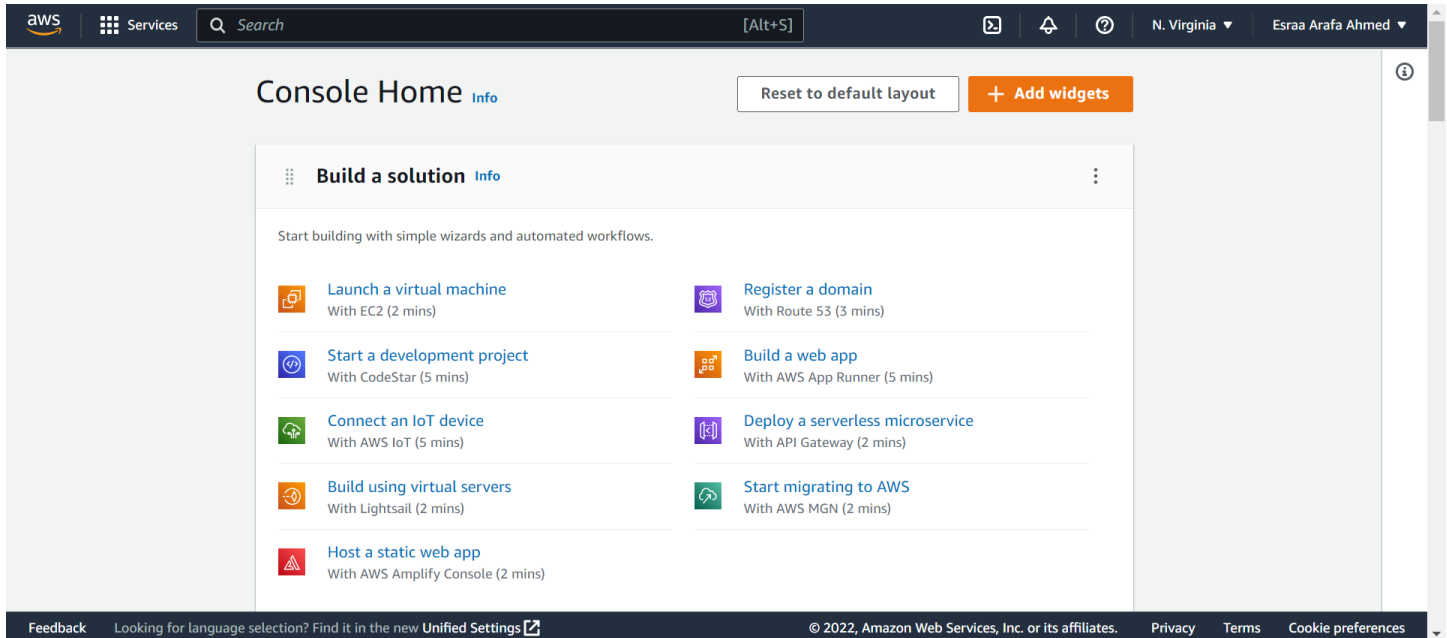


Lab1

1-

- **Create AWS account**

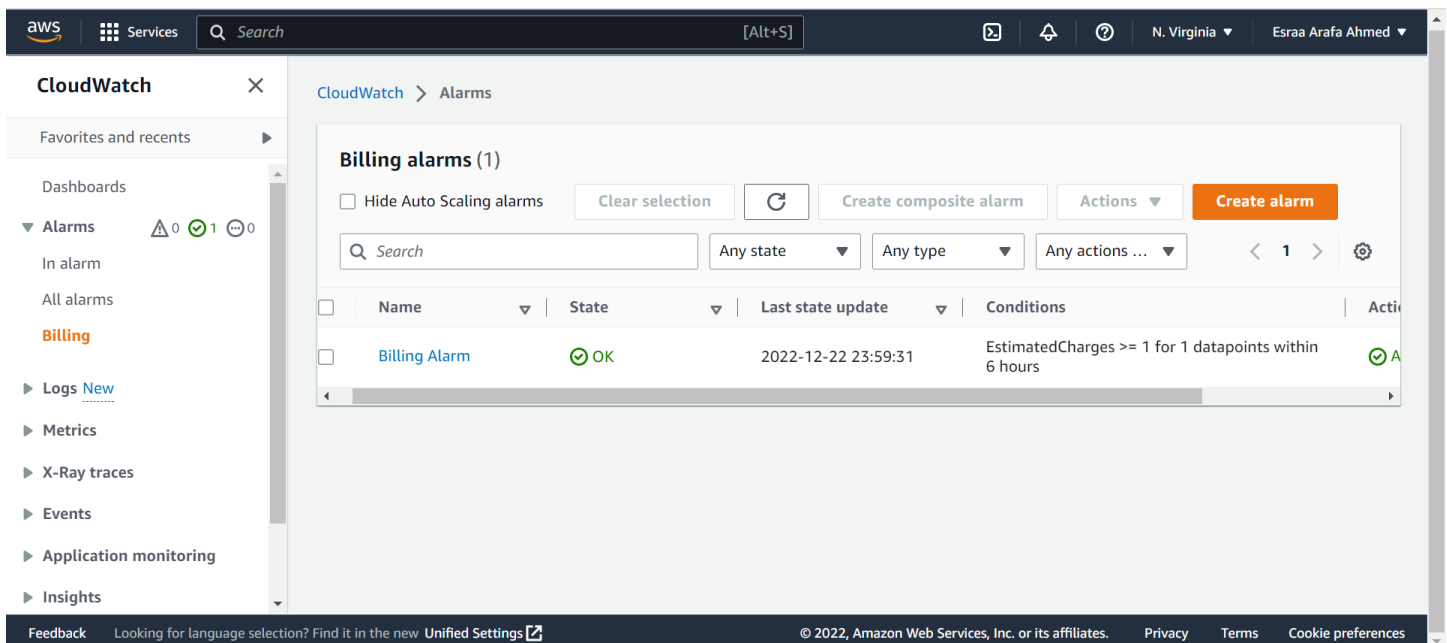


The screenshot shows the AWS Console Home page. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and user information (N. Virginia, Esraa Arafa Ahmed). Below the navigation bar, the 'Console Home' section is visible, featuring a 'Reset to default layout' button and an 'Add widgets' button. The main content area is titled 'Build a solution' and lists several quickstart options:

- Launch a virtual machine (With EC2 (2 mins))
- Register a domain (With Route 53 (3 mins))
- Start a development project (With CodeStar (5 mins))
- Build a web app (With AWS App Runner (5 mins))
- Connect an IoT device (With AWS IoT (5 mins))
- Deploy a serverless microservice (With API Gateway (2 mins))
- Build using virtual servers (With Lightsail (2 mins))
- Start migrating to AWS (With AWS MGN (2 mins))
- Host a static web app (With AWS Amplify Console (2 mins))

At the bottom, there's a footer with 'Feedback', a language selection prompt, copyright information (© 2022, Amazon Web Services, Inc. or its affiliates.), and links for 'Privacy', 'Terms', and 'Cookie preferences'.

