AWS

Agenda

- Introduction to AWS
- AWS Management Console
- Core AWS Services - Compute
- Core AWS Services - Storage
- Core AWS Services - Databases
- Core AWS Services - Networking
- Security, Identity, and Compliance
- Monitoring and Management
- Application Integration
- Cost Management
- Scalability and Performance
- Serverless Computing

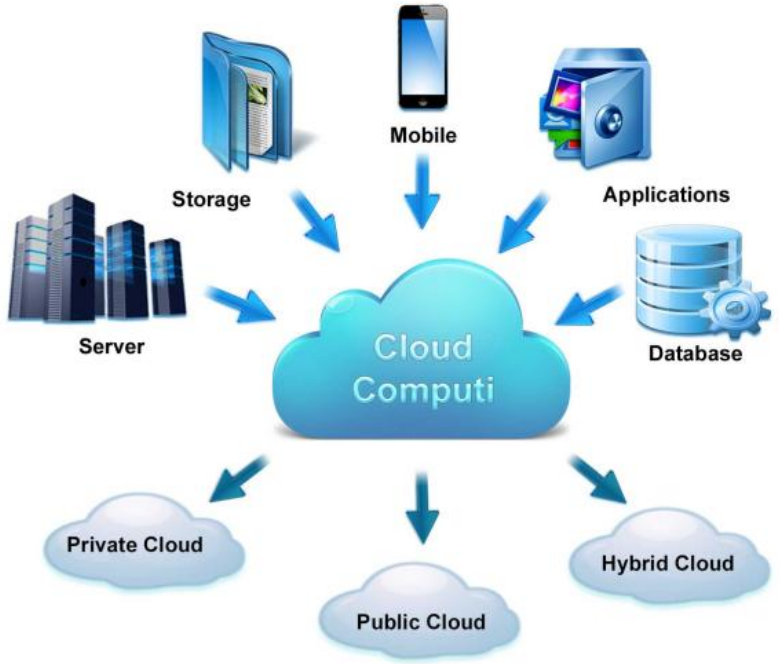
Overview of Cloud Computing

- Cloud computing refers to the delivery of computing services over the internet ("the cloud") to provide on-demand access to resources and services like servers, storage, databases, networking, software, and more, without the need for direct management by the user.

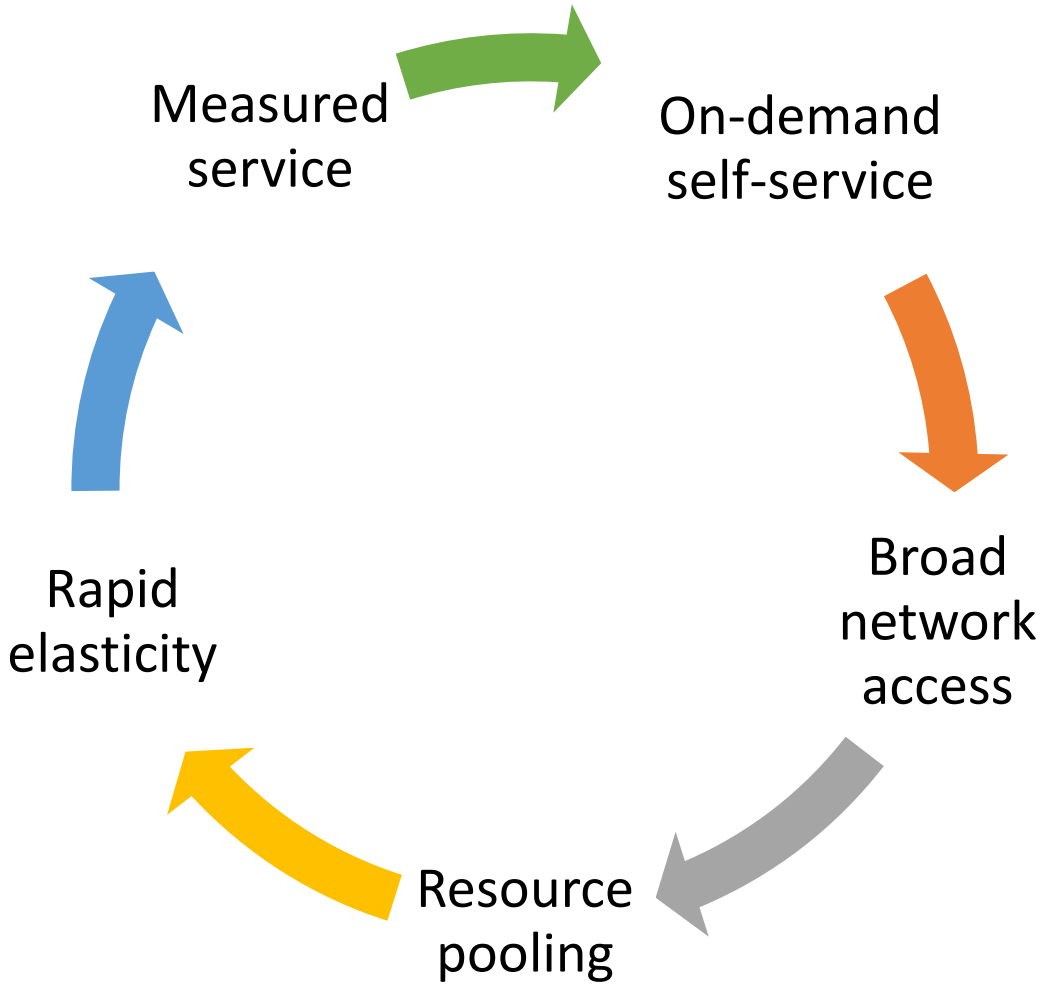
- Cloud computing can be called a technology through which things like software, processing, and data storage are outsourced.

Cloud Computing

- Central data center for providing services.
- On-demand, scalable, unlimited computation & storage.
- It's basically a data center.
- 4 characteristics of a Cloud:
  - ✓ Everything is a Service (backup, firewall, network…)
  - ✓ Elasticity in nature
  - ✓ HA – 99.99% SLA
  - ✓ Unlimited computation power.
- Any Data Center that provides above 4 chars is a cloud.



