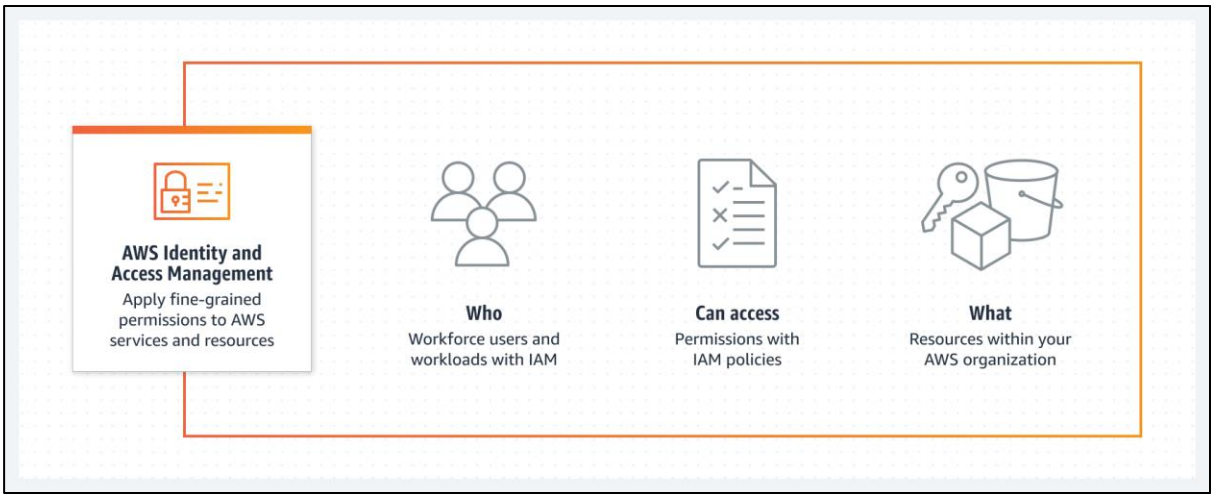
IAM:

IDENTIFY AND ACCESS MANAGEMENT

you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.


AWS Identity and Access Management
Apply fine-grained permissions to AWS services and resources
Who
Workforce users and workloads with IAM
Can access
Permissions with IAM policies
What
Resources within your AWS organization

WHY USE IAM:

Use IAM to manage and scale workload and workforce access securely supporting your agility and innovation in AWS.

- ALIAS URL
- USER
- GROUP
- HOW TO ACCES AWS VIA CLI(command line interface)
- ACCESS KEY
- SECRET ACCESS KEY
- MFA
- POLICY
- ROLES
- USER TO SERVICE COMMUNICATION
- SERVICE TO SERVICE COMMUNICATION

ALIAS URL:

The AWS account root user and AWS Identity and Access Management (IAM) users in the account sign in using a web URL.

If you want the URL for your IAM users to contain your company name (or another easy-to-remember identifier) instead of the AWS account ID, you can create an account alias.

MFA:

AWS Identity and Access Management (IAM) best practice that requires a second authentication factor in addition to user name and password sign-in credentials.

You can enable MFA at the AWS account level and for root and IAM users you have created in your account.

Two types: 1.Physical mfa (manual password)

2.Virtual mfa(fingerprint)

USER TO SERVICE COMMUNICATION:

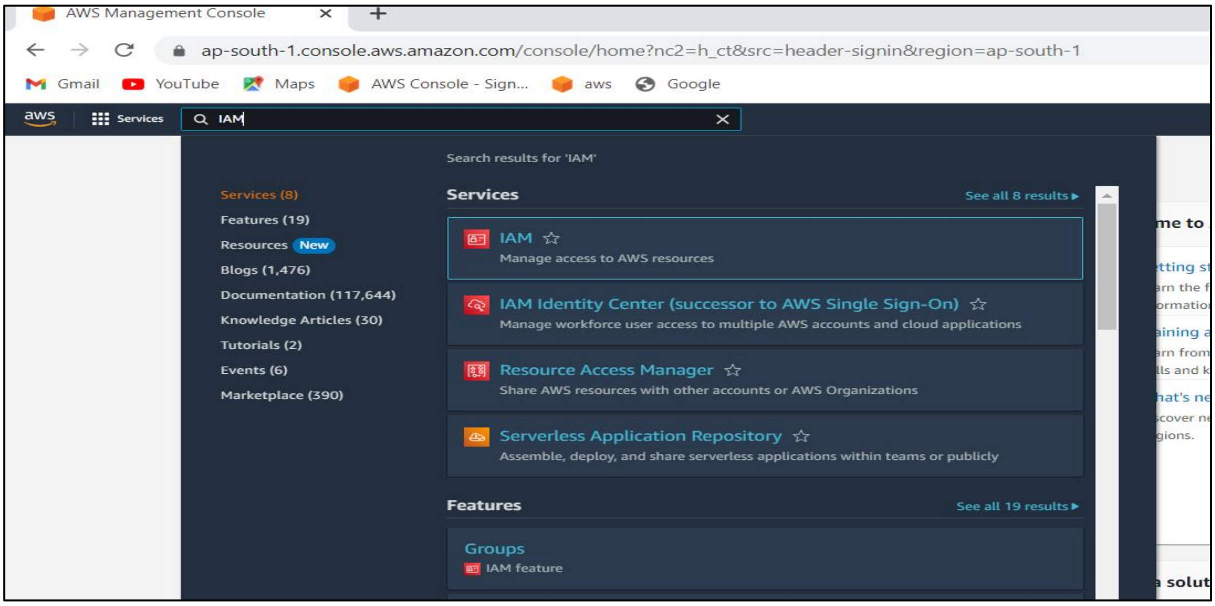
It working purpose for Root user create one instance now saw this instance for user

SERVICE TO SERVICE COMMUNICATION:

It is communicate between one service to another service same server.

USER TO SERVICE COMMUNICATION:

STEP1: Aws search bar--->IAM---->select



ap-south-1.console.aws.amazon.com/console/home?nc2=h_ct&src=header-signin&region=ap-south-1

IAM

Search results for 'IAM'

IAM
Manage access to AWS resources

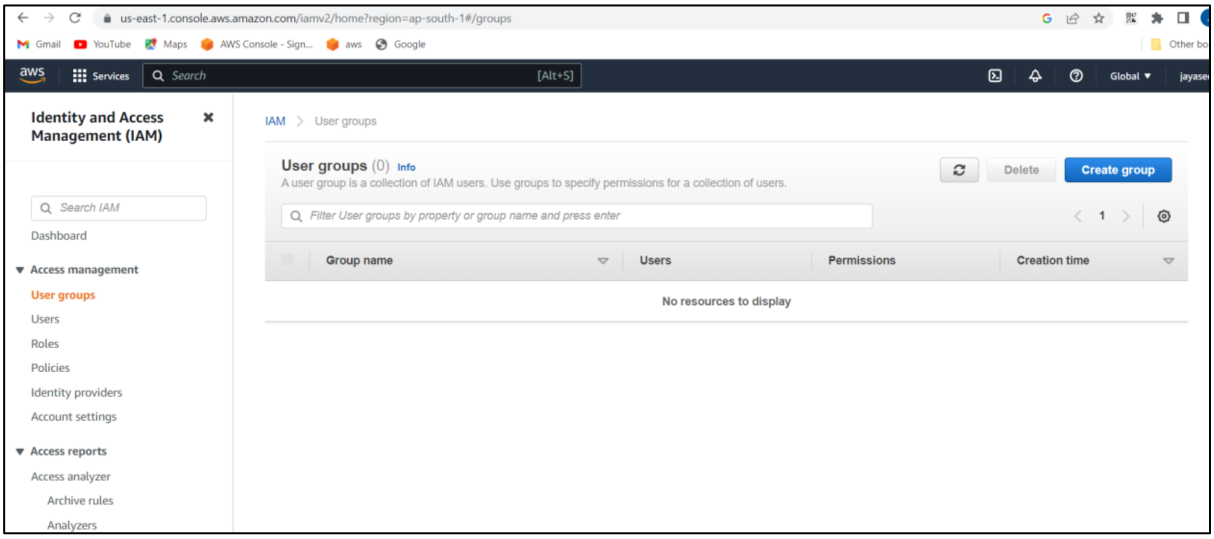
IAM Identity Center (successor to AWS Single Sign-On)
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager
Share AWS resources with other accounts or AWS Organizations

Serverless Application Repository
Assemble, deploy, and share serverless applications within teams or publicly

Groups
IAM feature

STEP2: Acces management ---->create group



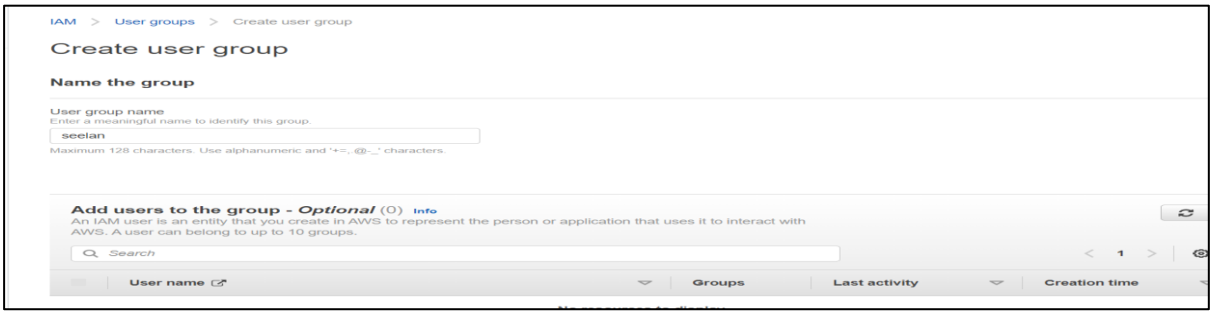
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups

User groups (0)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time

No resources to display

STEP2.1:create user group---->name of the group (any name)



IAM > User groups > Create user group

Create user group

Name the group

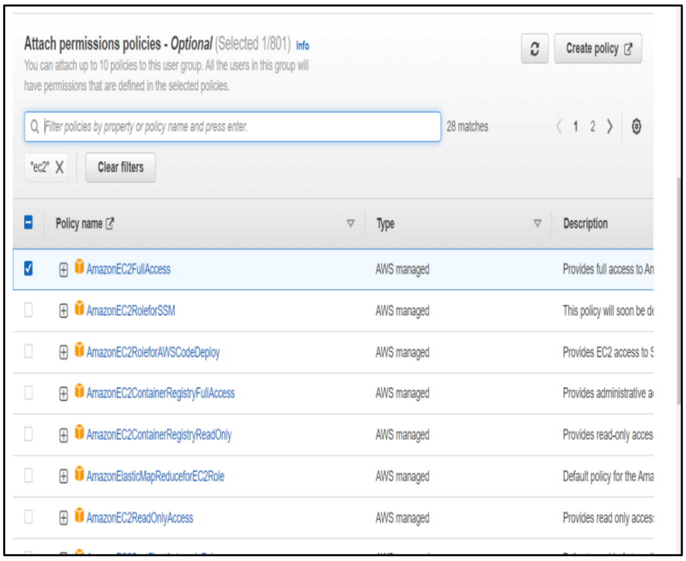
User group name
Enter a meaningful name to identify this group.
seelan
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (0)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

User name	Groups	Last activity	Creation time

STEP2.2: Attach permission polices--->search bar(1.ec2 enter)--->click amazon ec2 full acces ----->(2.s3 enter---> amazon ec2 full acces)

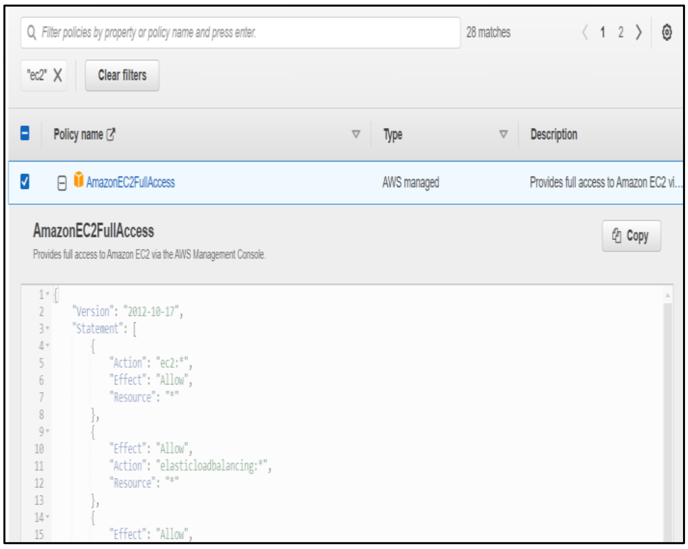
----->(3.IAM enter --> amazon ec2 full acces)



Attach permissions policies - *Optional* (Selected 1/801) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

	Policy name	Type	Description
☑	AmazonEC2FullAccess	AWS managed	Provides full access to An
□	AmazonEC2RoleforSSM	AWS managed	This policy will soon be de
□	AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S
□	AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative a
□	AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only acces
□	AmazonElasticMapReduceforEC2Role	AWS managed	Default policy for the Ama
□	AmazonEC2ReadOnlyAccess	AWS managed	Provides read only acces



	Policy name	Type	Description
☑	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 vi...

