Designing Applications and Architectures in AWS

(Aligned with AWS Solution Architect Associate Certification)

simplilearn

TECHNOLOGY

Security and IAM

simplilearn

A Day in the Life of Cloud Architect

You are a cloud architect in an organization and have been asked to address the pressing concerns surrounding security, data privacy, and recent financial losses attributed to cloud-based applications, particularly on AWS.

Your focus will be to implement proactive measures to prevent future failures.

This includes the implementation of robust threat detection mechanisms, enhancing the management of security protocols, and fortifying data privacy measures within the AWS accounts.

A Day in the Life of Cloud Architect

By conducting a comprehensive assessment of the current security landscape, you aim to design and implement strategies that mitigate risks, ensure compliance with industry standards, and safeguard sensitive data.

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

Learning Objectives

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

- Illustrate and configure models in AWS for resource optimization
- Define Identity and Access Management in AWS to enable resource management
- Protect the AWS accounts with intelligent threat detection using Amazon GuardDuty
- Manage data security and data privacy using AWS Macie

TECHNOLOGY

Responsibility Models in AWS

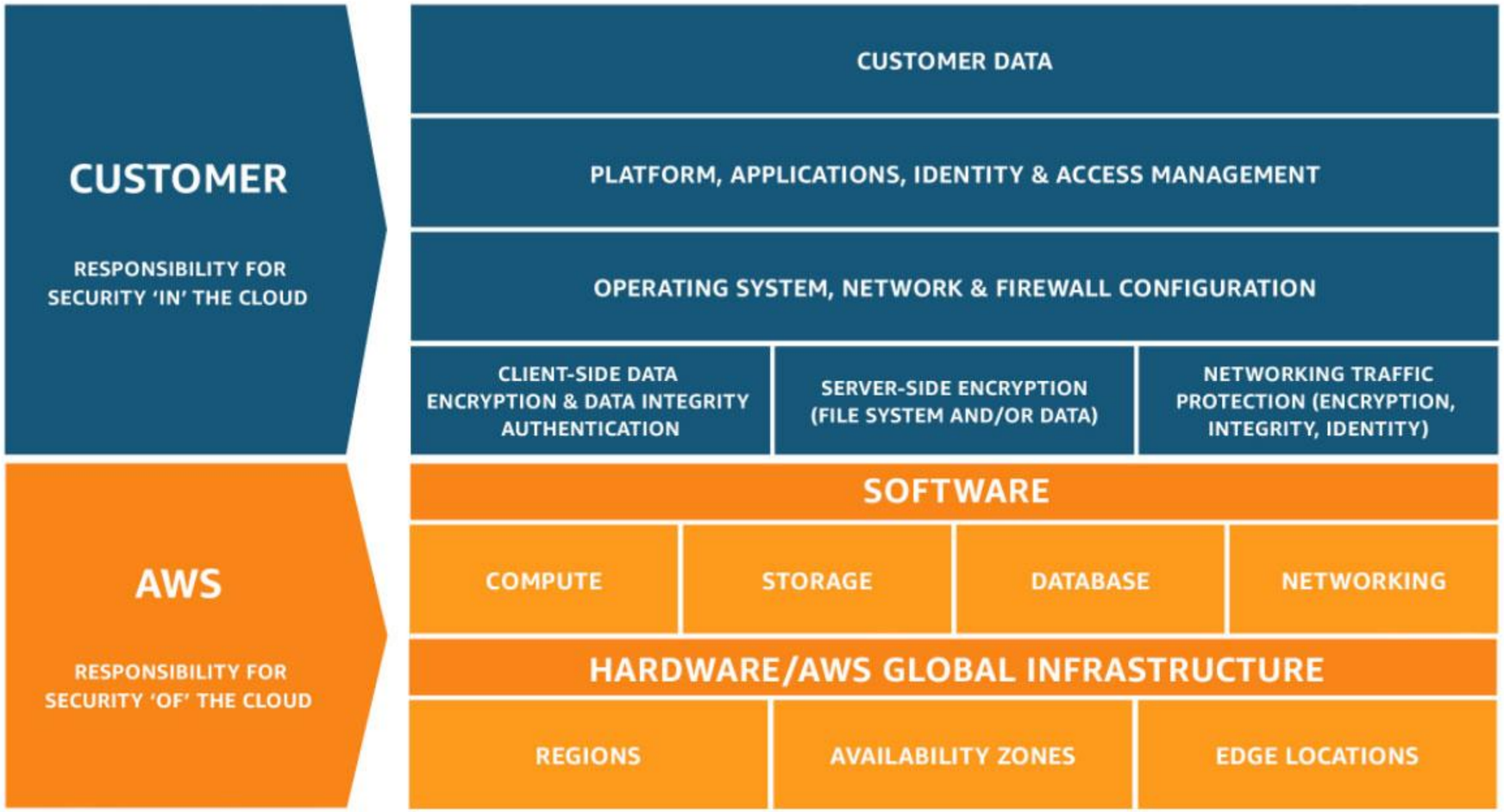
Shared Responsibility Model

AWS and the customer share responsibility for security and compliance.

- This shared approach helps reduce the operational load on the customer.
- AWS manages the host operating system, virtualization layer, and physical security of the buildings.

Shared Responsibility Model

Here is the working diagram of the AWS shared responsibility model:



Compliance Program

AWS and clients share compliance responsibilities when systems are built in the AWS Cloud.

- Customers can delve into the comprehensive security measures maintained by AWS.
- AWS Compliance Enablers bolster traditional programs by integrating governance-focused, audit-friendly service features aligned with relevant compliance standards.

AWS Artifacts

The following are the AWS artifacts:

- On-demand access to AWS
- Compliance reports
- Globally available
- Easy identification
- Quick assessments
- Continuous monitoring
- Enhanced transparency

Delegation

It is a crucial aspect of managing access and control in AWS, and it helps organizations efficiently distribute responsibilities while maintaining security and compliance.

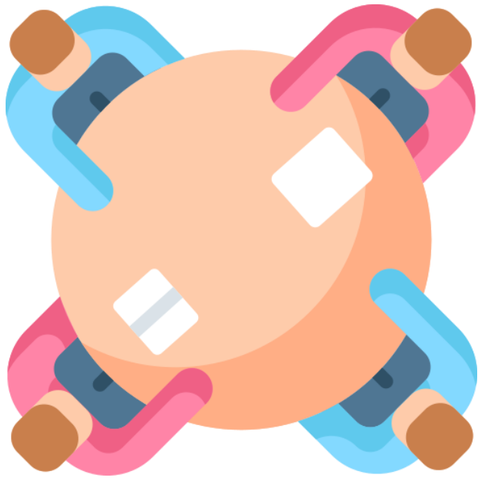
A registered member account is utilized for administrative AWS Single Sign-On (SSO) tasks.

The management account within AWS Organizations automatically generates an SSO instance.

The roles are easily managed across all member accounts within the organization using AWS.

Benefits of Delegation

Delegation in AWS offers the following benefits:



It reduces the need for numerous individuals to access the management account, helping to mitigate security risks.

It empowers a limited set of administrators to assign users and groups to applications and user accounts for organization members.

Federation

Identity federation is a trust-based system that connects two parties to authenticate users and transmit the necessary data to grant them access to resources.

Enabling Federated AWS Access

- Through federation, users can access their AWS accounts using single sign-on (SSO).
- Users can utilize AWS IAM to control fine-grained, federated access to AWS accounts.
- Users can enable federated access for user-facing mobile and online applications.

TECHNOLOGY

AWS IAM

Security Credentials

AWS offers a range of options to securely grant users access to their AWS resources, including:

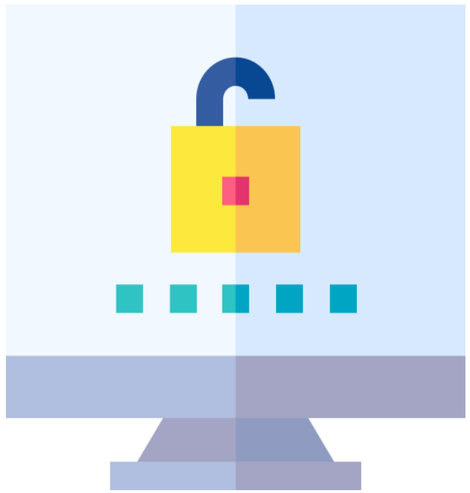
Email address and password:
They are used for signing into the AWS Console.

IAM username and password:
They provide access to an AWS account for diverse users and programs.

Access keys:
Access keys are utilized to authorize programmatic requests.

AWS Multi-Factor Authentication

Multi-factor authentication (MFA) adds a layer of security to the sign-in process.



It requires users to authenticate using an AWS-supported MFA method along with their sign-in credentials when accessing AWS services.

AWS Multi-Factor Authentication

The following AWS-supported MFA mechanisms are available:

Virtual MFA Devices

This type of MFA employs an application on a phone or other device to generate a six-digit numeric code.