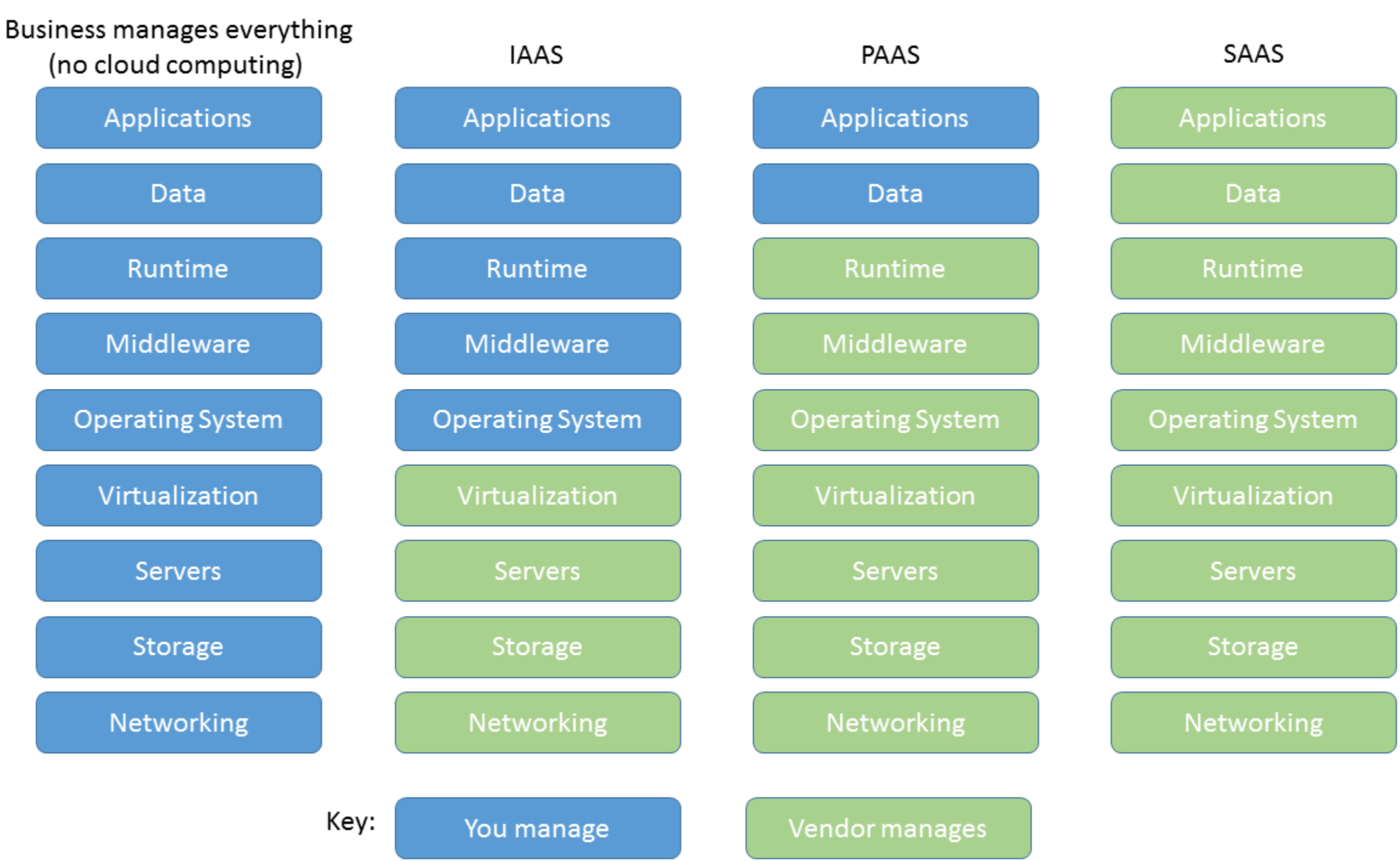
Characteristics of Cloud Computing



Cloud Service Models

- **Infrastructure as a Service (IaaS)**
  - Provides virtualized computing resources over the internet, allowing users to rent virtual machines, storage, and networking.
- **Platform as a Service (PaaS)**
  - Offers a platform allowing customers to develop, run, and manage applications without dealing with the underlying infrastructure complexities.
- **Software as a Service (SaaS)**
  - Delivers software applications over the internet on a subscription basis, eliminating the need for users to install, maintain, and upgrade software locally.

Pizza as a Service


Business manages everything
(no cloud computing)
Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking
IAAS
Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking
PAAS
Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking
SAAS
Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking
Key:
You manage
Vendor manages

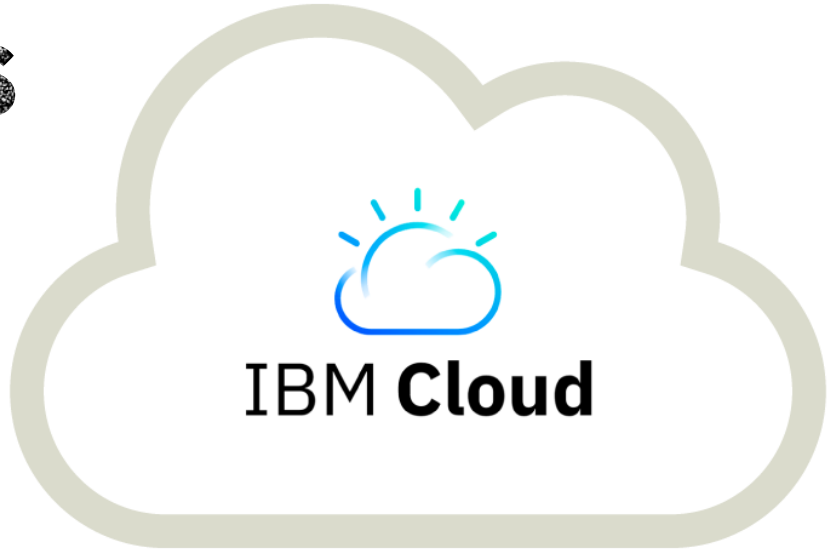
Cloud Deployment Models

- **Public Cloud**
  - ✓ Services are provided over the public internet and available to anyone who wants to purchase them.
- **Private Cloud**
  - ✓ Services are maintained on a private network, often within an organization's data center, offering more control, security, and customization.
- **Hybrid Cloud**
  - ✓ Combines public and private cloud resources, allowing data and applications to be shared between them while offering greater flexibility and deployment options.
- **Multi-cloud**
  - ✓ Involves using multiple cloud computing services from different providers, providing redundancy, diversity, and the ability to optimize for specific workloads.

Benefits of Cloud Computing

- Cost Savings
- Scalability
- Flexibility and Agility
- Reliability and Availability
- Security

Cloud Vendors



Google Cloud Platform

AWS Core Services

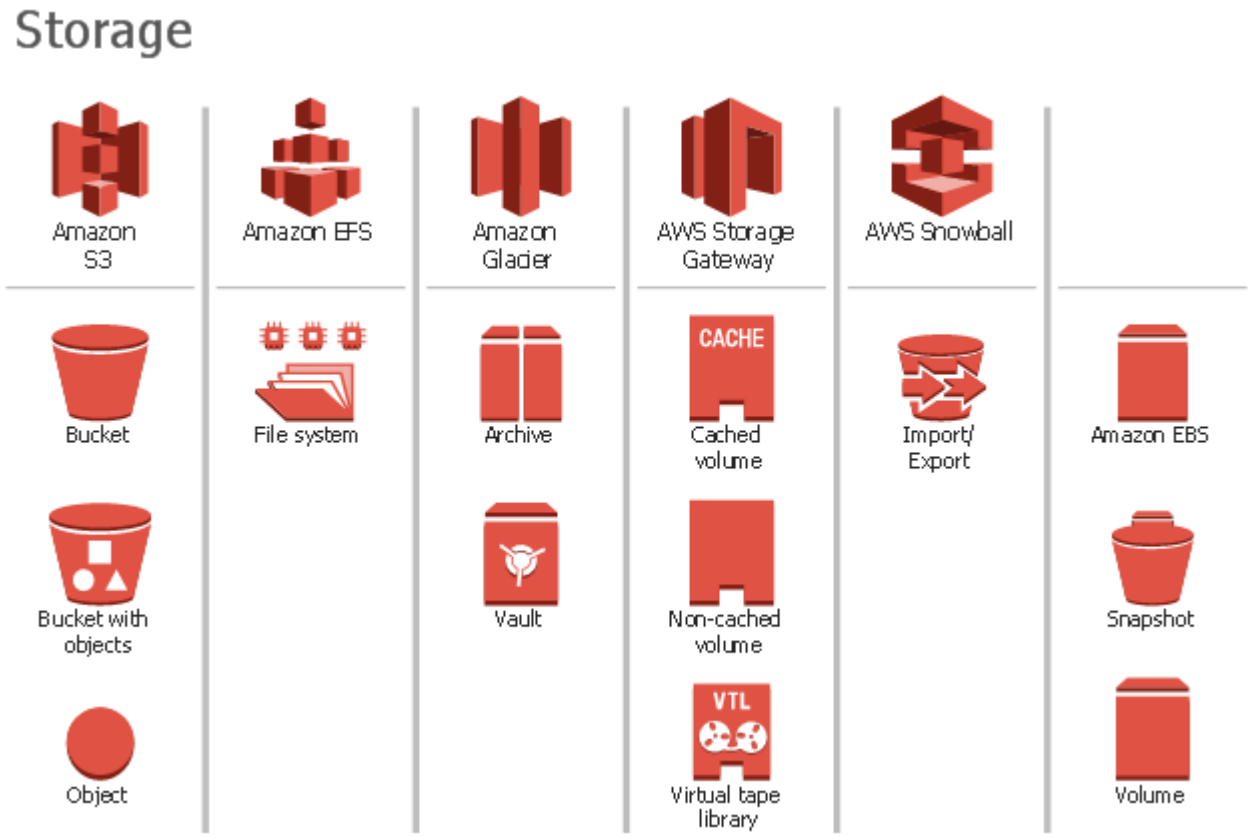
- ✓ Compute Services
- ✓ Amazon EC2 (Elastic Compute Cloud)
- ✓ Amazon EC2 Auto Scaling
- ✓ Amazon Elastic Container Service (ECS)
- ✓ Storage Services
- ✓ Amazon S3 (Simple Storage Service)
- ✓ Amazon EBS (Elastic Block Store)
- ✓ Amazon Glacier
- ✓ Networking Services
- ✓ Amazon VPC (Virtual Private Cloud)
- ✓ Amazon Route 53
- ✓ AWS Direct Connect

AWS Compute Services

Instance	Containers	Serverless
Amazon Elastic Compute Cloud	Amazon Elastic Container Service	AWS Lambda
Amazon EC2 Auto Scaling	Amazon Elastic Kubernetes Service	

AWS Storage Services

- AWS Backup
- Amazon Elastic Block Store
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon File Cache
- Amazon FSx for Lustre
- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File Server
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway



