(AWS) - PART II

accendnetworks

A Beginner's Guide to AMAZON WEB SERVICES

Introduction to Security and Access Management

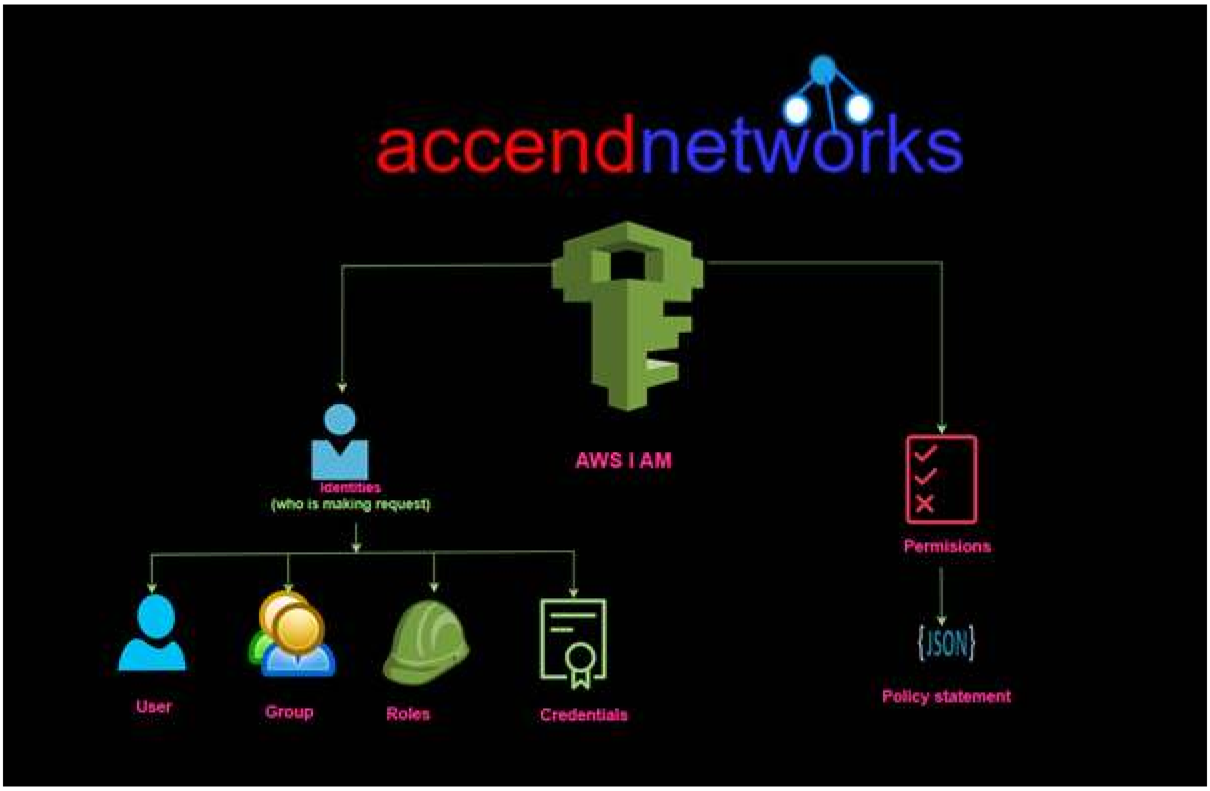
BY: **PAULA WONG**, CEO AND FOUNDER, CEH-MASTER,
CCIE SECURITY AND SWITCHING, C-7 #1086962
AWS CERTIFIED CLOUD PRACTITIONER

Security and Access Management

Mastering IAM Policies: A Guide to Cloud Security and Access Management

AWS Identity and Access Management (IAM) is at the core of securing your AWS resources by providing fine-grained control over access permissions. IAM policies are essential in defining what actions are allowed or denied on AWS resources. There are two main types of IAM policies: **managed policies** and **inline policies.** In this article, we'll break down these policies.

