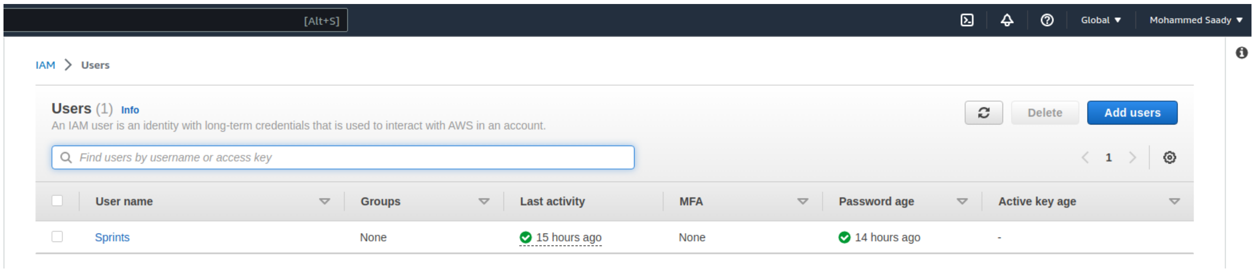
AWS_IAM Service

1-) Create aws account and set billing alarm

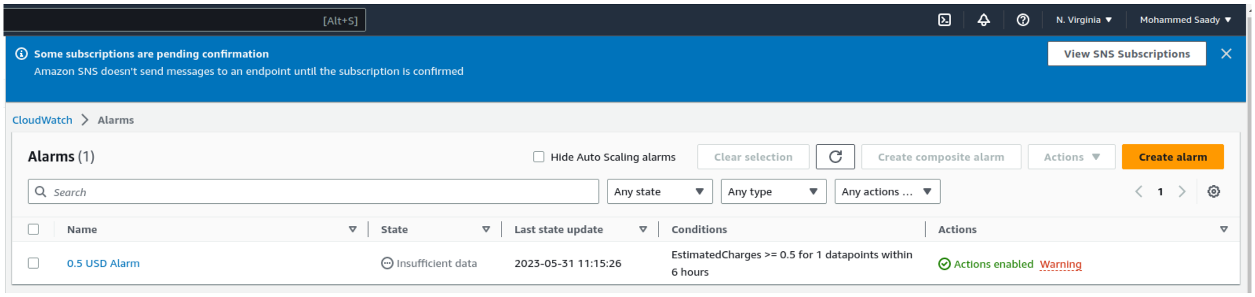


IAM > Users

Users (1) Info

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

□	User name	Groups	Last activity	MFA	Password age	Active key age
□	Sprints	None	✓ 15 hours ago	None	✓ 14 hours ago	-



Some subscriptions are pending confirmation

Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

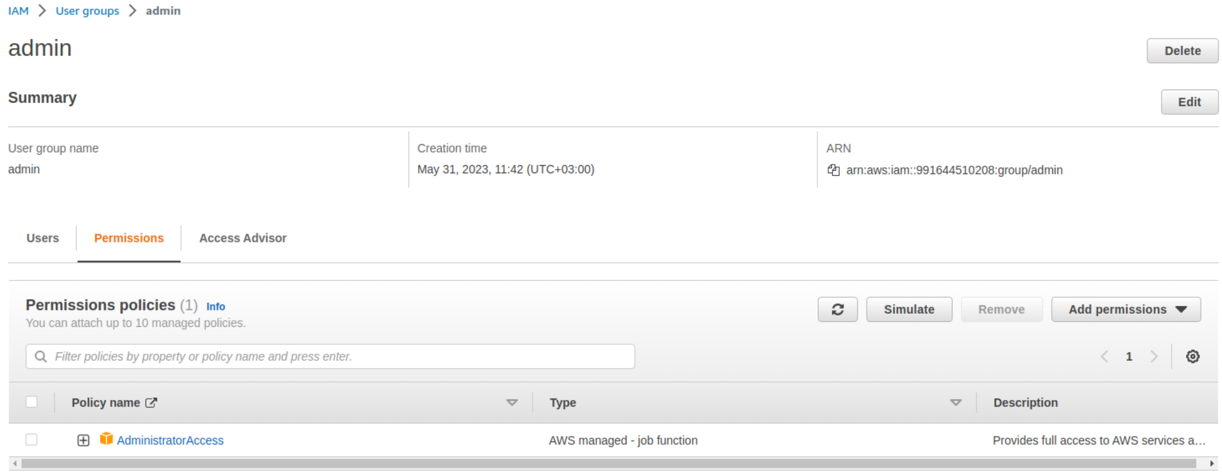
CloudWatch > Alarms

Alarms (1)

□	Name	State	Last state update	Conditions	Actions
□	0.5 USD Alarm	Insufficient data	2023-05-31 11:15:26	EstimatedCharges >= 0.5 for 1 datapoints within 6 hours	✓ Actions enabled Warning

