COURSEWARE

AWS IAM User Overview

Contents

Overview

Identity Access Management (IAM) is a service which can allow the root user to create account, roles and groups.
The root user also can grant permissions and has no restriction, this is mainly because the root user is paying for all the services being used.

This topic will discuss the importance of IAM User overview, as well as how we can configure the user for other use through AWS.

There are 5 tabs to view:

- Permissions
- Groups
- Tags
- Security Credentials
- Access Advisor

Permissions

There are 2 sections under this tab:

- Permissions Policies
- Permissions boundary

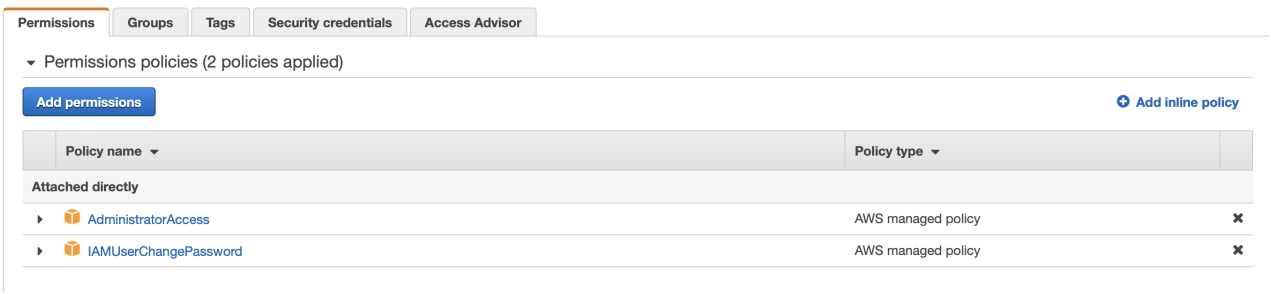
Permissions Policies

This shows an overview of the permissions which this specific user has.

You have the option to click on the drop-down icon on each permission to see the policy in JSON format.

There is a cross on the right of each permission to remove that specific policy.

You can click on **Add permissions**, to add another managed policy to the user.
You also have the option to add an *in-line* policy, this allows you to add in JSON format, a custom policy.
This is used if AWS does not have a policy or a group of policies that do not meet your requirement.



Permissions boundary

This is an advanced section for IAM, and would normally fall under the Systems Operations Exam.
This is similar to PErmissions Policies, however the distinct difference is that this sets the maximum permission the user is allowed to have.
This is enforced before the *Permissions Policies*.
So if theres a rule in Permissions boundary which provides only a maximum permission to use EC2 Instances, and the Permissions Policies tries to allow usage of S3 buckets, then the user will have permission issues when attempting to access S3 bucket.

Groups

This shows the list of groups which the specific user is in. There is also an option to add that user to another group.

Tags

These are key-value pairs you can add to your user. Tags can include user information, such as email address and so on. This will help organise, track or control access for this user.

Security Credentials

This will show all type of credentials which this user has. This includes the sign-in link, access keys for aws commands on terminals and more.

There are 5 sections to *Security Credentials*:

- Sign-in Credentials
- Access Keys
- SSH Keys for AWS CodeCommit
- HTTPS Git credentials for AWS CodeCommit
- Credentials for Amazon Managed Apache Cassandra Service

Sign-in Credentials

When creating a user and providing the user console access, this will generate a sign-in link, which has a unique id that will allow the user access to the root users AWS account.
You can also manage the user sign-in and password.
This includes removing the user from being able to sign in.
You can also set/generate a password for this user, this can be used to provide a new password if the old password has been forgotten.

You can also manage Multi Factor Authentication (MFA). As a root user, you have the option to ensure this user must login through MFA.

You can also upload a signing certificates to add more security to the user during login.

Access Keys

Generate an *Access* and *Secret* keys. This allows users to have access to AWS resources through the terminal, meaning, the user would be able to run AWS commands using the awscli, and have access to all resources that is permitted accoriding to the users IAM policy.