- **and set billing alarm**



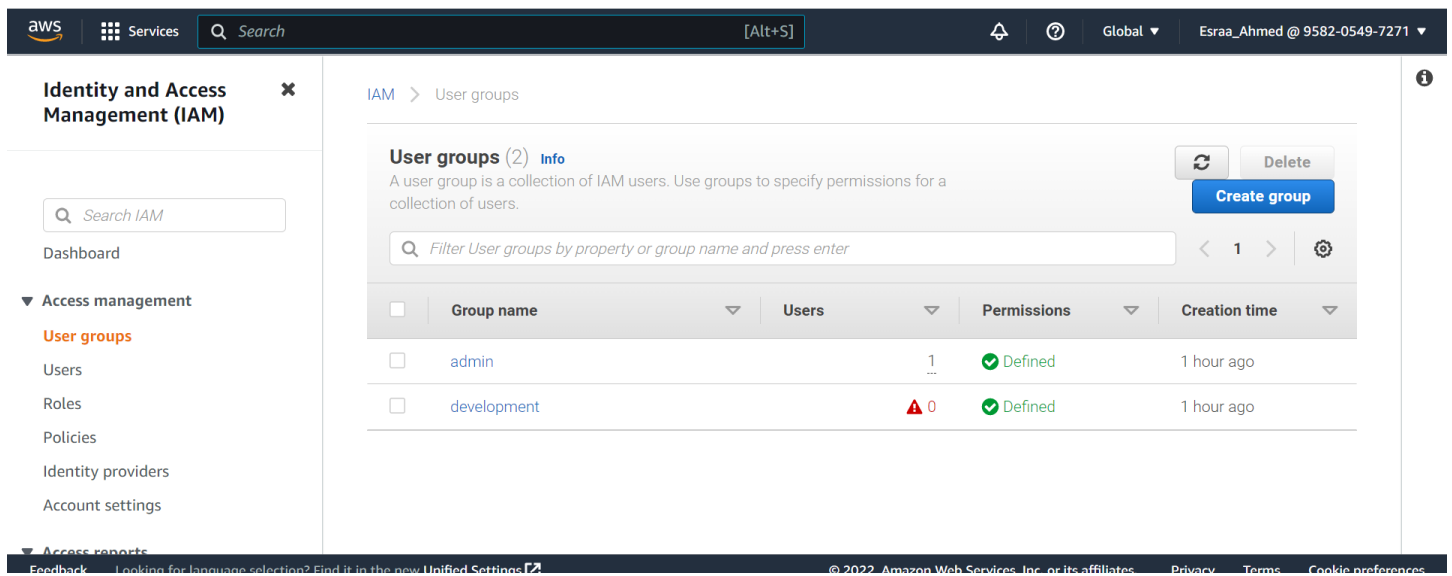
The screenshot shows the AWS CloudWatch Alarms page. The left sidebar contains a navigation menu with 'CloudWatch' at the top, followed by 'Favorites and recents', 'Dashboards', and a list of services including 'Alarms', 'Logs', 'Metrics', 'X-Ray traces', 'Events', 'Application monitoring', and 'Insights'. The main content area is titled 'CloudWatch > Alarms' and displays a 'Billing alarms (1)' section. This section includes a 'Hide Auto Scaling alarms' checkbox, a 'Clear selection' button, a 'Create composite alarm' button, and an 'Actions' dropdown menu. A 'Create alarm' button is also present. Below these controls is a table with one alarm listed:

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	Billing Alarm	OK	2022-12-22 23:59:31	EstimatedCharges >= 1 for 1 datapoints within 6 hours	

At the bottom, there's a footer with 'Feedback', a language selection prompt, copyright information (© 2022, Amazon Web Services, Inc. or its affiliates.), and links for 'Privacy', 'Terms', and 'Cookie preferences'.

2-

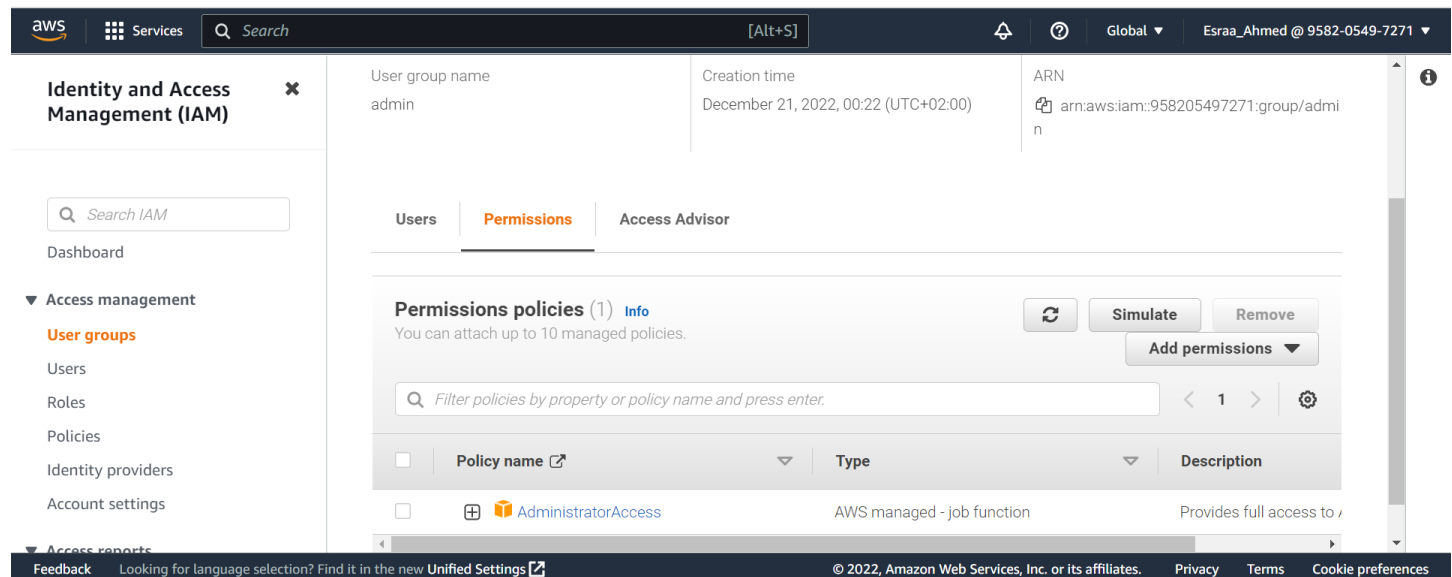
- create 2 groups one admin and one for development