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



IAM > User groups > admin

admin

Summary

User group name: admin

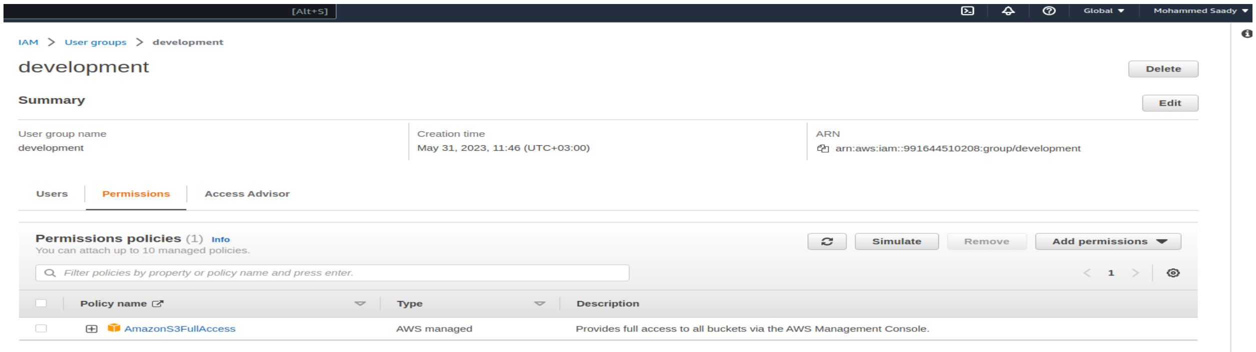
Creation time: May 31, 2023, 11:42 (UTC+03:00)

ARN: arn:aws:iam::991644510208:group/admin

Permissions policies (1) Info

You can attach up to 10 managed policies.

□	Policy name	Type	Description
□	⊞ AdministratorAccess	AWS managed - job function	Provides full access to AWS services a...



IAM > User groups > development

development

Summary

User group name: development

Creation time: May 31, 2023, 11:46 (UTC+03:00)

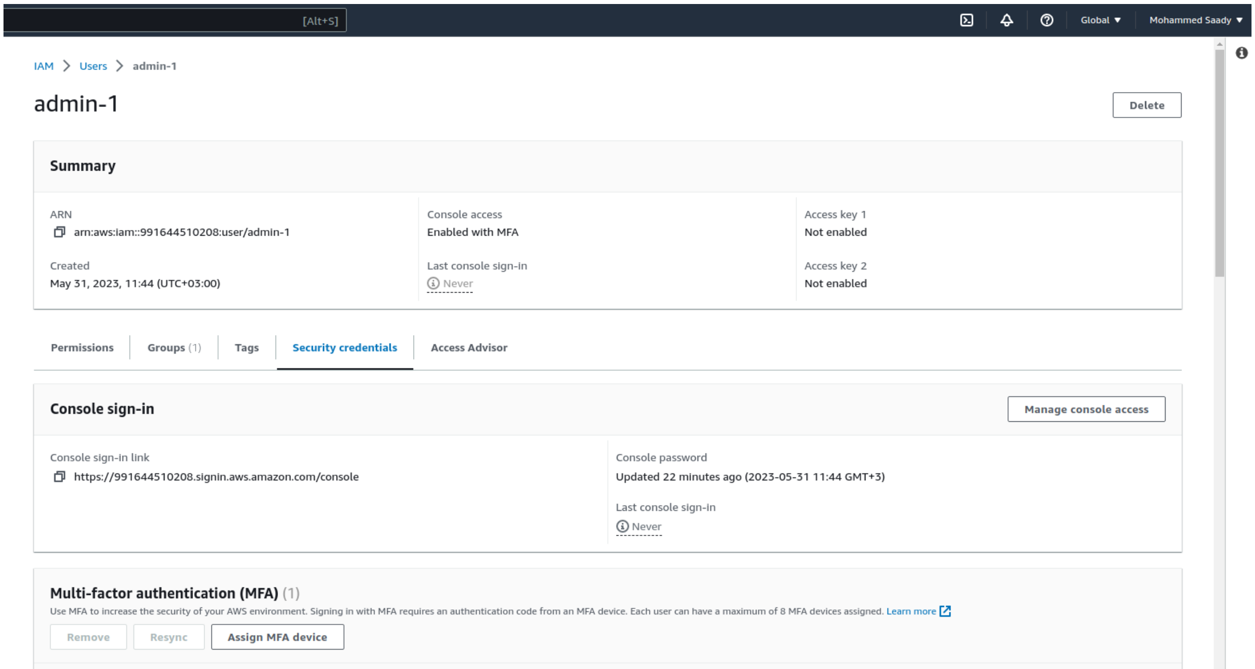
ARN: arn:aws:iam::991644510208:group/development

Permissions policies (1) Info

You can attach up to 10 managed policies.

