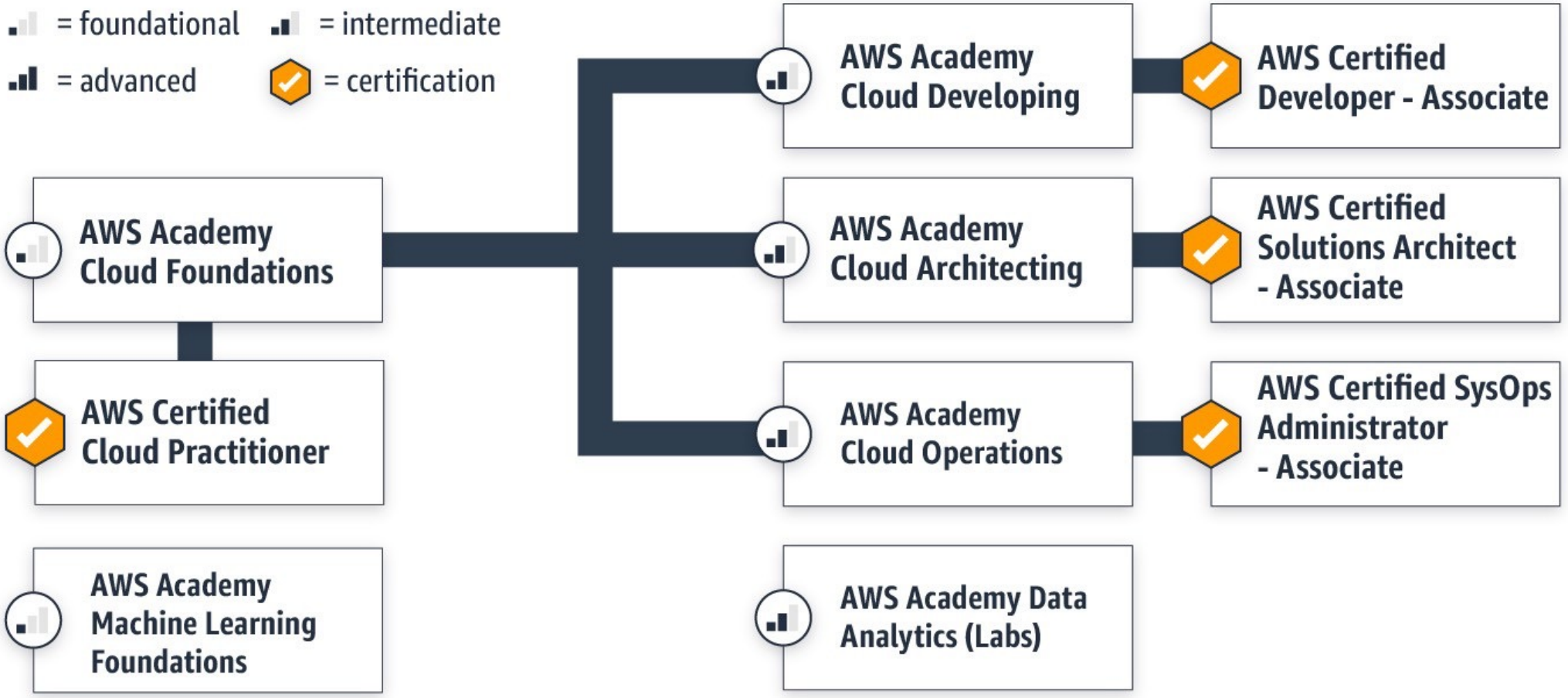
Leonardo AWS Course

Revision and Exam Preperation

Pavlos, Bill

Recommended learning paths



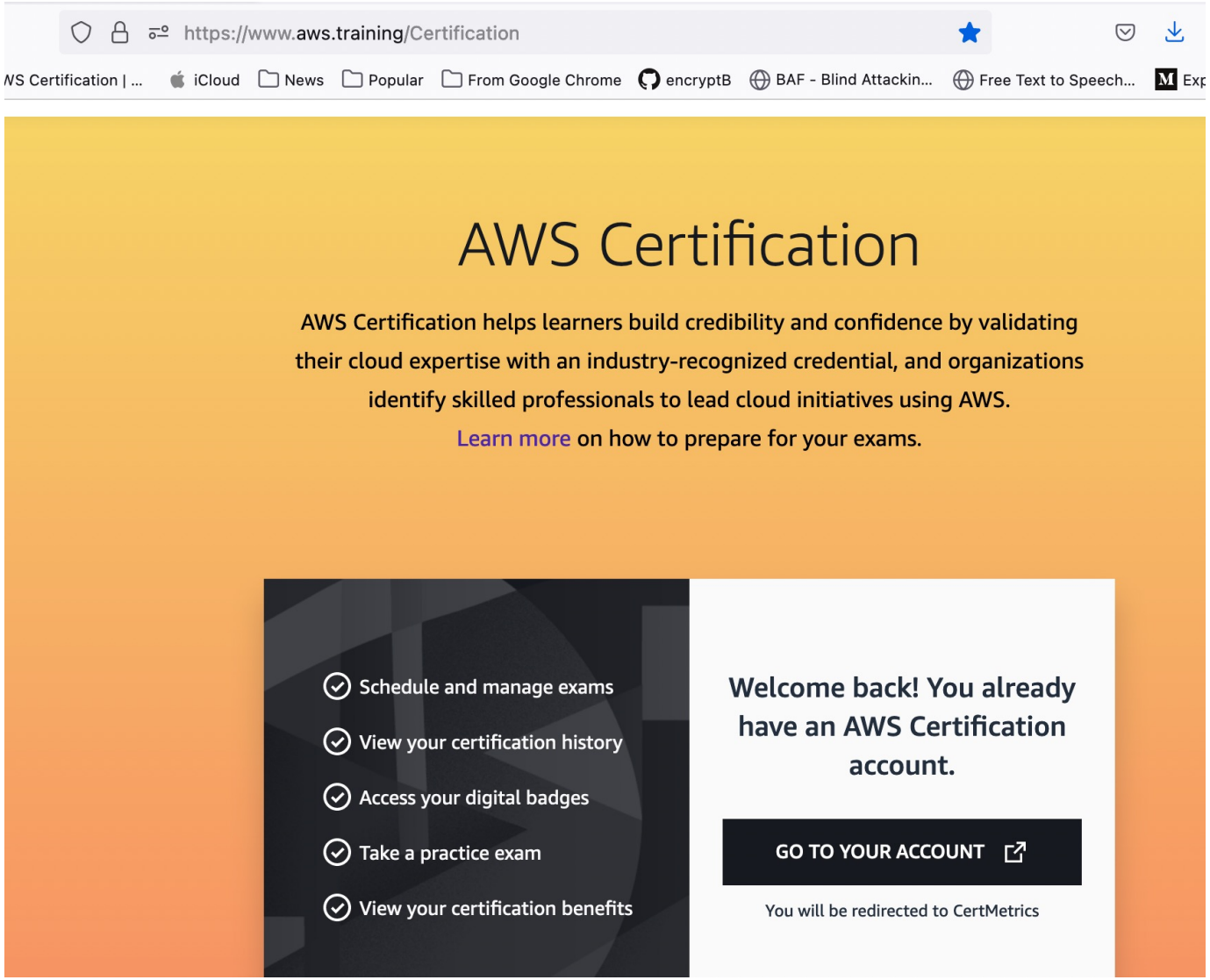
Course outline

- Module 1: Cloud Concepts Overview
- Module 2: Cloud Economics and Billing
- Module 3: AWS Global Infrastructure Overview
- Module 4: AWS Cloud Security
- Module 5: Networking and Content Delivery
- Module 6: Compute
- Module 7: Storage
- Module 8: Databases
- Module 9: Cloud Architecture
- Module 10: Automatic Scaling and Monitoring

Booking Exam

https://www.aws.training/Certification

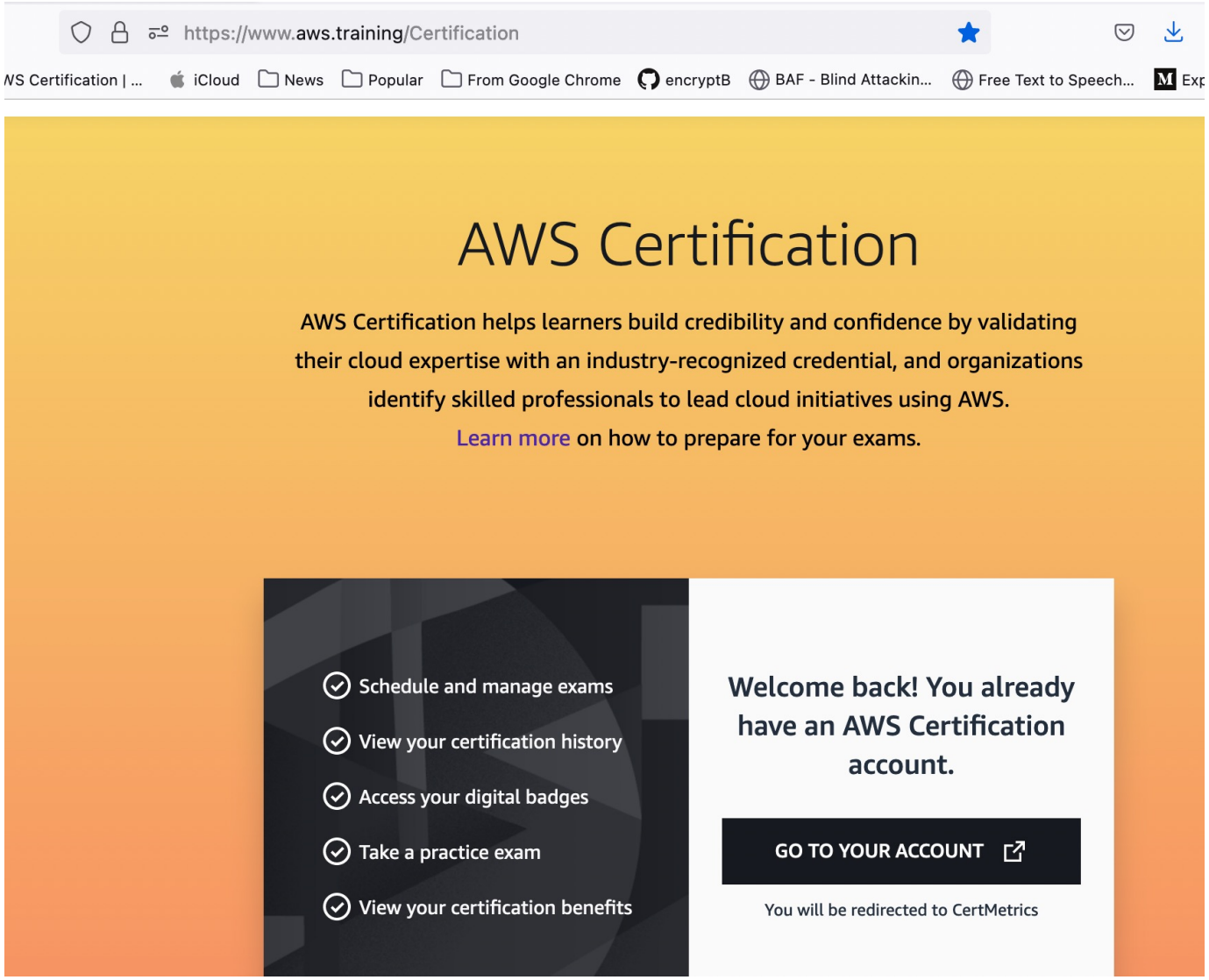
- 65 questions. 90 minutes.
- Next and Previous.
- Flag question.
- Opportunity to review the questions after last question.
- **Skill Builder's Course Catalog** and filter by Training Category for "Exam Preparation" *The Individual subscription starts at $29 USD per month and gives you access to all available resources*



Booking Exam

https://www.aws.training/Certification

- **Skill Builder's Course Catalog** and filter by Training Category for "Exam Preparation" *The Individual subscription starts at $29 USD per month and gives you access to all available resources.*
- Exam Cram.
- Books.
- https://aws.amazon.com/certification/certified-cloud-practitioner/



Exam

1.0 Cloud Concepts

- 1.1 Define the AWS Cloud and its value proposition
- 1.2 Identify aspects of AWS Cloud economics
- 1.3 Explain the different cloud architecture design principles

2.0 Security and Compliance

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

Exam

3.0 Technology

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

4.0 Billing and Pricing

- 4.1 Compare and contrast the various pricing models for AWS (for example, On-Demand Instances, Reserved Instances, and Spot Instance pricing)
- 4.2 Recognize the various account structures in relation to AWS billing and pricing
- 4.3 Identify resources available for billing support

Compute services –

- Amazon EC2
- AWS Lambda
- AWS Elastic Beanstalk
- Amazon EC2 Auto Scaling
- Amazon ECS
- Amazon EKS
- Amazon ECR
- AWS Fargate

Security, Identity, and Compliance services –

- AWS IAM
- Amazon Cognito
- AWS Shield
- AWS Artifact
- AWS KMS

Storage services –

- Amazon S3
- Amazon S3 Glacier
- Amazon EFS
- Amazon EBS

Database services –

- Amazon RDS
- Amazon DynamoDB
- Amazon Redshift
- Amazon Aurora

Networking and Content Delivery services –

- Amazon VPC
- Amazon Route 53
- Amazon CloudFront
- Elastic Load Balancing

Management and Governance services –

- AWS Trusted Advisor
- AWS CloudWatch
- AWS CloudTrail
- AWS Well-Architected Tool
- AWS Auto Scaling
- AWS Command Line Interface
- AWS Config
- AWS Management Console
- AWS Organizations

AWS Cost Management services –

- AWS Cost & Usage Report
- AWS Budgets
- AWS Cost Explorer

Module 1: Cloud Concepts Overview

AWS Academy Cloud Foundations

1. Cloud Fundamentals

- Pay as you go and no up-front costs. Infrastructure-as-a-service gives most control over IT.
- **Elastic Balancing** and **VPC** implements networking.
- Network ACLs, Security Groups and IAM implements security.
- Go global in minutes in a key advantage of using AWS.
- Economies with massive scale is a key advantage of using AWS.
- Trading **capital expense for variable expense** is a key advantage of using AWS.
- In AWS, networking is implemented with Elastic Balancing and VPC. In AWS, security is implemented with Network ACLs and IAM.
- Advantages of AWS include: **Go global in minutes**; Economies with massive scale; and Trade capital expense for variable expense.

