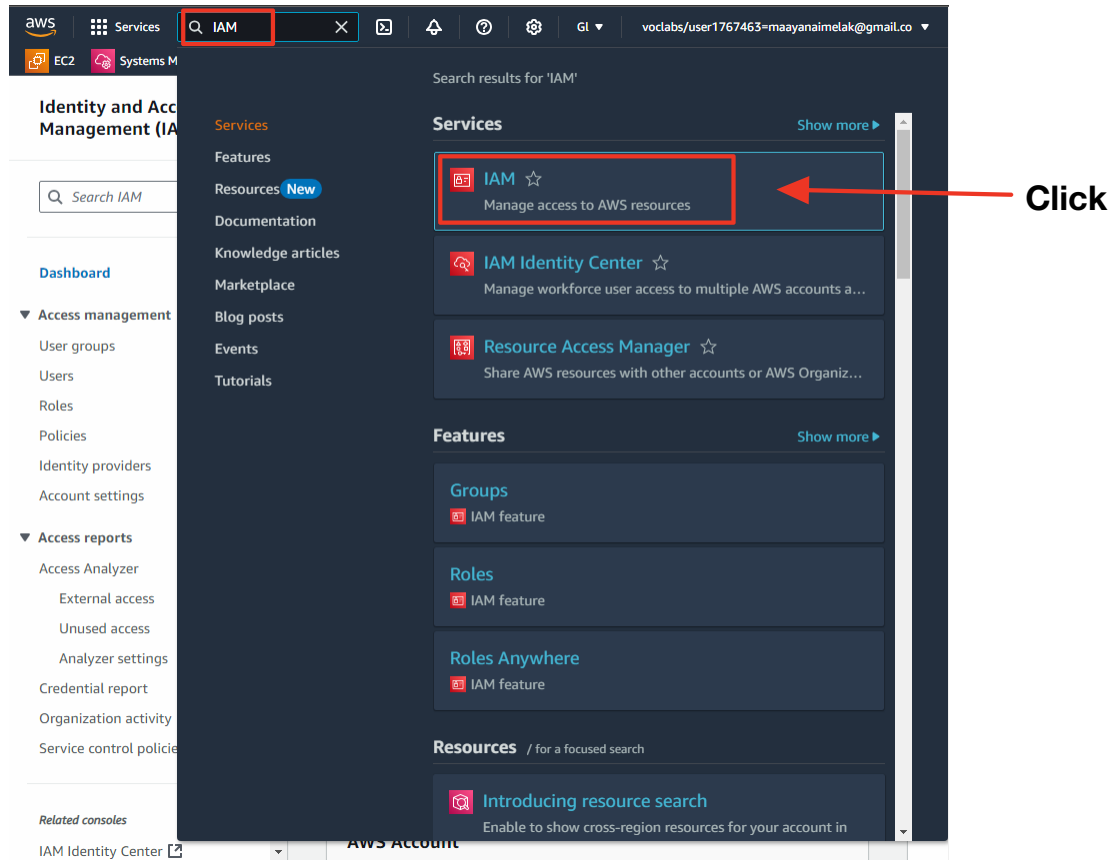
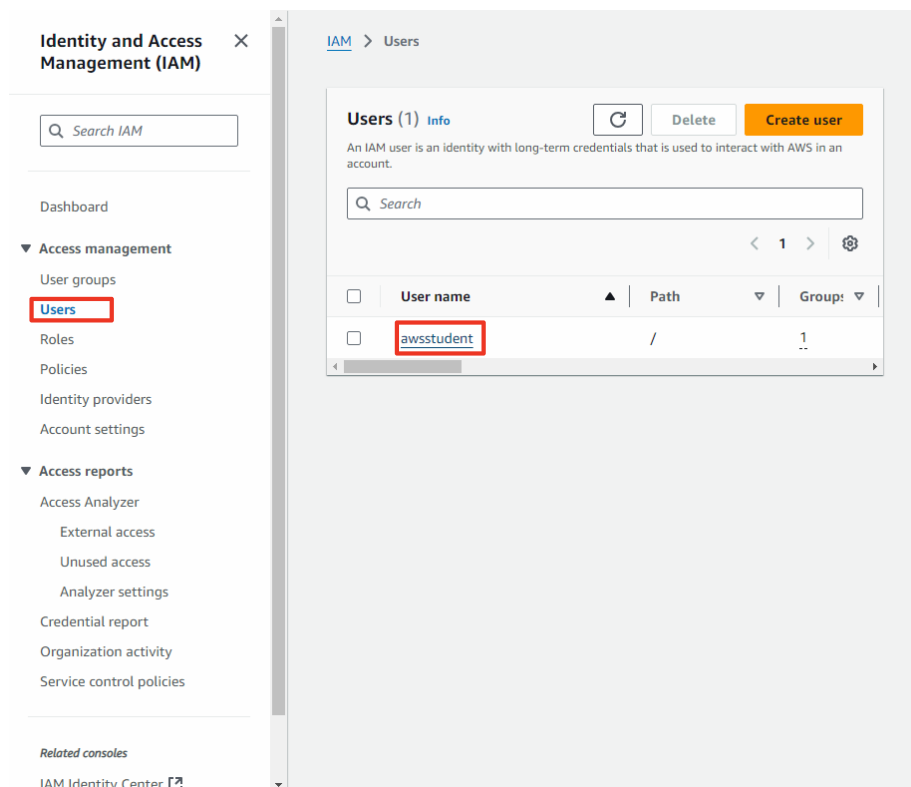