□	Policy name	Type	Description
□	⊞ AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.

- Create admin-1 user console access and mfa enabled in admin group



admin-1

Summary

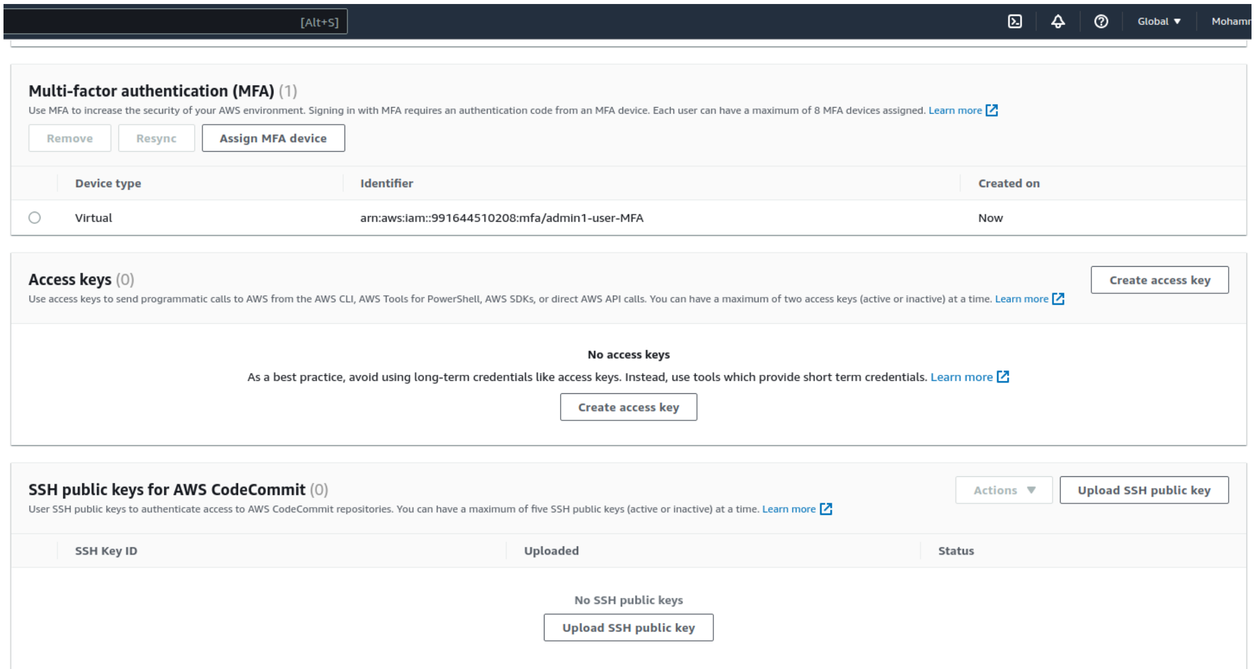
ARN arn:aws:iam::991644510208:user/admin-1	Console access Enabled with MFA	Access key 1 Not enabled
Created May 31, 2023, 11:44 (UTC+03:00)	Last console sign-in Never	Access key 2 Not enabled

Console sign-in

Console sign-in link https://991644510208.signin.aws.amazon.com/console	Console password Updated 22 minutes ago (2023-05-31 11:44 GMT+3) Last console sign-in Never

Multi-factor authentication (MFA) (1)

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



Multi-factor authentication (MFA) (1)

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

	Device type	Identifier	Created on
○	Virtual	arn:aws:iam::991644510208:mfa/admin1-user-MFA	Now

Access keys (0)

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

No access keys

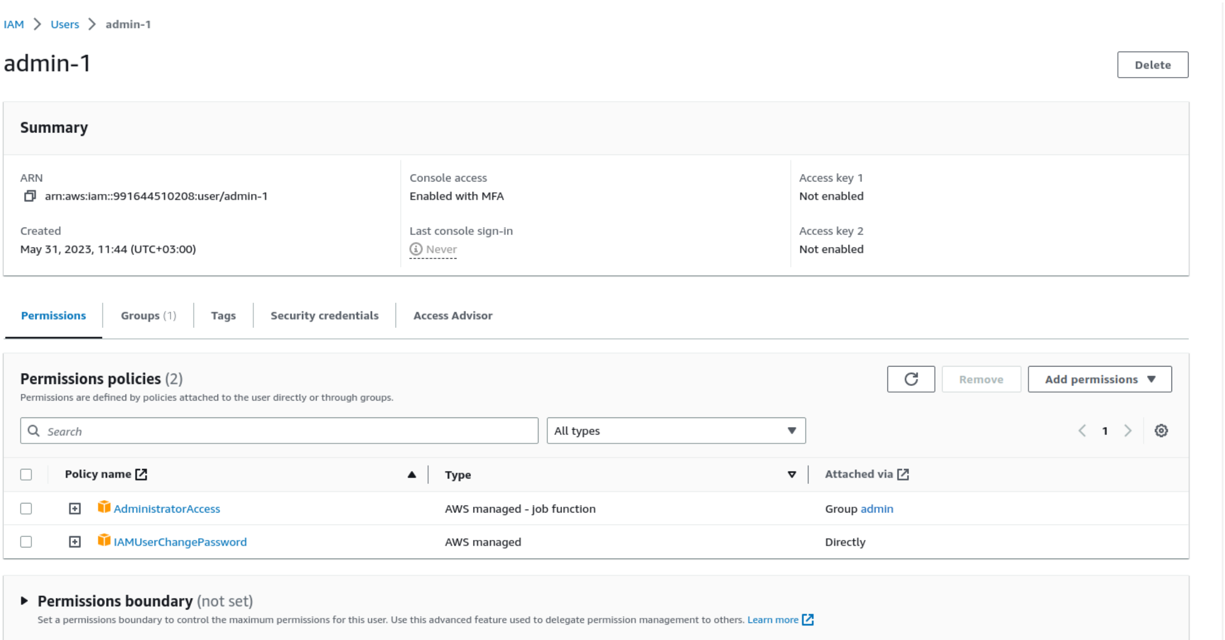
As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