1. Cloud Fundamentals

- Six advantages of cloud computing: Trade fixed expense for variable expense; Benefit from massive economies of scale; Stop guessing capacity; Increase speed and agility; Stop spending money running and maintaining data centers; and Go global in minutes.
- AWS Compute services include EC2, Lambda, Fargate and Elastic Beanstalk. AWS storage methods include S3, EFS and EBS. AWS services are configured with AWS Management Console; Command Line Interface; or Software Development Kit.
- Migrating from on-premise to the cloud eliminates **cost of data centre operations** and cost of physical service hardware.
- With AWS, we have the benefit for **increased business agility** by improving time to market.
- **Elasticity** – match demand to the provision.
- For application development, AWS reduces **upfront capital costs** and has **low variable expenses**, whilst having the ability to **scale-up in minutes**.
- Agility is the feature that **reduces time to deploy applications** from on-premise to the Cloud.
- In migration from on-premise to the Cloud, it is the customer's responsibility for application licences, and AWS's responsibility for the hardware infrastructure, the physical security and the power consumption of the AWS Cloud.

1. Cloud Fundamentals – Data Migration

AWS Storage Gateway

AWS Storage Gateway simplifies on-premises adoption of AWS Storage. Storage Gateway lets you seamlessly connect and extend your on-premises applications to AWS Storage. Customers use Storage Gateway to seamlessly replace tape libraries with cloud storage, provide cloud storage-backed file shares, or create a low-latency cache to access data in AWS for on-premises applications. The service provides three different types of gateways – File Gateway, Tape Gateway, and Volume Gateway.

- **File Gateway** file data is stored in Amazon S3 as durable objects using Amazon S3 File Gateway or in fully managed file shares using Amazon FSx File Gateway.
- **Tape Gateway** virtual tape library (VTL) configuration seamlessly integrates with your existing backup software for cost effective tape replacement in Amazon S3 and long term archival in S3 Glacier and S3 Glacier Deep Archive.
- **Volume Gateway** stores or caches block volumes locally, with point-in-time backups as EBS snapshots. These snapshots may be recovered in the cloud.

AWS Direct Connect

Customers select a Direct Connect dedicated physical connection to accelerate network transfers between their datacenters and AWS datacenters.

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This enables you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an **Amazon Virtual Private Cloud (VPC)** using private IP space, while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.

Explore our **AWS Direct Connect Partner Bundles** that help extend on-premises technologies to the cloud.

AWS DataSync

AWS DataSync is a data transfer service that makes it easy for you to automate moving data between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon EFS), or Amazon FSx for Windows File Server. DataSync automatically handles many of the tasks related to data transfers that can slow down migrations or burden your IT operations, including running your own instances, handling encryption, managing scripts, network optimization, and data integrity validation. You can use DataSync to transfer data at speeds up to 10 times faster than open-source tools. You can use DataSync to copy data over AWS Direct Connect or internet links to AWS for one-time data migrations, recurring data processing workflows, and automated replication for data protection and recovery.

AWS Transfer Family

The **AWS Transfer Family** provides fully managed support for file transfers directly into and out of Amazon S3. With support for Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS), and File Transfer Protocol (FTP), the AWS Transfer Family helps you seamlessly migrate your file transfer workflows to AWS by integrating with existing authentication systems, and providing DNS routing with Amazon Route 53 so nothing changes for your customers and partners, or their applications. With your data in Amazon S3, you can use it with AWS services for processing, analytics, machine learning, and archiving. Getting started with the AWS Transfer Family is easy; there is no infrastructure to buy and set up.

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration makes public internet transfers to Amazon S3 faster. You can maximize your available bandwidth regardless of distance or varying internet weather, and there are no special clients or proprietary network protocols. Simply change the endpoint you use with your S3 bucket and acceleration is automatically applied.

This is ideal for recurring jobs that travel across the globe, such as media uploads, backups, and local data processing tasks that are regularly sent to a central location.

AWS Snowcone

AWS Snowcone is the smallest member of the AWS Snow Family of edge computing and data transfer devices. Snowcone is portable, rugged, and secure.

Amazon Kinesis Data Firehose

Amazon Kinesis Data Firehose is the easiest way to load streaming data into AWS. It can capture and automatically load streaming data into Amazon S3

APN Partner Products

AWS has partnered with a number of **industry vendors** on physical gateway appliances that bridge the gap between traditional backup and cloud. Link

Module 2: Cloud Economics and Billing

AWS Academy Cloud Foundations

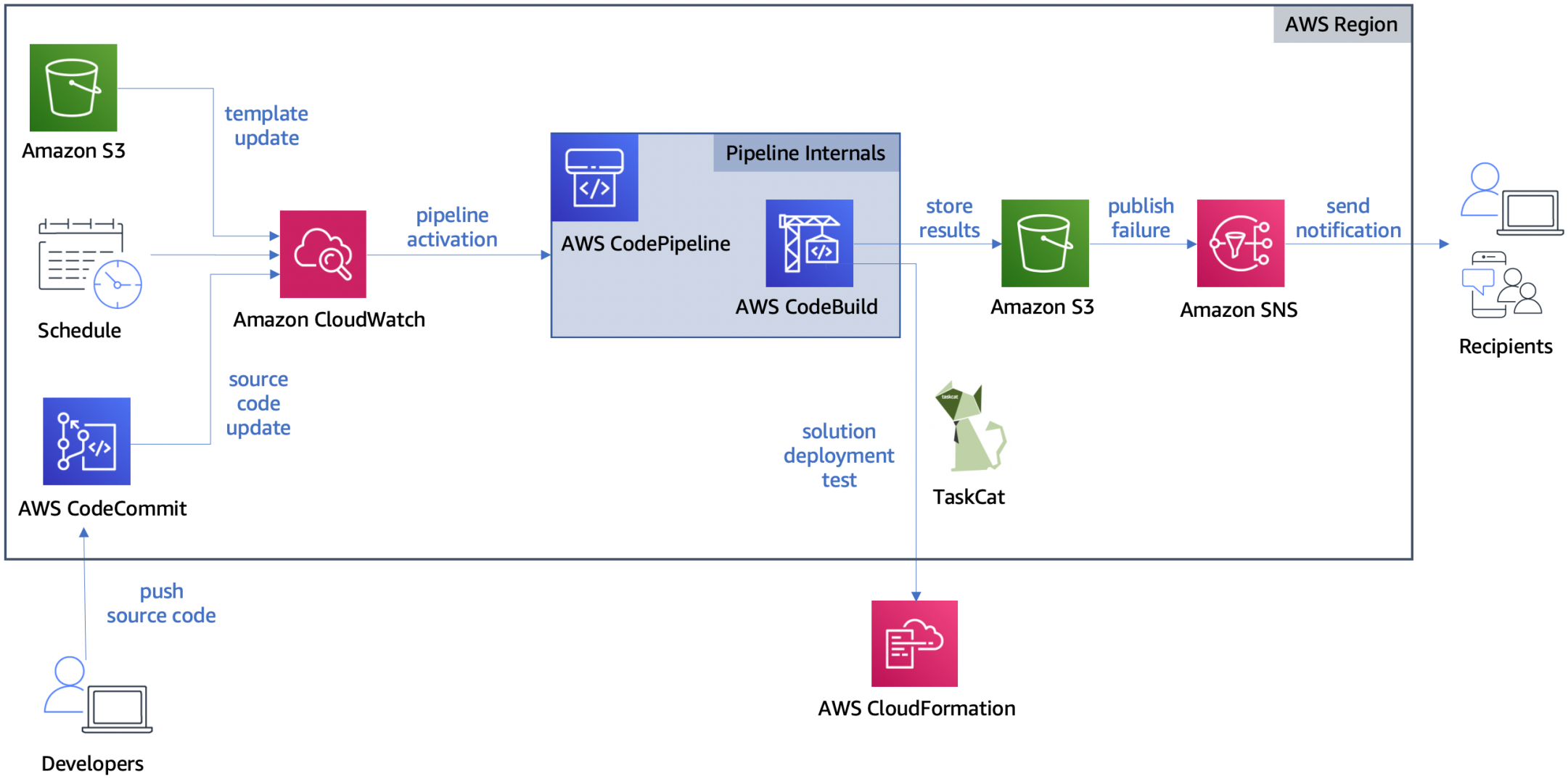
2 Billing

- To save money, turn off resources and you don't pay for them (apart from storage).
- You **pay per hour** or second dependent on the instance type.
- You **pay no upfront costs**.
- You do not pay termination costs for terminating an instance.
- Fundamental cost drivers: Compute, storage and data transfer.
- No charge for incoming data transfer/between services in same region.
- Data transfer is aggregated across services, and charged as a single amount.
- To save money, **reserve resources** in advance.
- Most savings for EC2 instances is for **All Upfront Reserved Instance** (AURI). 1 or 3 year.
- Free tier EC2 instances are free new customers for up to 1 year.
- Amazon VPC, Elastic Beanstalk, Auto Scaling, AWS CloudFormation, and AWS Identity and Access Management (IAM) are all free to use.
- **AWS Organisation** is a free account management service that mergers accounts into one.

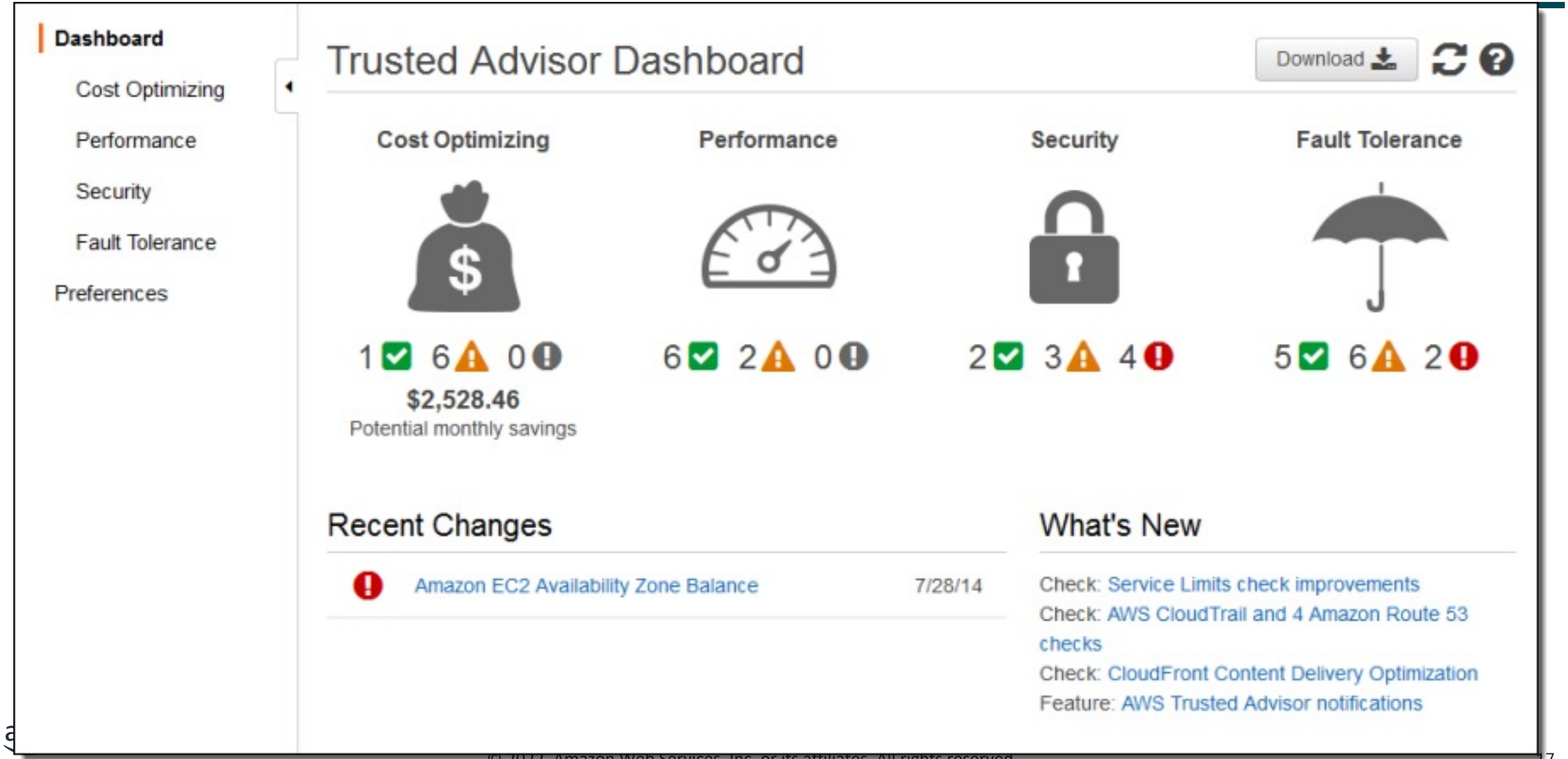
2 Billing

- The **AWS Pricing Calculator** allows for an estimate of the cost of planned resources for services (network, compute, storage and database) [here]. See Figure 9.
- **Consolidating billing** for organisations with multiple AWS accounts allows them to reach volume discount thresholds soon (including for reserved instances or saving plan discounts).
- **Economies of scale** is a key feature for AWS for lower variable costs in relation to high purchase volumes.
- The **AWS Concierge Support team** can support help around billing and how to implement best practices around billing.
- Advantages of consolidated billing are: One bill; Easy tracking; Combined usage; and No extra fee. [here]
- **AWS Trusted Advisor** provides information on cost optimization, performance, security, fault tolerance and service limits. It shows the regions that have the lowest cost (Figure 5). It can provide alerts when there is an impact on a company's resources. It defines best practices and can save money, enhance security and improve performance [here].
- **Trusted Advisor** gives advice on Amazon EBS Public Snapshots; Amazon RDS Public Snapshots; Amazon S3 Bucket Permissions; IAM Use; MFA on Root Account; and Security Groups – Specific Ports Unrestricted. [here]
- **AWS CloudTrail** enables the auditing of **user activity** and API calls [here]. See Figure 6.
- **AWS CloudFormation** supports the **templating** of the reliable provision, management and updating of AWS Cloud infrastructures (Figure 7).
- **AWS Organizations** allows you to integrate multiple AWS accounts into a single bill (Figure 8).
- AWS Organizations supports supports the removal of **unwanted accounts** and **underutilized resources** across a range of accounts.

