute Cloud (EC2) and container workloads** for software vulnerabilities and unintended network exposure

Thank you!

aws training and certification