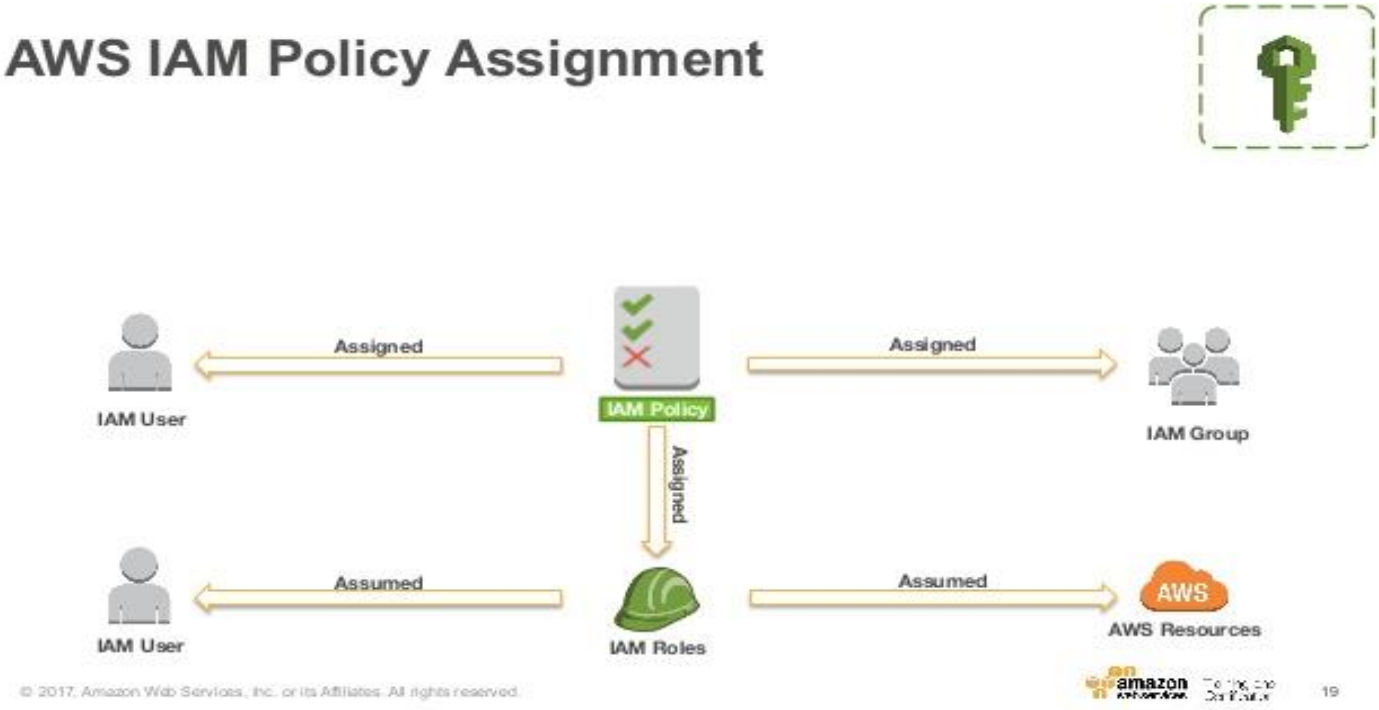
There are 4 components in IAM

Users

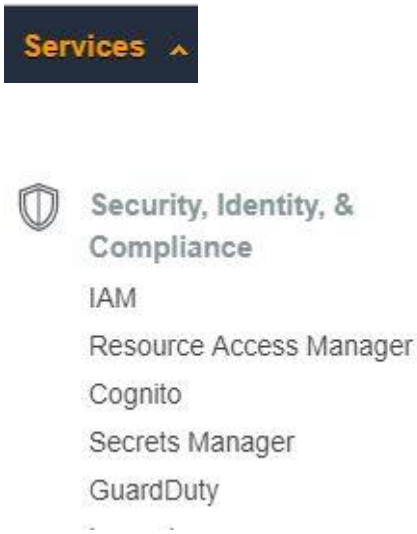
Group

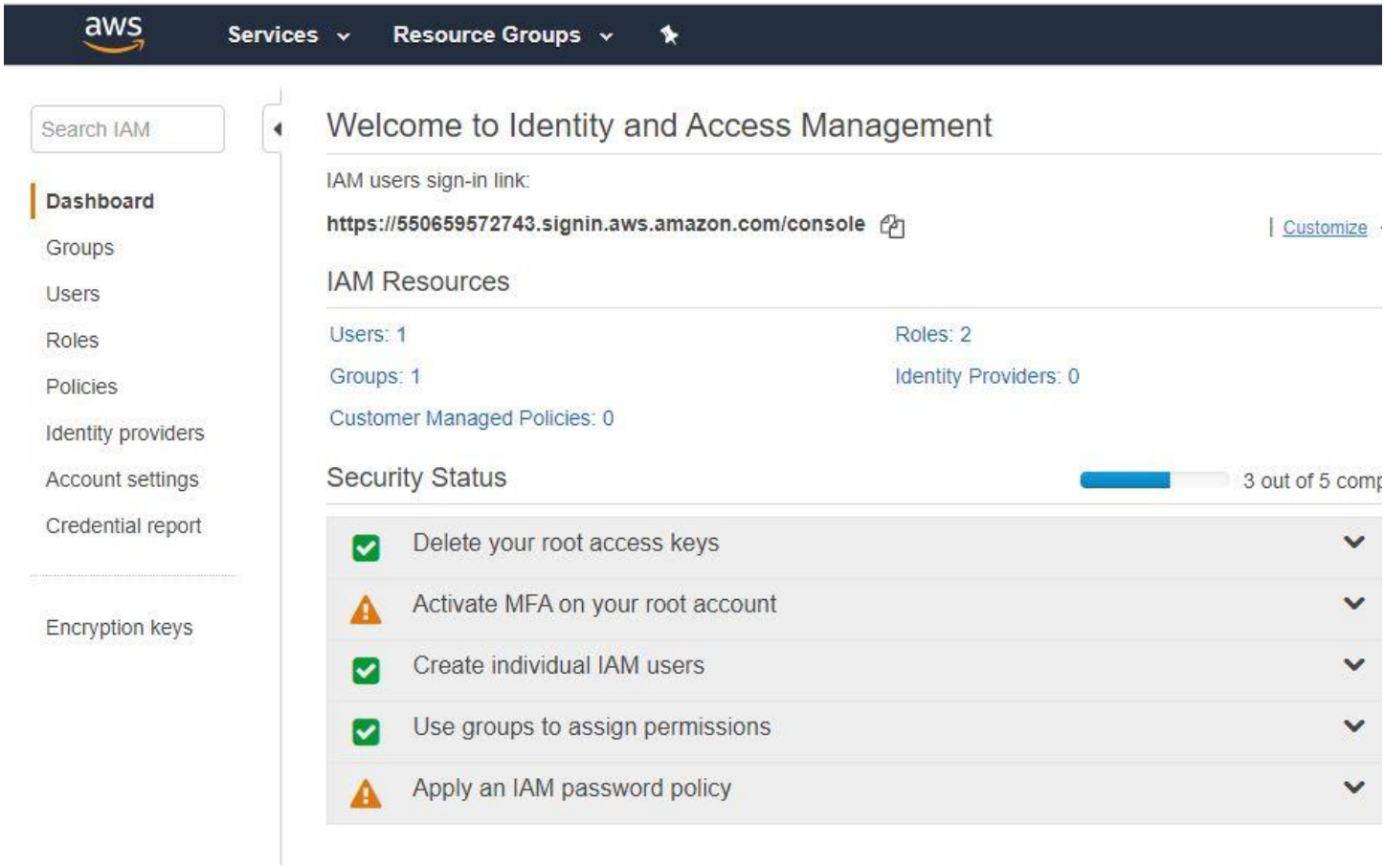
Roles

Policies



Step 1: Open IAM in services tab

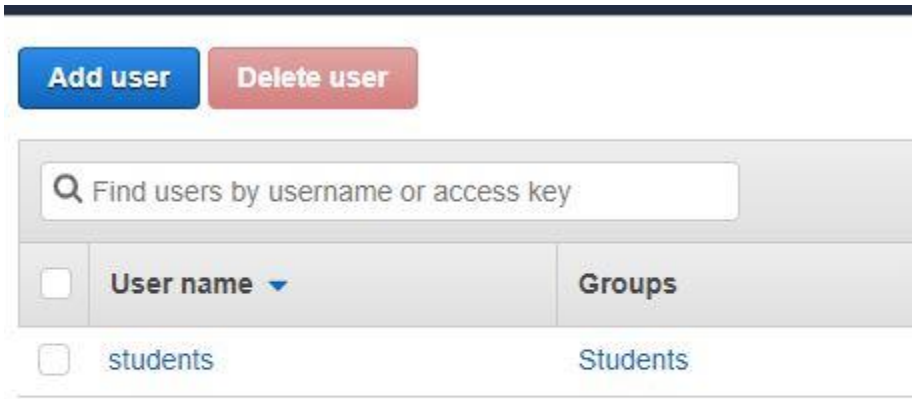