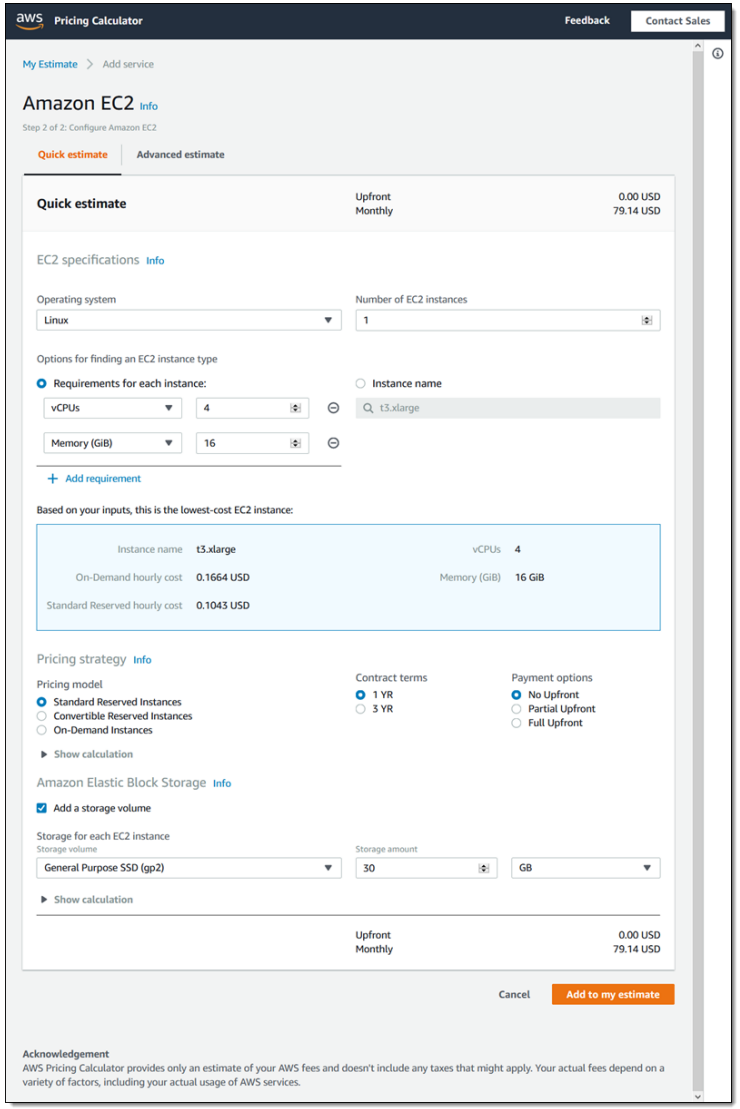
CloudFormation

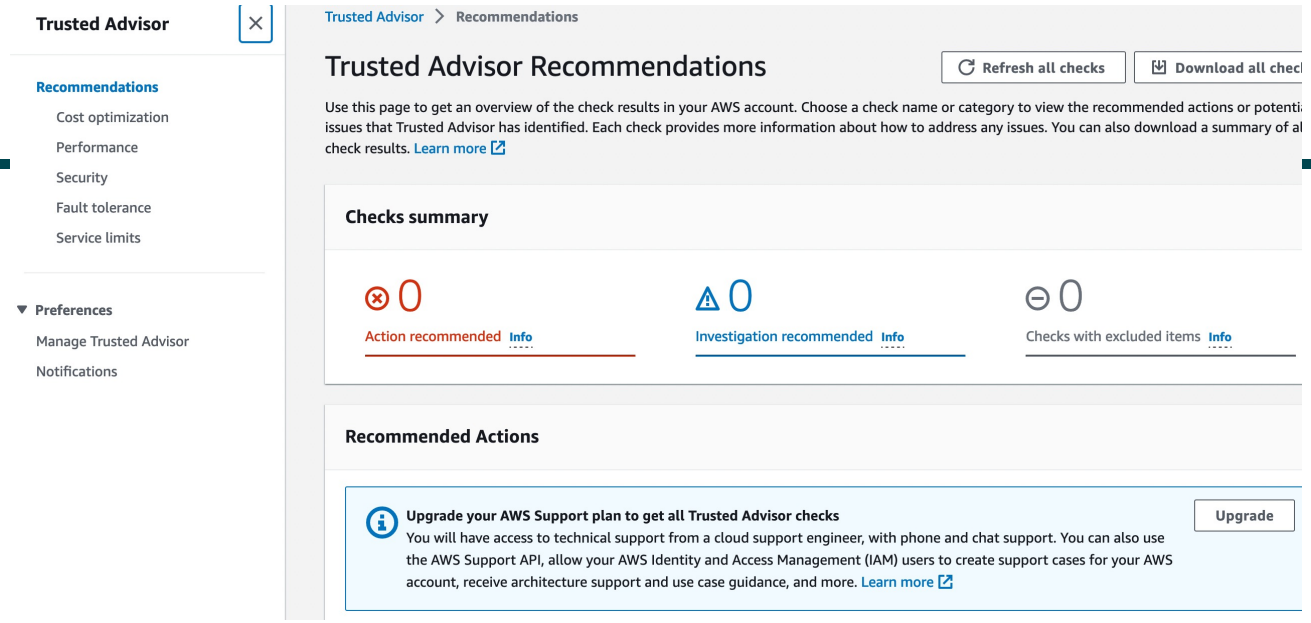


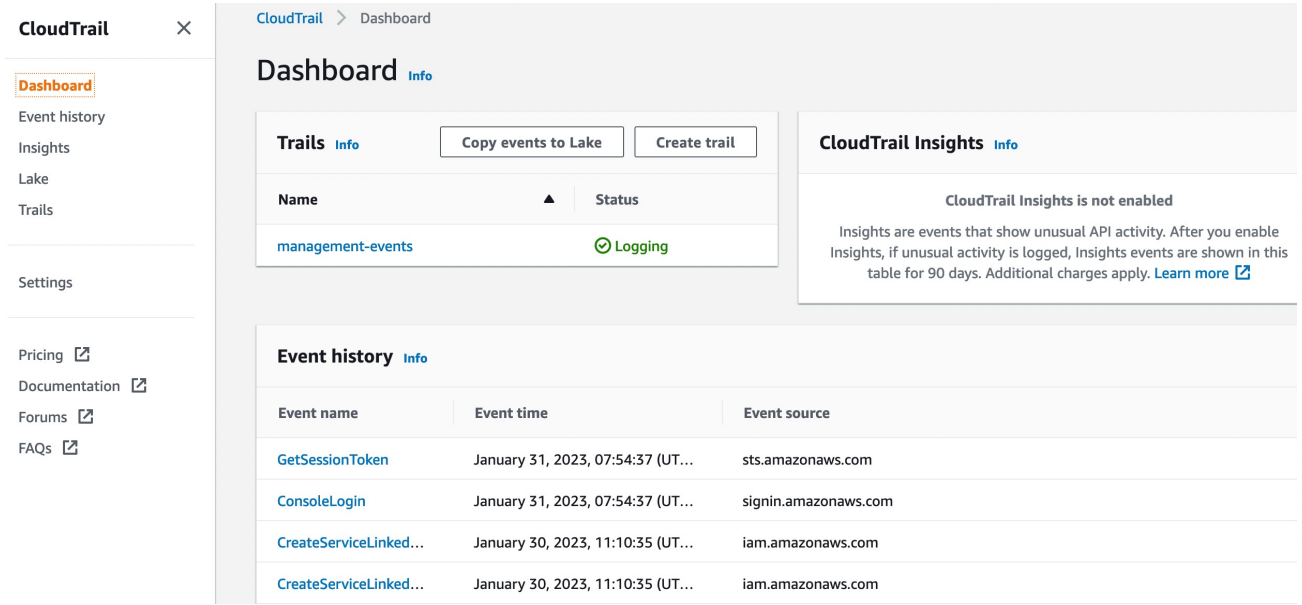
Trusted Advisor



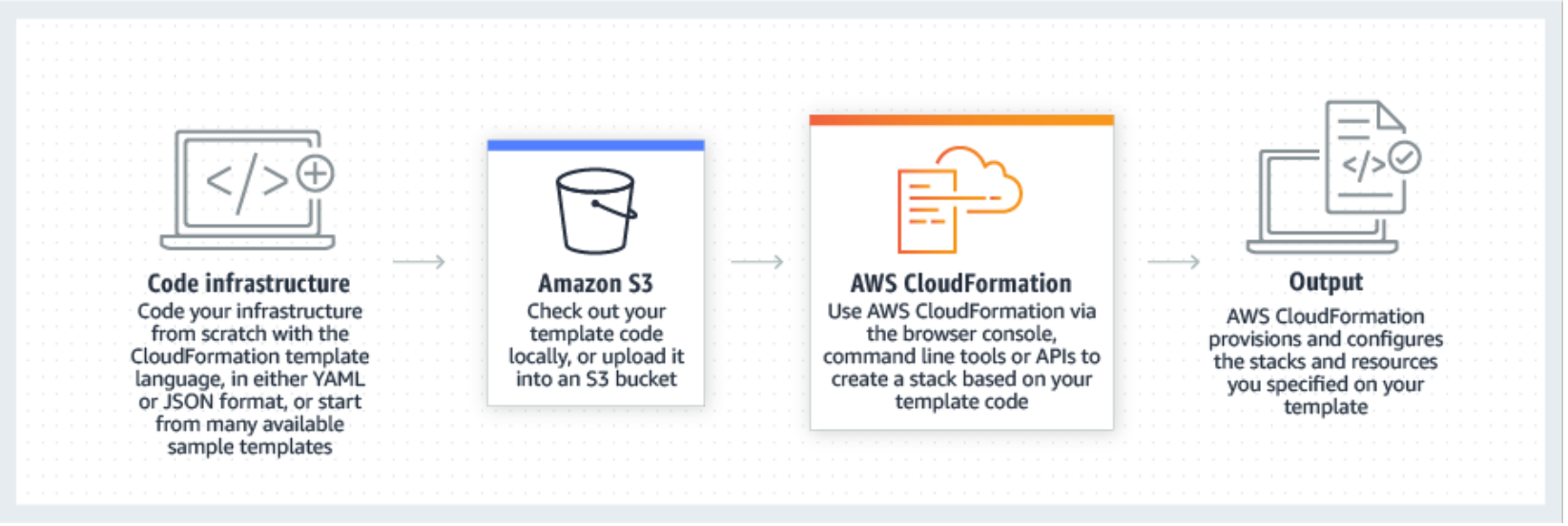
2 Billing

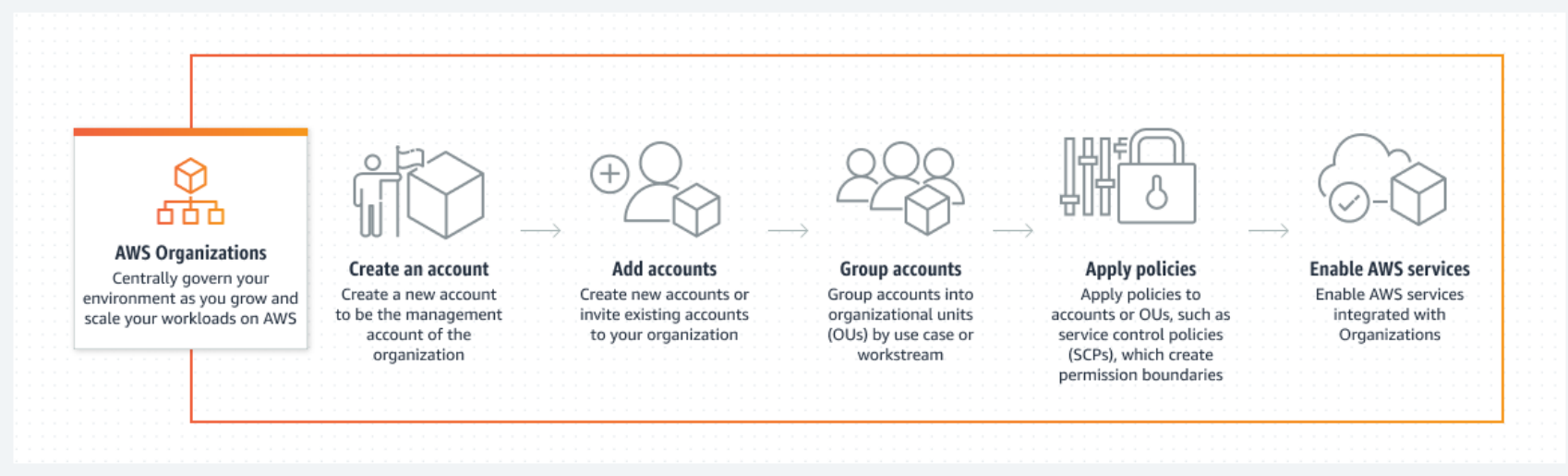




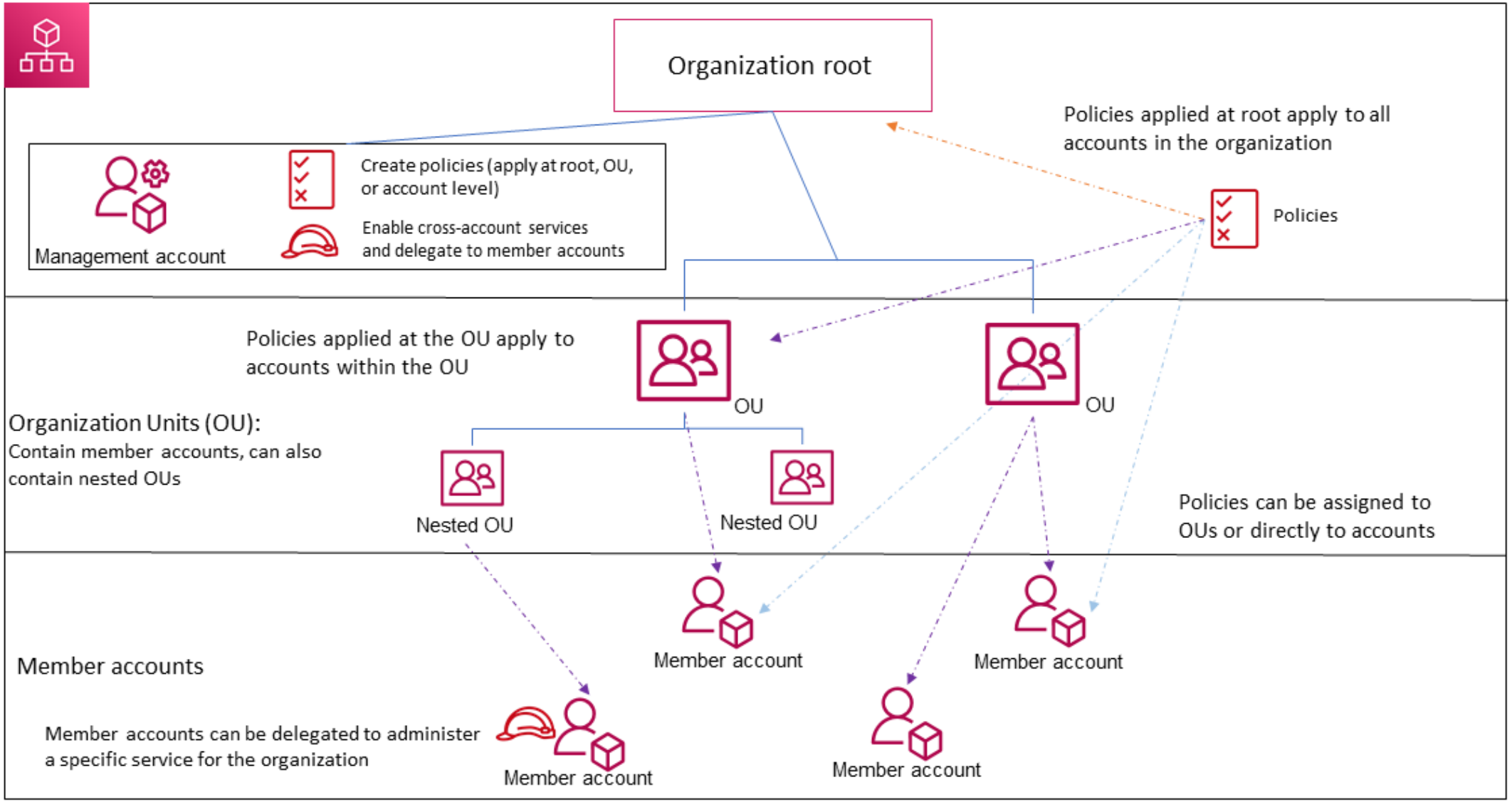


2 Billing





AWS Organisations



Module 3: AWS Global Infrastructure Overview

AWS Academy Cloud Foundations

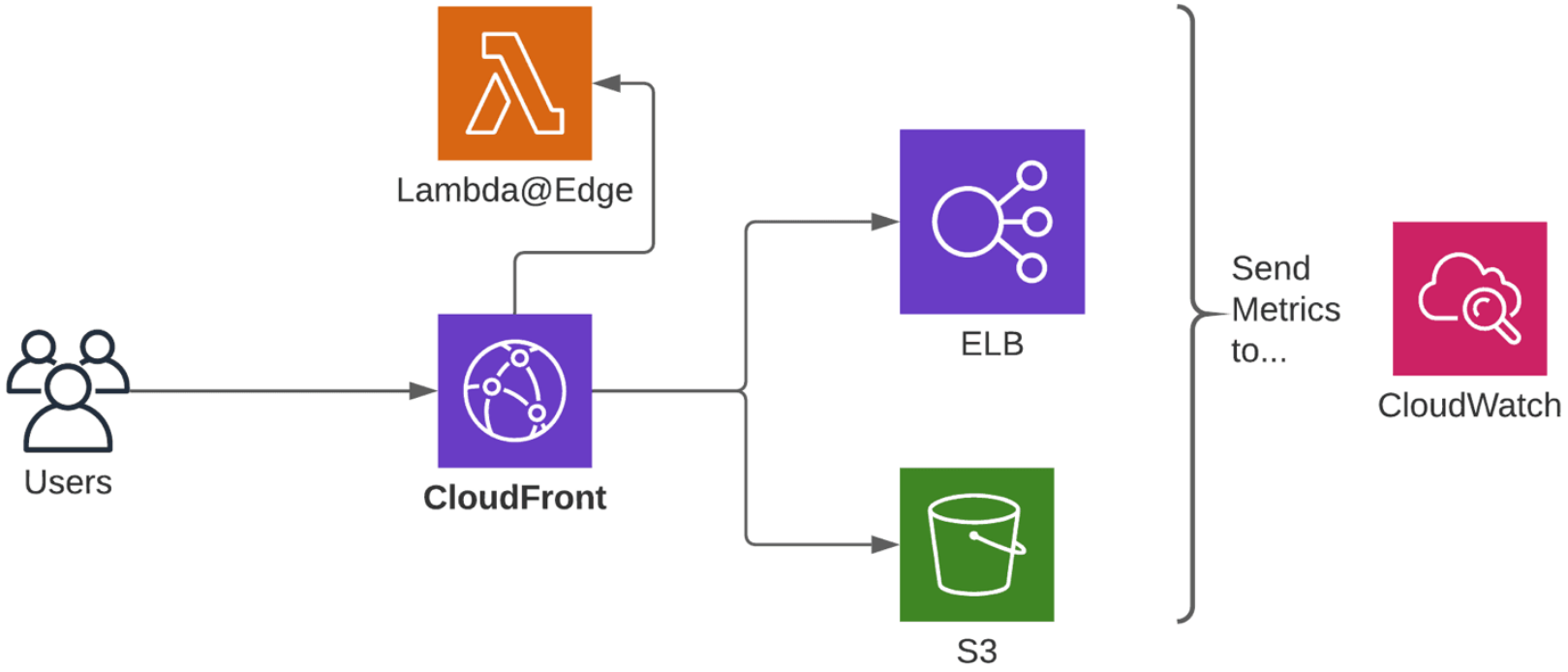
3. Global

- In AWS, AWS CloudFront is a content delivery network (CDN) used to distribute content to end users to reduce latency.
- Regions are isolated from one another and are not automatically replicated. Decision on selecting a region in AWS: Services available within the Region; Proximity to customers (latency); Costs (vary by Region); and Data governance, legal requirements
- If we have a region of eu-west-1, eu-west-1a is an **Availability Zone** contained in the region.
- For AWS to mitigate against environmental risks: Data centers have a redundant design; Critical system components are backed up across multiple Availability Zone; Data center locations are not disclosed; and On failure, automated processes move data traffic away from the affected area. For AWS, which are used for content with infrequent access regional edge caches.
- For AWS, Route 53 provides a DNS (Domain Name System) service.
- For AWS, **Points of presence** are located in most of the major cities of the world. For AWS, features of the AWS Global Infrastructure: The infrastructure is fault tolerant; It is elastic and scalable.
- For AWS storage, Amazon **Elastic Block Store** (Amazon EBS) is the high-performance block storage that is designed for use with Amazon EC2 for both throughput and transaction-intensive workloads.
