Configuring IAM Users, Groups, Policies, and Roles for Secure AWS Access

Introduction:

This report documents the creation and configuration of Identity and Access Management (IAM) resources in an AWS account. IAM provides a granular control system for managing user access and permissions to AWS services.

Components and Configuration:

1. IAM Users:

- A user named "my-new-user" was created using the `aws iam create-user` command. IAM users are individual identities that can be used to interact with AWS resources.

2. IAM Groups:

- A group named "my-new-group" was created using the `aws iam create-group` command. IAM groups are collections of users that simplify access management by allowing permissions to be assigned collectively.
- The user "my-new-user" was added to the group "my-new-group" using the `aws iam add-user-to-group` command. This allows the user to inherit any permissions assigned to the group.

3. IAM Policies:

- A policy named "my-new-policy" was created using the `aws iam create-policy` command. IAM policies define the specific actions users or roles are allowed to perform on AWS resources.

IAM Policy Document

The policy document for "my-new-policy" specifies the following:

- **Version:** The policy format version (2012-10-17 in this case).
- **Statement:** This section defines the permissions granted by the policy.
    - **Effect:** "Allow" indicates the actions are permitted.

    - **Action:** The allowed actions include "s3:ListBucket" (listing buckets) and "s3:GetObject" (retrieving objects) within S3.
    - **Resource:** This specifies the resources the actions apply to. The policy allows access only to objects within the bucket named "my-bucket" and its subfolders ("arn:aws:s3:::my-bucket/*").
- The policy "my-new-policy" was attached to the user "my-new-user" using the `aws iam attach-user-policy` command. This grants the user the permissions defined in the policy.

4. IAM Roles:

- A role named "my-new-role" was created using the `aws iam create-role` command. IAM roles are temporary security credentials that can be assumed by users, applications, or other AWS services. This allows for a more secure approach by controlling who can access resources.

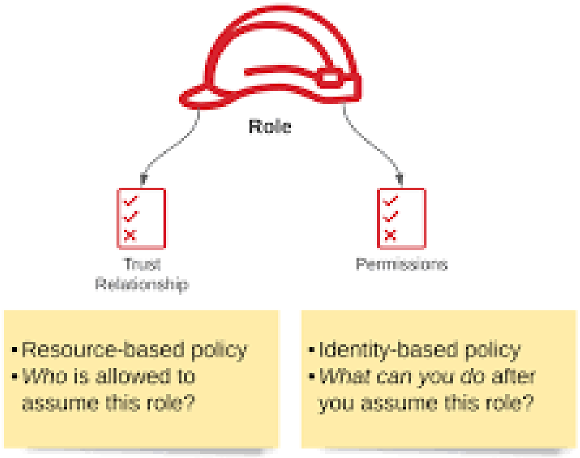
...

IAM Role with Assume Role Policy

The role creation includes an "Assume Role Policy Document":

- **Version:** The policy format version (2012-10-17 in this case).
- **Statement:** This section defines who can assume the role.
    - **Effect:** "Allow" indicates the action is permitted.

- **Principal:** This specifies who can assume the role. In this case, only the EC2 service ("Service": "ec2.amazonaws.com") is allowed.
- **Action:** The allowed action is "sts:AssumeRole," which grants temporary credentials to the EC2 service.


Role
Trust Relationship
Permissions
▪ Resource-based policy
▪ *Who is allowed to assume this role?*
▪ Identity-based policy
▪ *What can you do after you assume this role?*