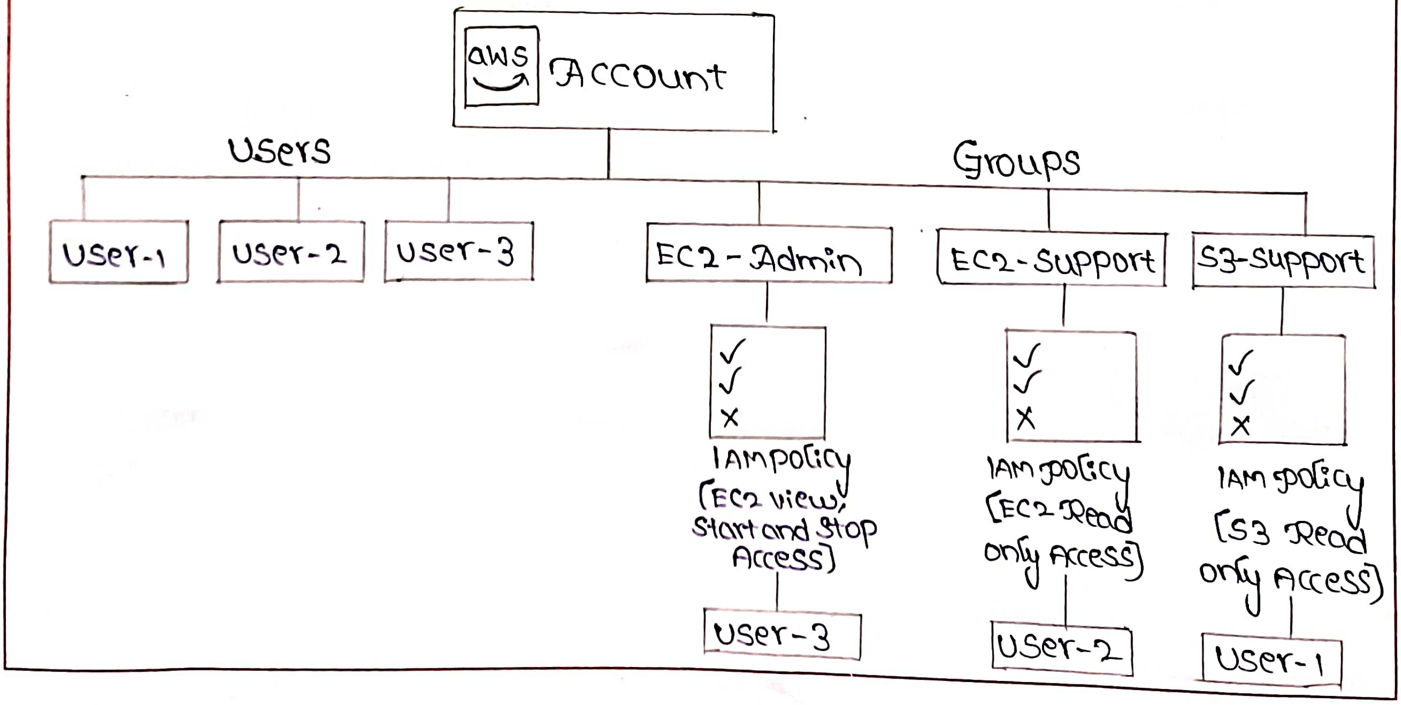
Lab-1::

Aim:: Introduction to AWS Identify and Access management.

Description:: AWS identify and Access Management (IAM) is a web services that enables Amazon web services (AWS) customers to manage users and user permissions in AWS. With IAM., we can centrally manage users, security credentials such as access keys and permissions that control which AWS resources users can access. AWS Identify and Access Management (IAM) can be used to manage IAM users and their access, manage IAM users Roles and their permissions.and manage feederated users and their permissions.

Architecture::


aws
Account
Users
Groups
User-1
User-2
User-3
EC2-Admin
EC2-Support
S3-Support
✓ ✓ X
✓ ✓ X
✓ ✓ X
IAM policy (EC2 view, Start and Stop Access)
IAM policy (EC2 Read only Access)
IAM policy (S3 Read only Access)
User-3
User-2
User-1

Steps followed for AWS IAM console:-

* Choose Start Lab to launch the Lab.

* Wait until the message "Lab status: ready".

* Choose AWS - This will open the AWS management console in a new browser tab. The system will automatically login.