- For AWS storage, Amazon **Elastic File System** (Amazon EFS) is a scalable, fully managed elastic Network File System (NFS) file system for use with AWS Cloud services and on-premises resources.
- For AWS storage, Amazon **Simple Storage Service Glacier** is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup.

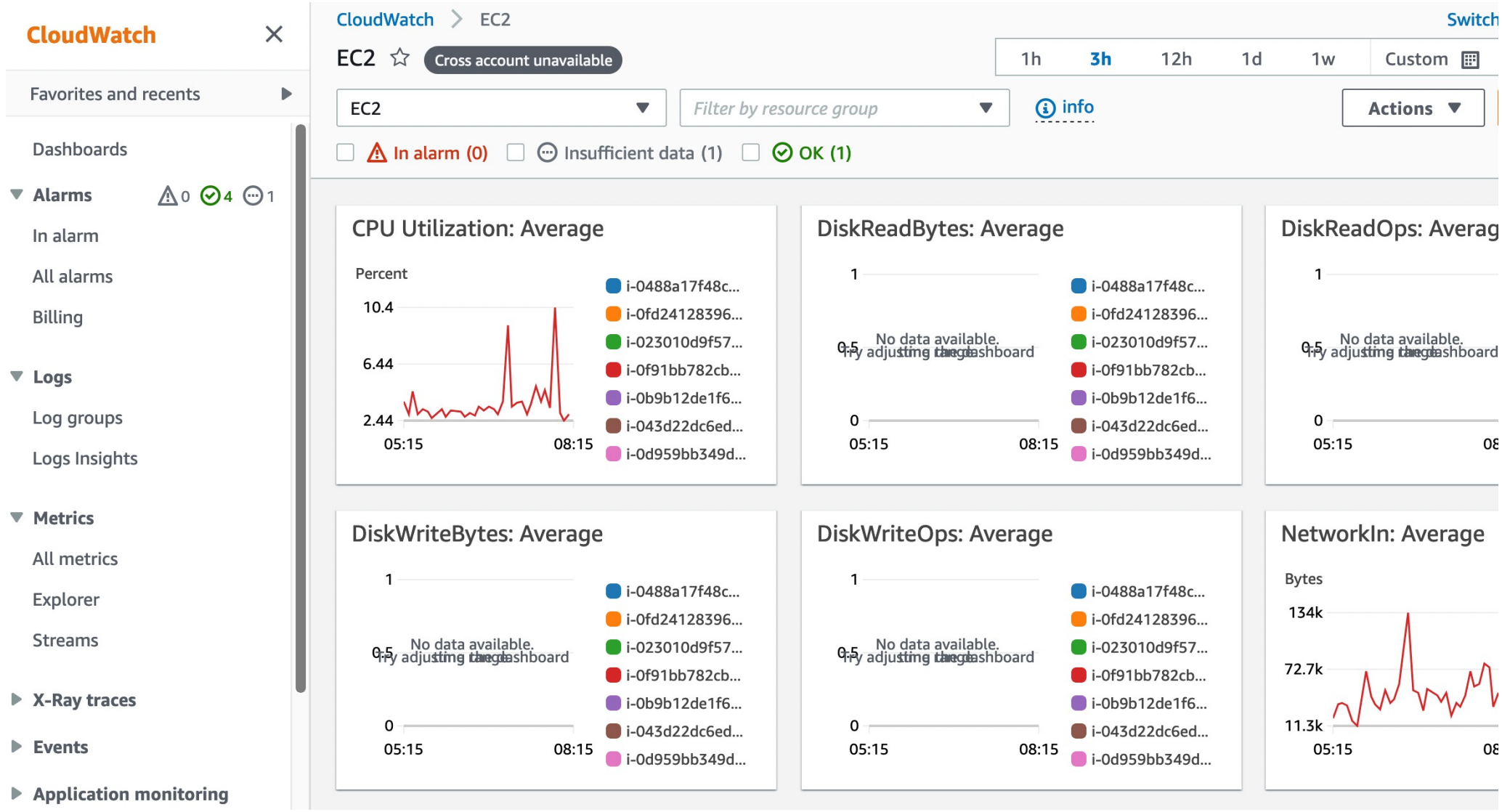
3. Global

- For AWS compute, AWS **Lambda** runs code without provisioning or managing servers. You pay only for the compute time that you consume.
- For AWS database services, Amazon **Relational Database Service** (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud.
- For AWS database services, Amazon **Relational Database Service** (Amazon RDS) is a MySQL and PostgreSQL-compatible relational database.
- For AWS database services, Amazon **Redshift** enables you to run analytic queries against petabytes of data that is stored locally in Amazon Redshift, and directly against exabytes of data that are stored in Amazon S3.
- For AWS database services, Amazon **DynamoDB** is a key-value and document database that delivers single-digit millisecond performance at any scale, with built-in security, backup and restores, and in-memory caching.
- For AWS networking services, Amazon **Virtual Private Cloud** (Amazon VPC) enables you to provision logically isolated sections of the AWS Cloud.
- For AWS networking services, **Elastic Load Balancing** automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.
- For AWS networking services, Amazon **CloudFront** is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and application programming interfaces (APIs) to customers globally, with low latency and high transfer speeds.
- For AWS networking services, AWS **Transit Gateway** is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.

