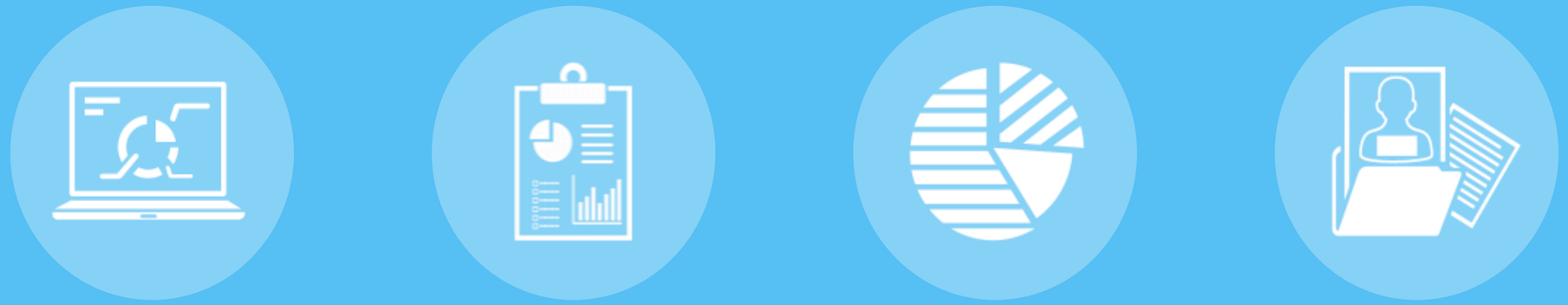
AWS Solutions Architect—Associate Level

Lesson 3: Identity and Access Management (IAM)



What You'll Learn

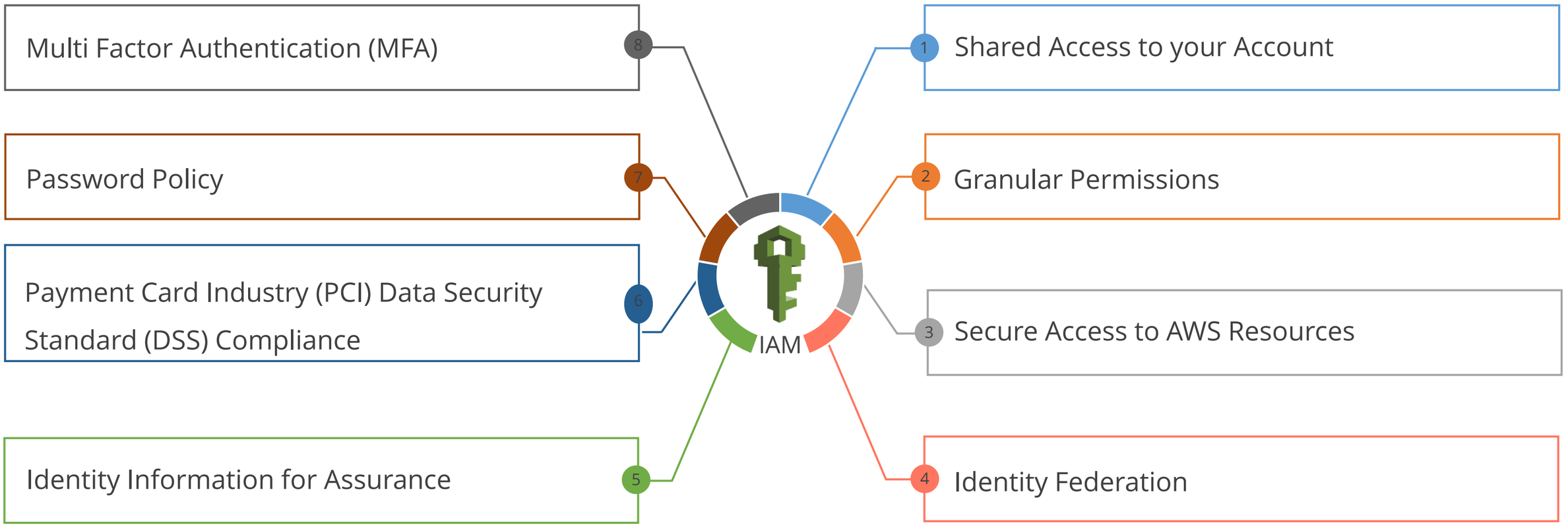
- Key Features of IAM
- AWS Policies
- AWS Users
- IAM Groups
- IAM Roles
- IAM Best Practices

IAM Overview

Overview of AWS IAM

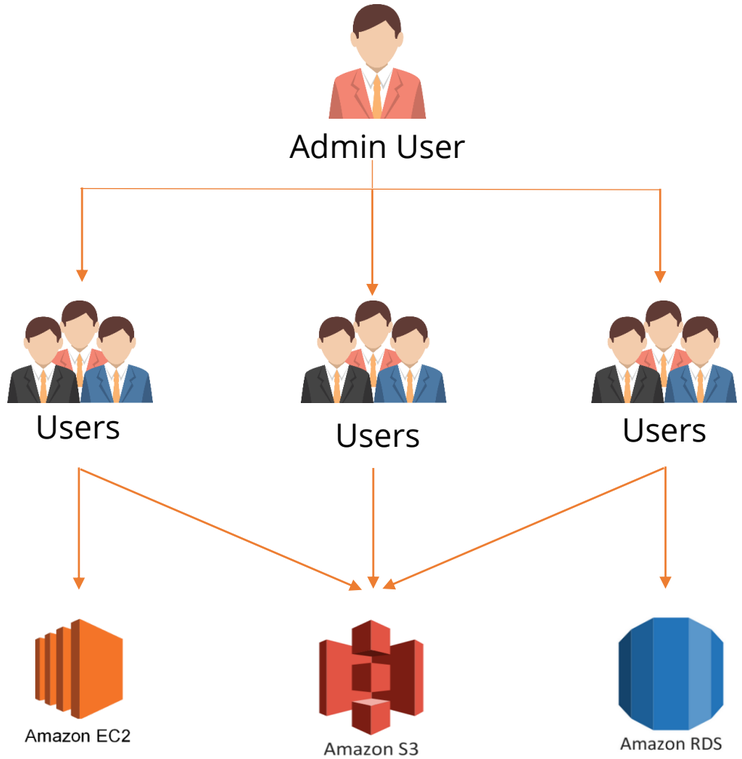
Identity and Access Management

The key features of IAM:



Shared Access

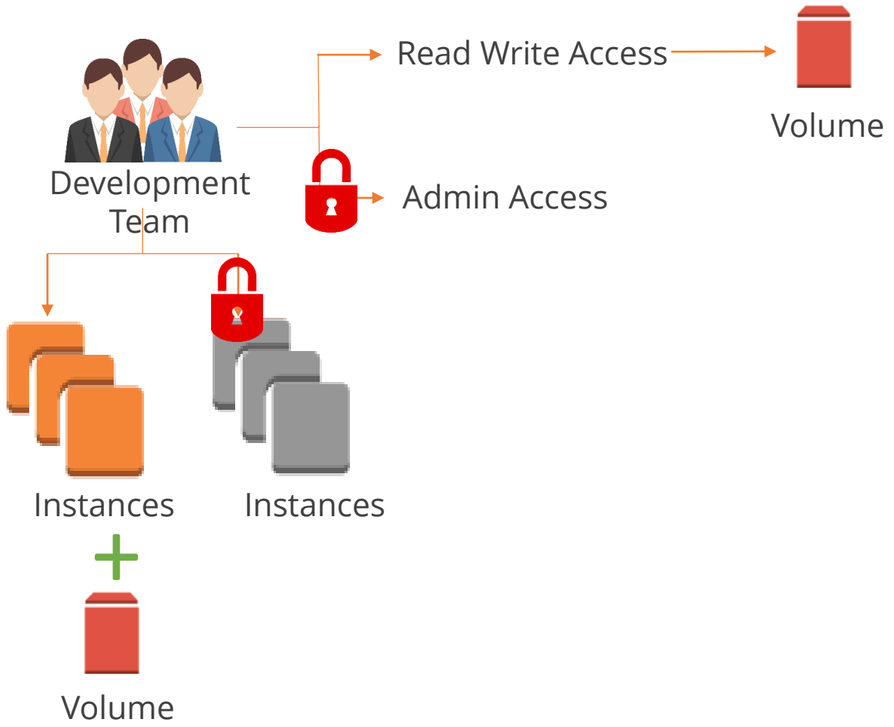
Grant permission to users to access and use resources in your AWS account without sharing your password.



