

TECHNOLOGY



Designing Applications and Architectures in AWS

(Aligned with AWS Solution Architect Associate Certification)

AWS Overview



A Day in the Life of a Cloud Architect

You are a cloud architect in an organization and have been asked to implement a solution in the AWS cloud. As a beginner in AWS, focus on AWS's core services, such as computing, storage, databases, networking services, and more.

You must set up an AWS account and use the AWS CLI to interact with AWS services and resources. Additionally, learn how to securely regulate access to AWS resources using AWS Identity and Access Management (IAM).

To achieve these, you will learn a few concepts in this lesson that will help you find a solution for the given scenario.



Learning Objectives

By the end of this lesson, you will be able to:

- Set up an AWS account, enabling access to and utilization of AWS services
- Configure billing alerts to monitor AWS charges for cost control and budget management
- Delegate access using IAM roles to enhance security and permissions management
- Set up and work with an AWS CLI for efficient interaction with AWS services



TECHNOLOGY

AWS Infrastructure

AWS Infrastructure

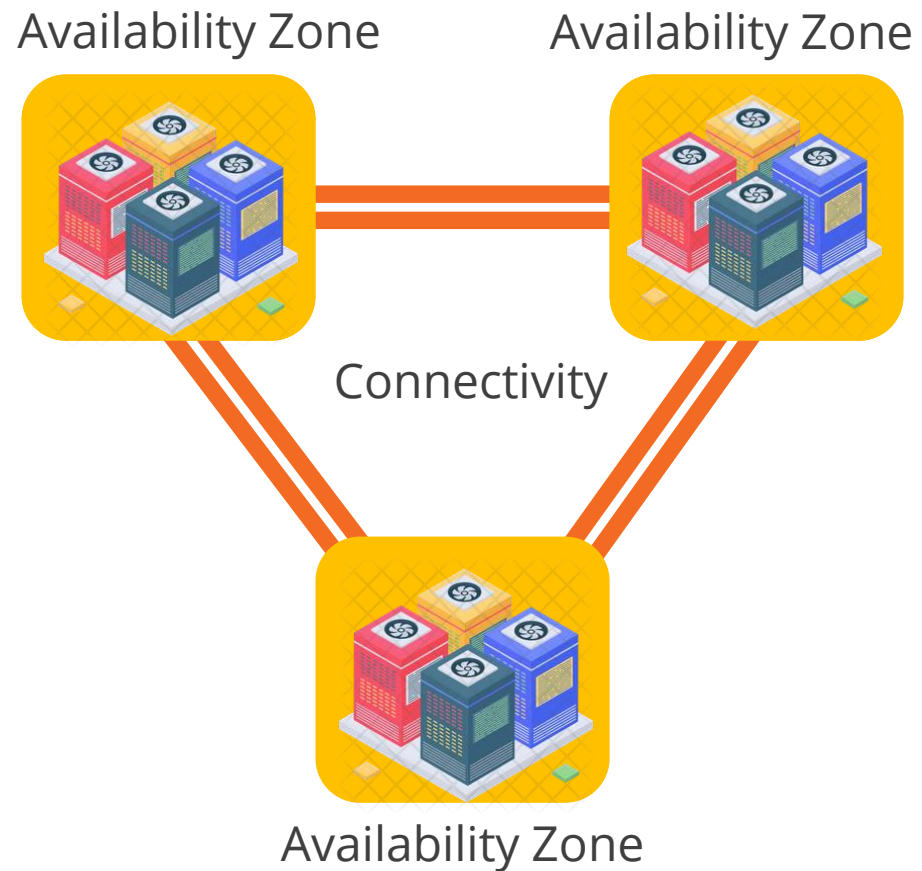
The AWS Global Cloud infrastructure offers unmatched security, broad reach, and reliability. As a cloud platform, it features over 200 services supported by data centers worldwide.



AWS Infrastructure

The foundation of the AWS Cloud Infrastructure lies in its Availability Zones and AWS Regions.

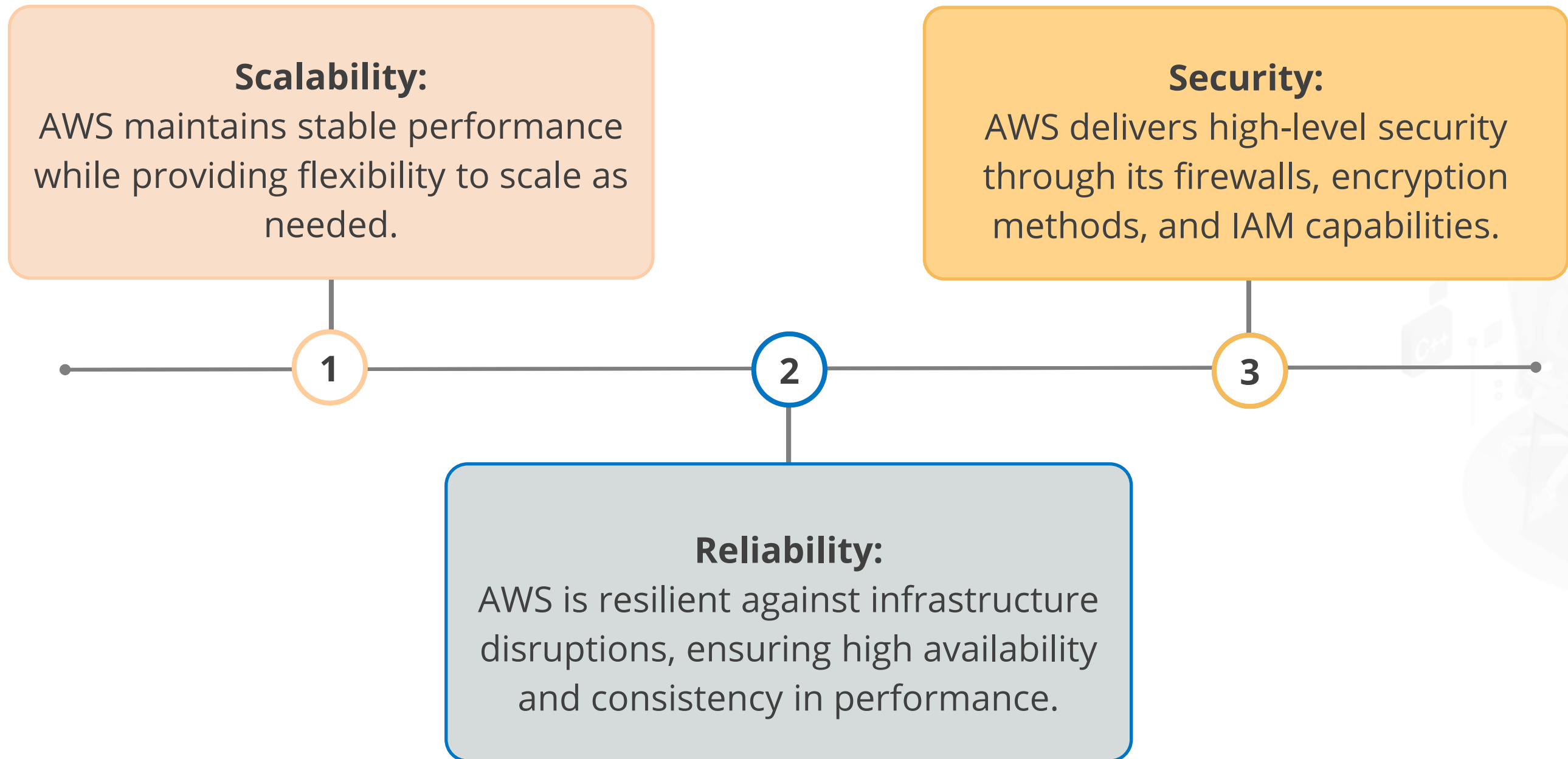
AWS Region



- An AWS Region corresponds to a geographical area housing multiple Availability Zones.
- Each Availability Zone comprises one or more separate data centers, each equipped with sufficient power, network setup, and reliable connections within distinct zones.

AWS Infrastructure

The AWS infrastructure offers the following benefits:



AWS Infrastructure

The AWS infrastructure offers the following benefits:

Performance Efficiency:

AWS efficiently runs services on a scalable cloud platform, managing traffic effortlessly with load balancers.

4

Cost Optimization:

AWS helps achieve business goals at minimum cost by optimizing expenses effectively with a pay-as-you-go model.