CloudFront With CloudWatch



CloudWatch



3. Global

- For AWS compute, Amazon **Elastic Compute Cloud** (Amazon EC2) provides resizable compute capacity as virtual machines in the cloud.
- For AWS compute, Amazon **Elastic Container Service** (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers.
- For AWS compute, Amazon **Elastic Container Registry** (Amazon ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images.
- For AWS compute, AWS **Elastic beanstalk** is a service for deploying and scaling web applications and services on familiar servers such as Apache and Microsoft Internet Information Services (IIS).

Module 4: AWS Cloud Security

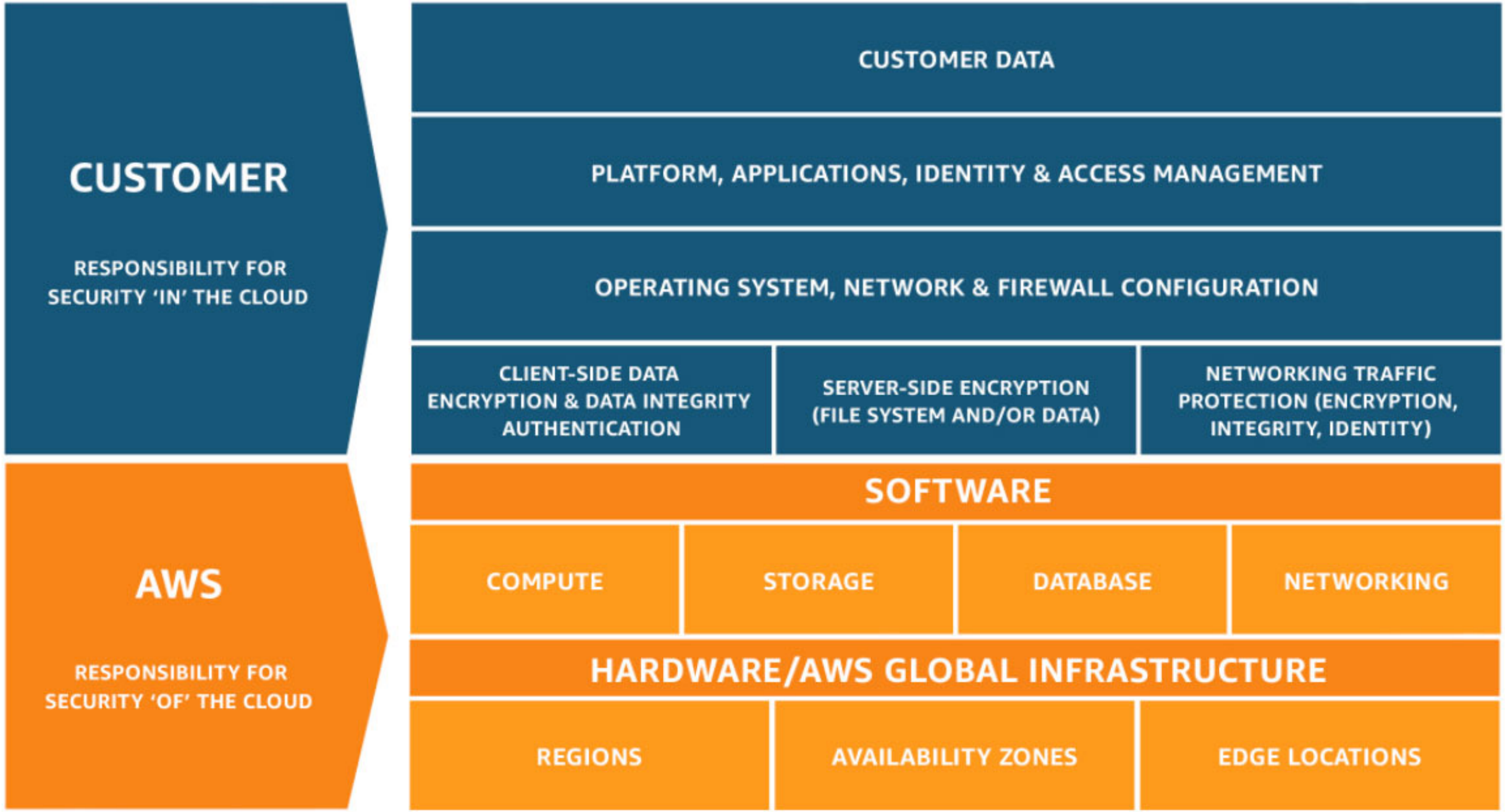
AWS Academy Cloud Foundations

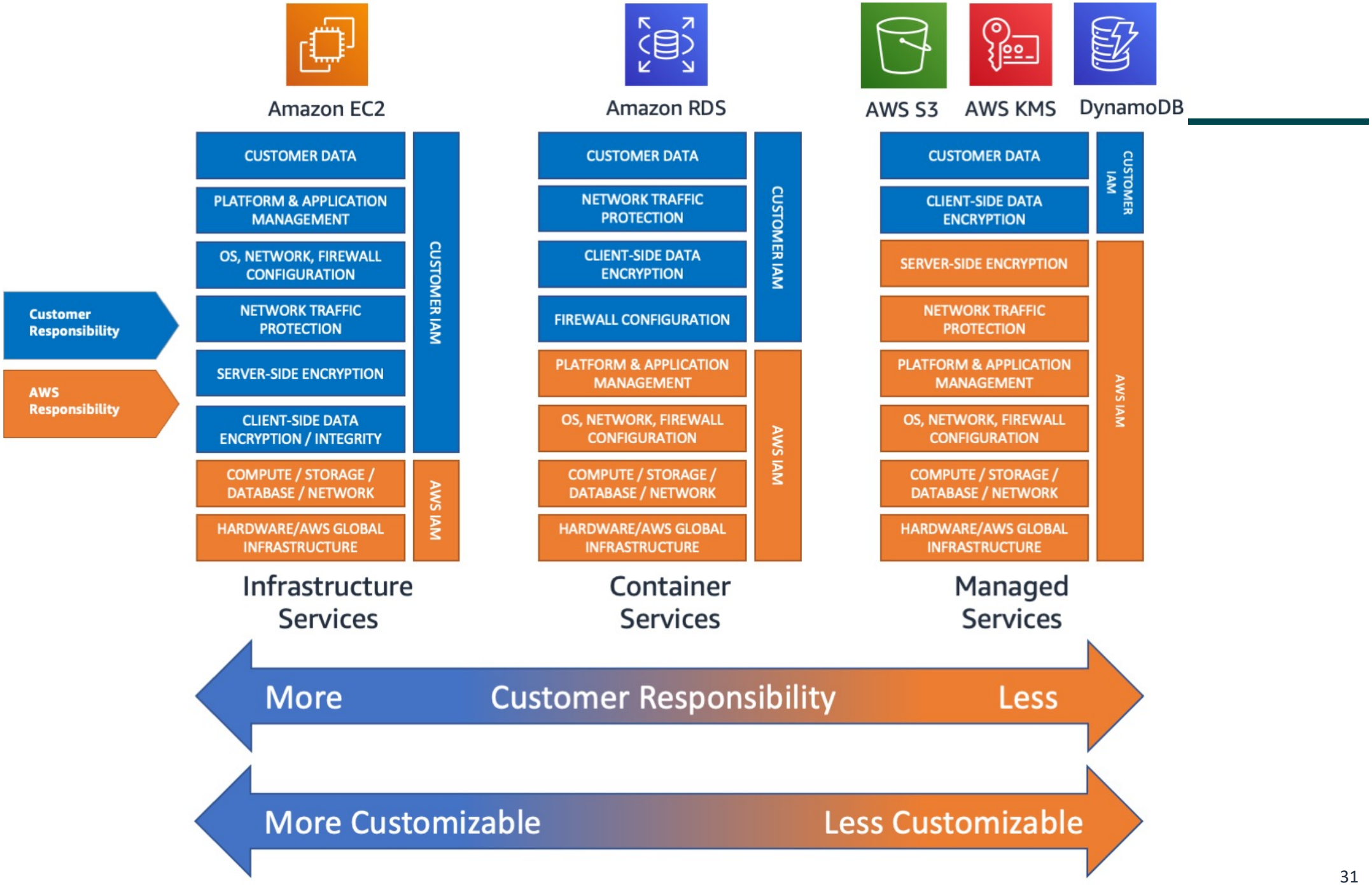
4. Security/Shared-Responsibility

- For security, AWS is responsible for client-side encryption and physical security for Availability Zones (see Figure 10).
- For security, the customer is responsible for server-side encryption and operating system, network and firewall configuration (see Figure 10).
- For security, the customer is responsible for **EC2 operating system patching** and API access control to AWS resources.
- For an application with a load balancer, EC2 instances and an Amazon RDS database, AWS is responsible for protecting against spoofing and packet sniffing, and also for installing the latest security patches on the RDS instance.
- It is the customer's responsibility to configure their infrastructure, and AWS's responsibility to protect the physical cloud infrastructure.
- The customer is always responsible for their own data.
- AWS and Customer **share responsibility** for Patch Management; Configuration Management and Awareness & Training.
- **AWS KMS** (Key Management Service) enhances security with encryption of data.
- With the **AWS Root Account user access keys** you can use them for access, but they should not be shared with anyone. This account should not be used for normal accesses [here].

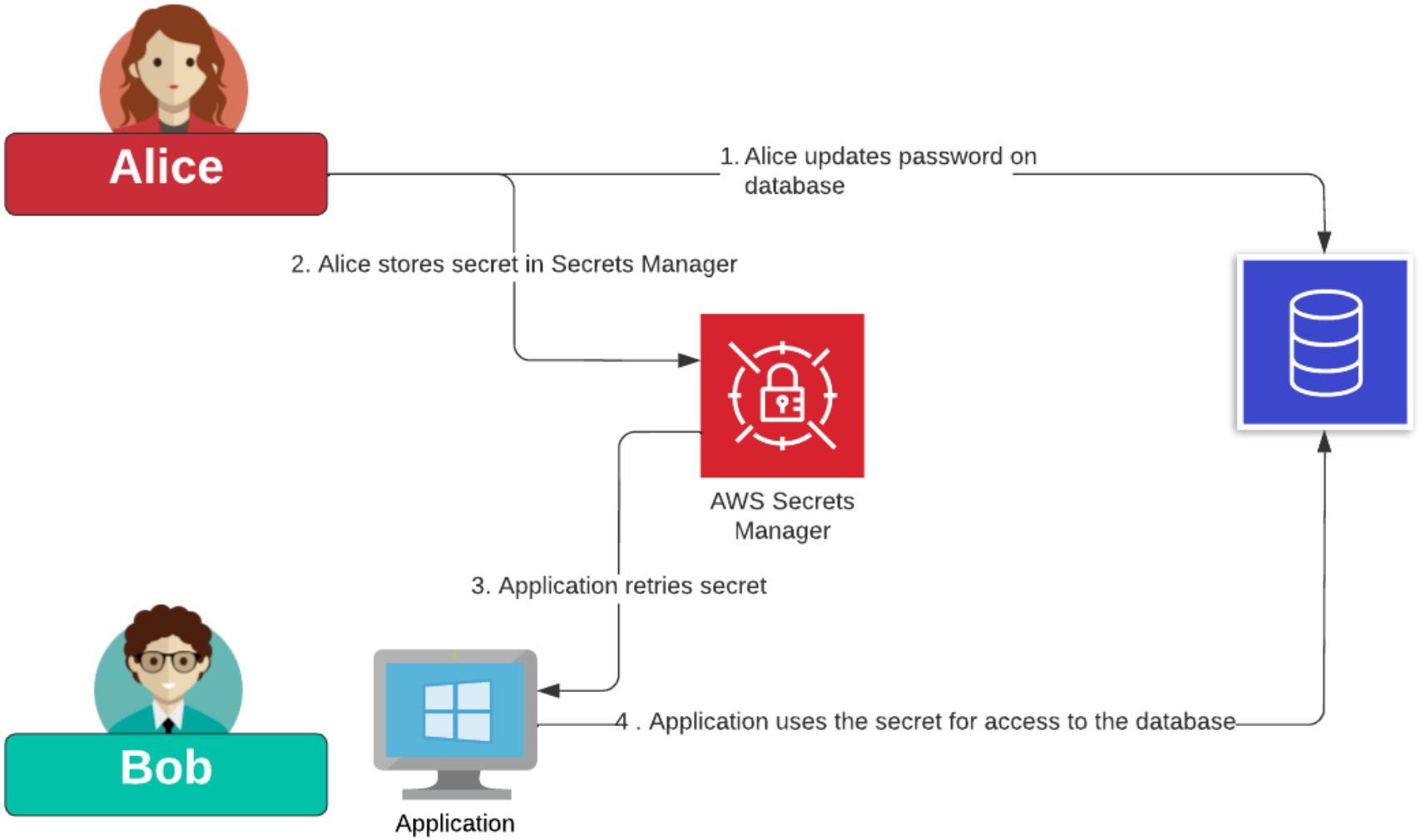
4. Security/IAM/Shared-Responsibility

- Best practices for **AWS IAM** (Identity and Access Management) are: rotation of credentials on a regular basis; the enablement of MFA (multi-factor authentication); regularly reviewing and removing unused users/roles/permissions/ policies and credentials; and least-privilege permissions. If there is an AWS account root user, delete it [here].
- **AWS Secrets Manager** supports the rotation of database credentials in AWS.
- **Amazon Detective** allows for the analysis, investigation and identification of security events and suspicious activates related to an AWS account (Figure 3).
- The **IAM Credential report** provides account details, such as passwords, access key and MFA devices (Figure 4).
- The **IAM** service can be used to grant permissions to applications that run within EC2 instances.
- **AWS Artifact** supports security validation and compliance verification for the AWS infrastructure and services. It generates reports which can be used by auditors and for compliance with local regulatory standards [here].
- An application in an EC2 instance uses configuration files stored in S3 buckets. We can enable an IAM role to setup the required permissions for access to the buckets.