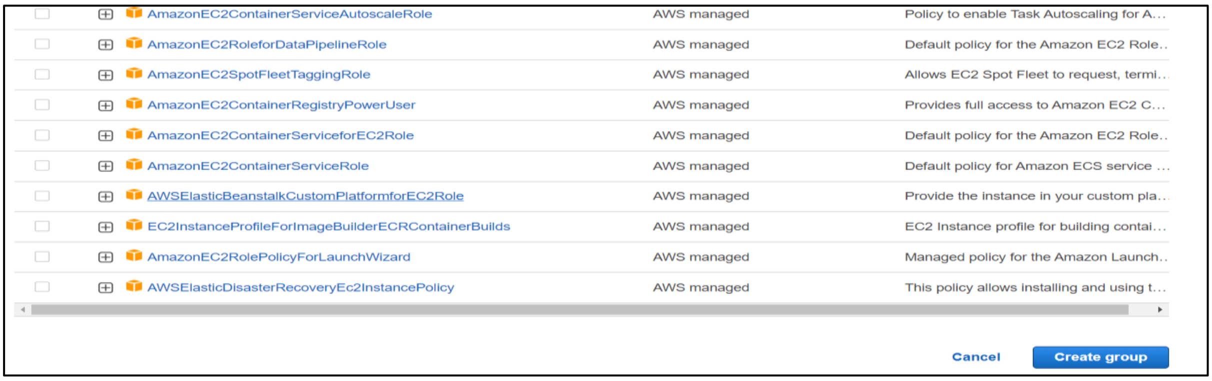
AmazonEC2FullAccess

Provides full access to Amazon EC2 via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:*",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

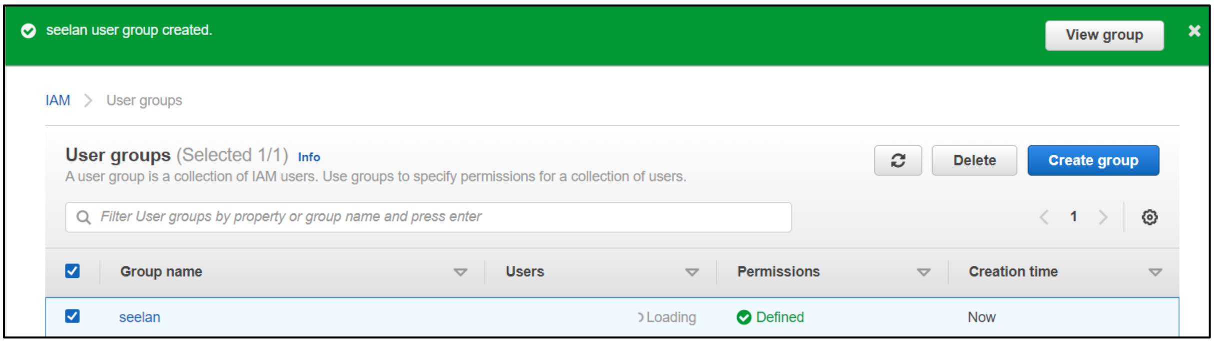
After select policies --->ec2 tag remove

STEP2.3:create group



	Policy name	Type	Description
□	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	Policy to enable Task Autoscaling for A...
□	AmazonEC2RoleforDataPipelineRole	AWS managed	Default policy for the Amazon EC2 Role..
□	AmazonEC2SpotFleetTaggingRole	AWS managed	Allows EC2 Spot Fleet to request, termi...
□	AmazonEC2ContainerRegistryPowerUser	AWS managed	Provides full access to Amazon EC2 C...
□	AmazonEC2ContainerServiceforEC2Role	AWS managed	Default policy for the Amazon EC2 Role..
□	AmazonEC2ContainerServiceRole	AWS managed	Default policy for Amazon ECS service ...
□	AWSElasticBeanstalkCustomPlatformforEC2Role	AWS managed	Provide the instance in your custom pla...
□	EC2InstanceProfileForImageBuilderECRContainerBuilds	AWS managed	EC2 Instance profile for building contai...
□	AmazonEC2RolePolicyForLaunchWizard	AWS managed	Managed policy for the Amazon Launch..
□	AWSElasticDisasterRecoveryEc2InstancePolicy	AWS managed	This policy allows installing and using t...

Group will created..



seelan user group created.

View group
IAM > User groups

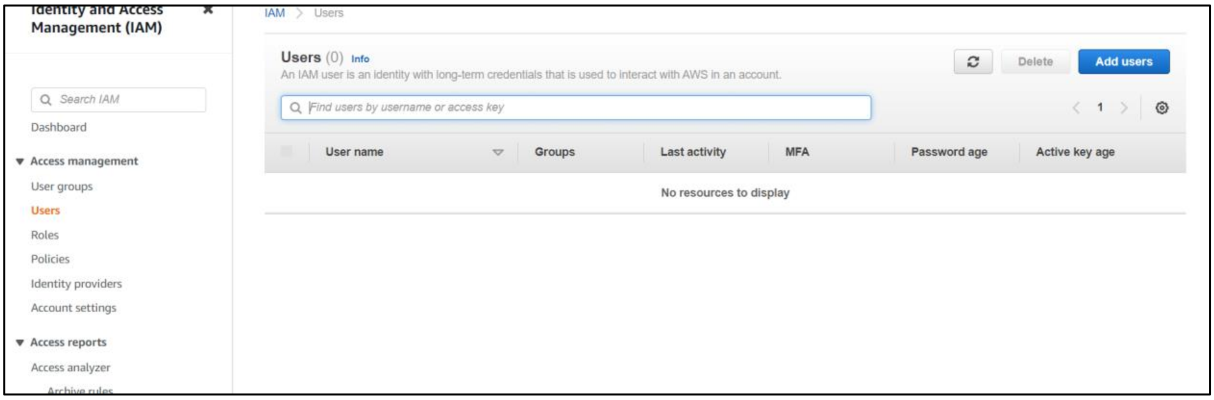
User groups (Selected 1/1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Delete
Create group
Filter User groups by property or group name and press enter
1

☑	Group name	Users	Permissions	Creation time
☑	seelan	Loading	Defined	Now

Step3: Access management--->users--->add users



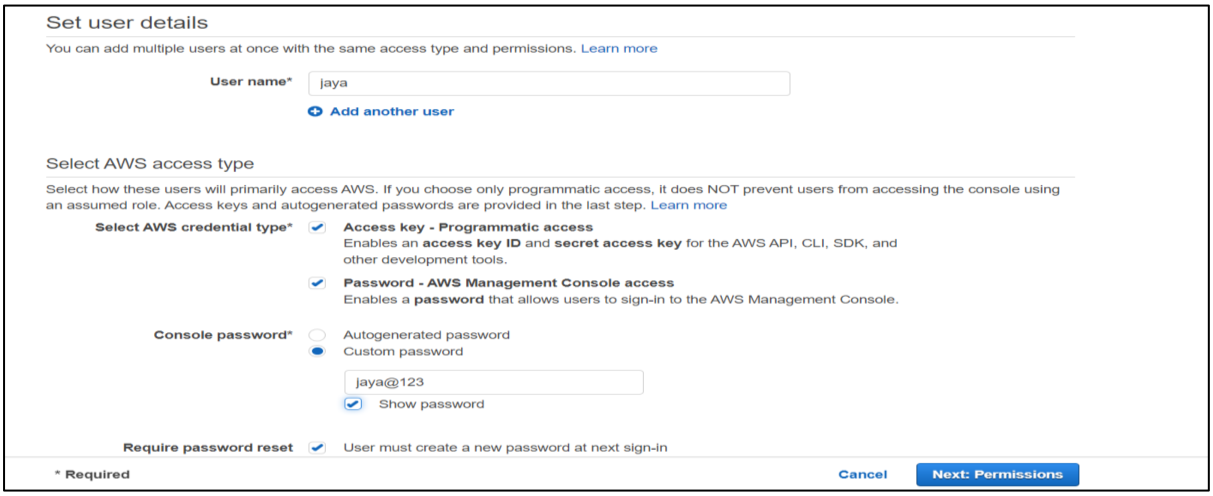
Users (0) Info

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

No resources to display

Step3.1:set user details--->user name(any name)--->click select aws credential type two boxes---->console password(any)--->next



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* jaya

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

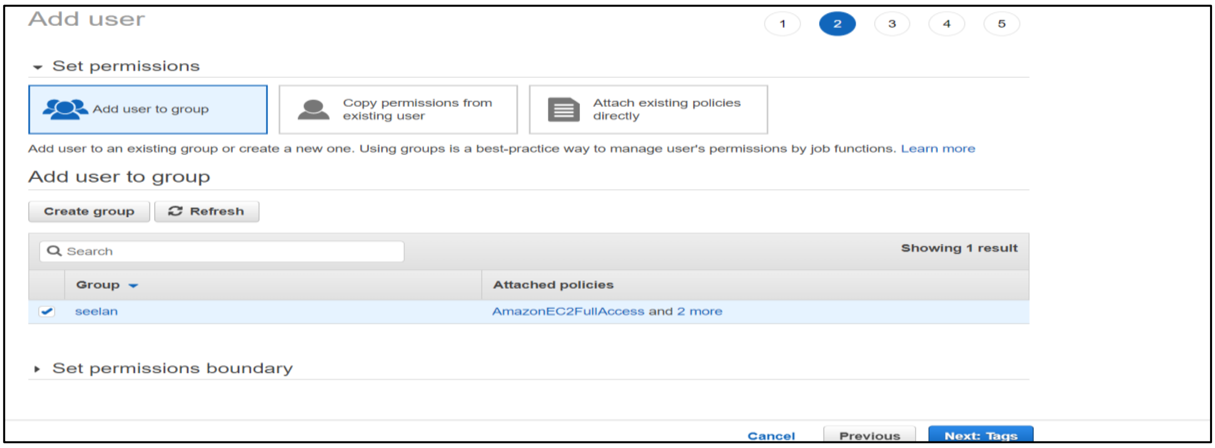
Select AWS credential type*
☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
☑ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*
○ Autogenerated password
● Custom password
jaya@123
☑ Show password