U2F Security Key

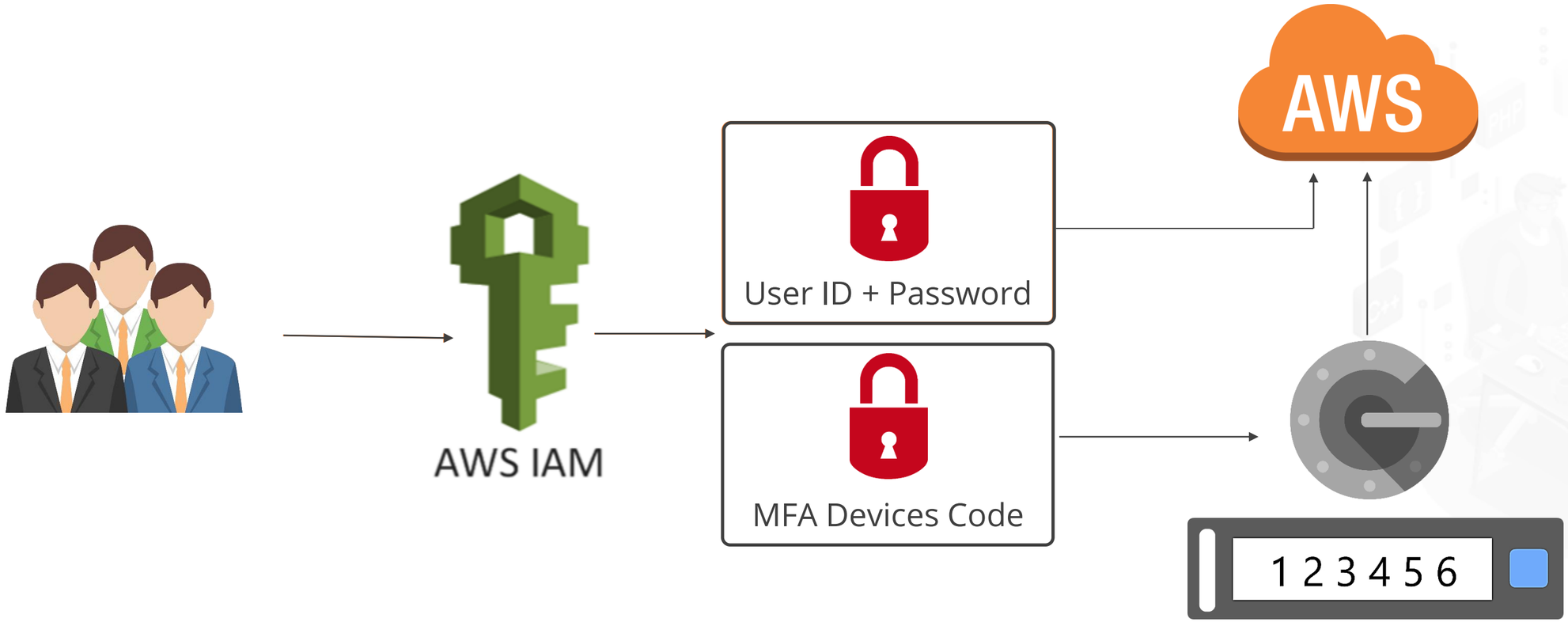
When a device is plugged into a USB port on the user's computer, the U2F security key serves as a form of MFA.

SMS Text Message-Based MFA

This MFA method involves adding the user's SMS-compatible cell phone number to the IAM user settings.

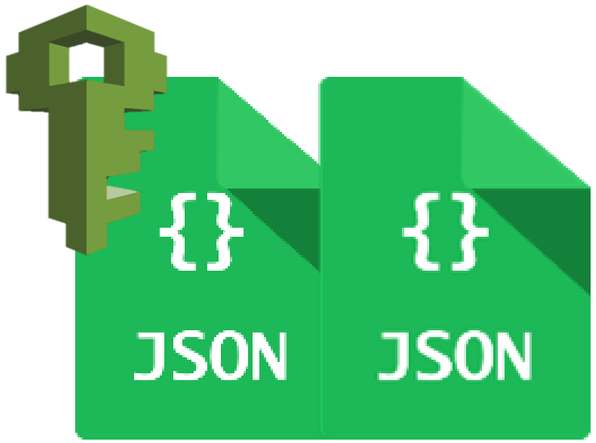
Multi-Factor Authentication

AWS IAM offers support for Multi-Factor Authentication (MFA), which ensures comprehensive security using MFA devices.



What Is IAM Policy?

An IAM policy is a document that defines individual or multiple permissions. These policies can be linked to users, groups, roles, and AWS resources, and are written in JSON format.



AWS IAM Policies

01 AWS provides a selection of predefined IAM Policies that users can choose from.

02 For increased customization, root users can modify these predefined policies.

03 Root users can create entirely new custom IAM policies from scratch.

Types of IAM Policies

Two types of IAM policies exist:

Identity-based policies

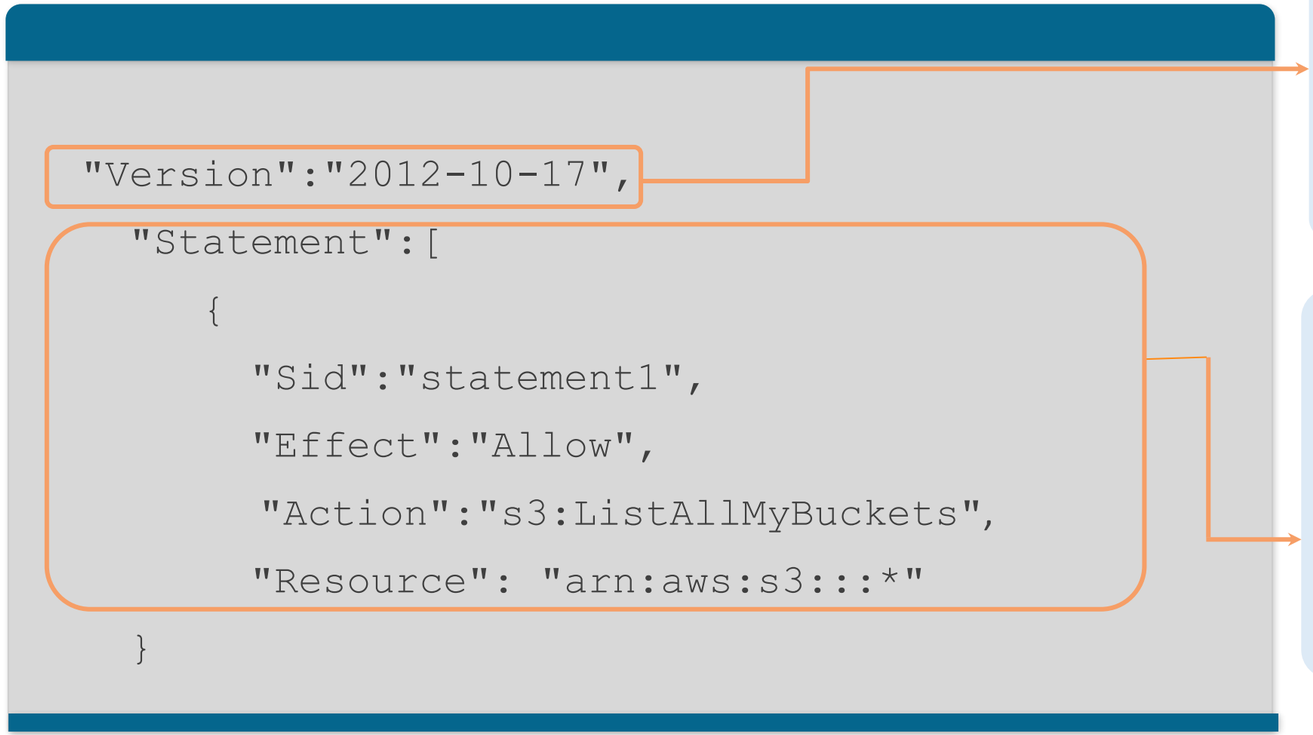
These policies can be directly linked to identities like users, groups, and roles.

Resource-based policies

These policies are attached to AWS resources such as Amazon S3, Amazon EC2, and more.

Syntax of Writing AWS IAM Policies

AWS policies are written using JavaScript Object Notation (JSON).



Policy-wide information:

Version: Date when the policy was created

One or more individual statements:

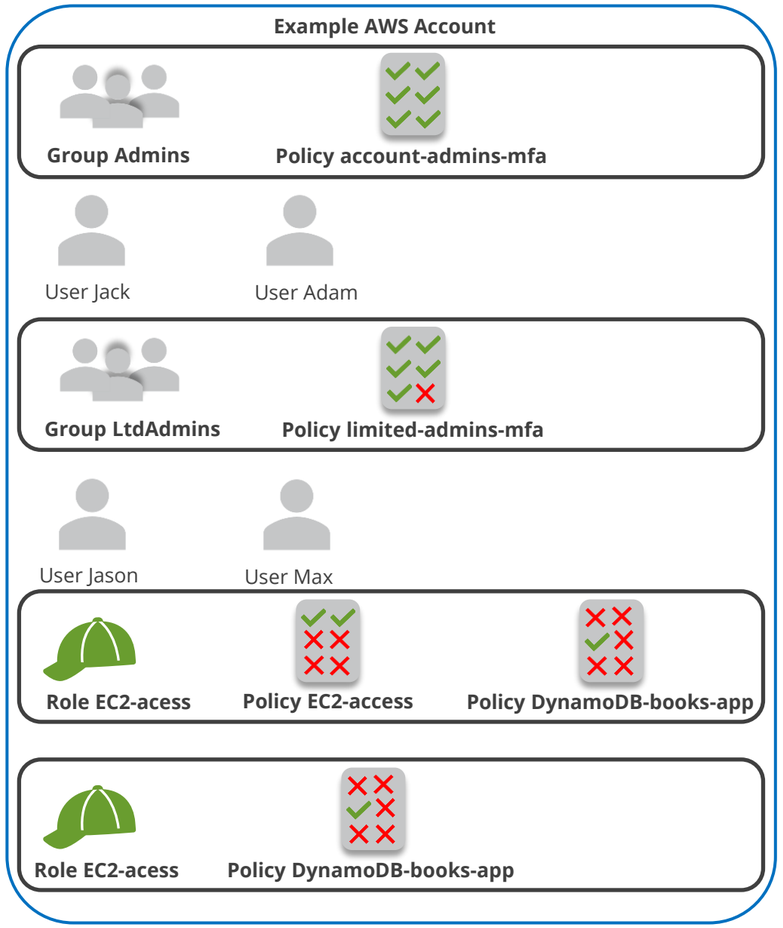
Effect: Allows permission
Action: Lists all the S3 buckets
Resource: Name of the S3 bucket

Inline Policy

An IAM identity can contain an inline policy, which is a policy directly embedded within the identity (user, group, or role).

