TECHNOLOGY

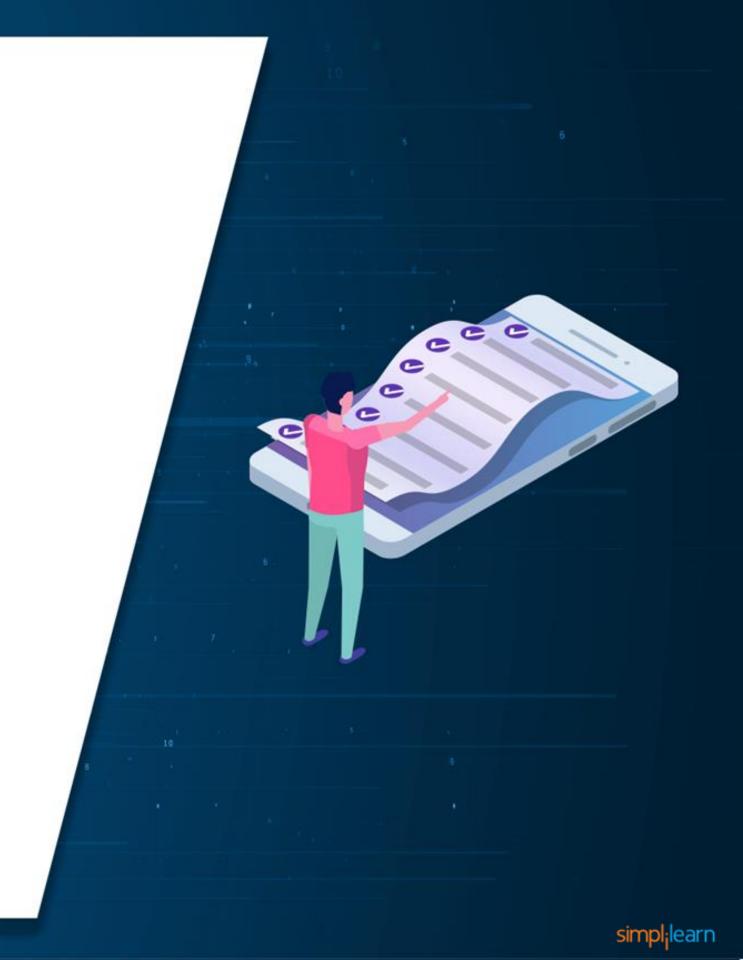**AWS Solutions Architect : Associate Level**

simplilearn

IAM and Security on AWS

Learning Objectives

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

- Define Identity and Access Management in AWS

- Create custom IAM Roles

- Create IAM users and assign roles

- Create IAM groups with multiple IAM users

- Assign roles to AWS Services

- Use AWS Directory Service

- Demonstrate MFA and SSO

Introduction to Identity and Access Management

What Is Identity and Access Management in AWS?

AWS Identity and Access Management or IAM is the service that enables you to securely control user access to all the AWS services and resources.

AWS IAM

Why Identity and Access Management

AWS IAM helps to:

01 Prevent security breaches and unauthorized logins

02 Track user information such as login credentials and more

03 Track the usage of all of the AWS resources and services

04 Provide granular level permissions to all of the AWS services

simplilearn

Terminologies in AWS IAM

Terminologies in AWS IAM

Users

An IAM user is an identity with login credentials and permissions attached to it.

Policies

An IAM policy is a set of permissions that control access to AWS resources and services. Policies are stored in JSON format.

Groups

An IAM group is a collection of multiple IAM users. They are used to grant permissions to multiple users simultaneously.
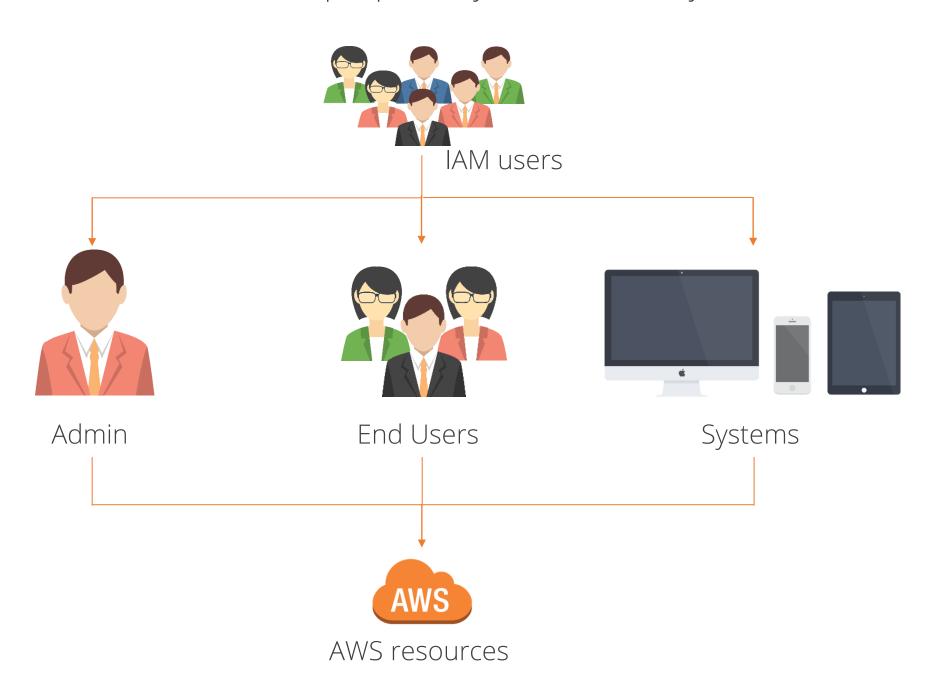
Roles

An IAM role is a set of permissions that define the actions that are allowed or denied for an AWS entity.

IAM Users

IAM Users

The IAM users are defined as the people or systems that use your AWS resources.

IAM users

Admin   End Users   Systems

AWS resources

Security Credentials

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

Email address and password:
They are used to sign-in to the AWS Console.

IAM username and password:
They can be used by multiple individuals and applications to access your AWS account.

Access keys :
Access keys can be used to grant access to programmatic requests.

Duration: 10 min.

