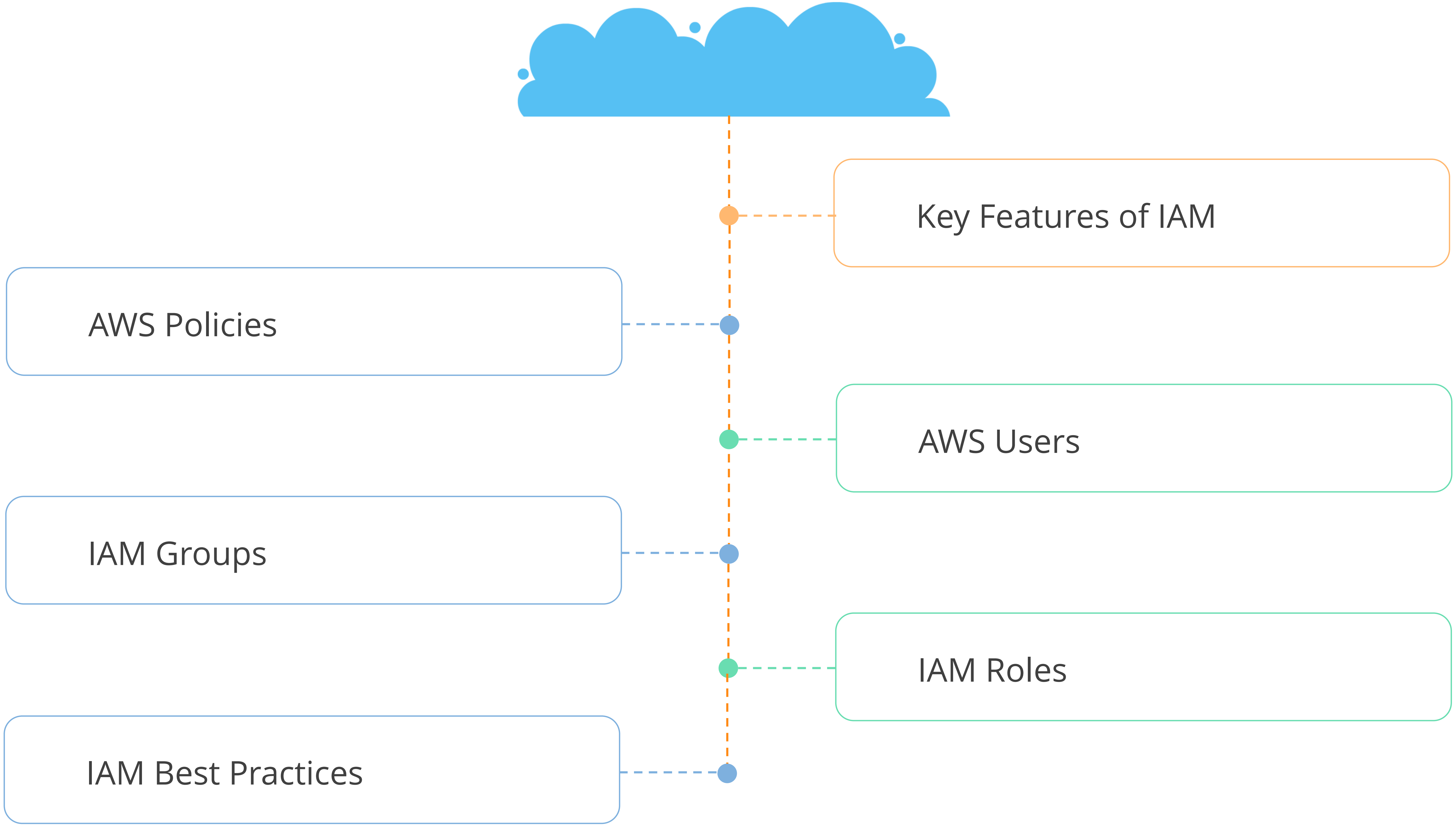
AWS Solutions Architect—Associate Level

Lesson 3: Identity and Access Management (IAM)

What You’ll Learn



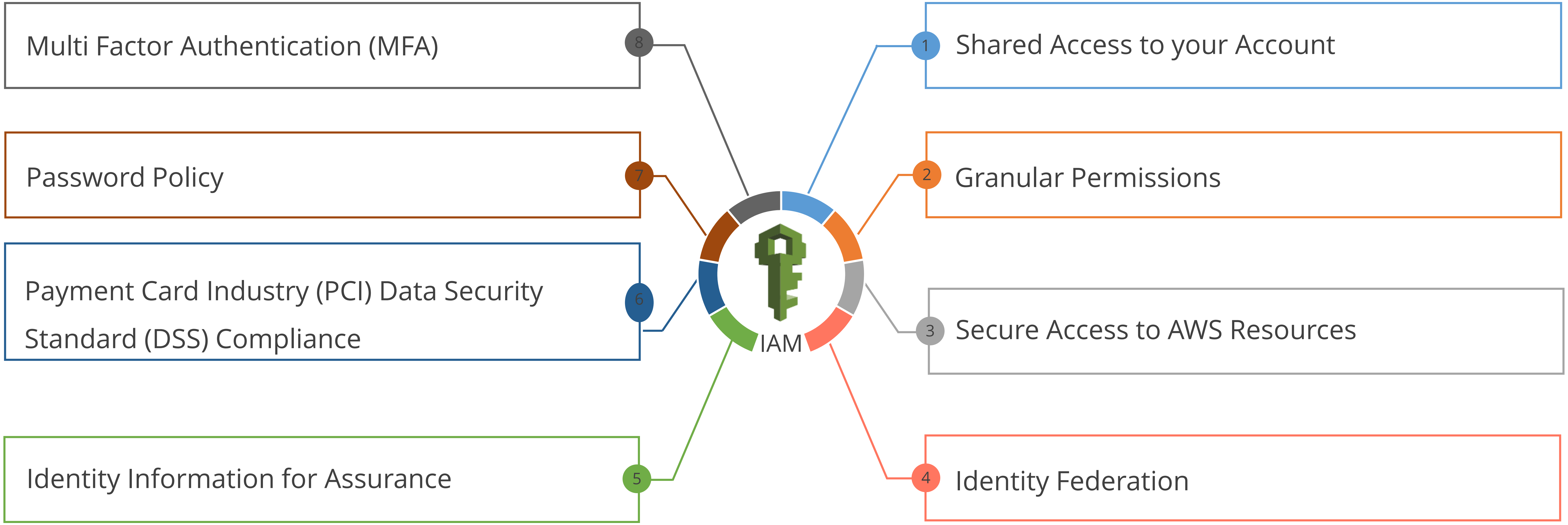
- Key Features of IAM
- AWS Policies
- AWS Users
- IAM Groups
- IAM Roles
- IAM Best Practices

IAM Overview

Overview of AWS IAM

Identity and Access Management

The key features of IAM:



1 Shared Access to your Account

2 Granular Permissions

3 Secure Access to AWS Resources

4 Identity Federation

5 Identity Information for Assurance

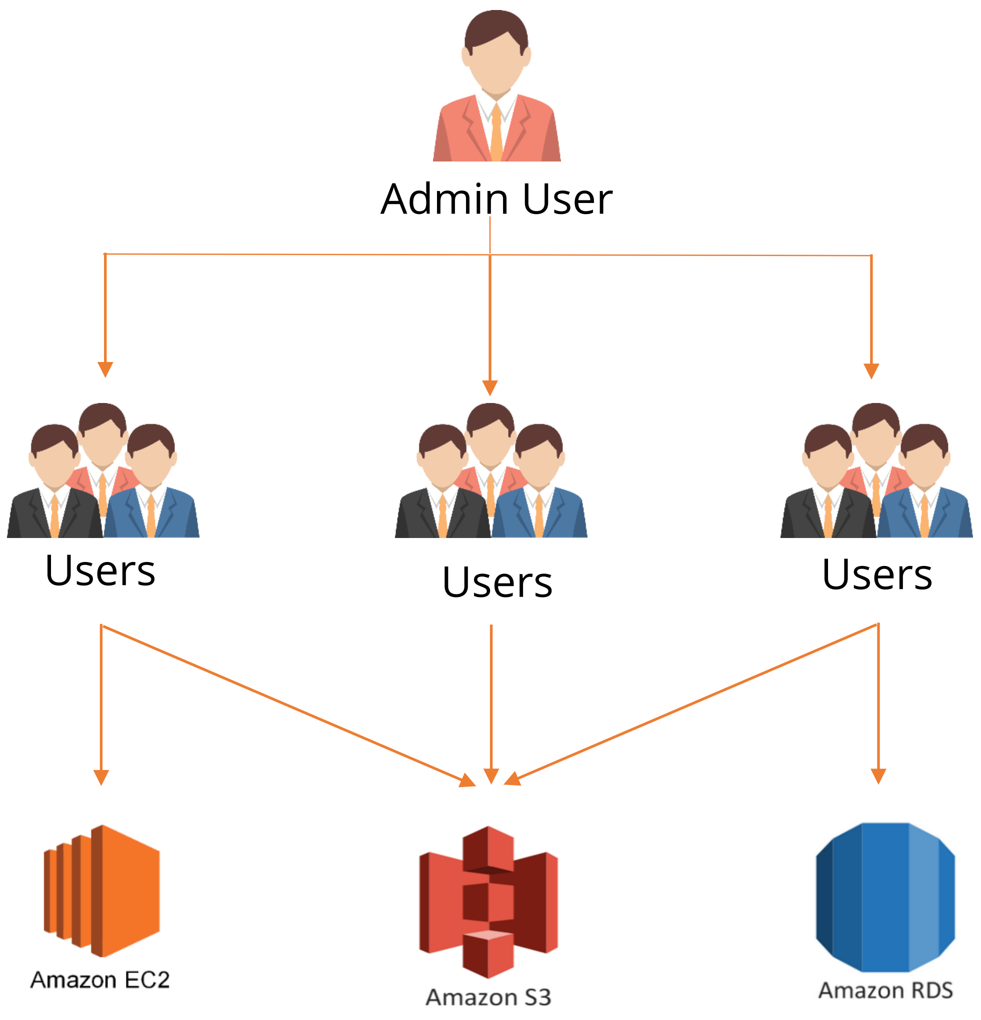
6 Payment Card Industry (PCI) Data Security Standard (DSS) Compliance

7 Password Policy

8 Multi Factor Authentication (MFA)

Shared Access

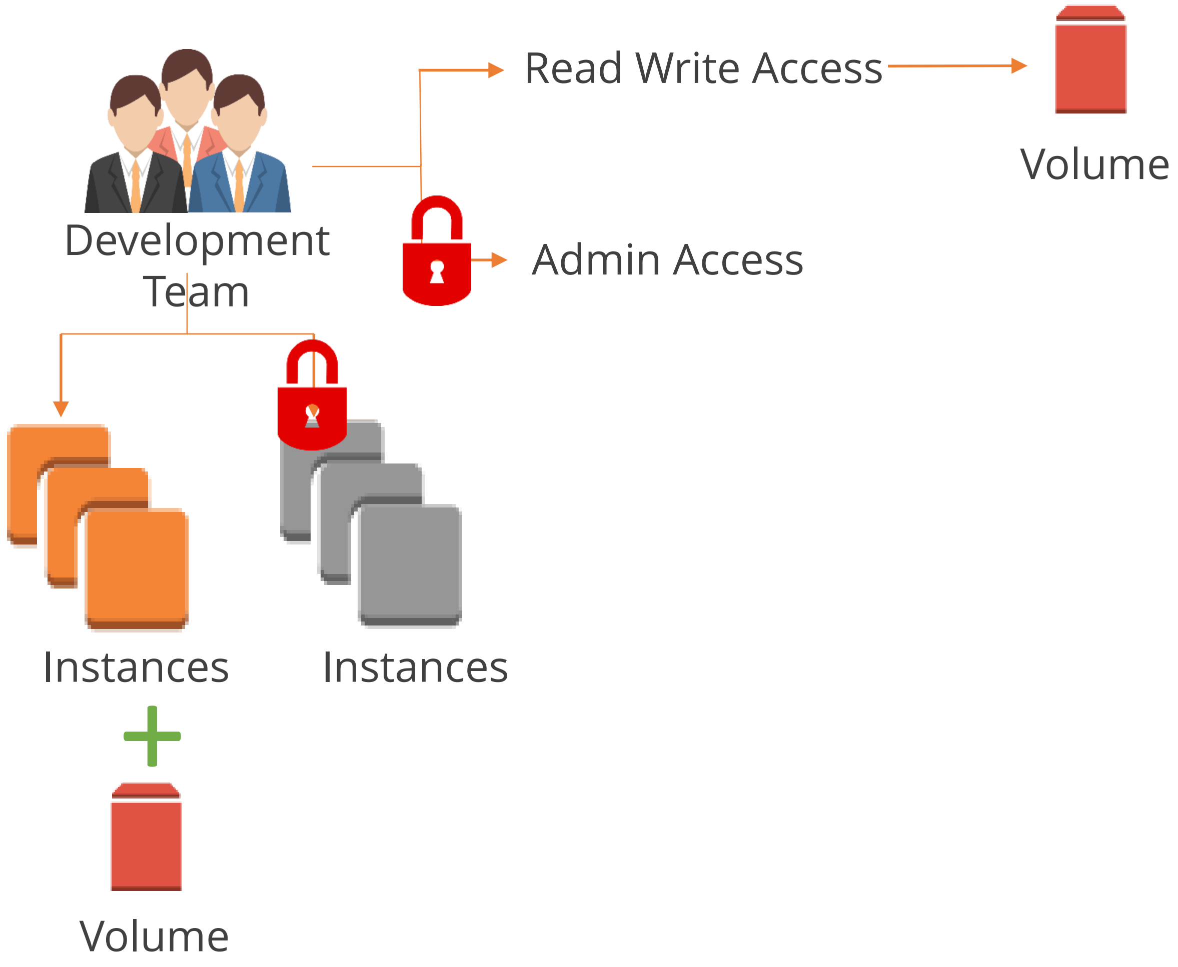
Grant permission to users to access and use resources in your AWS account without sharing your password.