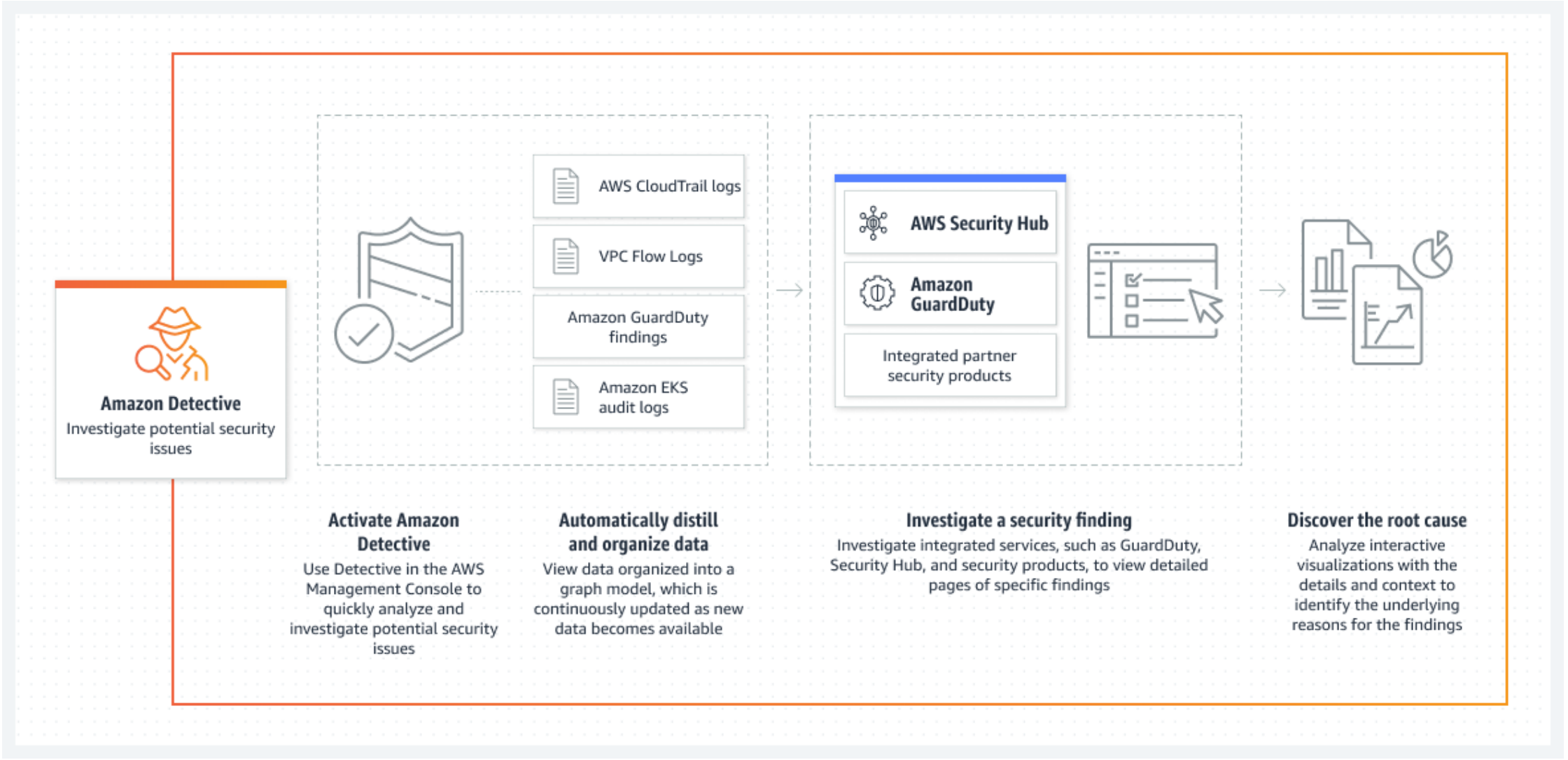

CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS


Amazon EC2
Amazon RDS
AWS S3
AWS KMS
DynamoDB
Customer Responsibility
AWS Responsibility
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
NETWORK TRAFFIC PROTECTION
SERVER-SIDE ENCRYPTION
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
NETWORK TRAFFIC PROTECTION
CLIENT-SIDE DATA ENCRYPTION
FIREWALL CONFIGURATION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
CLIENT-SIDE DATA ENCRYPTION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Infrastructure Services
Container Services
Managed Services
More
Customer Responsibility
Less
More Customizable
Less Customizable

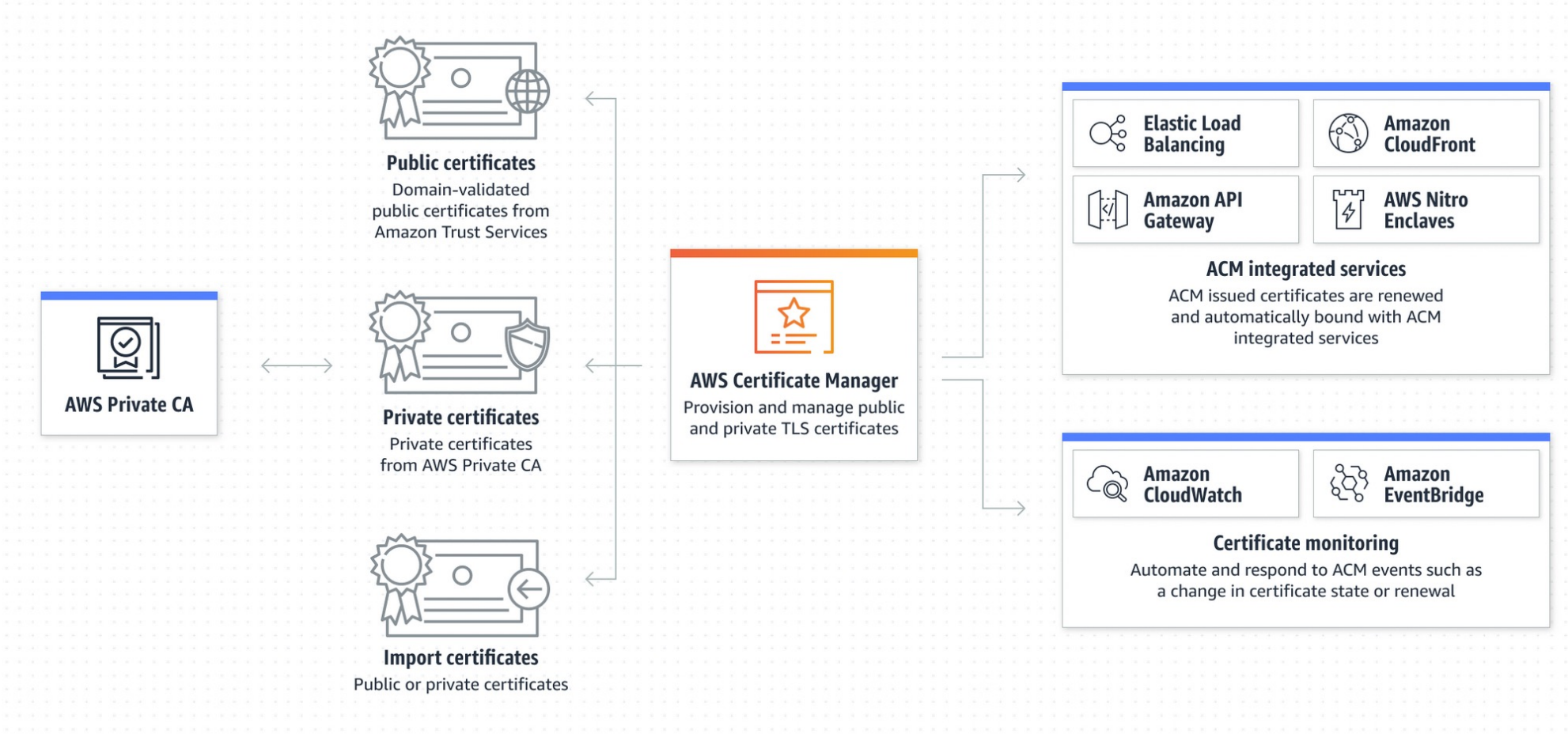
Secrets Manager



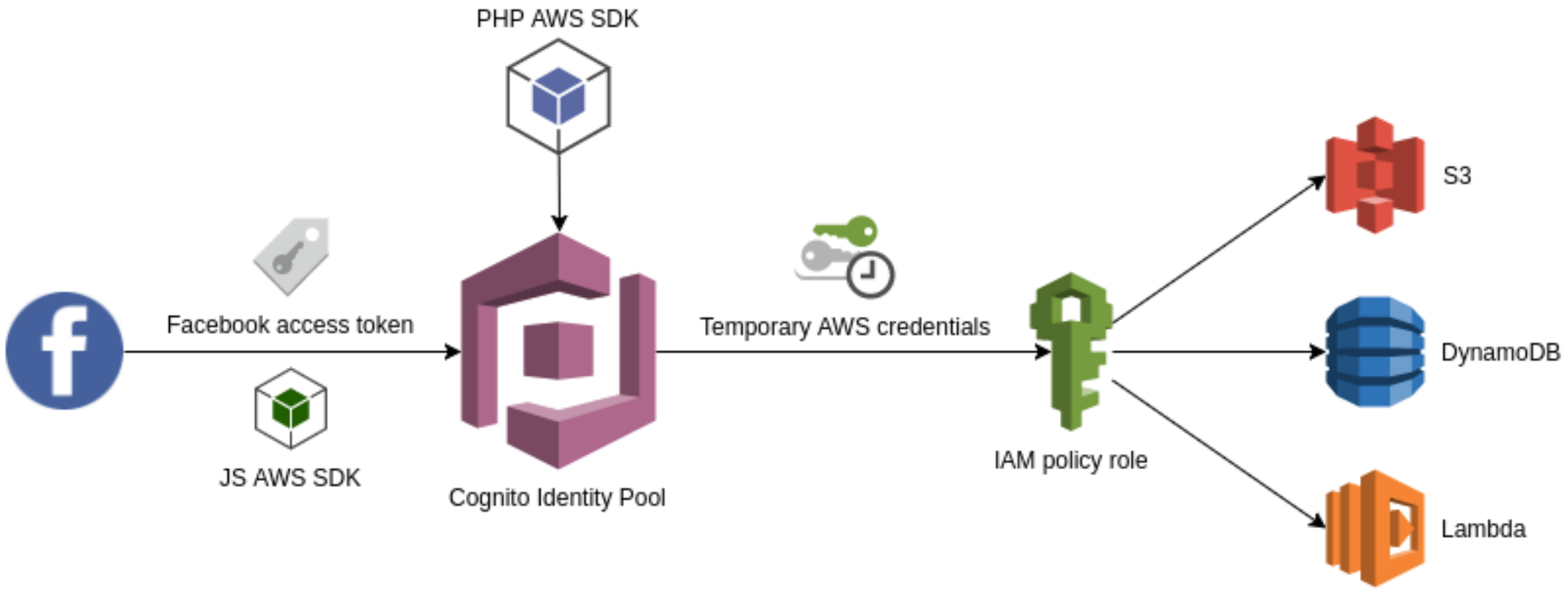
Amazon Detective



AWS Certificate Manager



AWS Cognito

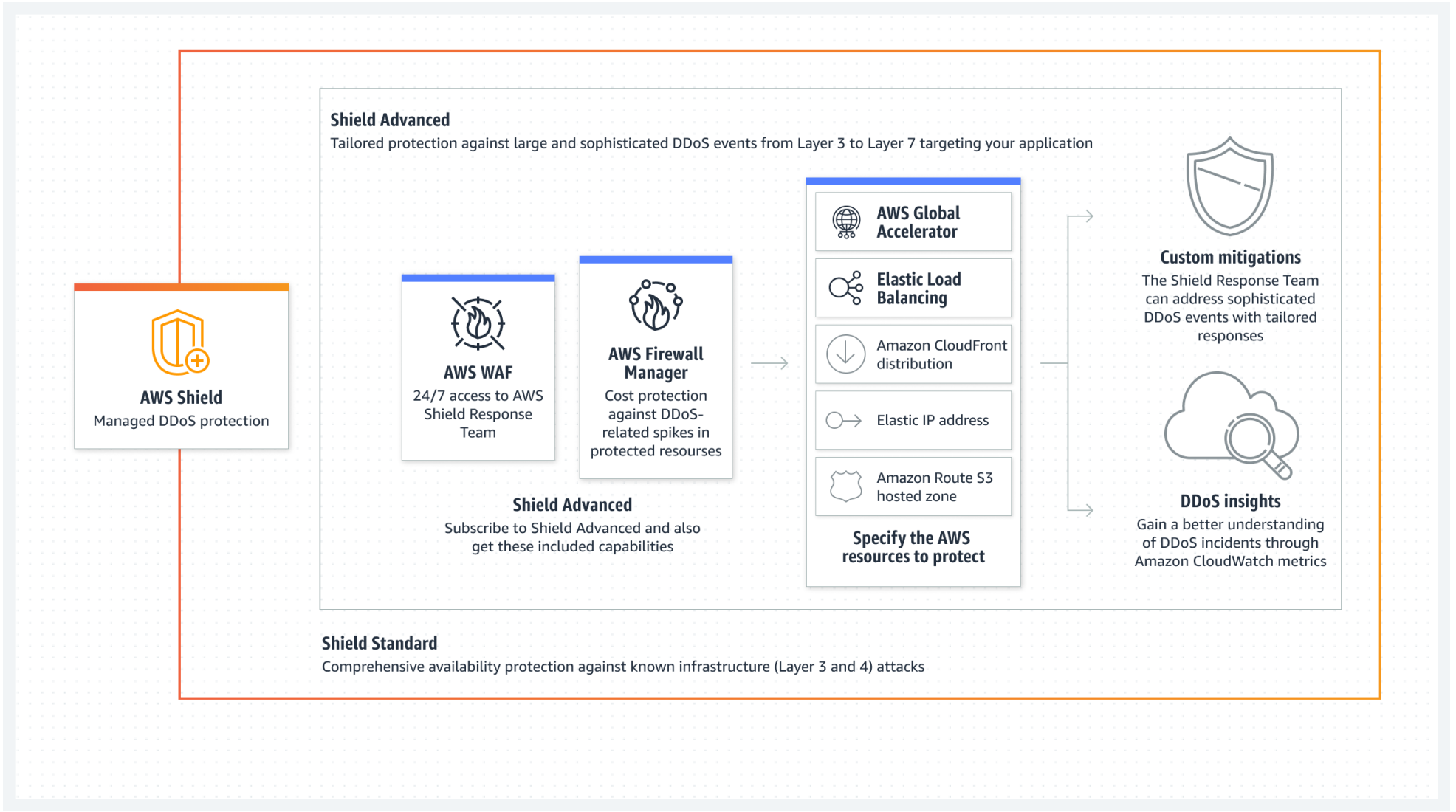


4. Security/IAM/Shared-Responsibility

- **AWS Certificate Manager** (ACM) supports the provisioning and management SSL/TLS certificates with AWS services and connected resources [here]
- **Amazon GuardDuty** monitors and analyzes data sources for malicious activity, such as for AWS CloudTrail data events. It can also analyse Amazon S3 logs, DNS logs, Amazon EBS volume data, and RDS login activity [here].
- **WAF** (Web Application Firewall) filters incoming traffic, and can protect for a range of threats.
- Best practice for access to AWS Management console is to **Enable multi-factor authentication** (MFA) and implement a **strong password policy**.