Problem Statement:

Create an IAM user using the Amazon console

Assisted Practice: Guidelines to Create an IAM User

Steps to perform:
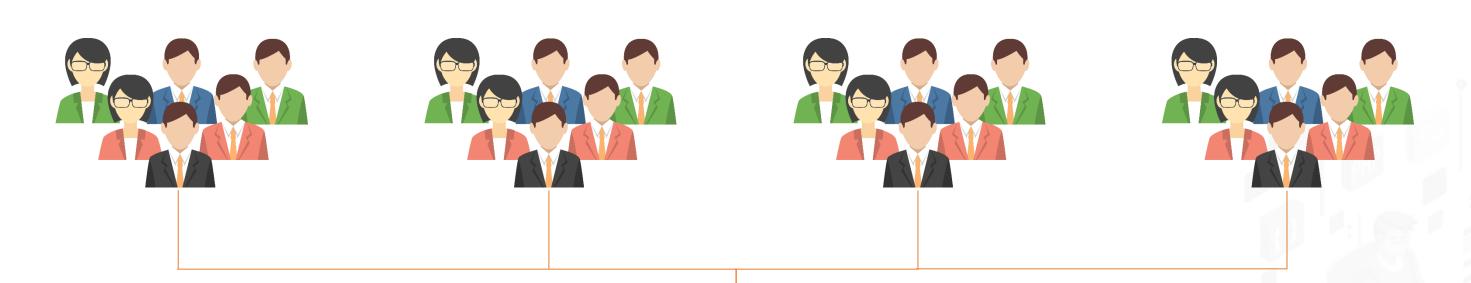
1. Go to your Amazon Console
2. Open the IAM user dashboard
3. Click on the Add user button
4. Fill in the details about the user
5. Skip to the review page and click on the Create user button

IAM Groups

IAM Groups

An IAM group is 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.
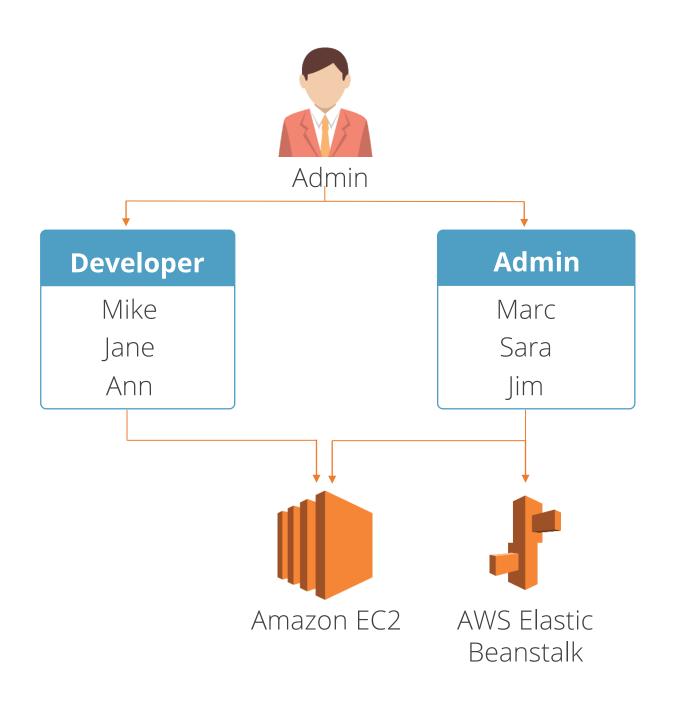
Attach Policy

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

Granting Permissions to IAM Groups

The following diagram shows how the permissions are granted to different IAM groups:

Admin

Developer	Admin
Mike	Marc
Jane	Sara
Ann	Jim

Amazon EC2

AWS Elastic Beanstalk

Creating and Adding IAM Users to an IAM Group

Duration: 10 min.

Problem Statement:

Create multiple IAM users and add them to an IAM group

Assisted Practice: Guidelines to Create and Add IAM Users to an IAM Group

Steps to perform:

1. Create multiple IAM users
2. Go to the IAM group dashboard
3. Click on Create IAM Group
4. Provide a name for the group
5. Go to the newly created group and click on Add users
6. Select the users you want to add to the group

IAM Roles

IAM Roles

IAM Roles are permissions and policies that determine the access available to the AWS identities.

More about IAM Roles:

01   IAM Roles function in a way similar to that of IAM users.
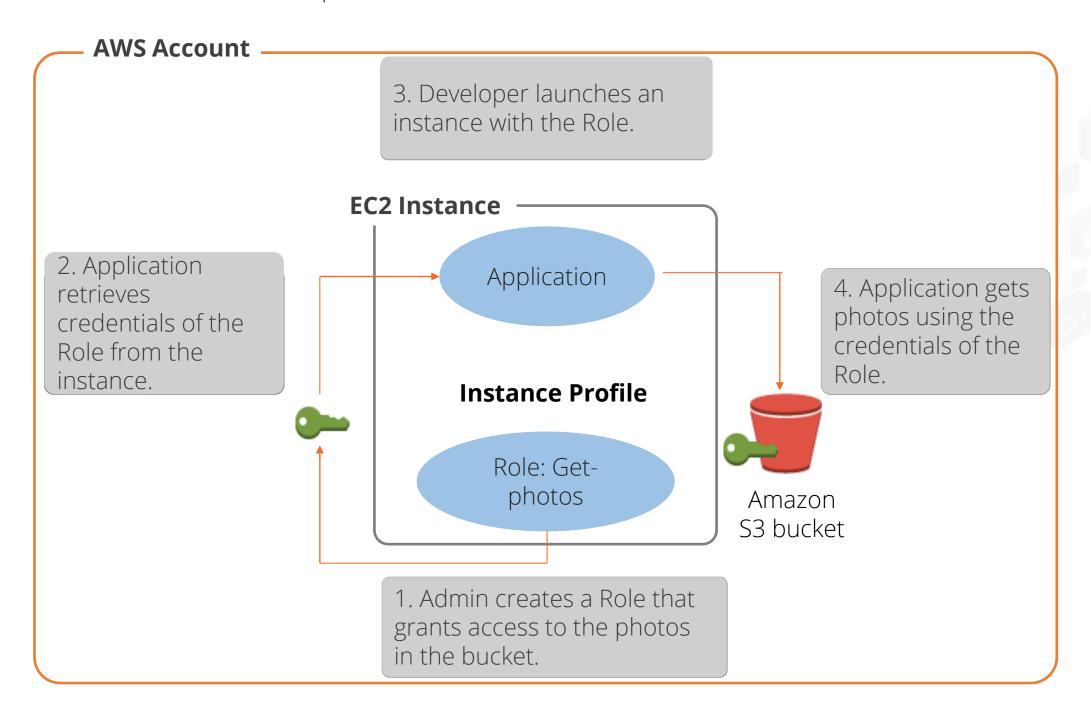
02   They are not password protected and do not require access keys.

03   These roles can be used by anyone who requires them.

IAM Roles

Various Functions of IAM Roles

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

AWS Account

EC2 Instance

3. Developer launches an instance with the Role.

2. Application retrieves credentials of the Role from the instance.

Application

Instance Profile

Role: Get-photos

4. Application gets photos using the credentials of the Role.

Amazon S3 bucket

1. Admin creates a Role that grants access to the photos in the bucket.

Duration: 10 min.

Problem Statement:

Create an IAM role using the Amazon console for an IAM user

ASSISTED PRACTICE

Assisted Practice: Guidelines to Create an IAM Role for an IAM User

Steps to perform:

1. Go to the IAM role dashboard
2. Click on the Create IAM role button
3. Select Another AWS Account tab
4. Provide a name for the role
5. Select a permission from the list of pre-defined permissions
6. Click on the Create role button

IAM Policies
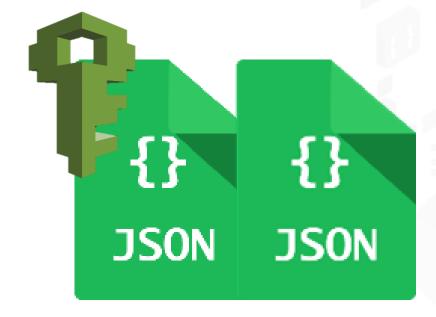
What Is IAM Policy?