Granular Permissions

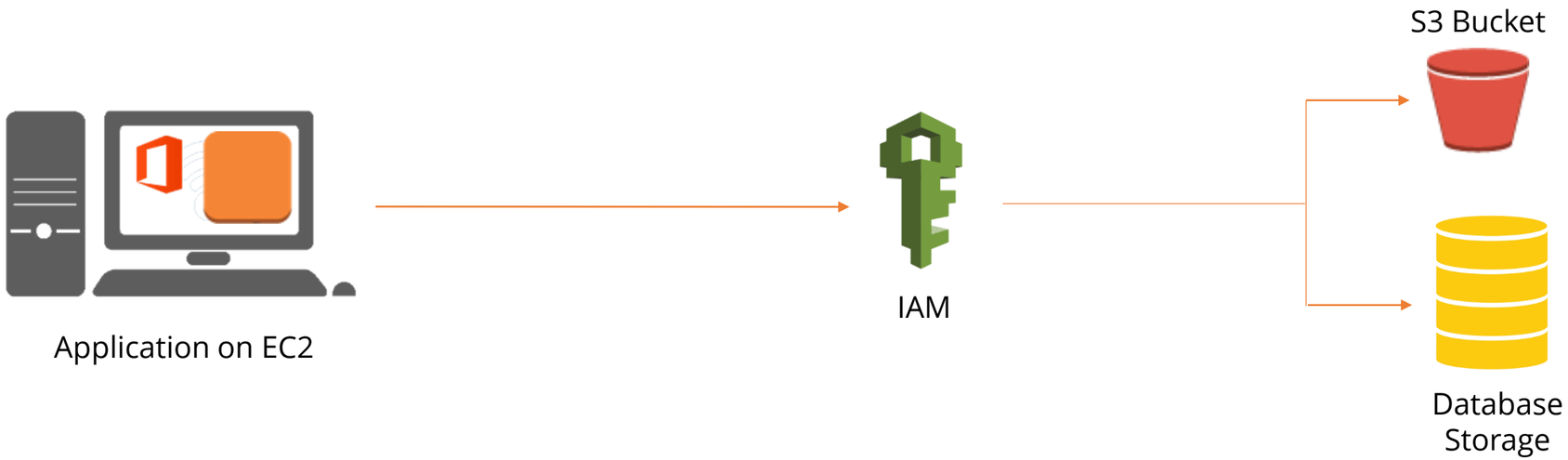
Granular permissions allow different permissions to various users to manage their access to AWS, such as:

- User access to specific services
- Specific permissions for actions
- Specific access to resources



Secure Access

Securely allocate credentials that applications on EC2 instances require to access other AWS resources.

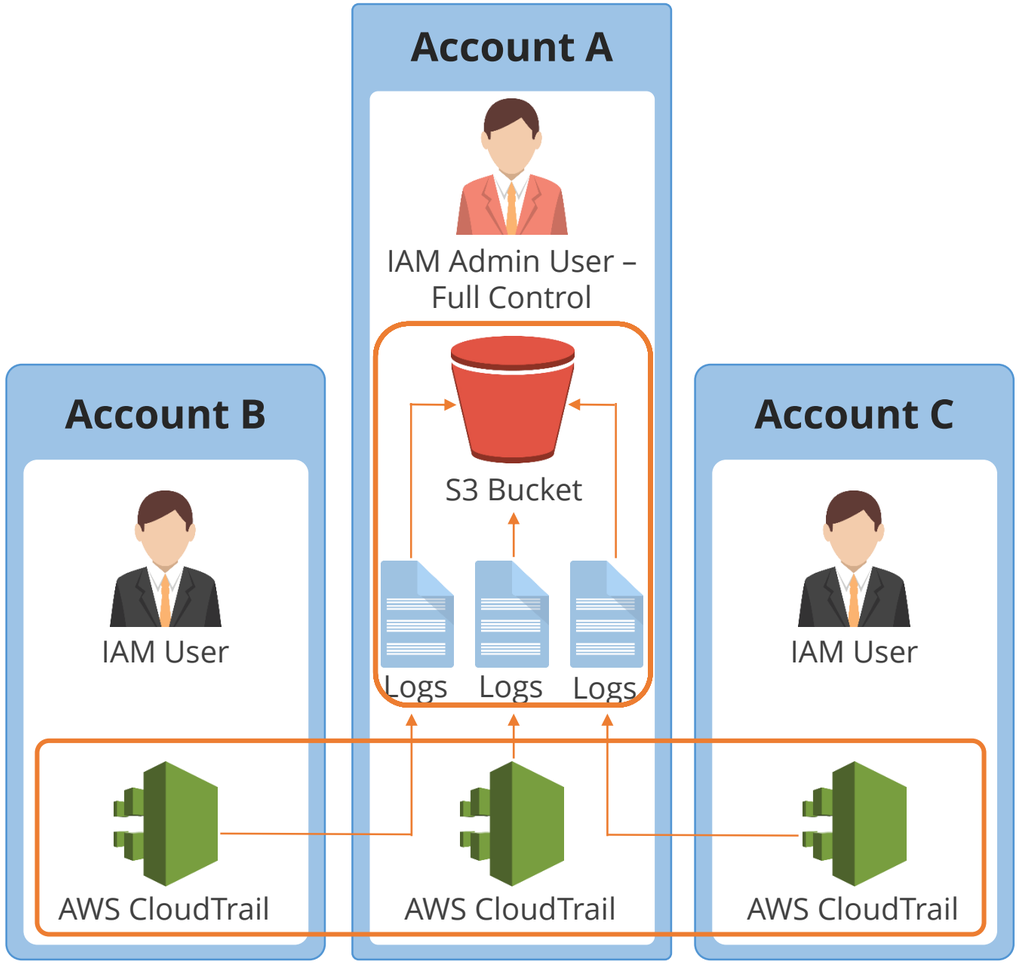


Identity Federation

Allows users with external accounts to get temporary access to AWS resources

Identity Information

Log, monitor, and track what users are doing with your AWS resources.