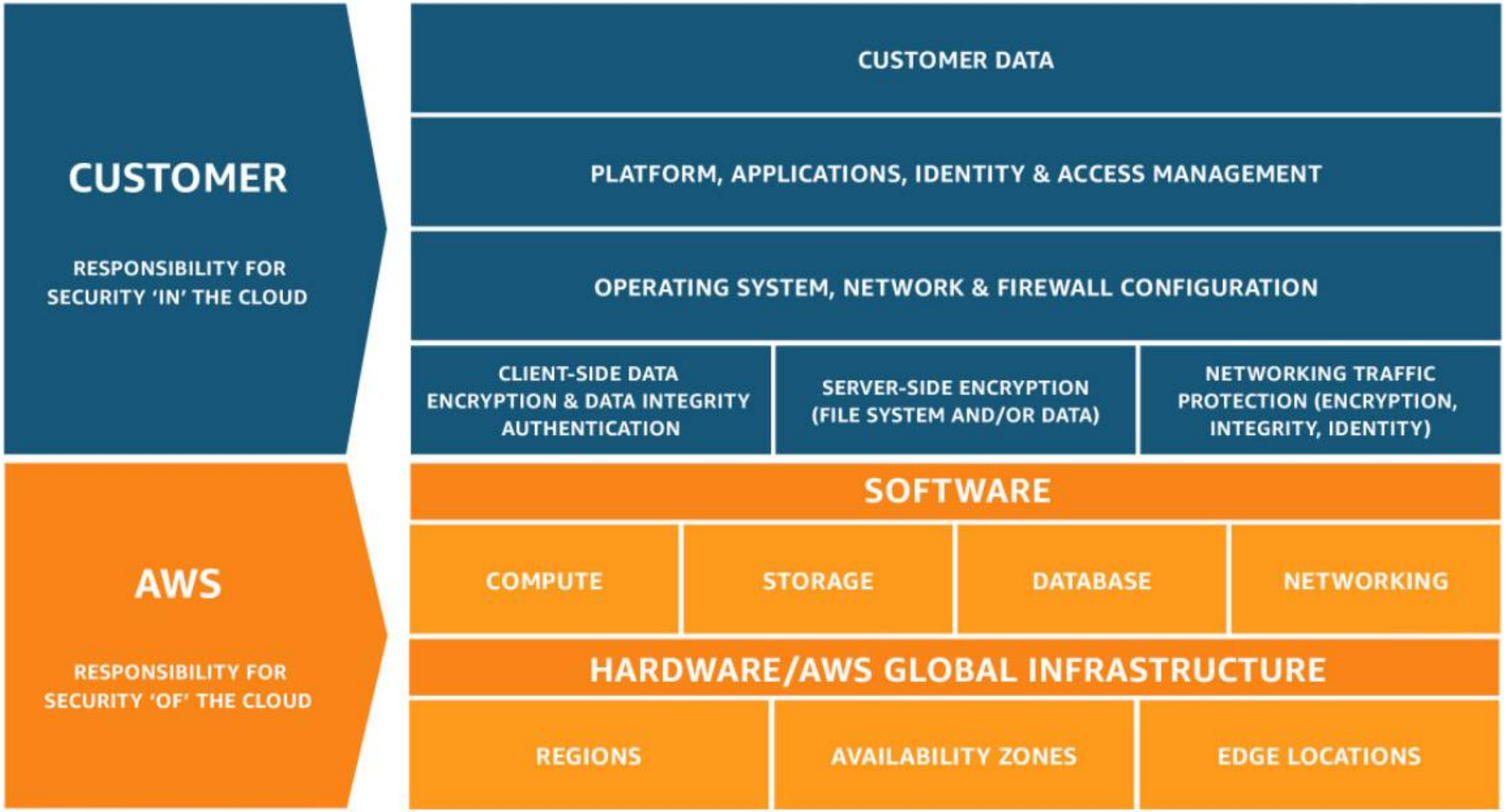
AWS Networking Services

- ✓ Amazon API Gateway
- ✓ Amazon CloudFront
- ✓ Amazon Route 53
- ✓ AWS Verified Access
- ✓ Amazon VPC
- ✓ Amazon VPC Lattice
- ✓ AWS App Mesh
- ✓ AWS Cloud Map
- ✓ AWS Direct Connect
- ✓ AWS Global Accelerator
- ✓ AWS PrivateLink
- ✓ AWS Private 5G
- ✓ AWS Transit Gateway
- ✓ AWS VPN
- ✓ Elastic Load Balancing
- ✓ Integrated Private Wireless on AWS

Security and Identity

- AWS Shared Responsibility Model
- AWS Identity and Access Management (IAM)

AWS Shared Responsibility Model

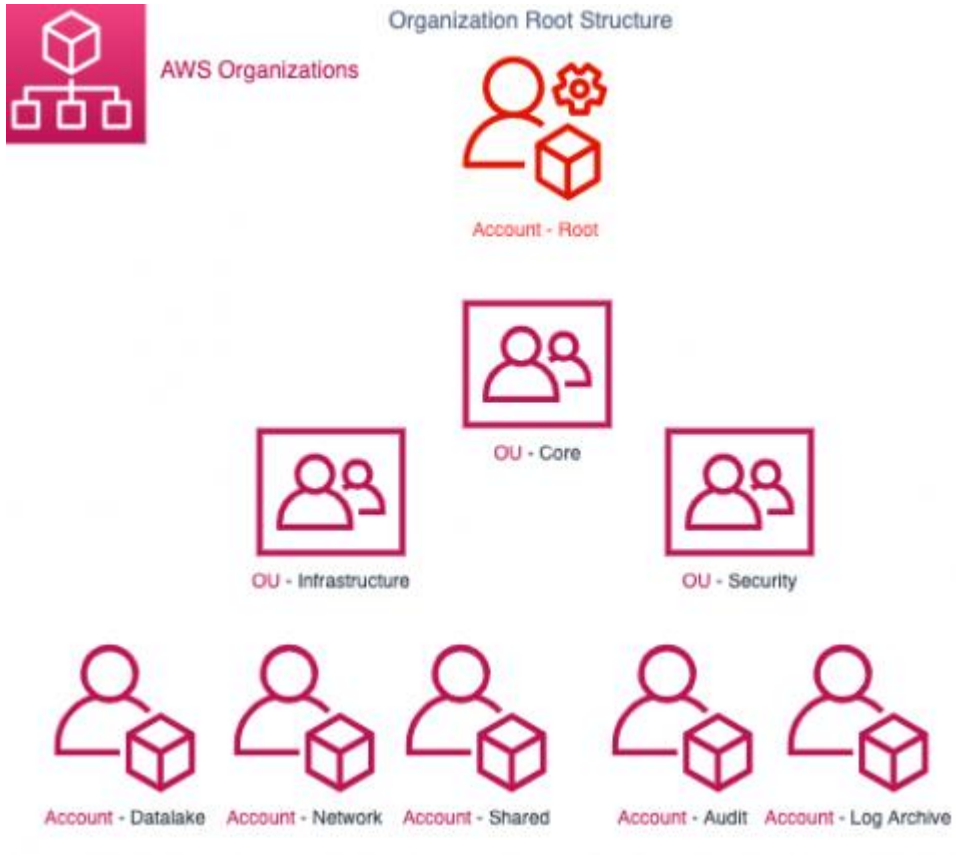


AWS Identity and Access Management (IAM)

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.
- With IAM, you can centrally manage permissions that control which AWS resources users can access.
- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account ➥ ROOT USER.
- This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account.

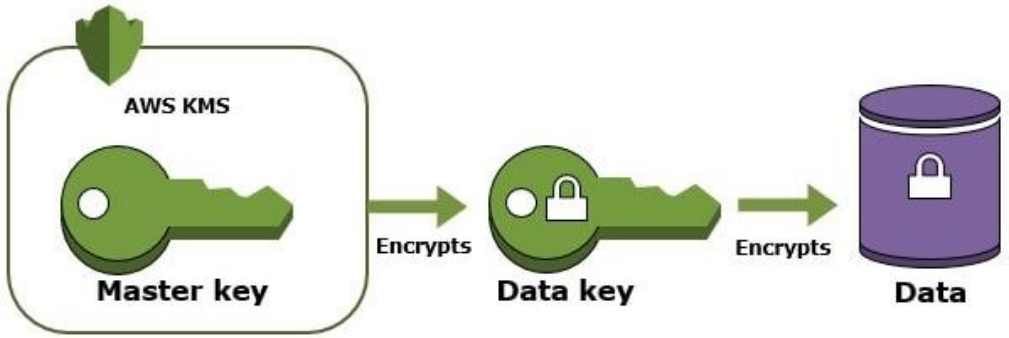
AWS Organizations

- AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.
- AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business.
- As an administrator of an organization, you can create accounts in your organization and invite existing accounts to join the organization.