Require password reset ☑ User must create a new password at next sign-in

* Required

Step3.1:set permissions--->add user group --->select group--->next



Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

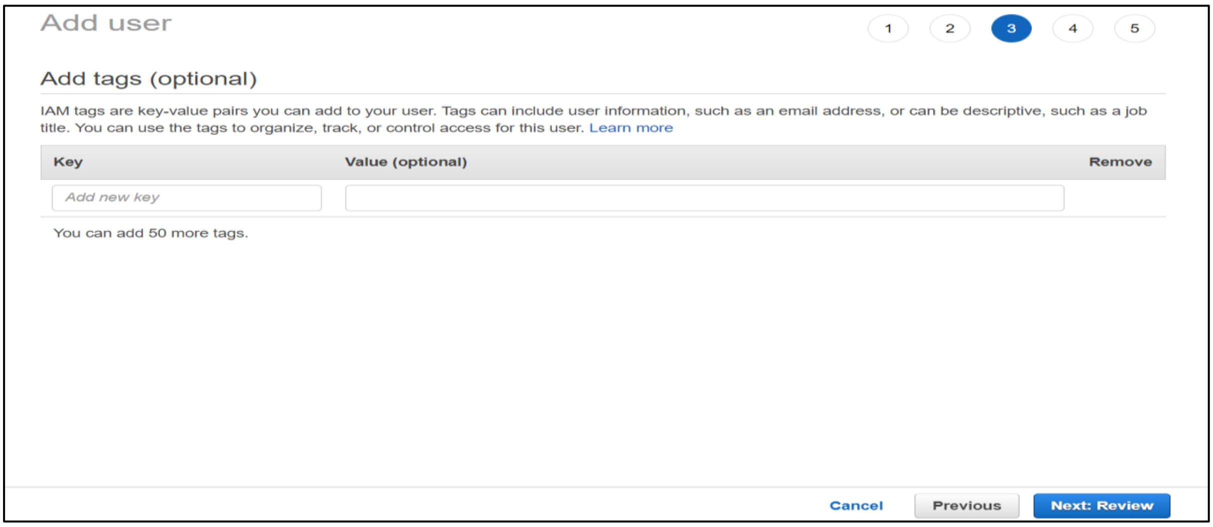
Add user to group

Showing 1 result

	Group	Attached policies
☑	seelan	AmazonEC2FullAccess and 2 more

Set permissions boundary

Step3.2: Add user--->add tags--->next



Add user

1 2 3 4 5

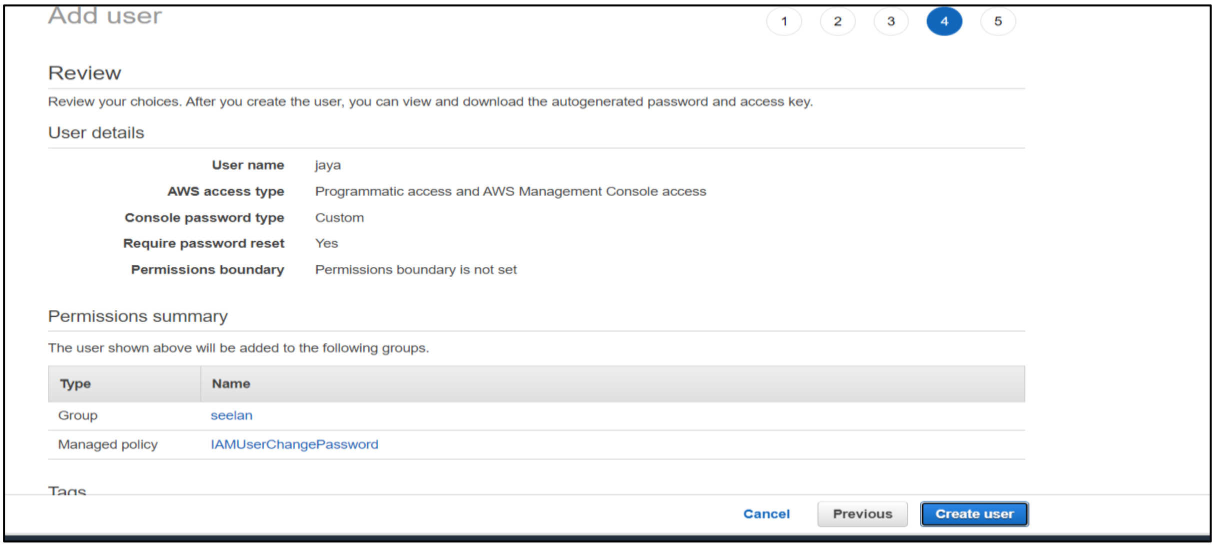
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Step3.3:review--->create user



Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	jaya
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

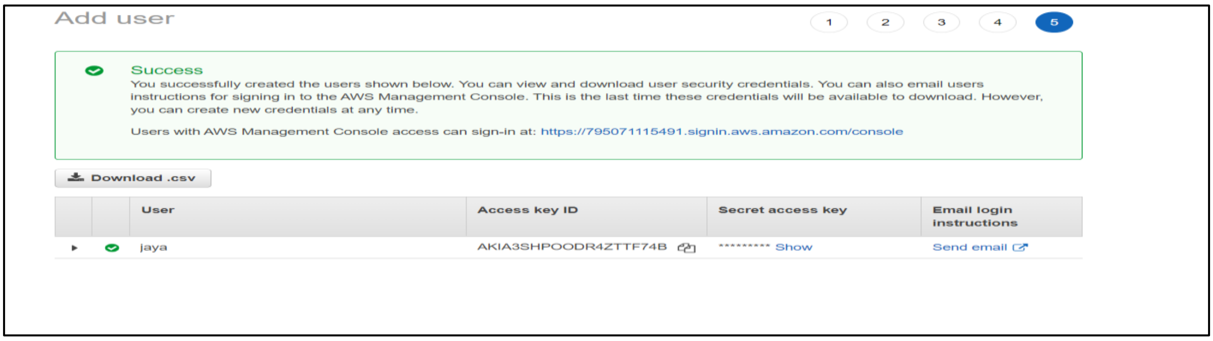
Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	seelan
Managed policy	IAMUserChangePassword

Tags

Step3.3:user attached group completed--->success--->download.ccv



Add user

1 2 3 4 5

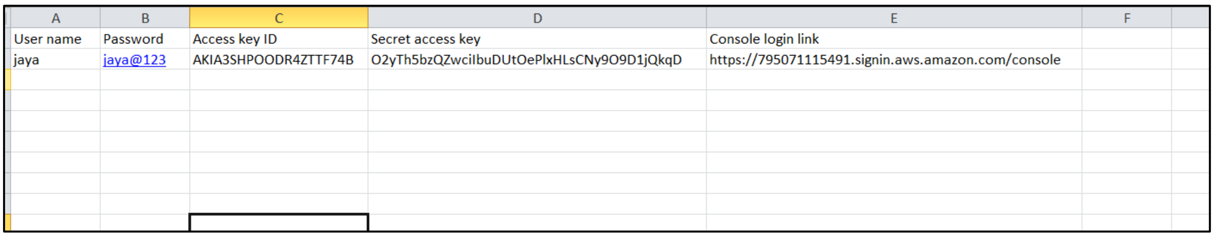
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://795071115491.signin.aws.amazon.com/console

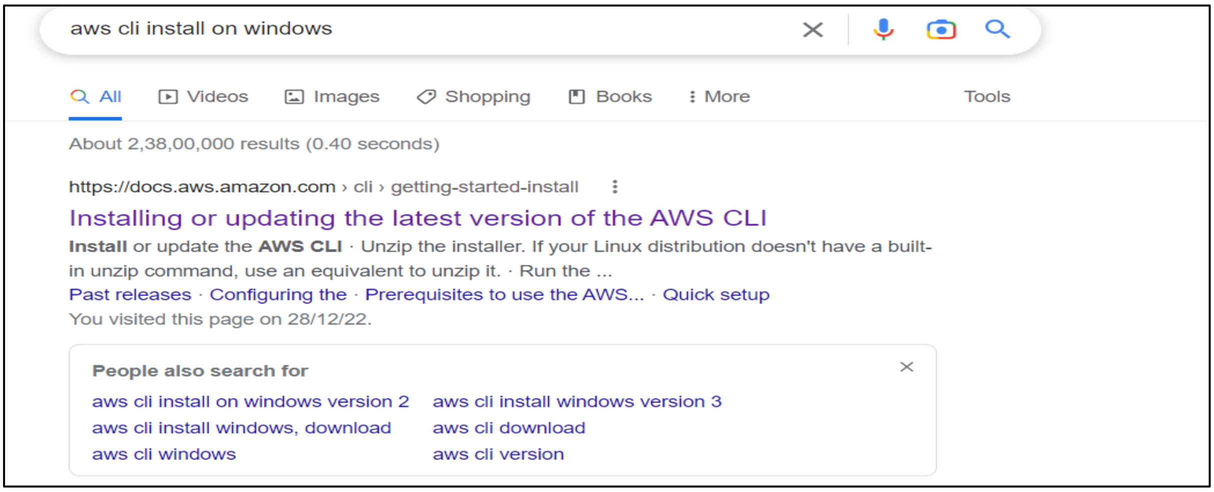
		User	Access key ID	Secret access key	Email login instructions
▸	✓	jaya	AKIA3SHPOODR4ZTTF74B	********* Show	Send email

Step3.4:open excel sheet--->user name,password,acces key id,secret acces key … --->shown



A	B	C	D	E	F
User name	Password	Access key ID	Secret access key	Console login link	
jaya	jaya@123	AKIA3SHPOODR4ZTTF74B	O2yTh5bzQZwcilbuDUtOePlxHLsCNy9O9D1jQkqD	https://795071115491.signin.aws.amazon.com/console	

Step3.5: install CLI--->Chrome(aws cli install on windows)--->select first link



About 2,38,00,000 results (0.40 seconds)

https://docs.aws.amazon.com › cli › getting-started-install

Installing or updating the latest version of the AWS CLI

Install or update the **AWS CLI** · Unzip the installer. If your Linux distribution doesn't have a built-in unzip command, use an equivalent to unzip it. · Run the ...

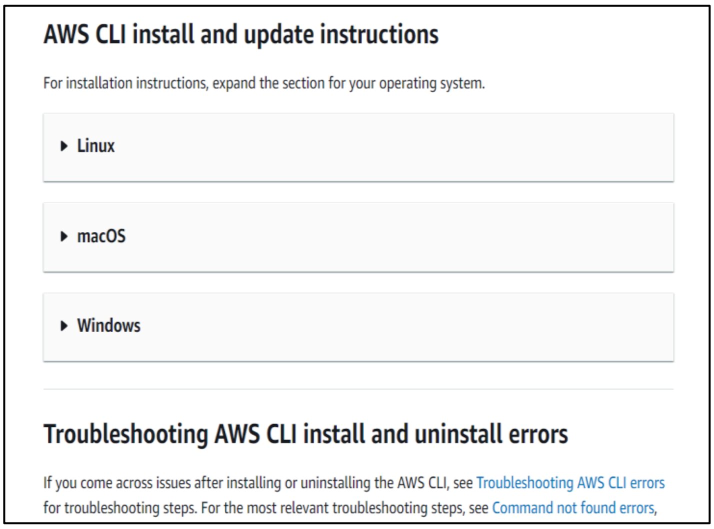
Past releases · Configuring the · Prerequisites to use the AWS... · Quick setup

You visited this page on 28/12/22.

People also search for

aws cli install on windows version 2 | aws cli install windows version 3
aws cli install windows, download | aws cli download
aws cli windows | aws cli version

Select--->windows--->download link--->download

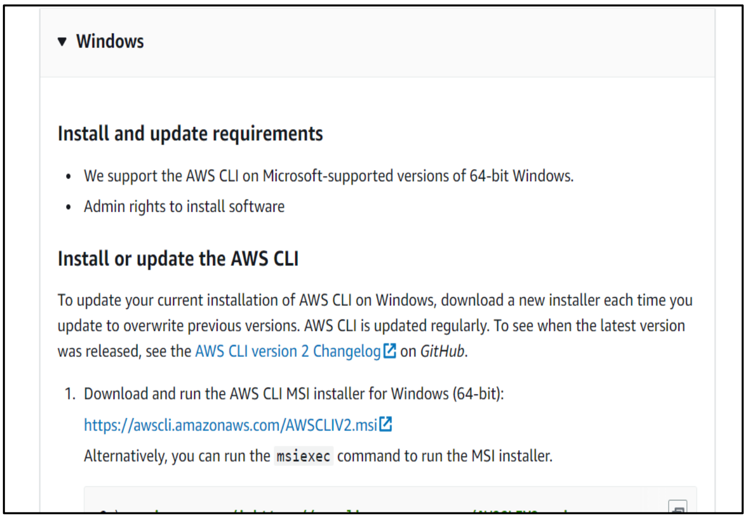


AWS CLI install and update instructions

For installation instructions, expand the section for your operating system.

Troubleshooting AWS CLI install and uninstall errors

If you come across issues after installing or uninstalling the AWS CLI, see Troubleshooting AWS CLI errors for troubleshooting steps. For the most relevant troubleshooting steps, see Command not found errors,



Install and update requirements

- We support the AWS CLI on Microsoft-supported versions of 64-bit Windows.
- Admin rights to install software

Install or update the AWS CLI

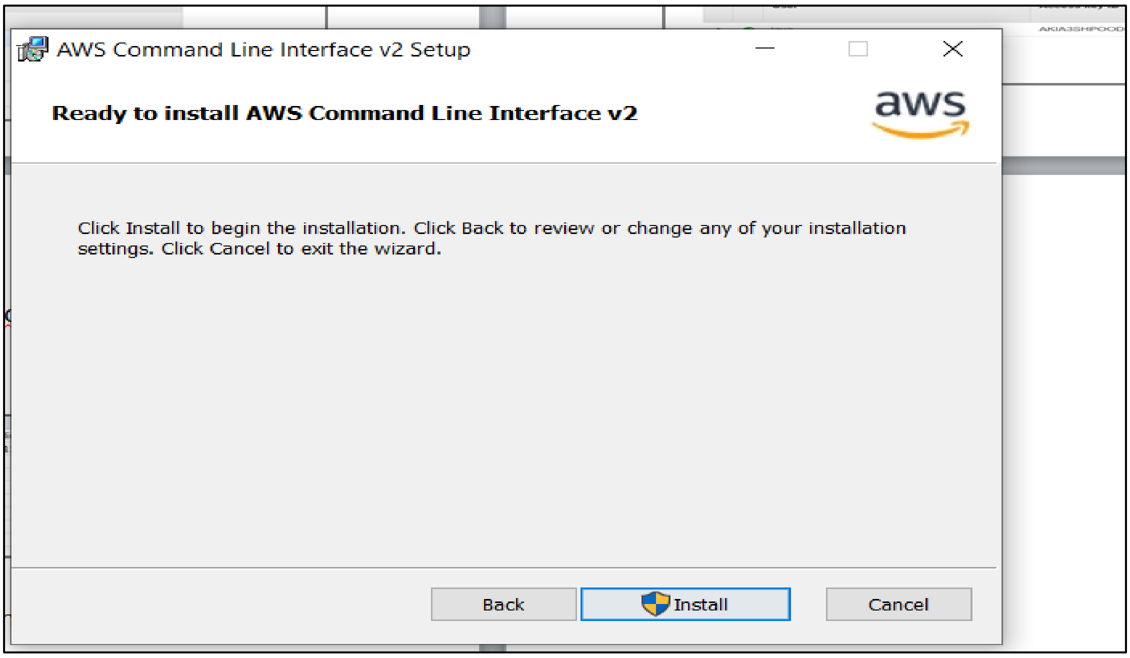
To update your current installation of AWS CLI on Windows, download a new installer each time you update to overwrite previous versions. AWS CLI is updated regularly. To see when the latest version was released, see the AWS CLI version 2 Changelog on *GitHub*.