Inline Policy

The following diagram explains inline policies:



Managed Policy

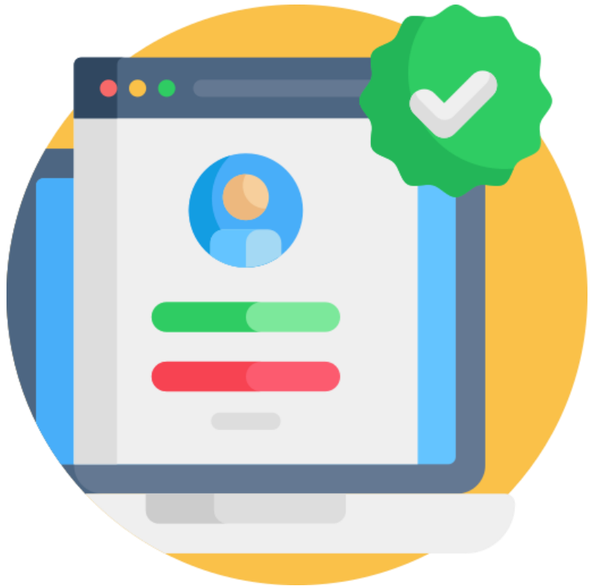
An AWS-managed policy is created and maintained by AWS as an independent policy.

Example:

```
arn:aws:iam::aws:policy/IAMReadOnlyAccess
```

Managed Policy

Managed policies assign the appropriate permissions to individuals, groups, and roles easily compared to user-written policies.



Amazon Resource Names (ARNs)

- AWS resources are uniquely identified by Amazon Resource Names (ARNs).
- When you need to specify a resource across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls, you must provide its ARN.

ARN Format

ARNs follow standard formats, and the specific format for a resource is specified by that resource itself.

```
arn:partition:service:region:account-id:resource-id
arn:partition:service:region:account-id:resource-type/resource-id
arn:partition:service:region:account-id:resource-type:resource-id
```

AWS Principals

The following principles are used in AWS:

01	AWS account and root user
02	IAM roles
03	Role sessions
04	IAM users

AWS Principals

The following principles are used in AWS:

05	Federated user sessions
06	AWS services
07	All principals

IAM Roles

These roles define permissions and policies that govern the access granted to AWS identities.

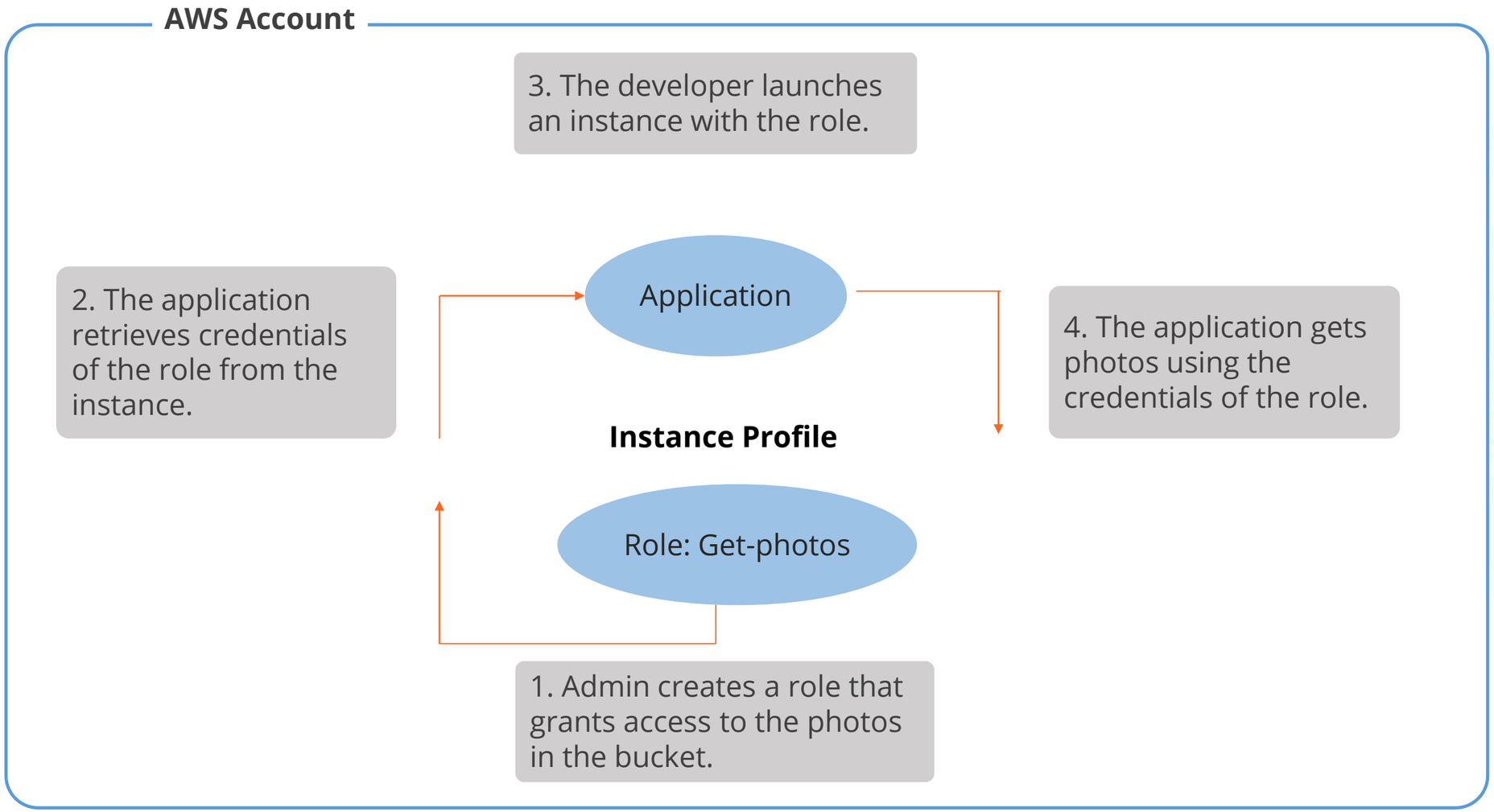
01 IAM roles operate similarly to IAM users.

02 They lack password protection and do not necessitate access keys.

03 These roles are available for use by any entity requiring them.

Various Functions of IAM Roles

IAM roles grant access to users, applications, and services that lack permission to utilize AWS resources.



Creating and Adding Policies to Groups Using Users

Duration:10 min

Problem Statement:

You have been assigned a task to create and add a policy to the group using a user to enable security management in various systems and applications.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create and manage policy
2. Attach policy and permissions directly to the group using group users
3. Create and manage S3 versioning

Configuring Resource-Based Policy Using Principles

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the process of configuring resource-based policies using principals to enable access to AWS resources.

ASSISTED PRACTICE

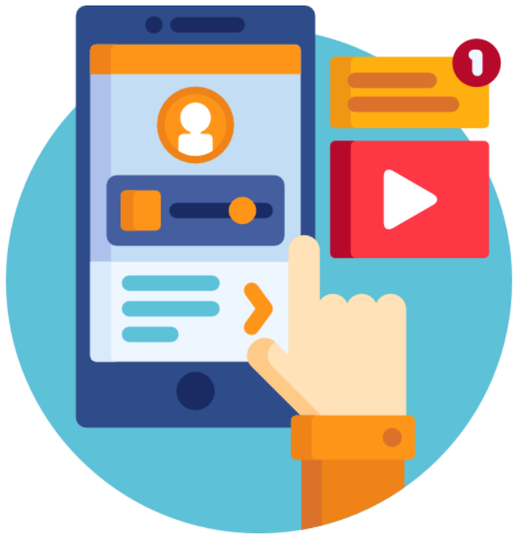
Assisted Practice: Guidelines

Steps to be followed are:

1. Create users and attach policies to them
2. Generate the policy using principals

AWS Cognito

AWS Cognito



Amazon Cognito manages web and mobile app authentication, authorization, and user management.

Users can sign in directly using a username and password or through third-party services like Facebook, Amazon, Google, or Apple.

It comprises two key components: user pools and identity pools.

Cognito: Example

This example is a combination of an Amazon Cognito user pool and an identity pool.

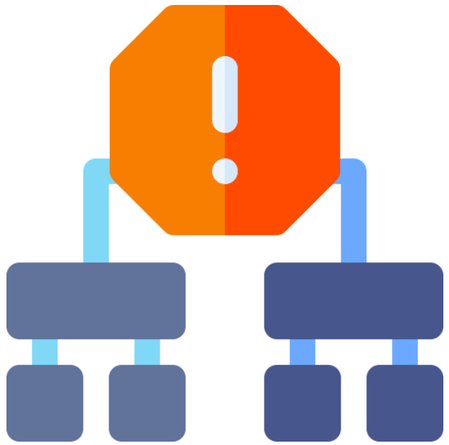
App users register through a user pool and obtain user pool tokens upon successful authentication.

Subsequently, the user app employs an identity pool to trade user pool tokens for AWS credentials.

