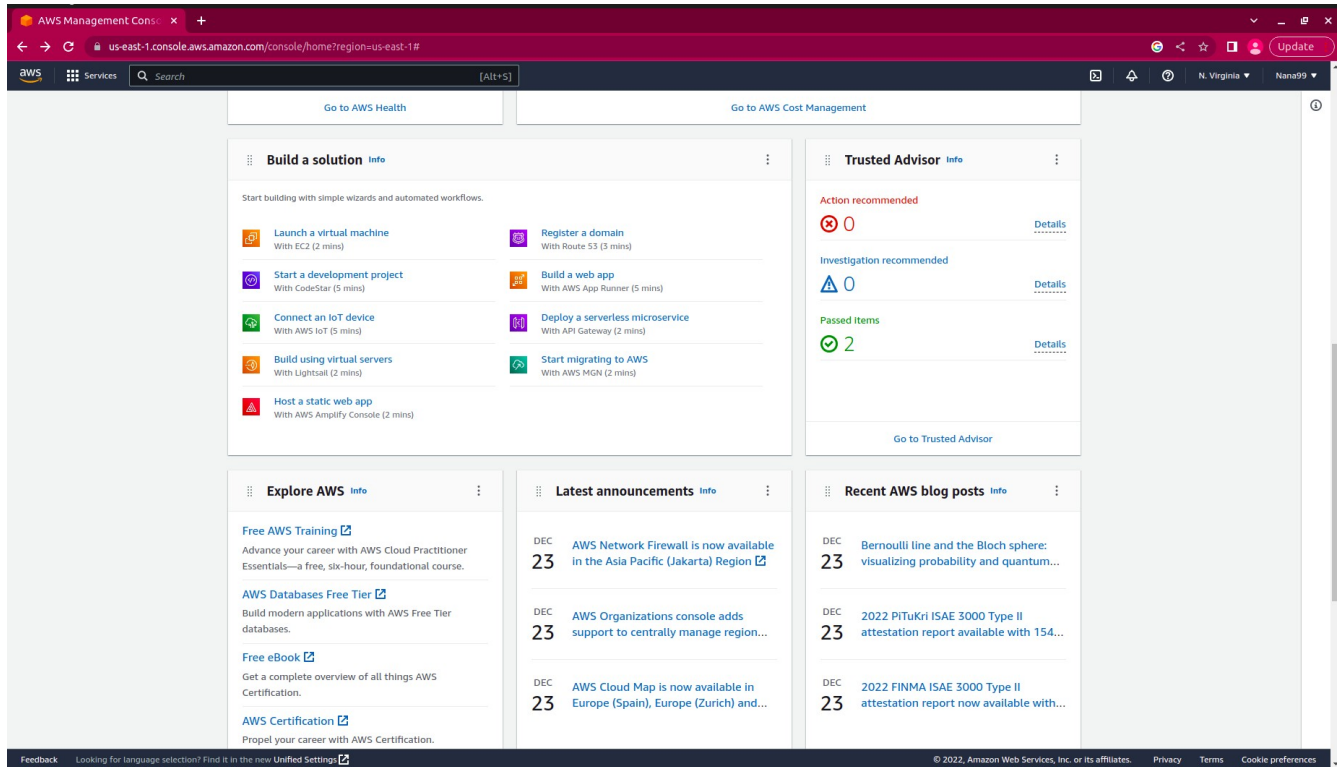
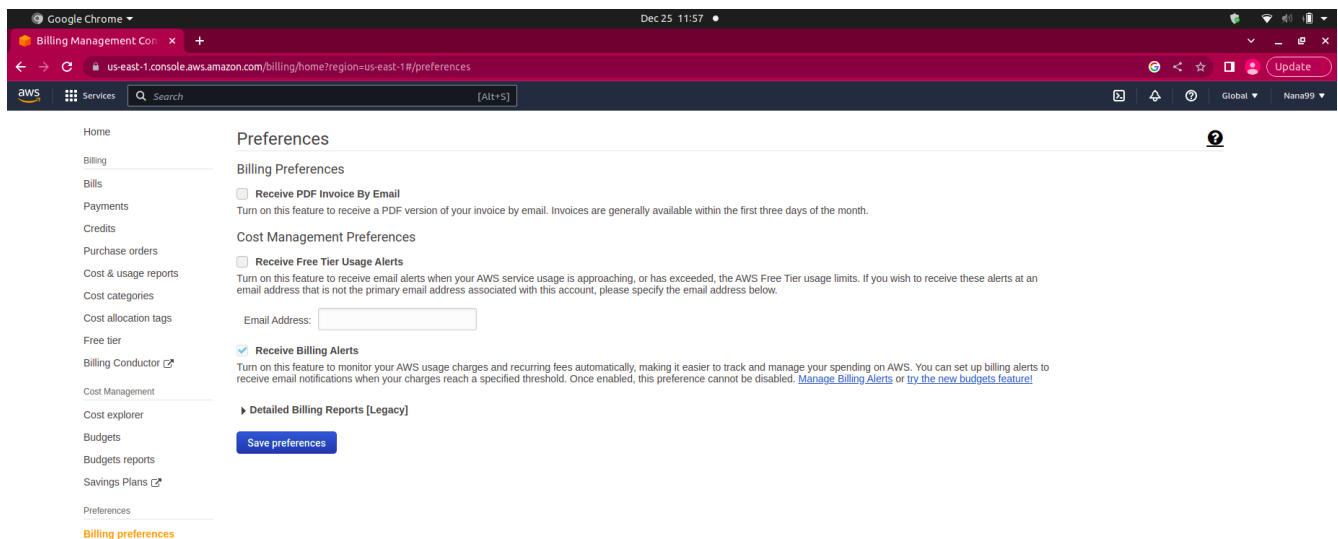