6

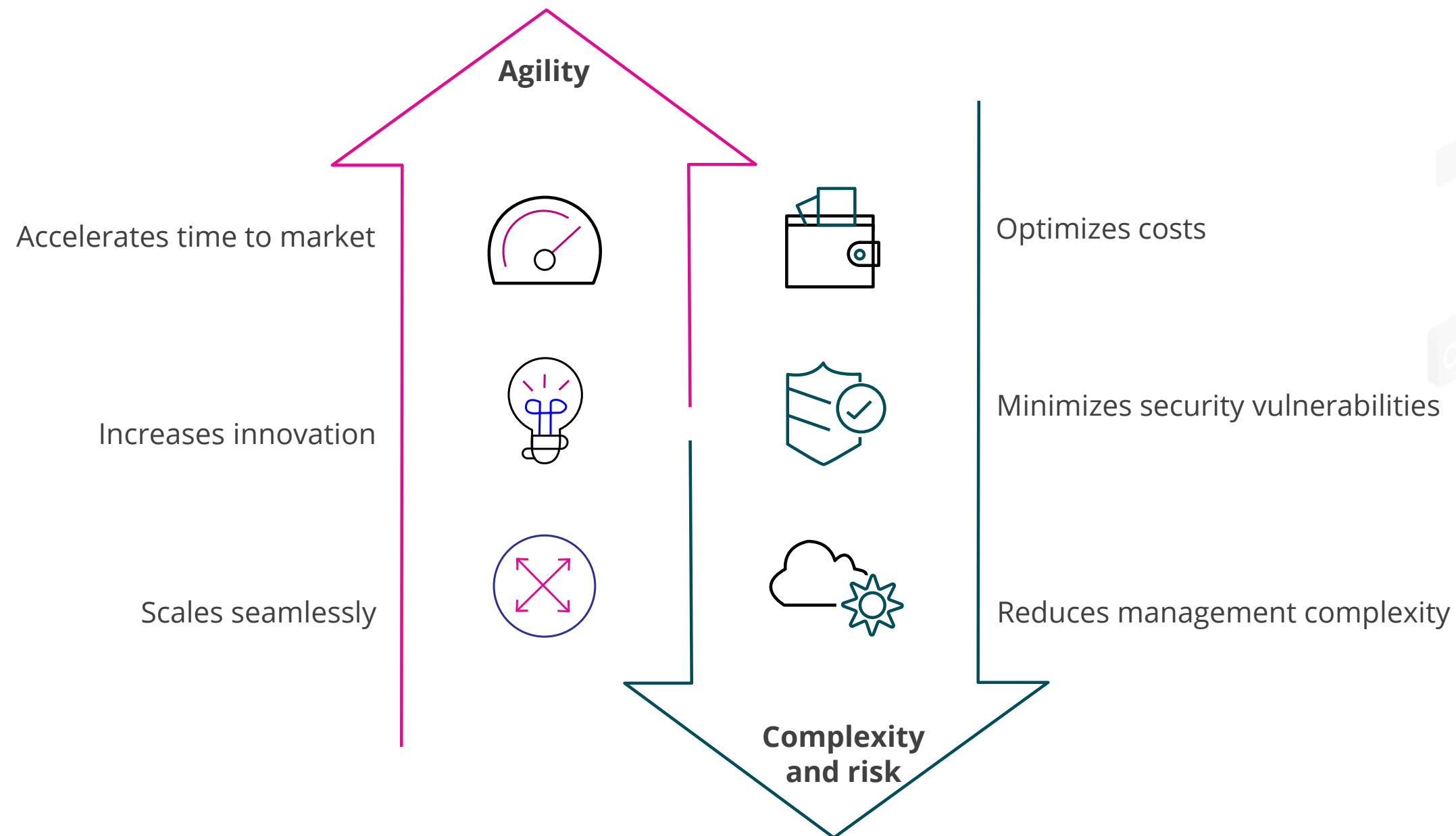
5

Flexibility

AWS allows the selection of your preferred operating system, programming language, and database.

AWS Infrastructure

Consumers choose AWS to enhance agility, reduce complexity, and mitigate risks, as it provides a wide range of services that can be easily configured.



TECHNOLOGY

AWS Core Services

Core AWS Services

Amazon offers various services that are broadly categorized into the following categories:



Compute



Storage



Database



Analytics



Networking



Mobile



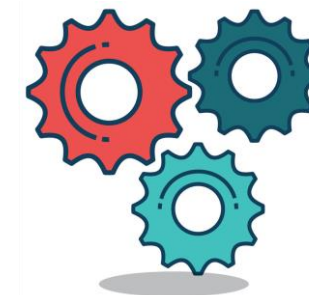
Developer tools



IoT



Security



Management tools



Enterprise applications

Compute Services

Compute services offer secure and resizable computing capacity in the cloud, simplifying web-scale computing for developers.



Here are some key features:

- They empower users to control their computing resources.
- They operate under a pay-as-you-go model, allowing users to boot new server instances within minutes.
- They enable quick scaling to meet changing computing requirements with quick and easy configuration of the services.

Compute Services

The following are some of the majorly used AWS compute services:



Amazon EC2



Amazon ECR



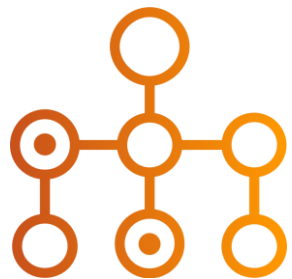
Amazon ECS



Amazon EKS



Amazon
Lightsail



AWS Batch



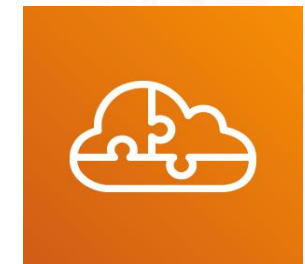
AWS Elastic
Beanstalk



AWS Fargate



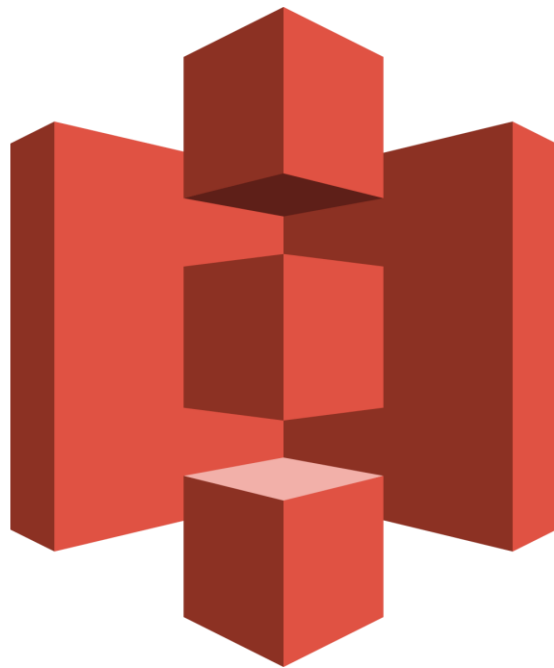
AWS Lambda



AWS Serverless
Application
Repository

Storage Services

The storage services offer a secure, reliable, and scalable storage solution for data in the AWS cloud, providing high efficiency, availability, durability, and performance.



The following are the features of the storage services:

- It allows users to store, access, and analyze data to reduce costs, increase agility, and accelerate innovation.
- It can be broadly categorized into object storage, file storage, block storage, and backup and data migration.

Storage Services

The following are some of the majorly used AWS storage services:



Amazon S3



Amazon EFS



Amazon FSx



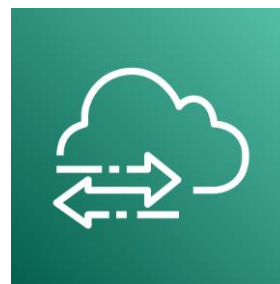
Amazon EBS



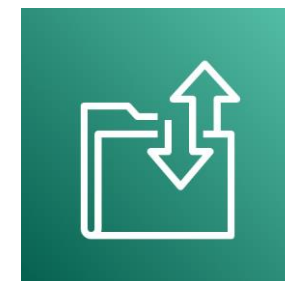
AWS Backup



AWS Storage
Gateway



AWS
DataSync



AWS Transfer
Family



AWS Snow
Family

Database Services

Amazon offers a comprehensive selection of purpose-built databases to suit various application needs.



These database services are fully managed, scalable, and highly efficient.



Database Services

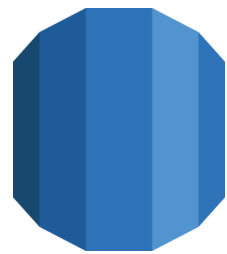


Database services have the following features:

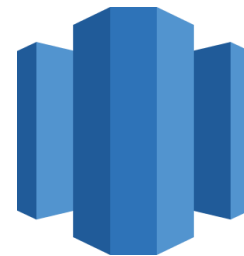
- They offer various types of database engines, including relational, key-value, in-memory, graph, time-series, and ledger.
- They support multi-region and multi-master replication, offering control over the data.

Database Services

The following are some of the majorly used Amazon database services:



Amazon
RDS



Amazon
Redshift



Amazon
DynamoDB



Amazon
ElastiCache



Amazon
DocumentDB



Amazon
Keyspaces



Amazon
Neptune



Amazon
QLDB



Networking Services

Amazon offers a broad set of networking services that provide essential security features and robust network solutions.



These services isolate resources, encrypt data, and provide private connections on the AWS global network.



Networking Services



The features of networking services are as follows:

- It offers the highest network availability, with very few downtime hours due to networking issues.
- It provides global coverage of 31 AWS Regions and 99 Availability Zones.