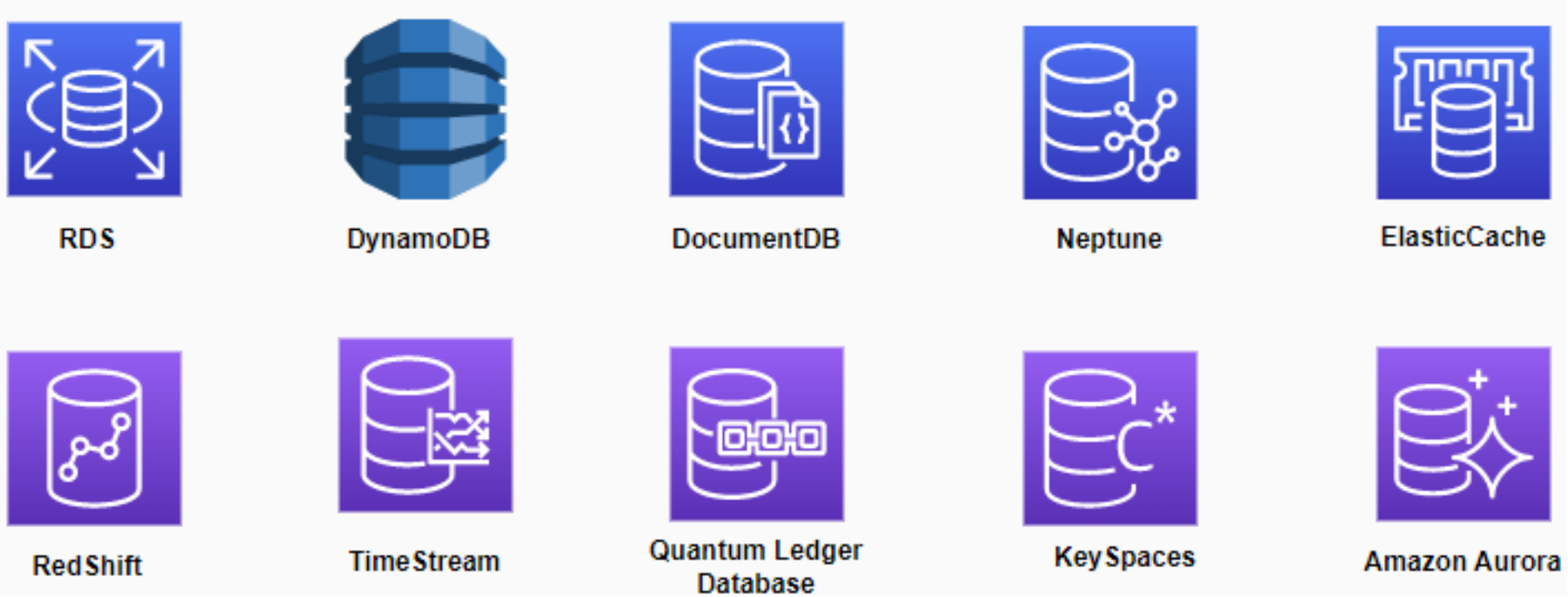


AWS Key Management Service (KMS)

- AWS Key Management Service (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.
- AWS KMS uses hardware security modules (HSM) to protect and validate your AWS KMS keys under the FIPS 140-2 Cryptographic Module Validation Program.
- AWS KMS integrates with most other AWS services that encrypt your data.
- AWS KMS also integrates with AWS CloudTrail to log use of your KMS keys for auditing, regulatory, and compliance needs.