Granular Permissions

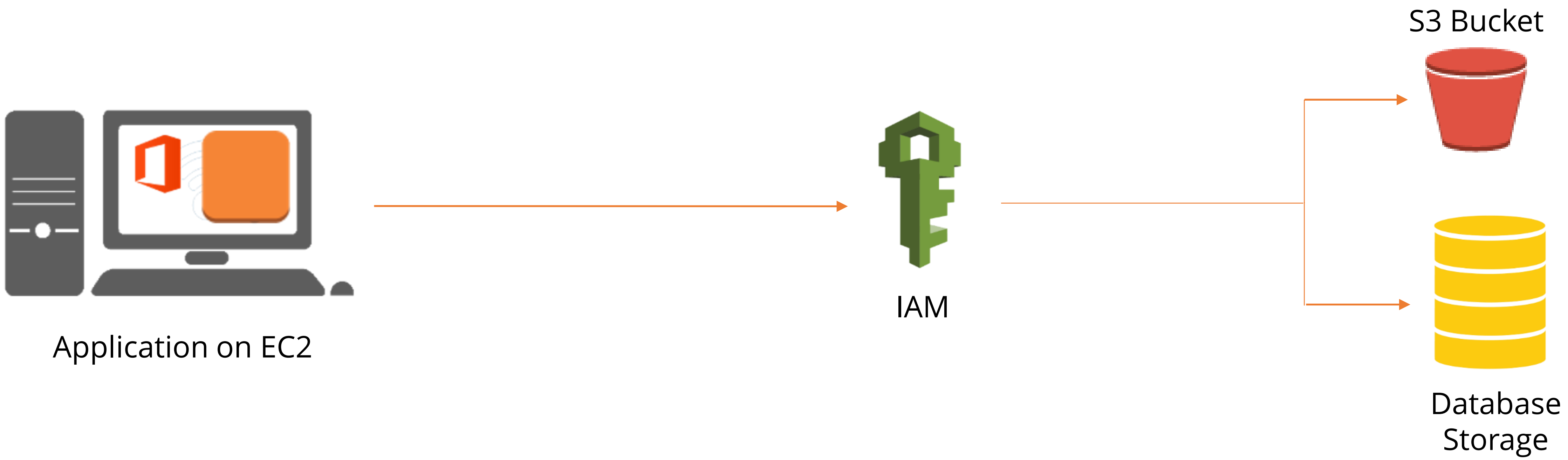
Granular permissions allow different permissions to various users to manage their access to AWS, such as:

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



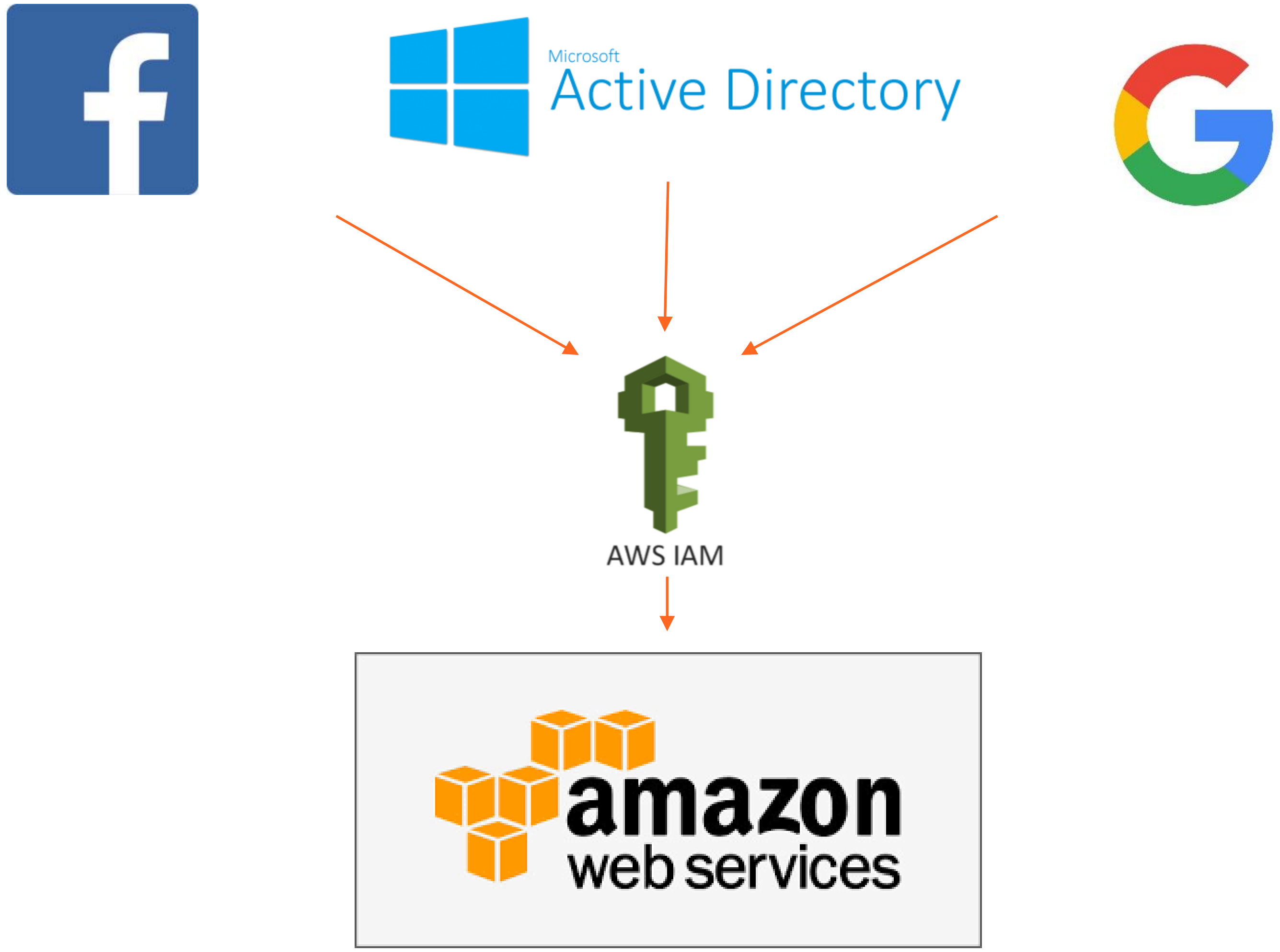
Secure Access

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



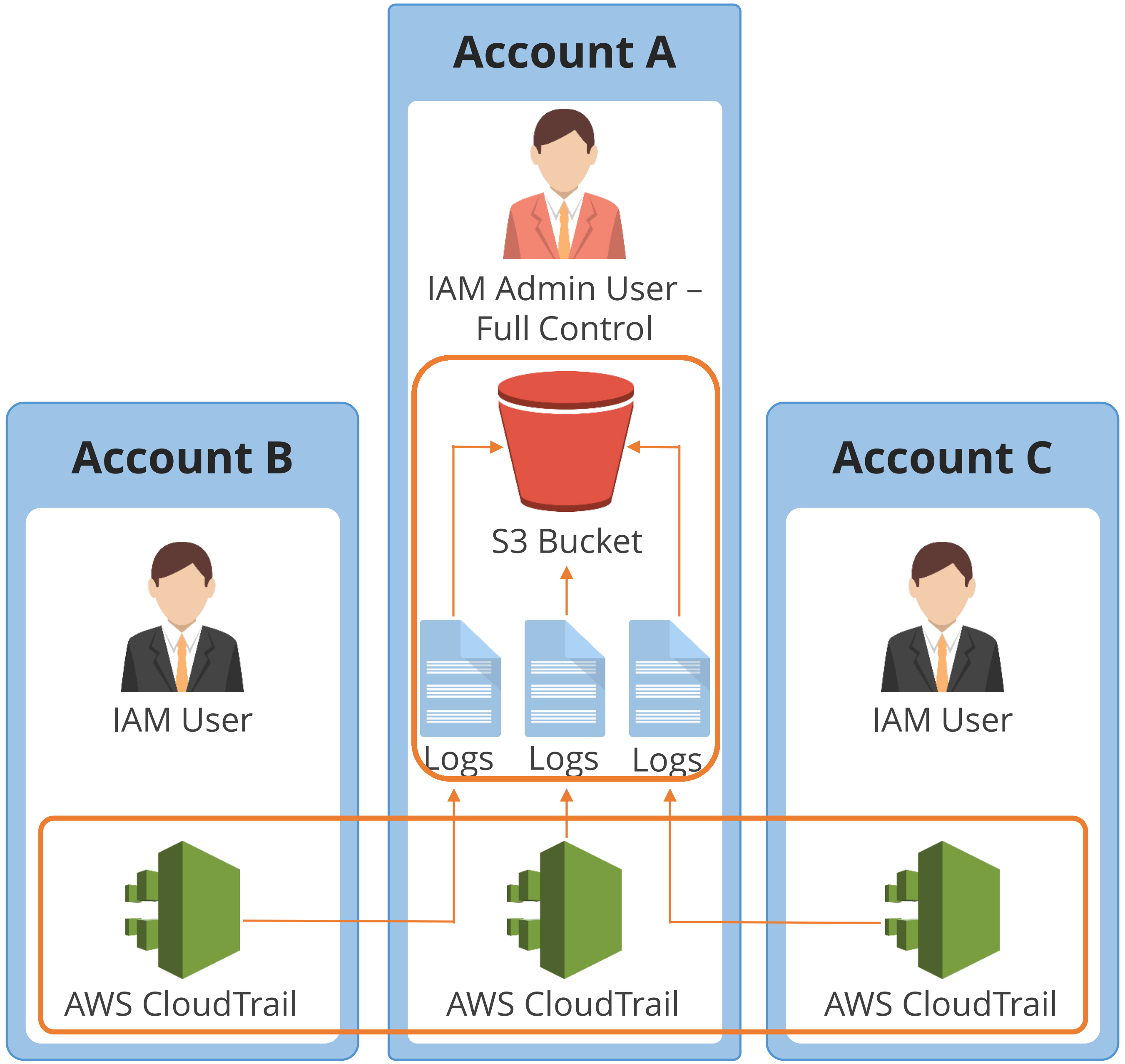
Identity Federation

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.

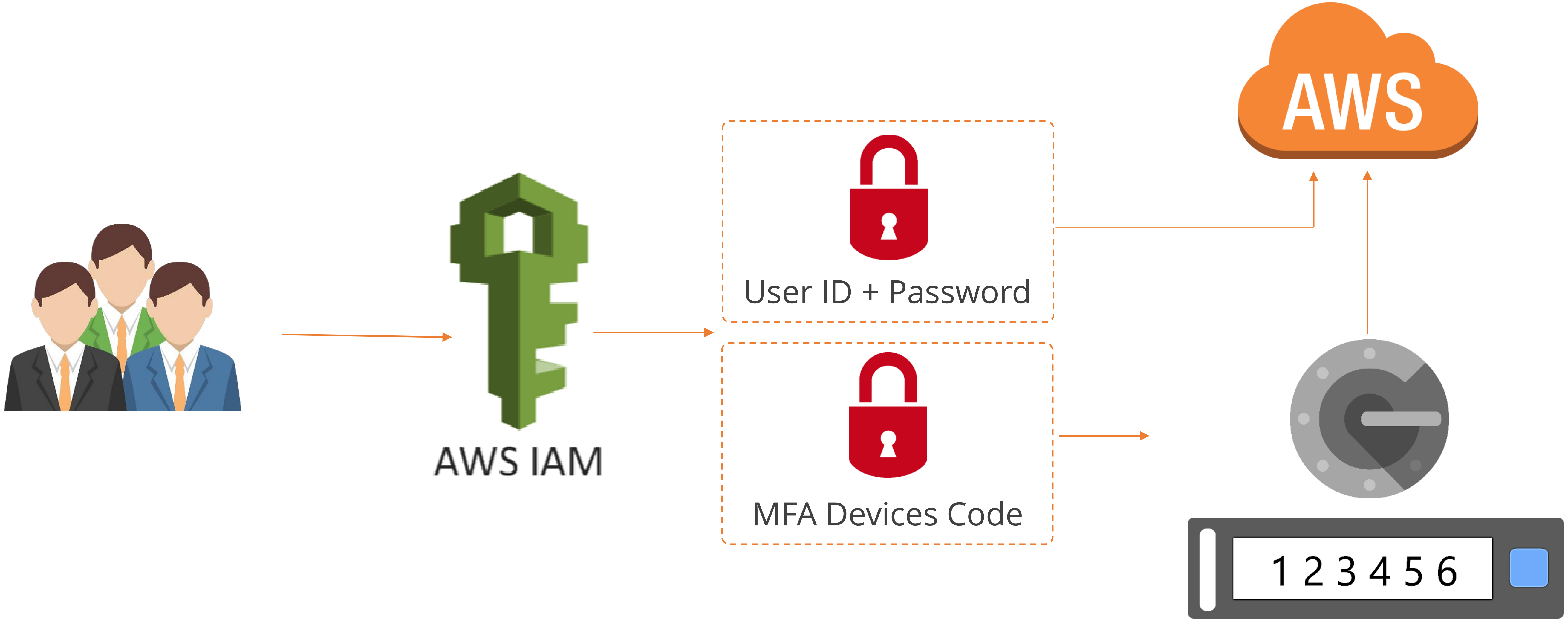


PCI DSS Compliance

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

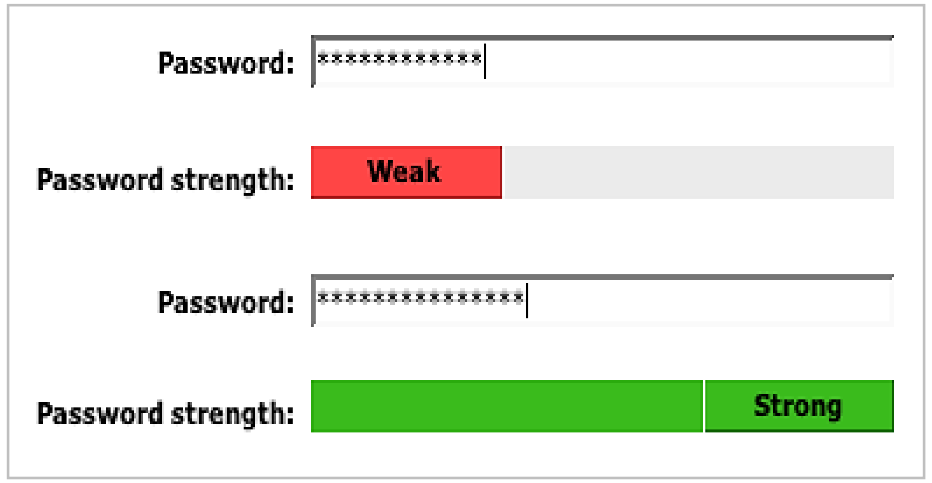
Multi-Factor Authentication

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.

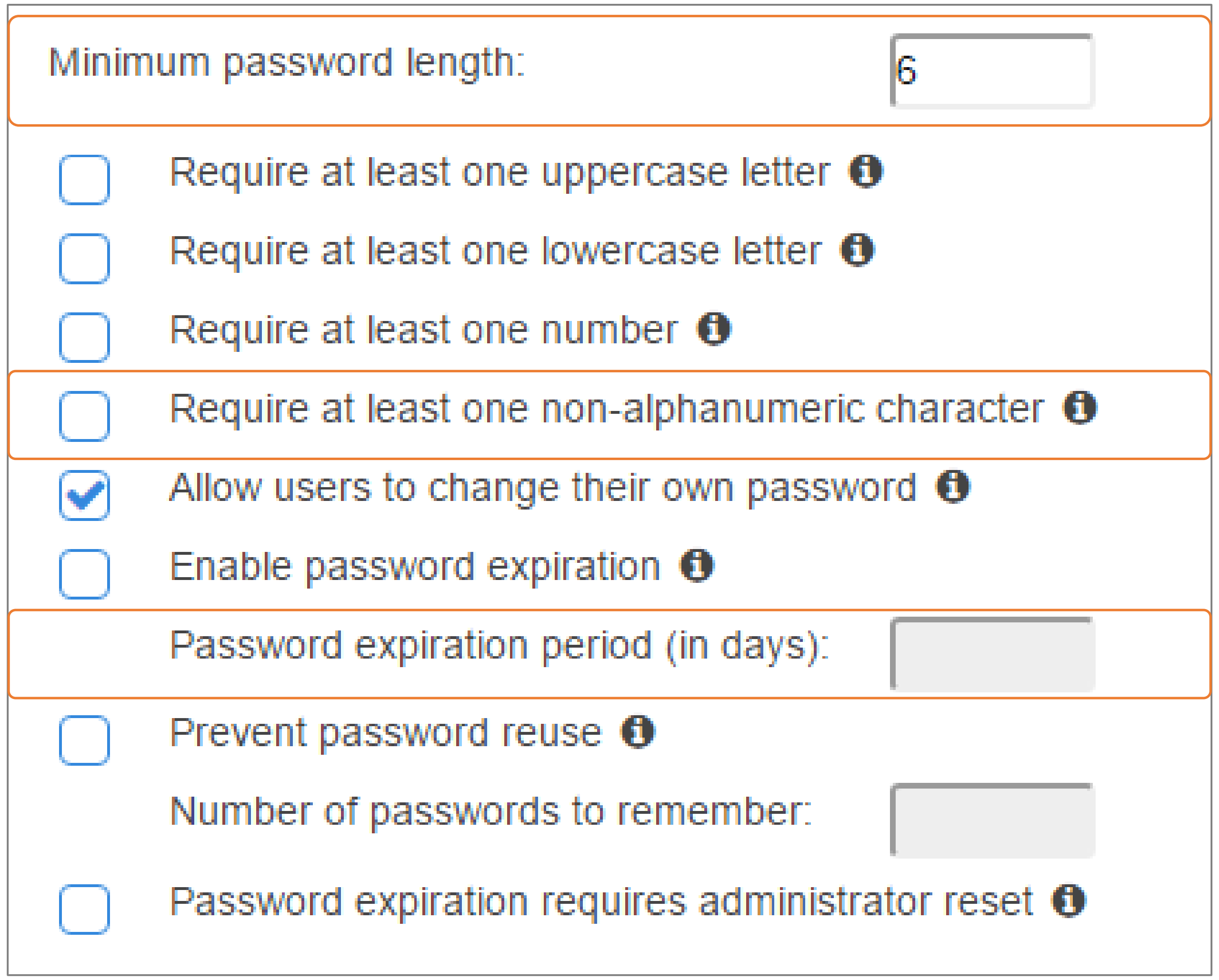


Password: ************

Password strength: Weak

Password: ***************

Password strength: Strong



Minimum password length: 6

□ Require at least one uppercase letter ℹ

□ Require at least one lowercase letter ℹ

□ Require at least one number ℹ

□ Require at least one non-alphanumeric character ℹ

☑ Allow users to change their own password ℹ

□ Enable password expiration ℹ

Password expiration period (in days):