1. Download and run the AWS CLI MSI installer for Windows (64-bit):

   https://awscli.amazonaws.com/AWSCLIV2.msi

   Alternatively, you can run the `msiexec` command to run the MSI installer.

Open cli--->install



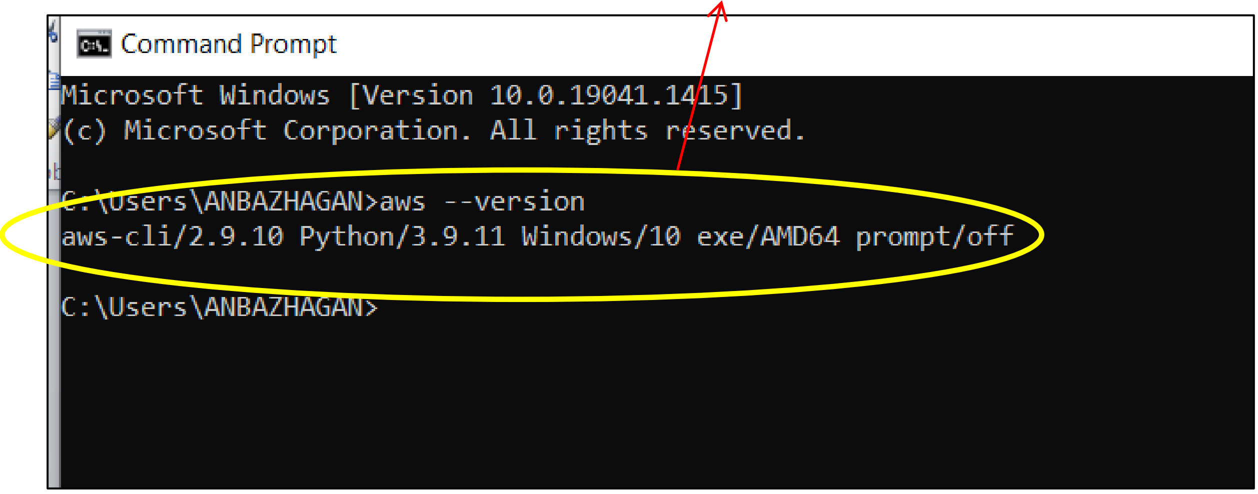
AWS Command Line Interface v2 Setup

Ready to install AWS Command Line Interface v2

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step3.6:now configure aws in cmd prompt

Step3.6.1:check aws --version -------->this is come aws configure succes

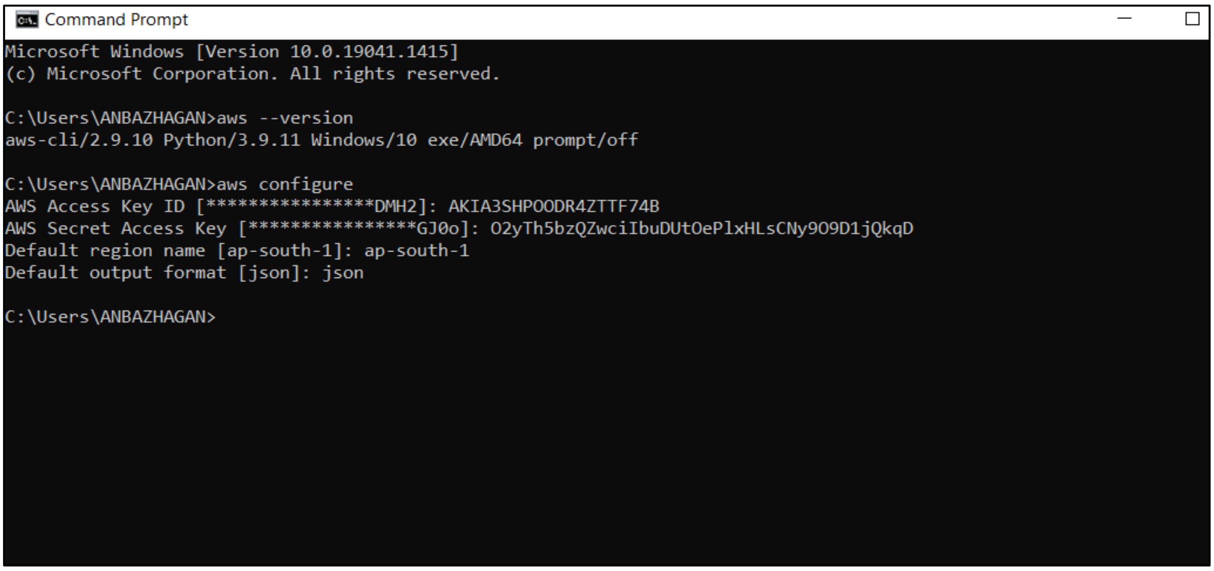


Command Prompt

```
Microsoft Windows [Version 10.0.19041.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ANBAZHAGAN>aws --version
aws-cli/2.9.10 Python/3.9.11 Windows/10 exe/AMD64 prompt/off

C:\Users\ANBAZHAGAN>
```

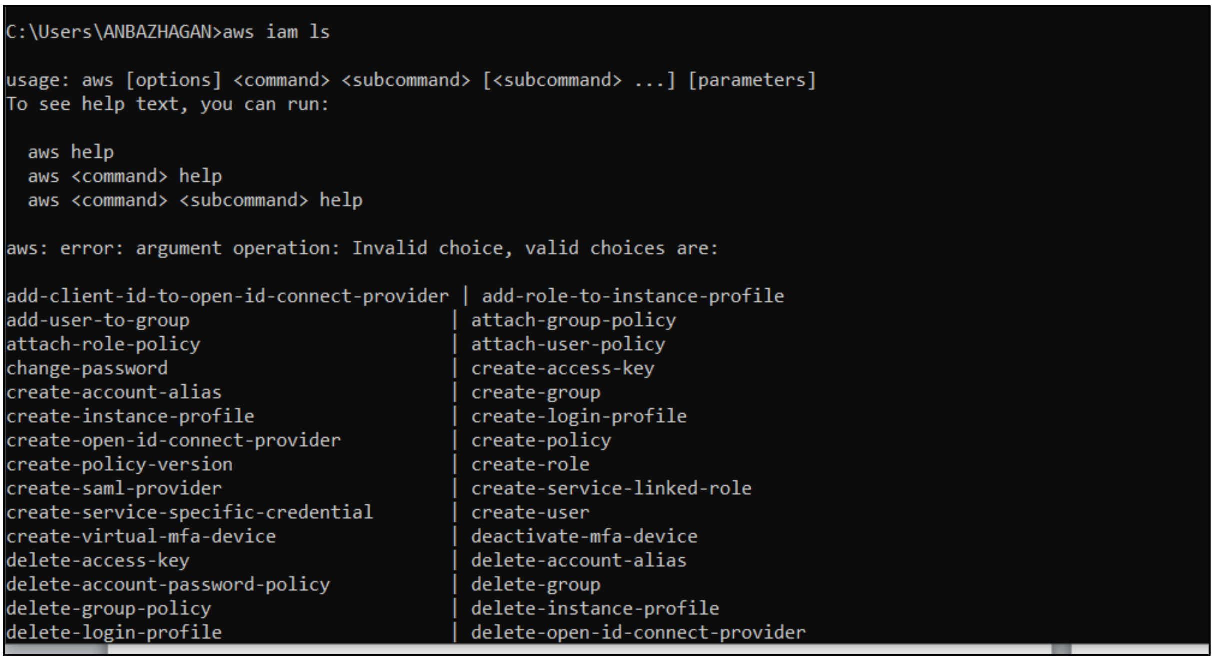
Step3.6.2:login(aws configure)---->put aws acces key--->put secret access key--->put default region--->put default output format(json)

------>login completed..



```
Microsoft Windows [Version 10.0.19041.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ANBAZHAGAN>aws --version
aws-cli/2.9.10 Python/3.9.11 Windows/10 exe/AMD64 prompt/off

C:\Users\ANBAZHAGAN>aws configure
AWS Access Key ID [****************DMH2]: AKIA3SHPOODR4ZTTF74B
AWS Secret Access Key [****************GJ0o]: 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
Default region name [ap-south-1]: ap-south-1
Default output format [json]: json

C:\Users\ANBAZHAGAN>
```

Step3.6.3:now check ec2 ls--->s3 ls--->iam ls---(eg:aws iam ls)--->all files will be listed

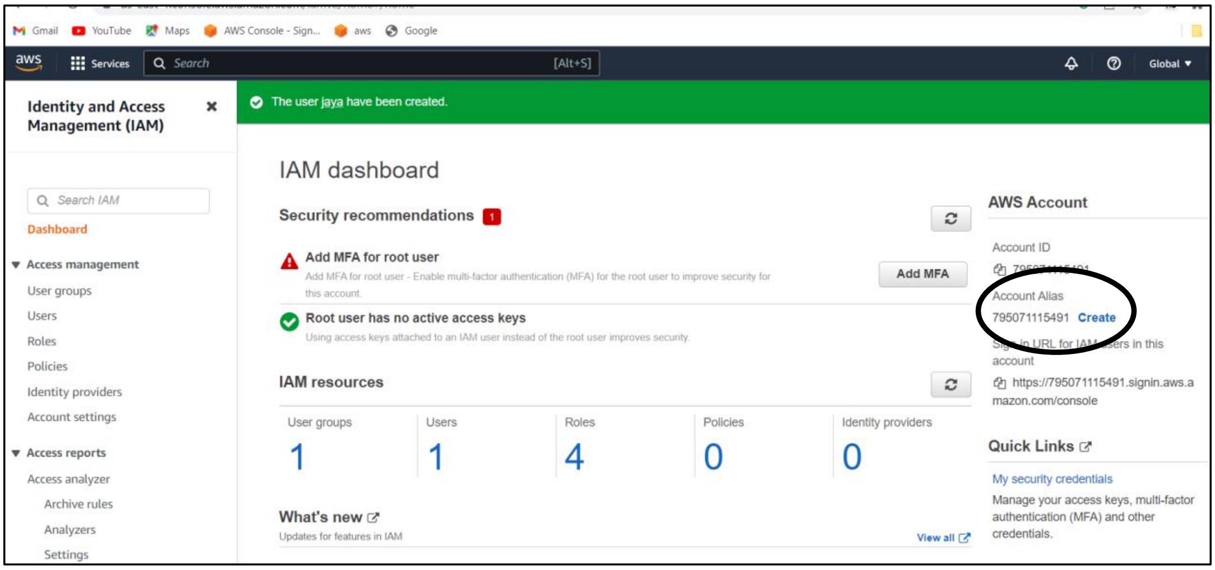


```
C:\Users\ANBAZHAGAN>aws iam ls

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help

aws: error: argument operation: Invalid choice, valid choices are:

add-client-id-to-open-id-connect-provider | add-role-to-instance-profile
add-user-to-group                        | attach-group-policy
attach-role-policy                       | attach-user-policy
change-password                          | create-access-key
create-account-alias                     | create-group
create-instance-profile                  | create-login-profile
create-open-id-connect-provider          | create-policy
create-policy-version                    | create-role
create-saml-provider                     | create-service-linked-role
create-service-specific-credential       | create-user
create-virtual-mfa-device                | deactivate-mfa-device
delete-access-key                        | delete-account-alias
delete-account-password-policy           | delete-group
delete-group-policy                      | delete-instance-profile
delete-login-profile                     | delete-open-id-connect-provider
```

AWS CLI CONFIGURED SUCCES..

STEP4:DOWNLOAD ALLIAS URL

STEP4.1: Dashboard ---->aws account--->account allias ---->create



The user jaya have been created.