With AWS credentials in hand, app users gain access to various AWS services, including Amazon S3 and DynamoDB.

AWS Control Tower

AWS Control Tower



- It is the easiest way to establish and manage a secure, multi-account AWS environment referred to as a landing zone.
- It provides users with a well-structured landing zone equipped with AWS Organizations, ensuring continuous account management, governance, and deployment best practices.

Benefits of AWS Control Tower

AWS Control Tower offers a range of advantages, including:

- Rapid environment setup
- Automated policy management
- Policy overview

Cloud Security

Cloud Security

- In cloud computing, users do not need to manage physical servers or storage components.
- Instead, they opt for software-based security measures to monitor and safeguard the data flowing into and out of their cloud resources.

Types of Cyber Attacks

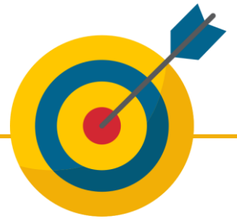
The following are some common threats:

- Phishing
- Password management
- Credential leaks
- Network security
- Insider threat
- Security incident recovery planning

Case Study: Netflix

Location: United States

Industry: On-demand media industry



Challenge

In 2008, Netflix faced a significant challenge when its primary focus was on DVD-by-mail services. During this period, they encountered a database corruption issue that led to a complete halt in DVD shipping for a duration of three days.

Solution

Netflix management decided to shift away from relational systems in their data centers and toward the cloud. The cloud was AWS which allowed the organization to scale as much as it required.

Amazon VPC

Amazon VPC provides users with full control over their virtual networking environment, encompassing resource allocation, connectivity, and security measures.

Use Cases:

- Launching a simple website or blog
- Hosting multi-tier web applications
- Creating hybrid connections

Amazon CloudFront

Amazon CloudFront is a CDN solution designed for great performance, security, and developer simplicity.

Use Cases:

- Deliver fast, secure websites
- Accelerate dynamic content delivery and APIs
- Stream live and on-demand video

Creating and Changing AWS Security Groups

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the process of configuring AWS security groups to control inbound and outbound traffic to and from AWS resources.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

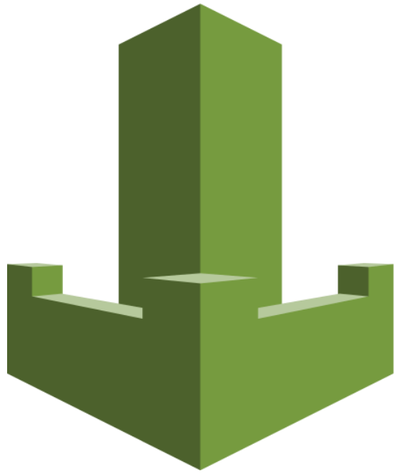
1. Create the security group
2. Change the security group

TECHNOLOGY

AWS Web Application Firewall (WAF)

What Is AWS WAF?

It is a web application firewall for monitoring HTTP/HTTPS requests to CloudFront, API Gateway, or Application Load Balancer.



AWS WAF

AWS WAF

It enables users to:

01	Allow all the requests except the ones that they specify
02	Block all the requests except the ones that they specify
03	Count the requests that match the properties that they specify

How to Handle False Positives in WAF?

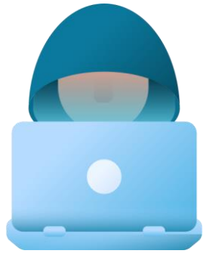
Users must use a web browser. To check for a false positive of **style==xxx** on their **example.com** domain, enter **example.com/style==xxx** in the web browser. The response is error code **403 Forbidden**.

```
$ curl -ikv http://example.com/[false positive]
```

Note:

Users apply curl and replace **users' false positive** for **false positive**.

Benefits of AWS WAF



Offers additional protection against web attacks

Provides real-time information and samples of web requests

Offers automated administration

Creating and Configuring AWS WAF

Duration:10 min

Problem Statement:

You have been assigned a task to demonstrate the process of configuring AWS WAF to protect your web applications and APIs hosted on the AWS environment.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create an IP set
2. Create Web ACL
3. Create a custom rule in Web ACL

AWS Shield

What Is AWS Shield?

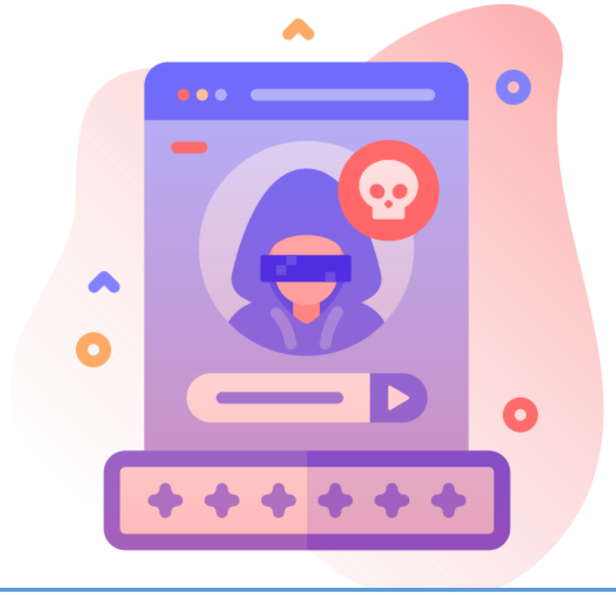
AWS Shield is a managed service designed to protect applications hosted on AWS from Distributed Denial of Service (DDoS) attacks.

AWS Shield

This service provides a comprehensive defense mechanism against malicious attempts to overwhelm and disrupt applications, ensuring their availability and performance.

AWS Shield Advance

AWS Shield Advanced is an enhanced subscription service that offers a comprehensive suite of features for advanced protection against Distributed Denial of Service (DDoS) attacks.



This service provides a higher level of security and customization to safeguard applications hosted on AWS.

Benefits of AWS Shield

AWS Shield offers a range of advantages, including:

01 Seamless integration and deployment

02 Customizable protection

03 Managed protection and attack visibility

04 Cost-efficiency

TECHNOLOGY

AWS Secrets Manager

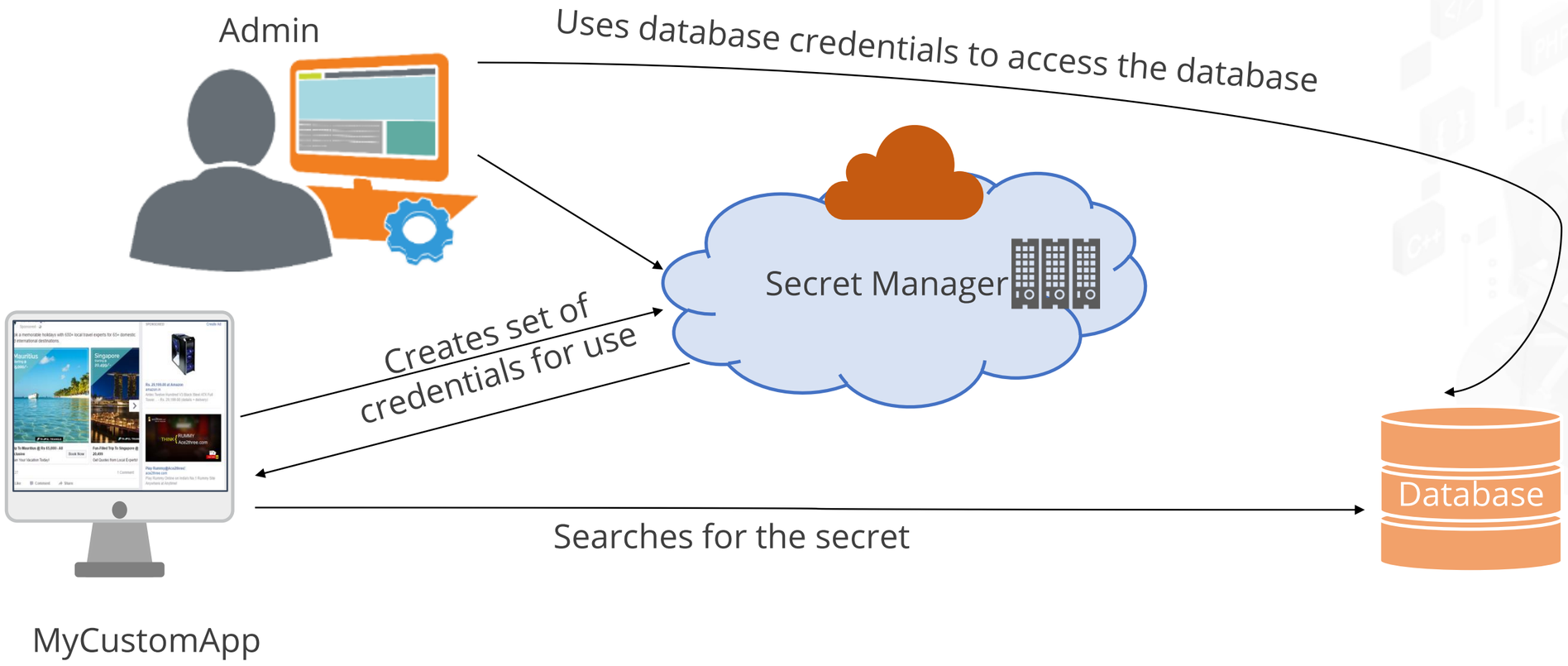
AWS Secrets Manager

It is a powerful service that offers a secure and efficient solution for managing sensitive credentials and secrets used in applications and services.