□ Prevent password reuse ℹ

Number of passwords to remember:

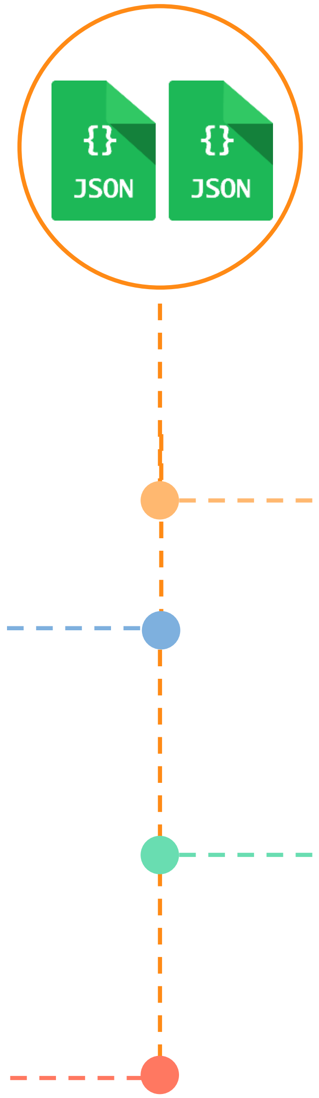
□ Password expiration requires administrator reset ℹ

IAM Policies

Description of IAM Policies

IAM Policies

An IAM policy is:



A document that defines one or more permissions

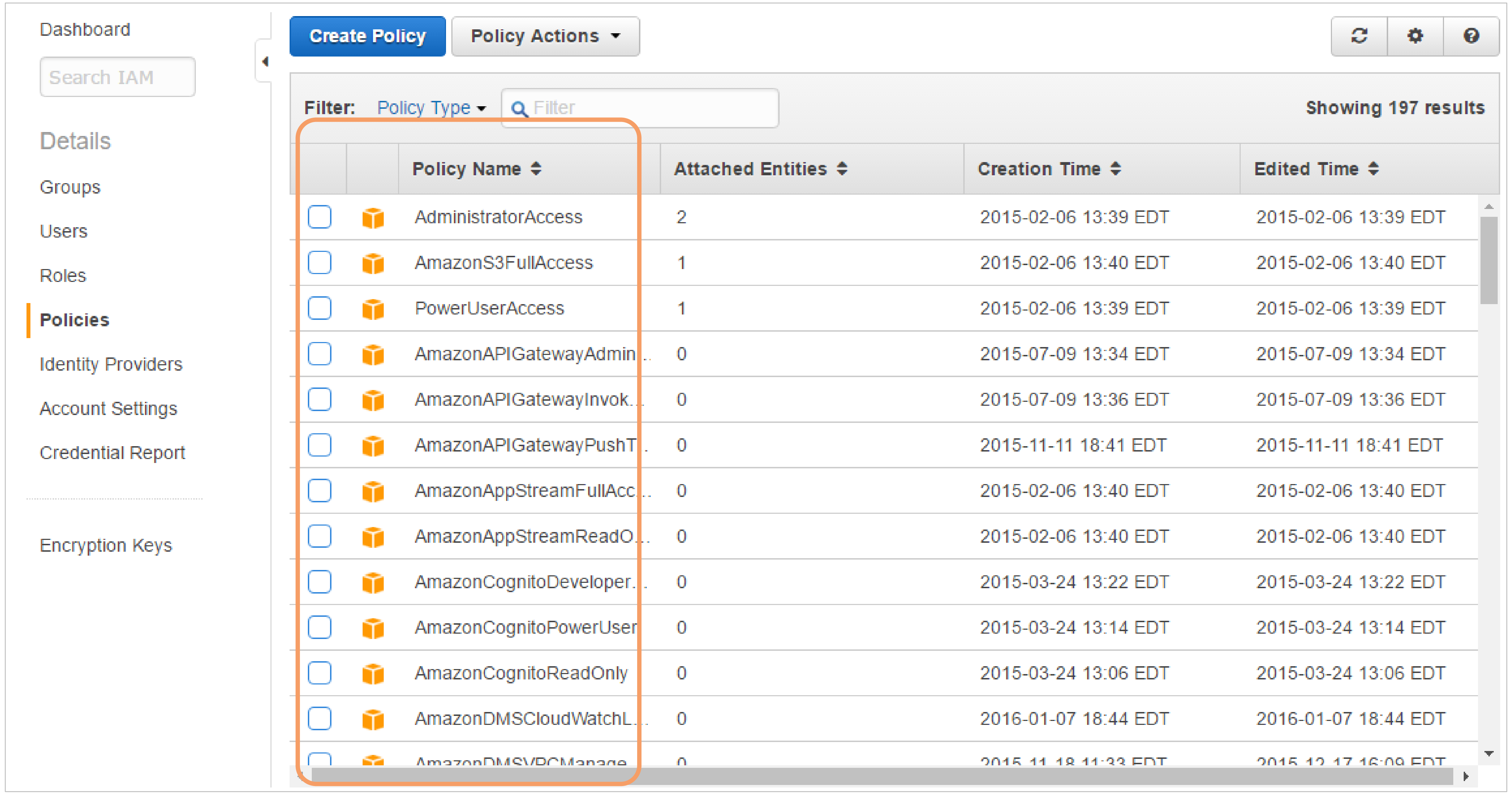
Attached to users, groups, and roles

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.



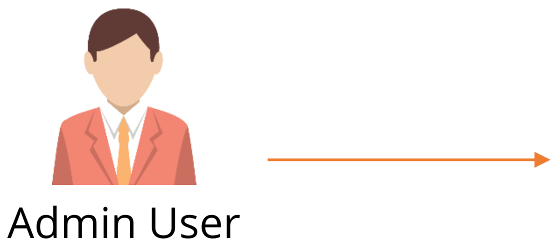
Showing 197 results

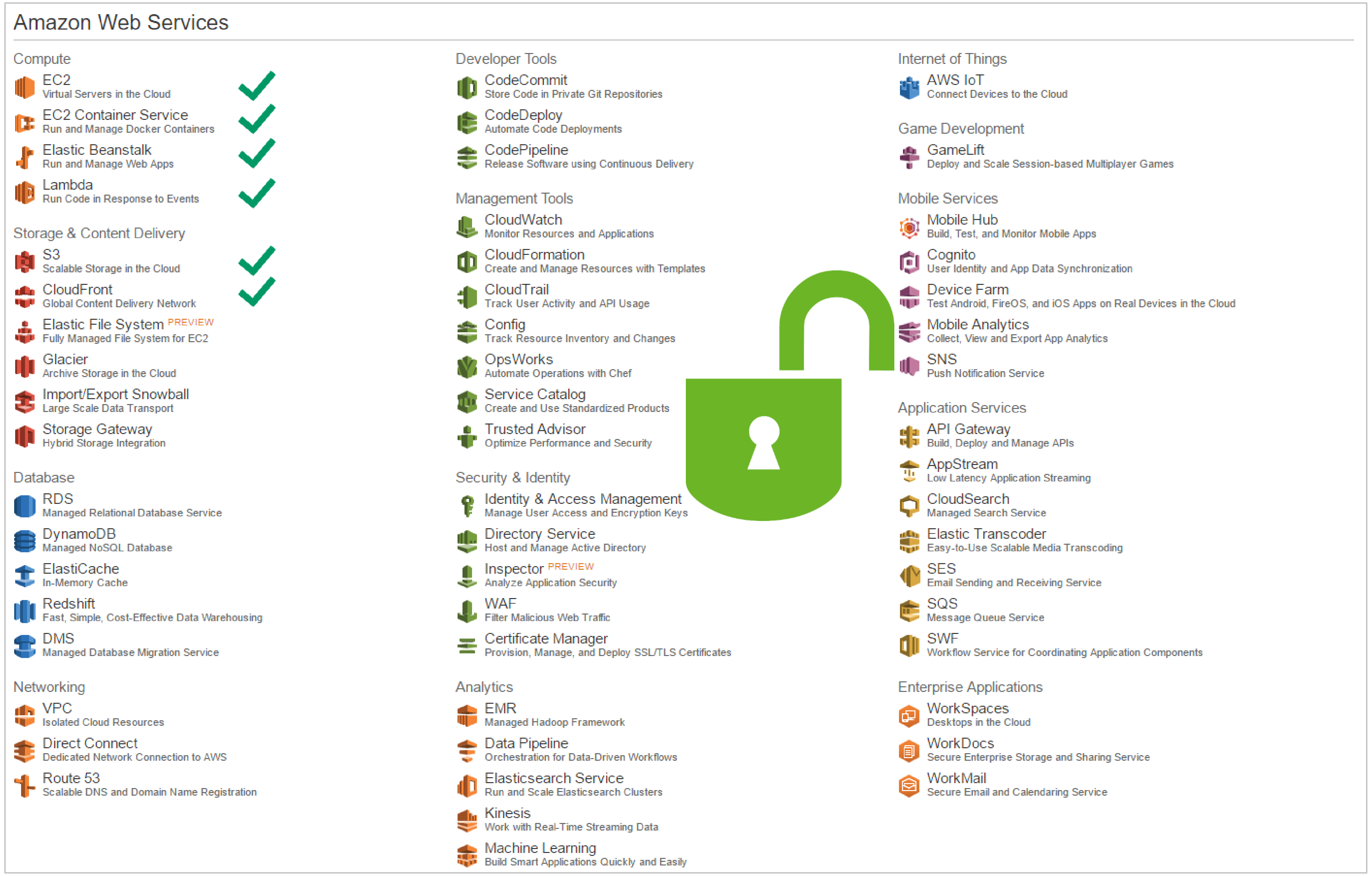
	Policy Name	Attached Entities	Creation Time	Edited Time
☐	AdministratorAccess	2	2015-02-06 13:39 EDT	2015-02-06 13:39 EDT
☐	AmazonS3FullAccess	1	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT
☐	PowerUserAccess	1	2015-02-06 13:39 EDT	2015-02-06 13:39 EDT
☐	AmazonAPIGatewayAdmin...	0	2015-07-09 13:34 EDT	2015-07-09 13:34 EDT
☐	AmazonAPIGatewayInvok...	0	2015-07-09 13:36 EDT	2015-07-09 13:36 EDT
☐	AmazonAPIGatewayPushT...	0	2015-11-11 18:41 EDT	2015-11-11 18:41 EDT
☐	AmazonAppStreamFullAcc...	0	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT
☐	AmazonAppStreamReadO...	0	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT
☐	AmazonCognitoDeveloper...	0	2015-03-24 13:22 EDT	2015-03-24 13:22 EDT
☐	AmazonCognitoPowerUser	0	2015-03-24 13:14 EDT	2015-03-24 13:14 EDT
☐	AmazonCognitoReadOnly	0	2015-03-24 13:06 EDT	2015-03-24 13:06 EDT
☐	AmazonDMSCloudWatchL...	0	2016-01-07 18:44 EDT	2016-01-07 18:44 EDT
☐	AmazonDMSVPCManage...	0	2015-11-18 11:33 EDT	2015-12-17 16:09 EDT

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

AdministratorAccess Policy

AdministratorAccess policy provides full access to AWS services and resources.





Amazon Web Services

Compute

- EC2 ✓
  Virtual Servers in the Cloud
- EC2 Container Service ✓
  Run and Manage Docker Containers
- Elastic Beanstalk ✓
  Run and Manage Web Apps
- Lambda ✓
  Run Code in Response to Events

Storage & Content Delivery

- S3 ✓
  Scalable Storage in the Cloud
- CloudFront ✓
  Global Content Delivery Network
- Elastic File System PREVIEW
  Fully Managed File System for EC2
- Glacier
  Archive Storage in the Cloud
- Import/Export Snowball
  Large Scale Data Transport
- Storage Gateway
  Hybrid Storage Integration

Database

- RDS
  Managed Relational Database Service
- DynamoDB
  Managed NoSQL Database
- ElastiCache
  In-Memory Cache
- Redshift
  Fast, Simple, Cost-Effective Data Warehousing
- DMS
  Managed Database Migration Service

Networking

- VPC
  Isolated Cloud Resources
- Direct Connect
  Dedicated Network Connection to AWS
- Route 53
  Scalable DNS and Domain Name Registration

Developer Tools

- CodeCommit
  Store Code in Private Git Repositories
- CodeDeploy
  Automate Code Deployments
- CodePipeline
  Release Software using Continuous Delivery

Management Tools

- CloudWatch
  Monitor Resources and Applications
- CloudFormation
  Create and Manage Resources with Templates
- CloudTrail
  Track User Activity and API Usage
- Config
  Track Resource Inventory and Changes
- OpsWorks
  Automate Operations with Chef
- Service Catalog
  Create and Use Standardized Products
- Trusted Advisor
  Optimize Performance and Security

Security & Identity

- Identity & Access Management
  Manage User Access and Encryption Keys
- Directory Service
  Host and Manage Active Directory
- Inspector PREVIEW
  Analyze Application Security
- WAF
  Filter Malicious Web Traffic
- Certificate Manager
  Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

- EMR
  Managed Hadoop Framework
- Data Pipeline
  Orchestration for Data-Driven Workflows
- Elasticsearch Service
  Run and Scale Elasticsearch Clusters
- Kinesis
  Work with Real-Time Streaming Data
- Machine Learning
  Build Smart Applications Quickly and Easily

Internet of Things

- AWS IoT
  Connect Devices to the Cloud

Game Development

- GameLift
  Deploy and Scale Session-based Multiplayer Games

Mobile Services

- Mobile Hub
  Build, Test, and Monitor Mobile Apps
- Cognito
  User Identity and App Data Synchronization
- Device Farm
  Test Android, FireOS, and iOS Apps on Real Devices in the Cloud
- Mobile Analytics
  Collect, View and Export App Analytics
- SNS
  Push Notification Service