An IAM policy is a document that defines one or more permissions. IAM policies can be attached to users, groups, roles, and AWS resources. They are written in JSON format.

More about IAM Policies:
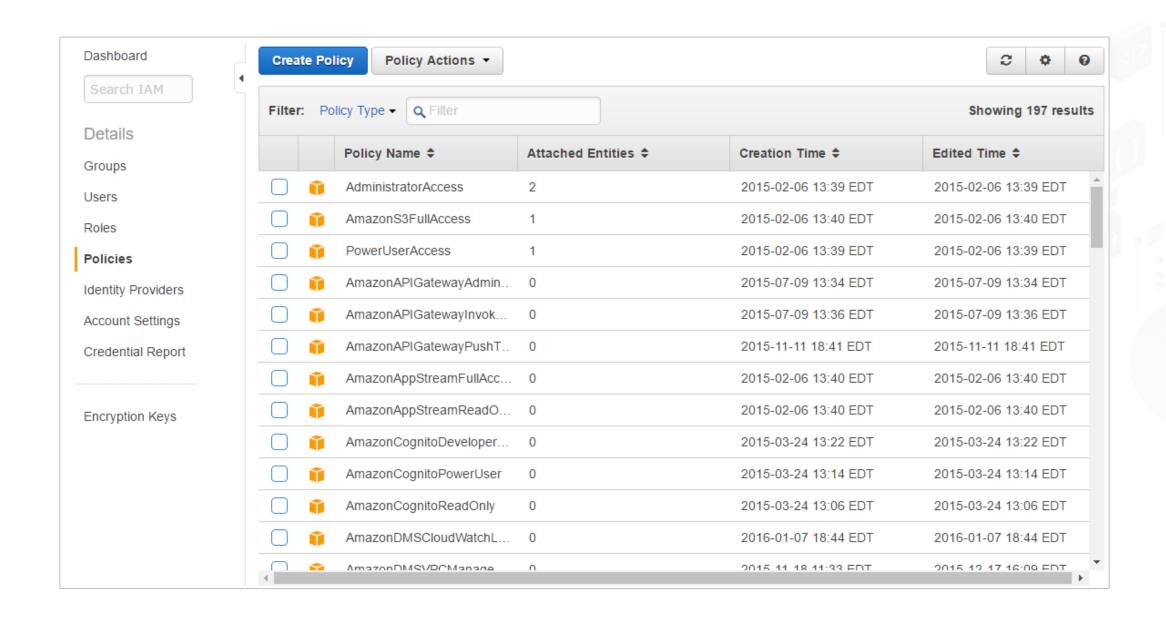
01 — IAM Policies can be preselected from the AWS list of predefined policies.

02 — Root users can edit the predefined policies to make customizations.

03 — Root users can create and define a custom IAM policy from scratch.

AWS IAM Policies

What Is IAM Policy?

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.

|		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

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

Create Policy Policy Actions ▾

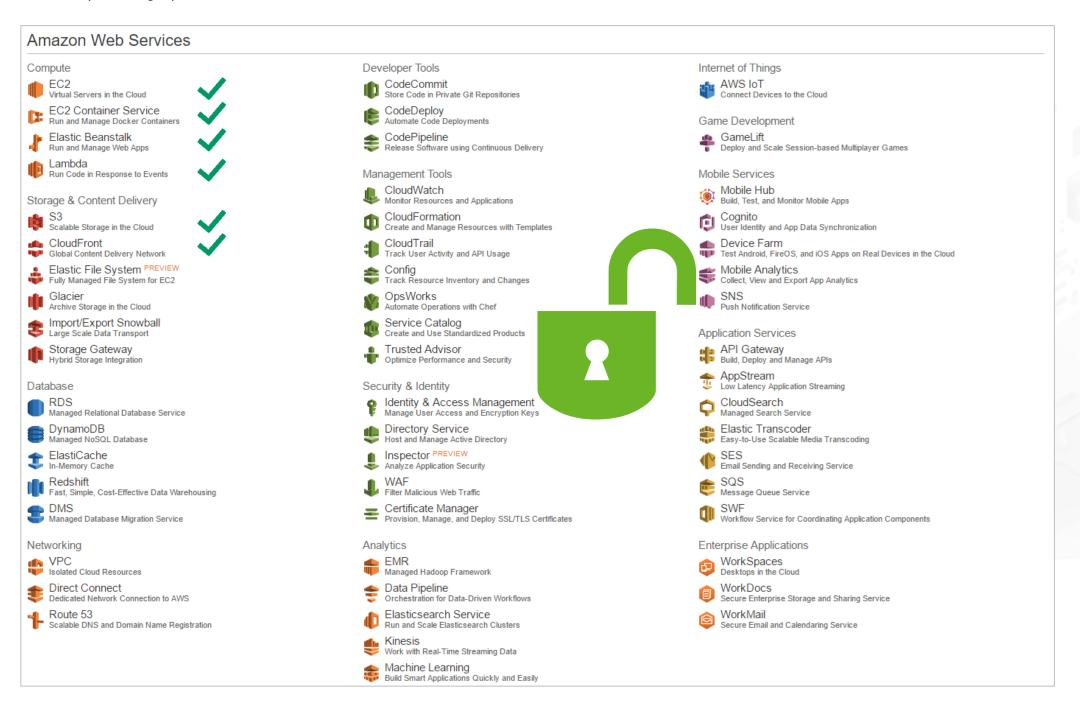Filter: Policy Type ▾ 🔍 Filter

Showing 197 results

AdministratorAccess Policy

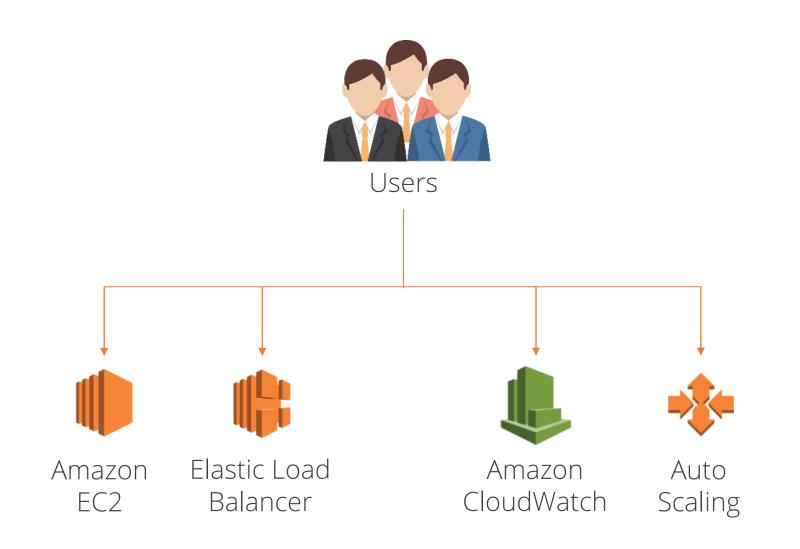AdministratorAccess policy provides full access to AWS services and resources.