The screenshot shows the AWS IAM console's 'User groups' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, and Account settings. The main content area shows a list of user groups. The 'admin' group has 1 user and 'Defined' permissions, while the 'development' group has 0 users and 'Defined' permissions. A 'Create group' button is located in the top right corner.

Group name	Users	Permissions	Creation time
admin	1	Defined	1 hour ago
development	0	Defined	1 hour ago

- in the admin group it has admin permission



The screenshot shows the AWS IAM console's 'Permissions policies' page for the 'admin' user group. The left sidebar is the same as the previous screenshot. The main content area shows the 'Permissions policies' section for the 'admin' group. It lists one policy named 'AdministratorAccess' with the description 'Provides full access to /'. The 'Add permissions' button is located in the top right corner.

Policy name	Type	Description
AdministratorAccess	AWS managed - job function	Provides full access to /

- and in the development only access to s3

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, and Account settings. The main content area is titled 'Permissions' and shows 'Permissions policies (1)'. A table lists the policy 'AmazonS3FullAccess' as 'AWS managed' with the description 'Provides full access to all bu'. The top navigation bar includes the AWS logo, Services, a search bar, and the user profile 'Esraa_Ahmed @ 9582-0549-7271'.

- create admin-1 user console access and MFA enabled

The screenshot shows the AWS IAM console interface for the 'admin-1' user. The left sidebar is the same as the previous screenshot. The main content area is titled 'Summary' and shows the user's details: 'User ARN: arn:aws:iam:958205497271:user/admin-1', 'Path: /', and 'Creation time: 2022-12-21 01:42 UTC+0200'. The 'Security credentials' tab is selected, showing 'Sign-in credentials'. The 'Summary' section lists the console sign-in link and MFA requirements. The 'Console password' is 'Enabled (never signed in)' and the 'Assigned MFA device' is 'arn:aws:iam:958205497271:mfa/admin-1 (Virtual TOTP)'. The 'Signing certificates' section shows 'None'. The top navigation bar is the same as the previous screenshot.

- and admin2-prog with cli access only

aws

Services

Search

[Alt+S]

Global

Esraa_Ahmed @ 9582-0549-7271

Identity and Access Management (IAM)

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Users > dmin2-prog

Summary

Delete user

User ARN

arn:aws:iam::958205497271:user/dmin2-prog

Path

/

Creation time

2022-12-21 02:03 UTC+0200

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Sign-in credentials

Summary

User does not have console management access

Console password

Disabled | Manage

Assigned MFA device

Not assigned | Manage

Signing certificates

None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, 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.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status
AKIA56GL7R63TGROMJWR	2022-12-21 02:03 UTC+0200	N/A	Active Make inactive X

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

Global

Esraa_Ahmed @ 9582-0549-7271

Identity and Access Management (IAM)

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Sign-in credentials

Summary

User does not have console management access

Console password

Disabled | Manage

Assigned MFA device

Not assigned | Manage

Signing certificates

None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, 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.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status
AKIA56GL7R63TGROMJWR	2022-12-21 02:03 UTC+0200	N/A	Active Make inactive X