Networking Services

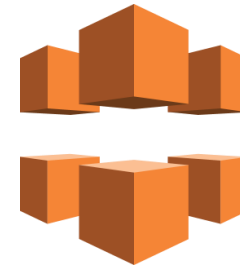
The following are some of the Amazon networking services:



Amazon
VPC



Amazon API
Gateway



Amazon
CloudFront



Amazon
Route 53



AWS VPN



AWS Direct
Connect



AWS Cloud
Map



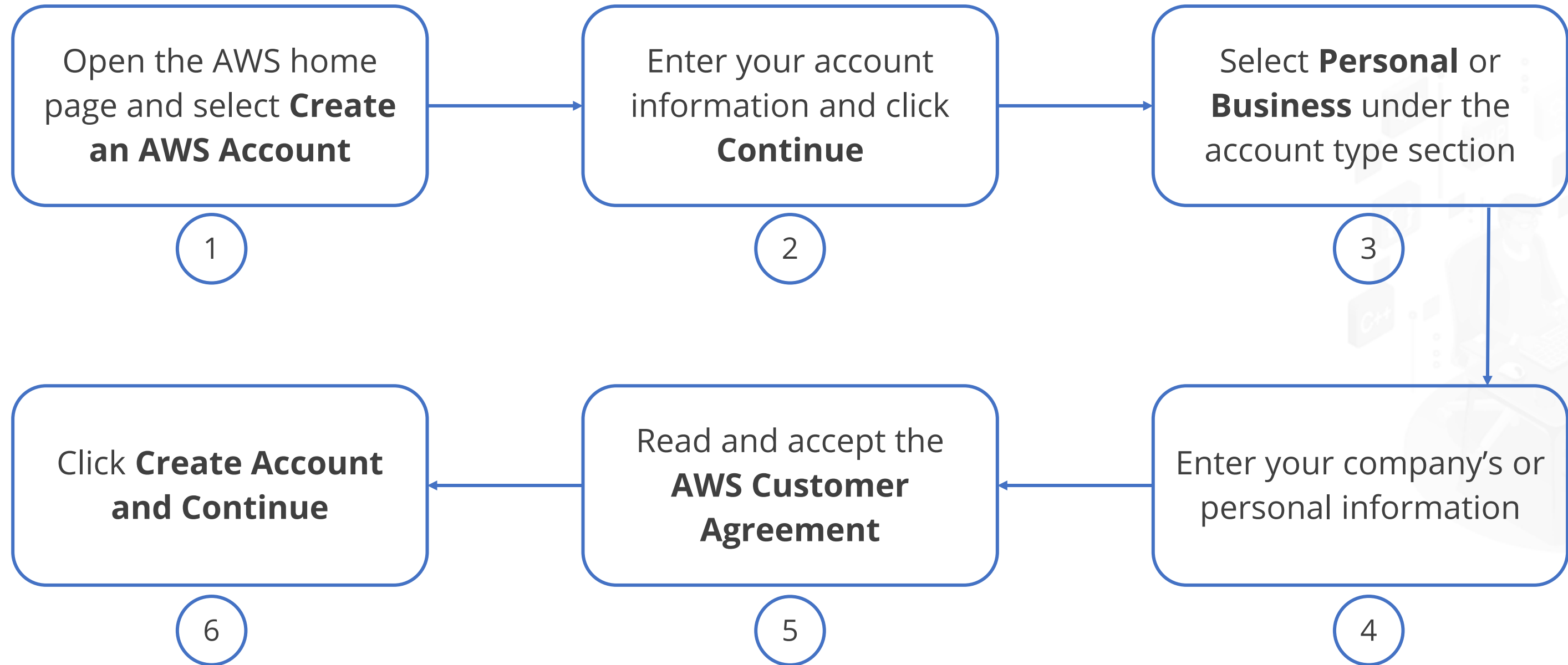
AWS App
Mesh



AWS Account Set Up

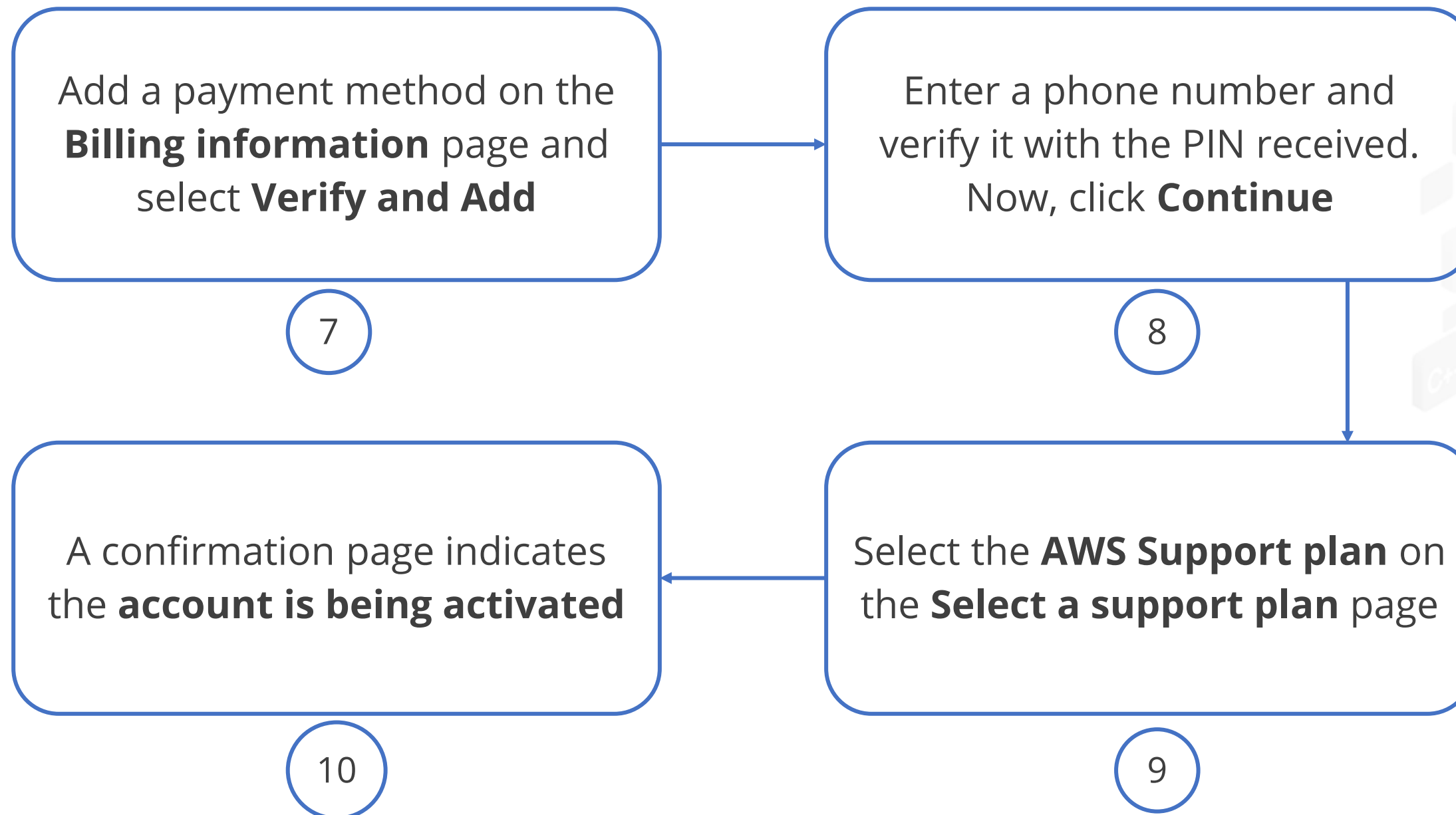
AWS Sign Up

The following are the steps to set up an AWS Account:



AWS Sign Up

The following are the steps to set up an AWS Account:



AWS Free Tier

The AWS Free Tier permits users to test numerous AWS services at no cost within certain usage limits.



- Upon creating an AWS account, users are automatically enrolled in the AWS Free Tier for 12 months.
- During this free tier period, users can utilize up to 750 Amazon EC2 Linux micro instance hours across all regions and 5 GB of Amazon S3 standard storage at no cost.