Application Services

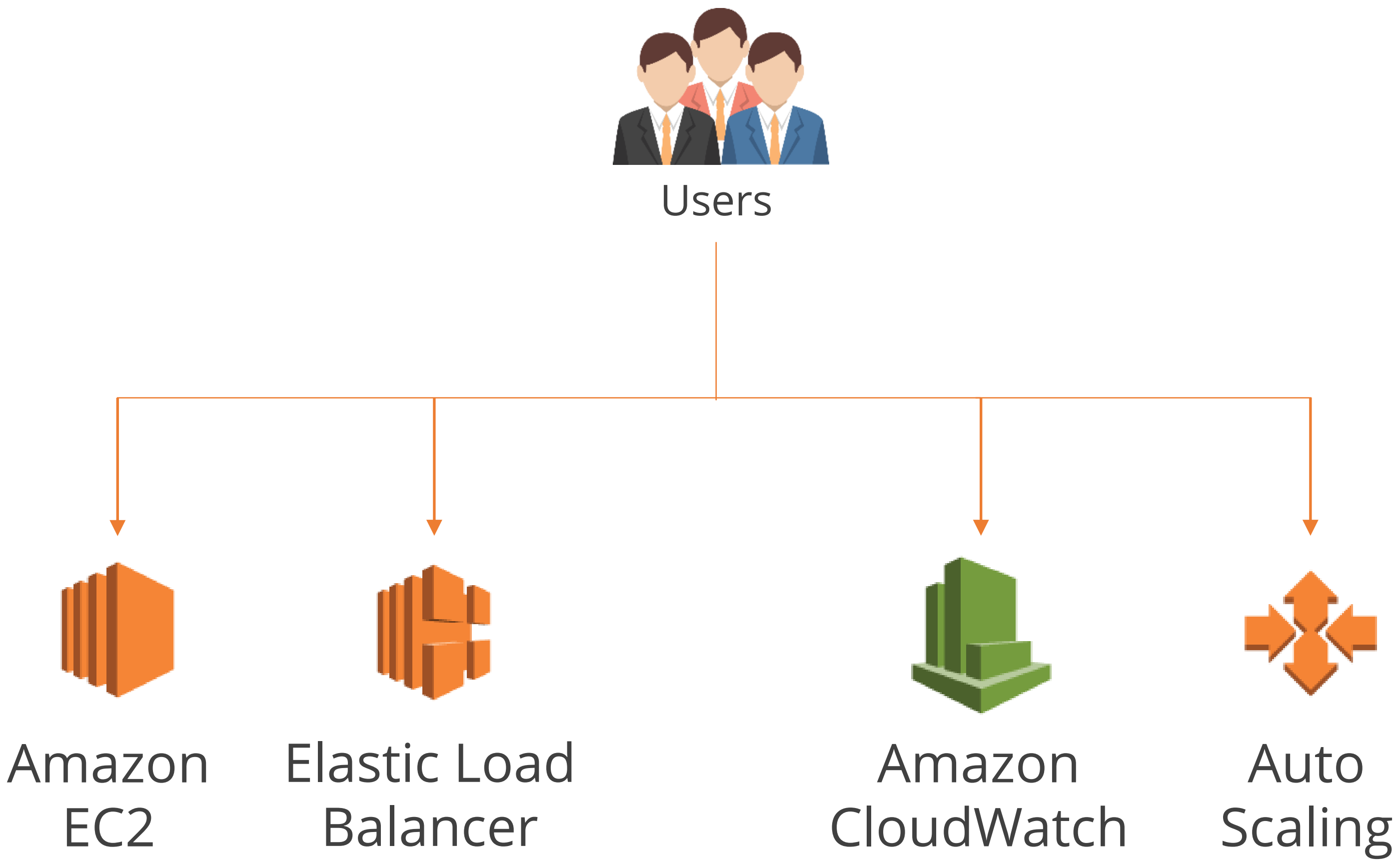
- API Gateway
  Build, Deploy and Manage APIs
- AppStream
  Low Latency Application Streaming
- CloudSearch
  Managed Search Service
- Elastic Transcoder
  Easy-to-Use Scalable Media Transcoding
- SES
  Email Sending and Receiving Service
- SQS
  Message Queue Service
- SWF
  Workflow Service for Coordinating Application Components

Enterprise Applications

- WorkSpaces
  Desktops in the Cloud
- WorkDocs
  Secure Enterprise Storage and Sharing Service
- WorkMail
  Secure Email and Calendaring Service

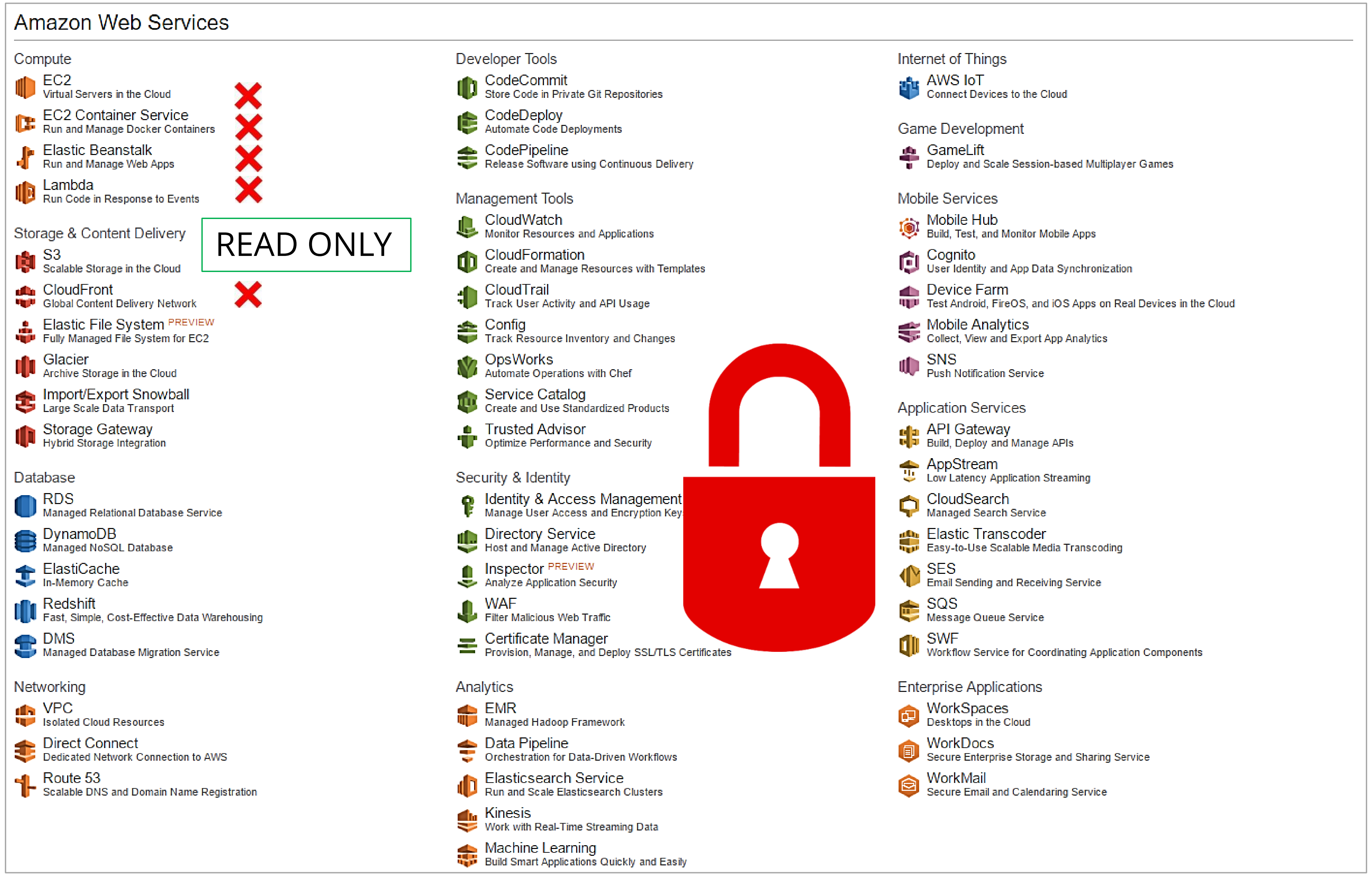
AmazonEC2FullAccess Policy

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.



Amazon Web Services

Compute

- EC2 – Virtual Servers in the Cloud ✗
- EC2 Container Service – Run and Manage Docker Containers ✗
- Elastic Beanstalk – Run and Manage Web Apps ✗
- Lambda – Run Code in Response to Events ✗

Storage & Content Delivery

- S3 – Scalable Storage in the Cloud — READ ONLY
- CloudFront – Global Content Delivery Network ✗
- Elastic File System PREVIEW – Fully Managed File System for EC2
- Glacier – Archive Storage in the Cloud
- Import/Export Snowball – Large Scale Data Transport
- Storage Gateway – Hybrid Storage Integration

Database

- RDS – Managed Relational Database Service
- DynamoDB – Managed NoSQL Database
- ElastiCache – In-Memory Cache
- Redshift – Fast, Simple, Cost-Effective Data Warehousing
- DMS – Managed Database Migration Service

Networking

- VPC – Isolated Cloud Resources
- Direct Connect – Dedicated Network Connection to AWS
- Route 53 – Scalable DNS and Domain Name Registration

Developer Tools

- CodeCommit – Store Code in Private Git Repositories
- CodeDeploy – Automate Code Deployments
- CodePipeline – Release Software using Continuous Delivery

Management Tools

- CloudWatch – Monitor Resources and Applications
- CloudFormation – Create and Manage Resources with Templates
- CloudTrail – Track User Activity and API Usage
- Config – Track Resource Inventory and Changes
- OpsWorks – Automate Operations with Chef
- Service Catalog – Create and Use Standardized Products
- Trusted Advisor – Optimize Performance and Security

Security & Identity

- Identity & Access Management – Manage User Access and Encryption Key
- Directory Service – Host and Manage Active Directory
- Inspector PREVIEW – Analyze Application Security
- WAF – Filter Malicious Web Traffic
- Certificate Manager – Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

- EMR – Managed Hadoop Framework
- Data Pipeline – Orchestration for Data-Driven Workflows
- Elasticsearch Service – Run and Scale Elasticsearch Clusters
- Kinesis – Work with Real-Time Streaming Data
- Machine Learning – Build Smart Applications Quickly and Easily

Internet of Things

- AWS IoT – Connect Devices to the Cloud

Game Development

- GameLift – Deploy and Scale Session-based Multiplayer Games

Mobile Services

- Mobile Hub – Build, Test, and Monitor Mobile Apps
- Cognito – User Identity and App Data Synchronization
- Device Farm – Test Android, FireOS, and iOS Apps on Real Devices in the Cloud
- Mobile Analytics – Collect, View and Export App Analytics
- SNS – Push Notification Service

Application Services

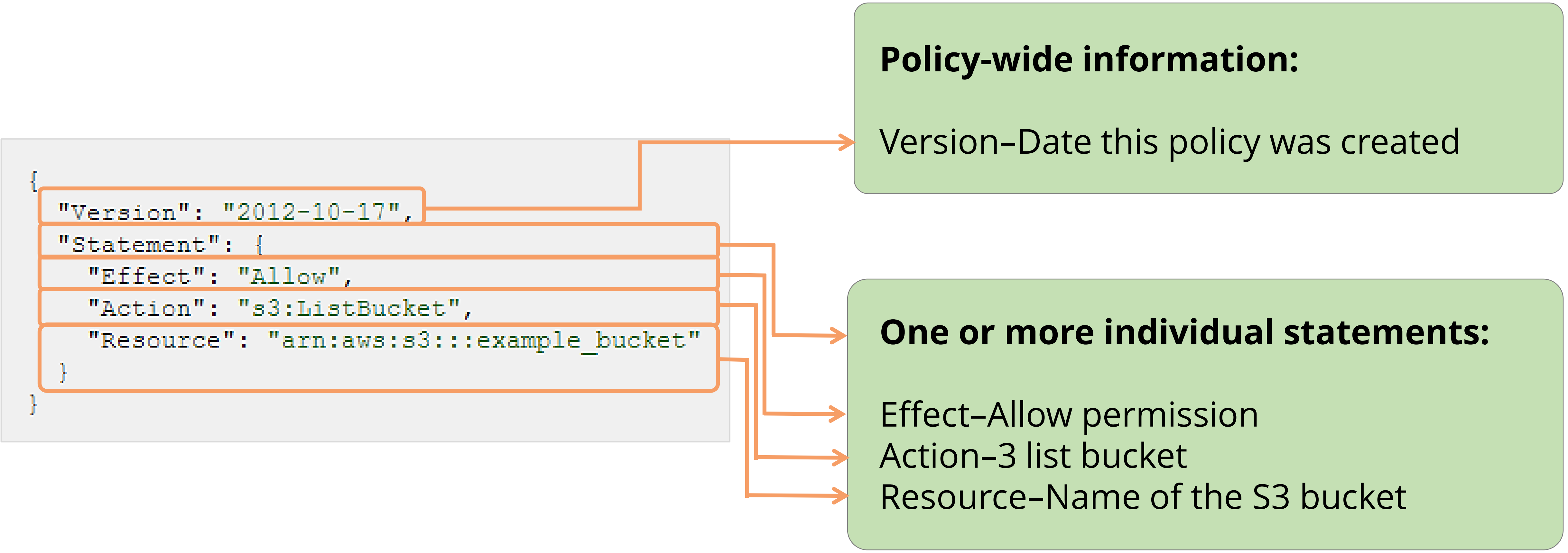
- API Gateway – Build, Deploy and Manage APIs
- AppStream – Low Latency Application Streaming
- CloudSearch – Managed Search Service
- Elastic Transcoder – Easy-to-Use Scalable Media Transcoding
- SES – Email Sending and Receiving Service
- SQS – Message Queue Service
- SWF – Workflow Service for Coordinating Application Components

Enterprise Applications

- WorkSpaces – Desktops in the Cloud
- WorkDocs – Secure Enterprise Storage and Sharing Service
- WorkMail – Secure Email and Calendaring Service