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

- and list all users and groups using it commands not console

```

esraa@10:~
File Edit View Search Terminal Help
[admin2-prog]
aws_access_key_id = AKIA56GL7R63TGROMJWR
aws_secret_access_key = mdpHiV0kPJSfTbueKi6V6k7SvWPDVbUPz1G7m+F

esraa@10:~
File Edit View Search Terminal Help
[admin2-prog]
region = eu-central-1
output = json

esraa@10:~$ aws iam list-groups --profile admin2-prog
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "admin",
      "GroupId": "AGPA56GL7R633GXLFFOK0",
      "Arn": "arn:aws:iam::958205497271:group/admin",
      "CreateDate": "2022-12-20T22:22:41+00:00"
    },
    {
      "Path": "/",
      "GroupName": "development",
      "GroupId": "AGPA56GL7R633UUXJ376JE",
      "Arn": "arn:aws:iam::958205497271:group/development",
      "CreateDate": "2022-12-20T22:48:17+00:00"
    }
  ]
}

esraa@10:~$ aws iam list-users --profile admin2-prog
{
  "Users": [
    {
      "Path": "/",
      "UserName": "admin-1",
      "UserId": "AIDA56GL7R635IX0ZAUM3",
      "Arn": "arn:aws:iam::958205497271:user/admin-1",
      "CreateDate": "2022-12-20T23:42:56+00:00"
    },
    {
      "Path": "/",
      "UserName": "dev-user",
      "UserId": "AIDA56GL7R634MX2PMN7G",
      "Arn": "arn:aws:iam::958205497271:user/dev-user",
      "CreateDate": "2022-12-21T01:41:24+00:00",
      "PasswordLastUsed": "2022-12-21T01:56:09+00:00"
    },
    {
      "Path": "/",
      "UserName": "dmin2-prog",
      "UserId": "AIDA56GL7R633KINJ4DVK",
      "Arn": "arn:aws:iam::958205497271:user/dmin2-prog",
      "CreateDate": "2022-12-21T00:03:13+00:00"
    },
    {
      "Path": "/",
      "UserName": "Esraa_Ahmed",
      "UserId": "AIDA56GL7R635RXLH5PVR",
      "Arn": "arn:aws:iam::958205497271:user/Esraa_Ahmed",
      "CreateDate": "2022-12-20T21:13:07+00:00",
      "PasswordLastUsed": "2022-12-22T16:12:43+00:00"
    }
  ]
}
(END)

```

- in the development group create user with name dev-user with programmatic and Admin access

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, and Archive rules. The main content area displays the details for a user named 'dev-user' with the ARN 'arn:aws:iam::958205497271:user/dev-user'. The user was created on 2022-12-21 03:41 UTC+0200. The 'Permissions' tab is selected, showing that two policies are applied: 'AdministratorAccess' (AWS managed policy) and 'AmazonS3FullAccess' (AWS managed policy from group 'development').

- try to access aws using it (take a screenshot from accessing ec2 and s3 console)

- ec2

The screenshot shows the AWS Management Console interface for the 'dev-user' in the 'N. Virginia' region. The 'EC2 Dashboard' is active, displaying a 'Resources' section with a table of EC2 resources in the US East (N. Virginia) Region. The table lists various resources and their counts: Instances (running) (0), Elastic IPs (0), Key pairs (0), Placement groups (0), Snapshots (0), Dedicated Hosts (0), Instances (0), Load balancers (0), Security groups (1), and Volumes (0). A notification banner at the bottom of the Resources section states: 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more'. The right sidebar shows 'Account attributes' including 'Supported platforms' (VPC), 'Default VPC' (vpc-0fa75e3ffcfc4e719), 'Settings' (EBS encryption, Zones, EC2 Serial Console, Default credit specification, Console experiments), and 'Explore AWS'.

- s3

Amazon S3

Replicate data within and between AWS Regions using Amazon S3 Replication.

View tutorial

Amazon S3 > Buckets

Account snapshot

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

View Storage Lens dashboard

Buckets (1) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

	Na...	AWS Region	Access	Creation date
<input type="radio"/>	sprents	EU (Stockholm) eu-north-1	Bucket and objects not public	December 22, 2022, 21:28:48 (UTC+02:00)

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Also access cli using it and try to get all users and groups using it

```
esraa@10:~  
[dev-user]  
aws_access_key_id = AKIA56GL7R633WLM3K4M  
aws_secret_access_key = zzzCo5MxoEfZONSi/rgD7B+Ia0AlUp7gH5Z6lJx  
6.40 Bot
```

```
esraa@10:~  
[esraa@10 ~]$ aws iam list-groups --profile dev-user  
{  
  "Groups": [  
    {  
      "Path": "/",  
      "GroupName": "admin",  
      "GroupId": "AGPA56GL7R633GXLFFOKO",  
      "Arn": "arn:aws:iam::958205497271:group/admin",  
      "CreateDate": "2022-12-20T22:22:41+00:00"  
    },  
    {  
      "Path": "/",  
      "GroupName": "development",  
      "GroupId": "AGPA56GL7R63UUXJ376JE",  
      "Arn": "arn:aws:iam::958205497271:group/development",  
      "CreateDate": "2022-12-20T22:48:17+00:00"  
    }  
  ]  
}
```