AWS Free Tier

The AWS Free Tier offers three types of packages:



12-Month Free Tier



Always Free

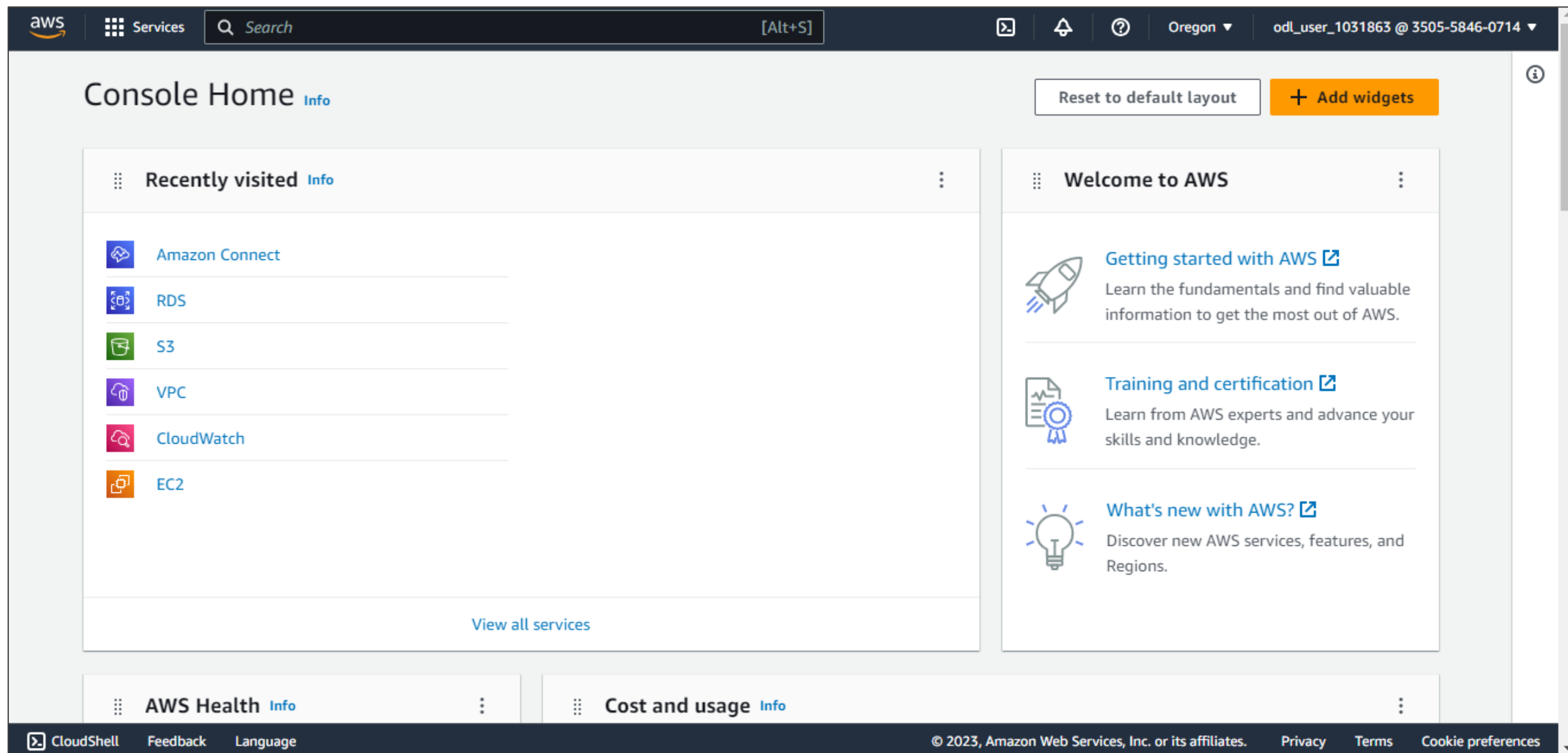


Short-Term Trials

Introduction to AWS Management Console

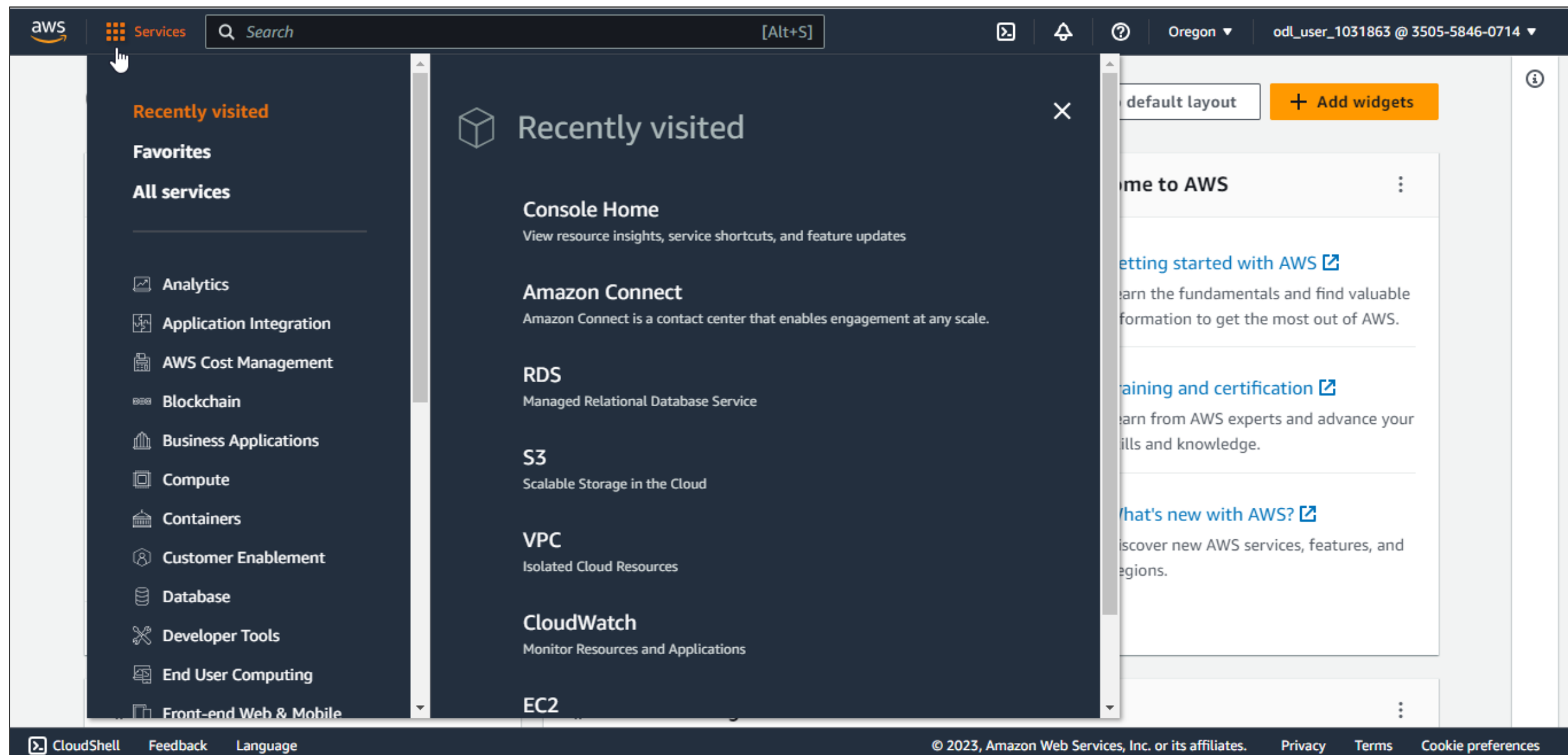
AWS Management Console

The AWS Management Console is a web application. It offers a broad set of service consoles for managing Amazon Web Services.



AWS Management Console

The home page of the AWS Management Console has access to each service console, like Amazon S3, EC2, CloudFront, and others.



AWS Management Console

AWS Resource Groups menu allows users to manage AWS resources, such as EC2 instances or S3 buckets, collectively as a group.

The screenshot displays the AWS Management Console interface for creating a new resource group. The left sidebar shows the 'AWS Resource Groups' menu with options for 'Resources' (Create Resource Group, Saved Resource Groups) and 'Tagging' (Tag Editor, Tag Policies). The main content area is titled 'Create query-based group' and includes a breadcrumb trail: 'AWS Resource Groups > Saved resource groups > Create new group'.

Create query-based group

Group type
Select a group type to define a group based on resource types and tags, or create a group based on your existing CloudFormation stack.

- ☒ **Tag based**
Group resources by specifying tags that are shared by the resources.
- ☐ **CloudFormation stack based**
Create a resource group based on an existing CloudFormation stack. The group will have the same logical structure as the stack.

Grouping criteria
Define a group based on resource types and tags.

Resource types
Select resource types

All supported resource types

Tags

Tag key Optional tag value Add

Preview group resources

AWS Management Console

Users can also use the Resource Groups menu to access the Tag Editor, a tool for managing and applying labels or tags to organize resources.

AWS Resource Groups

Resources

Create Resource Group

Saved Resource Groups

Tagging

Tag Editor

Tag Policies

Tag Editor

Find resources to tag

You can search for resources that you want to tag across regions. Then, you can add, remove, or edit tags for resources in your search results. [Learn more](#)

Regions

Select regions

us-east-1

Resource types

Select resource types

Tags – Optional

Tag key

Optional tag value

Add

Type the tag key and optional values shared by the resources you want to search for, and then choose Add or press Enter.