IAM dashboard

Security recommendations 1

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	1	4	0	0

What's new
Updates for features in IAM

AWS Account

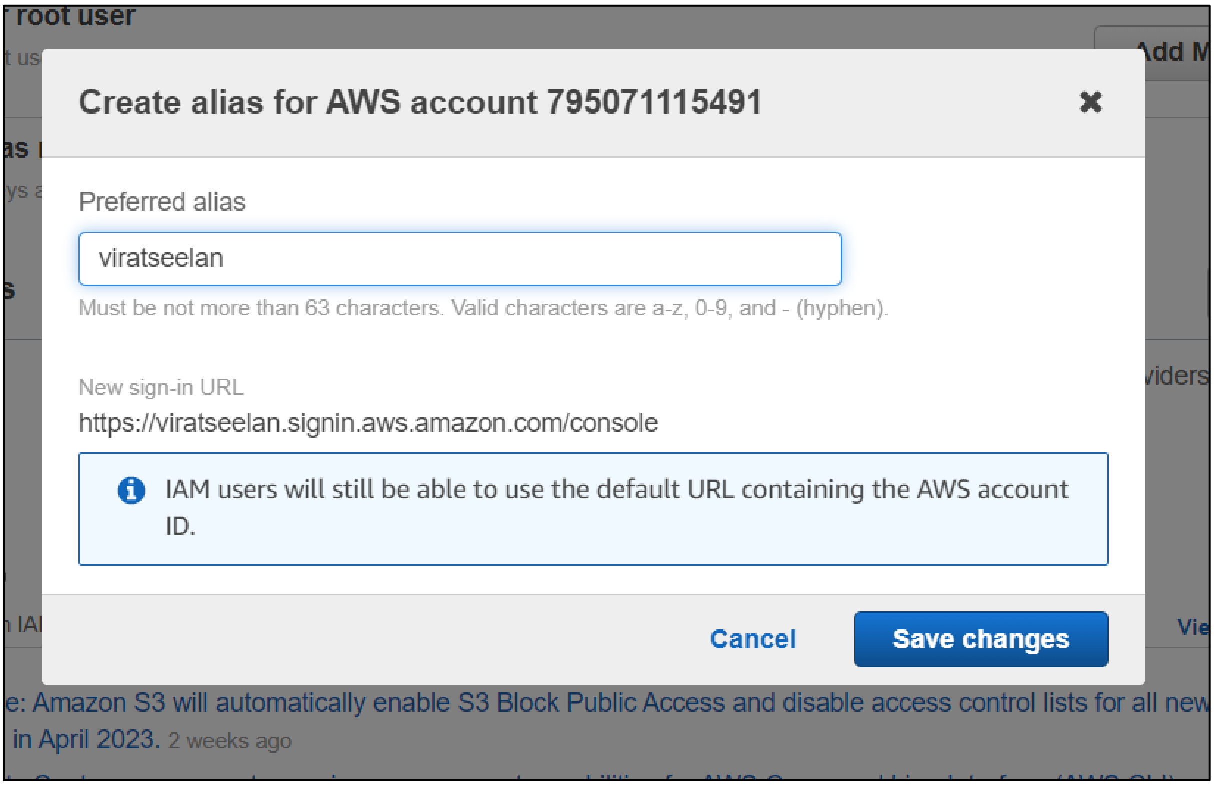
Account ID
795071115491

Account Alias
795071115491 Create

Sign-in URL for IAM users in this account
https://795071115491.signin.aws.amazon.com/console

Manage your access keys, multi-factor authentication (MFA) and other credentials.

STEP4.2:Preffered allias(any name)--->save changes--->allias created



Create alias for AWS account 795071115491

Preferred alias

viratseelan

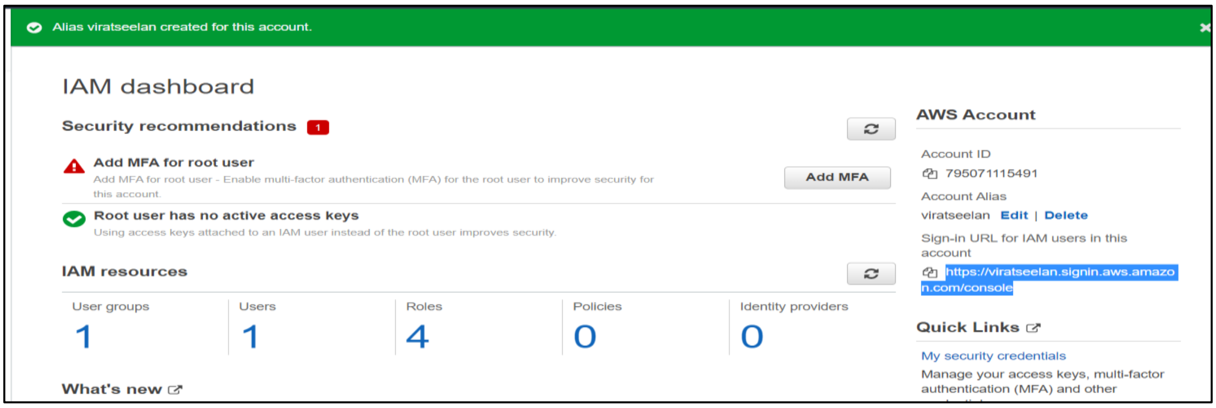
Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL
https://viratseelan.signin.aws.amazon.com/console

IAM users will still be able to use the default URL containing the AWS account ID.

e: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new in April 2023. 2 weeks ago

Allias created..



Alias viratseelan created for this account.

IAM dashboard

Security recommendations 1

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	1	4	0	0

What's new

AWS Account

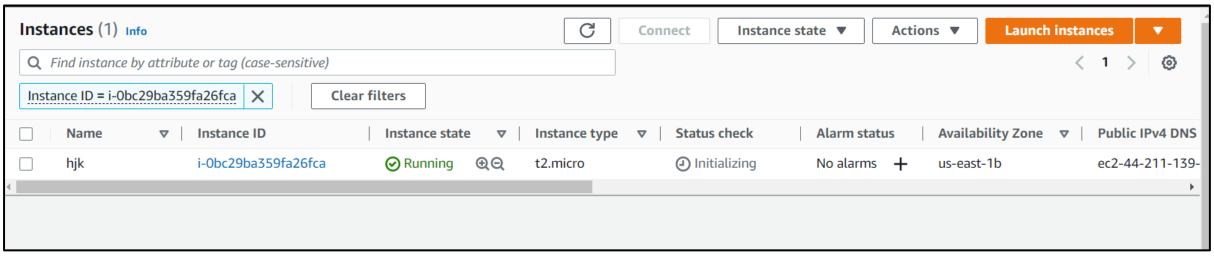
Account ID
795071115491

Account Alias
viratseelan Edit | Delete

Sign-in URL for IAM users in this account
https://viratseelan.signin.aws.amazon.com/console

Manage your access keys, multi-factor authentication (MFA) and other

STEP5:instance create in root account



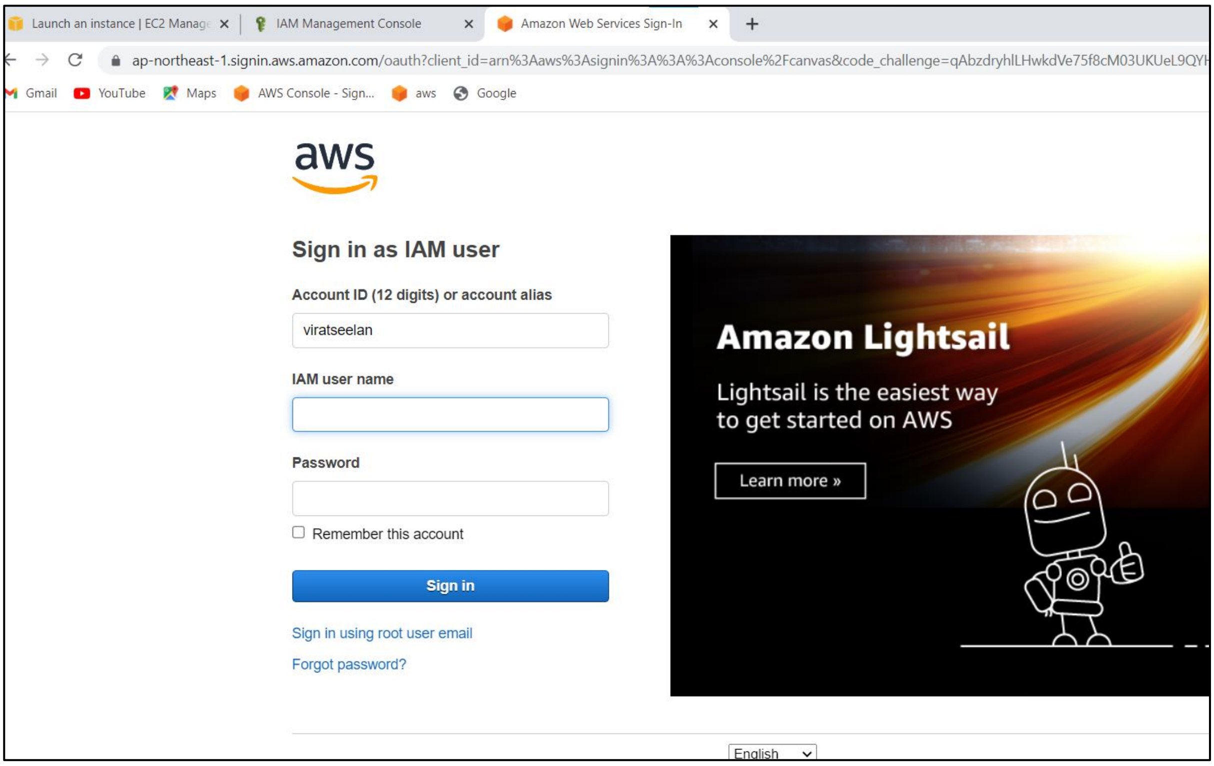
Instances (1) Info

Find instance by attribute or tag (case-sensitive)

Instance ID = i-0bc29ba359fa26fca

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
hjk	i-0bc29ba359fa26fca	Running	t2.micro	Initializing	No alarms	us-east-1b	ec2-44-211-139-

STEP6:copy allias url ---put chrome(open user aws account)



ap-northeast-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=qAbzdryhlLHwkdVe75f8cM03UKUeL9QYI

Sign in as IAM user

Account ID (12 digits) or account alias: viratseelan

IAM user name:

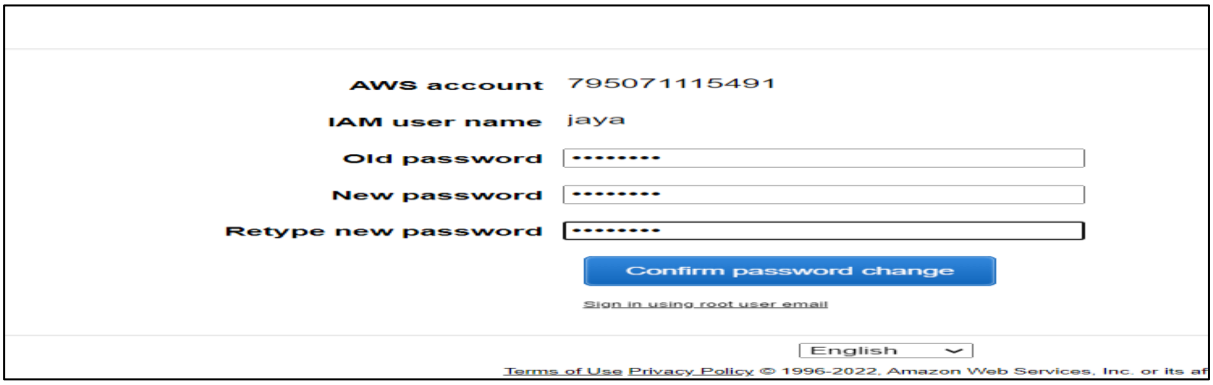
Password:

□ Remember this account

Sign in using root user email

Forgot password?

STEP6.1:created user name and password put--->next page --->password change--->login user account



AWS account 795071115491

IAM user name jaya

Old password ••••••••

New password ••••••••

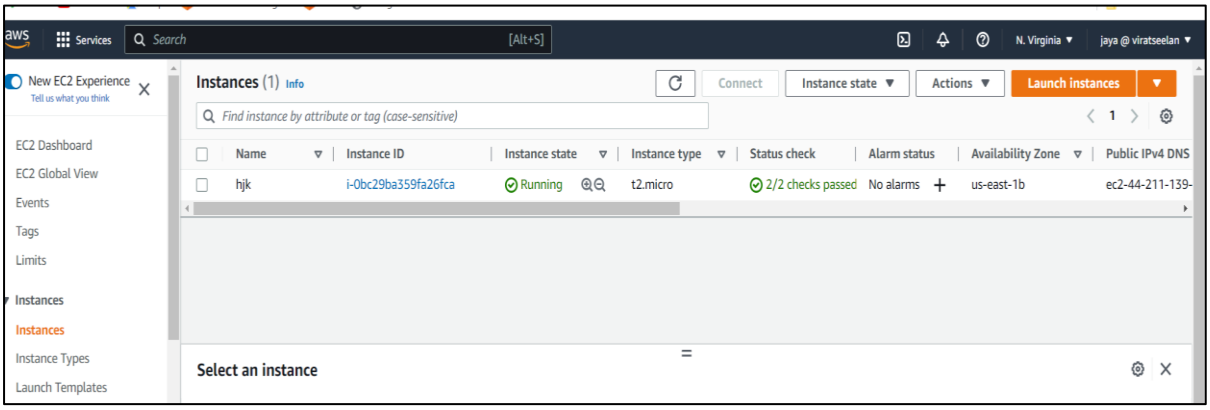
Retype new password ••••••••

Sign in using root user email

Terms of Use Privacy Policy © 1996-2022, Amazon Web Services, Inc. or its af

STEP6.2:same zone shown for root account(eg:Mumbai) then only saw root account works..