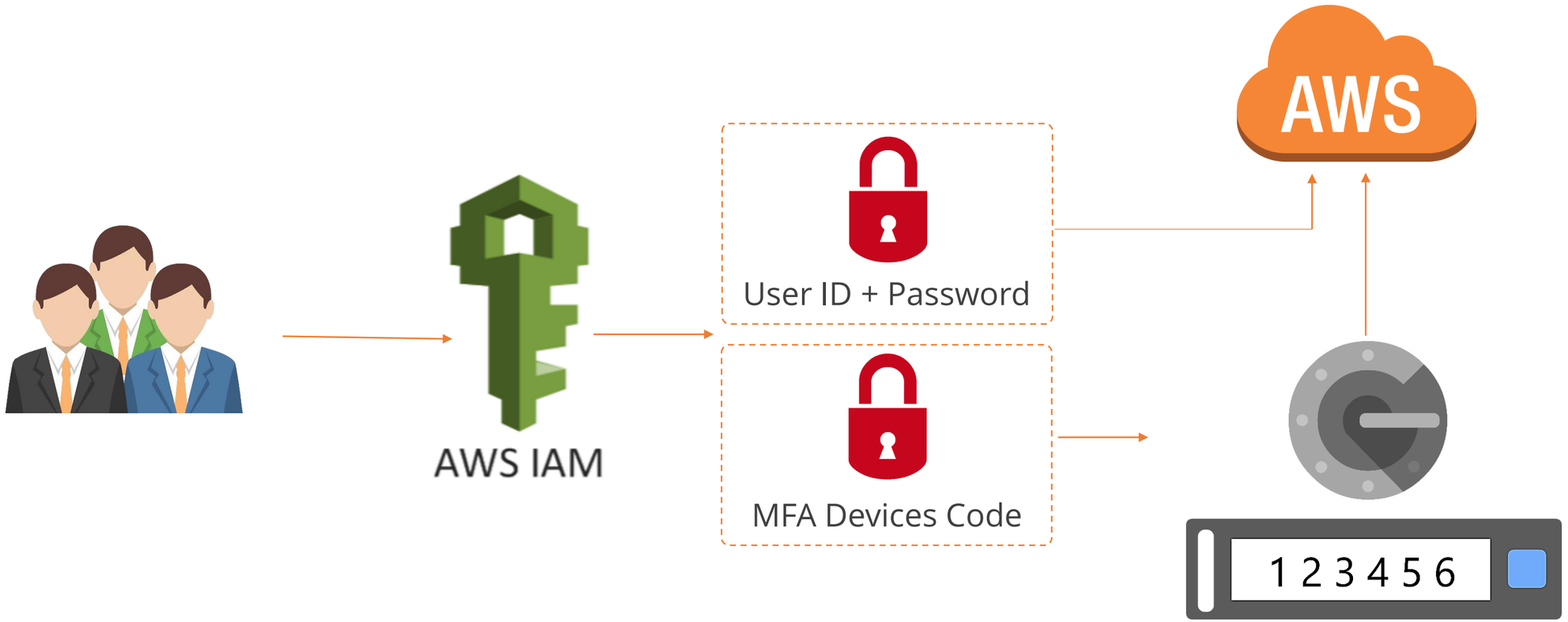


PCI DSS Compliance

Payment Card Industry (PCI) and Data Security Standard (DSS) compliant

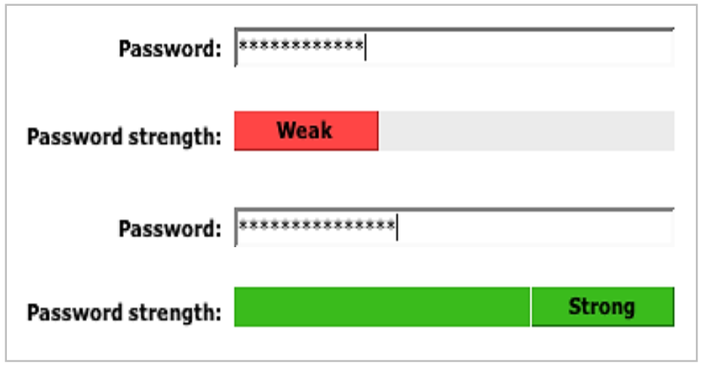
Multi-Factor Authentication

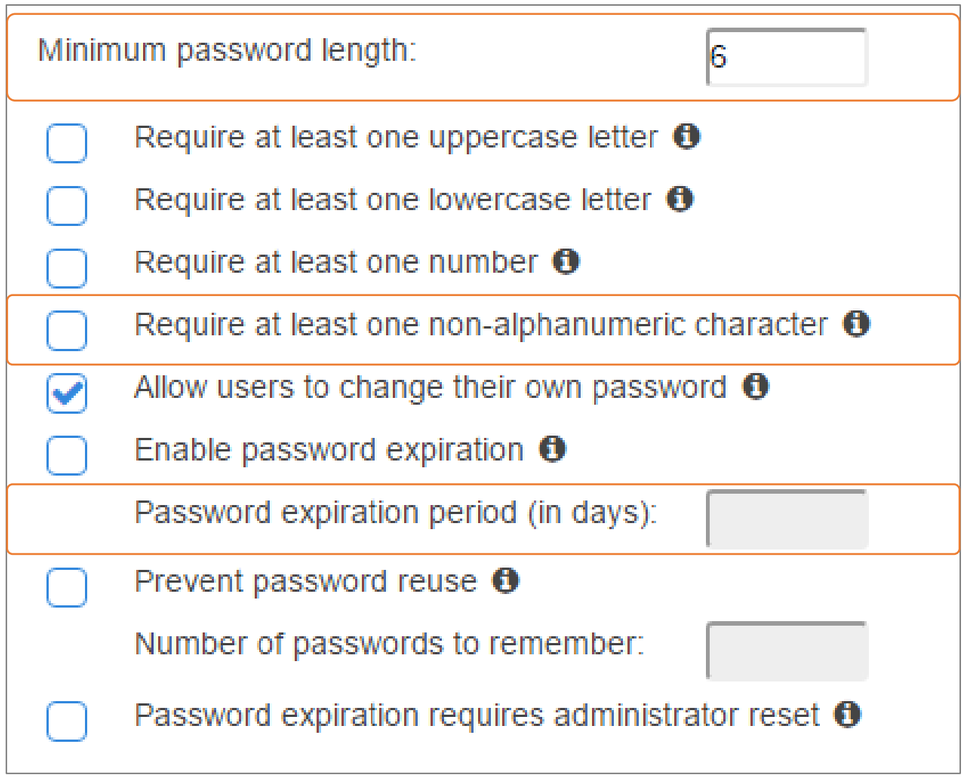
Two-Factor Authorization for users and resources to ensure absolute security using MFA devices



Password Policy

IAM allows you to define password strength and rotation policies.





IAM Policies

Description of IAM Policies

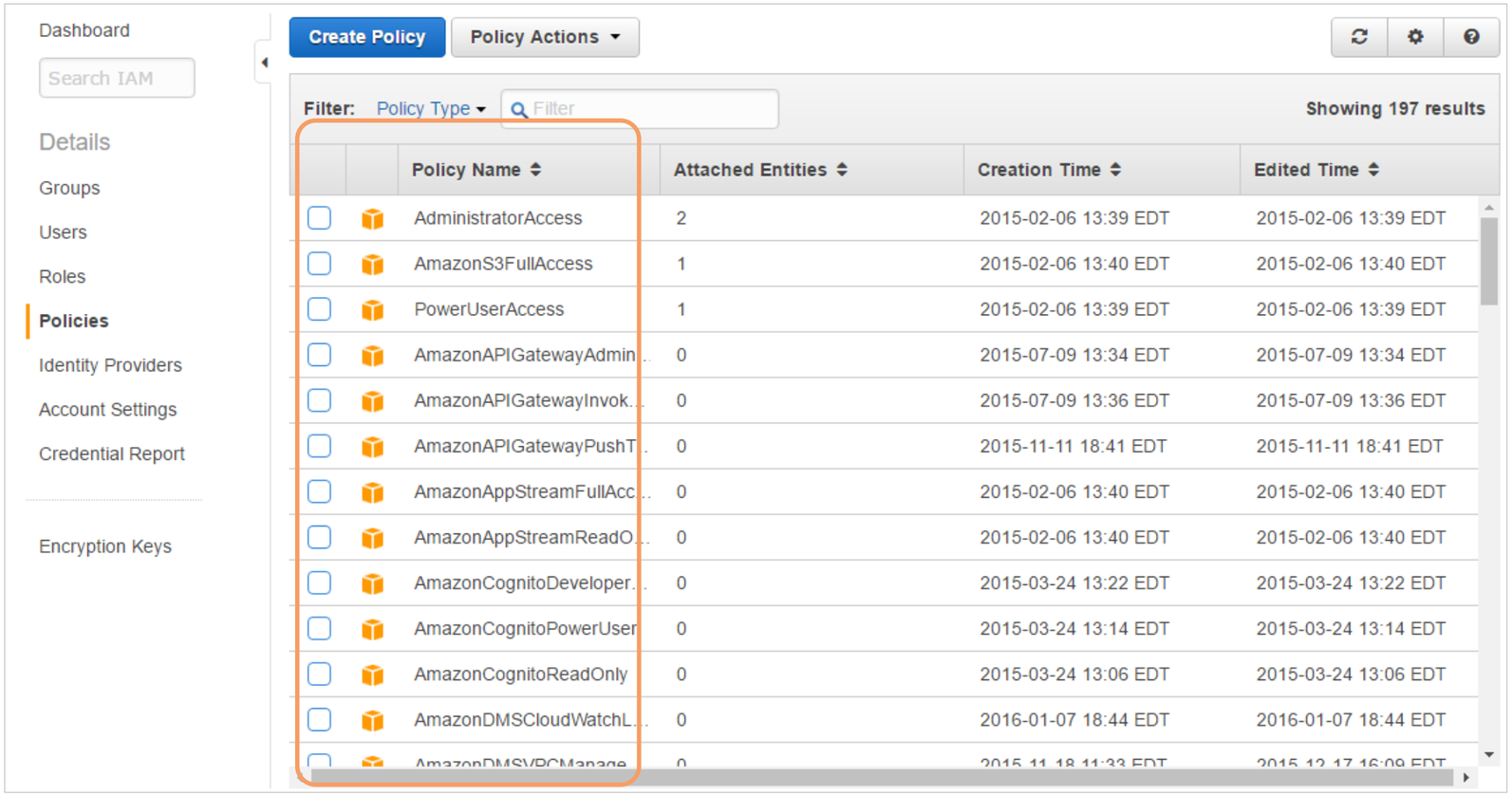
IAM Policies

An IAM policy is:

- A document that defines one or more permissions
- Attached to users, groups, and roles
- Written in JavaScript Object Notation (JSON)
- Selected from a pre-defined AWS list of policies, or you can create your own policy

AWS Policies

AWS has many predefined policies which allow you to define granular access to AWS resources.



There are around 200 predefined policies available for you to choose from.

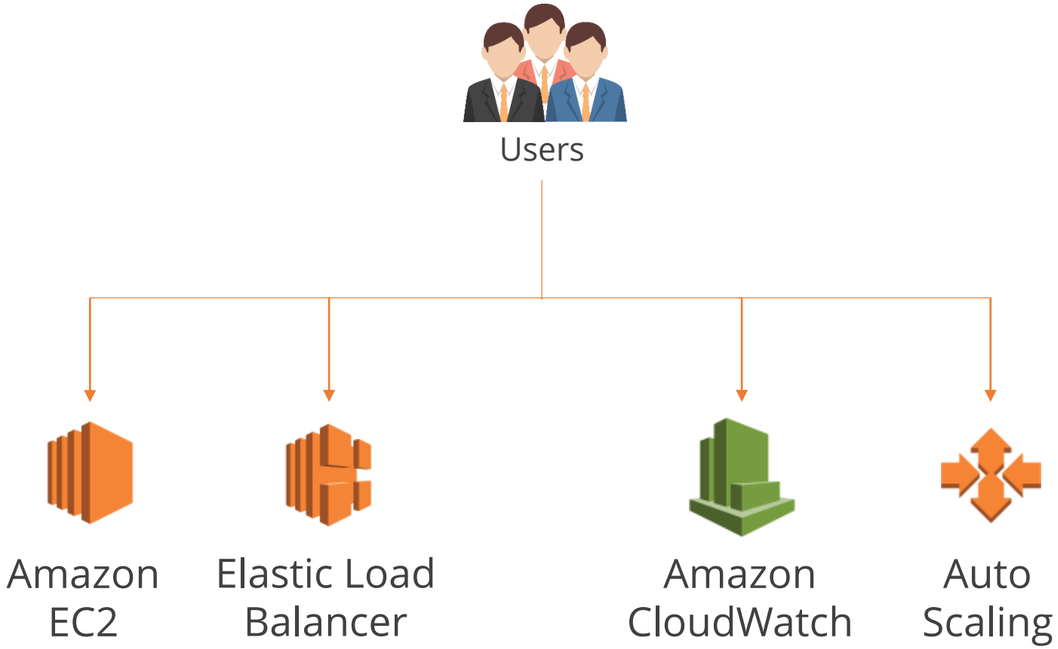
AdministratorAccess Policy

AdministratorAccess policy provides full access to AWS services and resources.

Admin User

AmazonEC2FullAccess Policy

AmazonEC2FullAccess policy provides AWS Directory Service user or groups full access to the Amazon EC2 services and resources.