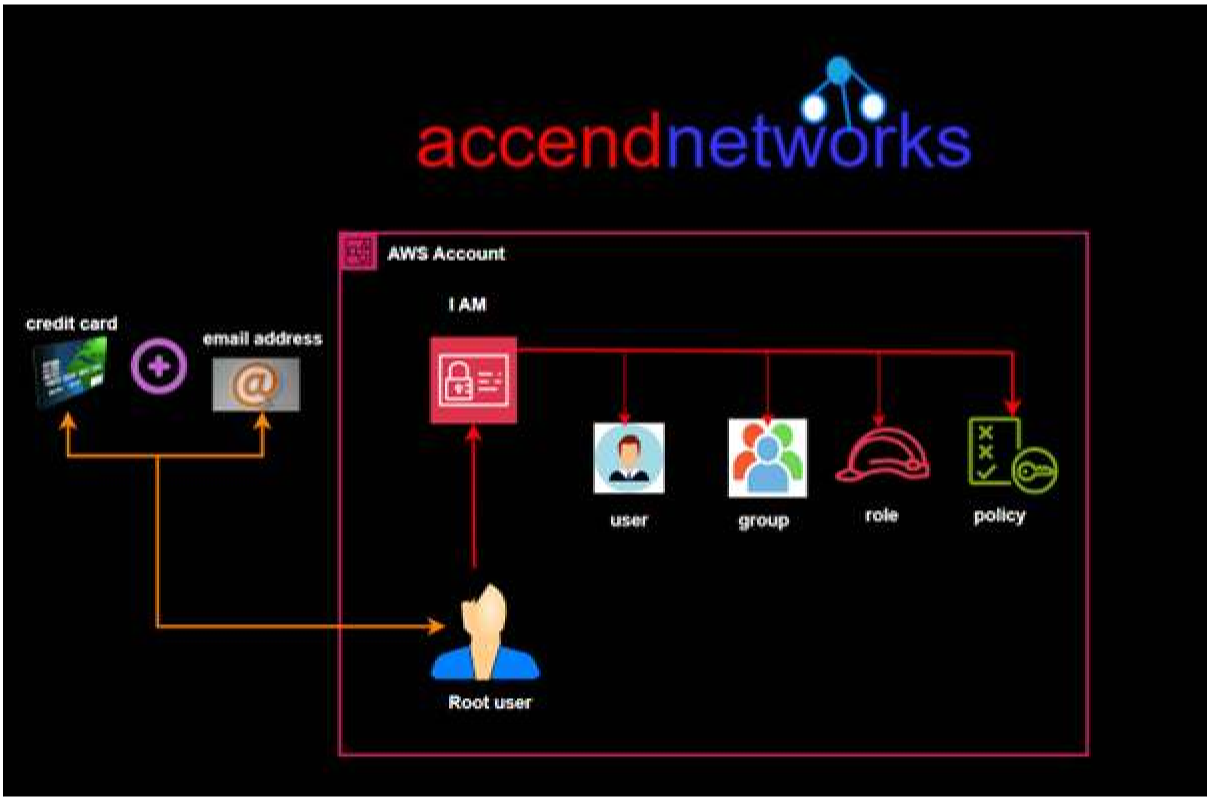
When thinking about IAM, there are two broad categories to consider, **Identities** and **permissions.**



Identities refer to the various mechanisms that AWS provides to identify who is requesting a particular AWS action, authenticate that person or entity, and organize similar entities into groups, all are essential to mastering IAM policies.

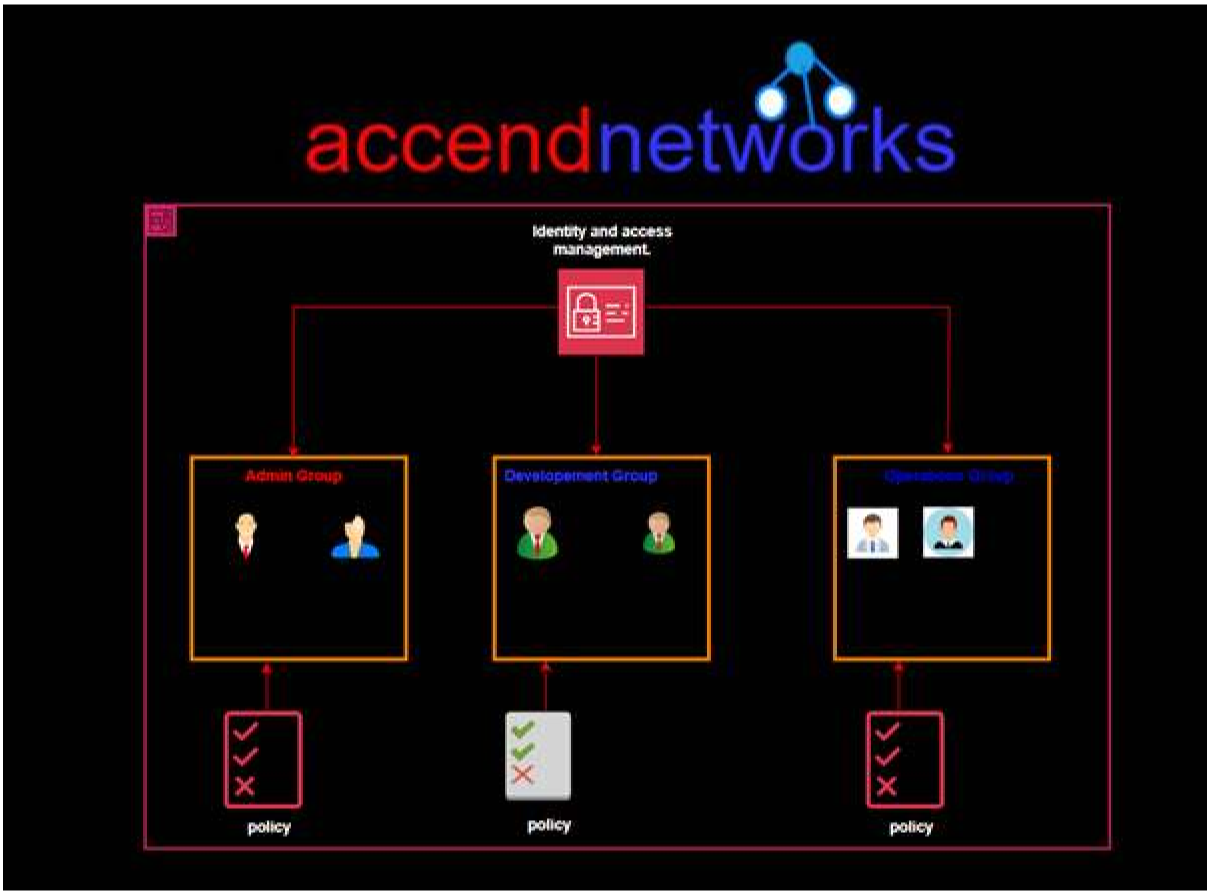
Permissions refer to what a particular identity is allowed to do in the AWS account.