Task 3: Observe IAM configuration details in the AWS Management Console.

In the **Search** box, enter **IAM**:



Choose **Users**, click on **awsstudent**:



@MaayanAimelak

In the **Permissions** tab, click on + next to **lab_policy**:

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

AWS Organizations

ARN
arn:aws:iam::439499134388:user/awsstudent

Console access
Disabled

Created
October 30, 2024, 13:02 (UTC+02:00)

Last console sign-in
-

Access key 1
AKIAWMVBQSW2H355CHNV - Active
Never used. Created today.

Access key 2
AKIAWMVBQSW2MIOJ2GPD - Active
Never used. Created today.

Permissions

Groups (1)

Tags (1)

Security credentials

Last Accessed

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

Policy name	Type	Attached via
lab_policy	Customer managed	Directly
ReadOnlyAccess	AWS managed - ...	Group QLReadOnly

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

AWS Organizations

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

Policy name	Type	Attached via
lab_policy	Customer managed	Directly
ReadOnlyAccess	AWS managed - ...	Group QLReadOnly

Permissions boundary (not set)

Generate policy based on CloudTrail events

lab_policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "cloudformation:List*",
7         "cloudformation:Describe*",
8         "cloudformation:Detect*",
9         "cloudformation:EstimateTemplateCost",
10        "cloudformation:Get*",
11        "cloudwatch:*",
12        "ec2:*Address*",
13        "ec2:*Associate*",
14        "ec2:AttachVolume",
15        "ec2:BundleInstance",
16        "ec2:Cancel*",
17        "ec2:Capacity*",
18        "ec2:CreateInstanceExportTask",
19        "ec2:CreateFlowLogs",
20        "ec2:*Credit*"
21      ]
22    }
23  ]
24 }
```

This lab_policy document is formatted in JSON. The IAM policy grants the awsstudent user access to specific AWS services in this account.

Choose the **Security credentials** tab, in the **Access Keys** section, locate the **awsstudent** user's access key ID:

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

AKN

arn:aws:iam::439499134388:user/awsstudent

Access key 1

AKIAWMVBQSW2H355CHNV - Active

Never used. Created today.

Last console sign-in

-

Console access

Disabled

Created

October 30, 2024, 13:02 (UTC+02:00)

Access key 2

AKIAWMVBQSW2MIOJ2GPD - Active

Never used. Created today.

Permissions

Groups (1)

Tags (1)

Security credentials

Console sign-in

Enable console access

Console sign-in link

https://439499134388.signin.aws.amazon.com/console

Console password

Not enabled

Multi-factor authentication (MFA) (0)

Remove

Resync

Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type

Identifier

Certifications

Scroll down

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

Access keys (2)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

AKIAWMVBQSW2H355CHNV

Actions

Description

-

Status

Active

Last used

None

Created

31 minutes ago

Last used region

N/A

Last used service

N/A

AKIAWMVBQSW2MIOJ2GPD

Actions

Description

-

Status

Active

Last used

None

Created

31 minutes ago

Last used region

N/A

Last used service

N/A

SSH public keys for AWS CodeCommit (0)

Actions

Upload SSH public key

awsstudent user's access key ID

Note: Once the access key is created, you must save the secret access key locally at the time that the key is created. For this lab, you can find the access key ID and the secret access key in the **Details** dropdown list at the top of these instructions.

@MaayunAimelak