AmazonEC2FullAccess Policy

AmazonEC2FullAccess policy provides users or groups full access to the Amazon EC2 services and resources.

Users

Amazon
EC2

Elastic Load
Balancer

Amazon
CloudWatch

Auto
Scaling

AmazonS3ReadOnlyAccess Policy

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

Users

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 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

Types of IAM Policies

Types of IAM Policies

There are two types of IAM policies:

Identity-based policies

- Identity-based policies can be attached directly to identities such as users, groups, and roles.

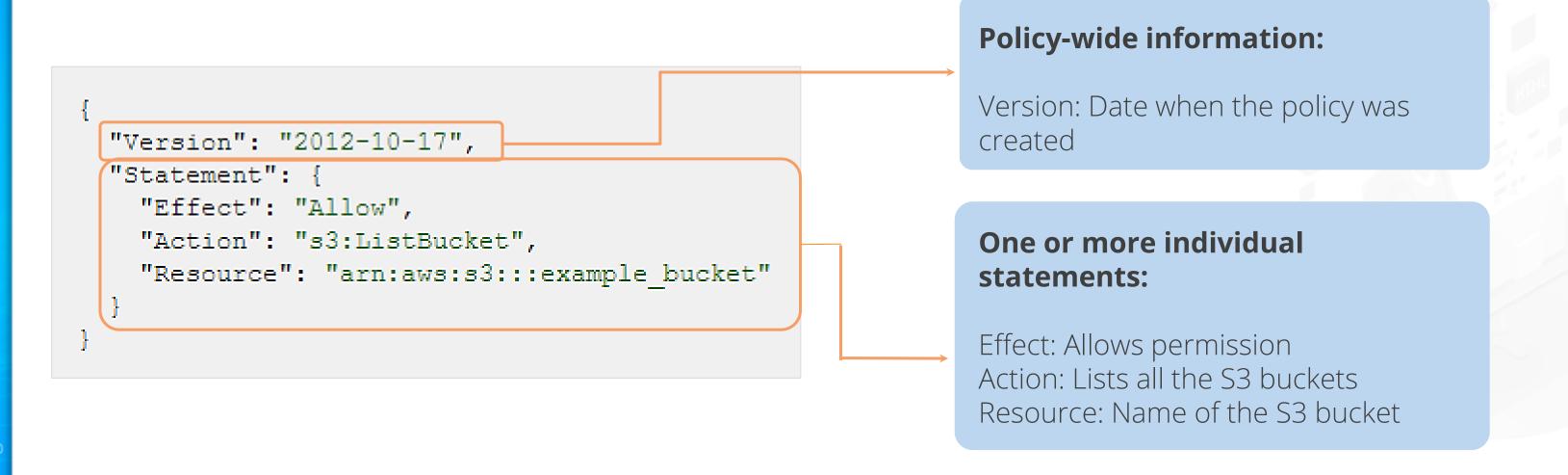- These policies define the permissions such as allow or deny for the identities.

Resource-based policies

- Resource-based policies are attached to AWS resources such as Amazon S3, Amazon EC2, and more.

- These policies define the permissions such as allow or deny for the AWS resources.

Syntax of Writing AWS IAM Policies

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 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

Example of an Identity-based Policy

Allowing a user to access Amazon EC2 from us-east-1:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:*"
],
"Resource": "*",
"Condition": {
"StringEquals": {
"aws:RequestedRegion": "us-east-1"
}
}
}
]
}
```

Example of a Resource-based Policy

Allowing EC2 to access Amazon S3 from its public IP:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
                        "ec2:*"
            ],
"Resource": "*",
"Condition": {
                "IpAddress": {

"aws:SourceIp": [

"public_ipv4"

]
                                        }
                        }
}
]
}
```

Assigning IAM Roles to Amazon Services

Creating an IAM Role for Amazon EC2 Service

Duration: 15 min.

Problem Statement:

Create and assign an IAM role to Amazon EC2 Service

Assisted Practice: Guidelines to Create an IAM Role for Amazon EC2 Service

Steps to perform:

1. Go to the IAM role dashboard
2. Click on the Create IAM role button
3. Click on the AWS Service tab and select EC2 service
4. Provide a name for the role
5. Select a permission from the list of pre-defined permissions
6. Click on the Create role button

simplilearn

Features of AWS IAM

Features of AWS IAM

AWS IAM offers the following features:

| 01 | **Multi Factor Authentication (MFA)** |

| 02 | **Strong Password Policy** |

| 03 | **Payment Card Industry (PCI)** |

| 04 | **Identity Information for Assurance** |

Features of AWS IAM

AWS IAM offers the following features:

05	Shared Access to AWS accounts
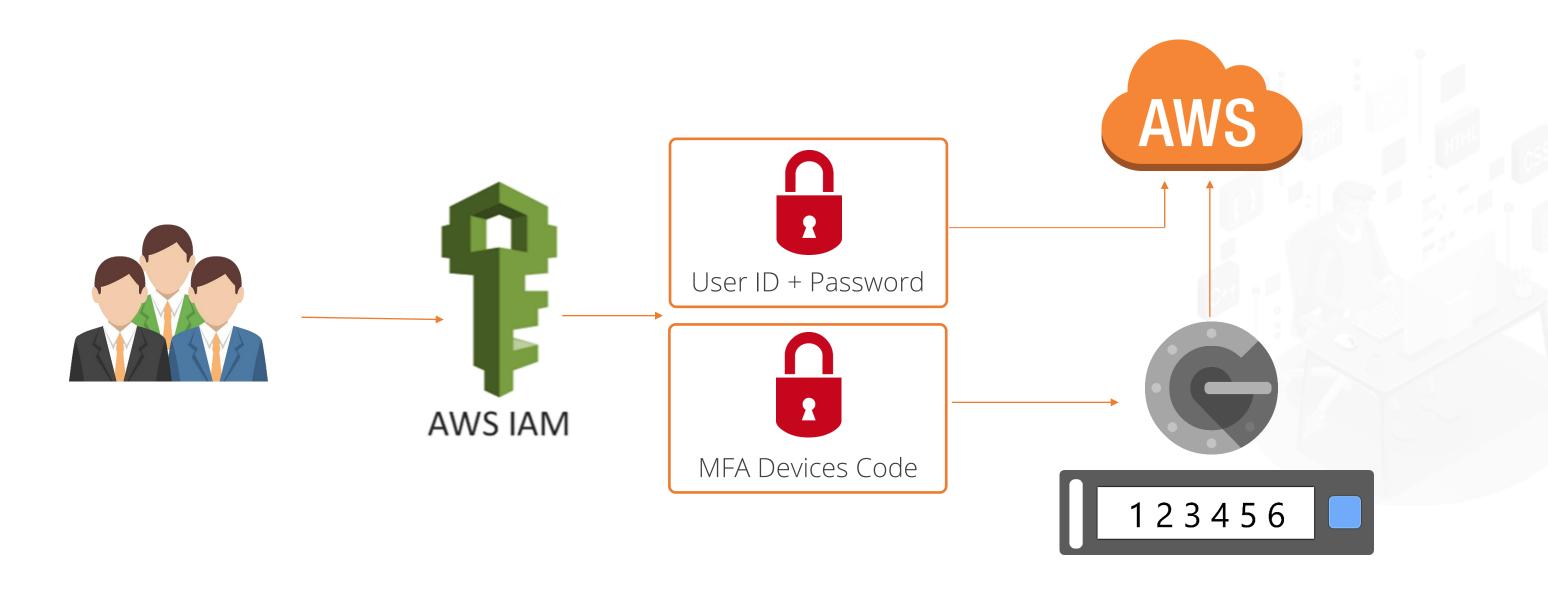
06	Granular Permissions

07	Secure Access to AWS Resources

08	Identity Federation

Multi Factor Authentication

AWS IAM supports Multi Factor Authentication (MFA) for users and resources to ensure absolute security by using MFA devices.