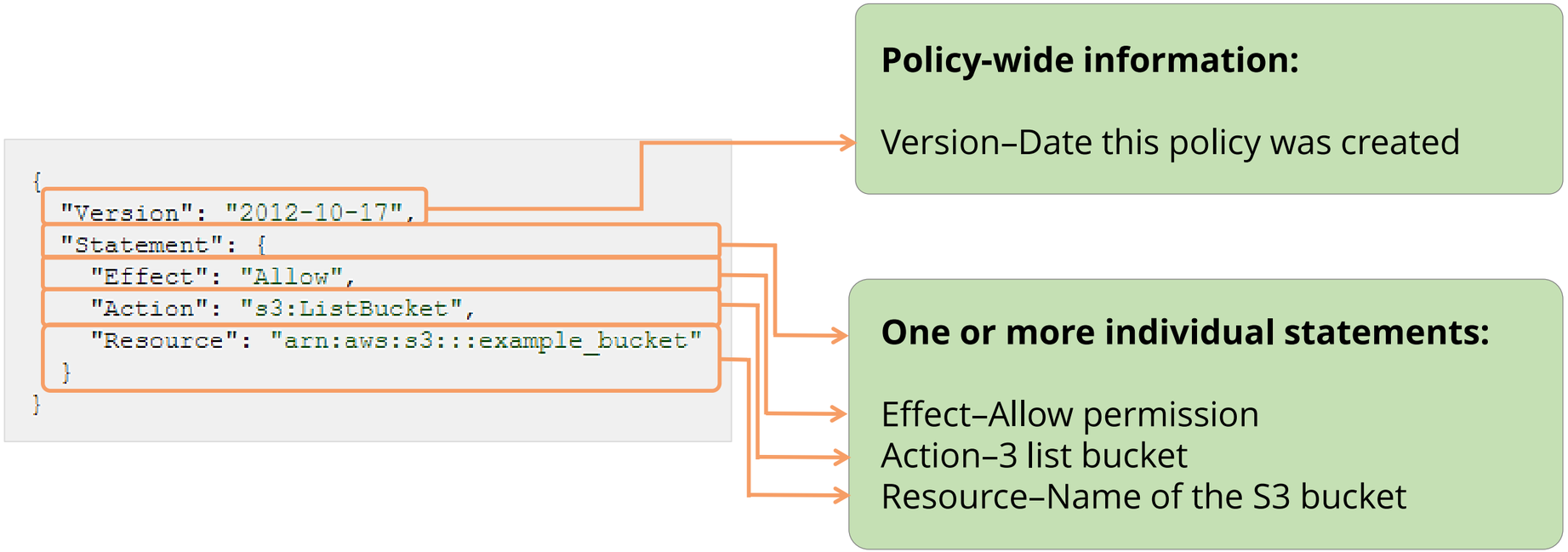
AmazonS3ReadOnlyAccess Policy

AmazonS3ReadOnlyAccess policy provides read-only access to all buckets using the AWS Management Console.

Users

JSON

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



Demo 1: Creating an IAM Policy

Demonstrate how to create an IAM Policy.

Knowledge Check

KNOWLEDGE CHECK	What does JSON stand for?

a. JavaScript Orientated Notation

b. JavaScript Object Notation

c. JavaScript Object Notes

d. JavaScript Open Notation

KNOWLEDGE CHECK

What does JSON stand for?

a. JavaScript Orientated Notation

b. JavaScript Object Notation

c. JavaScript Object Notes

d. JavaScript Open Notation

The correct answer is **b**.

JSON stands for JavaScript Object Notation and is used to write IAM Policies.

KNOWLEDGE CHECK	In a JSON policy, what does the "effect" statement define?

a. Whether the user is granted or denied permission

b. The commands a user can perform

c. The resources a user can run a command against

d. Whether the user needs to use MFA to authenticate

KNOWLEDGE CHECK

In a JSON policy, what does the "effect" statement define?

a. Whether the user is granted or denied permission

b. The commands a user can perform

c. The resources a user can run a command against

d. Whether the user needs to use MFA to authenticate

The correct answer is **a**.

The “effect” statement defines what the effect will be when the user requests access—either allow or deny.

KNOWLEDGE CHECK

What permissions would the AmazonEC2FullAccess policy give a user?

a. Full Access to permissions to only EC2 instances

b. Full Access to all AWS resources including EC2

c. Full Access permissions to Amazon EC2 and only Elastic Load Balancing

d. Full access to Amazon EC2, Elastic Load Balancer, and Amazon CloudWatch

KNOWLEDGE CHECK

What permissions would the AmazonEC2FullAccess policy give a user?

a. Full Access to permissions to only EC2 instances

b. Full Access to all AWS resources including EC2

c. Full Access permissions to Amazon EC2 and only Elastic Load Balancing

d. Full access to Amazon EC2, Elastic Load Balancer, and Amazon CloudWatch

The correct answer is **d**.

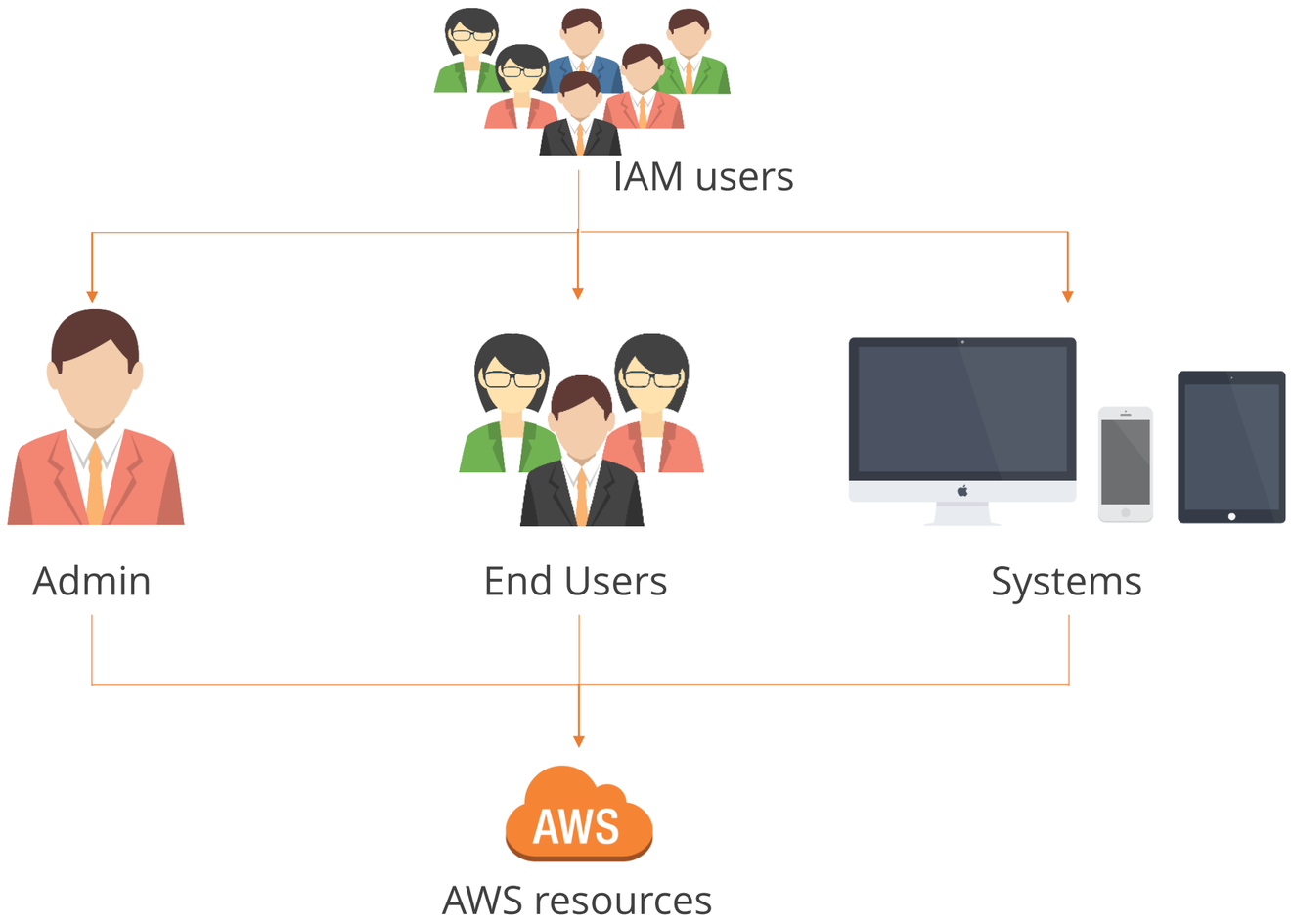
This role provides an AWS Directory Service user or group with full access to Amazon EC2 services and the associated services and resources: Amazon Elastic Compute Cloud, Elastic Load Balancing, Amazon CloudWatch, and Auto Scaling.

IAM Users

Description of IAM Users

IAM Users

Users are defined as the people or systems that use your AWS resources.



