

Module 03 : Identity and Access Management

Root Account

The "root user" refers to the account created when signing into AWS using the email and password associated with the account. This user has unrestricted access to the AWS account and can perform critical actions such as:

- Changing the support plan
- Modifying payment methods
- Closing the AWS account
- Transferring ownership of the account

The root user functions is similar to an admin on a computer, with the ability to install, modify, or delete any aspect of the system.

Given the level of access, it is crucial to secure the root user. This can be done by enabling multi-factor authentication (MFA) or two-factor authentication (2FA) to add an extra layer of security.

Multi Factor Authentication for Users

Enabling MFA for AWS Users:

1. After logging into your AWS account, search for the IAM service.
2. Under **Security Recommendations**, choose to add MFA for the root user.
3. Alternatively, in the top-right corner of the dashboard, click on **Security Credentials**.
4. Under **Multi-factor authentication (MFA)**, select **Assign MFA device**.

Types of MFA Devices:

1. **Authenticator App**: Applications like Google Authenticator, Microsoft Authenticator, etc., generate one-time codes.

2. **Security Key:** A physical device (similar to a USB drive) that must be connected to your computer or laptop.
3. **TOTP (Time-based One-Time Password Token):** A hardware device (resembling a USB drive) that continuously displays a six-digit code, which must be entered during login. This functions like an RSA token.

Note: The **Security Key** is considered the most secure option, as it physically needs to be present. In contrast, apps or TOTP devices can expose their codes if left unattended or forgotten in places like home.

IAM User: Identity and Access Management.

IAM (Identity and Access Management) allows us to create users and groups, and manage their permissions to access AWS resources.

Example:

In a large project, multiple resources may be involved, and IAM helps us assign specific permissions based on roles:

1. AWS Engineer:

- For handling **EC2/server issues**, we create a user with their own username and password, but restrict their access to only specific resources. For example, they can be given **EC2 full access**, but any attempt to perform actions outside of this scope would be denied.

2. Database Administrator:

- For resolving **database issues**, a separate user with individual credentials is created, and they are granted **RDS full access**.


3. Monitoring:


- To **monitor AWS resources**, a user is created with **read-only access**, allowing them to view resources but not make any changes.

Key Concepts:

- **Least Privilege Mechanism:** This principle ensures that users are granted the minimum permissions necessary to perform their job functions. IAM allows us to enforce this by

restricting user access to specific operations and resources based on their roles.

 **Important for Certification:** Understanding and implementing least privilege is crucial for security best practices.

 **Note:** In real-world organizations, users rarely operate as root users. Instead, they work as IAM users with specific permissions tailored to their role.

Policy:

A policy is a document that defines a set of permissions for AWS services, controlling which actions can be performed and on which resources.

IAM Password Policies

Creating Customer Managed Policies

Policy Generator

IAM Policy Simulator

Auditing User Activity