JSON

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



```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

Policy-wide information:

Version–Date this policy was created

One or more individual statements:

Effect–Allow permission
Action–3 list bucket
Resource–Name of the S3 bucket

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**.

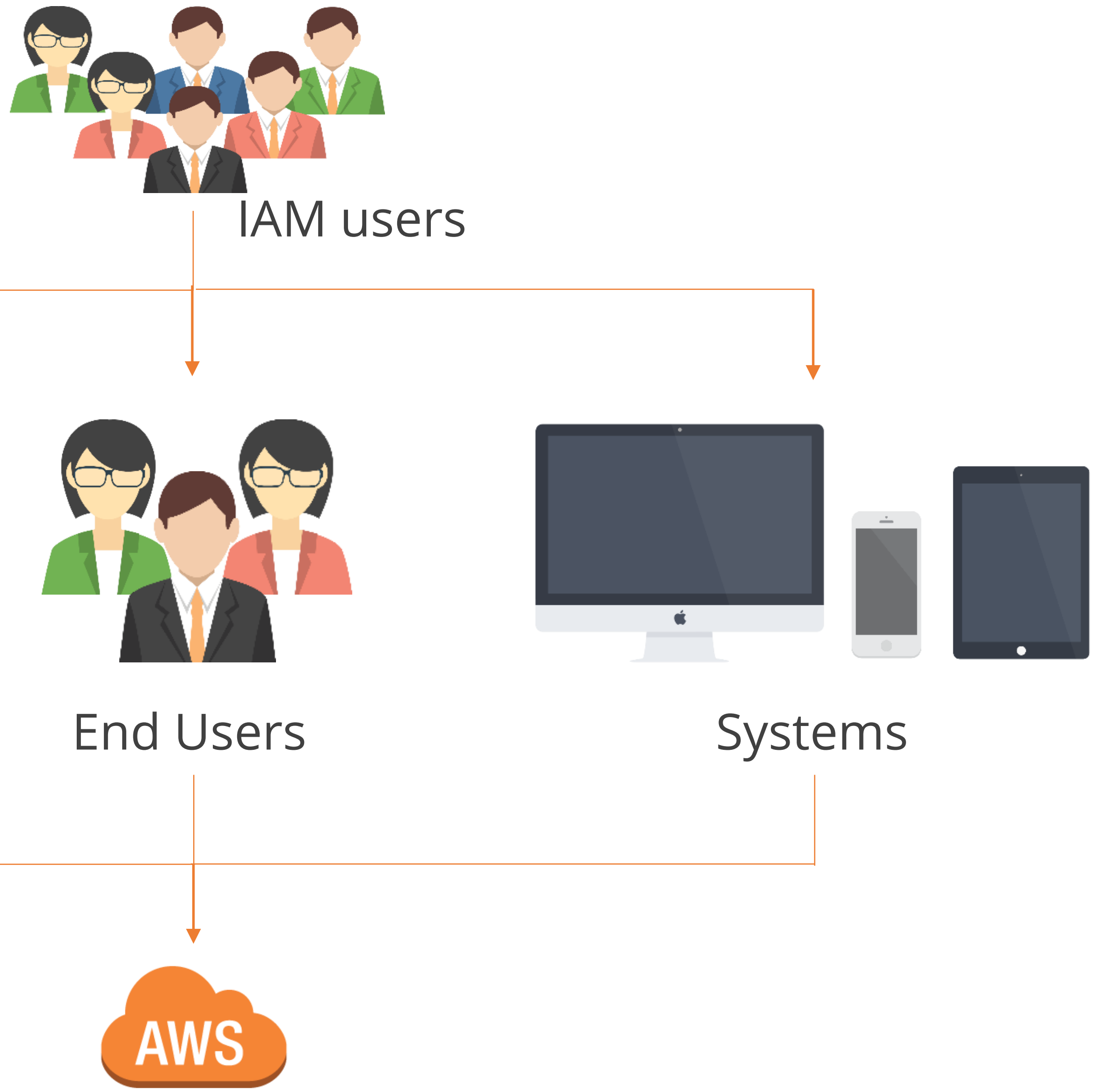
This role provides an AWS Directory Service user or group with full access to Amazon EC2 services and the associated services and resources: Amazon Elastic Compute Cloud, Elastic Load Balancing, Amazon CloudWatch, and Auto Scaling.

IAM Users

Description of IAM Users

IAM Users

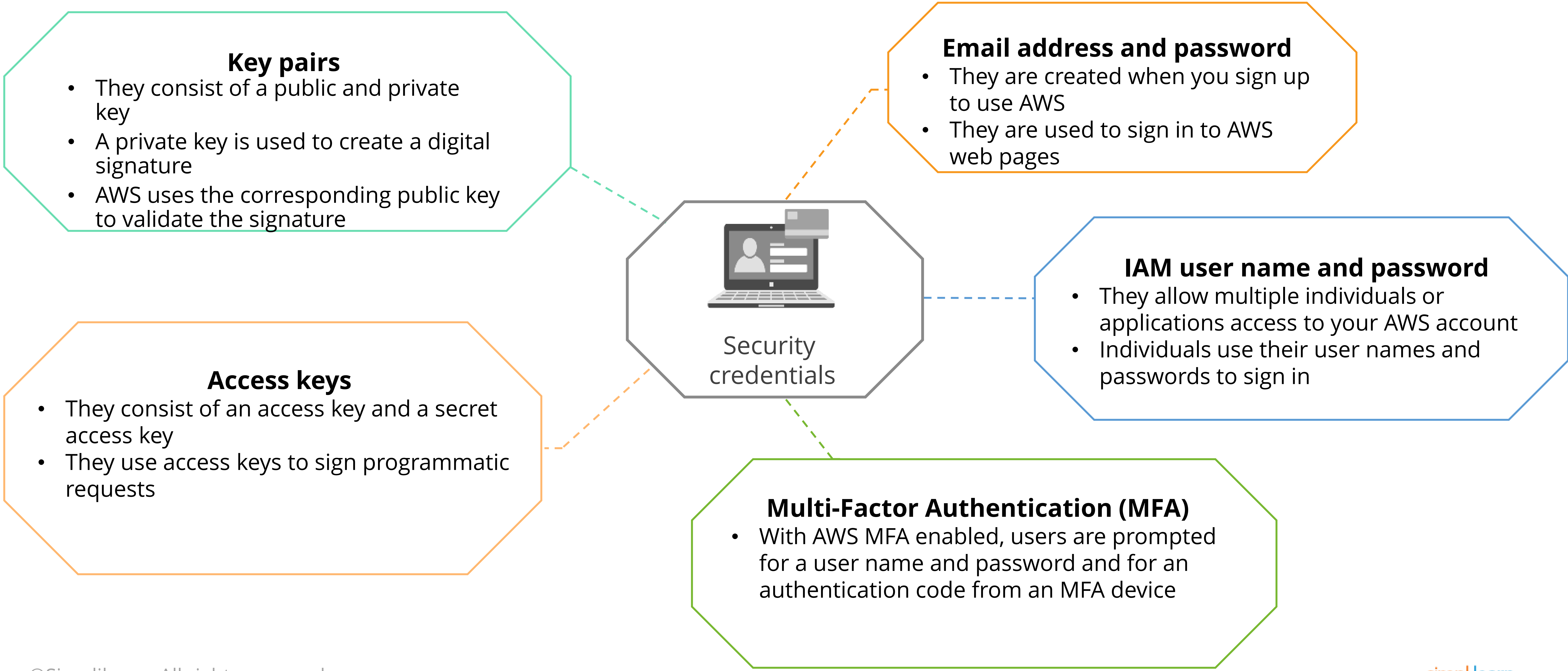
Users are defined as the people or systems that use your AWS resources.



AWS resources

Security Credentials

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



Security credentials

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

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

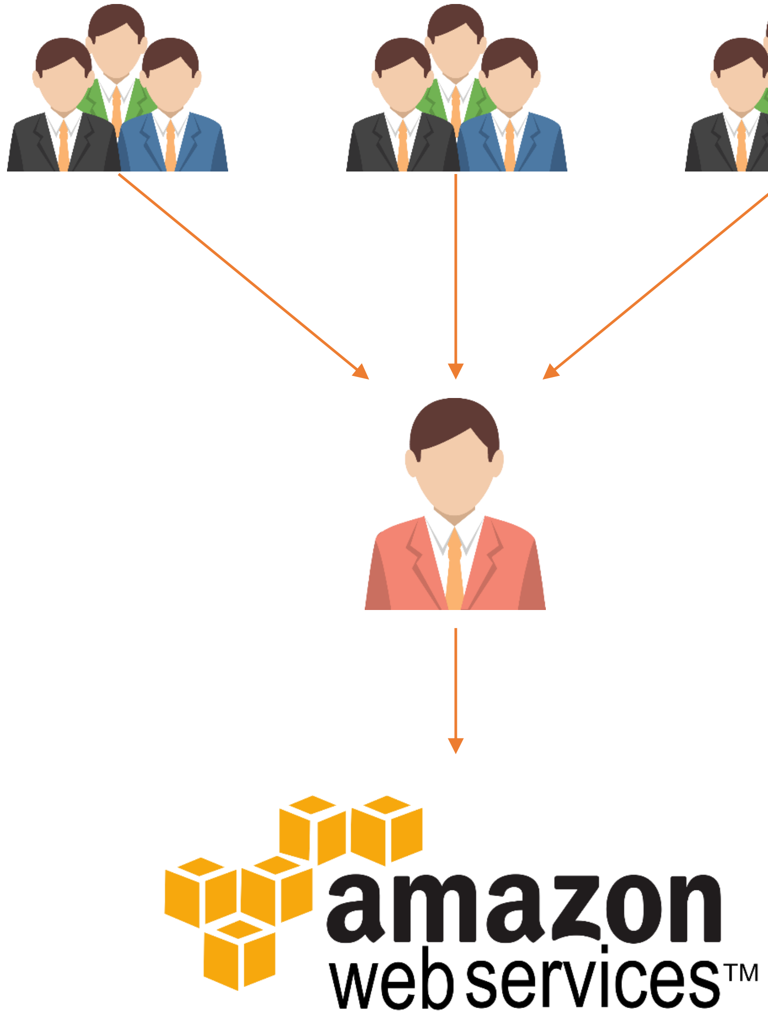
Multi-Factor Authentication (MFA)

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

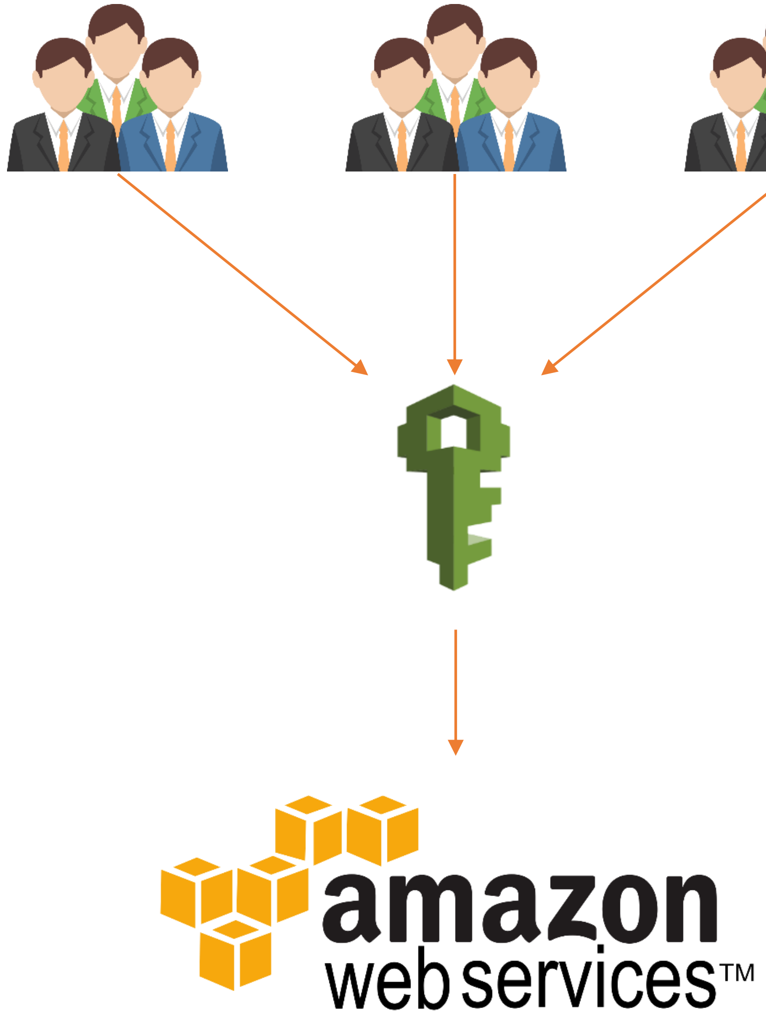
Scenario

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?

A



B



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.

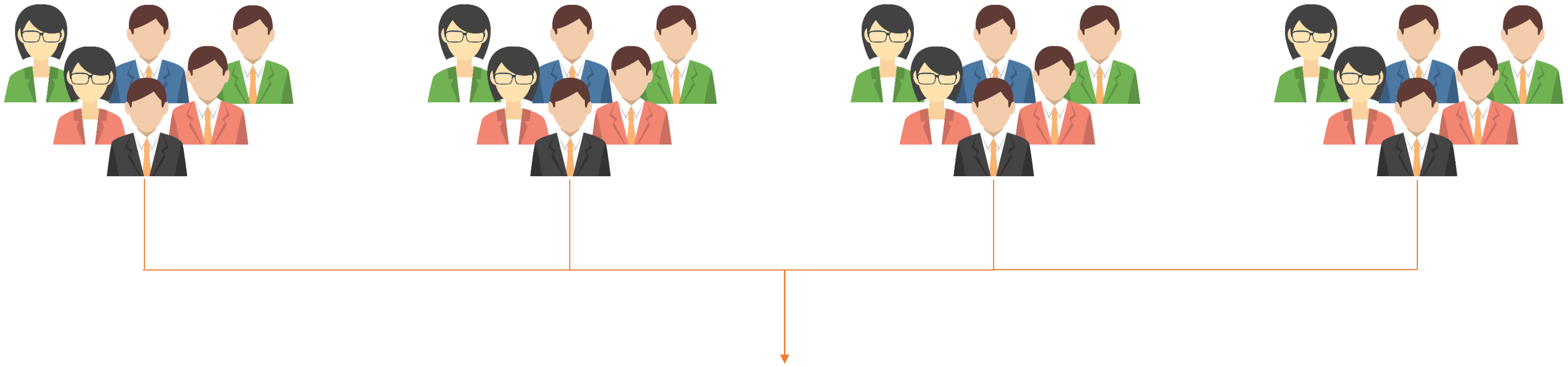
The first step is to create an account using your company email address. This account will be the root account.

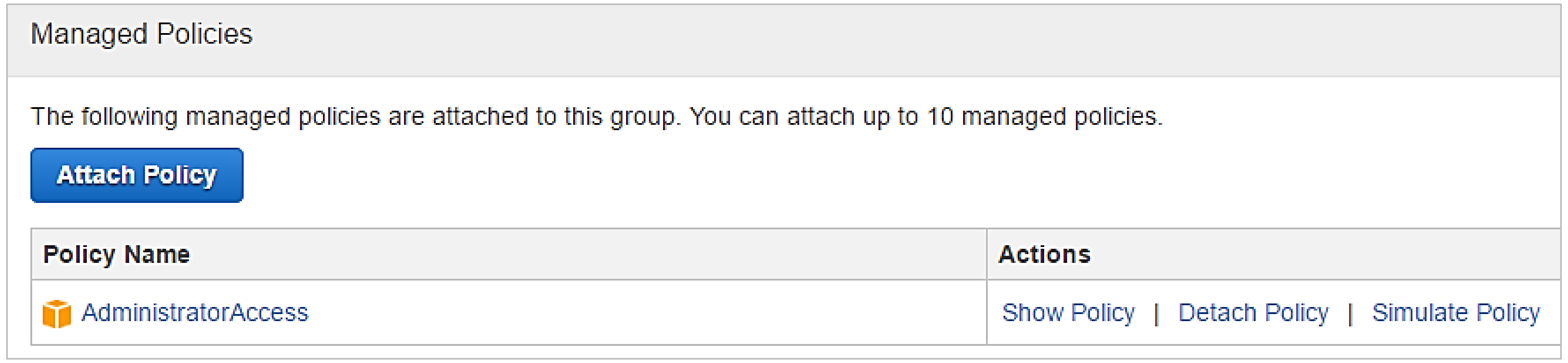
IAM Groups

Description of IAM Groups

IAM Groups

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





Managed Policies

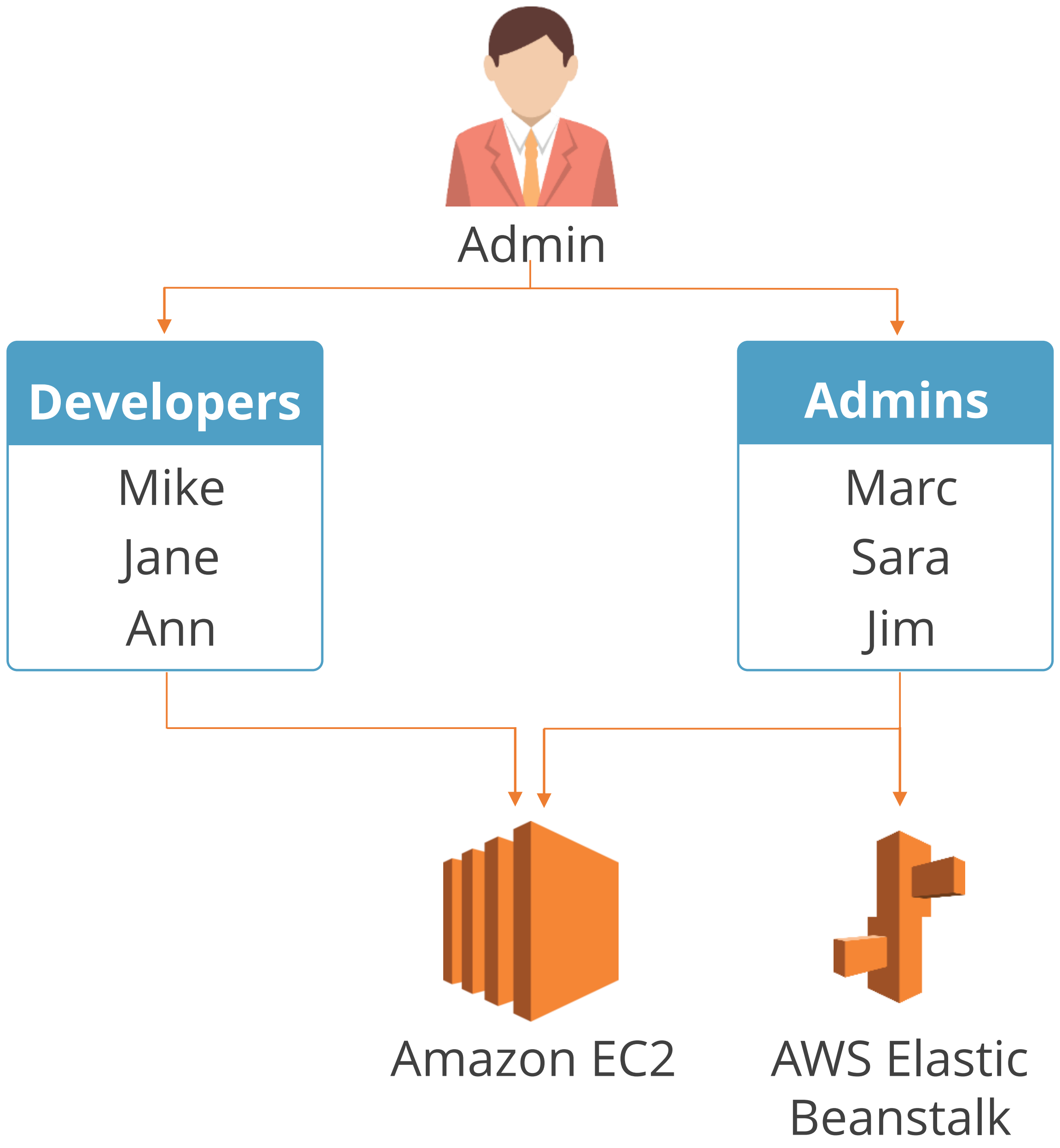
The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy

Granting Permissions to Groups

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



Admin

Developers

Mike
Jane
Ann

Admins

Marc
Sara
Jim

Amazon EC2

AWS Elastic Beanstalk

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.**

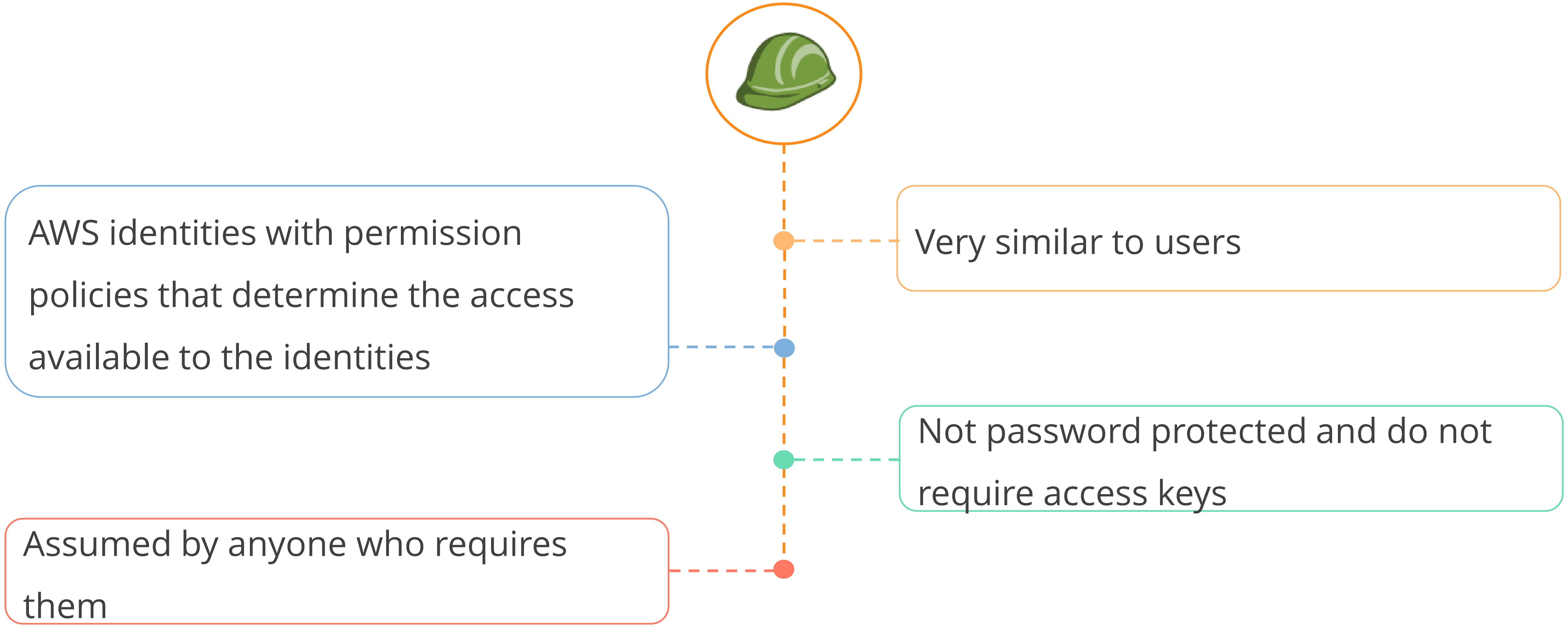
An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.

IAM Roles

Description of IAM Roles

IAM Roles

IAM Roles are:



Very similar to users

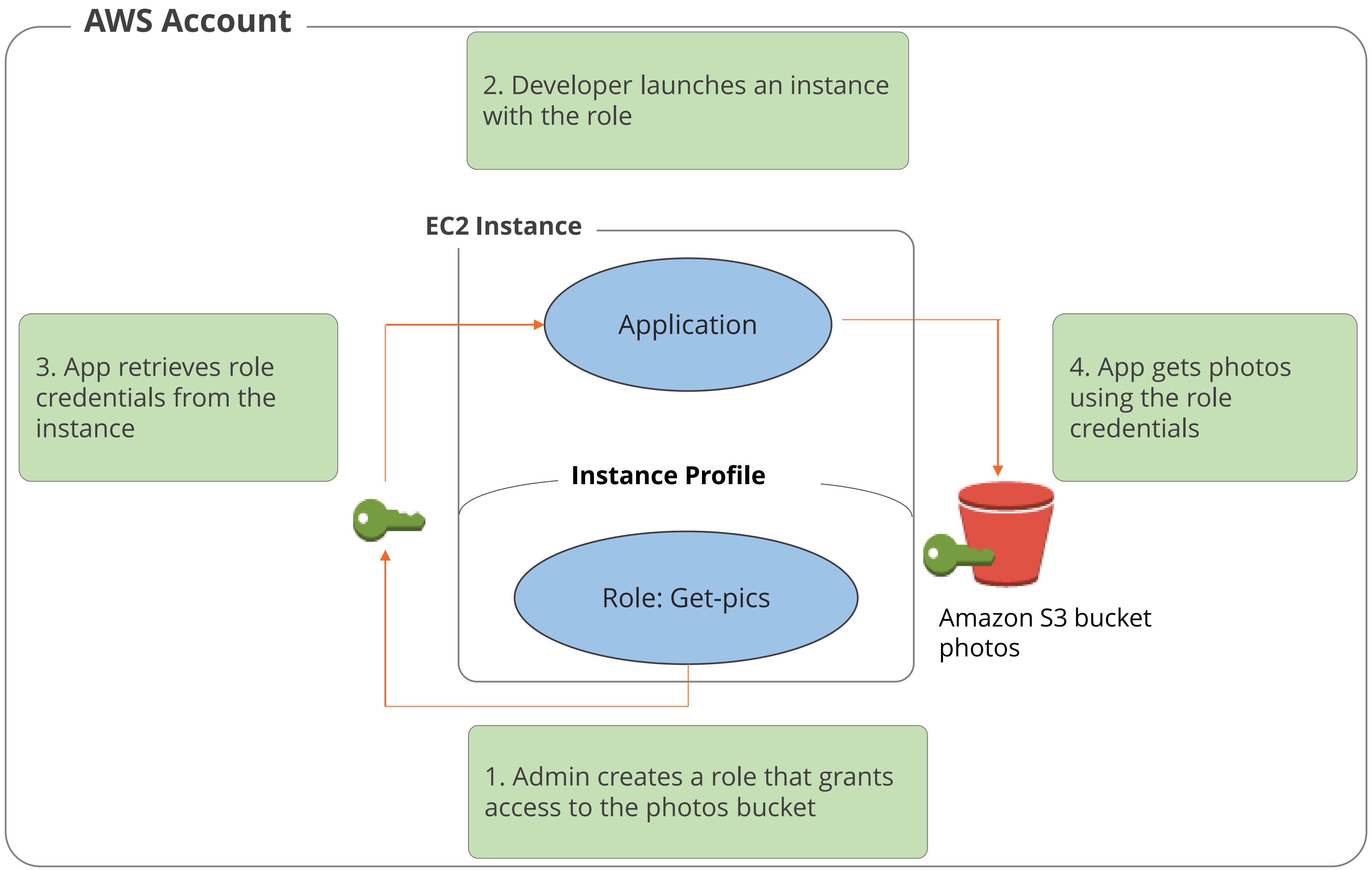
AWS identities with permission policies that determine the access available to the identities

Not password protected and do not require access keys

Assumed by anyone who requires them

Various Functions of Roles