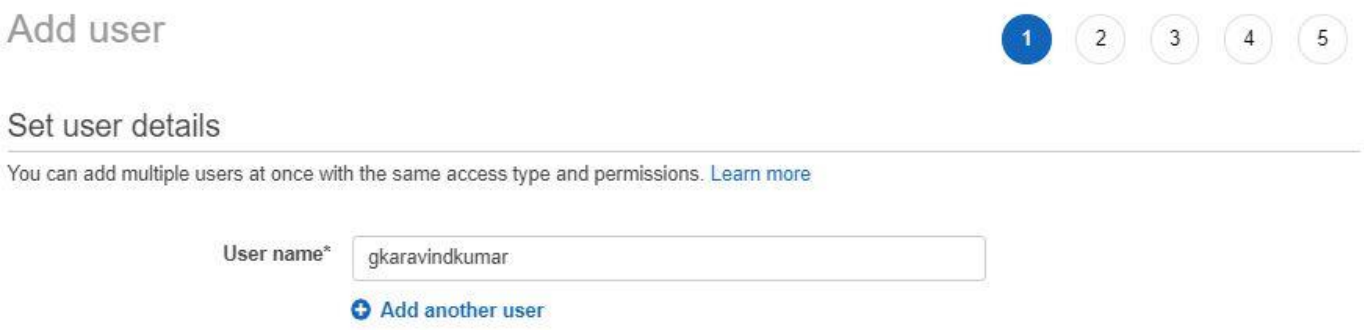
You can see the dashboard of IAM and you will see the URL link for IAM users

Step 2 create a user with group attach the policies to group.

Click Add user button



Enter Username



Select the Access type and password details

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ◉ Autogenerated password
○ Custom password

Require password reset ☑ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

Cancel | **Next: Permissions**

Next add a group click “Create group”