Best Practices for IAM Policies: IAM Users



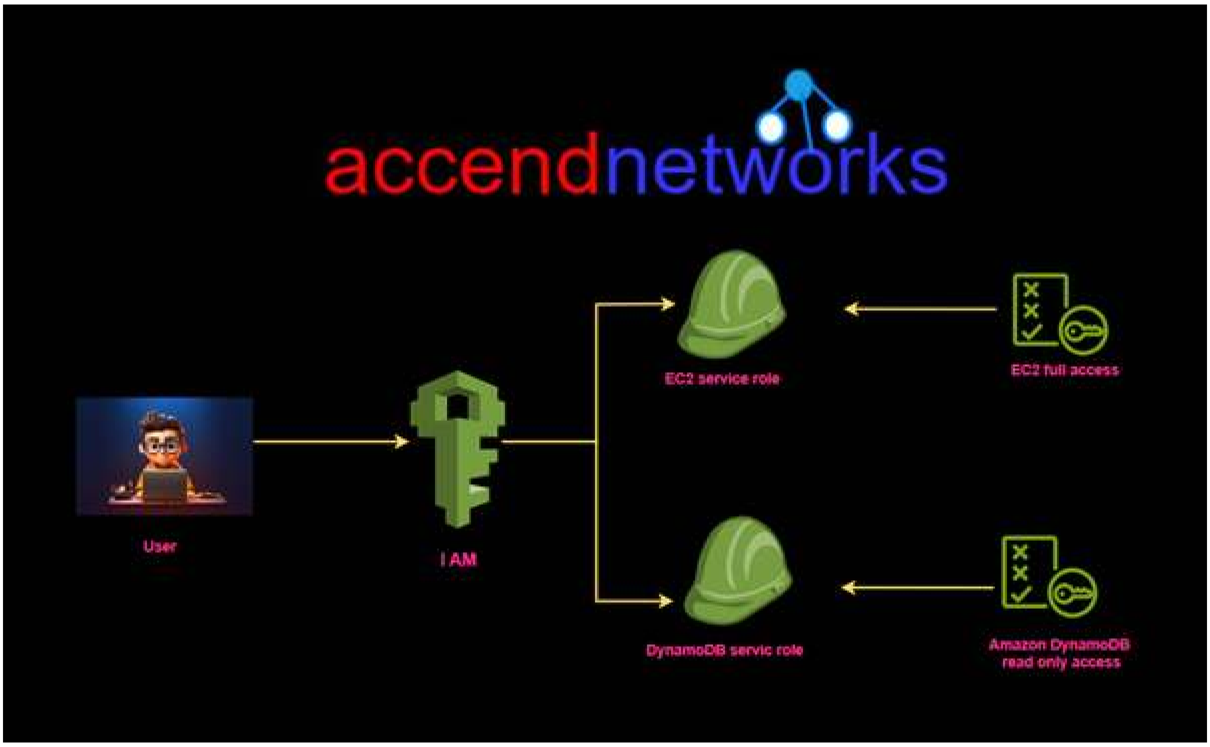
IAM users are individual entities within your AWS account representing people or applications interacting with AWS services. Each IAM user has a unique identity and can be assigned specific permissions that dictate what AWS resources they can access and what actions they can perform. IAM users can authenticate using an AWS Management Console login, access keys for programmatic access (CLI or API), or both. Users are often created for individuals in an organization who need access to AWS resources and are assigned policies that define their permissions.