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



AWS Account
2. Developer launches an instance with the role
EC2 Instance
Application
3. App retrieves role credentials from the instance
4. App gets photos using the role credentials
Instance Profile
Role: Get-pics
Amazon S3 bucket photos
1. Admin creates a role that grants access to the photos bucket

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.

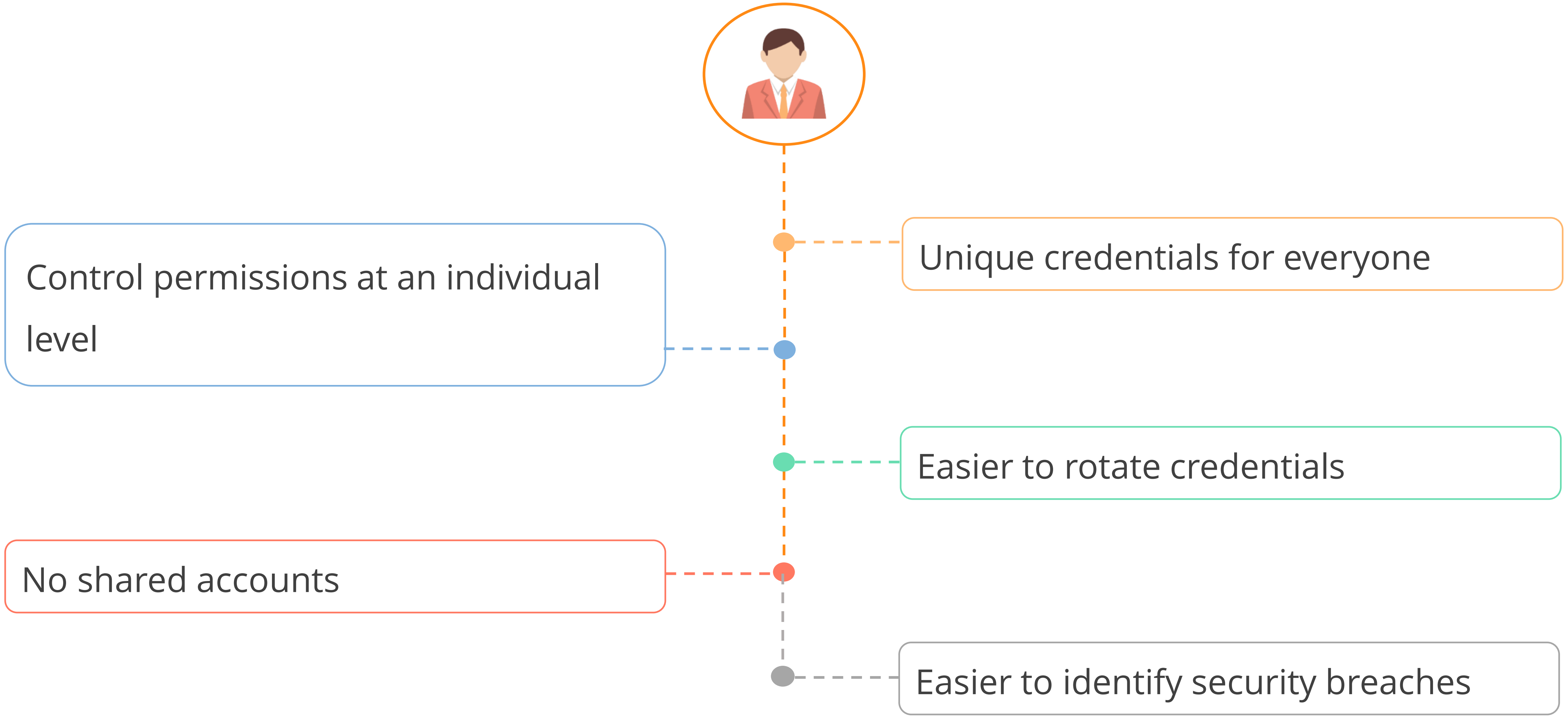
A policy document written in JSON is used to assign permissions.

IAM Best Practices

Overview of the IAM Best Practices

Create Individual IAM Users

The benefits of creating individual IAM users:



Unique credentials for everyone

Control permissions at an individual level

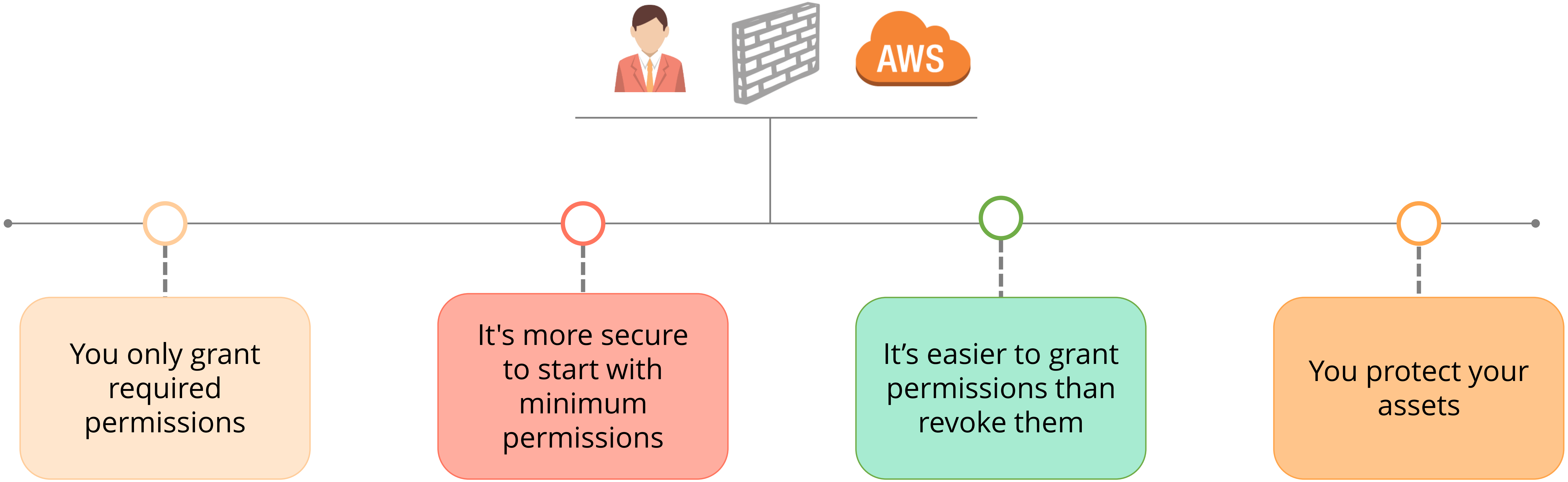
Easier to rotate credentials

No shared accounts

Easier to identify security breaches

Grant Least Privilege

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



You only grant required permissions

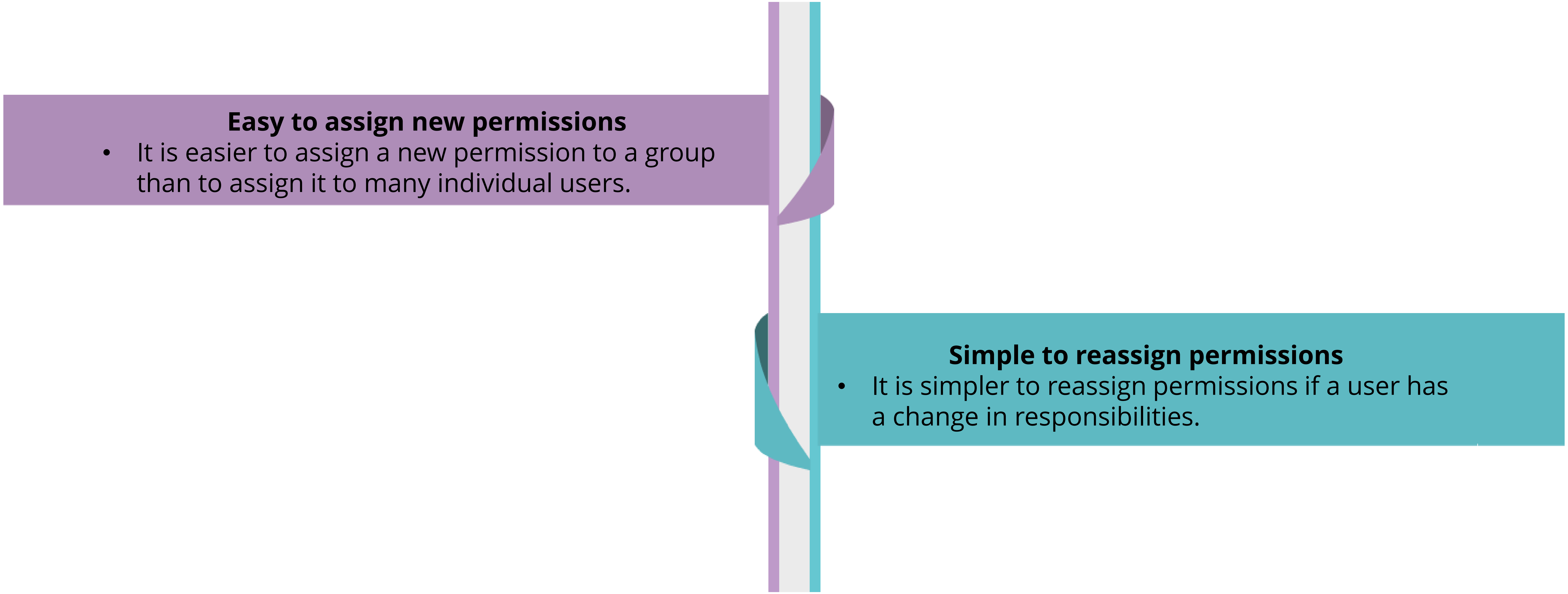
It's more secure to start with minimum permissions

It’s easier to grant permissions than revoke them

You protect your assets

Manage Permissions with Groups

Use permissions with groups to minimize the workload



Easy to assign new permissions

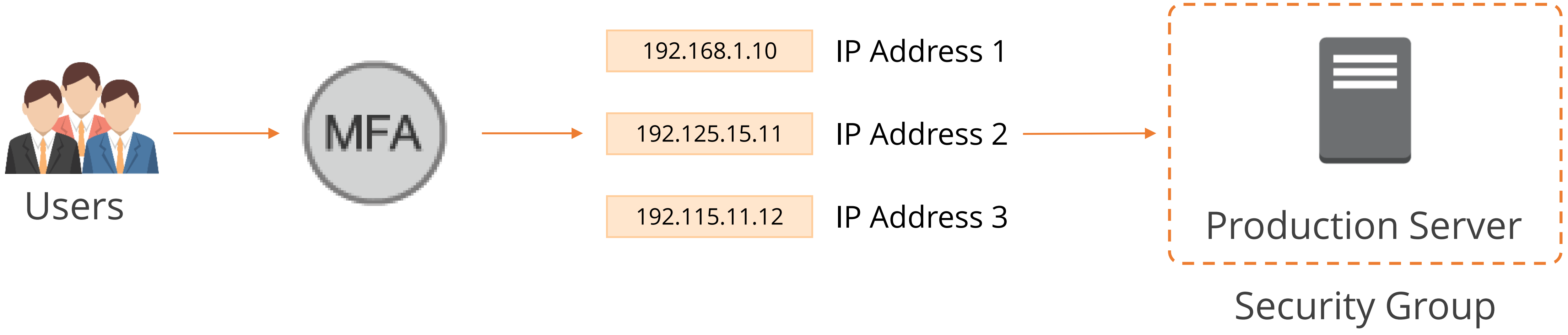
- It is easier to assign a new permission to a group than to assign it to many individual users.

Simple to reassign permissions

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

Restrict Access with Further Conditions

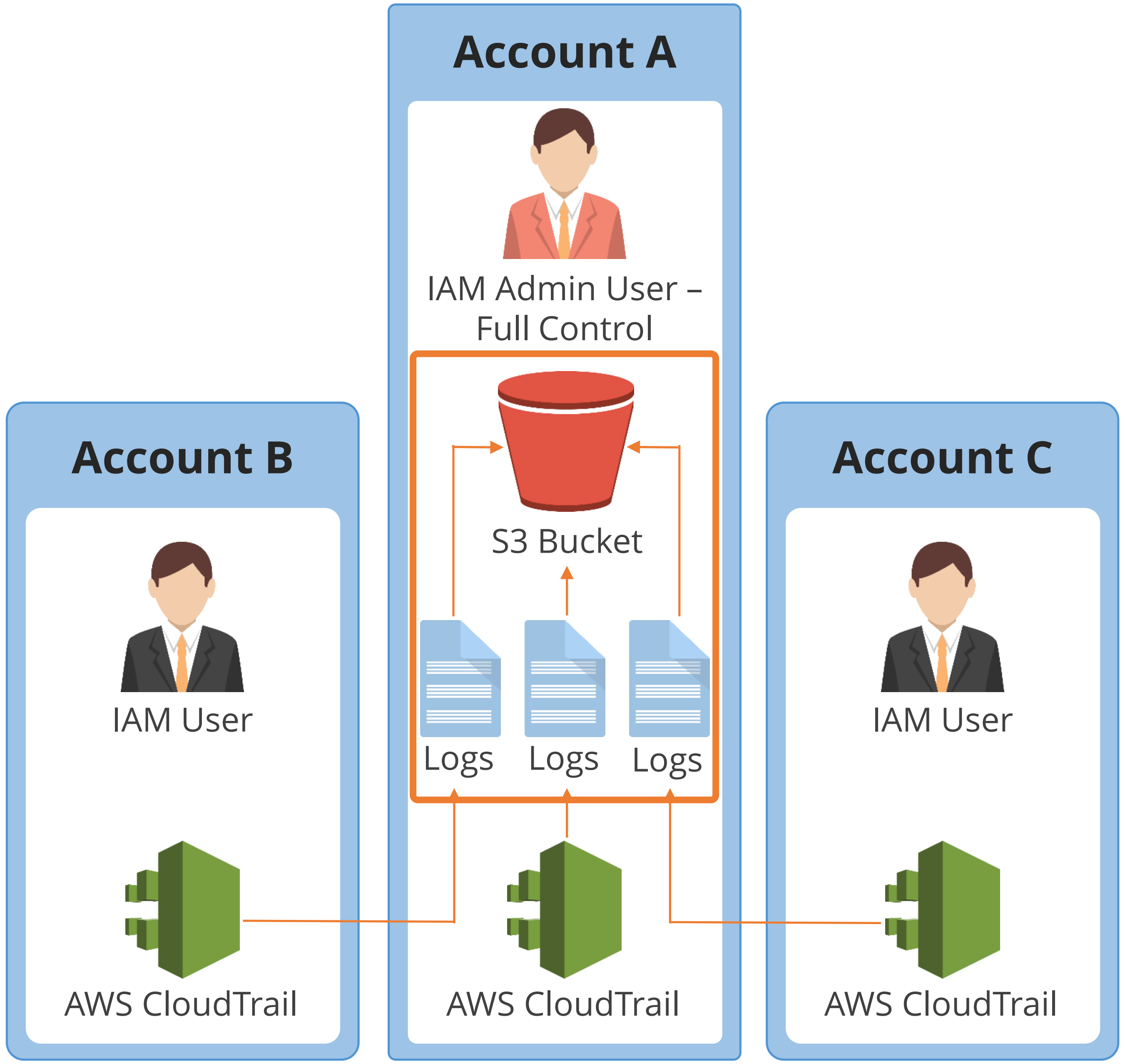
Use additional conditions such as MFA and Security Groups to ensure only the intended users get access.



Monitor Activity in your AWS Account (contd.)

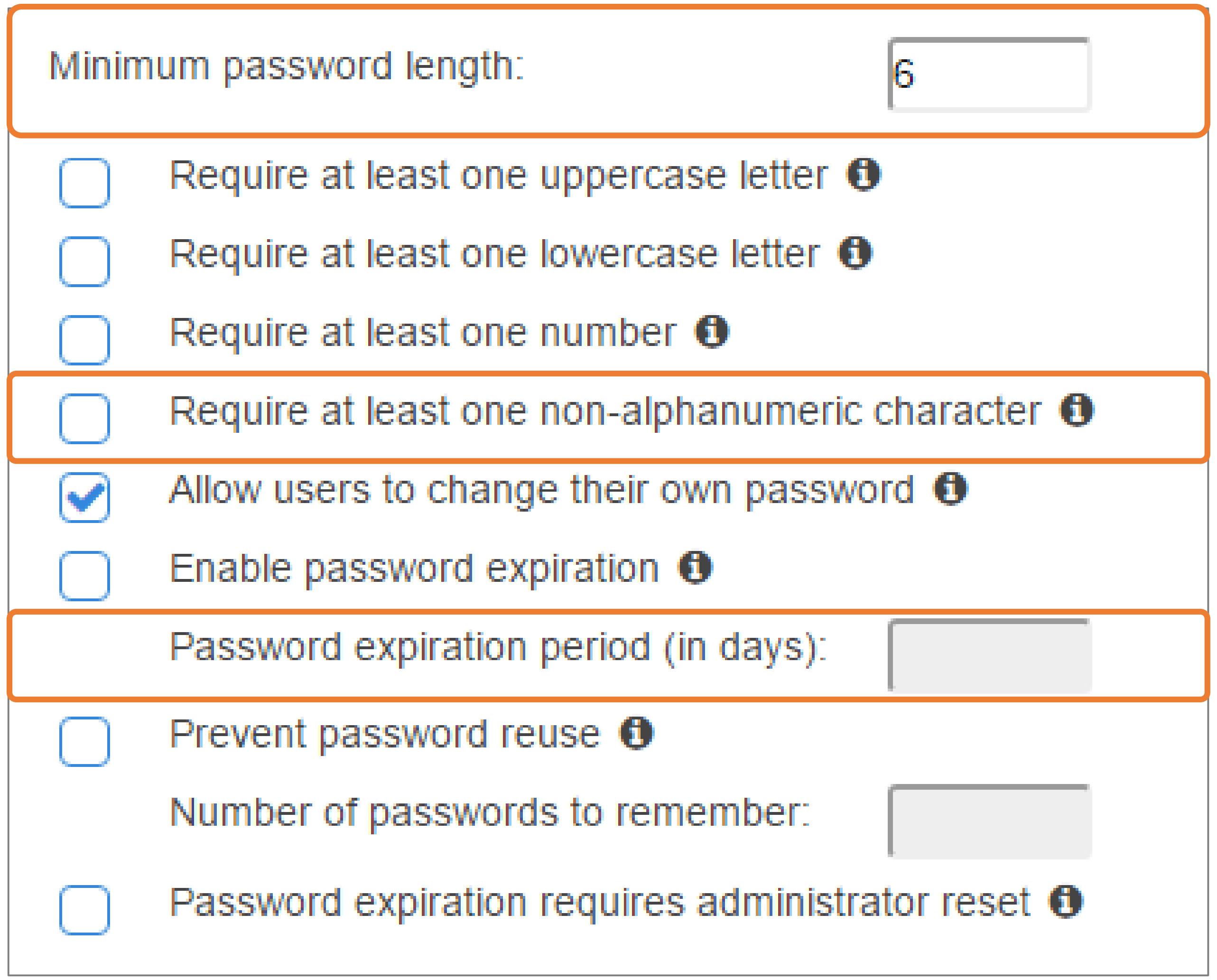
AWS has several features to log user actions.

- Logs
- AWS Cloudtrail



Create a Strong Password Policy

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

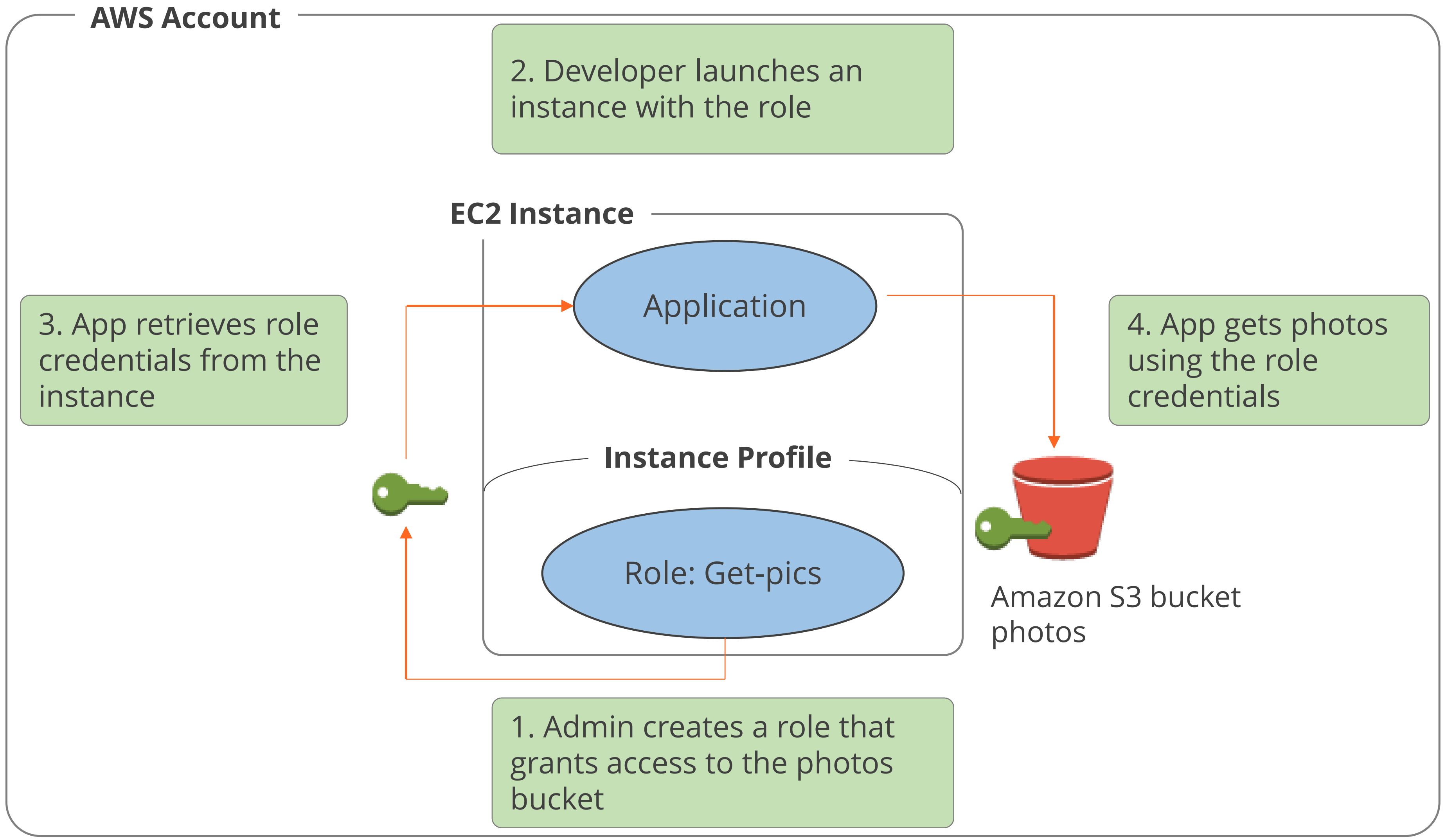


Minimum password length: 6

☐ Require at least one uppercase letter
☐ Require at least one lowercase letter
☐ Require at least one number
☐ Require at least one non-alphanumeric character
☑ Allow users to change their own password
☐ Enable password expiration
Password expiration period (in days):
☐ Prevent password reuse
Number of passwords to remember:
☐ Password expiration requires administrator reset