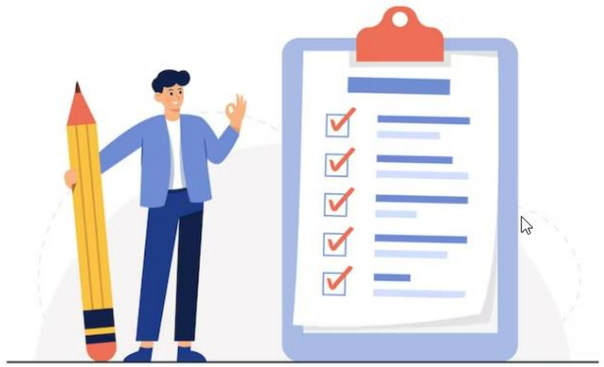
This service eliminates the need to hardcode sensitive information, such as passwords and API keys, directly into code or configuration files.

AWS Secrets Manager Scenario

The diagram below depicts how the users can save database credentials in Secrets Manager and then use those credentials in an application to access the database.



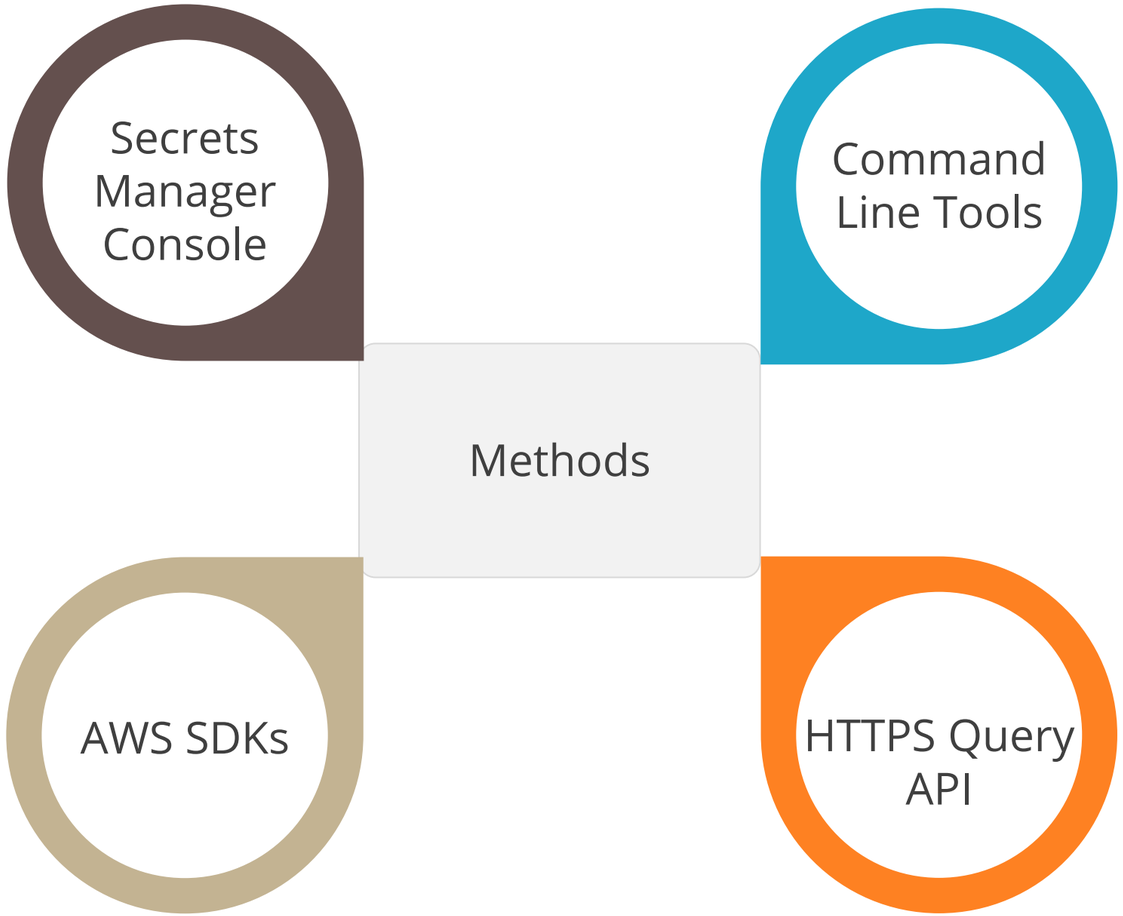
AWS Secrets Manager: Features



- Allows the users to replace stored credentials with a runtime call to the Secrets Manager Web service dynamically
- Is easy to create, leaving users time to focus on creating the applications
- Returns the most recently encrypted secret value version
- Provides users with scalability and reliability provided by AWS

Working with AWS Secrets Manager

Any of the following methods can be used to interact with Secrets Manager:



Working with AWS Secrets Manager

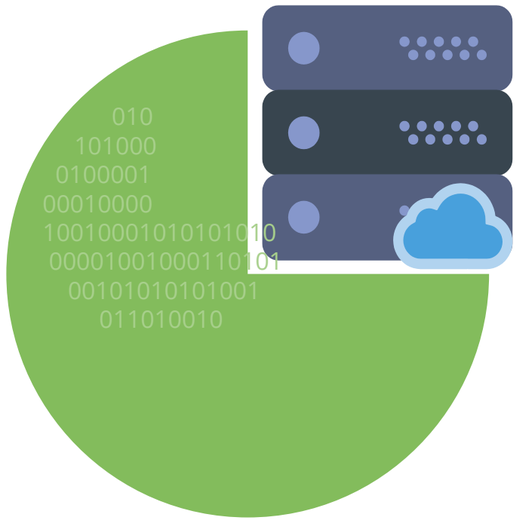
Secrets Manager Console

The browser-based Secrets Manager console allows users to manage the secrets and perform any task related to the secrets.

Working with AWS Secrets Manager

Command line tools

The AWS command line tools enable users to perform Secrets Manager and other AWS tasks by issuing commands from the system command line.



Working with AWS Secrets Manager

AWS SDKs

The AWS SDKs include libraries and sample code for a variety of programming languages and platforms, including Java, Python, Ruby, .NET, and others.

Working with AWS Secrets Manager

HTTPS Query API

It allows users to access Secrets Manager and AWS programmatically.

API

Secrets Manager Administrator Permissions

End users should not be granted administrator permissions that help them to carry out the following tasks:

- Focusing on how an organization performs work
- Viewing the value delivery of an organization

Permissions to Access Secrets

Users may manage which people or services have access to the secrets by using IAM authorization policies. A permissions policy specifies who can do what on which resources.

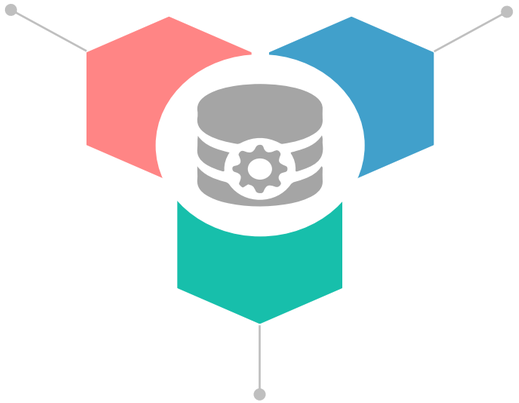
Users may:

- Attach a permissions policy to an identity
- Attach a permissions policy to a secret

Attach a Permissions Policy to an Identity

Identity-based policies can be used to:

Give a user access to several secrets

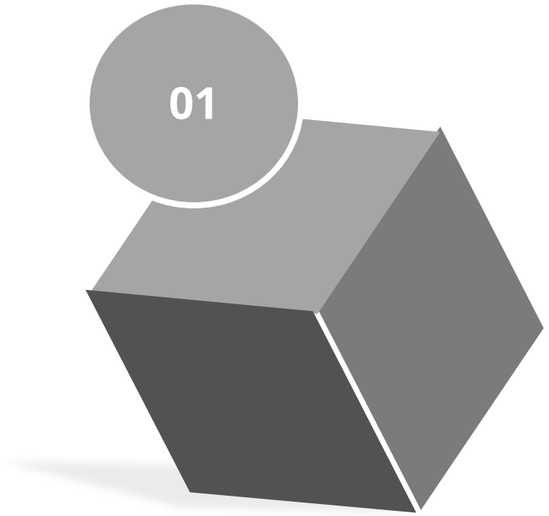


Allow an IAM group to access secrets

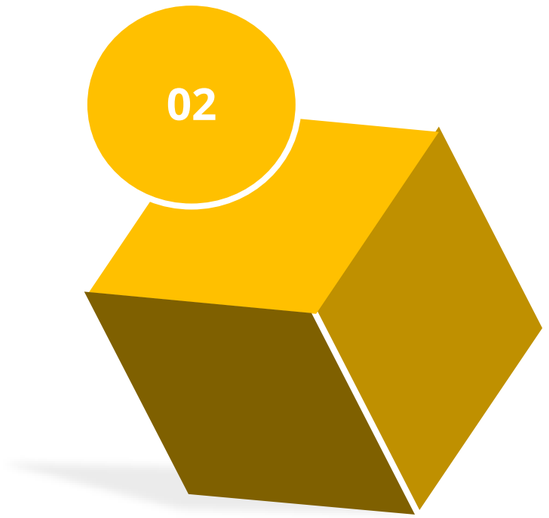
Control who can create new secrets and who can access already generated secrets

Attach a Permissions Policy to a Secret

In a resource-based policy, users determine who will have access to the secret and what actions they may take with it. Resource-based policies can be used to:



Grant access to a single secret to multiple users and roles



Grant access to users or roles in other AWS accounts

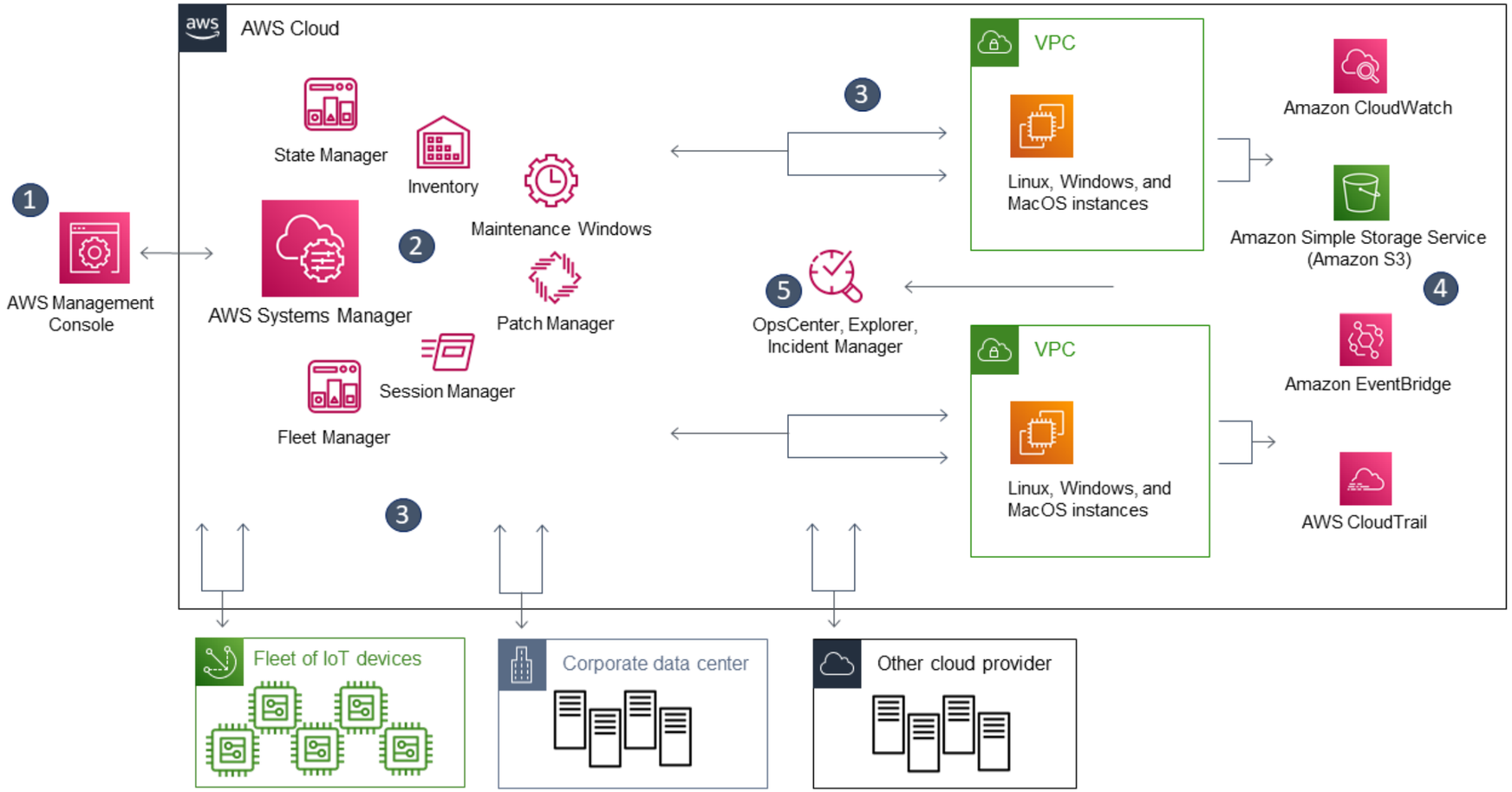
AWS Systems Manager

AWS Systems Manager

It offers a comprehensive suite of tools designed to aid users in efficiently managing the infrastructure and applications hosted on the AWS Cloud.

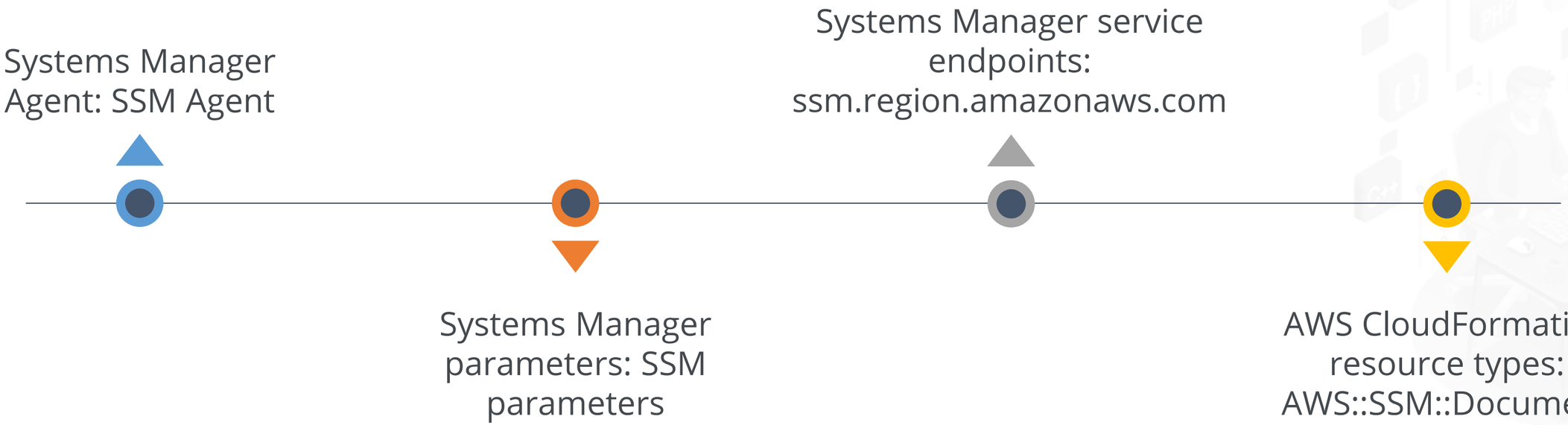
How Systems Manager Works?

The activities performed by the Systems Manager on the resources are shown in the following diagram with a detailed description of each interaction between different components:



Systems Manager Service Name History

The previous names for AWS Systems Manager are listed below:



Systems Manager Service Name History

The previous names for AWS Systems Manager are listed below:

AWS Config rule identifier: EC2_INSTANCE_MANAGED_BY_SSM

AWS Command Line Interface (AWS CLI) commands: aws ssm describe-patch-baselines

AWS Identity and Access Management (IAM) managed policy names: AmazonSSMReadOnlyAccess

Systems Manager resource ARNs: arn:aws:ssm:region:account-id:patchbaseline/pb-07d8884178EXAMPLE

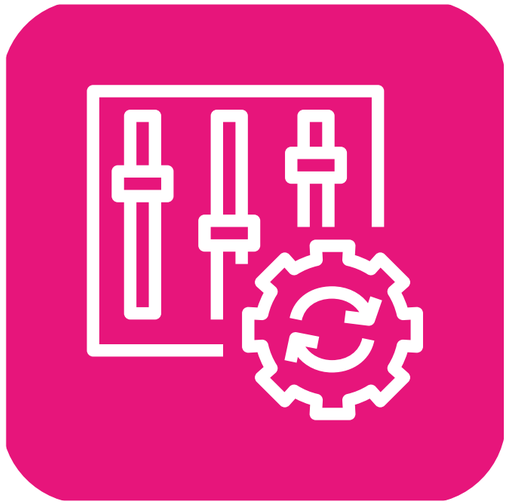
TECHNOLOGY

AWS Config

simplilearn

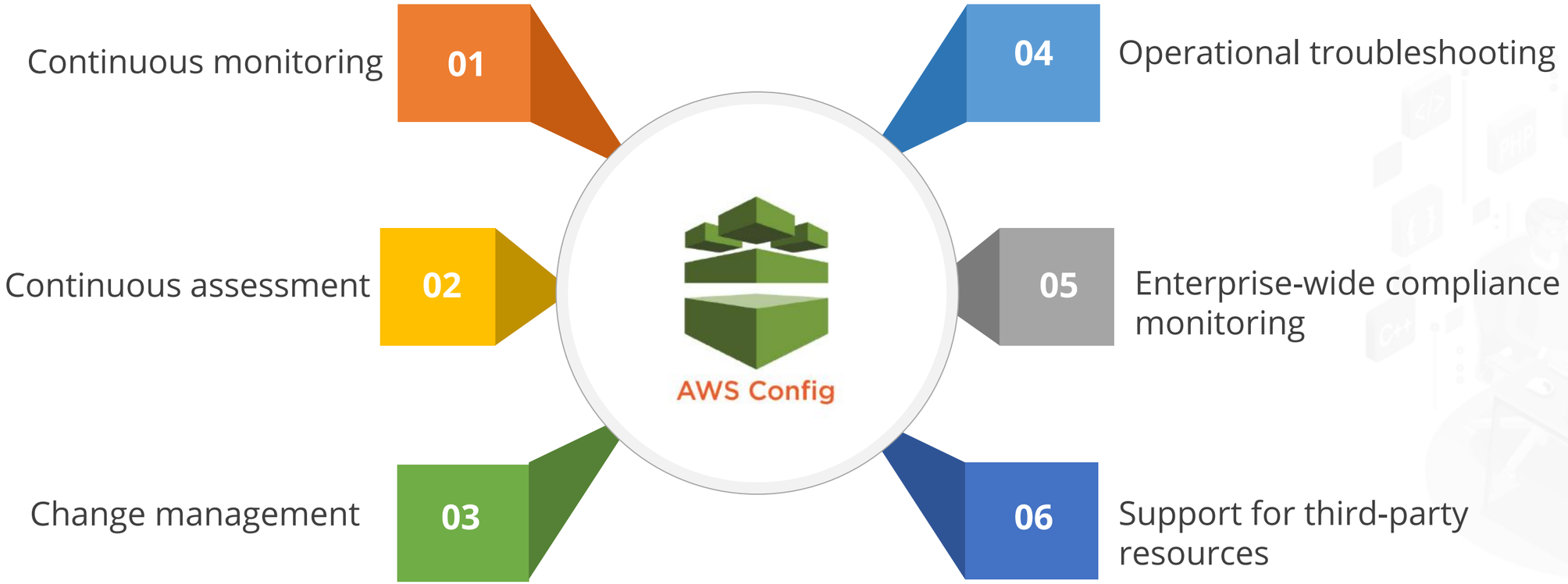
AWS Config

It is a powerful service that provides continuous monitoring and assessment of your AWS resources' configurations.