IAM Groups



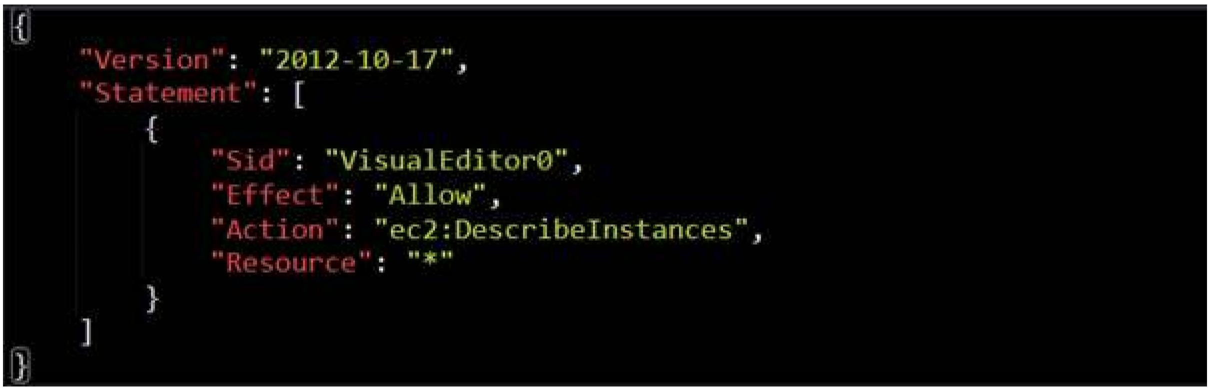
IAM groups are collections of IAM users that share the same set of permissions. Instead of managing permissions for each user, you can attach policies to a group, and all users within that group will inherit those permissions. This makes it easier to manage users with similar access needs, such as developers, administrators, or auditors.

IAM Roles



IAM roles used to grant temporary access to AWS resources without requiring long-term credentials like passwords or access keys. Instead, roles are assumed by trusted entities such as IAM users, applications, or AWS services (e.g., EC2, Lambda) when they need to perform certain actions. Roles have permissions associated with them through policies, and when an entity assumes a role, it temporarily gains those permissions.

What are IAM Policies?



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

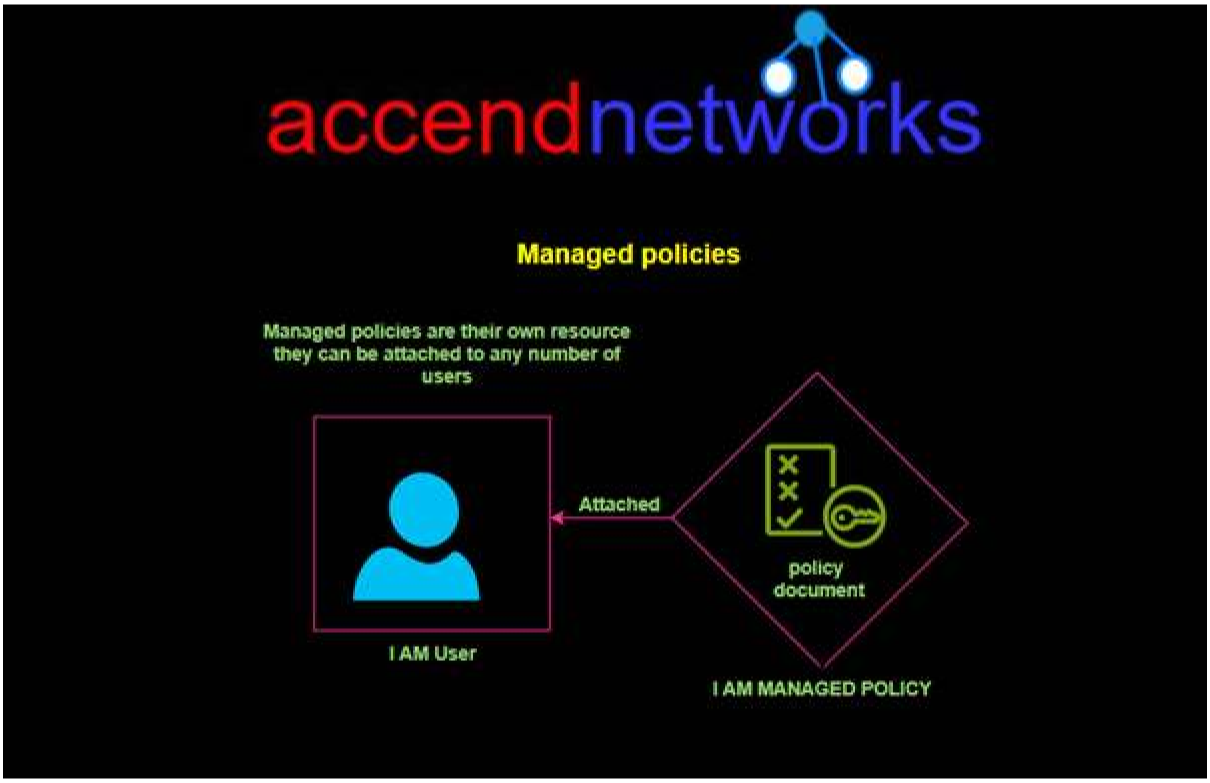
An **IAM policy** is a JSON document that defines what actions are allowed or denied on specific AWS services and resources. It contains statements with actions, resources, and conditions under which access is granted or denied.