Search resources

©Simplilearn. All rights reserved.

simplilearn

AWS Billing

AWS Billing

The AWS Billing Console provides tools for:

- Paying the AWS bills
- Organizing and reporting your AWS costs and usage
- Managing consolidated billing for the members of AWS Organizations



Features of Billing



1. Managing an AWS account

It includes changing the default currency, adding or removing Regions, altering the tax information, and closing the AWS account.

2. Viewing the bill

It provides a section that describes how to view the bills, generate PDF copies of the charges, and set up monthly email notifications to receive the invoices.



Features of Billing



3. Managing the payments

It enables users to view estimated bills and pay AWS invoices in the desired currency by setting up a payment currency.

4. Managing the purchase orders

It allows users to perform self-service management of AWS purchase orders, allowing them to handle multiple purchase orders in one place.



Features of Billing



5. Managing the costs

It allows users to efficiently manage AWS costs with AWS Cost Categories by classifying the cost and usage into meaningful categories.

6. Managing the payment profiles

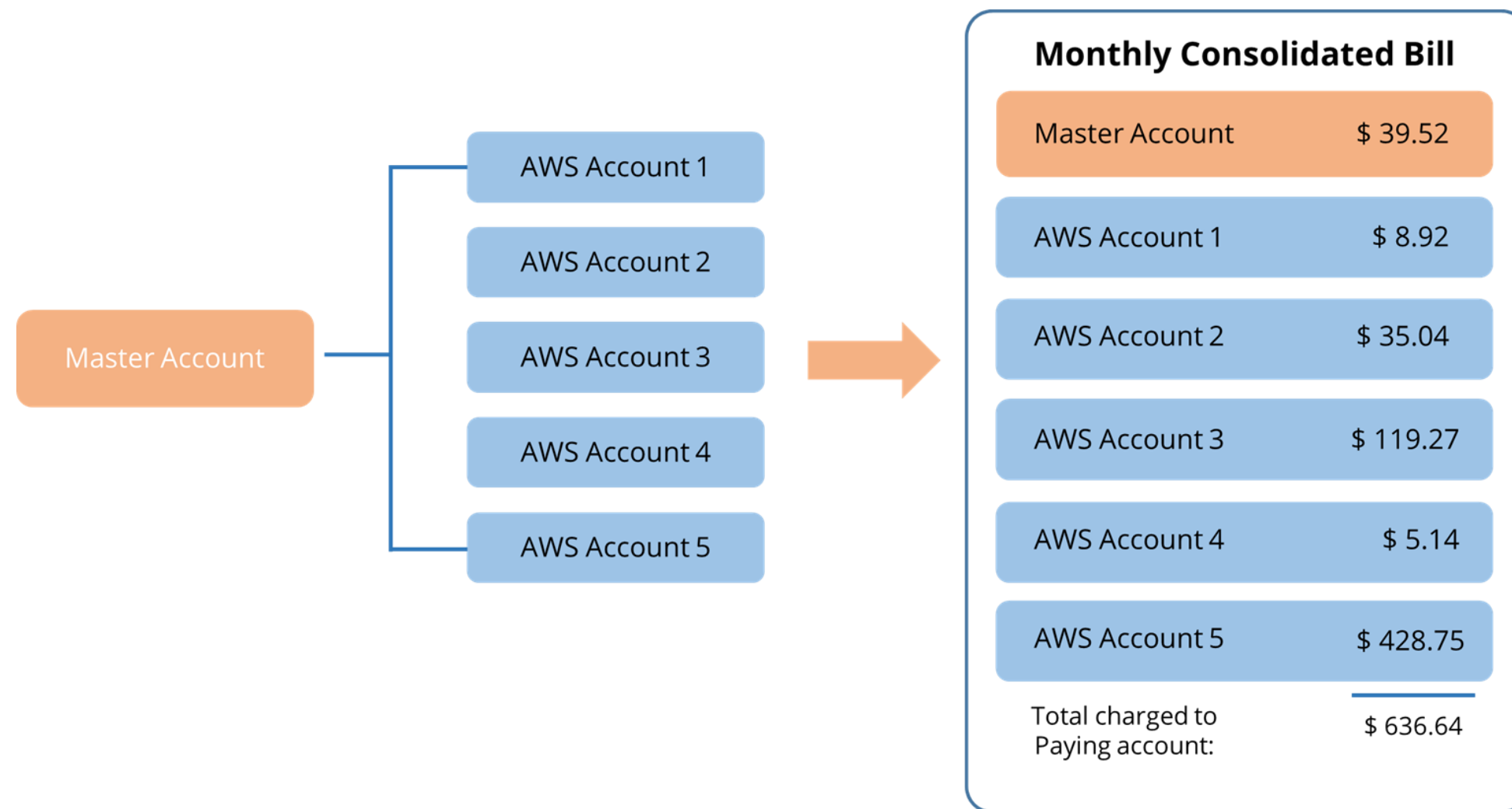
It allows users to utilize payment profiles, enabling them to assign multiple payment methods to their automatic payments.



Features of Billing

7. Consolidate billing for AWS Organizations

It enables users to use the AWS Organizations' consolidated billing feature to consolidate billing and payment for numerous AWS accounts or multiple Amazon Internet Services Pvt. Ltd. (AISPL) accounts.



TECHNOLOGY

AWS Support

AWS Support



- AWS Support provides a variety of plans that allow access to tools and expertise that support the success and operational health of AWS solutions.
- All support plans provide 24x7 access to customer service, AWS documentation, technical papers, and support forums.

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
AWS Trusted Advisor Best Practice Checks	Service Quota and basic Security checks	Full set of checks	Full set of checks	Full set of checks
Technical Support	<ul style="list-style-type: none">• Web access to Cloud Support Associates during business hours• Unlimited cases with 1 primary contact• Prioritized responses on AWS re:Post	<ul style="list-style-type: none">• 24/7 phone, web, and chat access to Cloud Support Engineers• Unlimited cases and unlimited contacts (IAM supported)• Prioritized responses on AWS re:Post• Access to AWS Support App in Slack	<ul style="list-style-type: none">• 24/7 phone, web, and chat access to Cloud Support Engineers• Unlimited cases and unlimited contacts (IAM supported)• Prioritized responses on AWS re:Post• Access to AWS Support App in Slack	<ul style="list-style-type: none">• 24/7 phone, web, and chat access to Cloud Support Engineers• Unlimited cases and unlimited contacts (IAM supported)• Prioritized responses on AWS re:Post• Access to AWS Support App in Slack

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
AWS Trusted Advisor Priority	None	None	None	None
Case Severity or Response Times	<ul style="list-style-type: none">General guidance: < 24 hoursSystem impaired: < 12 hours	<ul style="list-style-type: none">General guidance: < 24 hoursSystem impaired: < 12 hoursProduction system impaired: < 4 hoursProduction system down: < 1 hour	<ul style="list-style-type: none">General guidance: < 24 hoursSystem impaired: < 12 hoursProduction system impaired: < 4 hoursProduction system down: < 1 hourBusiness-critical system down: < 30 minutes	<ul style="list-style-type: none">General guidance: < 24 hoursSystem impaired: < 12 hoursProduction system impaired: < 4 hoursProduction system down: < 1 hourBusiness/Mission-critical system down: < 15 minutes

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
Architectural Guidance	General	Contextual to your use cases	Consultative review and guidance based on your applications (one per year)	Consultative review and guidance based on your applications
Programmatic Case Management	None	AWS Support API	AWS Support API	AWS Support API

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
Third-Party Software Support	None	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting
Proactive Programs and Self Service	Access to Support Automation Workflows with prefixes AWS Support	<ul style="list-style-type: none">Access to Infrastructure Event Management for an additional feeAccess to Support Automation Workflows with prefixes AWS Support and AWS Premium Support	<ul style="list-style-type: none">Infrastructure Event Management (one per year)Access to Support Automation Workflows with prefixes AWS Support and AWS Premium Support	<ul style="list-style-type: none">Infrastructure Event ManagementAccess to proactive reviews, workshops, and deep divesAccess to Support Automation Workflows with prefixes AWS Support and AWS Premium Support

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
AWS Incident Detection and Response	None	None	None	Access to AWS Incident Detection and Response for an additional fee
AWS Managed Services	None	Access to AWS Managed Services (AMS) for an additional fee	Access to AWS Managed Services (AMS) for an additional fee	Access to AWS Managed Services (AMS) for an additional fee

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
Technical Account Management	None	None	A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts	Designated Technical Account Manager (TAM) to proactively monitor your environment to coordinate access to programs and AWS experts
Training	None	None	None	Access to online self-paced labs

AWS Support Plans Comparison

	Developer	Business	Enterprise On-Ramp	Enterprise
Account Assistance	None	None	Concierge Support Team	Concierge Support Team
Pricing	Greater of \$29 / month*** or 3% of monthly AWS usage	<ul style="list-style-type: none">Greater of \$100 / month*** or 10% of monthly AWS usage for the first \$0-\$10K7% of monthly AWS usage from \$10K-\$80K5% of monthly AWS usage from \$80K-\$250K3% of monthly AWS usage over \$250K	Greater of \$5,500 or 10% of monthly AWS usage	<ul style="list-style-type: none">Greater of \$15,000 or 10% of monthly AWS usage for the first \$0-\$150K7% of monthly AWS usage from \$150K-\$500K5% of monthly AWS usage from \$500K-\$1M3% of monthly AWS usage over \$1M

Billing Alerts

Billing Alerts

AWS billing alerts allow users to monitor the charges on their bill.