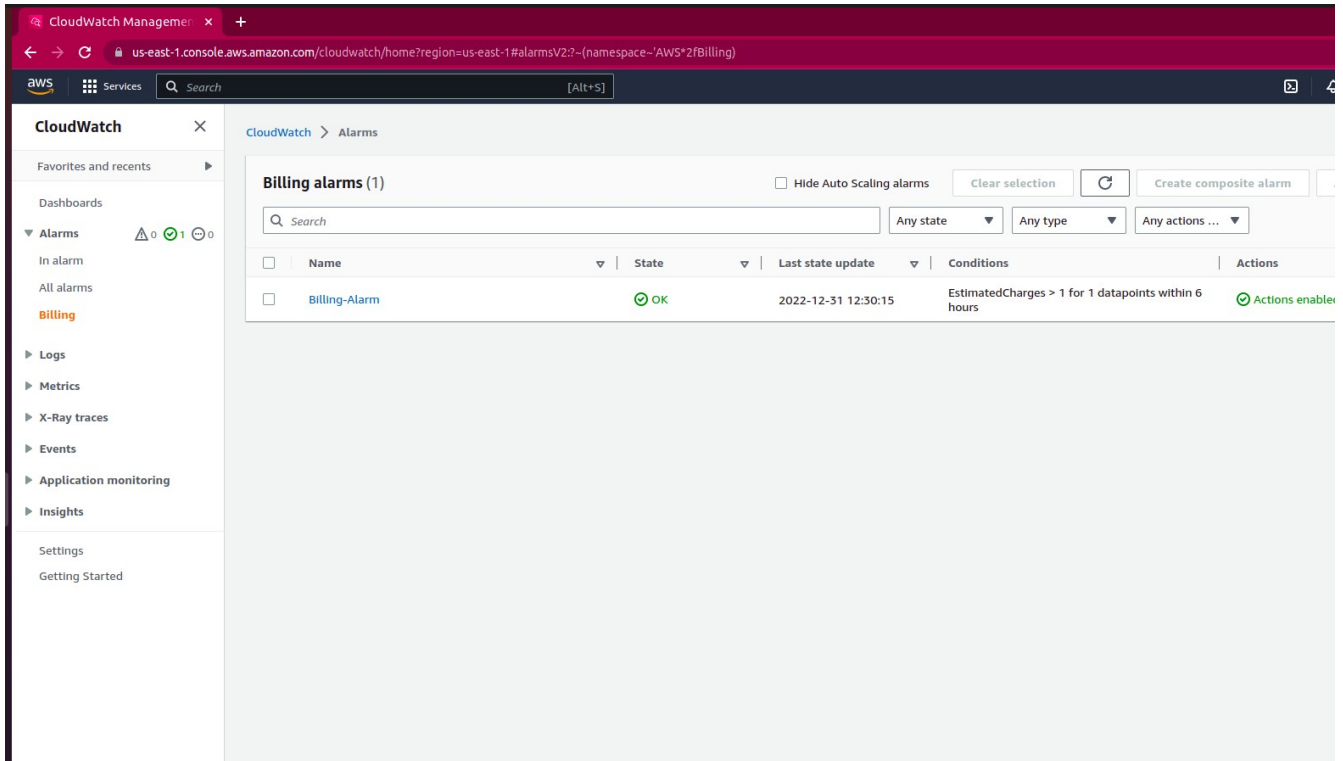
LAB 1 – AWS

1- Create AWS account:

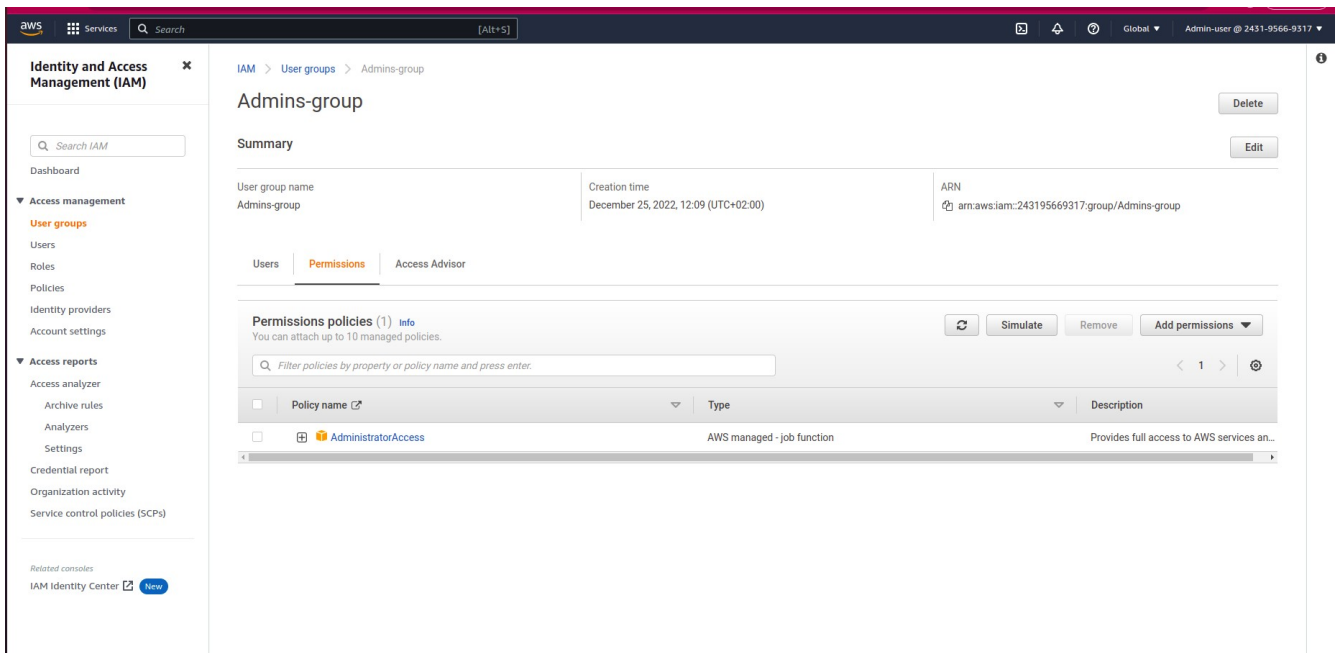


2- Set billing alarm:





3- Create 2 groups one admin and one for development:



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)

Related consoles

IAM Identity Center [New](#)

IAM > User groups > Development-Group

Development-Group

Delete

Edit

Summary

User group name: Development-Group

Creation time: December 31, 2022, 12:59 (UTC+02:00)

ARN: arn:aws:iam:243195669317:group/Development-Group

Users | **Permissions** | Access Advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

Filter policies by property or policy name and press enter.

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS ...