Security Credentials

AWS provides numerous ways to provide secure user access to your AWS resources:

Key pairs

- They consist of a public and private key
- A private key is used to create a digital signature
- AWS uses the corresponding public key to validate the signature

Email address and password

- They are created when you sign up to use AWS
- They are used to sign in to AWS web pages

Security credentials

IAM user name and password

- They allow multiple individuals or applications access to your AWS account
- Individuals use their user names and passwords to sign in

Access keys

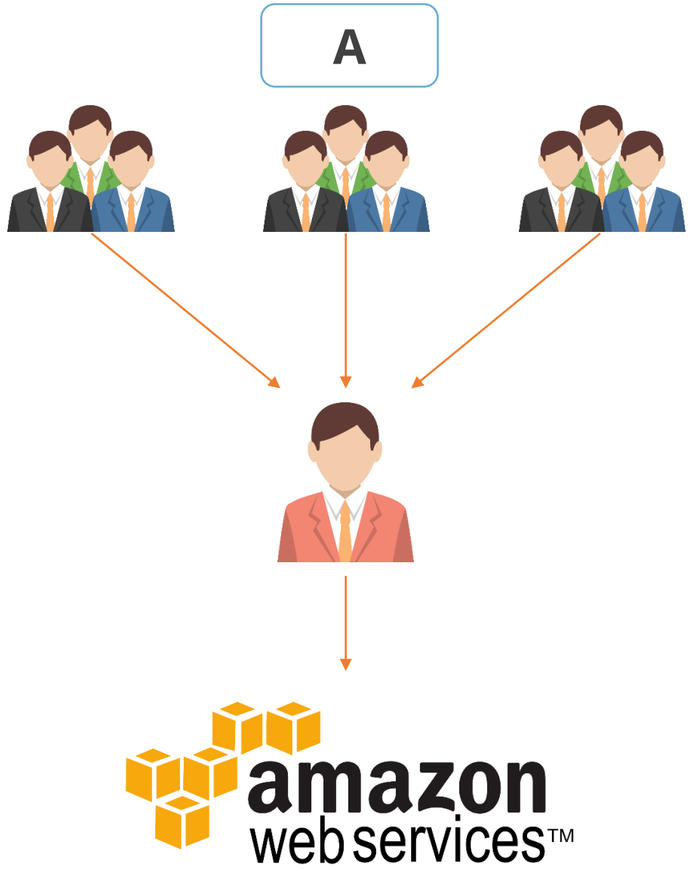
- They consist of an access key and a secret access key
- They use access keys to sign programmatic requests

Multi-Factor Authentication (MFA)

- With AWS MFA enabled, users are prompted for a user name and password and for an authentication code from an MFA device

Scenario

If you were the AWS administrator of your company, which of the following options would you use to grant user access to the AWS account?



Demo 2: Creating an IAM User

Demonstrate how to create an IAM User.

Knowledge Check

KNOWLEDGE CHECK	What will automatically be generated when you create a new user?

a. Access Key ID and Secret Access Key

b. MFA token and password

c. Secret Key and Encrypted Key

d. Access Token and Access Key

KNOWLEDGE CHECK

What will automatically be generated when you create a new user?

a. Access Key ID and Secret Access Key

b. MFA token and password

c. Secret Key and Encrypted Key

d. Access Token and Access Key

The correct answer is **a**.

New users have an Access Key ID and Secret Access Key ID generated, which are viewable only at the time the IDs are created.

KNOWLEDGE CHECK

What is the first step when you set up an AWS account?

a. Use CloudTrail to configure your account

b. Setup a role that has the same name as your company

c. Setup an account with your company email address

d. Create a JSON policy to define who in your company can log in

KNOWLEDGE CHECK

What is the first step when you set up an AWS account?

a. Use CloudTrail to configure your account

b. Setup a role that has the same name as your company

c. Setup an account with your company email address

d. Create a JSON policy to define who in your company can log in

The correct answer is **c**.

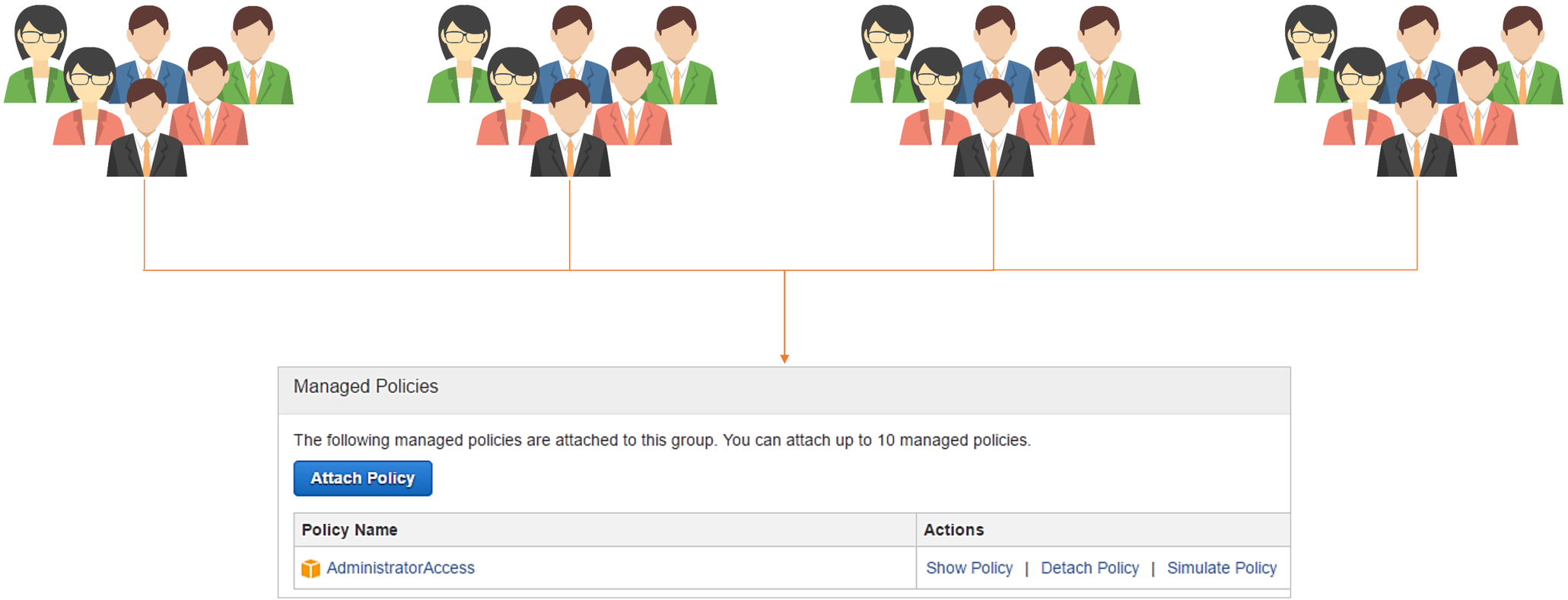
The first step is to create an account using your company email address. This account will be the root account.

IAM Groups

Description of IAM Groups

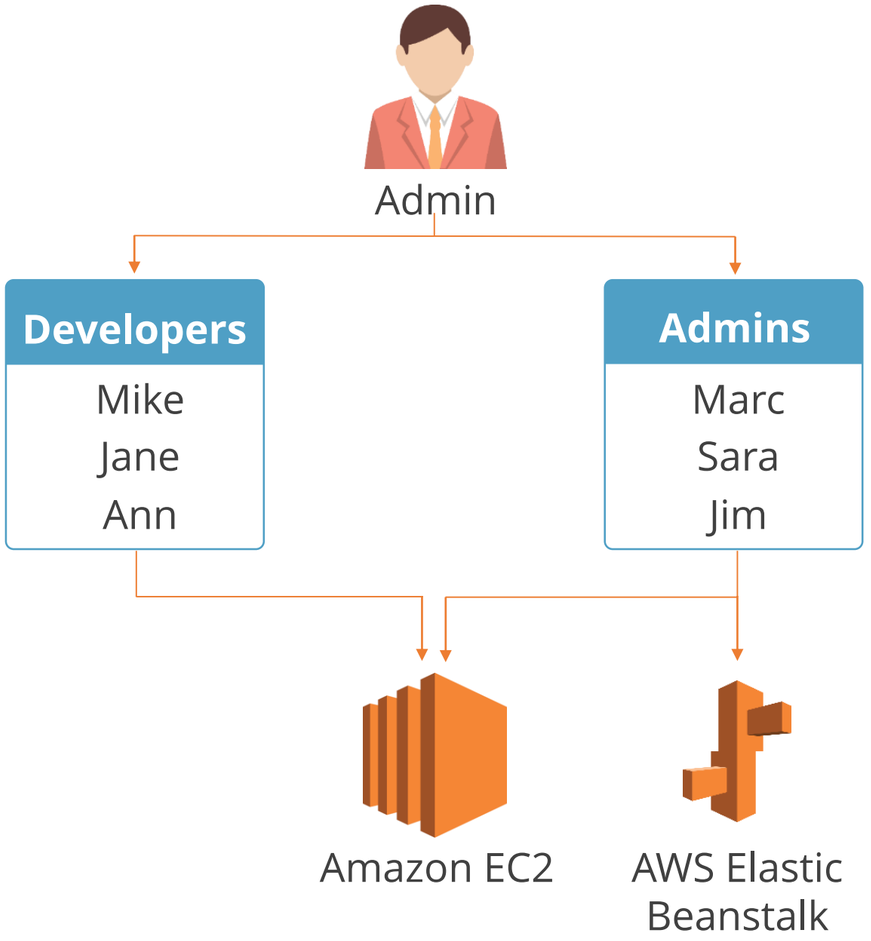
IAM Groups

AWS defines a group as a collection of users that inherit the same set of permissions.



Granting Permissions to Groups

AWS defines a group as a collection of users that inherit the same set of permissions.



Demo 3: Creating an IAM Group

Demonstrate how to create an IAM Group.