SSH public keys for AWS CodeCommit (0)

User SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. Learn more

	SSH Key ID	Uploaded	Status

No SSH public keys



IAM > Users > admin-1

admin-1

Summary

ARN
arn:aws:iam::991644510208:user/admin-1

Created
May 31, 2023, 11:44 (UTC+03:00)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Not enabled

Access key 2
Not enabled

Permissions policies (2)

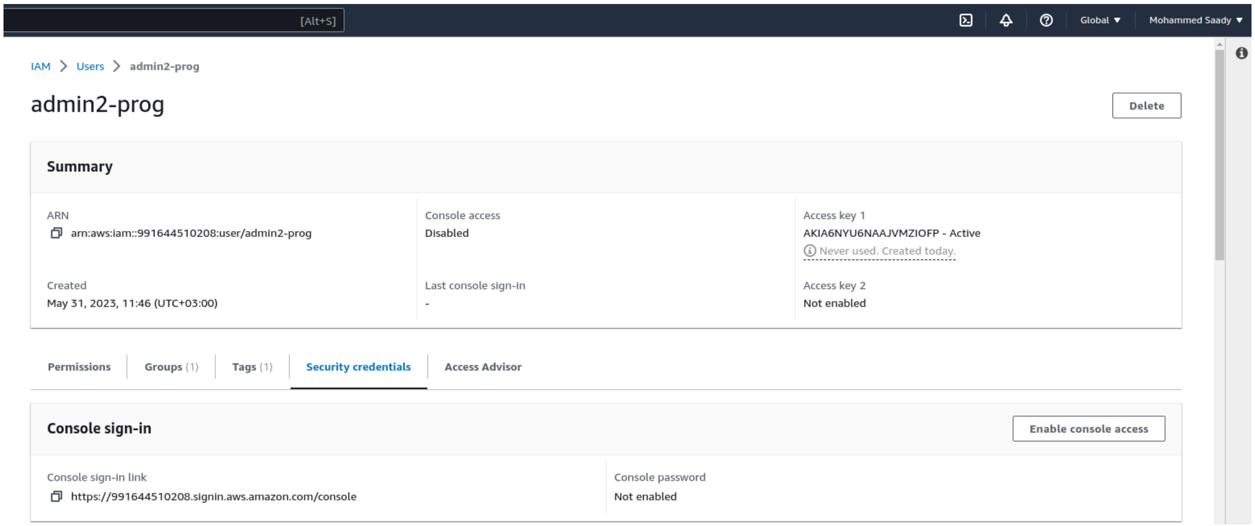
Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Group admin
□	IAMUserChangePassword	AWS managed	Directly

Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

- And admin-2-prog with cli access only and list all users and groups using commands not console



IAM > Users > admin2-prog

admin2-prog

Summary

ARN
arn:aws:iam::991644510208:user/admin2-prog

Created
May 31, 2023, 11:46 (UTC+03:00)