4- Create admin-1 user console access and mfa enabled:

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)

Related consoles

IAM Identity Center [New](#)

Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

IAM > Users

Users (2) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Refresh](#) [Delete](#) [Add users](#)

Find users by username or access key

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin-1console	Admins-group	3 minutes ago	Virtual	2 minutes ago	-
<input type="checkbox"/>	Admin-user	Admins-group	32 minutes ago	Virtual	5 days ago	5 days ago

Identity and Access Management (IAM)

Users > admin-1-console

Summary

User ARN: `arn:aws:iam::243195669317:user/admin-1-console`
 Path: `/`
 Creation time: 2022-12-31 13:13 UTC+0200

Permissions **Groups (1)** **Tags (1)** **Security credentials** **Access Advisor**

Sign-in credentials

Summary

- Console sign-in link: <https://243195669317.signin.aws.amazon.com/console>
- MFA is required when signing in. [Learn more](#)

Console password: Enabled (last signed in Today) | [Manage](#)

Signing certificates: None

Multi-factor authentication (MFA)

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

[Manage](#) [Assign MFA device](#)

Serial number	Device type	Created
<input type="radio"/> <code>arn:aws:iam::243195669317:mfa/Admin1-console-MFA</code>	Virtual TOTP	2022-12-31 13:18 UTC+0200

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](#)

5- Create admin2-prog with cli access and list all users and groups using commands:

Identity and Access Management (IAM)

Introducing the new Users list experience
 We've redesigned the Users list experience to make it easier to use. [Let us know what you think](#)

IAM > Users

Users (3) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin-1-console	Admins-group	14 minutes ago	Virtual	28 minutes ago	-
<input type="checkbox"/>	Admin-user	Admins-group	Now	Virtual	5 days ago	5 days ago
<input type="checkbox"/>	Admin2-prog	Admins-group	Never	None	None	9 minutes ago

[Add users](#)

[IAM Identity Center](#) [New](#)

Services

Search

[Alt+S]

Global

Admin-user @ 2431-9566-9317

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 243195669317

New feature to generate a policy based on CloudTrail events.

AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > Admin2-prog

Summary

Delete user

User ARNarn:aws:iam:243195669317:user/Admin2-prog

Path/

Creation time2022-12-31 13:35 UTC+0200

Permissions

Groups (1)

Tags (1)

Security credentials

Access Advisor

Sign-in credentials

Summary

User does not have console management access

Console password

Disabled

Manage

Signing certificates

None

Multi-factor authentication (MFA)

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

Manage

Assign MFA device

No MFA assigned.

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

```
Dec 31 15:55
nihal@nihal-Inspiron-5570: ~/aws$ aws iam list-users --profile=Admin2-prog
{
  "Users": [
    {
      "Path": "/",
      "UserName": "admin-1console",
      "UserId": "AIDATRH4XNMC7AMK7KGHZ",
      "Arn": "arn:aws:iam:243195669317:user/admin-1console",
      "CreateDate": "2022-12-31T11:13:06+00:00",
      "PasswordLastUsed": "2022-12-31T11:30:51+00:00"
    },
    {
      "Path": "/",
      "UserName": "Admin-user",
      "UserId": "AIDATRH4XNMC5GXCPCG7NO",
      "Arn": "arn:aws:iam:243195669317:user/Admin-user",
      "CreateDate": "2022-12-25T12:00:31+00:00",
      "PasswordLastUsed": "2022-12-31T11:44:29+00:00"
    },
    {
      "Path": "/",
      "UserName": "Admin2-prog",
      "UserId": "AIDATRH4XNMCUL26XKT6A",
      "Arn": "arn:aws:iam:243195669317:user/Admin2-prog",
      "CreateDate": "2022-12-31T11:35:45+00:00"
    }
  ],
  "...skipping..."
}
}
```

```
nihal@nihal-Inspiron-5570:~/.aws$ aws iam list-groups --profile=Admin2-prog
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "Admins-group",
      "GroupId": "AGPATRH4XNNCSVF6FFENB",
      "Arn": "arn:aws:iam::243195669317:group/Admins-group",
      "CreateDate": "2022-12-25T10:09:47+00:00"
    },
    {
      "Path": "/",
      "GroupName": "Development-Group",
      "GroupId": "AGPATRH4XNNCXCFDETYMX",
      "Arn": "arn:aws:iam::243195669317:group/Development-Group",
      "CreateDate": "2022-12-31T10:59:30+00:00"
    }
  ]
}
nihal@nihal-Inspiron-5570:~/.aws$
```

6- Create user dev-user with programmatic and admin access in the development group and try to access ec2 and s3 console:

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Users > dev-user' and shows a 'Summary' tab. The summary displays the User ARN as 'arn:aws:iam::243195669317:user/dev-user', Path as '/', and Creation time as '2022-12-31 16:22 UTC+0200'. Below this, there are tabs for 'Permissions', 'Groups (1)', 'Tags (1)', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Permissions policies (2 policies applied)'. It lists two policies: 'AdministratorAccess' (AWS managed policy) and 'AmazonS3FullAccess' (AWS managed policy from group Development-Group). There is also a section for 'Permissions boundary (set)' with a 'Change boundary' button. At the bottom, there is a section for 'Generate policy based on CloudTrail events' with a 'Generate policy' button.

aws

Services

Search

[Alt+S]

N. Virginia

dev-user @ 2431-9566-9317

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Resources

EC2 Global view

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)0

Dedicated Hosts0

Elastic IPs0

Instances0

Key pairs0

Load balancers0

Placement groups0

Security groups1

Snapshots0

Volumes0

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

Scheduled events

US East (N. Virginia)

No scheduled events

Migrate a server

Service health

AWS Health Dashboard

Region: US East (N. Virginia)

Status: ✔ This service is operating normally

Zones

Zone name	Zone ID
us-east-1a	use1-az4
us-east-1b	use1-az6
us-east-1c	use1-az1
us-east-1d	use1-az2
us-east-1e	use1-az3

Account attributes

Supported platforms

VPC

Default VPC

vpc-0cb16b37998d93279

Settings

EBS encryption

Zones

EC2 Serial Console

Default credit specification

Console experiments

Explore AWS

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. [Learn more](#)

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. [Learn more](#)

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. [Learn more](#)

Additional information

[Getting started guide](#)

aws

Services

Search

[Alt+S]

Global

dev-user @ 2431-9566-9317

Amazon S3

Buckets

Account snapshot

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

View Storage Lens dashboard

Buckets (1)

Info

Find buckets by name

Copy ARN

Empty

Delete

Create bucket

Name	AWS Region	Access	Creation date
nihal-bucket1	US East (N. Virginia) us-east-1	Bucket and objects not public	December 31, 2022, 16:32:06 (UTC+02:00)

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

7- Access cli and get all users and groups using it:

```
nihal@nihal-Inspiron-5570: ~/aws
nihal@nihal-Inspiron-5570:~/aws$ aws iam list-groups --profile=dev-user
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "Admins-group",
      "GroupId": "AGPATRH4XNNC5VF6FFENB",
      "Arn": "arn:aws:iam::243195669317:group/Admins-group",
      "CreateDate": "2022-12-25T10:09:47+00:00"
    },
    {
      "Path": "/",
      "GroupName": "Development-Group",
      "GroupId": "AGPATRH4XNNCXCDFETVMX",
      "Arn": "arn:aws:iam::243195669317:group/Development-Group",
      "CreateDate": "2022-12-31T10:59:30+00:00"
    }
  ]
}
nihal@nihal-Inspiron-5570:~/aws$
```

```
nihal@nihal-Inspiron-5570: ~/aws
nihal@nihal-Inspiron-5570:~/aws$ aws iam list-users --profile=dev-user
{
  "Users": [
    {
      "Path": "/",
      "UserName": "admin-1console",
      "UserId": "AIDATRH4XNNC7AMK7KGHZ",
      "Arn": "arn:aws:iam::243195669317:user/admin-1console",
      "CreateDate": "2022-12-31T11:13:06+00:00",
      "PasswordLastUsed": "2022-12-31T11:30:51+00:00"
    },
    {
      "Path": "/",
      "UserName": "Admin-user",
      "UserId": "AIDATRH4XNNCSGXCPG7NO",
      "Arn": "arn:aws:iam::243195669317:user/Admin-user",
      "CreateDate": "2022-12-25T12:00:31+00:00",
      "PasswordLastUsed": "2022-12-31T14:16:13+00:00"
    },
    {
      "Path": "/",
      "UserName": "Admin2-prog",
      "UserId": "AIDATRH4XNNCULZ6XKT6A",
      "Arn": "arn:aws:iam::243195669317:user/Admin2-prog",
      "CreateDate": "2022-12-31T11:35:45+00:00"
    },
    {
      "Path": "/",
      "UserName": "dev-user",
      "UserId": "AIDATRH4XNNCQ5VE74M55",
      "Arn": "arn:aws:iam::243195669317:user/dev-user",
      "CreateDate": "2022-12-31T14:22:02+00:00",
      "PasswordLastUsed": "2022-12-31T14:26:31+00:00"
    }
  ]
}
nihal@nihal-Inspiron-5570:~/aws$
```