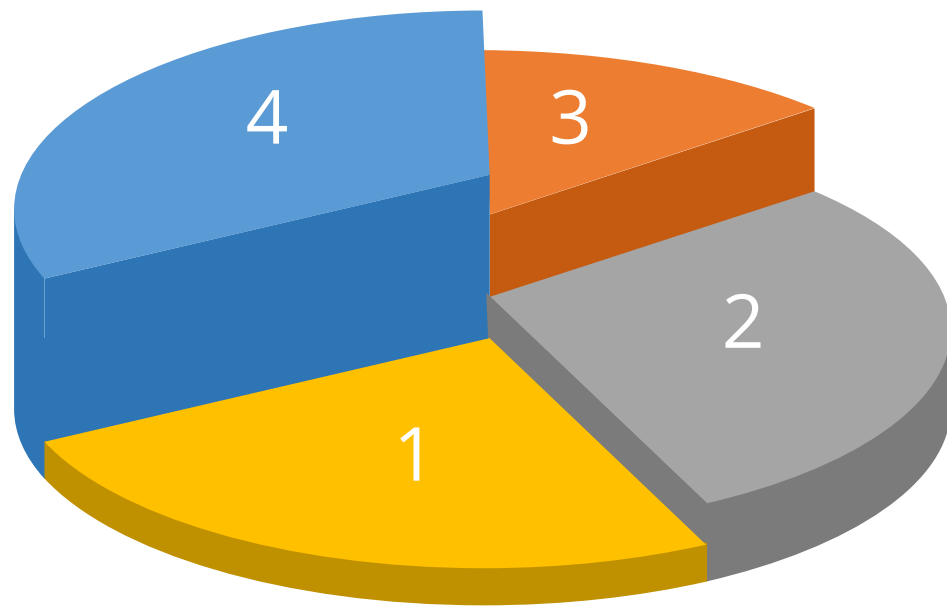


Users can set up an alert to receive e-mail notifications when estimated charges reach a specific threshold.



Billing Alerts

The steps to enable the monitoring of estimated charges are as follows:



- Open the **AWS Billing** console
- Choose **Billing Preferences** in the navigation pane
- Choose **Receive Billing Alerts**
- Choose **Save preferences**



Delegate Access

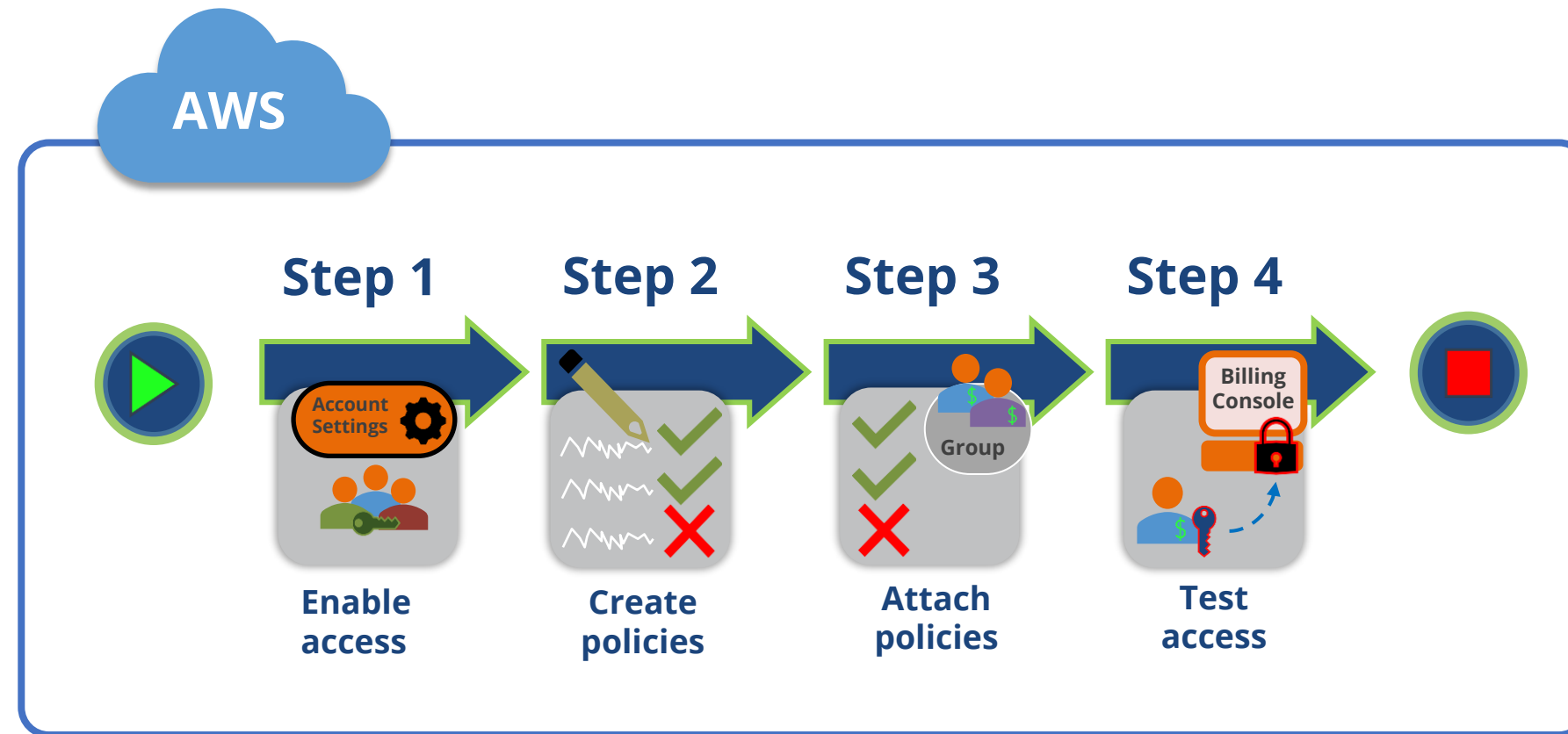
Delegate Access to the Billing Console

AWS account owners can delegate access to specific IAM users that need to access or manage the AWS Billing and Cost Management data for an AWS account.



Delegate Access to the Billing Console

The process of delegating access to the billing console consists of four key steps:



Workflow: Delegate Access to the Billing Console



Step 1: Activate access to billing data

- If the users create a single AWS account, only the AWS account owner can view and manage billing information.
- IAM users cannot access billing data until the account owner activates IAM access and attaches policies that provide billing actions to other users or roles.

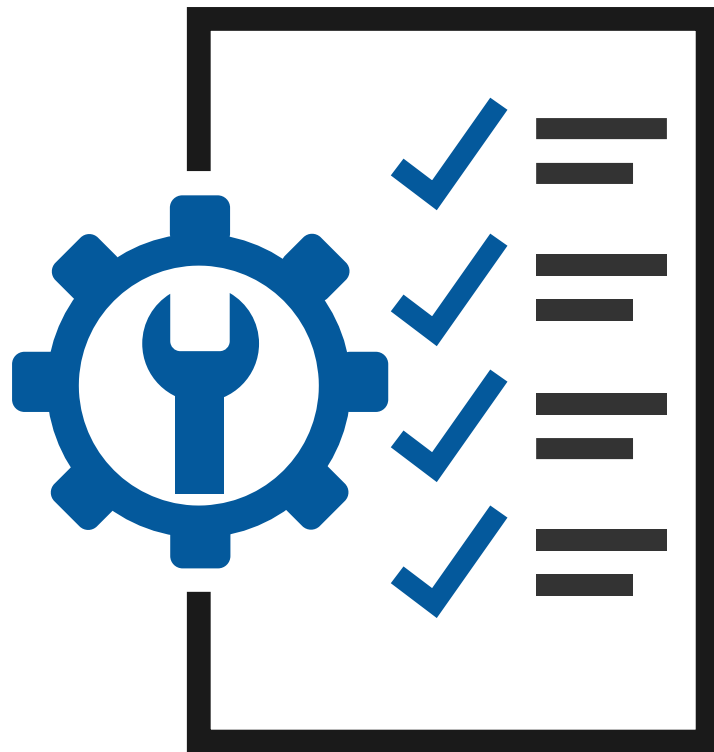
Workflow: Delegate Access to the Billing Console



Step 2: Create IAM policies

- The users must explicitly allow access to billing data to a particular IAM user or user group after enabling billing access on an account.
- The account owner grants access under a customer-managed policy.