Task 1: Explore the users and Groups:-

* In AWS management console, on the services menu, select IAM.

* In Navigation plane, choose users.

  The following users have been created automatically

  - User-1
  - User-2
  - User-3

* Choose user-1, Here the permissions tab will be displayed.

* Notice that user-1 does not have any permissions.

* Choose the Groups tab, Here observe that user-1 is not a member of any groups.

* Choose the security credentials tab. Here user-1 is assigned to a console password.

* In navigation plane, Choose user groups.

  The following groups have been created automatically:

  - EC2 - Admin
  - EC2 - Support
  - S3 - Support

* Choose the EC2-Support group.

* Choose permissions tab. This group has a managed policy associated with it, called AmazonEC2ReadonlyAccess. Managed policies are pre-built policies that can be attached to IAM users and Groups.

* Choose plus(+) icon next to the AmazonEC2ReadonlyAccess policy. to view policy details.

The basic structure of the statements in an IAM policy is:-

- Effect:- It says whether to Allow or Deny the permissions.
- Action:- It specifies the API calls that can be made against an AWS services.
- Resources:- It defines the scope of entities covered by the policy rule.

* Choose minus (-) icon to hide the policy details.

* In navigation Plane, choose user groups.

* Choose the S3-Support group and then choose permissions tab.

- The S3-Support group has the AmazonS3ReadonlyAccess policy attached.

* Choose the plus(+) option to view the policy details.

- This policy will grant permissions to get and list resources in Amazon S3.

* Choose minus (-) icon to hide the policy details.

* In navigation plane, choose user groups.

* Choose the EC2-Admin group and then choose the permissions tab.
  - It has Inline policy, which is a policy assigned to just one user or Group.

* Choose the plus(+) icon to view the policy details.
  - This policy grants permissions to view information about AmazonEC2

* Choose the minus(-)icon to hide the policy details.

Task2:- Add users to Groups:-

Add user-1 to the S3-Support Group:-

* In navigation plane, choose user groups.
* Choose the users tab.
* In the users tab, choose Add users.
* In the Add users to S3-support window, configure the following:-
  - select user-1.
  - At bottom of screen, choose Add users.
* In the users tab we will see that user-1 has been added to the group.

Add user-2 to the EC2-Support Group:-

* Use the similar process for adding the user-2 to the EC2-support group.

* In the users tab we will see that user-2 has been added to the group.

Add user-3 to the EC2-Admin Group:-

* Use the similar steps, add the user-3 to the EC2-Admin group.

* User-3 should now be part of the EC2-Admin group.

Task-3:- Sign-in and Test users:-

* In navigation pane, choose Dashboard.

* An IAM users sign-in link is displayed on the right. It will look similar to: https://123456789012.signin.aws.amazon.com/console.

* copy the sign-in URL for IAM users in this account to a text editor.

* open a Incognito window.

* Paste the IAM users sign-in link into the address bar of private browser session and press Enter.

* Sign-in with:

IAM username: user-1

Password: Lab-password1

* In the services menu, choose S3.

* choose the name of bucket that exists in the account and browse the contents.

-o Now, test whether they have access to Amazon EC2.

* In the services menu, choose EC2.

* In the navigation pane, choose Instances. But here we see a message that states you are not authorized to perform this operation.

* Sign user-1 out of the AWS management console by completing the

following actions:

- At top ~~of~~ the screen, choose user-1.
- choose signout

* paste the IAM users sign-in link into private window tab's address bar and press Enter.
* sign-in with:
  - IAM username : user-2
  - password: Lab-password2.
* In the services menu, choose EC2.
* In the navigation pane, choose the Instances.
  - select the instance named LabHost.
* In the Instance state menu, select stop instance.
* In the stop instance window, select stop. but we will receive an Error stating that you are not authorised to perform this operation.
* In the services, choose S3.
  - you will see the message you don't have permissions to list buckets.
* sign user-2 out of AWS management console by completing the following actions:.
  - At top of the screen, choose user-2.
  - choose sign-out
* paste the IAM users sign-in link into private window tab's address bar and press Enter.

* Sign-in with:
    - IAM User name: user-3
    - Password: Lab-password3
* In the services menu, choose EC2.
* In the navigation pane, choose Instances.
    - select the instance named LabHost.
* In the Instance State menu, choose stop Instances.
* In the stop instance window, choose stop.
* close private browser window.
* Choose End Lab and then select Yes to confirm that you want to end the lab.