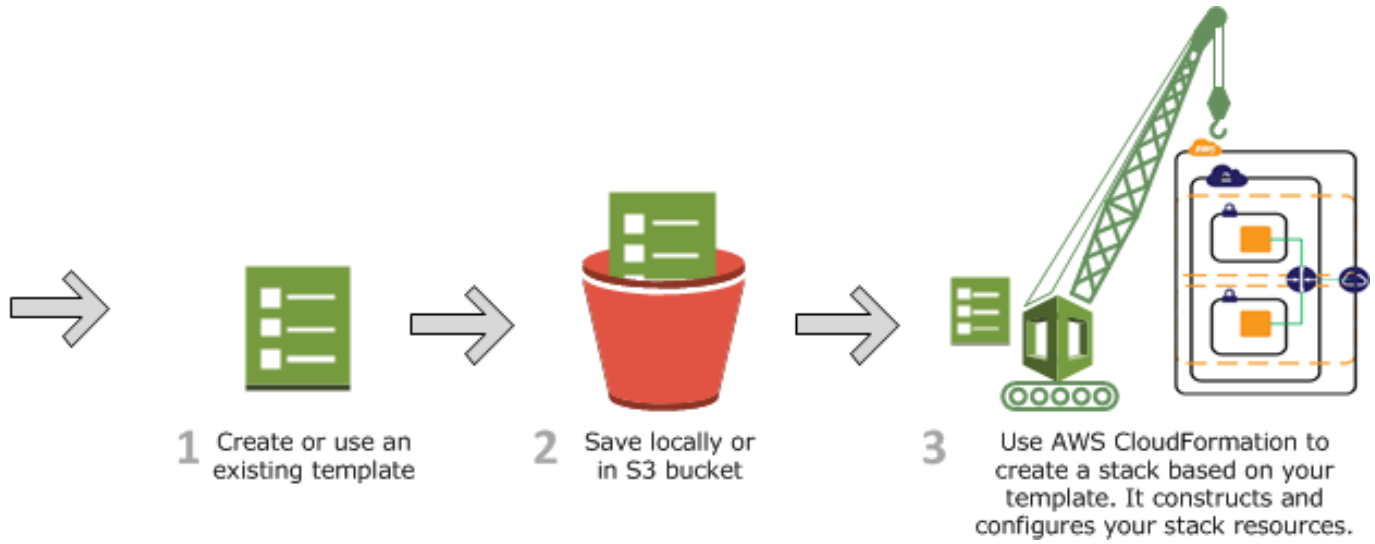


Database Services

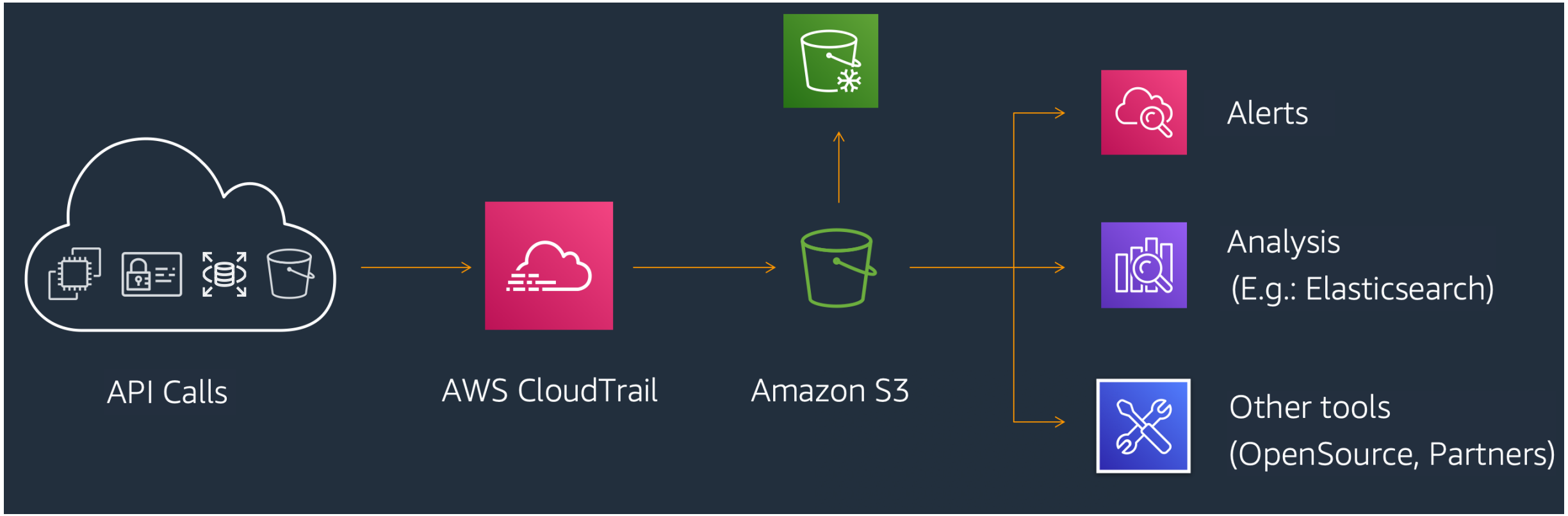


AWS Management Tools - AWS CloudFormation

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Description": "A simple EC2 instance",
    "Resources": {
        "MyEC2Instance": {
            "Type": "AWS::EC2::Instance",
            "Properties": {
                "ImageId": "ami-0ff8a91507f77f867",
                "InstanceType": "t2.micro"
            }
        }
    }
}
```

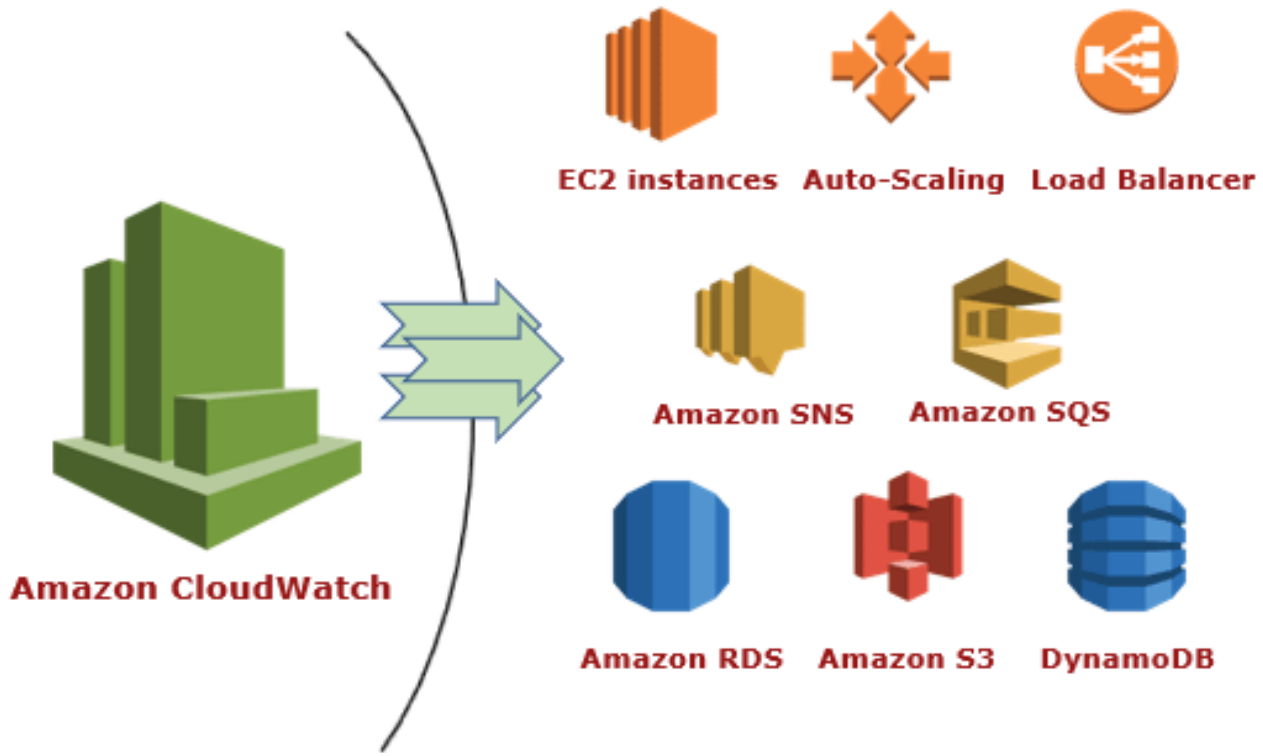


AWS Management Tools - AWS CloudTrail



AWS Management Tools - Amazon CloudWatch

- CloudWatch enables you to monitor your complete stack (applications, infrastructure, network, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR).

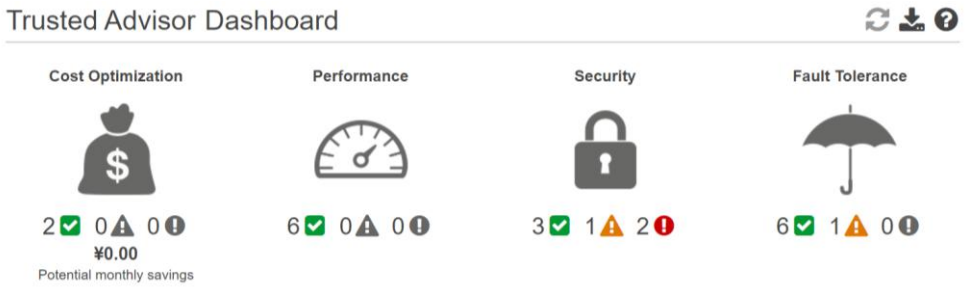


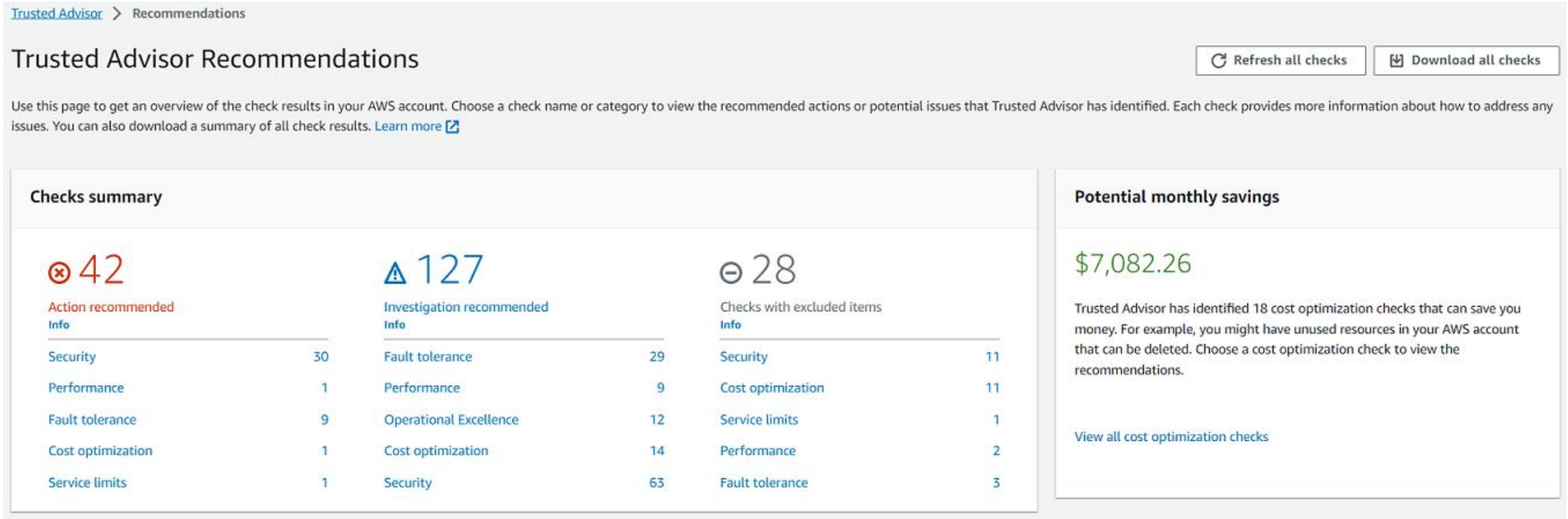
AWS Management Tools - AWS Config

- AWS Config is a service provided by Amazon Web Services (AWS) that enables continuous monitoring and assessment of AWS resource configurations.
- It automatically evaluates the configuration of AWS resources against desired configurations specified by users, helping to ensure compliance with security policies, industry regulations, and best practices.
- AWS Config provides a detailed inventory of AWS resources, including configuration history and relationships between resources, facilitating resource tracking and management.
- It offers configuration snapshots, which capture the state of AWS resources at specific points in time, enabling users to audit and troubleshoot configuration changes.

AWS Trusted Advisor

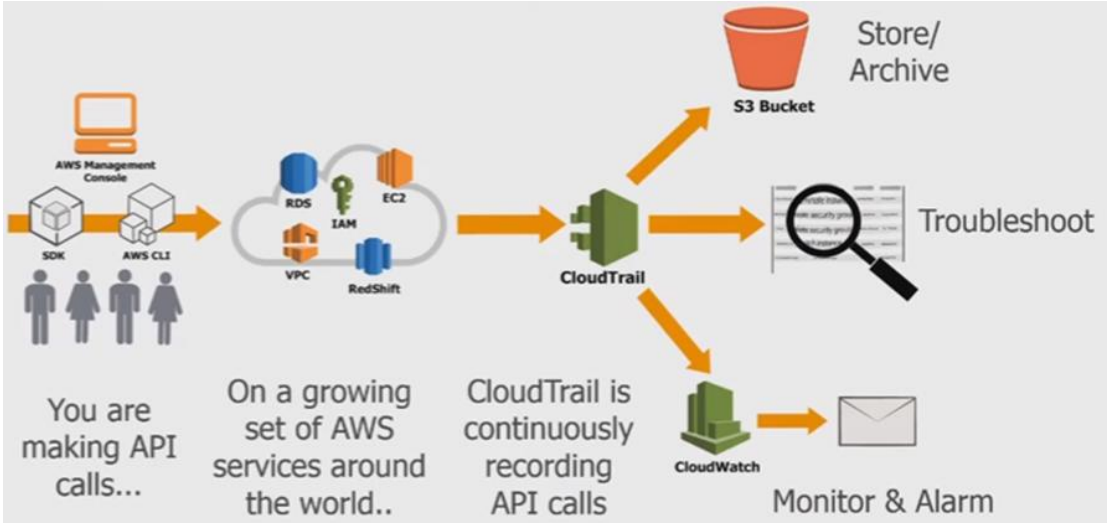
- AWS Trusted Advisor is a service that continuously analyzes your AWS accounts and provides recommendations to help you to follow AWS best practices and AWS Well-Architected guidelines.





AWS CloudTrail

- AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account.
- Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.



- Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
- CloudTrail is active in your AWS account when you create it and doesn't require any manual setup.
- When activity occurs in your AWS account, that activity is recorded in a CloudTrail event.

AWS Pricing Models

- ✓Pay-as-you-go
- ✓Reserved Instances (RIs)
- ✓Spot Instances
- ✓Savings Plans
- ✓Reserved Capacity
- ✓Free Tier
- ✓Pay-as-you-go with Commitments
- ✓Data Transfer Pricing
- ✓Data Transfer Acceleration
- ✓Content Delivery Network (CDN)

AWS Pricing Models - Offerings

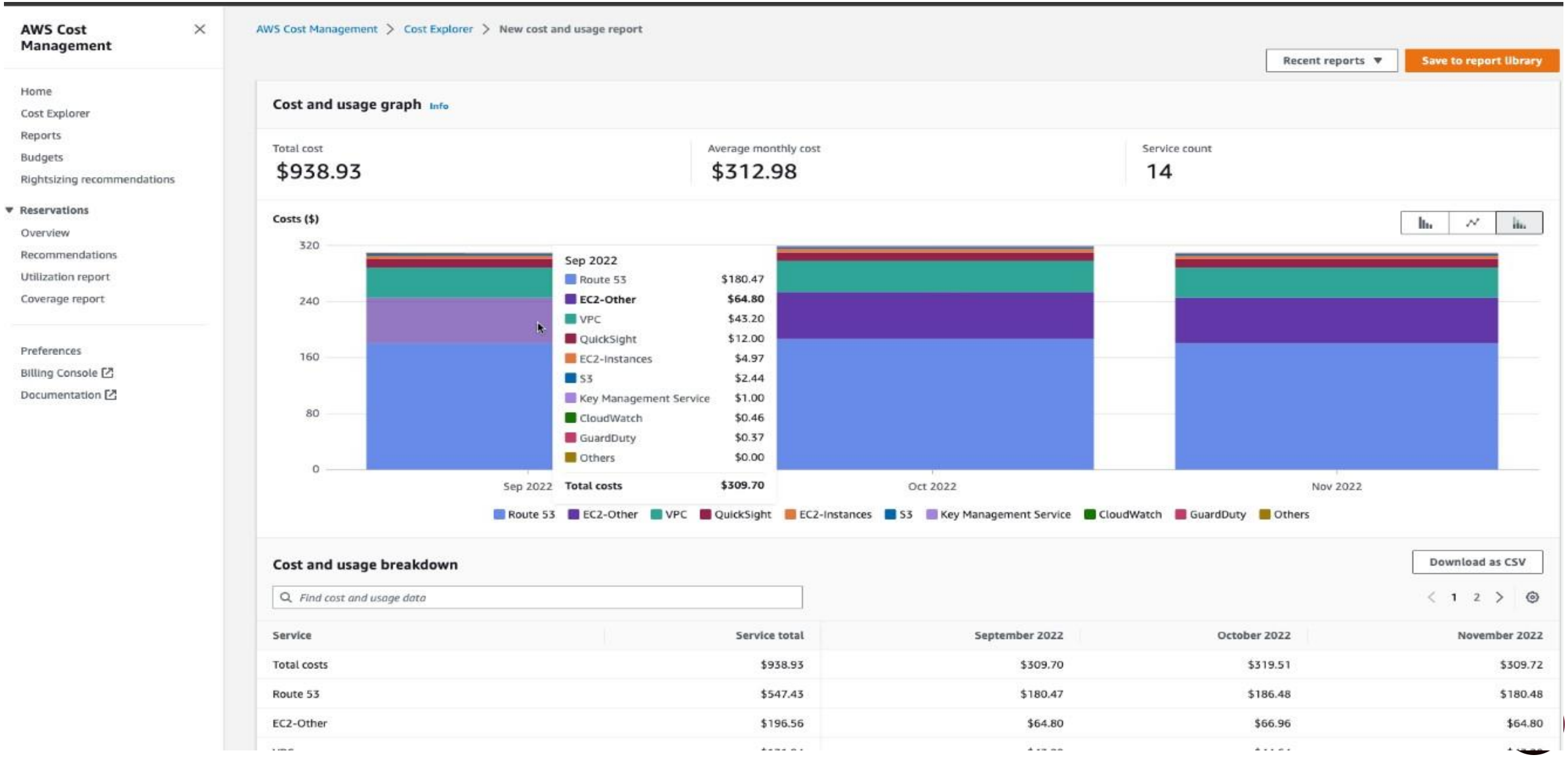
- ✓ **Amazon EC2** – 750 Hours
- ✓ **Amazon S3** – 5GB
- ✓ **Amazon RDS** – 750Hrs of Single-AZ instance, 20GB storage/month.
- ✓ **Amazon Lambda** – The monthly compute price is $0.0000166667 per GB-s and the free tier provides 400,000 GBs.
- ✓ **Amazon DynamoDB** – 25GB (with 25 provisioned Write and 25 provisioned Read Capacity Units) which is enough to handle 200M requests per month.
- ✓ **Amazon CloudWatch** – EC2, S3, Kinesis send metrics automatically for free to CloudWatch.
- ✓ **Amazon SNS** - One million requests free per month.