Actions: These define what the policy allows or denies.

Resources: These are the AWS resources on which actions are performed, such as an S3 bucket or an EC2 instance.

Conditions: Optional filters that refine when the policy applies, such as applying only to a specific IP address.

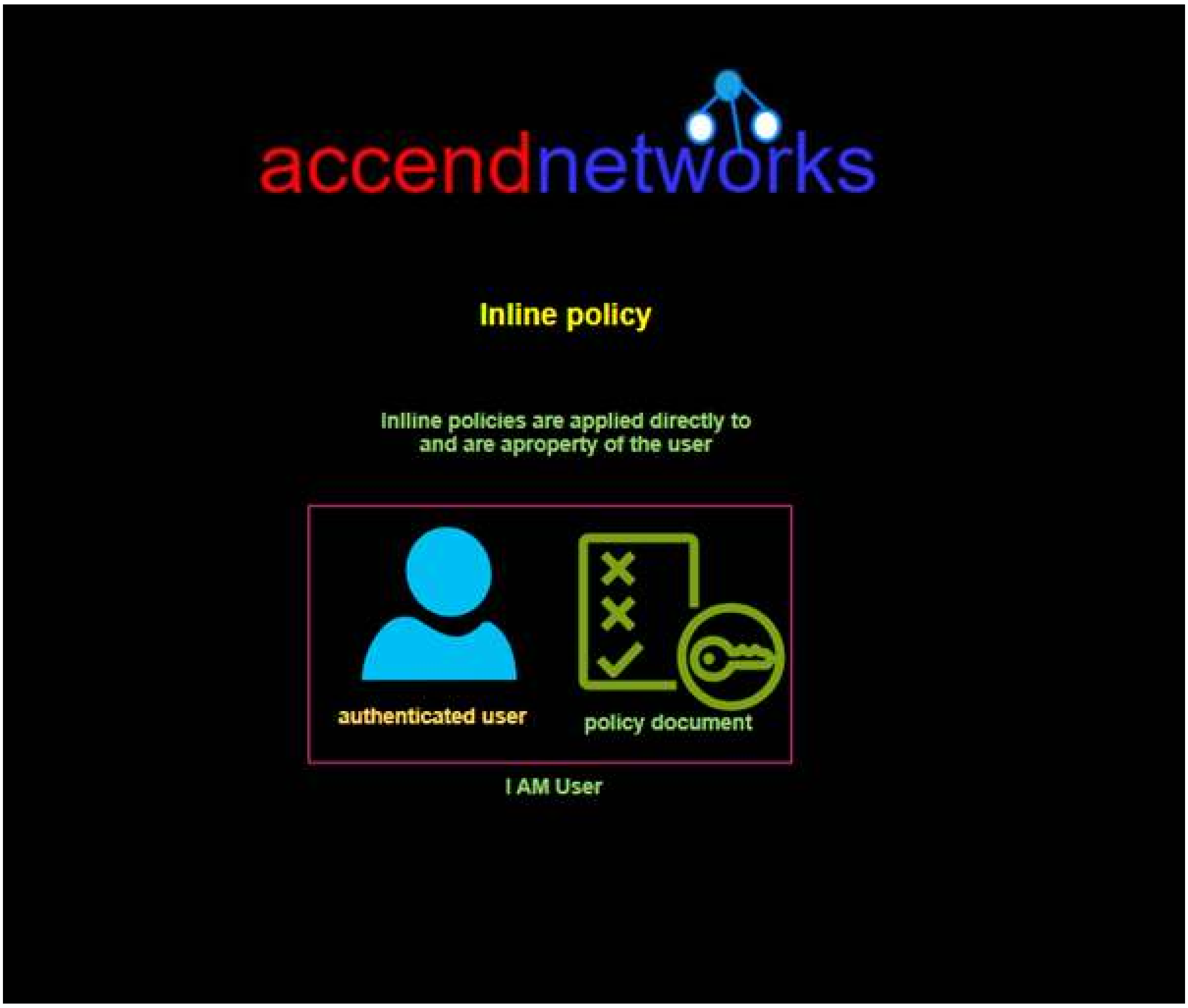
Managed Policies


accendnetworks
Managed policies
Managed policies are their own resource they can be attached to any number of users
Attached
policy document
I AM User
I AM MANAGED POLICY

Managed policies are standalone policies that can be attached to multiple users, roles, or groups. They are easier to maintain because any changes to a managed policy apply across all entities attached to it. Managed policies come in two types:

1. **AWS Managed Policies:** Predefined policies created and maintained by AWS. These cover common use cases, like **AdministratorAccess** which grants full access to all AWS resources, or **ReadOnlyAccess** which allows viewing but not modifying resources.
2. **Customer Managed Policies:** Policies created and managed by AWS users. These are useful when predefined AWS-managed policies don't meet specific business needs, allowing you to create custom policies tailored to your organization's security requirements.

Inline Policies


accendnetworks
Inline policy
Inlline policies are applied directly to and are aproperty of the user
authenticated user
policy document
I AM User