Add user

1 2 3 4 5

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

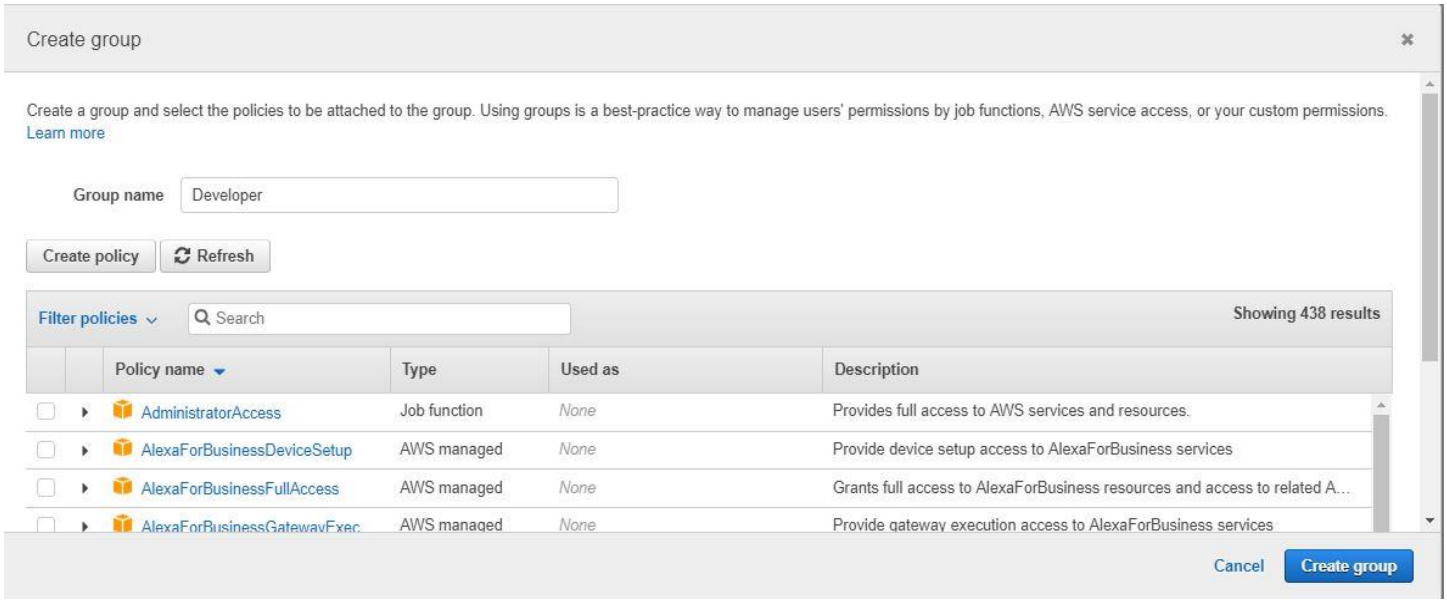
Create group | Refresh

Search

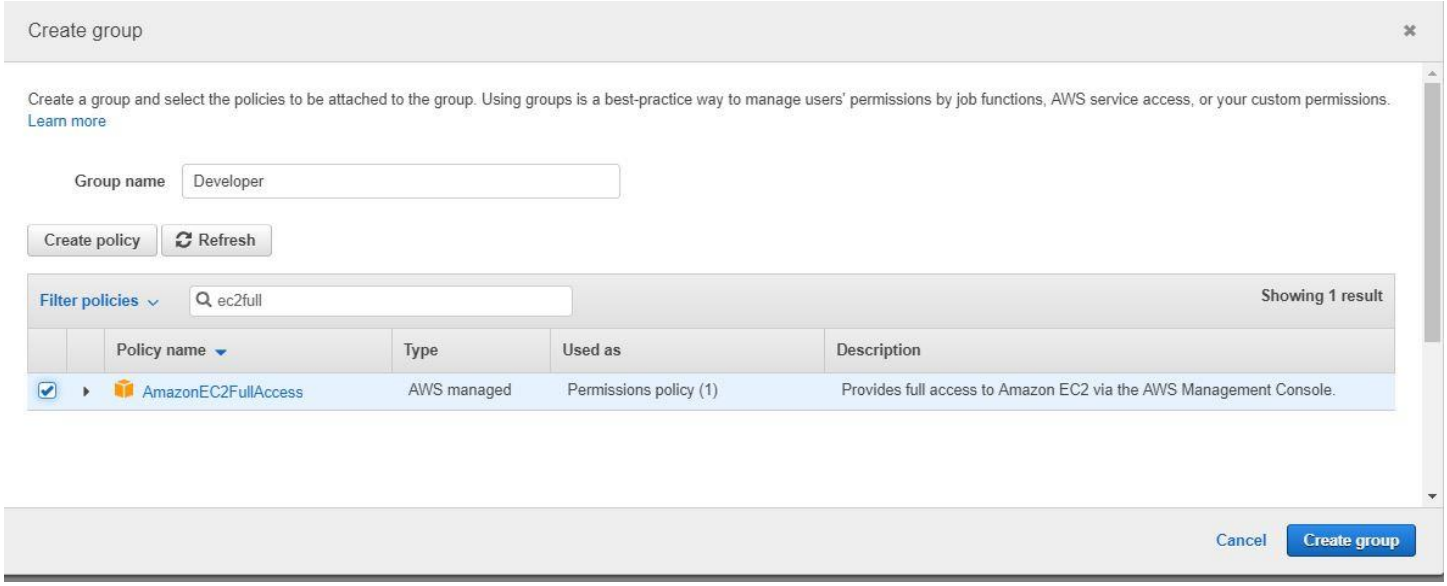
Showing 1 result

Group	Attached policies
Students	AmazonS3ReadOnlyAccess

Give a group name



Search the related policies in default policies and attach it to the group



Attach the user to the respective group

Add user

1 2 3 4 5

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

Create group | Refresh

Search

Showing 2 results