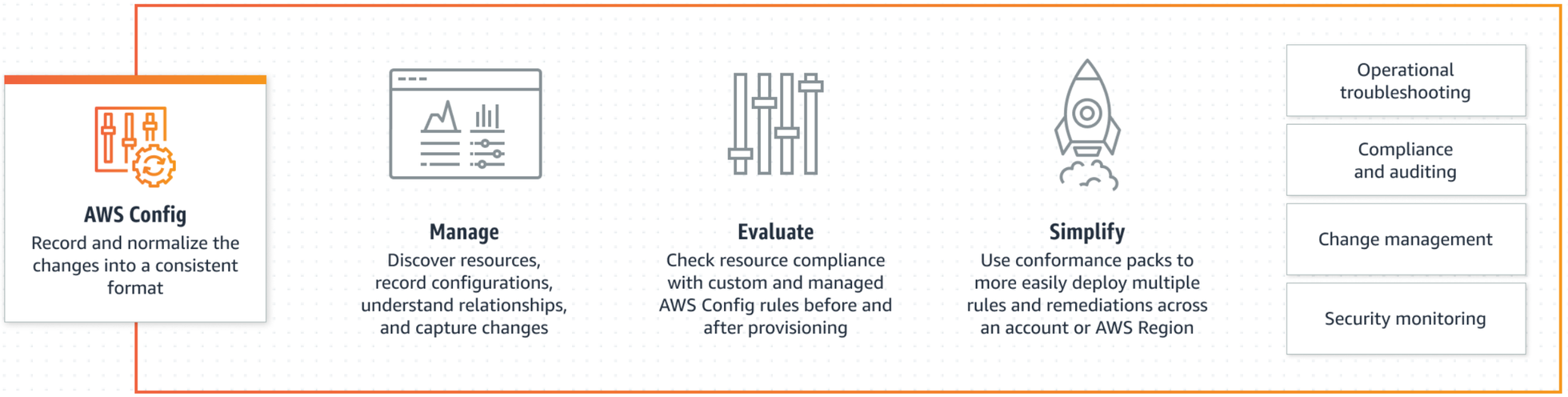
AWS Config ensures that your infrastructure complies with desired configurations and helps you maintain security, compliance, and governance across your cloud environment.

Benefits of AWS Config



How Does AWS Config Work?

AWS Config generates configuration items when a resource's configuration changes, and it maintains a historical record of these items from the moment the configuration recorder is initiated by users.



Setting Up AWS Config and Creating Rules in it

Duration:15 min

Problem Statement:

You have been assigned a task to configure AWS Config and create rules in it to enable compliance monitoring in the AWS environment.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Set up AWS Config
2. Create rules in AWS Config

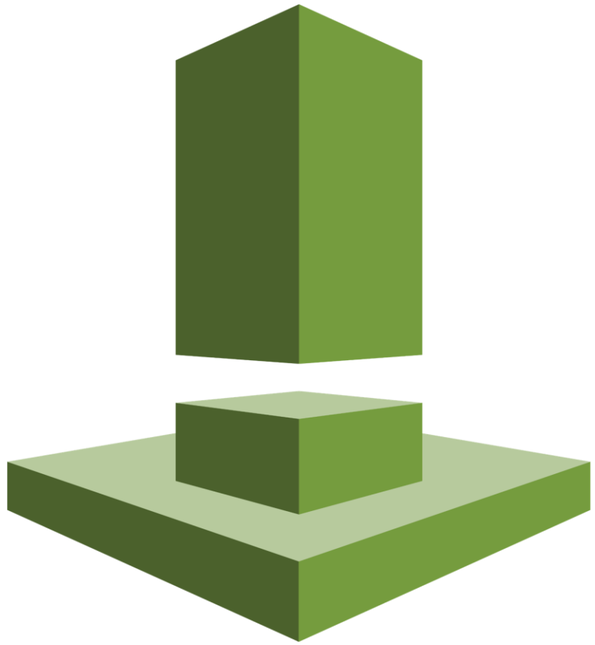
TECHNOLOGY

AWS Inspector and Trusted Advisor

simplilearn

AWS Inspector

AWS Inspector is a valuable security assessment service offered by Amazon Web Services. It assists in analyzing the security and compliance of applications deployed on the AWS Cloud.



AWS Inspector: Features

- Provides recommendations following the AWS best practices
- Performs searches to optimize the security of the AWS infrastructure
- Aids in reducing cost, boosting performance, and enhancing security

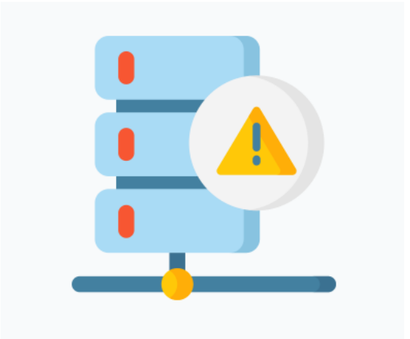
Benefits of AWS Inspector

Cost optimization

Performance

Security

Services



Fault tolerance

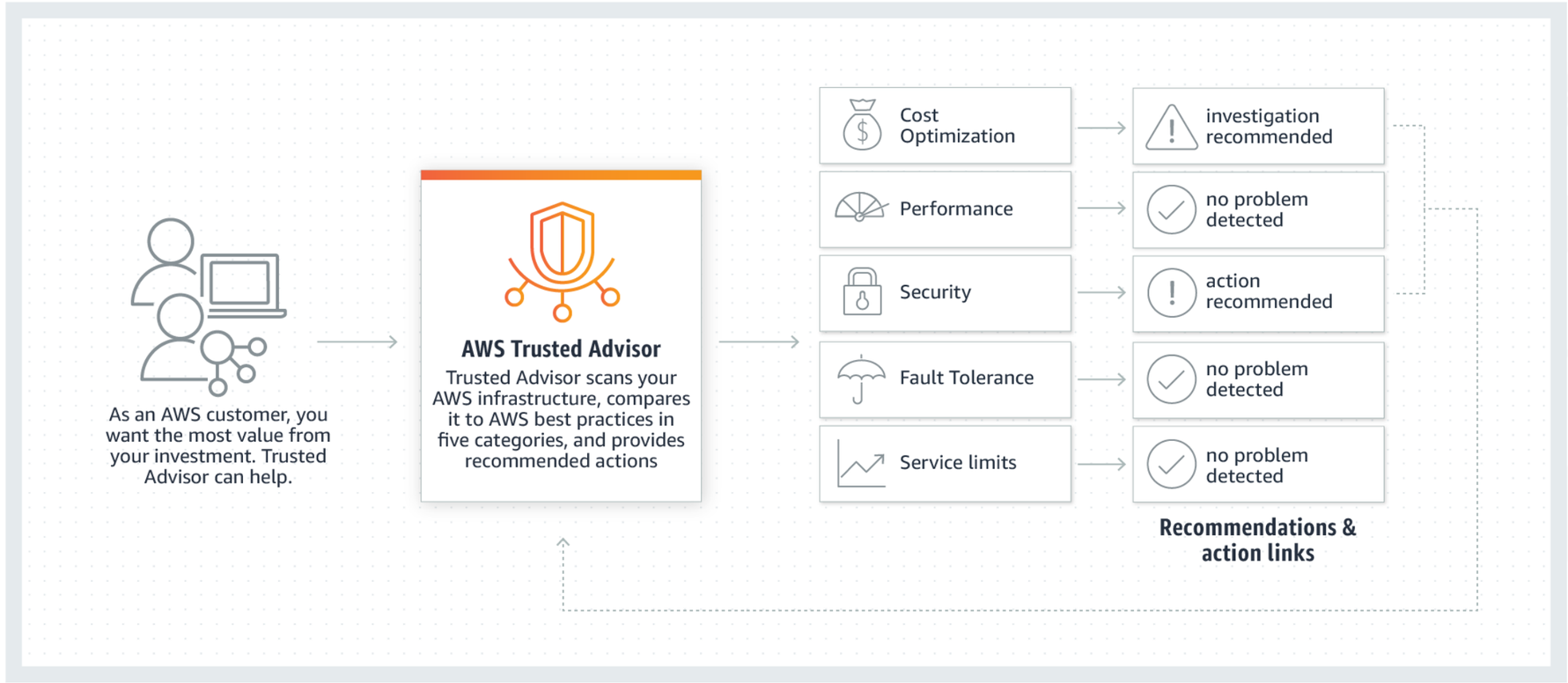
Trusted Advisor

AWS Trusted Advisor provides recommendations that help users follow AWS best practices.