Knowledge Check

KNOWLEDGE CHECK	How does AWS define a group?

a. A collection of roles that share similar policy documents

b. A collection of users that all inherit the same set of permissions

c. An entity that controls secure access to EC2 resources

d. A resource to use when setting up MFA

KNOWLEDGE CHECK	How does AWS define a group?

a. A collection of roles that share similar policy documents

b. A collection of users that all inherit the same set of permissions

c. An entity that controls secure access to EC2 resources

d. A resource to use when setting up MFA

The correct answer is **b.**

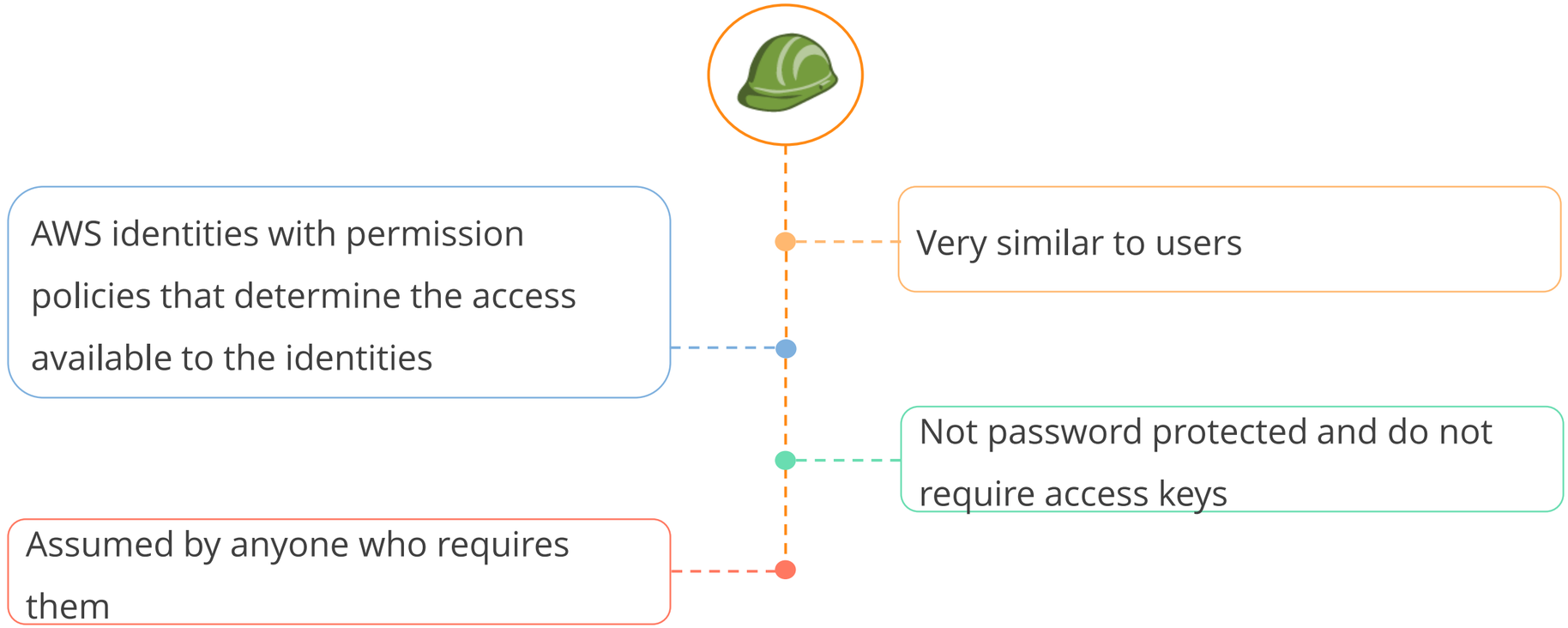
An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.

IAM Roles

Description of IAM Roles

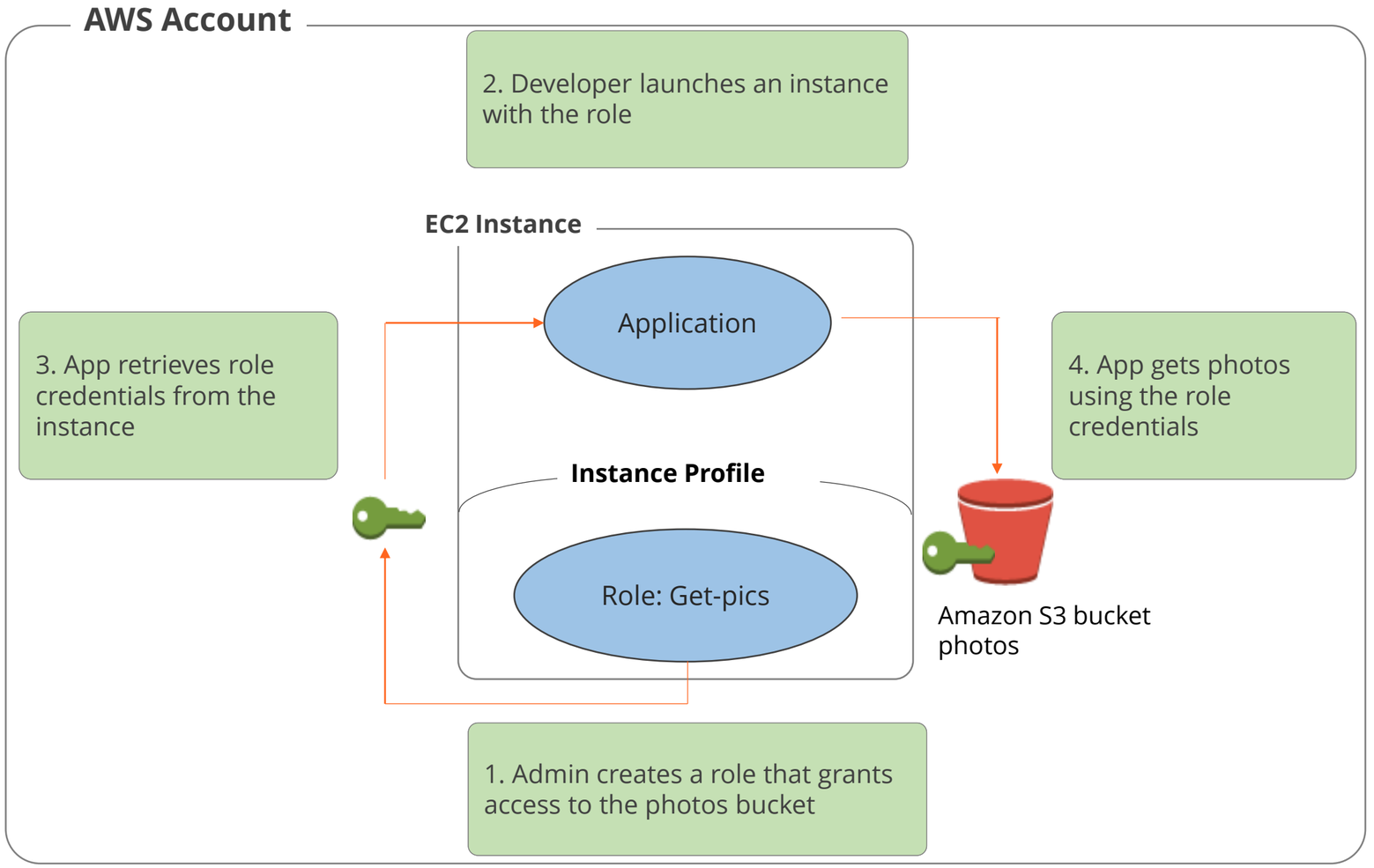
IAM Roles

IAM Roles are:



Various Functions of Roles

Roles are used to provide access to users, applications, and services that do not have permissions to use AWS resources.



Demo 4: Creating an IAM Role

Demonstrate how to create an IAM Role.

Knowledge Check

KNOWLEDGE CHECK	How do you assign permissions to an IAM user, group, or role?

a. Using a security group

b. Using a permissions document

c. Using a policy document

d. Using Identity Federation

KNOWLEDGE CHECK

How do you assign permissions to an IAM user, group, or role?

a. Using a security group

b. Using a permissions document

c. Using a policy document

d. Using Identity Federation

The correct answer is **c**.