AWS GuardDuty and AWS WAF

AWS Shield – DDoS Protection

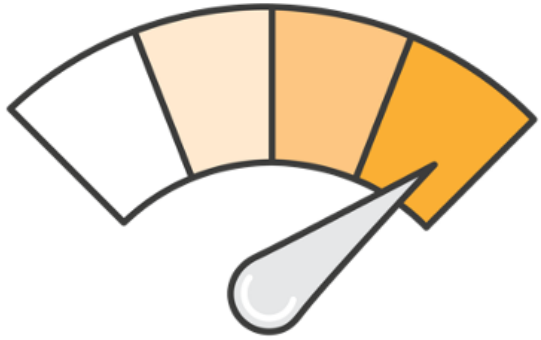


AWS Artifact

Support plans

Support plans

AWS Support offers four support plans:



- **Basic Support** – Resource Center access, Service Health Dashboard, product FAQs, discussion forums, and support for health checks
- **Developer Support**: Support for early development on AWS
- **Business Support**: Customers that run production workloads
- **Enterprise Support**: Customers that run business and mission-critical workloads

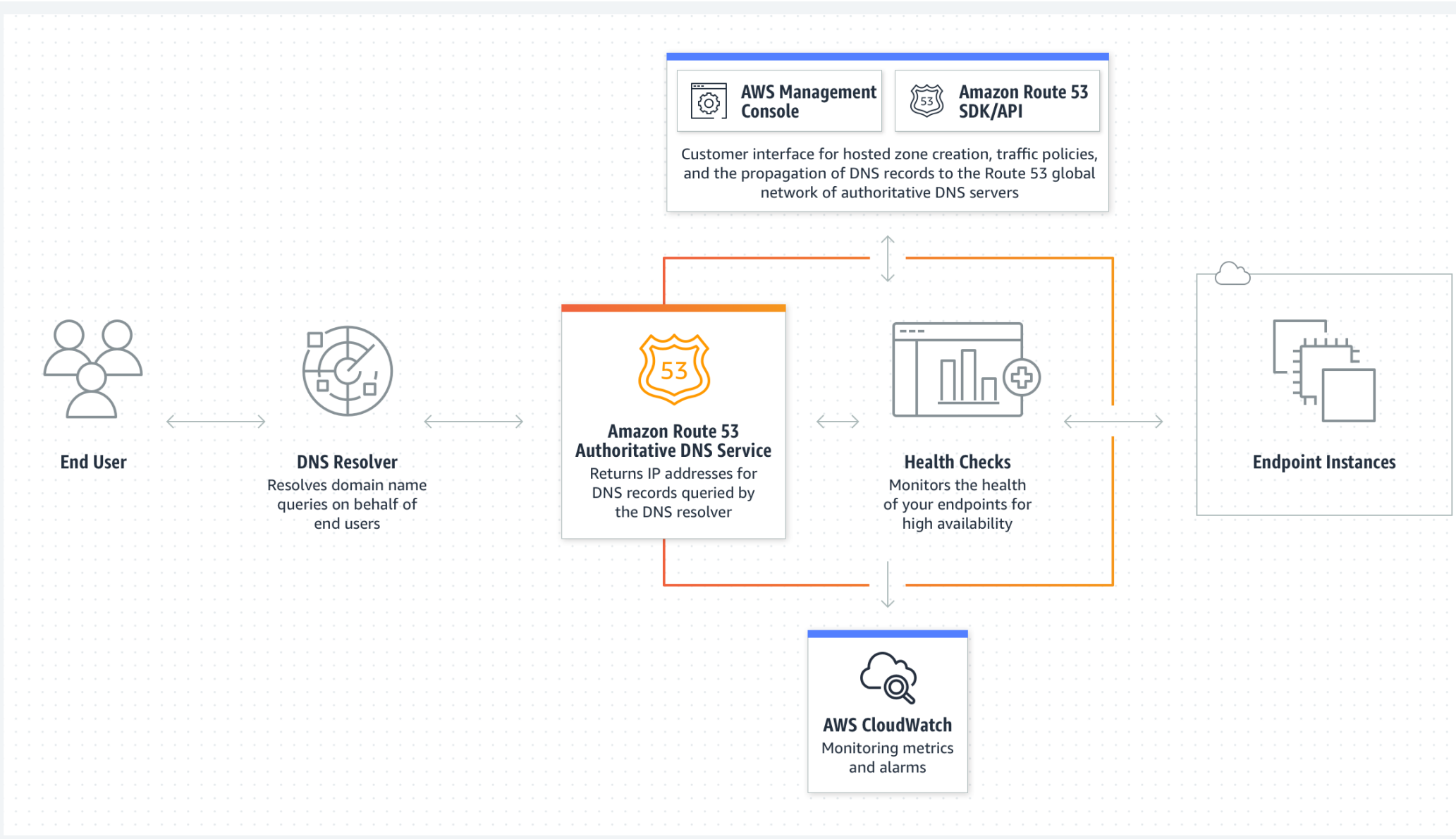
Module 5: Networking and Content Delivery

AWS Academy Cloud Foundations

5. Networking and Content Delivery

- A **VPC** (Virtual Private Cloud) isolates virtual networks in order to connect AWS resources and services [here].
- **Amazon Route 53** supports **DNS failover**, and can detect a Web site outage, and redirect users to a working Web site [here].
- An **Availability Zone** consists of one or more isolated data centres that are contained within a defined region, and which have low latency connections.
- We can create an isolated environment for enhanced security using **separate VPCs** to host resources. This creates separate subnets.
- An **AWS VPN** can be used to create an encrypted tunnel between the AWS infrastructure and a remote connection.
- An **AWS Local Zone** extends an AWS Region and provides more granular locations. The allow for low-latency applications that are closer to end users and on-premises infrastructures [here].
- An **AWS Region** provides a physical location in the world in which there is clustering of data centers.
- Network ACLs and Security groups define security between subnets.

Route 53


AWS Management Console
Amazon Route 53 SDK/API
Customer interface for hosted zone creation, traffic policies, and the propagation of DNS records to the Route 53 global network of authoritative DNS servers
End User
DNS Resolver
Resolves domain name queries on behalf of end users
Amazon Route 53 Authoritative DNS Service
Returns IP addresses for DNS records queried by the DNS resolver
Health Checks
Monitors the health of your endpoints for high availability
Endpoint Instances
AWS CloudWatch
Monitoring metrics and alarms

Module 6: Compute

AWS Academy Cloud Foundations

6. Compute

- The **elasticity** feature which has key benefits to eliminate underutilized CPU capacity, and to connect multiple regions for low-latency and high throughputs, and for redundancy.
- **elasticity** allows for the right size of resources when required by the demand, and release when no longer needed. Also, the ability to quickly gain access to resources and scale them.
- For **EC2 auto-scaling**, we scale the number of instances in or out in an automated manner, and based on the current demand.
- **Spot instances** are cost-effective and can be used if an application can be interrupted and is often used over short time periods. AWS will remove the spot instance when the capacity is no longer available [here]. Good for stateless.
- **On-demand instances** are cost-effective and are where the customer defines how the instance will be interrupted (stopped, hibernated or terminated) [here].
- Two key features of a serverless approach is: **built-in fault tolerance** and **that the application can scale, on-demand**.
- Amazon EC2 **Auto Scaling** allows for a steady and predictable performance for EC2 instances (and with a low cost) [here].
- If an instance needs licences that need require to be brought to AWS, and has the physical licencing of cores, we can launch a **dedicated host** [here].

6. Compute

- If a company just need to run a data processing for a few hours each week, **AWS Lambda** is often a good choice over Amazon EC2. [here].
- A Web site that runs continuously and cannot be interrupted. The most cost-effective option is to use **reserved instances** and a **savings plan** [Reserved Instances][Saving plans]. With savings plans we can reserve for 1 or 3 years.
- Amazon **Lightsail** [here] launches and manages a virtual private server, and AWS **Batch** supports the running of match batch files [here].
- **On-Demand Instances**: Pay by the hour and no long-term commitments.
- **Dedicated Hosts**: A physical server with EC2 instance capacity fully dedicated to your use.
- **Dedicated Instances**: Instances that run in a VPC on hardware that is dedicated to a single customer.
- **Reserved Instances**: Purchase a capacity reservation that is always available on a recurring schedule you specify.
- **Spot Instances**: Instances run as long as they are available and your bid is above the Spot Instance price.

Module 7: Storage

AWS Academy Cloud Foundations

7. Storage

- Amazon **Elastic File Systems** (EFS) provides file sharing across multiple EC2 instances [here].
- Amazon **S3** provides object storage which has a high-level performance, scalability and data availability, and offers **virtually unlimited scalability** at very low costs [here].
- **S3** and **RDS** can provide cross-region replication.
- **EBS** only replicates with an Availability Zone and not cross-region.
- By default, Amazon **Elastic Block Store** (EBS) [here] and Amazon **Redshift** [here] are available across more than one Availability Zones Amazon S3 is an object storage system.
- Ephemeral storage is temporary storage that is added to an Amazon EC2 instance. Amazon EBS is persistent, mountable storage that can be mounted as a device to an Amazon EC2 instance.
- Amazon EFS is a shared file system that multiple Amazon EC2 instances can mount at the same time.
- Amazon S3 is persistent storage where each file becomes an object and is available through a Uniform Resource Locator Amazon S3 Glacier is for cold storage for data that is not accessed frequently (for example, when you need long-term data storage for archival or compliance reasons). Amazon EBS is persistent block storage volumes for use with Amazon EC2 instances.
- Amazon EBS volumes are automatically replicated within its Availability Zone.
- If we change a single character in a file for block storage, only the block that contains the character will be changed. If we change a single character in a file for object storage, the whole of the file object will be changed. Block storage typically has the lowest latency and least bandwidth used.
- A snapshot is a backup of Amazon EBS storage. The first snapshot in Amazon EBS storage is the baseline snapshot. Solid State Drives (SSD) with Amazon EBS storage provides the be