- It provides recommendations that help users follow AWS best practices.
- It evaluates a user's account by using checks.
- These audits help users optimize their AWS infrastructure, boost performance and security, reduce expenses, and keep an eye on service quotas.

How Trusted Advisor works?

This diagram depicts the working of AWS Trusted Advisor:



Configuring AWS Inspector for Network Reachability and Vulnerability

Duration:15 min

Problem Statement:

You have been assigned a task to demonstrate the process of configuring AWS Inspector to enhance the security and compliance of the AWS environment.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Create security group and launch instances
2. Configure the AWS Inspector

Configuring Trusted Advisor

Duration:10 min

Problem Statement:

You have been assigned a task to configure Trusted Advisor to check the security vulnerabilities in the AWS environment and ensure performance improvement.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Open Trusted Advisor and set up the preferences

Amazon GuardDuty

Amazon GuardDuty

Amazon GuardDuty, a threat detection service, provides comprehensive security findings for visibility and remediation.

It continuously scans your AWS accounts and workloads to identify malicious activities.

Benefits of Amazon GuardDuty

Amazon GuardDuty offers a range of advantages, including:

- Comprehensive threat identification
- Security enhancement through automation
- Enterprise scale and central management

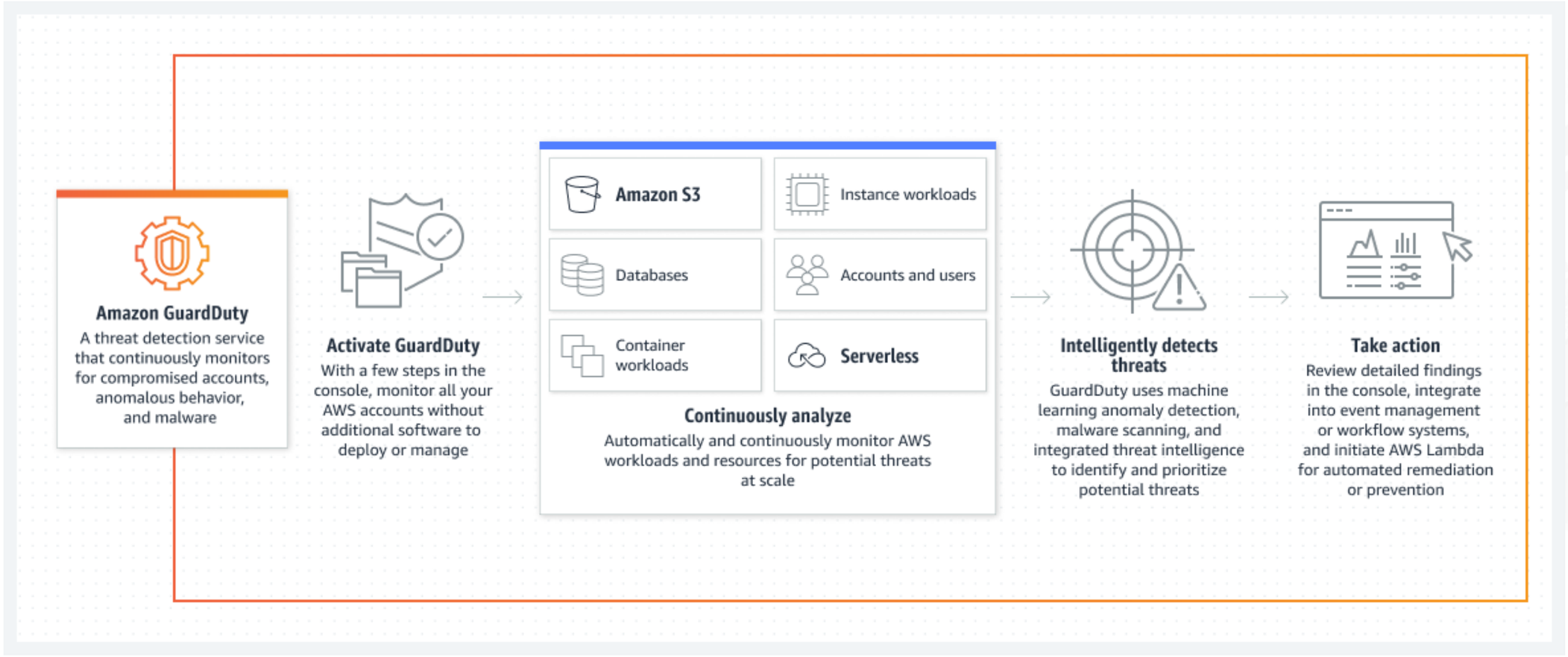
Accessing GuardDuty

With GuardDuty, users can cooperate in the following ways:

- GuardDuty Console
- SDKs for AWS
- HTTPS API for GuardDuty

How GuardDuty Works?

This diagram depicts the working of Amazon GuardDuty:



Languages Supported by Amazon GuardDuty

Information about GuardDuty is accessible in a total of eight languages, which encompass Chinese, English, French, German, Japanese, Korean, Portuguese, and Spanish.

Amazon Macie

Amazon Macie

It is a fully managed data security and data privacy solution that discovers and protects sensitive data in AWS using machine learning and pattern matching.

Benefits of Macie

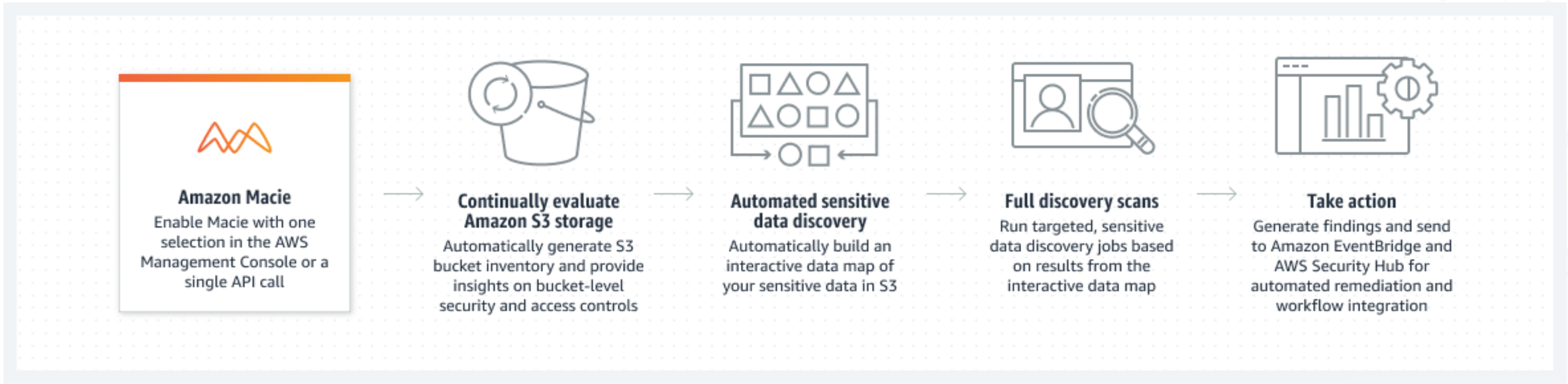
01 Discover your sensitive data at scale

02 Visibility of your data security posture

03 Easy to setup and manage

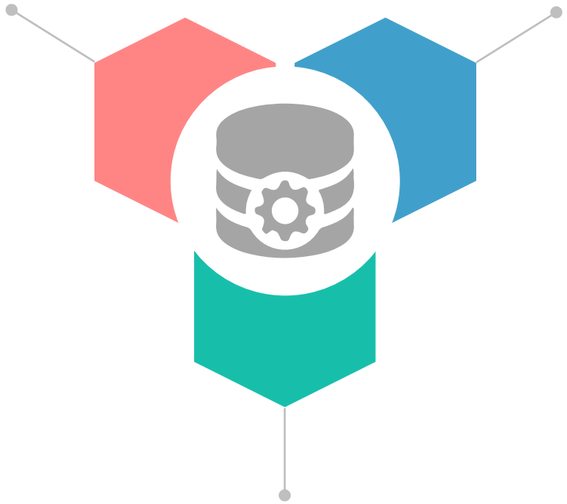
Working of Macie

After activating Macie for the AWS account, the S3 bucket list will be created in the same region. Macie will also start monitoring the access control and security of the buckets.



Features Of Macie

Data discovery and classification



Data retention monitoring

Customizable policies

Key Takeaways

- IAM policies let users control employee and system access to ensure least-privilege access.
- For web and mobile apps, Amazon Cognito enables quick, secure user authentication, authorization, and management.
- AWS WAF gives control over how traffic enters the applications, allowing users to establish security rules to block common attack vectors.
- AWS Shield offers always-on detection and automatic inline mitigations that reduce application downtime and latency.

Key Takeaways

- Users can automate the process of creating and configuring numerous accounts made possible by AWS Control Tower.
- Users can secure, analyze, and manage secrets in the AWS Cloud, on external services, and on-premises using Secrets Manager.
- Amazon Macie continually checks the Amazon S3 environment and provides an S3 resource summary across all the accounts.
- Users can compare their environment to security best practices and standards with the aid of AWS Security Hub.

Create and Configure Groups and Users Using Policies

Duration: 30 mins

Project agenda: To demonstrate how to use AWS IAM to create and configure groups and users with different policies and permissions

Description: The admin of a corporation wants to create three groups of IAM users, each with two users and two policies assigned to them. The policies will define the permissions and roles for the users to perform their tasks in their respective groups.

Perform the following:

1. Create a group
2. Configure the user for CLI operation

LESSON-END PROJECT

TECHNOLOGY

Thank You

simplilearn