- ✓ **Amazon SQS** - One million requests free per month.
- ✓ **Amazon Glacier** – 10GB

Free Trials

12 months free

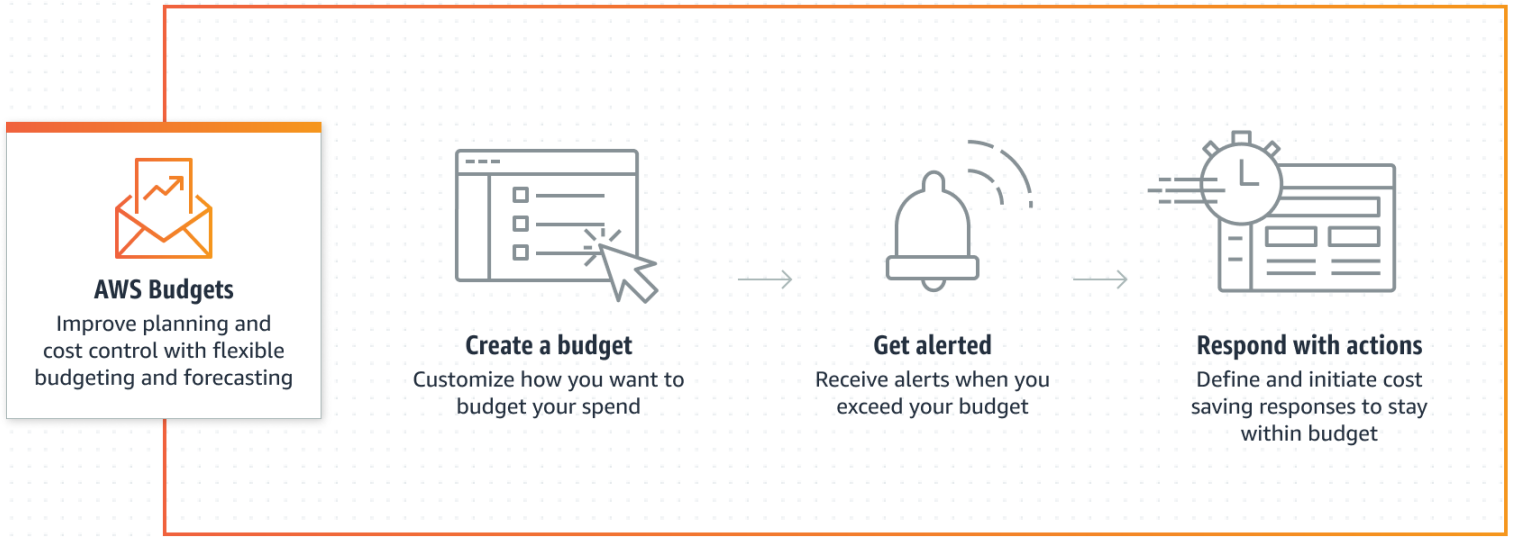
Always free

AWS Cost Explorer



AWS Budgets

- Types of AWS budgets
  - ✓ Cost Budget
  - ✓ Usage Budget
  - ✓ RI Utilization Budget
  - ✓ RI Coverage Budget
  - ✓ Savings Plans Utilization
  - ✓ Savings Plans Coverage



AWS Architecture Best Practices

AWS Well-Architected and the Six Pillars

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.

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.

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.

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.

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.

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.

Well-Architected Framework

Operational Excellence

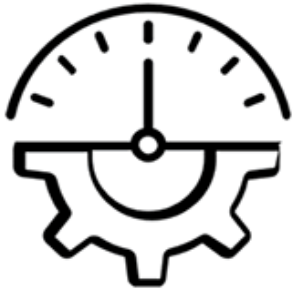
Run, manage and monitor production workload to deliver business value and continuous improve on supporting process and events

Security

Protecting information, systems, and assets along from outside world with risk assessment, unplanned failures, and mitigation strategies

Reliability

Auto recover workload from infrastructure, power or system failures with dynamic resource management to meet operational threshold.



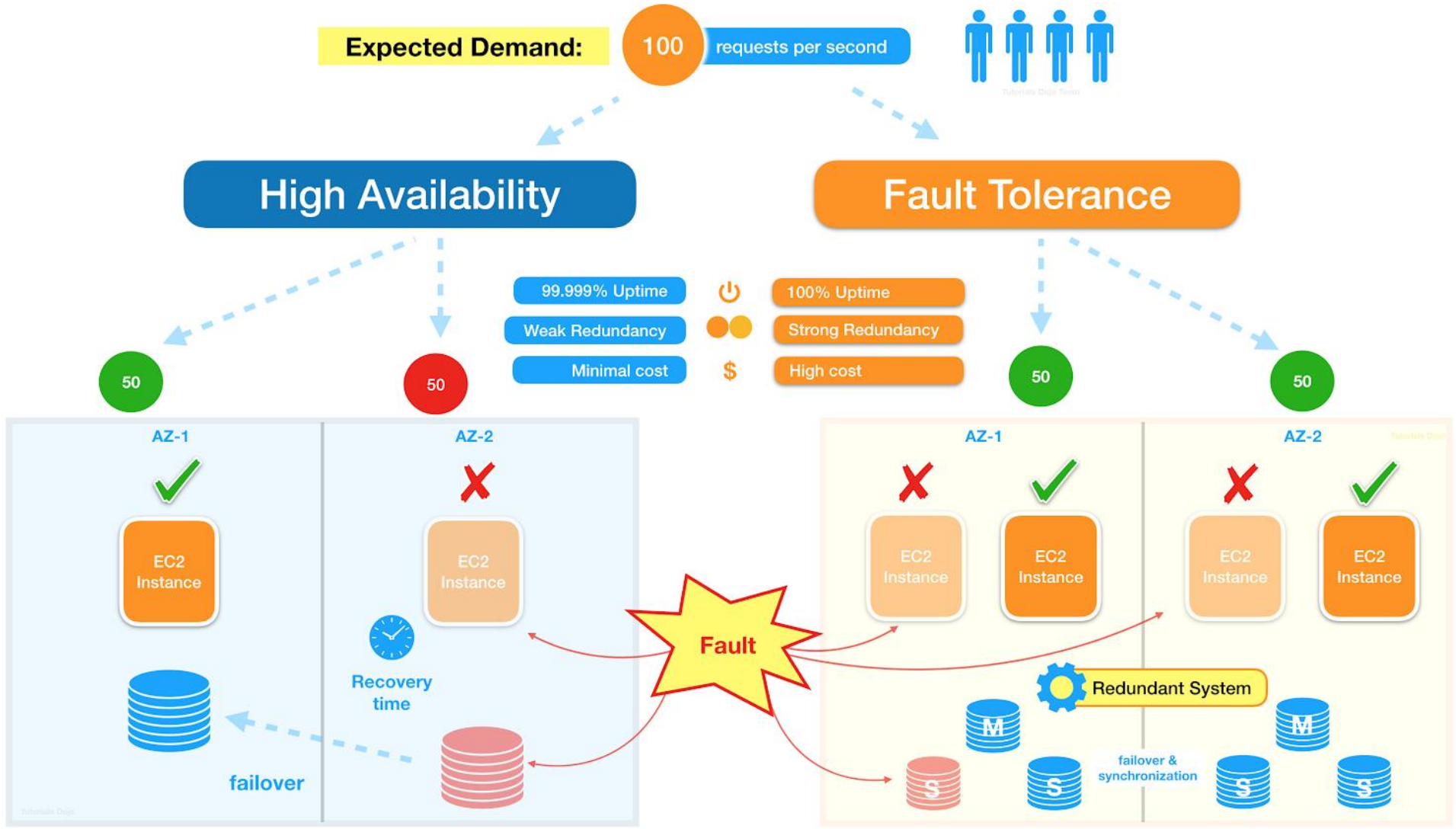
Performance Efficiency

Use computing resources efficiently to support on demand changes for delivering workload with maximum performance to meet the SLA

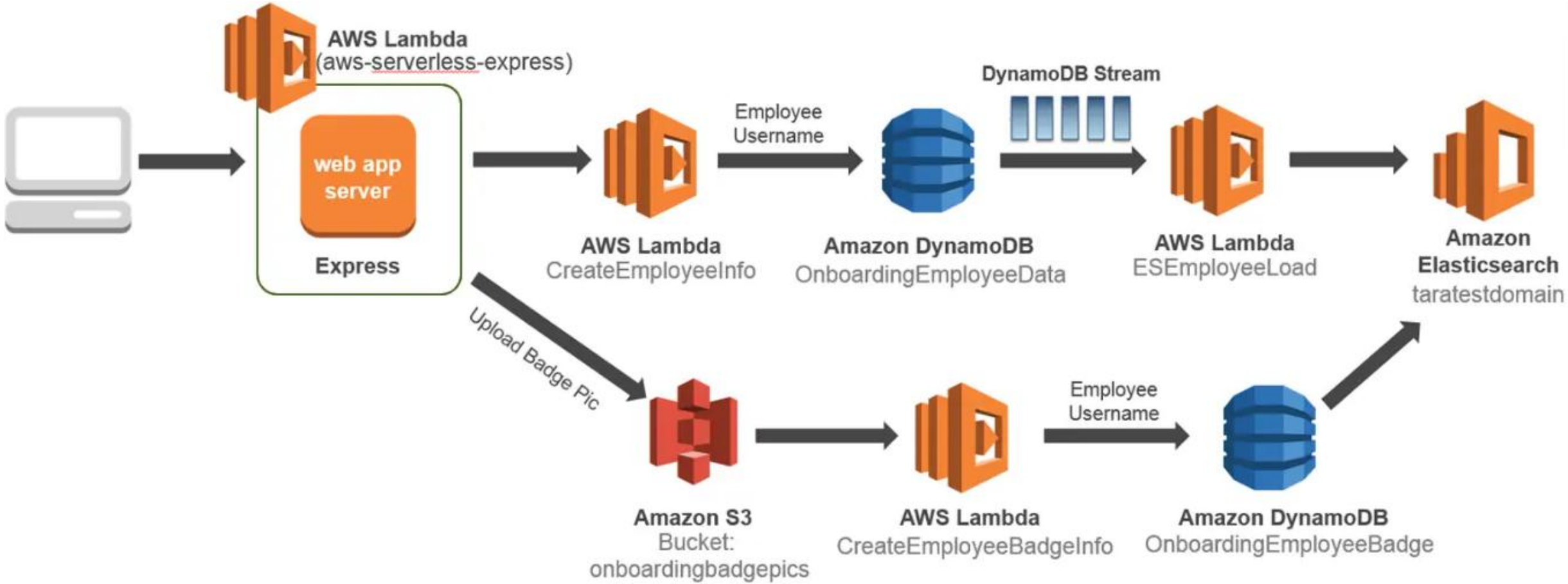
Cost Optimization

Avoiding & eliminate un-needed cost or replace resources with cost-effective resources without impacting the best practices and business need

AWS High Availability and Fault Tolerance



AWS Scalability



AWS Scalability – Vertical Scaling

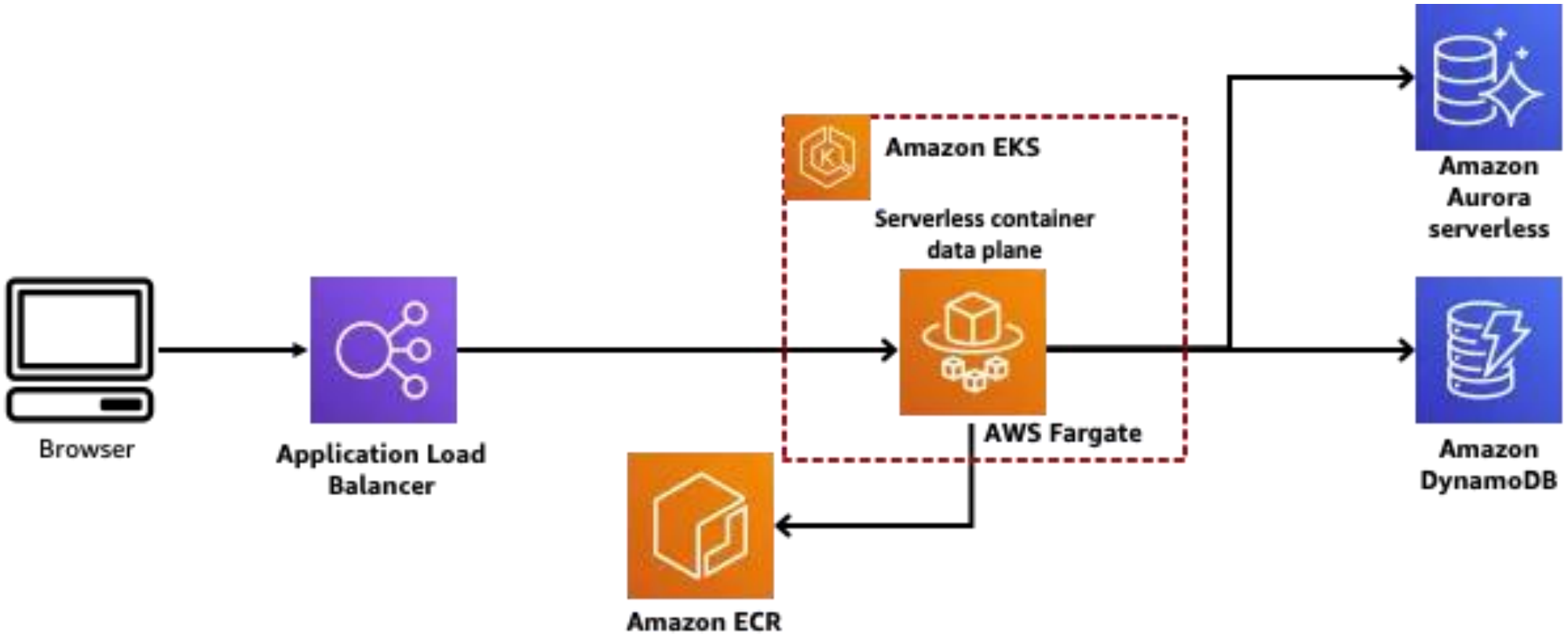
- Vertical scaling, also known as scaling up, refers to the process of increasing the capacity or capabilities of an individual hardware or software component within a system.
- You can add more power to your machine by adding better processors, increasing RAM, or other power-increasing adjustments.

Vertical Scaling

AWS Scalability – Horizontal Scaling

- Horizontal scaling, also known as scaling out, refers to the process of increasing the capacity or performance of a system by adding more machines or servers to distribute the workload across a larger number of individual units.
- In this approach, there is no need to change the capacity of the server or replace the server.

AWS Elasticity



AWS Storage Services

- **AWS S3 bucket** (Simple Storage Service)
  - URL based storage
  - we store objects (file, mp3, mp4…)
- **Amazon EFS** (Elastic File System)
  - simple, serverless, elastic file system to share file data without managing storage.
- **Amazon FSx**
  - fully managed, cost-effective with high performance open-source file system.
- **Amazon Elastic Block Storage (EBS)**
  - easy to use
  - high performance disk for the EC2 instance.
- **Amazon File Cache**
  - high-speed cache for heavy workloads.

AWS S3 terminologies