(suppose root account zone is virgenia and user account zone ismumbai) --->cant saw root account works



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	hjk	i-0bc29ba359fa26fca	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-44-211-139-

i.e: I will creat ec2 instance in root account and now shown user account for same instance

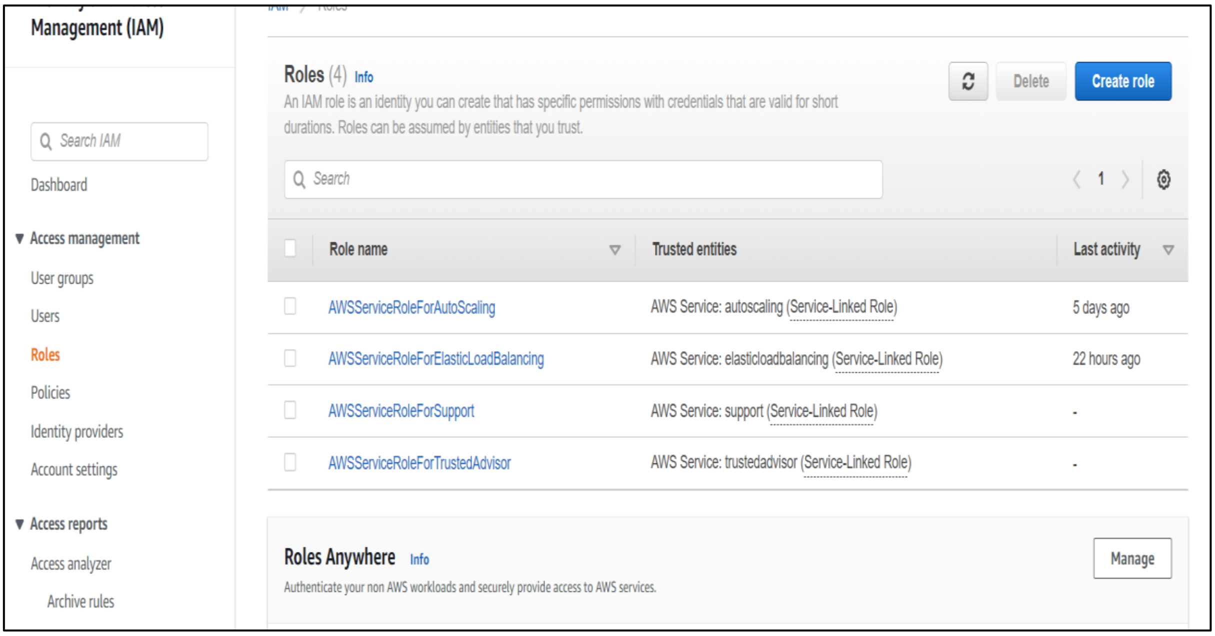
user to service communication will success..

After Root account---> user account group and user will delete and user account will deleted..

SERVICE TO SERVICE COMMUNICATION:

It is communicate between one service to another service same server.

STEP1:IAM--->Roles --->create role



Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Roles (4) Info

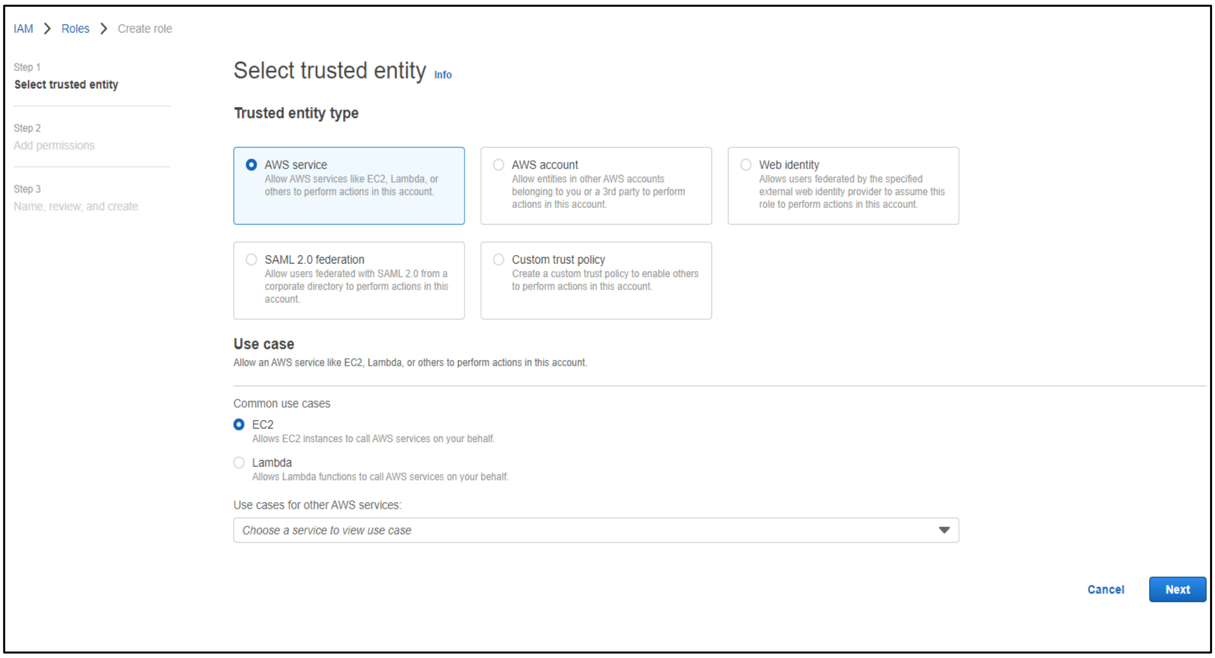
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	5 days ago
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	22 hours ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

STEP1.1: Aws service---->Ec2--->Next



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

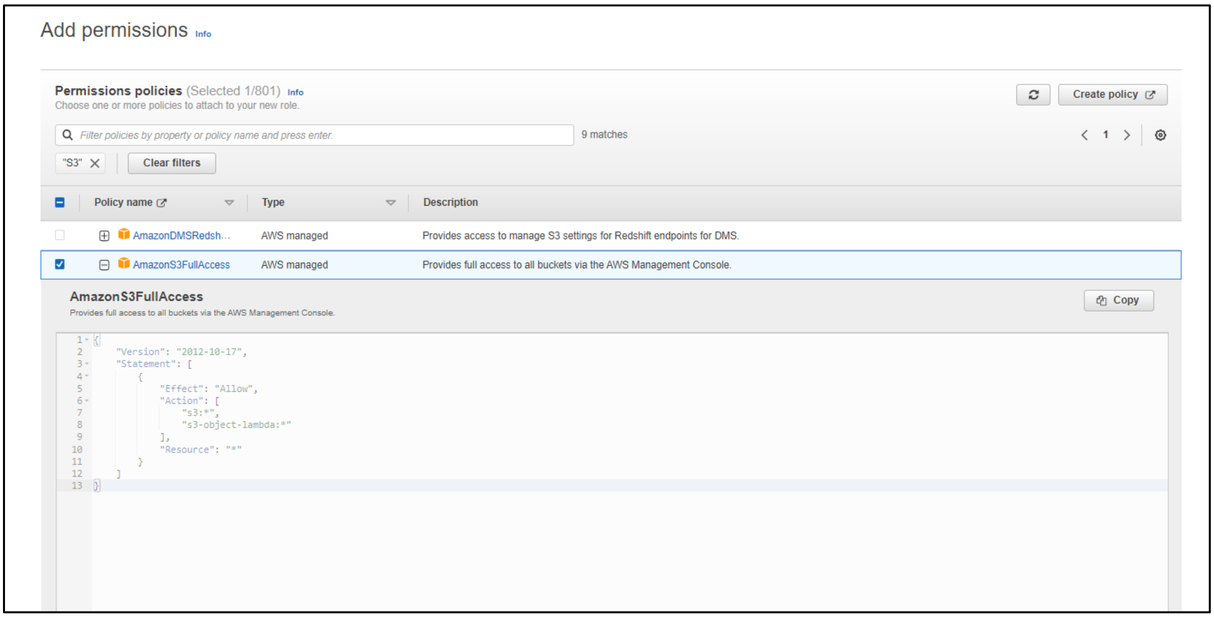
● EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

STEP1.2: Permission policiees---->IAM(eg:any service)---->amazon IAM ful acces--->next


Add permissions Info

Permissions policies (Selected 1/801) Info
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 9 matches

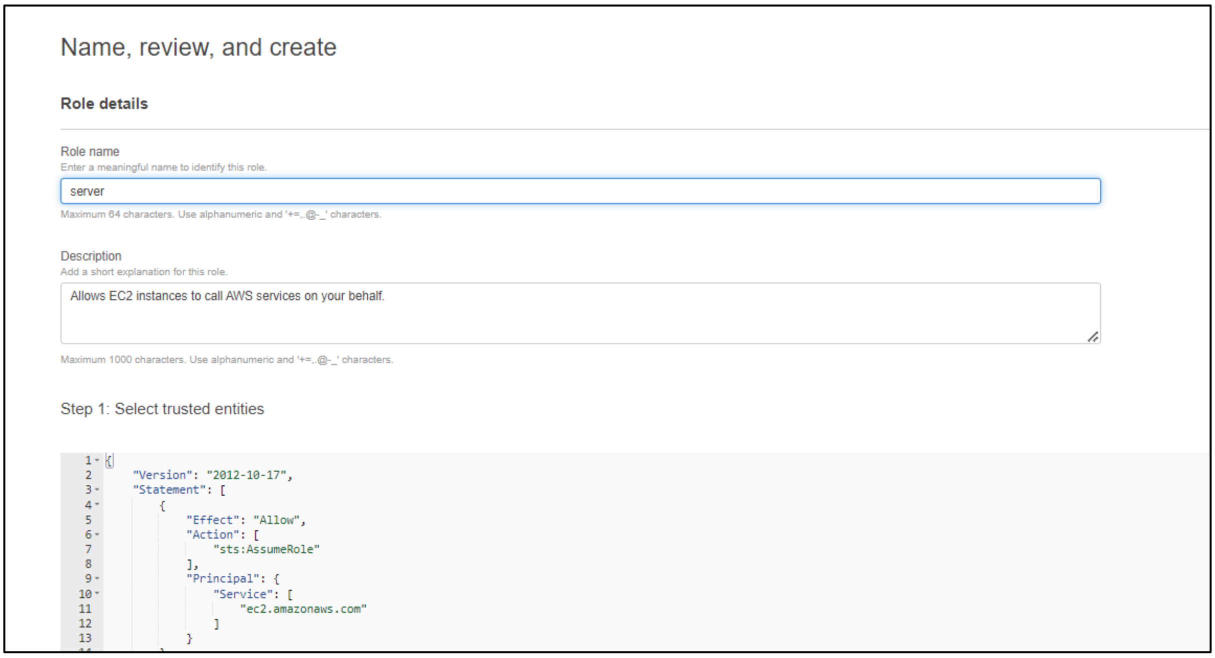
"S3" ✕ Clear filters

☐	Policy name	Type	Description
☐	⊞ AmazonDMSRedsh...	AWS managed	Provides access to manage S3 settings for Redshift endpoints for DMS.
☑	⊟ AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.

AmazonS3FullAccess
Provides full access to all buckets via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "s3-object-lambda:*"
            ],
            "Resource": "*"
        }
    ]
}
```

STEP1.3:role details--->role name(any)----->create role


Name, review, and create

Role details

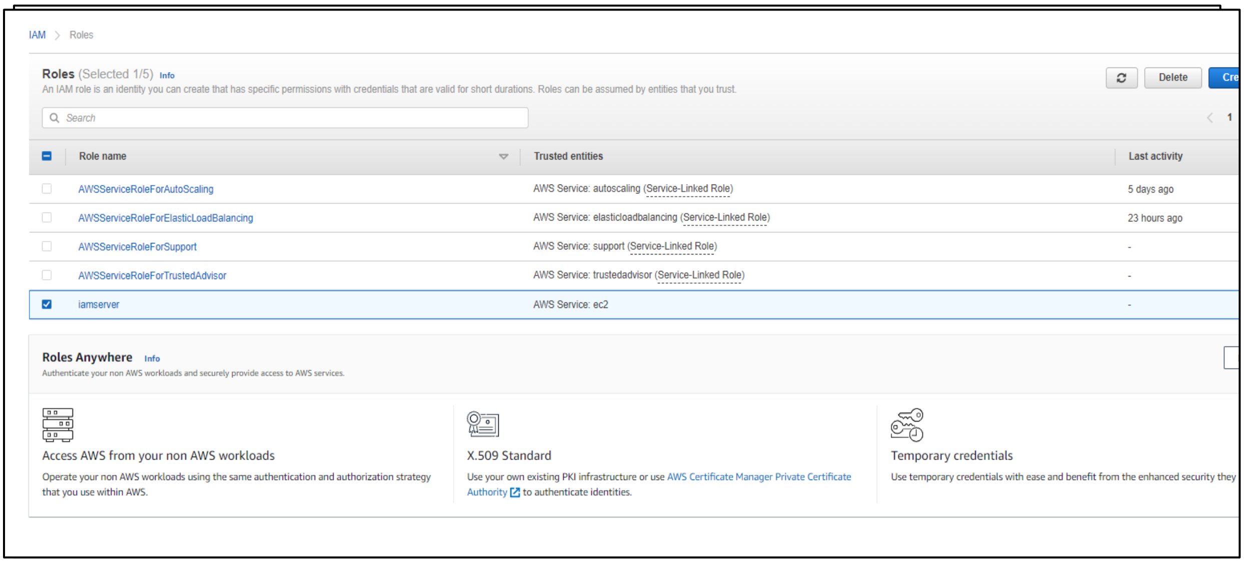
Role name
Enter a meaningful name to identify this role.
server
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
```

role created succefully...