AWS IAM

User ID + Password

MFA Devices Code

AWS

1 2 3 4 5 6

Strong 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 ⓘ
- ☐ 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):

simplilearn

Payment Card Industry
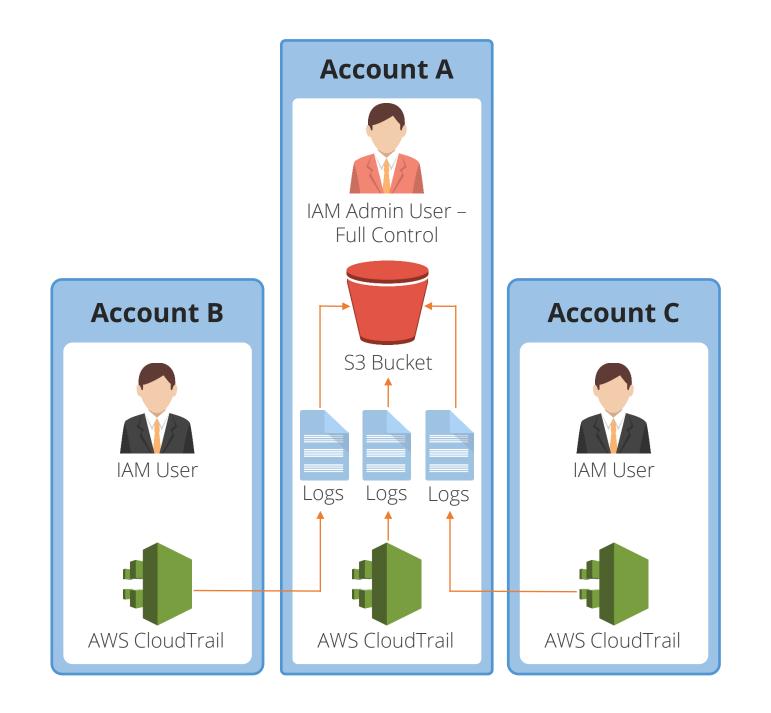
AWS IAM supports Payment Card Industry (PCI) which enables users to process, store, and transmit credit card data from a merchant or a service provider.

Identity Information for Assurance
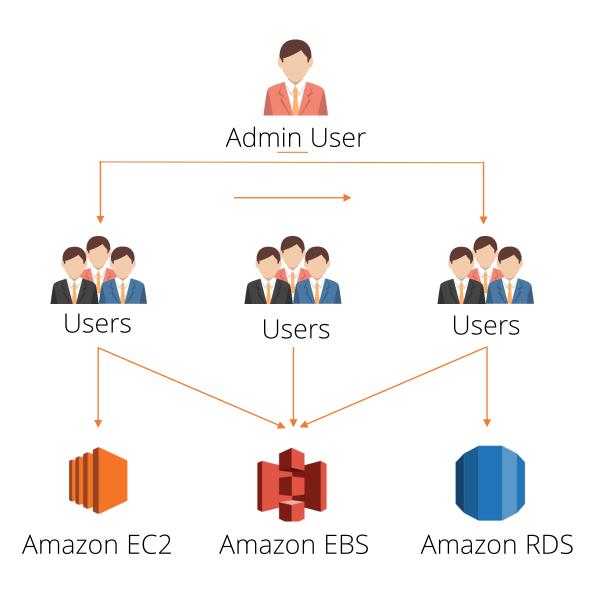
AWS IAM used with CloudTrail can be used to log, monitor, and track what users are doing with your AWS resources.

Shared Access to AWS Accounts

AWS IAM can be used to grant permissions to users for accessing and using resources in your AWS account without sharing your password.

Admin User

Users   Users   Users

Amazon EC2   Amazon EBS   Amazon RDS

Granular Permissions
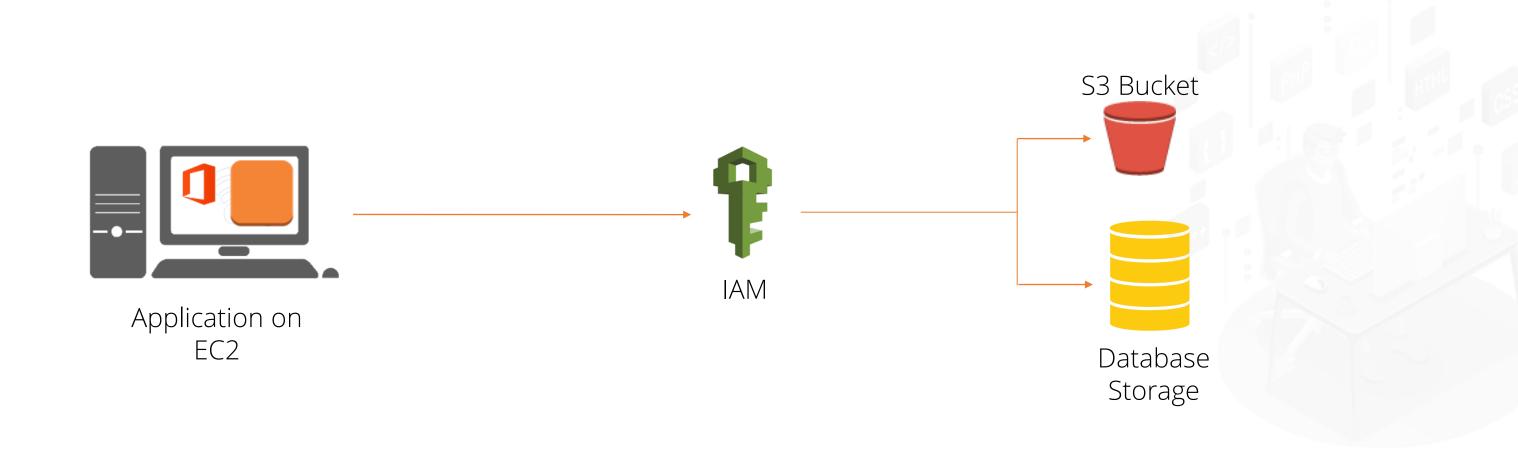
Granular permissions allow granting permissions to various users. These permissions include user access to specific services, specific permissions for action, specific access to resources, and more.