- **Bucket**:- A container for storing objects. All objects are stored in buckets. Buckets have a globally unique name across all of AWS.
- **Object**:- The fundamental entity stored in Amazon S3. An object consists of data, a key (unique within a bucket), and metadata.
- **Key**:- The unique identifier for an object within a bucket. The combination of a bucket, a key, and a version ID uniquely identify each object in a bucket.
- **Amazon Resource Name (ARN):-** A way to identify AWS resources across services. S3 buckets and objects have ARNs that can be used in IAM policies to control access.

AWS S3 terminologies

- **Access Control List (ACL):-** A set of permissions attached to an S3 bucket or object that specify which AWS accounts or users are granted access and what type of access they have (e.g., read or write).
- **Bucket Policy:-** A resource-based AWS Identity and Access Management (IAM) policy that applies to an S3 bucket. It defines who can access the bucket and under what conditions.
- **Storage Class**:- S3 offers different storage classes, each with different performance, durability, and cost characteristics. Common storage classes include STANDARD, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, and DEEP_ARCHIVE.

AWS S3 terminologies

- **Versioning**:- A feature that allows you to preserve, retrieve, and restore every version of every object stored in a bucket. Versioning helps protect against accidental deletion or overwrites.
- **Lifecycle Configuration**:- Defines rules for automatically transitioning objects between storage classes or deleting them when they are no longer needed.
- **Transfer Acceleration**:- A feature that enables fast, easy, and secure transfers of files to and from S3 using Amazon CloudFront's globally distributed edge locations.

AWS S3 terminologies

- **Server-Side Encryption (SSE):-** A feature that helps protect data at rest by automatically encrypting objects when they are stored in S3. There are different SSE options, including SSE-S3, SSE-KMS, and SSE-C.
- **Multipart Upload**:- A feature that allows you to upload large objects in parts, which can improve performance and reliability, especially for large files.
- **Event Notifications**:- S3 can generate events when certain operations occur, such as object creation or deletion. You can configure event notifications to trigger AWS Lambda functions or SQS queues.

AWS S3 Advance Features:

- Versioning
- Cross-Region Replication (CRR)
- Transfer Acceleration
- Event Notifications
- Multipart Upload
- Transfer Manager
- Server-Side Encryption (SSE)
- Access Control
- Lifecycle Policies
- Intelligent-Tiering

Amazon S3 Storage Classes:

- **S3 Standard**
  - Frequently accessed data (more than once a month) with milliseconds access.
- **S3 Intelligent-Tiering**
  - Data with changing or unknown access patterns.
- **S3 Standard-IA**
  - Infrequently accessed data (once a month) with milliseconds access.
- **S3 One Zone-IA**
  - Re-creatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access

Amazon S3 Storage Classes:

- **S3 Glacier Instant Retrieval**