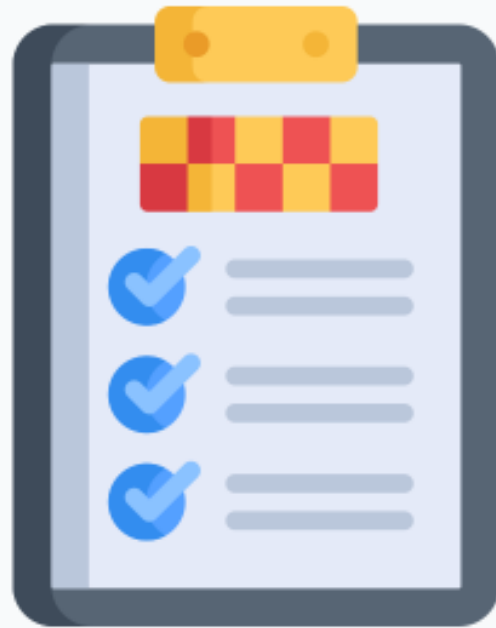
Workflow: Delegate Access to the Billing Console



Step 3: Attach billing policies

- When users assign a policy to a user group, all members of that user group are granted all the permissions associated with that policy.
- The account owner attaches the new billing policies to user groups containing only those users who require billing access.

Workflow: Delegate Access to the Billing Console



Step 4: Test access to the billing console

- Users must test the policy after completing the core tasks.
- It ensures that the policy works as intended.

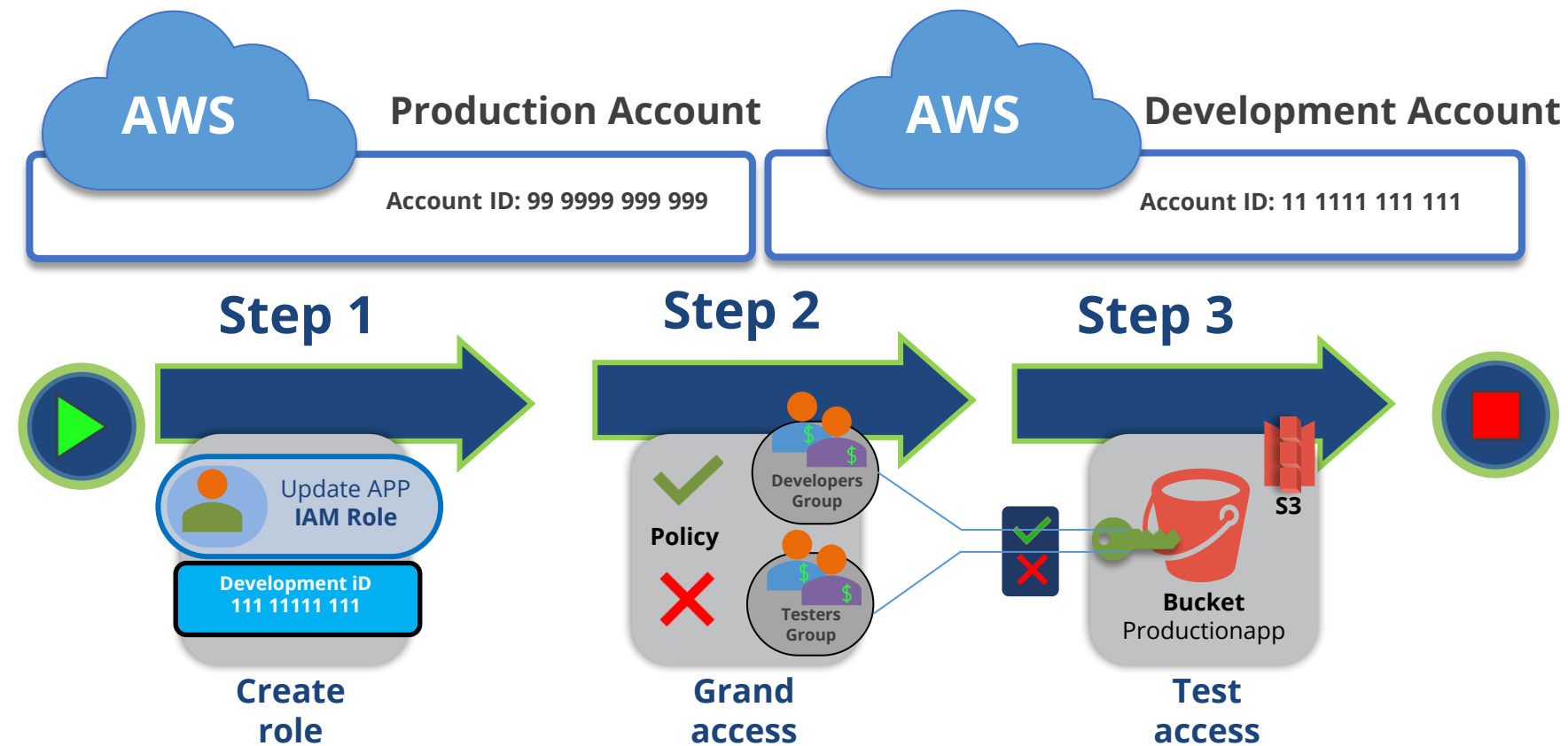
Delegate Access Using IAM Roles

AWS account owners can use a role to delegate access to resources in different AWS accounts called **Production** and **Development**.



Delegate Access Using IAM Roles

The process of delegating access using the IAM role consists of three key steps:



Workflow: Delegate Access Using IAM Roles



Step 1: Create a role in the Production account

The owners specify a permissions policy that permits trusted users to change the bucket in the Production account and define the Development account as a trusted entity when they create a role.

Workflow: Delegate Access Using IAM Roles



Step 2: Grant access to the role

- AWS account owners can modify the IAM user group policy to deny testers access to the role.
- The testers have **PowerUser** access in this scenario. Hence, the owners must explicitly deny the ability to use the role.

Workflow: Delegate Access Using IAM Roles



Step 3: Test access by switching roles

Finally, as a **Developer**, the AWS account owners use the role to update the bucket in the **Production** account.

AWS Identity and Access Management (IAM)

IAM

AWS Identity and Access Management (IAM) is a web service that enables users to securely regulate access to AWS resources.



IAM helps in determining the authentication (signed-in) and authorization (permissions) of users to utilize resources.



IAM Features



1. Shared access to the AWS account

Users can authorize others to administer and utilize resources in their AWS account without sharing their password or access key.

2. Granular permissions

Users can assign various permissions to multiple users for different resources.



IAM Features



3. Secure access to AWS resources

IAM features enable the secure provision of credentials for applications running on EC2 instances.

4. Multi-factor authentication (MFA)

Users can enhance security by enabling two-factor authentication for their accounts and individual users.



IAM Features

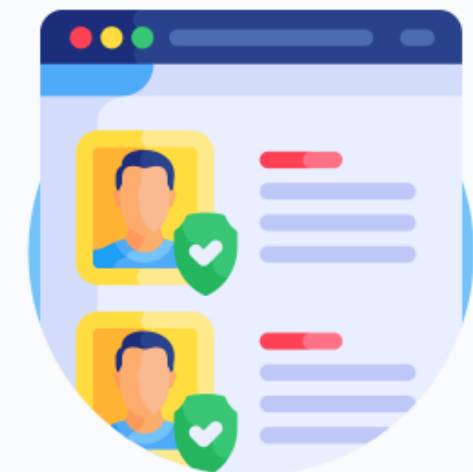


5. Identity federation

Users can provide temporary access to an AWS account for users who already have passwords elsewhere, such as their company network or an online identity provider.

6. Identity information for assurance

AWS CloudTrail offers log records that contain data about those who requested resources in the users' accounts.



IAM Features



7. PCI DSS compliance

IAM enables a merchant or service provider to process, store, and transmit credit card data compatible with the Payment Card Industry Data Security Standard (PCI DSS).

8. Integrated with many AWS services

Numerous AWS services support various IAM functions.



IAM Features



9. Consistent

IAM achieves high availability by replicating data across numerous servers located across Amazon's global data centers.