Console access
Disabled

Last console sign-in
-

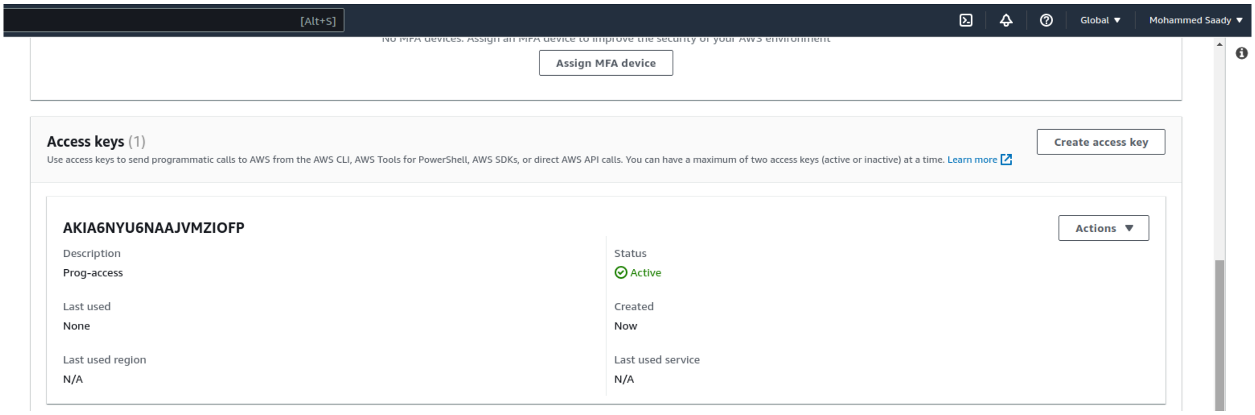
Access key 1
AKIA6NYU6NAAJVMZIOFP - Active
Never used. Created today.

Access key 2
Not enabled

Console sign-in

Console sign-in link
https://991644510208.signin.aws.amazon.com/console

Console password
Not enabled



No MFA devices. Assign an MFA device to improve the security of your AWS environment

Access keys (1)