Use Roles for Applications that run on EC2

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


AWS Account
2. Developer launches an instance with the role
EC2 Instance
Application
3. App retrieves role credentials from the instance
4. App gets photos using the role credentials
Instance Profile
Role: Get-pics
Amazon S3 bucket photos
1. Admin creates a role that grants access to the photos bucket

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.

AWS Security Token Service (STS)

It is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management users that you authenticate.

AWS STS

AWS Security Token Service (STS) (Contd.)

01
02
AWS STS
04
03

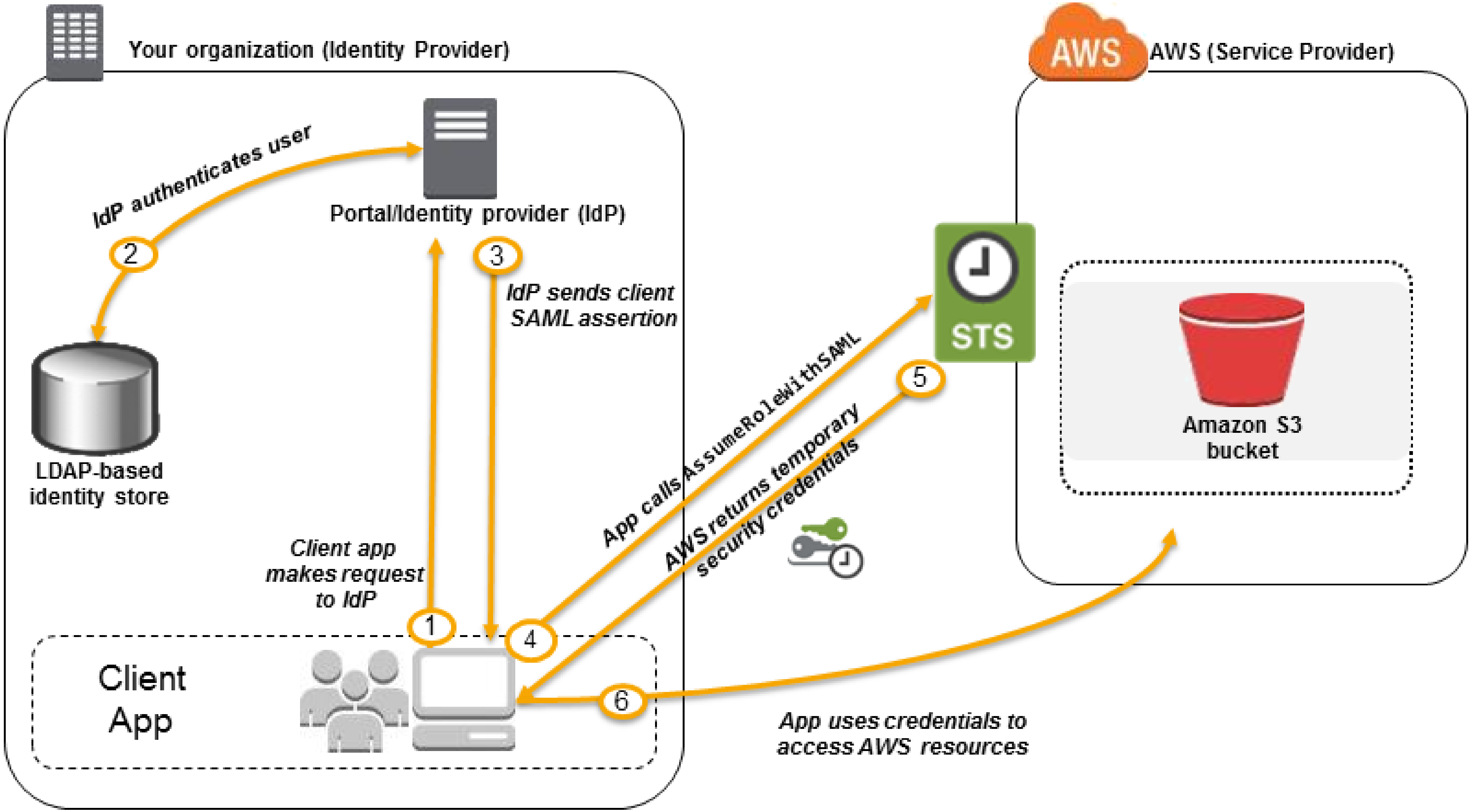
Federation
Allows you to combine users across domains

Identity Broker
Allows you to federate identities from point A to point B

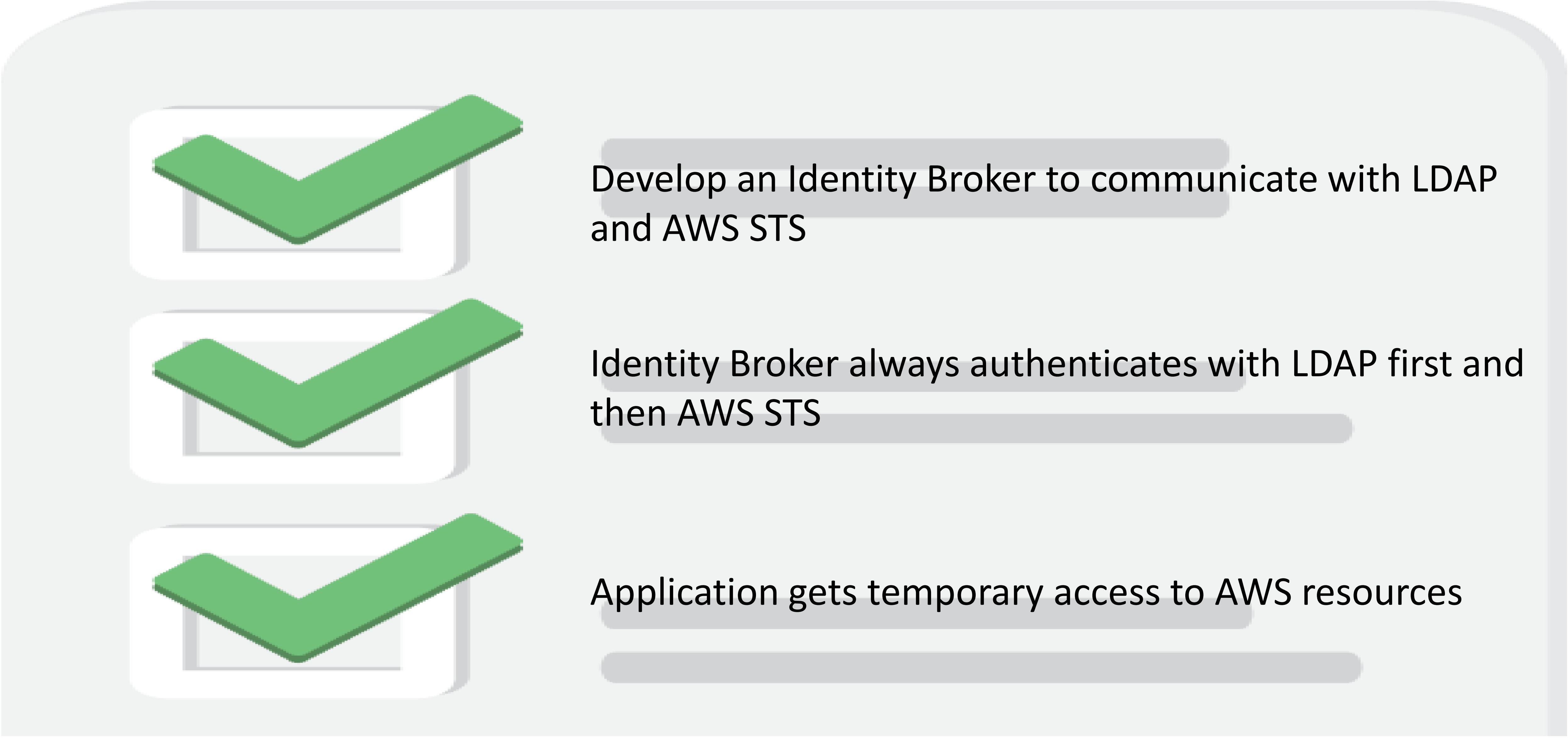
Identities
User of a service such as a user of LinkedIn or Amazon

Identity Store
Is a service like LinkedIn, Google, or Active Directory

AWS Security Token Service (STS) (Contd.)


Your organization (Identity Provider)
AWS
AWS (Service Provider)
IdP authenticates user
2
Portal/Identity provider (IdP)
3
IdP sends client SAML assertion
LDAP-based identity store
STS
Amazon S3 bucket
5
App calls AssumeRoleWithSAML
AWS returns temporary security credentials
Client app makes request to IdP
1
4
6
Client App
App uses credentials to access AWS resources

STS: Things To Remember



- Develop an Identity Broker to communicate with LDAP and AWS STS
- Identity Broker always authenticates with LDAP first and then AWS STS
- Application gets temporary access to AWS resources

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.

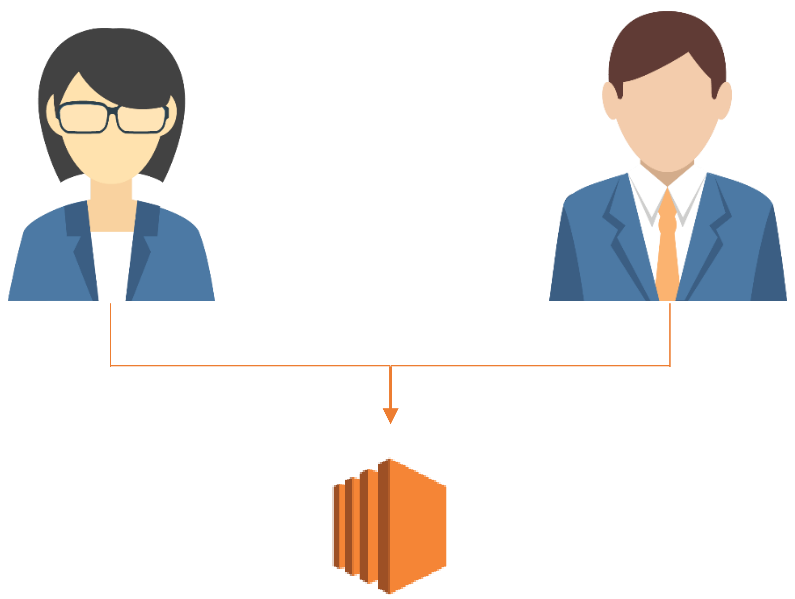
Practice Assignment: Configuring IAM Access

Use IAM to configure user access to AWS

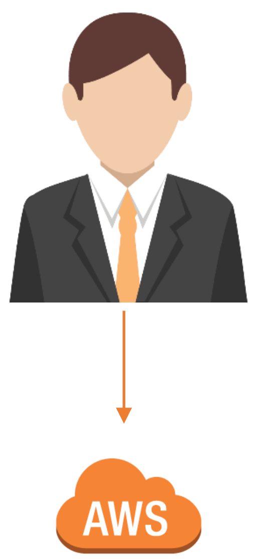
Configuring IAM Access

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

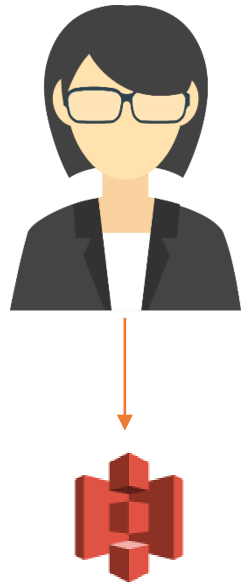
Two users require full access to EC2.



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.

?
Quiz

QUIZ

1

What are IAM entities?

a. User, Teams, Roles

b. User, Group, Companies

c. Sessions, Group, Organizations

d. User, Group, Roles

QUIZ

1

What are IAM entities?

a. User, Teams, Roles

b. User, Group, Companies

c. Sessions, Group, Organizations

d. User, Group, Roles

The correct answer is **d**