IAM > Roles

Roles (Selected 1/5) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	5 days ago
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	23 hours ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
☑	iamserver	AWS Service: ec2	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

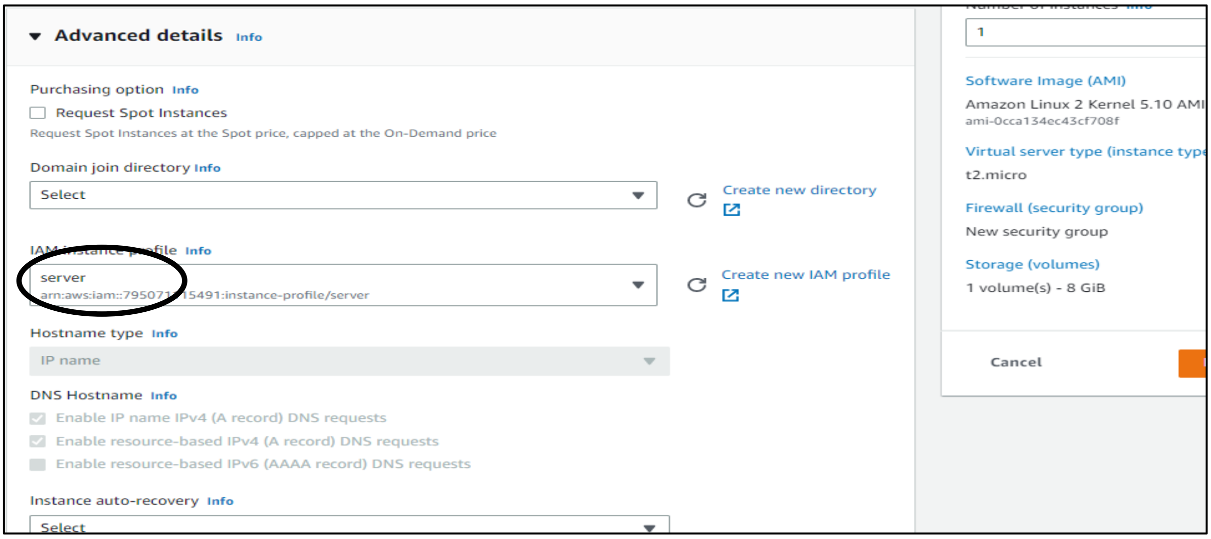
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they

STEP2: Ec2 instance create(normally one instance create)

STEP2.1:advanced details---->IAM instance profile(add)(creating iam role add)



Advanced details Info

Purchasing option Info

□ Request Spot Instances

Request Spot Instances at the Spot price, capped at the On-Demand price

Domain join directory Info

Select

Create new directory

IAM instance profile Info

server

arn:aws:iam::795071_15491:instance-profile/server

Create new IAM profile

Hostname type Info

IP name

DNS Hostname Info

☑ Enable IP name IPv4 (A record) DNS requests

☑ Enable resource-based IPv4 (A record) DNS requests

□ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery Info

Select

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI

ami-0cca134ec43cf708f

Virtual server type (instance type

t2.micro

Firewall (security group)

New security group

Storage (volumes)

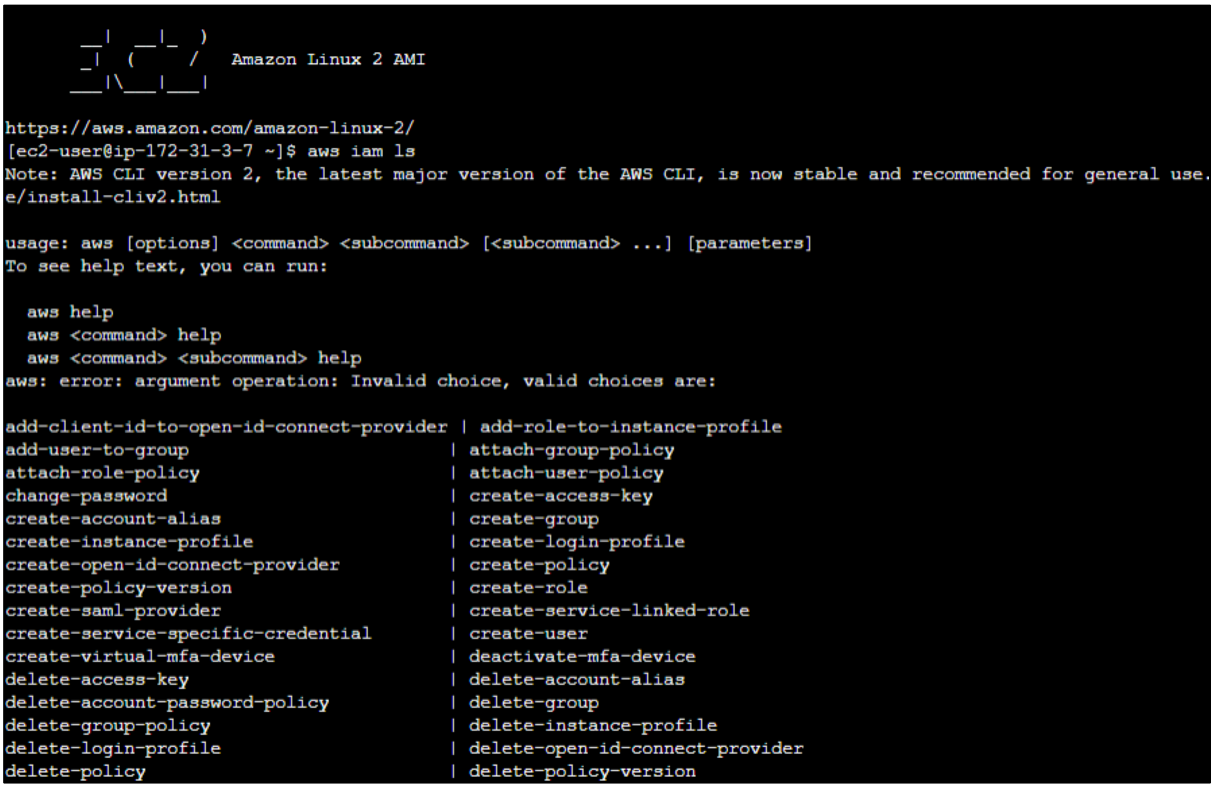
1 volume(s) - 8 GiB

STEP2.2: Launch instance

STEP2.3:AFTER LAUNCH INSTANCE--->CONNECT LINUX

----->check IAM service in linux(because IAM policy will give in roles---->step ref:1.2)

Check command:aws iam ls



```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-3-7 ~]$ aws iam ls
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use.
e/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: argument operation: Invalid choice, valid choices are:

add-client-id-to-open-id-connect-provider | add-role-to-instance-profile
add-user-to-group                        | attach-group-policy
attach-role-policy                       | attach-user-policy
change-password                          | create-access-key
create-account-alias                     | create-group
create-instance-profile                  | create-login-profile
create-open-id-connect-provider          | create-policy
create-policy-version                    | create-role
create-saml-provider                     | create-service-linked-role
create-service-specific-credential       | create-user
create-virtual-mfa-device                | deactivate-mfa-device
delete-access-key                        | delete-account-alias
delete-account-password-policy           | delete-group
delete-group-policy                      | delete-instance-profile
delete-login-profile                     | delete-open-id-connect-provider
delete-policy                            | delete-policy-version
```

After Show List Iam Servers It Will Sucsess...

MFA(MULTI FACTOR AUTHENTICATION):

AWS Identity and Access Management (IAM) best practice that requires a second authentication factor in addition to user name and password sign-in credentials.

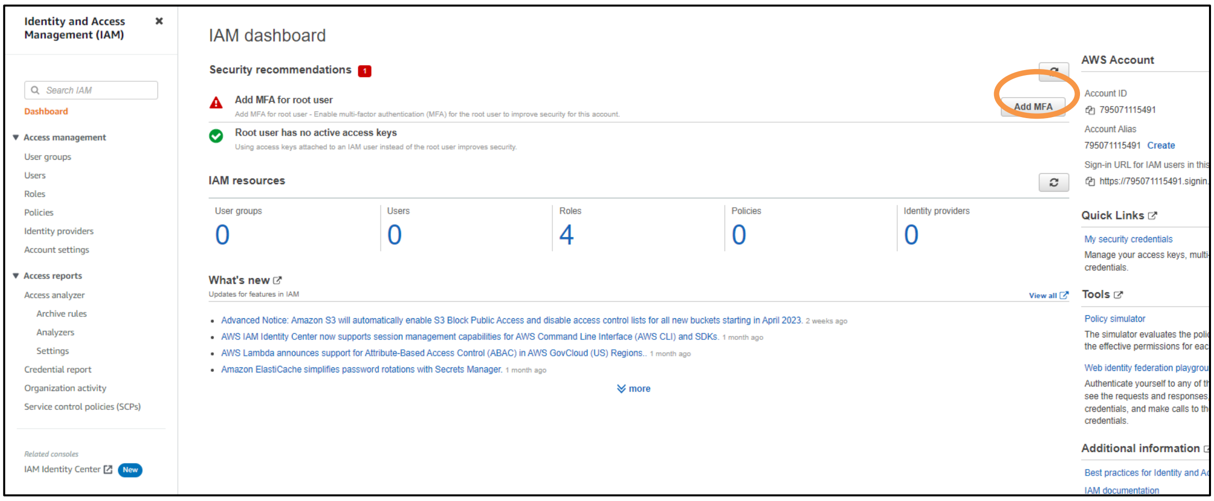
You can enable MFA at the AWS account level and for root and IAM users you have created in your account.

Two types: 1.Physical mfa (manual password)

2.Virtual mfa(fingerprint)

Steps to create MFA:

STEP1:IAM Dashboard---->Add MFA



IAM dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	4	0	0

What's new

Updates for features in IAM

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 2 weeks ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 1 month ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 1 month ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 1 month ago

AWS Account

Account ID

795071115491

Account Alias

795071115491 Create

Sign-in URL for IAM users in this

https://795071115491.signin.

My security credentials

Manage your access keys, multi credentials.

Policy simulator

The simulator evaluates the poli the effective permissions for eac

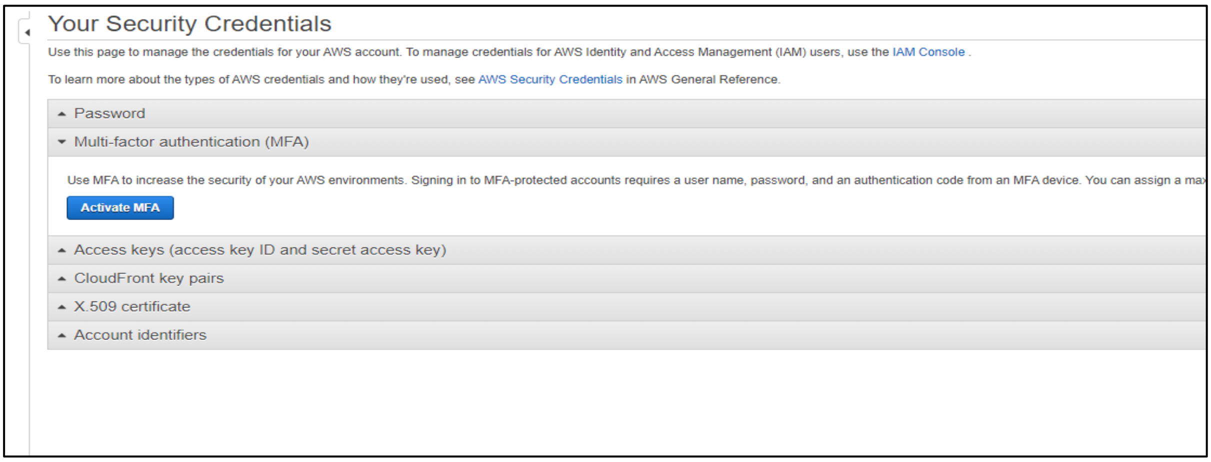
Web identity federation playgrou

Authenticate yourself to any of th see the requests and responses credentials, and make calls to th credentials.