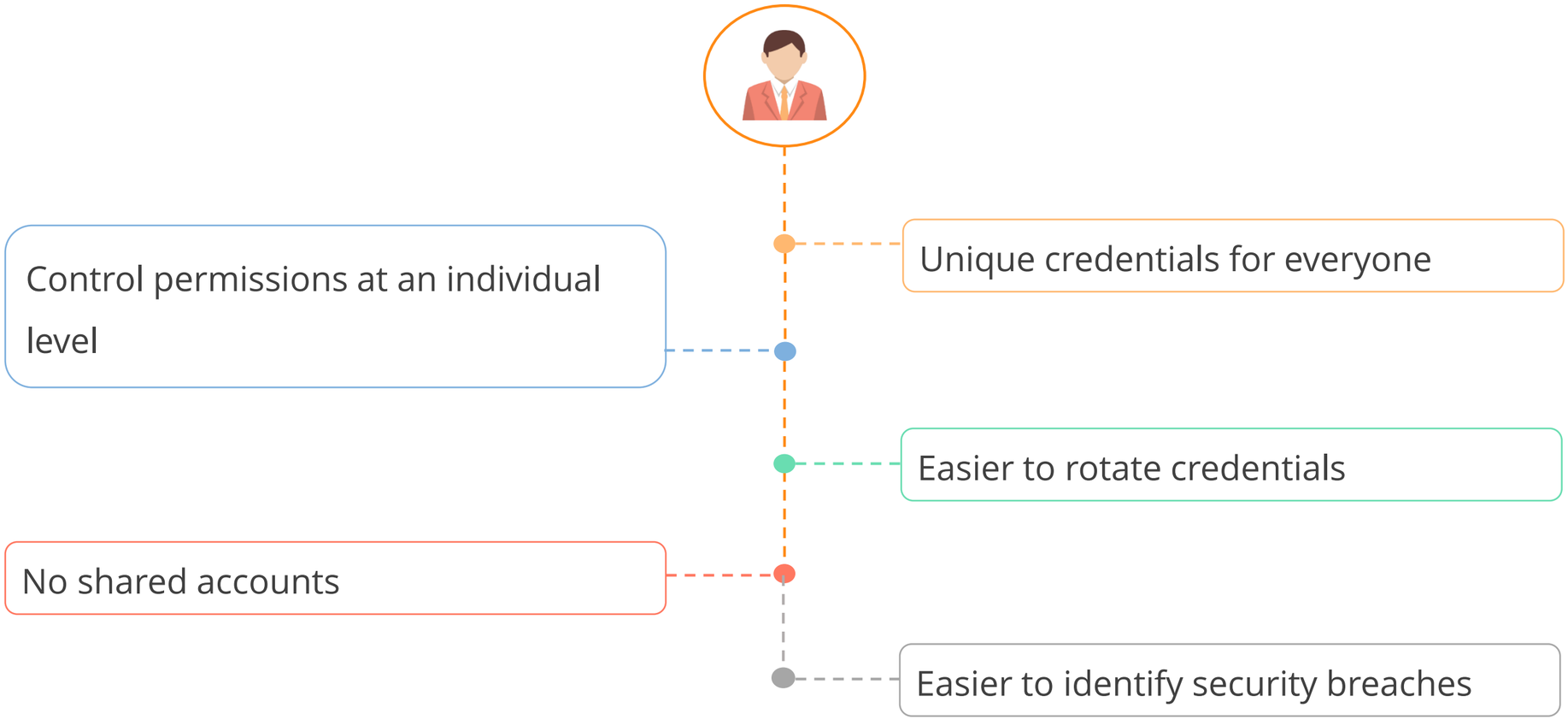
A policy document written in JSON is used to assign permissions.

IAM Best Practices

Overview of the IAM Best Practices

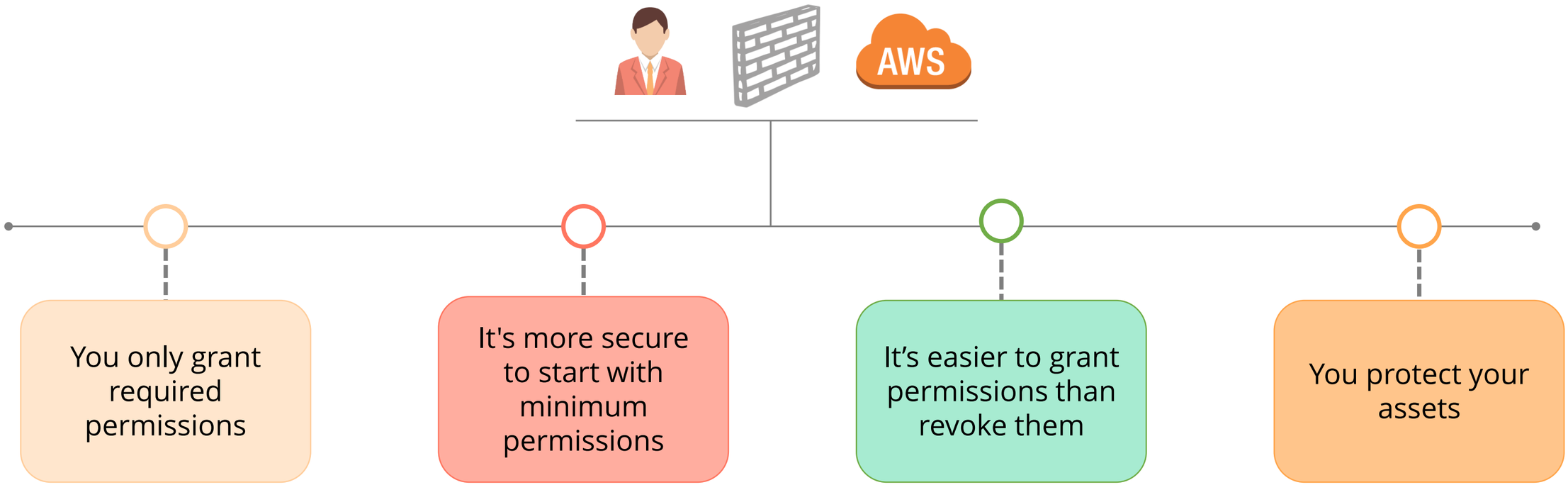
Create Individual IAM Users

The benefits of creating individual IAM users:



Grant Least Privilege

When creating IAM policies, granting ”least privilege,” means that:



Manage Permissions with Groups

Use permissions with groups to minimize the workload

Easy to assign new permissions

- It is easier to assign a new permission to a group than to assign it to many individual users.

Simple to reassign permissions

- It is simpler to reassign permissions if a user has a change in responsibilities.

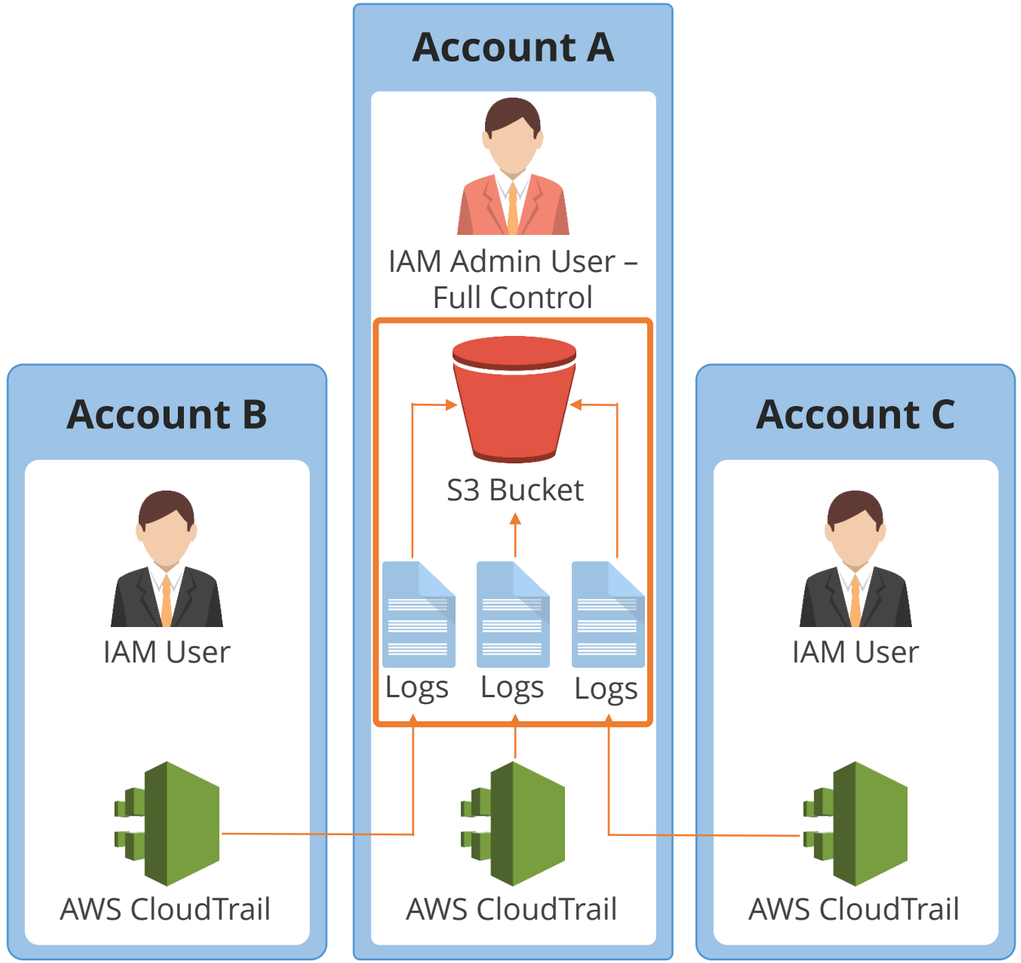
Restrict Access with Further Conditions

Use additional conditions such as MFA and Security Groups to ensure only the intended users get access.

Monitor Activity in your AWS Account (contd.)