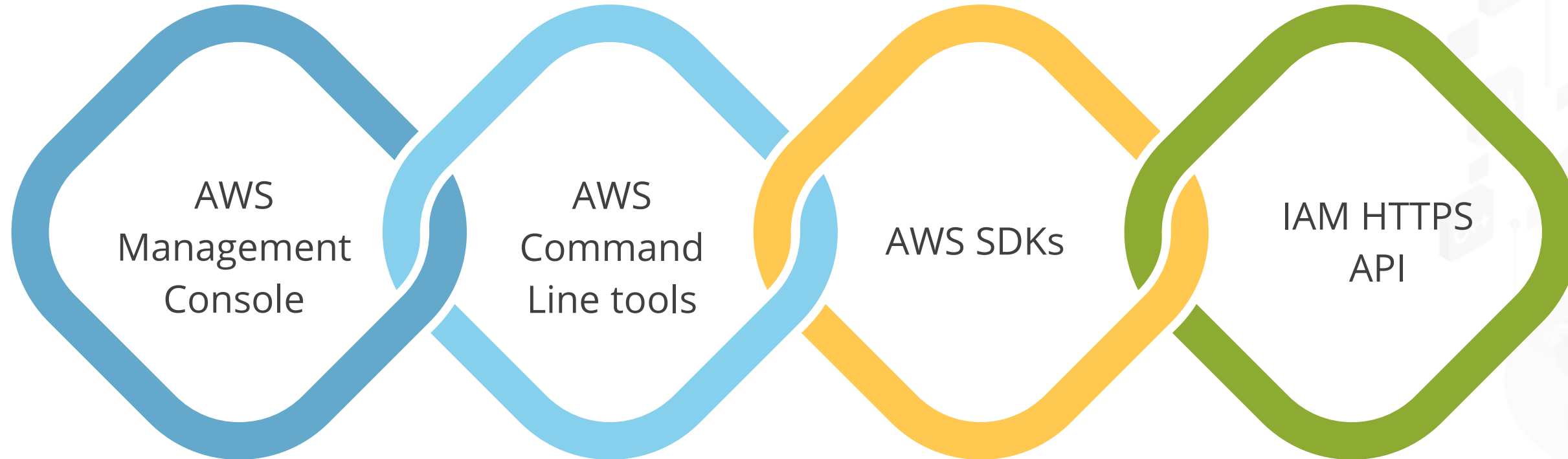
10. Free to use

AWS Identity and Access Management (IAM) and Security Token Service (AWS STS) are features of an AWS account offered at no extra cost.

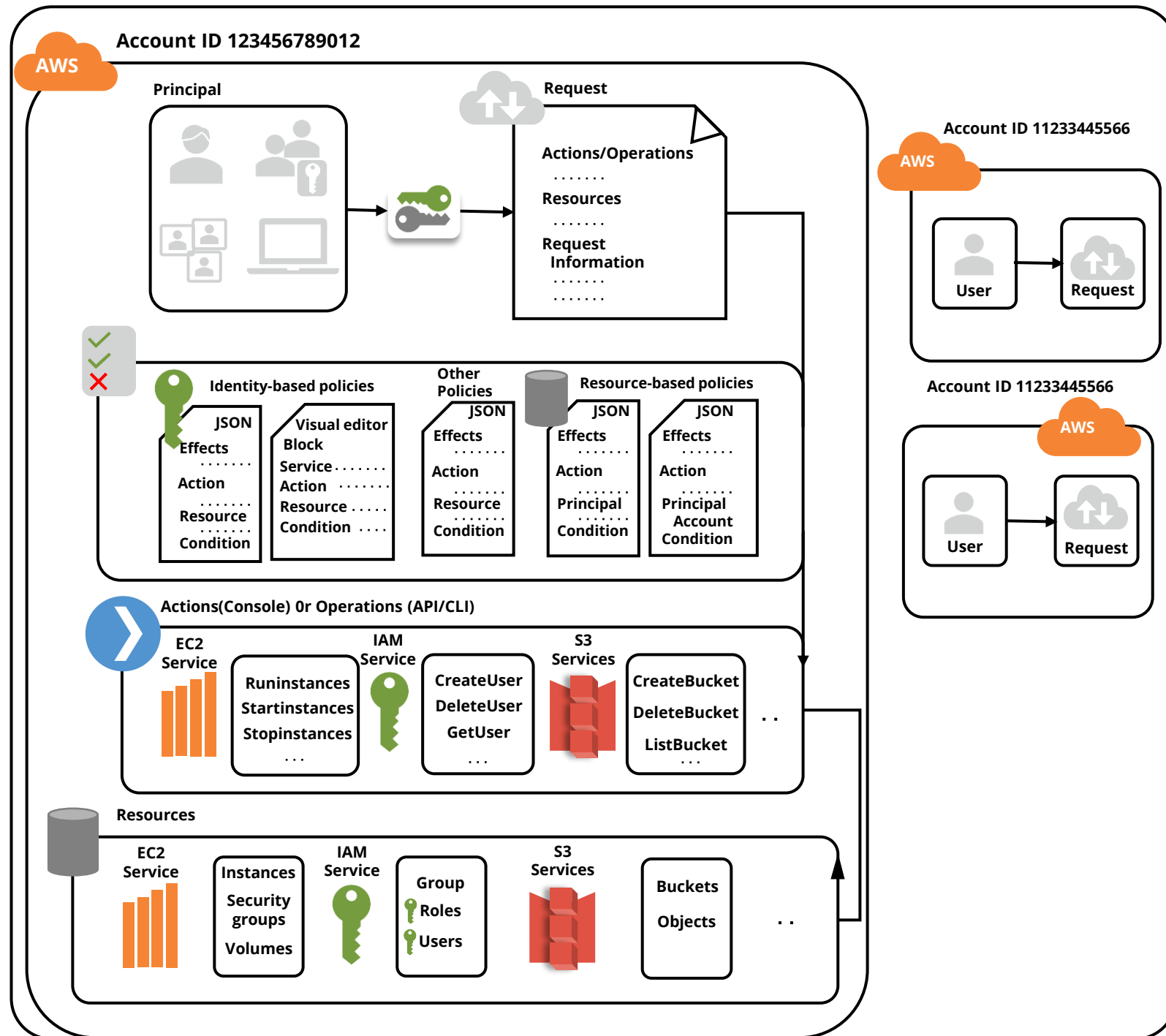


Accessing IAM

IAM can be accessed in any of the following ways:



Working of IAM



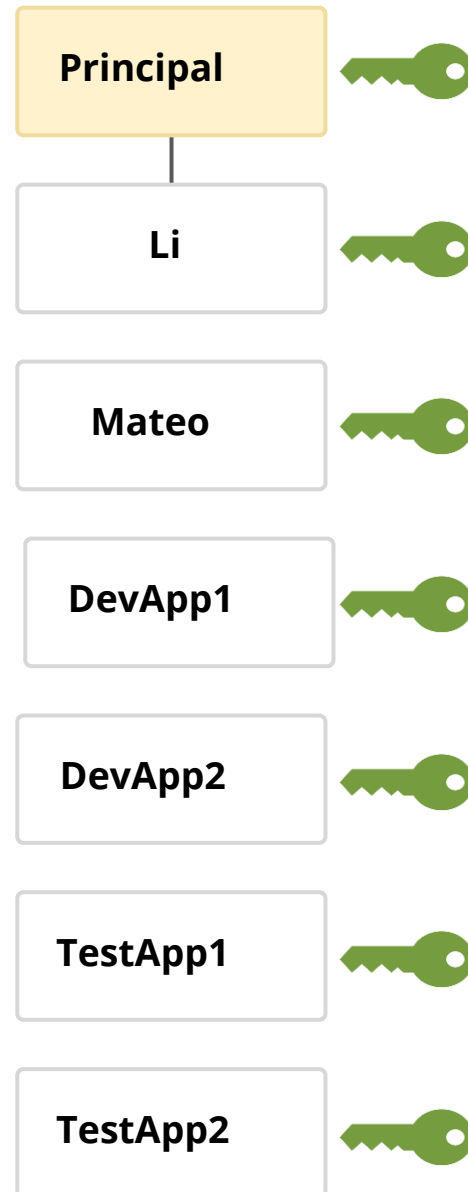
- IAM offers the infrastructure required to manage an account's authentication and authorization.
- The IAM infrastructure consists of the following components:
 1. IAM identities and entities
 2. Principal
 3. Request
 4. Authentication
 5. Authorization
 6. Actions or operations
 7. Resources

IAM Users

IAM users are users within an account, not separate accounts. Each user can have a password to access the AWS Management Console.



IAM Users



- IAM users can also provide everyone with their access key, allowing them to perform programmatic requests to operate with resources in their account.
- For example, users **Li**, **Mateo**, **DevApp1**, **DevApp2**, **TestApp1**, and **TestApp2** have been added to a single AWS account. Each user has their own set of credentials.

AWS Command Line Interface (AWS CLI)

AWS CLI

The AWS Command Line Interface (AWS CLI) is an open-source tool that allows users to communicate with AWS services using commands in their command-line shell.



AWS CLI: New Configuration Setup

The **aws configure** command is the quickest way to set up the AWS CLI installation.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

The AWS CLI prompts the users for the information which must be replaced with the user's credentials.

AWS CLI: Existing Configuration Setup

The AWS CLI can be used if the users already have configuration and credential files.

1

To use the **config** and **credentials** files, move them to the folder named **.aws** in your home directory.

2

The users can specify a non-default location for the **config** and **credentials** files by setting the **AWS_CONFIG_FILE** and **AWS_SHARED_CREDENTIALS_FILE** environment variables to another local path.

Key Takeaways

- Availability Zones include one or more distinct data centers with redundant power, networking, and connectivity in separate facilities.
- Users are automatically signed up for the AWS Free Tier for 12 months when they create an AWS account.
- The credentials for the applications running on EC2 instances can be securely provided using IAM features.
- Users can enable two-factor authentication for their accounts and specific users to increase security.



TECHNOLOGY

Thank You