Development Team

Read Write Access

Volume

Admin Access

Instances

Instances

Volume

Secure Access to AWS Services

AWS IAM lets you securely allocate credentials that are required by the applications hosted on EC2 instances in order to access other AWS resources.

S3 Bucket

Application on
EC2

IAM

Database
Storage

Identity Federation

AWS IAM allows users with external accounts to get temporary access to AWS resources.
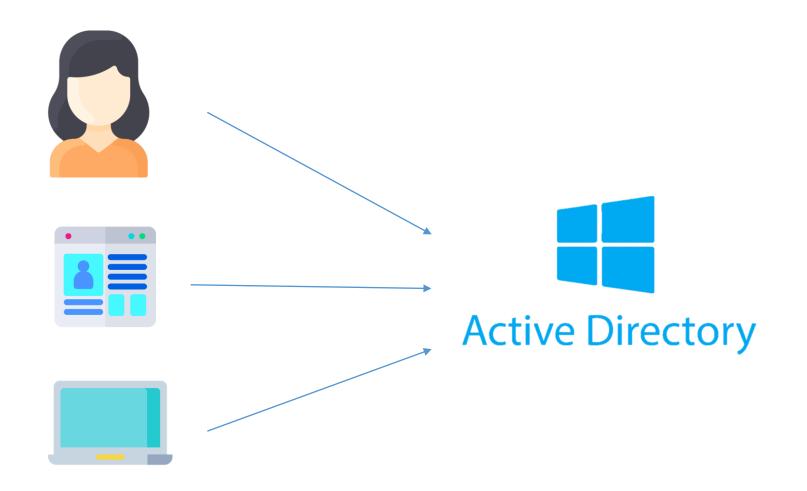
AWS Directory Service

What Is an Active Directory?

Active Directory or AD is a Microsoft product that offers services compatible with Windows servers. It is used by organizations to store their information such as number of users, computers, printers, networks, and more.

Active Directory

What Is AWS Directory Service?

AWS Directory Service offers multiple ways for users to use Microsoft Active Directory with AWS services and resources. It is built on actual Microsoft Active Directory and does not require the synchronization or replication of data from your existing Active Directory to the cloud.

AWS Directory Service

When to Use AWS Directory Service

AWS Directory Service can be used when you:
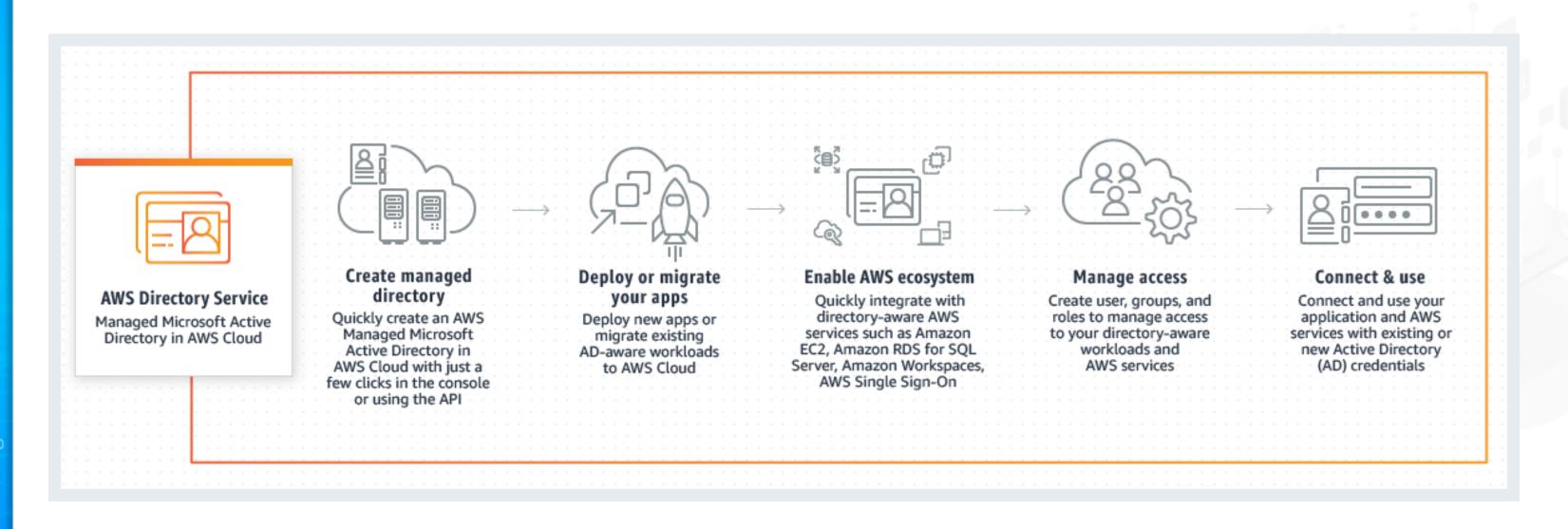
Need actual Active Directory features to support AWS applications or services

Want to extend the on-premise Active Directory to the AWS cloud

Provide Single Sign-On feature to the applications hosted on cloud

How AWS Directory Service Works

The following diagram shows the working of AWS Directory Service:

Source: aws.amazon.com

AWS Resource Access Manager

TECHNOLOGY

simplilearn
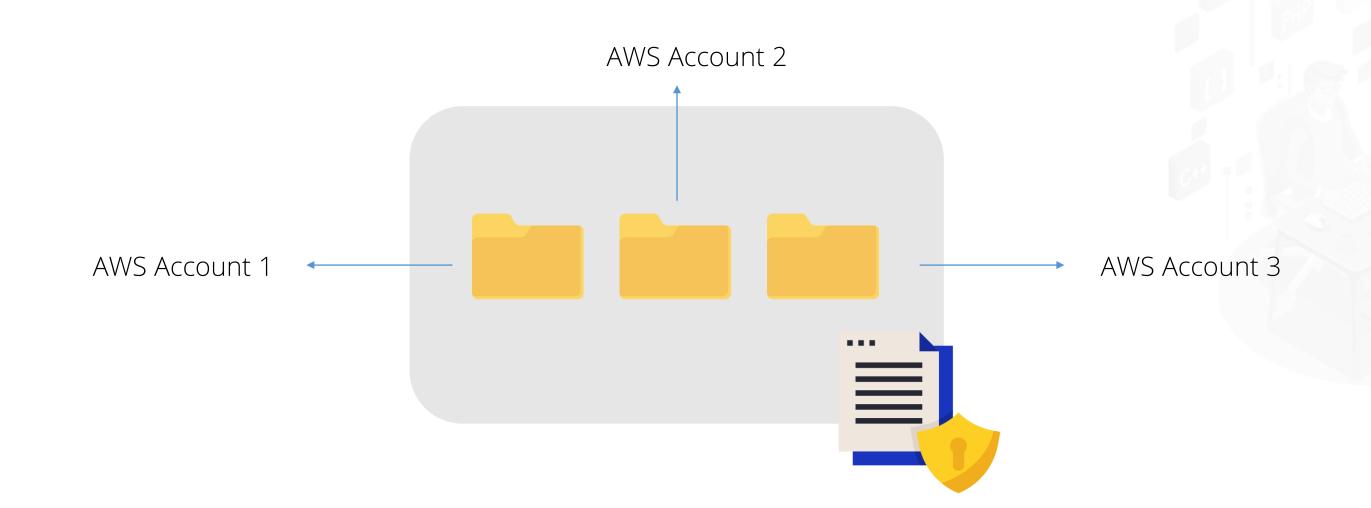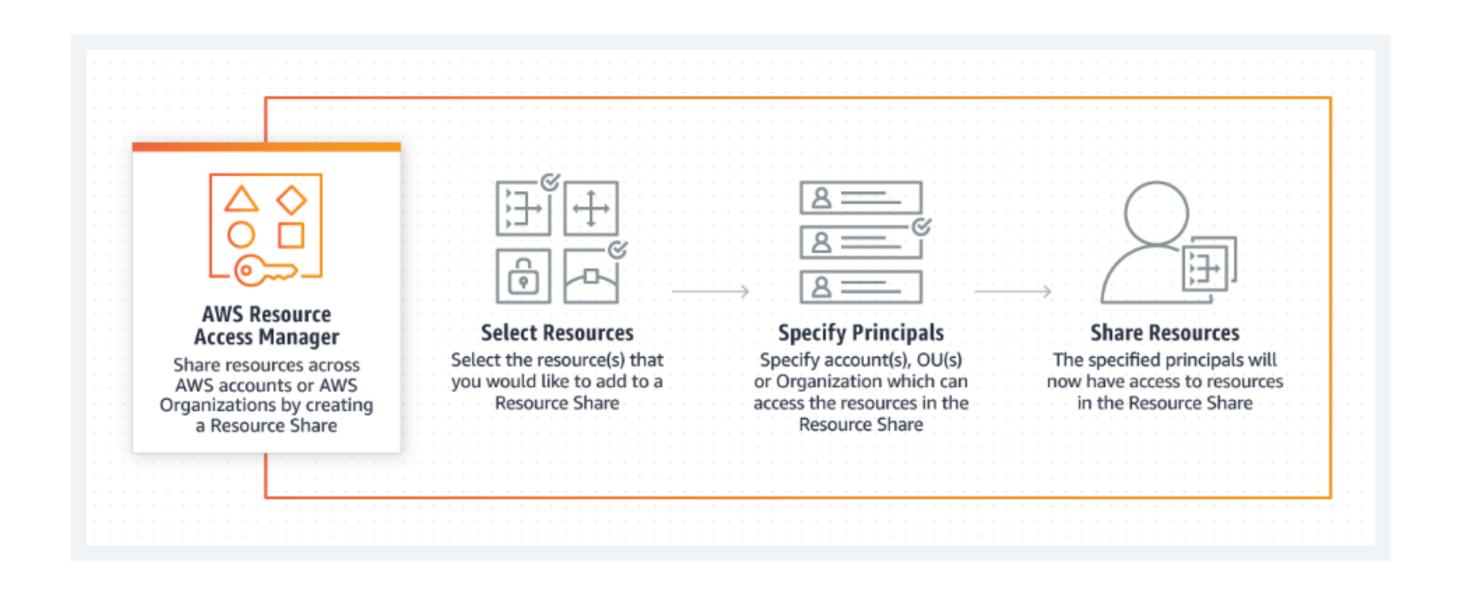
What Is AWS Resource Access Manager?

AWS Resource Access Manager or AWS RAM allows you to share your AWS resources securely with any AWS account. Users can create AWS resources centrally in a multi-account environment.

AWS Account 2

AWS Account 1

AWS Account 3
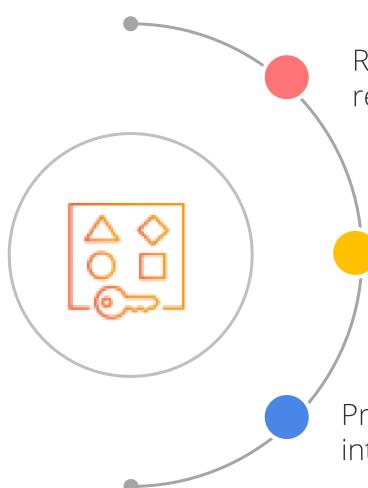
How AWS RAM Works

The following diagram shows the working of AWS RAM:

Benefits of AWS RAM

Reduces operational overhead by eliminating the need to provide duplicate resources in every account

Provides security and consistency by allowing users to use existing policies and permissions to govern the consumption of shared resources

Provides comprehensive visibility into the usage of shared details when integrated with CloudWatch to CloudTrail

Accessing AWS RAM

The following are the three different ways to access AWS RAM:

AWS RAM Console	AWS Command Line Interface	AWS Tools for Windows PowerShell
AWS RAM service offers a web-based user interface that can be accessed from Amazon console.	The AWS CLI provides direct access to the AWS RAM API operations from platforms such as windows, linux, and macOS.	AWS offers commands for developers who script in the PowerShell environment. These commands are also available for AWS RAM.

simplilearn
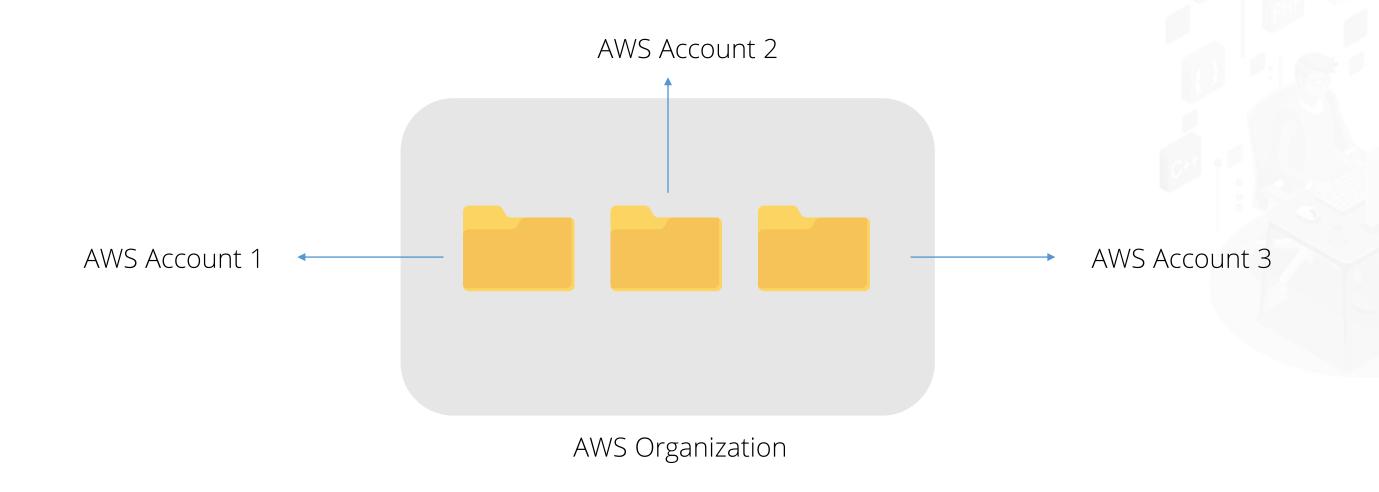
AWS Organizations

What Is AWS Organization?