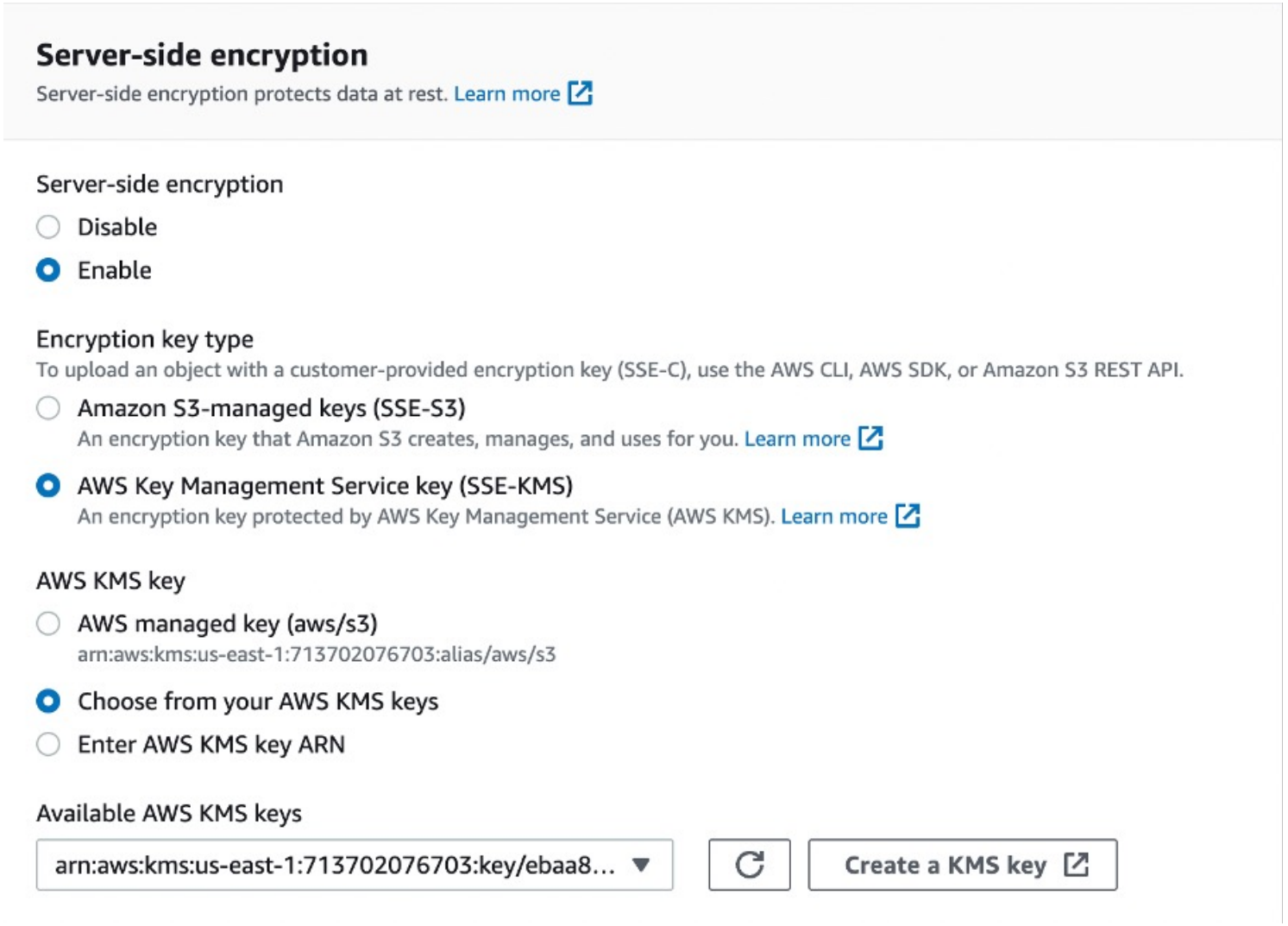
Data Types

Database type	Use cases	AWS service
Relational	Traditional applications, enterprise resource planning (ERP), customer relationship management (CRM), ecommerce	**Amazon Aurora** **Amazon RDS** **Amazon Redshift**
Key-value	High-traffic web applications, ecommerce systems, gaming applications	**Amazon DynamoDB**
In-memory	Caching, session management, gaming leaderboards, geospatial applications	**Amazon ElastiCache** **Amazon MemoryDB for Redis**
Document	Content management, catalogs, user profiles	**Amazon DocumentDB (with MongoDB compatibility)**
Wide column	High-scale industrial apps for equipment maintenance, fleet management, and route optimization	**Amazon Keyspaces**
Graph	Fraud detection, social networking, recommendation engines	**Amazon Neptune**
Time series	Internet of Things (IoT) applications, DevOps, industrial telemetry	**Amazon Timestream**
Ledger	Systems of record, supply chain, registrations, banking transactions	**Amazon Ledger Database Services (QLDB)**

7. Storage

- With disaster recovery (DR) protection, Amazon **EBS snapshots** can be copied to different regions.
- With data encryption for Amazon EBS, encryption does not cost anything to use.
- Cost elements for Amazon EBS are: IOPS (Input/output operations per second); Volume size; and Volume type (SSD or HDD). Bucket names in Amazon S3 are universal and must be unique across all existing bucket names.
- **5TB** is the maximum size for an object in Amazon S3. **Almost unlimited storage**.
- With Amazon S3, the **data is not public by default**.
- Amazon S3 Standard is designed for high durability, availability, and performance object storage for frequently accessed data.
- Amazon S3 Intelligent-Tiering is designed to optimize costs by automatically moving data to the most cost-effective access tier without performance impact or operational overhead. Amazon S3 One Zone-Infrequent Access is a storage class for data that is accessed less frequently but requires rapid access when needed and stores in a single Availability Zone.
- **Amazon S3 Glacier** is a secure, durable, and low-cost storage class for data archiving. Amazon S3 Glacier Deep Archive is the lowest-cost storage class for Amazon S3.
- To reduce cost, move less used data into **S3 buckets**.
- S3 buckets can be encrypted either with **Amazon S3-managed keys** (SSE-S3) or **AWS Key Management Service** (AWS KMS) keys.

S3 Encryption

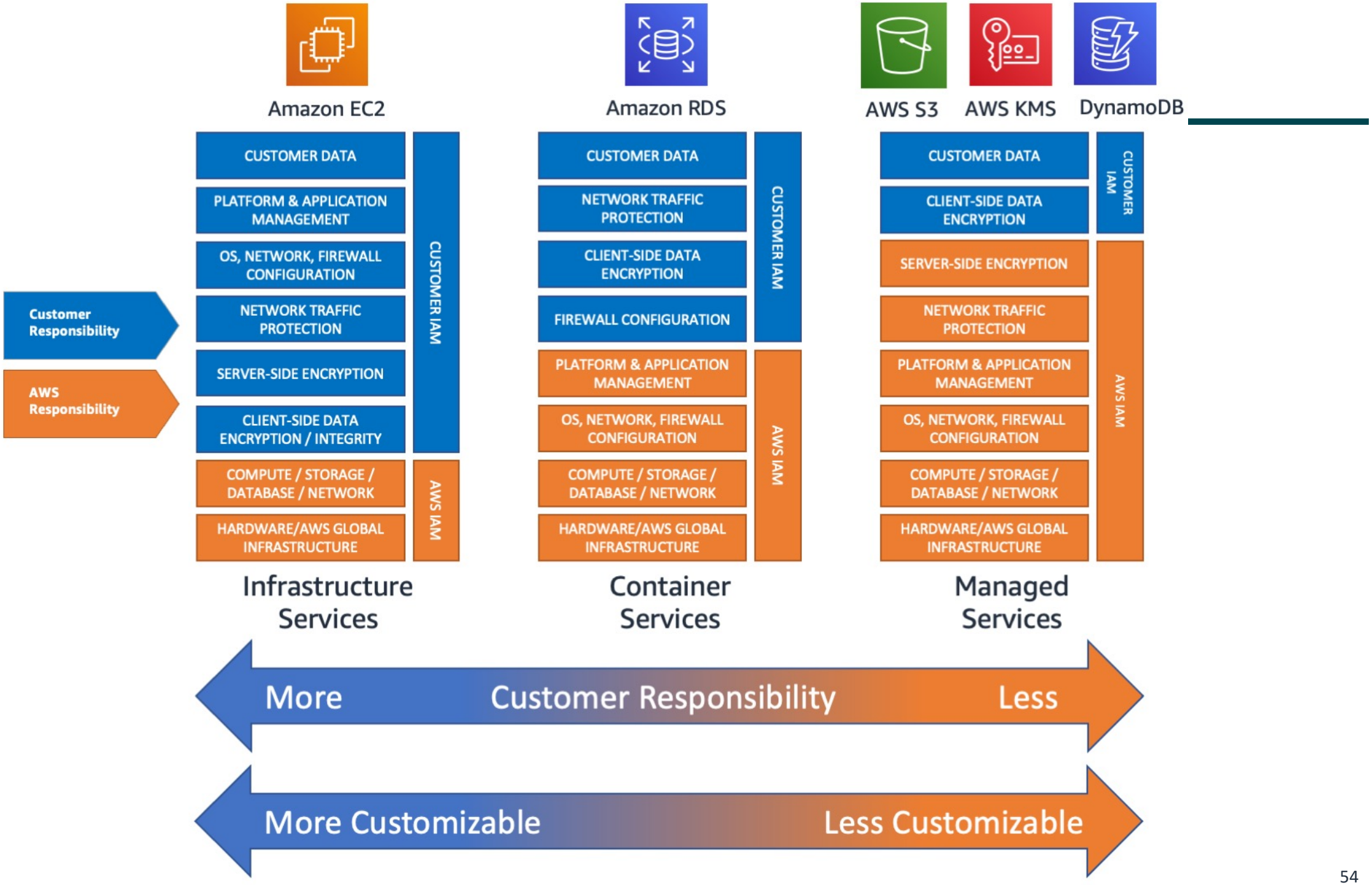


Module 8: Databases

AWS Academy Cloud Foundations

8. Databases

- **Amazon ElasticCache** is an in-memory data service. We can use it to improve database performance with microsecond latency [here]
- **Amazon DynamoDB** supports a NoSQL data, and uses a JSON key-value pair for data objects.
- The customer is responsible for **encryption options** for an RDS database.
- **Amazon Aurora** is a relational database which supports MySQL and PostgreSQL [here].
- Amazon **DynamoDB** is a fast and flexible NoSQL database service for any scale.
- Amazon **RDS** is an enterprise-class relational database which is not fully managed by AWS.
- Amazon **Aurora** is an enterprise-class relational database which is fully managed by AWS.
- Amazon **Redshift** is well matched to Enterprise data warehouse (EDW) and Big Data applications.
- Amazon Aurora is relational database and supports MySQL and PostgreSQL.
- A company has a MySQL database and Window's servers and needs to migrate to AWS. It can use Amazon RDS for the migration.
- A company has an **Oracle or Microsoft SQL** database and needs to migrate to AWS. Amazon RDS can be used for the migration.
- Amazon **RDS** supports Microsoft SQL and PostgreSQL.
- An **unmanaged database** service allows for scaling, fault tolerance, and availability to be managed **by the customer**.
- A **managed database** service allows for scaling, fault tolerance, and availability are typically integrated **into the service** (by AWS).


Amazon EC2
Amazon RDS
AWS S3
AWS KMS
DynamoDB
Customer Responsibility
AWS Responsibility
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
NETWORK TRAFFIC PROTECTION
SERVER-SIDE ENCRYPTION
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
NETWORK TRAFFIC PROTECTION
CLIENT-SIDE DATA ENCRYPTION
FIREWALL CONFIGURATION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
CLIENT-SIDE DATA ENCRYPTION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Infrastructure Services
Container Services
Managed Services
More
Customer Responsibility
Less
More Customizable
Less Customizable

Amazon Data Migration Service

Module 9: Cloud Architecture

AWS Academy Cloud Foundations

9. Cloud Architecture/Well Architected Framework

- **Reliability** allows an organisation to recover from a failure. It supports changes to be made to the infrastructure **using automation**, and reduces the need to **guess capacity**.
- **Operational excellence** supports continuous and small changes in order to deliver business value (Figure 13).
- **Security** supports the protection of data, systems and assets for improved overall security (Figure 13).
- **Performance Efficiency** supports the efficient usage of resources in order to meet the system requirements, and evolve to meet demand and technological changes (Figure 13).
- **Cost optimization** supports finding the lowest price point for the effective delivery of business value (Figure 13).
- **Sustainability** supports the reduction of energy consumption and in improving resource utilization (Figure 13).

9. Cloud Architecture

Operational Excellence Pillar

The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

HTML | Labs

Security Pillar

The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

HTML | Labs

Reliability Pillar

The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.

HTML | Labs

Performance Efficiency Pillar

The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

HTML | Labs

Cost Optimization Pillar

The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.

HTML | Labs

Sustainability Pillar

The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

HTML | Labs

Module 10: Automatic Scaling and Monitoring

AWS Academy Cloud Foundations

10. Cloud Scaling and Monitoring

- Amazon **Elastic Load Balancing** scales your load balancer as traffic to your application changes over time.
- **Application Load Balancer** is a load balancer which is matched to Hypertext Transfer Protocol (HTTP) and Secure HTTP (HTTPs) traffic.
- Application Load Balancer is a load balancer which focuses on Amazon EC2 instances, containers, IP addresses, and Lambda functions, and based on the content of the request.
- **Network Load Balancer** is a load balancer which is matched to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic.
- **Classic Load Balancer** is a load balancer which supports the load balancing of applications that use HTTP, HTTPS, TCP, and SSL, and is an older load balancer than newer implementations.
- Listeners are required to be set up for a load balancer to operate. For load balancing health checks, when the load balancer detects an unhealthy target, it stops routing traffic to the target and resumes when healthy again.
- With Application Load Balancers and Network Load Balancers, we register targets in target groups and route traffic to the target groups.
- With Classic Load Balancers, we. Use case for load balancers: achieve high availability and better fault toleran**register instances with the load balancer**ce for your applications; automatically load balance containerized applications; and automatically scale your applications.
- Application Load Balancer is a load balancer and used to support traffic to a containerized application.
- Network Load Balancer is a load balancer and used for extremely spiky and unpredictable TCP traffic.

10. Cloud Scaling and Monitoring

- Classic Load Balance is a load balancer and used for simple load balancing with multiple protocols.
- Network Load Balancer is a load balancer and used with a **static or Elastic IP address or for an IP target outside a VPC**.
- Network Load Balancer is a load balancer that can handle millions of requests per second while maintaining low latencies.
- Application Load Balancer is a load balancer that supports **HTTPs requests**.
- Monitoring methods that can be used to monitor load balancers, analysing traffic patterns, and also troubleshoot are Amazon CloudWatch metrics; Amazon CloudTrail logs; and Amazon logs.
- In CloudWatch, metrics that can be used for a trigger include CPU utilization; Network connections; Read operations for EBS; and Estimated charges.
- An **Auto Scaling group** is a collection of EC2 instances that are treated as a logical grouping for automatic scaling and management.
- With Amazon EC2 Auto Scaling, launching instances referred to as **scaling out**.
- With Amazon EC2 Auto Scaling, terminating instances referred to as **scaling in**.
- Amazon SNS (**Simple Notification Service**) publishes alerts from Amazon CloudWatch. A company needs to collect utilization metrics on Amazon EC2 instances and Amazon DynamoDB. They can use Amazon CloudWatch.
- Amazon SES (**Simple Email Service**) can integrate with CloudWatch to send an email on an alert.

CloudTrail