

BY Sabreen Salama

## AWS LAB1:

- 1- Create aws account and set billing alarm
- 2-
  - create 2 groups one admin and one for development
  - in the admin group it has admin permission , and in the development only access to s3
  - create admin-1 user console access and mfa enabled in admin group
  - and admin2-prog with cli access only and list all users and groups using commands not console
  - in the development group create user with name dev-user with programmatic and console access then try to access aws using it (take a screenshot from accessing ec2 and s3 console)
  - Also access cli using dev-user and try to get all users and groups using it

Required:

Screenshot from each group with users and permissions attached to it

Screenshot from using dev-user to access ec2 and s3 from console

Screenshot from listing users and groups using admin2-prog

Screenshot from listing users and groups using dev-users

## 1) Group admins:

Identity and Access Management (IAM)

Q Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > admins

admins

Summary

User group name

admins

Creation time

May 31, 2023, 16:30 (UTC+03:00)

ARN

arn:aws:iam::951412713666:group/admins

Users

Permissions

Access Advisor

Users in this group (2)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Q Search

< 1 >

⌕

☐

User name

↗

Groups

Last activity

▼

Creation time

▼

☐

admin-1

1

None

13 hours ago

☐

admin2-prog

1

None

13 hours ago

Identity and Access Management (IAM)

Q Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > admins

admins

Summary

User group name

admins

Creation time

May 31, 2023, 16:30 (UTC+03:00)

ARN

arn:aws:iam::951412713666:group/admins

Users

Permissions

Access Advisor

Permissions policies (1)

Info

You can attach up to 10 managed policies.

Q Filter policies by property or policy name and press enter.

< 1 >

⌕

☐

Policy name

↗

Type

▼

Description

☐

AdministratorAccess

AWS managed - job function

Provides full access to AWS services and resources.

## 2) Group developers:

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > developers

developers

Summary

User group name

developers

Creation time

May 31, 2023, 16:52 (UTC+03:00)

ARN

arn:aws:iam::951412713666:group/developers

Users

Permissions

Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

< 1 >

User name

Groups

Last activity

Creation time

dev-user

1

None

12 hours ago

IAM > User groups > developers

developers

Summary

User group name

developers

Creation time

May 31, 2023, 16:52 (UTC+03:00)

ARN

arn:aws:iam::951412713666:group/developers

Users

Permissions

Access Advisor

Permissions policies (1)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

< 1 >

Policy name

Type

Description

AmazonS3FullAccess

AWS managed

Provides full access to all buckets via the AWS Management Console.

## 3) Dev-user accessing s3

AWS

Services

Search

[Alt+S]

Global

dev-user @ 9514-1271-3666

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets

Info

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 >

Name

AWS Region

Access

Creation date

No buckets

You don't have any buckets.

Create bucket

#### 4) Dev-user trying to access ec2

The screenshot shows the AWS Management Console for the 'dev-user' in the 'Stockholm' region. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Limits, Instances, Images, Elastic Block Store, and Lifecycle Manager. The main content area is the 'EC2 Dashboard' showing a grid of resource counts and status. Most resources show an 'API Error' status. The 'Launch instance' button is prominent. The 'Service health' section indicates the EC2 service is operating normally. The 'Account attributes' section shows errors for supported platforms and default VPC. The 'Explore AWS' section shows GuardDuty and Spot Instances promotions.

#### 5) Listing users and groups using admin2-prog

```
heba@heba-HP-ProBook-450-G4:~$ aws iam get-user --query 'User.UserName' --output text
admin2-prog
heba@heba-HP-ProBook-450-G4:~$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "admin-1",
      "UserId": "AIDA53BE55DBKQT36BDK3",
      "Arn": "arn:aws:iam::951412713666:user/admin-1",
      "CreateDate": "2023-05-31T13:33:51+00:00"
    },
    {
      "Path": "/",
      "UserName": "admin2-prog",
      "UserId": "AIDA53BE55DBKTIHYWNYJ",
      "Arn": "arn:aws:iam::951412713666:user/admin2-prog",
      "CreateDate": "2023-05-31T13:42:34+00:00"
    },
    {
      "Path": "/",
      "UserName": "dev-user",
      "UserId": "AIDA53BE55DBGNXZ054JF",
      "Arn": "arn:aws:iam::951412713666:user/dev-user",
      "CreateDate": "2023-05-31T13:54:22+00:00",
      "PasswordLastUsed": "2023-06-01T02:53:35+00:00"
    }
  ]
}
```

#### 6) Listing users and groups using dev-user

```
heba@heba-HP-ProBook-450-G4:~$ aws iam get-user --query 'User.UserName' --output text
An error occurred (AccessDenied) when calling the GetUser operation: User: arn:aws:iam::951412713666:user/dev-user is not authorized to perform: iam:GetUser on resource: user dev-user because no identity-based policy allows the iam:GetUser action
heba@heba-HP-ProBook-450-G4:~$ aws iam list-users
An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::951412713666:user/dev-user is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::951412713666:user/ because no identity-based policy allows the iam:ListUsers action
heba@heba-HP-ProBook-450-G4:~$
```