AWS Organization is an account management service that allows users to consolidate multiple AWS accounts into a group called an organization that they can create and manage centrally.

AWS Account 2

AWS Account 1

AWS Account 3

AWS Organization

What Is AWS Organization?

AWS Organization is used with AWS RAM to share resources across a group of AWS accounts. It helps to centrally manage billing, control access, compliance, and security across the member AWS accounts of the organization.

More about AWS Organization:

01	Accounts are grouped into logical groups called organizational units (OUs).
02	The parent container for all the accounts in all OUs is called the root.
03	The OU that contains the member AWS accounts is called the custom OU.
04	The OU that contains the log archive account and details such as what resources are being shared among the accounts is called the core.

simpli|learn

AWS Single Sign-On

What Is AWS Single Sign-On?

AWS Single Sign-On is a property of identification and access management that allows users to authenticate their AWS accounts by signing in once and using a single set of credentials.
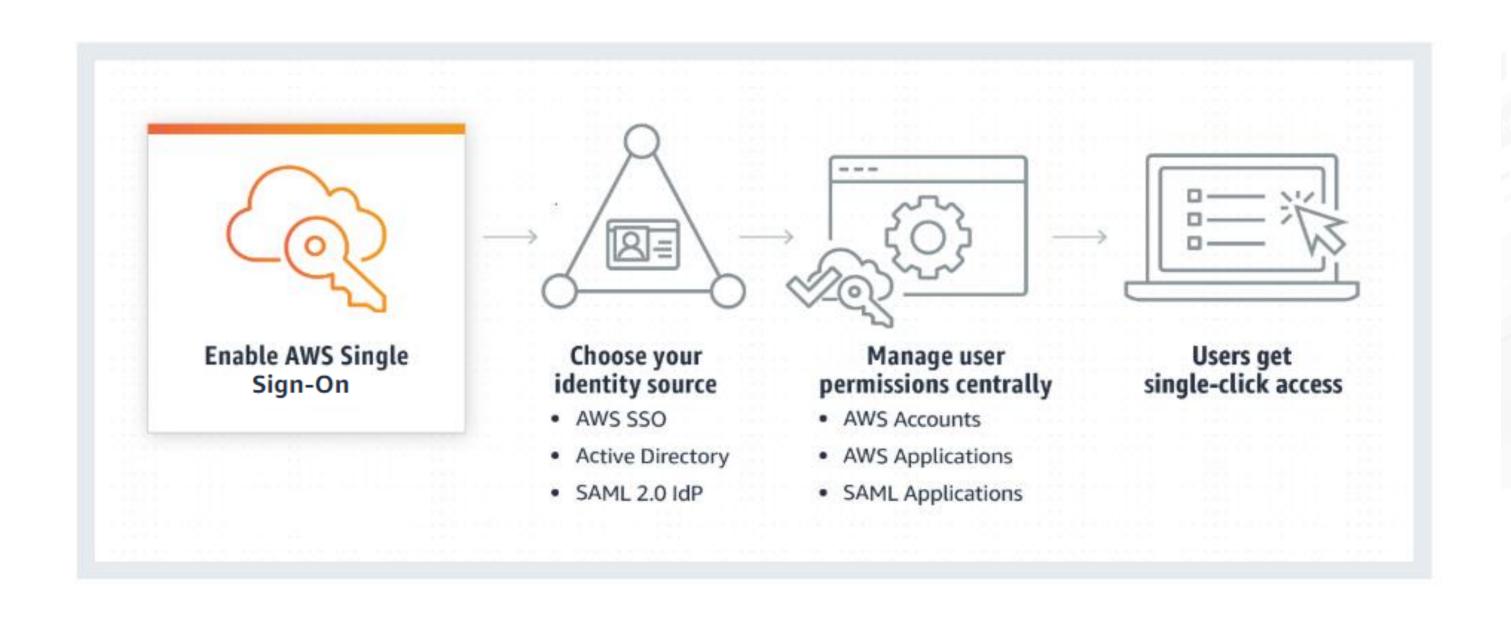
AWS Single Sign-On

Working of AWS Single Sign-On

The following diagram shows the working of AWS Single Sign-On:

Source: aws.amazon.com

Enabling AWS Single Sign-On for a User

Duration: 15 min.

Problem Statement:

Enable AWS Single Sign-On for a user using AWS SSO console

ASSISTED PRACTICE

Assisted Practice: Guidelines to Enable AWS Single Sign-On for a User

Steps to perform:

1. Open AWS SSO console and select Users
2. Click on the create user button
3. Provide an email address for the user
4. Create a group and add the user in that group
5. Sign in using the AWS SSO account

AWS Multi Factor Authentication

AWS Multi Factor Authentication

Multi Factor Authentication or MFA adds an extra layer of security to the signing-in process. It requires users to authenticate from an AWS supported MFA mechanism in addition to their sign-in credentials when they access AWS services.

Multi Factor Authentication

AWS Multi Factor Authentication

The following are the AWS supported MFA mechanisms:

Virtual MFA Devices	U2F Security Key	SMS Text Message-Based MFA
• This is a type of MFA where an application running on a phone or other devices generates a six-digit numeric code. • The user is required to type the code from the device on the webpage while signing-in.	• This is a type of MFA where U2F security key is enabled after a device is plugged into a USB port on the user's computer. • The users sign in by entering their credentials and then tapping the device instead of manually entering a code.	• This is a type of MFA where the IAM user settings include a phone number of user's SMS compatible mobile. • When the users sign in, they are required to type the six-digit code sent by AWS to the provided mobile number.

Enabling Multi Factor Authentication

Duration: 15 min.

Problem Statement:

Enable Multi Factor Authentication for the root user

Assisted Practice: Guidelines to Enable Multi Factor Authentication

Steps to perform:

1. Open AWS SSO console
2. Choose settings from the navigation pane
3. Enable Multi Factor Authentication
4. Choose authentication methods for the AWS accounts
5. Click on the Save changes button
6. Login using the AWS account for which MFA is enabled

Key Takeaways

- AWS IAM is the service that enables you to securely control user access to all the AWS services and resources.

- An IAM policy is a document that defines one or more permissions and are written in JSON format.

- AWS Directory Service can be used with on-premise AD services for managing the AWS services and resources.

- AWS RAM and AWS Organization are used to share resources across groups of AWS accounts.

- AWS Single Sign-On and Multi Factor Authentication request the users to provide AWS supported MFA entities for authentication in addition to their credentials.

simplilearn

Secure the Access to AWS Services

Duration: 60 min.

Problem Statement:

You have been asked to utilize AWS IAM options to secure the access to AWS services for the users in your organization.

Perform the following:
- Open the Amazon IAM dashboard
- Create IAM groups for the production and development departments
- Create IAM users in both the Product and Developers IAM groups
- Attach the relevant IAM policies to the Developers group
- Attach the relevant IAM policies to the Product group