Important to note that you can view the *Secret* key once, unless downloaded.Otherwise, the *Secret* key cannot be viewed in the console, and would require you to generate a new key if forgotten/lost.

SSH Keys for AWS CodeCommit

This relates to how AWS ensures security when using AWS Version Control Service, AWS CodeCommit.
You have to generate your own public and private key.
And upload your public key onto AWS.
This will allow you to clone, push and so on to your repository.

HTTPS Git Credentials for AWS CodeCommit

Again, this related to how AWS ensures security when using AWS Version Control Service, AWS CodeCommit.
AWS will generate username and password credentials.
This credential will have to be used, when cloning and pushing from AWS CodeCommit repo.

Credentials for Amazon Managed Apache Cassandra Service (MCS)

Generate a username and password that can be used to authenticate to Amazon MCS.

Access Advisor

This will show a list of permissions that the user has access to, and which policy has granted access to this user.
This is helpful to revise the policies granted and adjustment to allow the least amount of policies that the user needs.

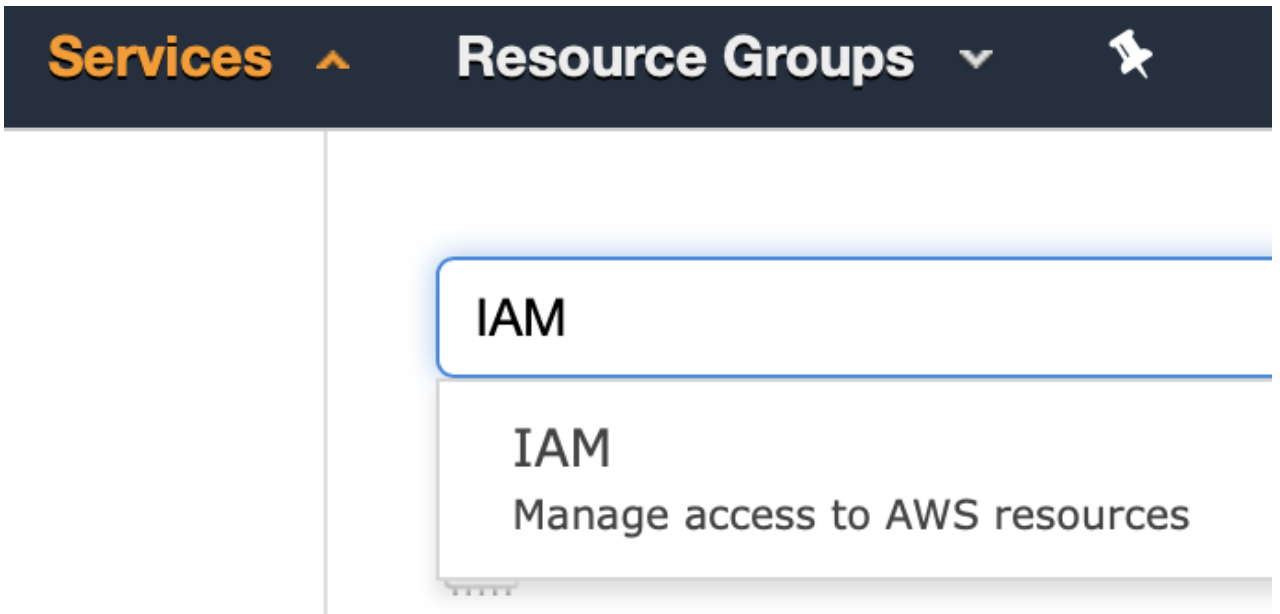
Pre-requisite

Topics:

- AWS SignUp
- AWS IAM Users

Tutorial

1. Navigate to the AWS Console and sign in here
2. Search for IAM under the services drop-down menu.



3. You will then be redirected to the IAM Dashboard.
   On the left navigation panel, click on the *Users* section.
4. Select one of the user that have been created.

5. Navigate through all the tabs that are discussed in the *Overview* section above.

Exercises