  - Long-lived archive data accessed once a quarter with instant retrieval in milliseconds.
- **S3 Glacier Flexible Retrieval (formerly known as "Glacier")**
  - Long-lived archive data accessed once a year with retrieval of minutes to hours.
- **S3 Glacier Deep Archive**
  - Long-lived archive data accessed less than once a year with retrieval of hours.

Amazon S3 Standard (S3 Standard)

- Low latency and high throughput performance
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Designed for 99.99% availability over a given year
- Backed with the Amazon S3 SLA for availability
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

- S3 Intelligent-Tiering is the first cloud storage that automatically reduces your storage costs on a granular object level by automatically moving data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead.
  - ✓ The Infrequent Access tier saves up to 40% on storage costs
  - ✓ The Archive Instant Access tier saves up to 68% on storage costs
  - ✓ Deep Archive Access tier has the same performance as Glacier Deep Archive and saves up to 95% for rarely accessed objects
  - ✓ Designed for durability of 99.999999999% of objects across multiple Availability Zones and for 99.9% availability over a given year
  - ✓ Objects smaller than 128KB can be stored in S3 Intelligent-Tiering but will always be charged at the Frequent Access tier rates, and are not charged the monitoring and automation charge.

Amazon S3 Standard-IA

- S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed.
- Same low latency and high throughput performance of S3 Standard
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Data is resilient in the event of one entire Availability Zone destruction
- Designed for 99.9% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

AWS Storage logging and monitoring

Automated monitoring tools

- **Amazon CloudWatch metrics for Amazon S3**
  - Tracks health of S3 resources and configure billing alerts when it reaches defined threshold.
- **AWS CloudTrail**
  - Record actions taken by a user, a role, or an AWS service in Amazon S3.
  - CloudTrail logs provide you with detailed API tracking for S3 bucket-level and object-level operations.

AWS Storage logging and monitoring

Manual monitoring tools

- **Server access logging**
  - Get detailed records for the requests that are made to a bucket.
  - You can use server access logs for many use cases, such as conducting security and access audits, learning about your customer base, and understanding your Amazon S3 bill.
- **AWS Trusted Advisor**
  - Evaluate your account by using AWS best practice checks to identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas.

Amazon Identity & Access Management (IAM)

- Identity & Access Management.
- It helps in securely connect & access AWS resources.
- You can centrally manage permissions for users to access resources.
- Takes care of authentication & authorization.
- For accessing IAM:
  - ✓ AWS Management Console
  - ✓ AWS Command Line Tools
  - ✓ AWS SDKs
  - ✓ IAM Query API


That's all Folks!