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

AKIA6NYU6NAAJVMZIOFP

Description
Prog-access

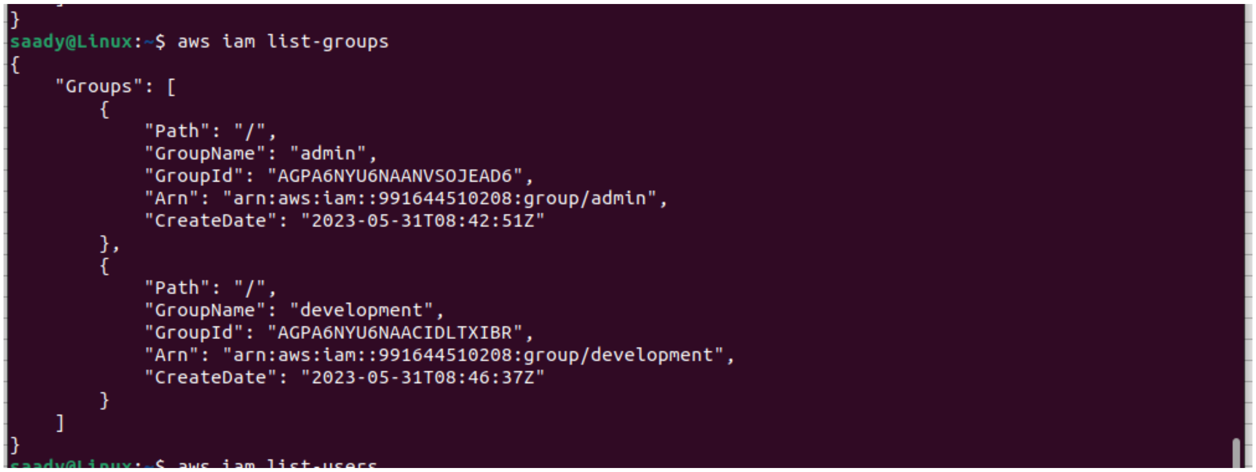
Status
Active

Last used
None

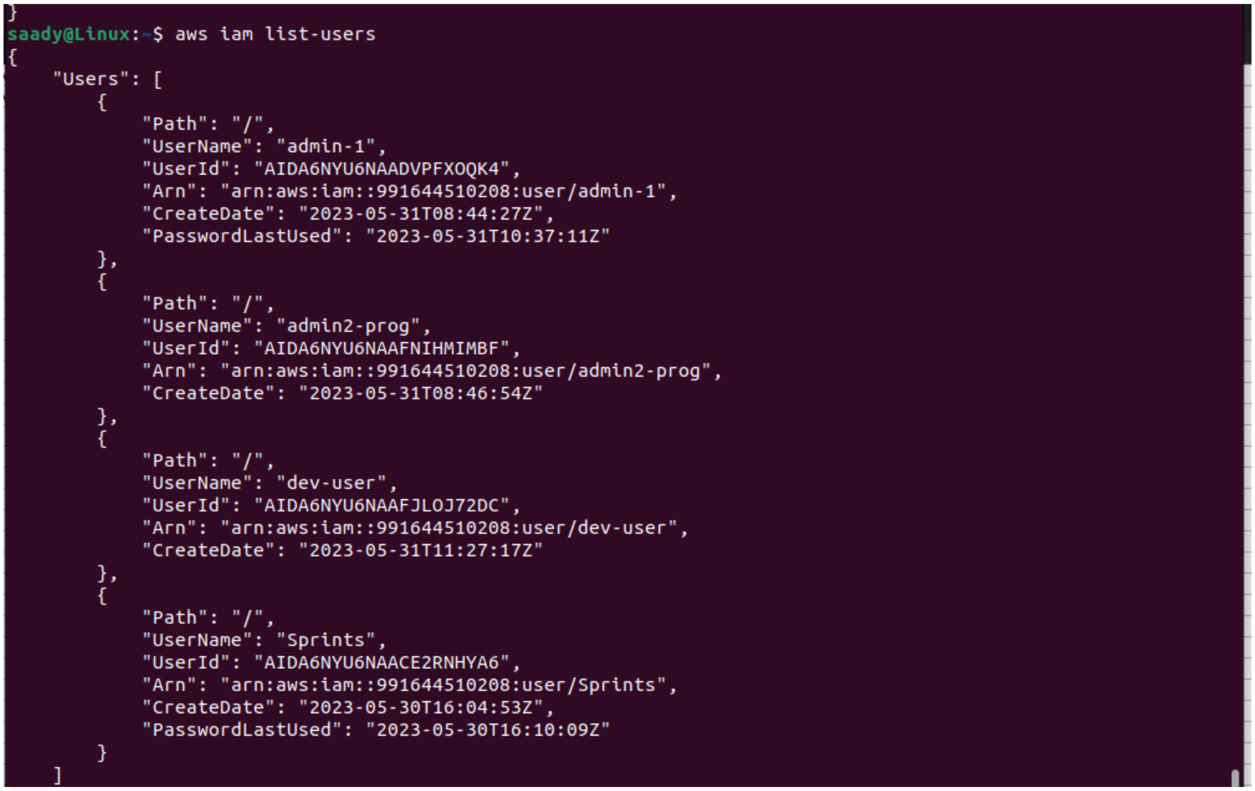
Created
Now

Last used region
N/A

Last used service
N/A

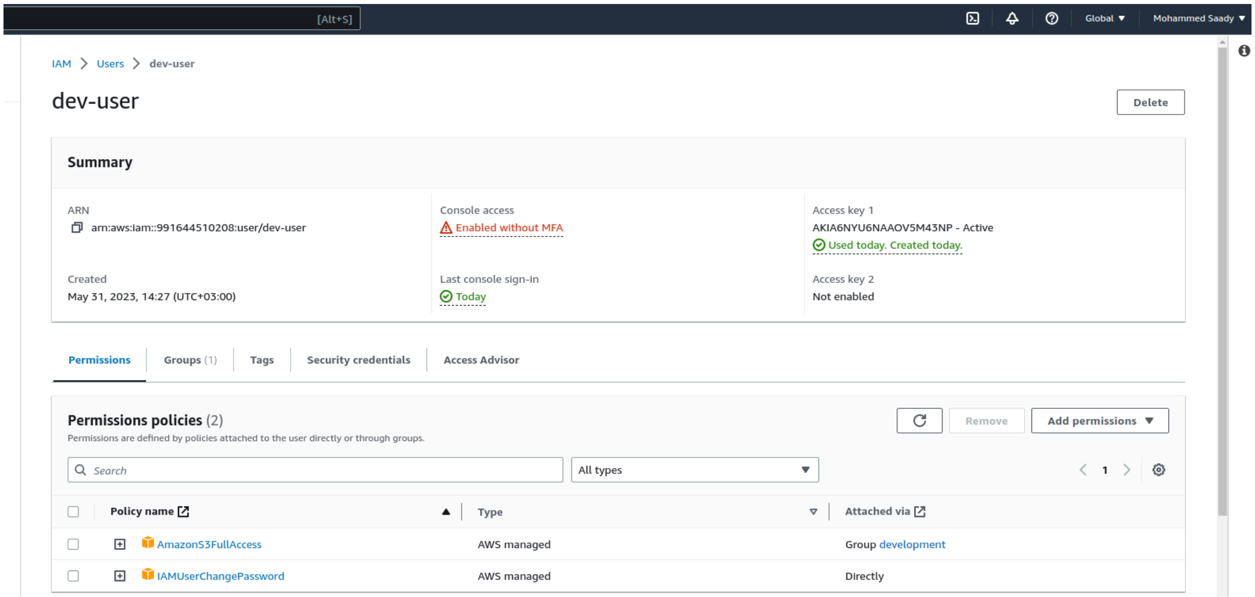


```
}
saady@Linux:~$ aws iam list-groups
{
    "Groups": [
        {
            "Path": "/",
            "GroupName": "admin",
            "GroupId": "AGPA6NYU6NAANVSOJEAD6",
            "Arn": "arn:aws:iam::991644510208:group/admin",
            "CreateDate": "2023-05-31T08:42:51Z"
        },
        {
            "Path": "/",
            "GroupName": "development",
            "GroupId": "AGPA6NYU6NAACIDLTXIBR",
            "Arn": "arn:aws:iam::991644510208:group/development",
            "CreateDate": "2023-05-31T08:46:37Z"
        }
    ]
}
saady@Linux:~$ aws iam list-users
```



```
}
saady@Linux:~$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "admin-1",
            "UserId": "AIDA6NYU6NAADVPFXOQK4",
            "Arn": "arn:aws:iam::991644510208:user/admin-1",
            "CreateDate": "2023-05-31T08:44:27Z",
            "PasswordLastUsed": "2023-05-31T10:37:11Z"
        },
        {
            "Path": "/",
            "UserName": "admin2-prog",
            "UserId": "AIDA6NYU6NAAFNIHMIMBF",
            "Arn": "arn:aws:iam::991644510208:user/admin2-prog",
            "CreateDate": "2023-05-31T08:46:54Z"
        },
        {
            "Path": "/",
            "UserName": "dev-user",
            "UserId": "AIDA6NYU6NAAFJLOJ72DC",
            "Arn": "arn:aws:iam::991644510208:user/dev-user",
            "CreateDate": "2023-05-31T11:27:17Z"
        },
        {
            "Path": "/",
            "UserName": "Sprints",
            "UserId": "AIDA6NYU6NAACE2RNHYA6",
            "Arn": "arn:aws:iam::991644510208:user/Sprints",
            "CreateDate": "2023-05-30T16:04:53Z",
            "PasswordLastUsed": "2023-05-30T16:10:09Z"
        }
    ]
```