Inline policies are policies directly embedded within an IAM user, group, or role. Unlike managed policies, inline policies exist solely within the entity they are attached to and cannot be reused. Inline policies are best when you need strict control over specific permissions, such as granting temporary or highly tailored access to a particular user.

Comparison of Managed Policies vs. Inline Policies

Managed policies can be attached to multiple users, roles, or groups, making them reusable across various entities. In contrast, **inline policies** are attached to a specific user, role, or group and cannot be reused.

When it comes to maintenance, **managed policies** are easier to update because any changes apply to all the entities they are attached to. On the other hand, **inline policies** need to be handled individually for each user, role, or group they are attached.

The typical use case for **managed policies** is to provide general-purpose permissions that can be reused across multiple accounts, while **inline policies** are ideal for fine-grained control over specific entities.

Conclusion:

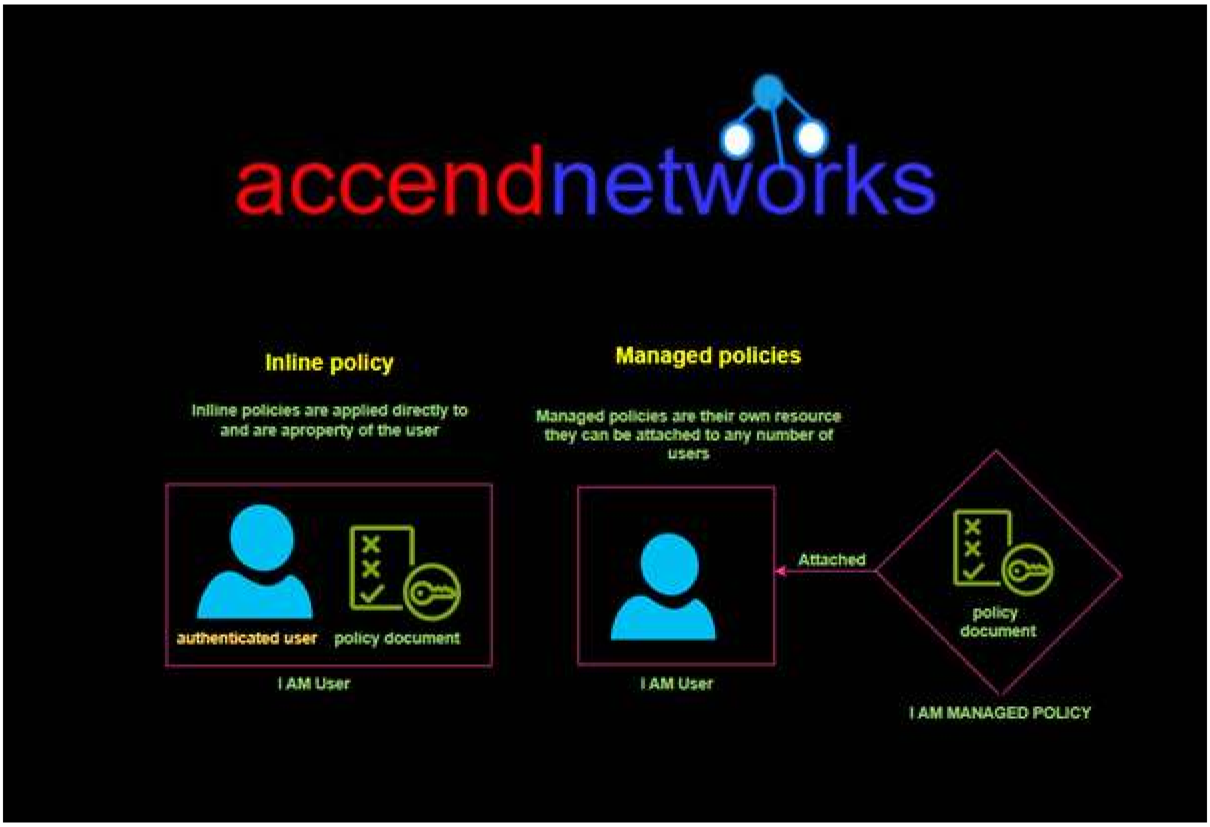
AWS IAM policies provide the fine-grained access control needed to manage who can access your resources and what actions they can perform. **Managed policies** are reusable, making them easier to manage across multiple entities, while **inline policies** provide more granular control for individual users or roles. Understanding when to use each type is key to maintaining security and flexibility in your AWS environment.