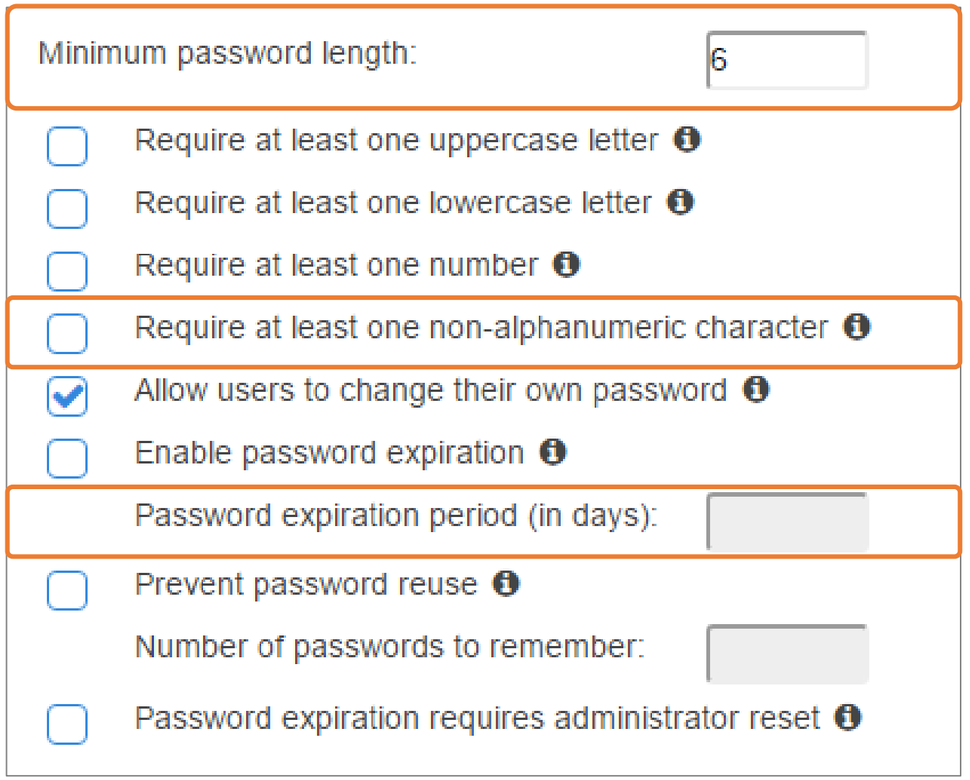
AWS has several features to log user actions.

- Logs
- AWS Cloudtrail



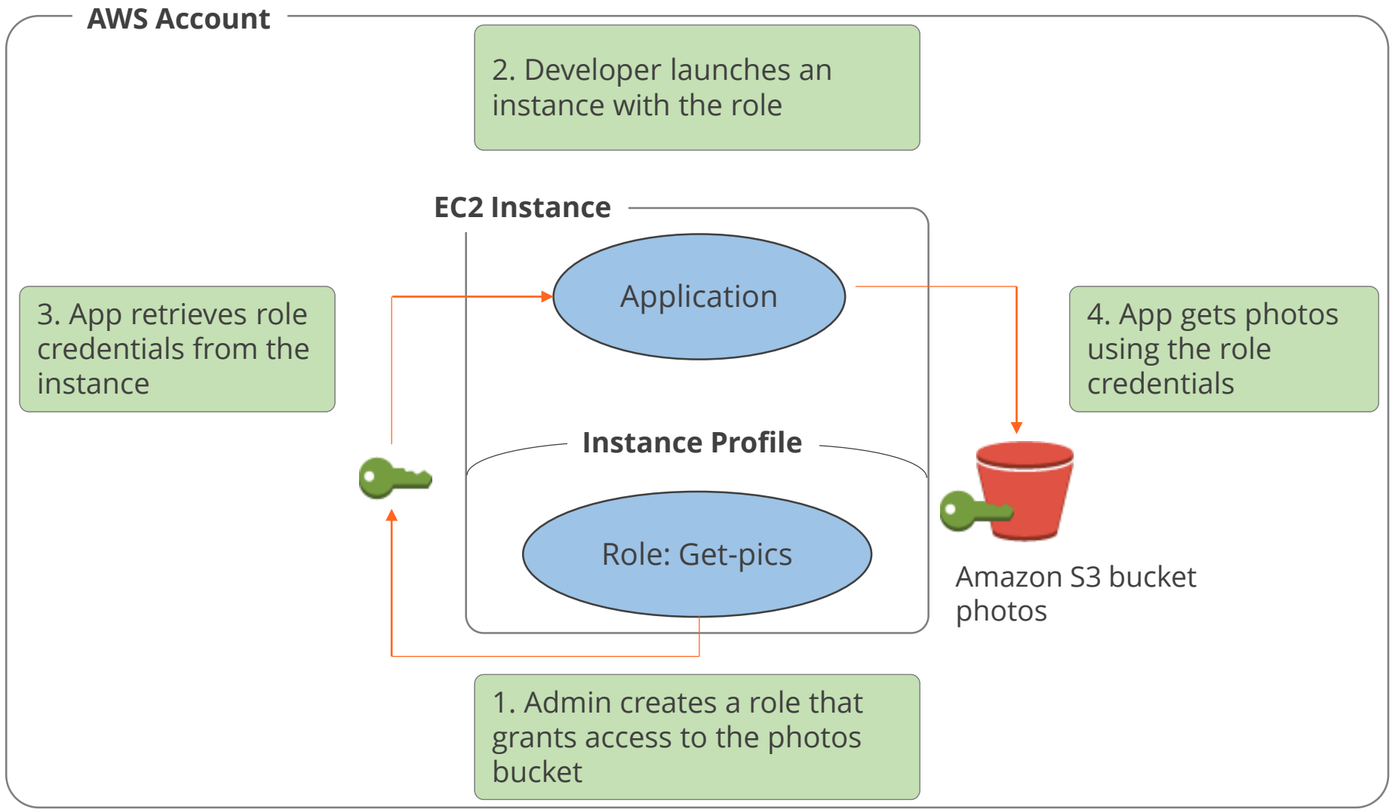
Create a Strong Password Policy

Ensure that all your users have strong passwords and they rotate their passwords regularly.



Use Roles for Applications that run on EC2

IAM Roles remove the need for your developers to store or pass credentials to AWS EC2.



Reduce or Remove Unnecessary Credentials

To reduce the potential for misuse, run a credential report to identify users that are no longer in use and can be removed.

Knowledge Check

KNOWLEDGE CHECK

What does MFA stand for?

a. Multi-Faced Access

b. Multi-Factor Administration

c. Mission Factored Authentication

d. Multi-Factor Authentication

KNOWLEDGE CHECK

What does MFA stand for?

a. Multi-Faced Access

b. Multi-Factor Administration

c. Mission Factored Authentication

d. Multi-Factor Authentication

The correct answer is **d**.

For increased security, AWS recommends that you configure multi-factor authentication (MFA) to help protect your AWS resources. MFA adds extra security because it requires users to enter a unique authentication code from an approved authentication device or SMS text message when they access AWS websites or services.

KNOWLEDGE CHECK	What AWS tool is used to track, monitor, and log IAM user activity?

a. CloudFormation

b. Inspector

c. CloudWatch

d. CloudTrail

KNOWLEDGE CHECK

What AWS tool is used to track, monitor, and log IAM user activity?

a. CloudFormation

b. Inspector

c. CloudWatch

d. CloudTrail

The correct answer is **d**.

CloudTrail is used to track user activity. CloudFormation allows you to manage resources with templates, CloudWatch monitors application activity, and Inspector analyzes application security.

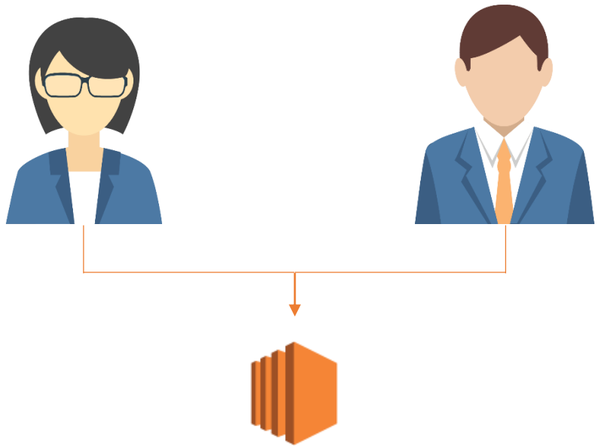
Practice Assignment: Configuring IAM Access

Use IAM to configure user access to AWS

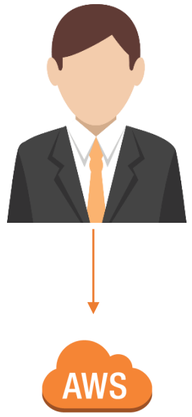
Configuring IAM Access

As the admin for your company's AWS account, you need to assign permissions to four new users:

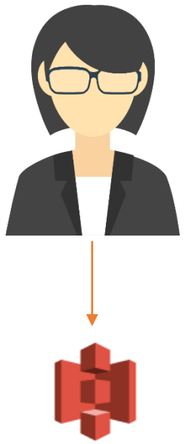
Two users require full access to EC2.



One user requires administration access to all AWS resources.



One user requires read-only access to S3.



Use AWS Best Practices when configuring the user access; so ensure you use groups.

Key Takeaways

Key Takeaways

- AWS Identity and Access Management (IAM) allows you to securely control access to AWS services and resources for your users.
- Policies are written in JSON and allow you to define granular access to AWS resources.
- Users are the people or systems that use your AWS resources, like admins, end users, or systems, which need permissions to access your AWS data.
- Groups are a collection of users that inherit the same set of permissions and can be used to reduce your user management overhead.
- IAM roles can be assumed by anyone who needs them, and they do not have an access keys or passwords associated with them.
- AWS has a list of IAM best practices to ensure your environment is secure and safe.

This concludes “Identity and Access Management.”

The next lesson is “Virtual Private Cloud.”