- In the development group create user with name dev-user with programmatic and console access then try to access aws using it(take screenshot from accessing ec2 and s3 console)
- Also access cli using dev-user and try to get all users and try to get all users and groups using it



dev-user

Summary

ARN
arn:aws:iam::991644510208:user/dev-user

Console access
Enabled without MFA

Access key 1
AKIA6NYU6NAAOV5M43NP - Active
Used today. Created today.

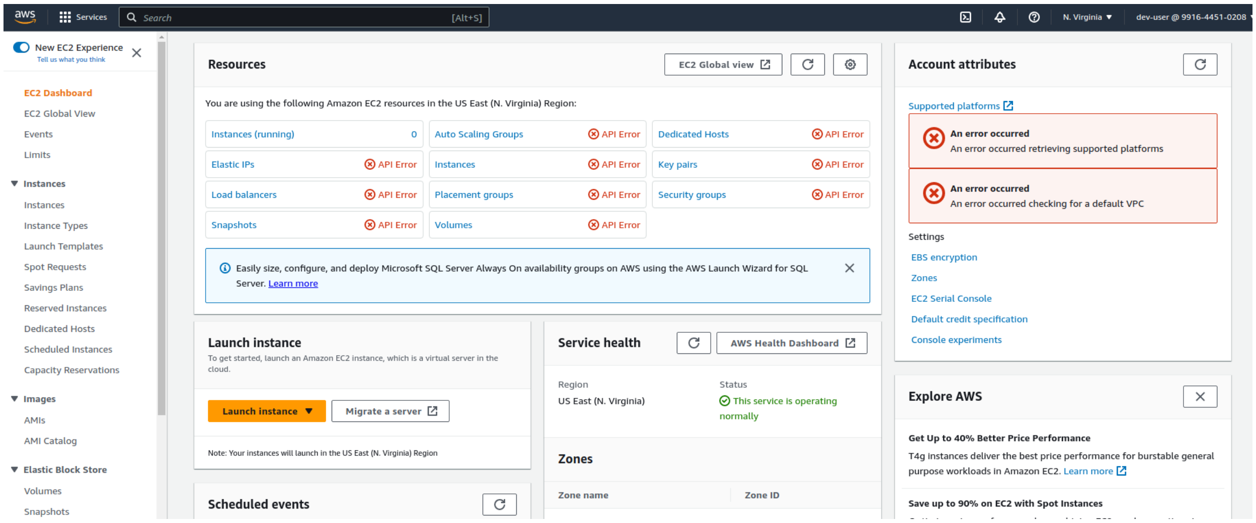
Created
May 31, 2023, 14:27 (UTC+03:00)

Last console sign-in
Today

Access key 2
Not enabled

Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonS3FullAccess	AWS managed	Group development
IAMUserChangePassword	AWS managed	Directly



Resources

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

Instances (running)	0	Auto Scaling Groups	API Error	Dedicated Hosts	API Error
Elastic IPs	API Error	Instances	API Error	Key pairs	API Error
Load balancers	API Error	Placement groups	API Error	Security groups	API Error
Snapshots	API Error	Volumes	API Error		

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.

