EXPERIMENT:7- IMPLEMENT ACCESS MANAGEMENT IN CLOUD ENVIROINMENT

Aim:

To implement access management in cloud management in cloud environment.

Algorithm:

To implement the access management in cloud

environment, there are several steps considered

in it.

Step:1 open aws console

Step:2-search iam [identity access management]

in console.

Step:3-in 'iam' there are certain access

management like, user groups ,users, roles and

polices.

User Groups:

At first, we should create a group, like giving a meaningful group name with attaching a permission policy.

Users:

First give an username, and while giving an console access to person should give only in IAM user. user should have console password and it has two ways of getting the password they are auto generated and custom password.

Next add the users to the created group.by doing this user will be created successfully and user will get the password in the way of csv file or the instructions will be mailed by the owner and then the user should change the password.

Roles:

Select the trusted entity, while creating role,now here we use a function called ,"lambda". The work of the lambda is to call, 'aws' services on your behalf.

Next adding permission to the role owner giving permission to the user for example user getting ec2 full access. and give the role name which is going to played by the user.

ec2:it is an web service that provides secure, resizable compute capacity in the cloud.

there are certain trusted entities which will be in default

trusted policy:

```
{
"version:" 2012-10-17",
"statement":[
{
"effect":"allow",
"action":[
"sts":assumerole
];
"principal":{"service":[
"lamda.amazonaws.com"
]
}
}
]
}
```

Now add permission to it and in description give the lambda function and after doing this the role for the user is created successfully.

Policy:

A policy is an object in the aws, that defines permission and now the policy we going give is "ec2fullaccess"

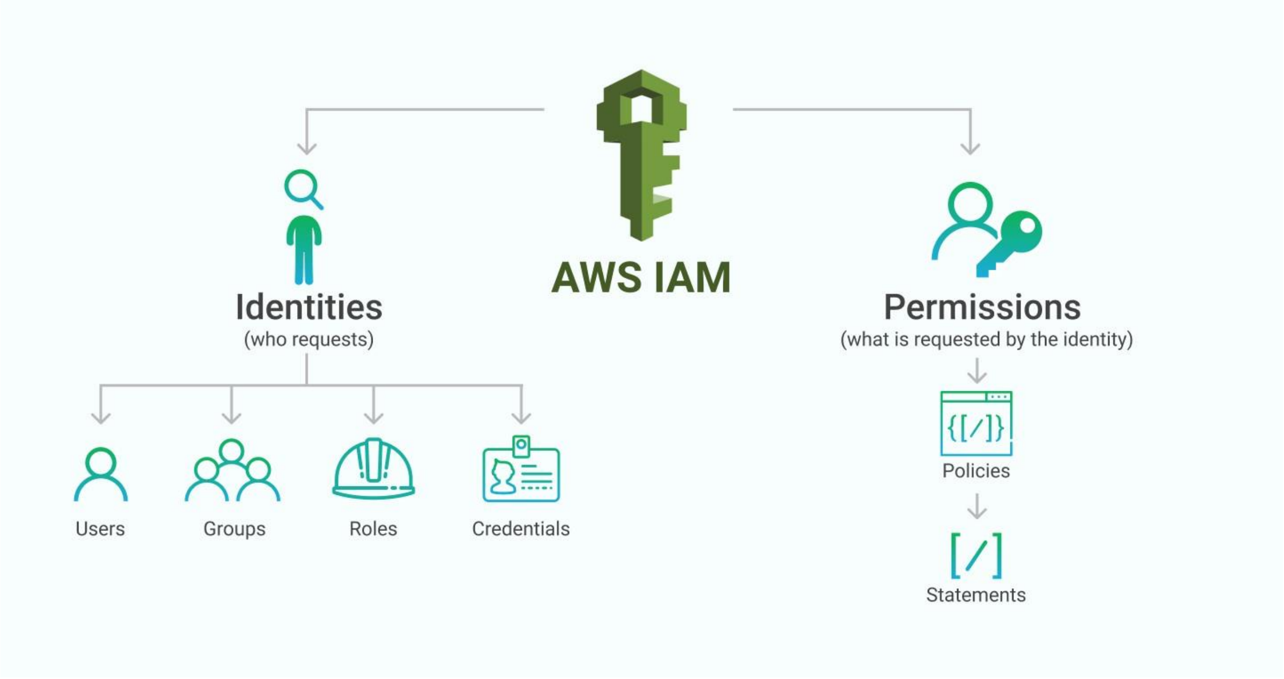
Next, specify the permission select the service the 'ec2', now owner can give an action which is allowed to the user, there will be certain access level and give the meaningful access name

After this policy will be created successfully.

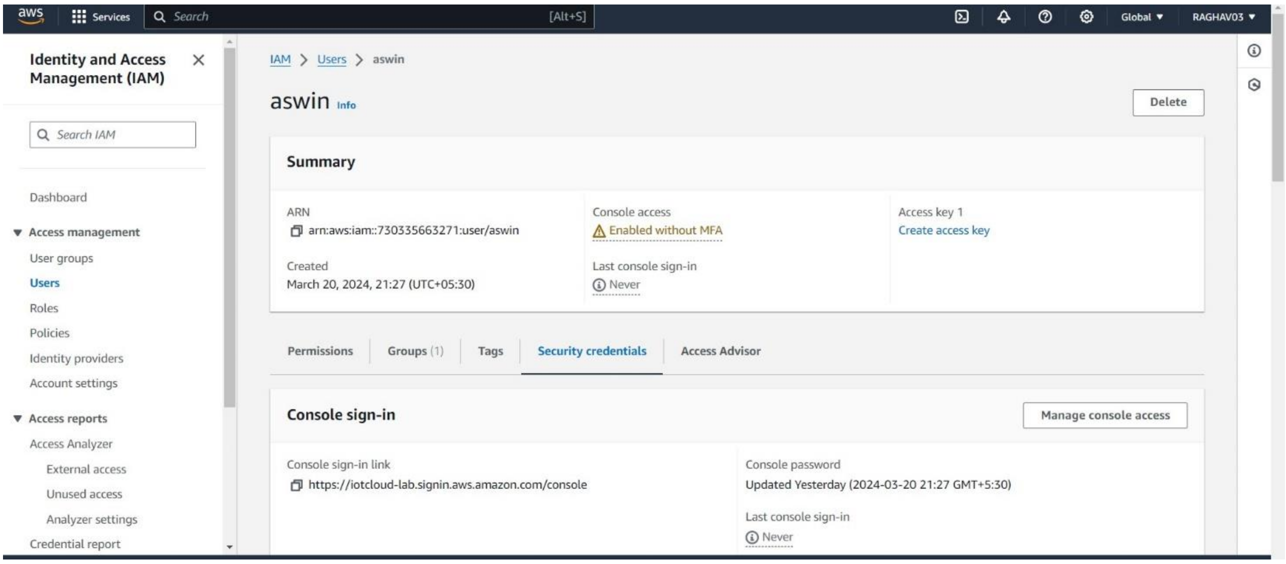
Result:

To implementation of access management in cloud environment is done successfully and the output is verified.

Diagram:



OUTPUT:



aswin

Summary

ARN
arn:aws:iam::730335663271:user/aswin

Created
March 20, 2024, 21:27 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Console sign-in

Console sign-in link
https://iotcloud-lab.signin.aws.amazon.com/console

Console password
Updated Yesterday (2024-03-20 21:27 GMT+5:30)

Last console sign-in
Never