Best practices for Identity and Ac

IAM documentation

STEP2: Activate MFA


Password
Multi-factor authentication (MFA)
Activate MFA
Access keys (access key ID and secret access key)
CloudFront key pairs
X.509 certificate
Account identifiers

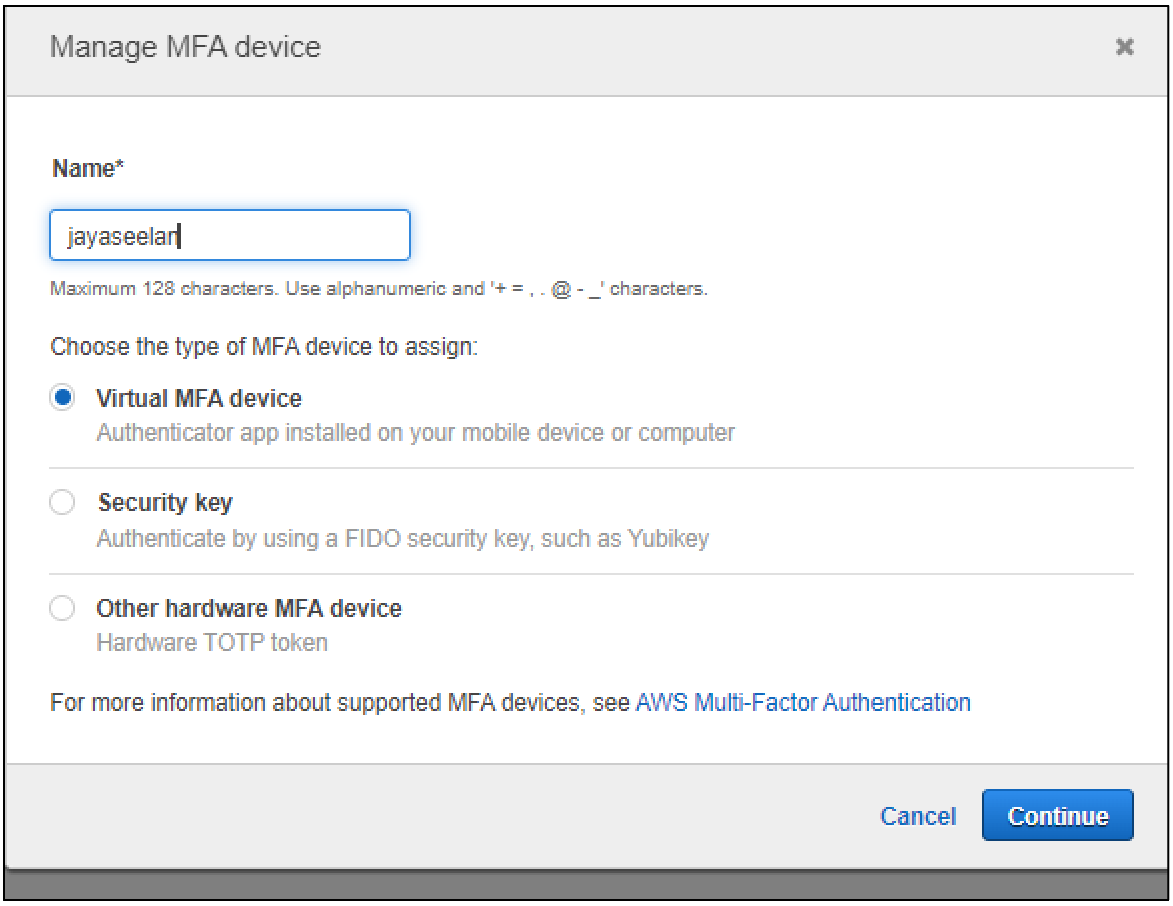
Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device. You can assign a ma

STEP3: Name any--->virtual MFA device --->continue



Manage MFA device

Name*

jayaseelan

Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

Choose the type of MFA device to assign:

● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

○ **Security key**
Authenticate by using a FIDO security key, such as Yubikey

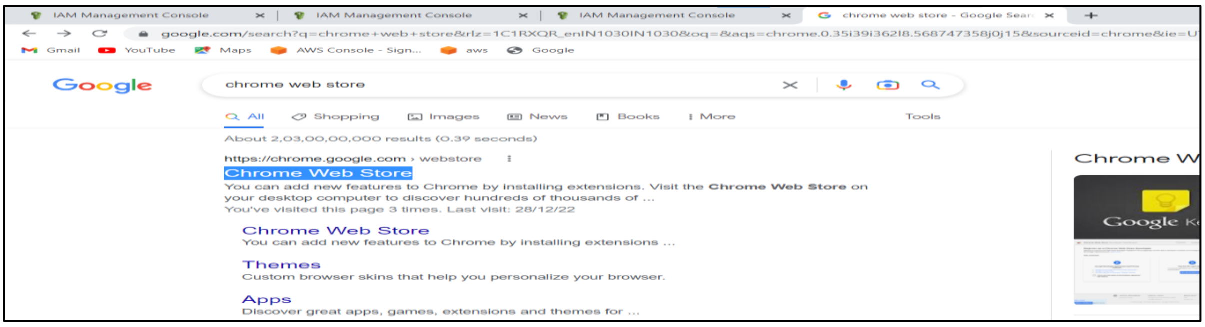
○ **Other hardware MFA device**
Hardware TOTP token

For more information about supported MFA devices, see AWS Multi-Factor Authentication

STEP4:barcode shown----->scan barcode auntheticator--->otp will show--->15 sec otp change two otp put..

How to download authenticator:

Chrome webstore---->search(authenticator)--->shown authenticator application --->click--->add to chrome.



google.com/search?q=chrome+web+store&rlz=1C1RXQR_enIN1030IN1030&oq=&aqs=chrome.0.35i39i362l8.568747358j0j15&sourceid=chrome&ie=U

chrome web store

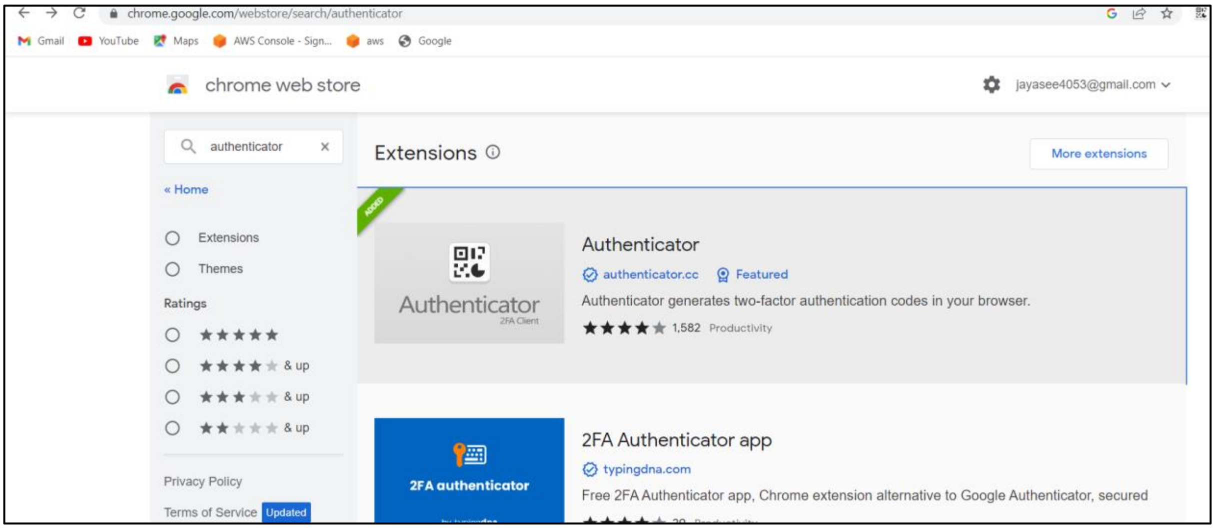
About 2,03,00,00,000 results (0.39 seconds)

https://chrome.google.com › webstore
Chrome Web Store
You can add new features to Chrome by installing extensions. Visit the **Chrome Web Store** on your desktop computer to discover hundreds of thousands of ...
You've visited this page 3 times. Last visit: 28/12/22

Chrome Web Store
You can add new features to Chrome by installing extensions ...

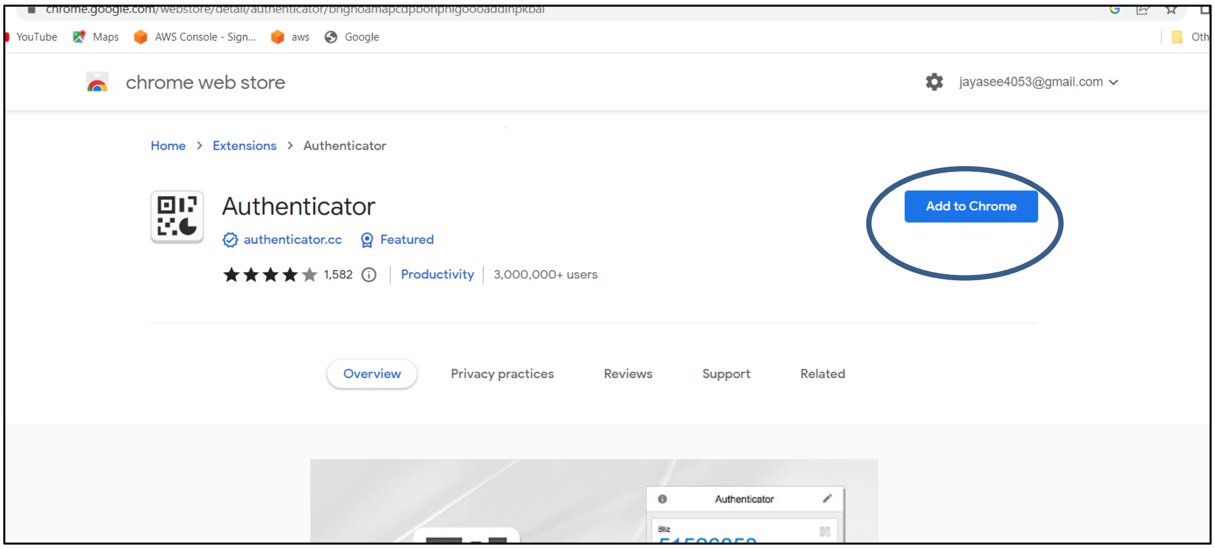
Themes
Custom browser skins that help you personalize your browser.

Apps
Discover great apps, games, extensions and themes for ...


chrome.google.com/webstore/search/authenticator

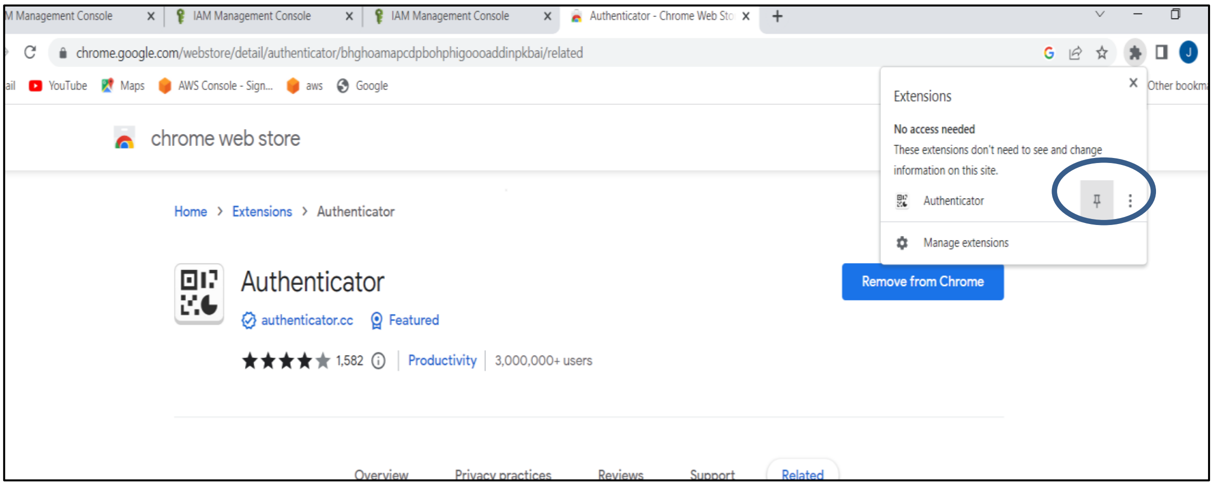
Authenticator
authenticator.cc Featured
Authenticator generates two-factor authentication codes in your browser.
★★★★★ 1,582 Productivity

2FA Authenticator app
typingdna.com
Free 2FA Authenticator app, Chrome extension alternative to Google Authenticator, secured


chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai

Authenticator
authenticator.cc Featured
★★★★★ 1,582 | Productivity | 3,000,000+ users

Authenticator download after---->pin to chrome corner..


chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai/related

No access needed
These extensions don't need to see and change information on this site.

Authenticator
authenticator.cc Featured
★★★★★ 1,582 | Productivity | 3,000,000+ users