Thanks for reading and stay tuned for more. Make sure you clean up.

If you have any questions concerning this article or have an AWS project that requires our assistance, please reach out to us by leaving a comment below or email us at: sales@accendnetworks.comr.

Thank you!

Exploring Managed and Inline Policies for Cloud Security: Hands-On Demo

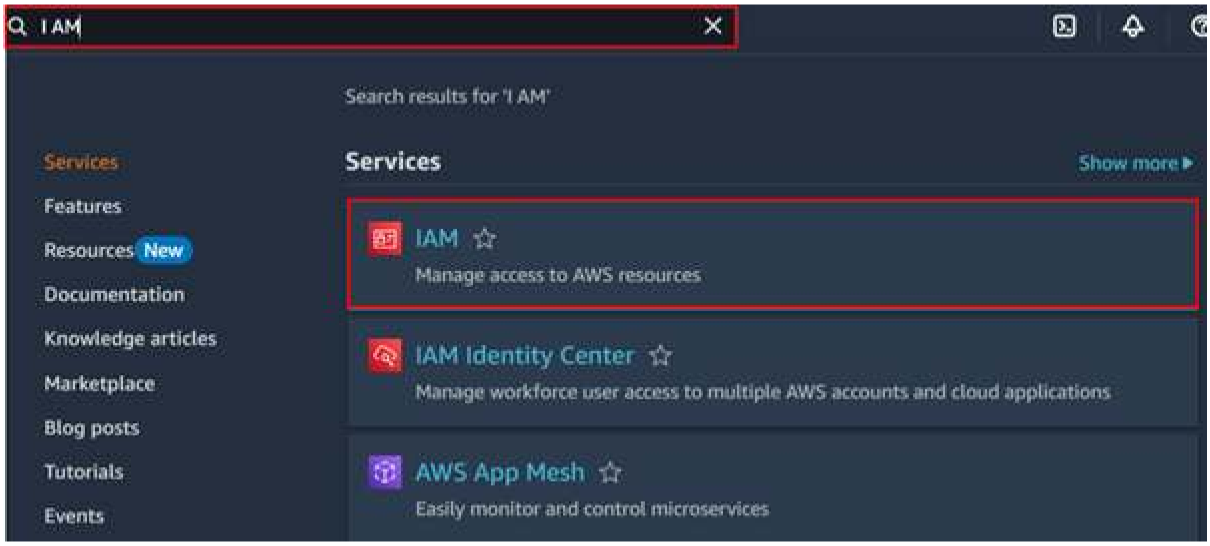

accendnetworks
Inline policy
Inlline policies are applied directly to and are aproperty of the user
authenticated user
policy document
I AM User
Managed policies
Managed policies are their own resource they can be attached to any number of users
I AM User
Attached
policy document
I AM MANAGED POLICY

AWS Identity and Access Management (IAM) is a powerful tool that helps control access to AWS resources. By managing who can access what, IAM ensures the security and flexibility of your AWS environment. In this blog, we will be exploring Managed and Inline Policies for Cloud Security and provide a hands-on lab to demonstrate how to create an IAM user and attach an inline policy to the user.