Explanations: User, Groups, and Roles are the entities used in IAM.

QUIZ

2

Which AWS compliance allows you to safely and securely manage and store credit card data?

a. HIPAA

b. PCI DSS

c. JSON

d. EC2

QUIZ

2

Which AWS compliance allows you to safely and securely manage and store credit card data?

a. HIPAA

b. PCI DSS

c. JSON

d. EC2

The correct answer is **b**

Explanations: IAM is Payment Card Industry (PCI) Data Security Standard (DSS) compliant so you can process, store, and transmit credit card data from a merchant or service provider.

QUIZ 3	What language is used to authenticate IAM with Federated Access?

a. JSON

b. ODBC

c. SSL

d. SAML 2.0

QUIZ 3	What language is used to authenticate IAM with Federated Access?

a. JSON

b. ODBC

c. SSL

d. SAML 2.0

The correct answer is **d**

Explanations: This feature enables federated single sign-on (SSO), so users can log in to the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization.

QUIZ

4

What does a user need to login to the AWS console?

a. Username, Access Key ID, and Secret Access Key ID

b. MFA token

c. Username and password

d. Username and policy document

QUIZ

4

What does a user need to login to the AWS console?

a. Username, Access Key ID, and Secret Access Key ID

b. MFA token

c. Username and password

d. Username and policy document

The correct answer is **c**

Explanations: The Access Key ID and Secret Access Key ID are generated when you create a user, but to log in to the AWS console you need to generate a password for the user.

QUIZ

5

What is a good way to restrict AWS user access using further conditions?

a. Inform users they can only login at certain times

b. Make users commit their Access Key ID to memory

c. Use Multi-Factor Authentication

d. Only use policies for administration users

QUIZ

5

What is a good way to restrict AWS user access using further conditions?

a. Inform users they can only login at certain times

b. Make users commit their Access Key ID to memory

c. Use Multi-Factor Authentication

d. Only use policies for administration users

The correct answer is **c**

Explanations: MFA request users to pass an additional authentication check to be able to login. Other examples of further conditions are specifying that access to certain resources can only come from a particular IP address.

This concludes “Identity and Access Management.”

The next lesson is “Virtual Private Cloud.”