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

Scheduled events

Service health

Region
US East (N. Virginia)

Status
This service is operating normally

Zones

Zone name	Zone ID

Account attributes

Supported platforms

An error occurred
An error occurred retrieving supported platforms

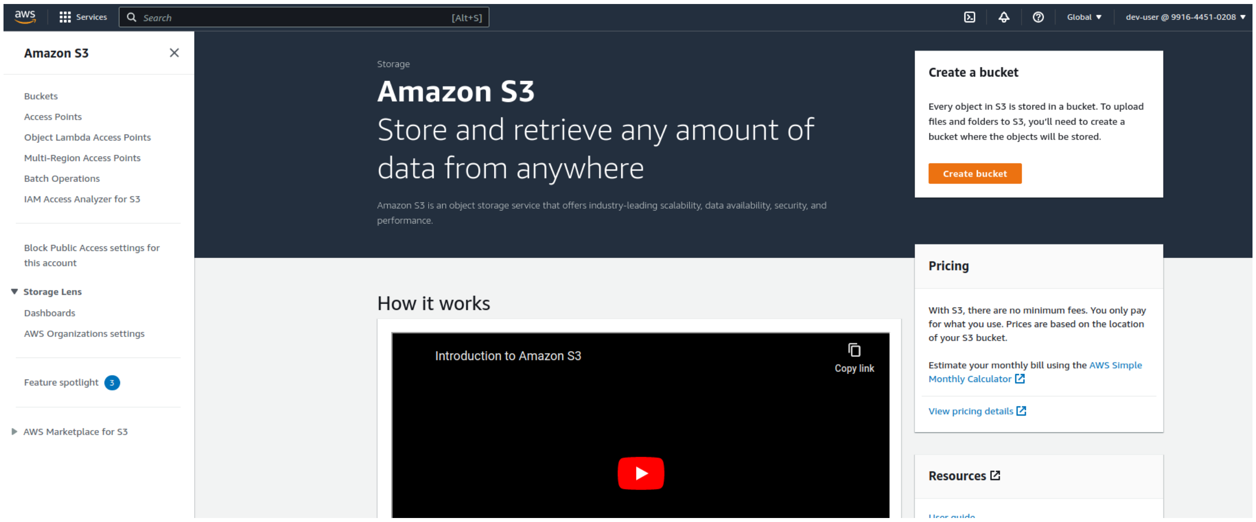
An error occurred
An error occurred checking for a default VPC

Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments

Explore AWS

Get Up to 40% Better Price Performance
T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more

Save up to 90% on EC2 with Spot Instances



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 3

▶ AWS Marketplace for S3

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

How it works

Pricing

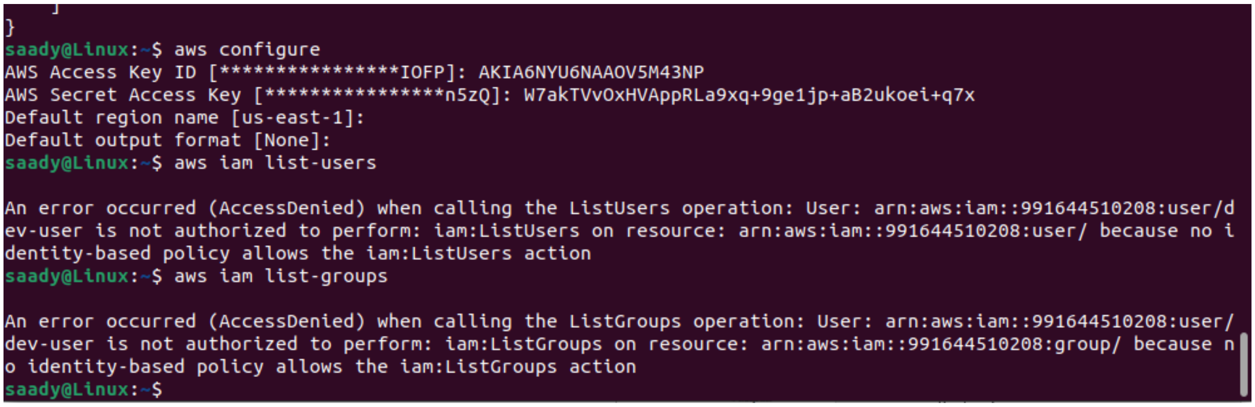
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

Resources

User guide



```
    ]
}
saady@Linux:~$ aws configure
AWS Access Key ID [****************IOFP]: AKIA6NYU6NAAOV5M43NP
AWS Secret Access Key [****************n5zQ]: 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
Default region name [us-east-1]:
Default output format [None]:
saady@Linux:~$ aws iam list-users

An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::991644510208:user/d
ev-user is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::991644510208:user/ because no i
dentity-based policy allows the iam:ListUsers action
saady@Linux:~$ aws iam list-groups

An error occurred (AccessDenied) when calling the ListGroups operation: User: arn:aws:iam::991644510208:user/
dev-user is not authorized to perform: iam:ListGroups on resource: arn:aws:iam::991644510208:group/ because n
o identity-based policy allows the iam:ListGroups action
saady@Linux:~$
```