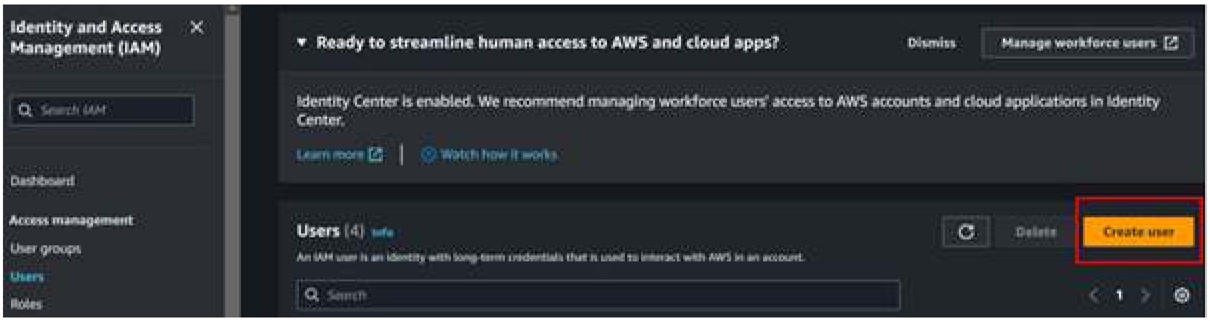
We will start by creating an IAM user through the AWS Management Console and attaching a managed policy that allows the user to change only their password. After creating the user, we will log in with their credentials and attempt to describe EC2 instances, which will result in access being denied due to insufficient permissions.

Next, we will create an inline policy specifically for the user, permitting them to describe EC2 instances. This will provide the user with the necessary access to view instance details while maintaining fine-grained control over their permissions.

To begin, log into the AWS Management Console using an IAM user with administrative privileges. In the AWS Console, navigate to the search bar, type IAM, and select **IAM** from the list of services. This will take you to the IAM dashboard, where we can manage users, roles, and policies.


I AM
Search results for 'I AM'
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Tutorials
Events
Services
Show more ▶
IAM ☆
Manage access to AWS resources
IAM Identity Center ☆
Manage workforce user access to multiple AWS accounts and cloud applications
AWS App Mesh ☆
Easily monitor and control microservices

In the left side UI of the I AM console, select users then click Create User.



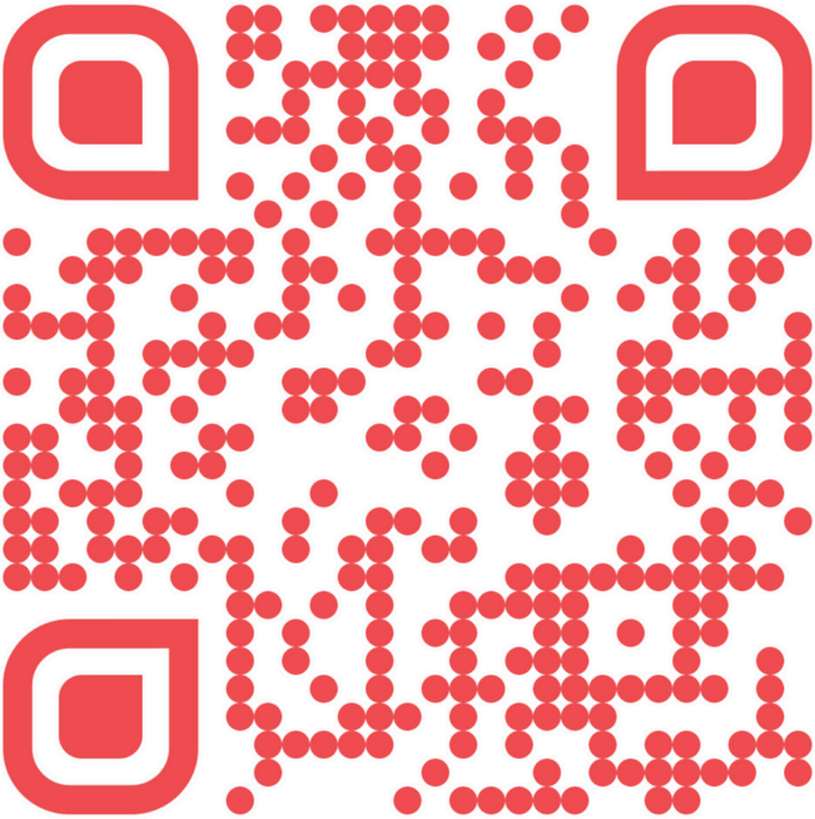
▾ Ready to streamline human access to AWS and cloud apps?

Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Fill in the user's details, including a preferred name. Afterward, check the box labeled Provide user access to the AWS Management Console to allow the user to log in. Next, select the radio button that says I want to create an IAM user.

accendnetworks



www.accendnetworks.com