Group	Attached policies
Developer	AmazonEC2FullAccess
Students	AmazonS3ReadOnlyAccess

Attach Name tag

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
Name	aravind	✖
Add new key		

You can add 49 more tags.

Cancel | Previous | Next: Review

Review the details and create user wit group

User details

User name	gkaravindkumar
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
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	Developer
Managed policy	IAMUserChangePassword

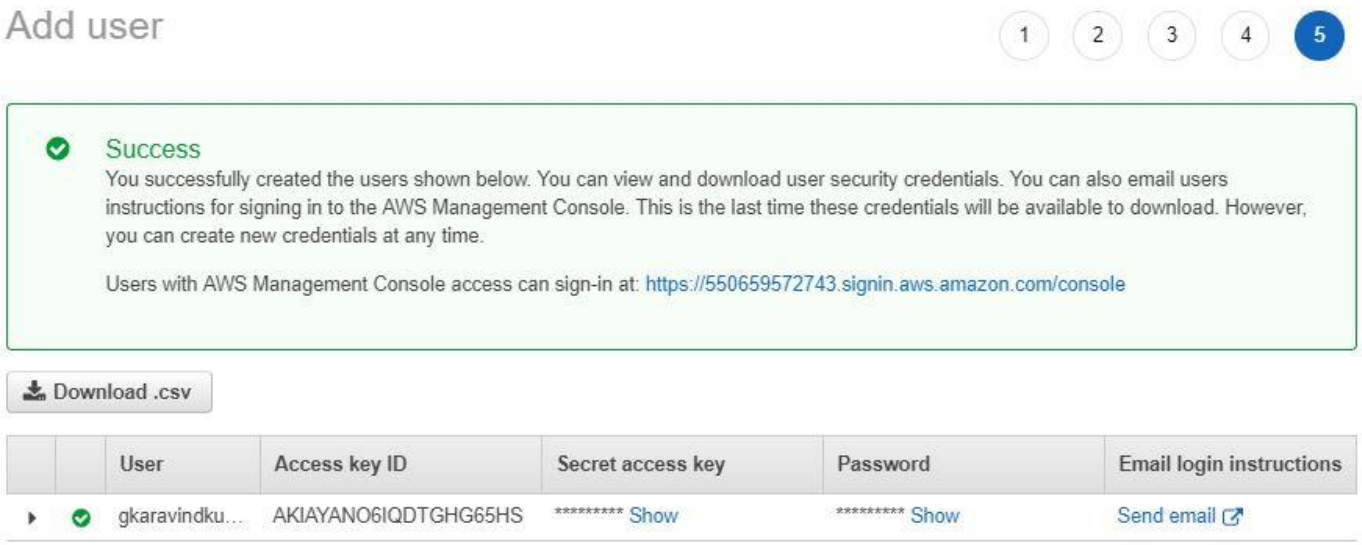
Tags

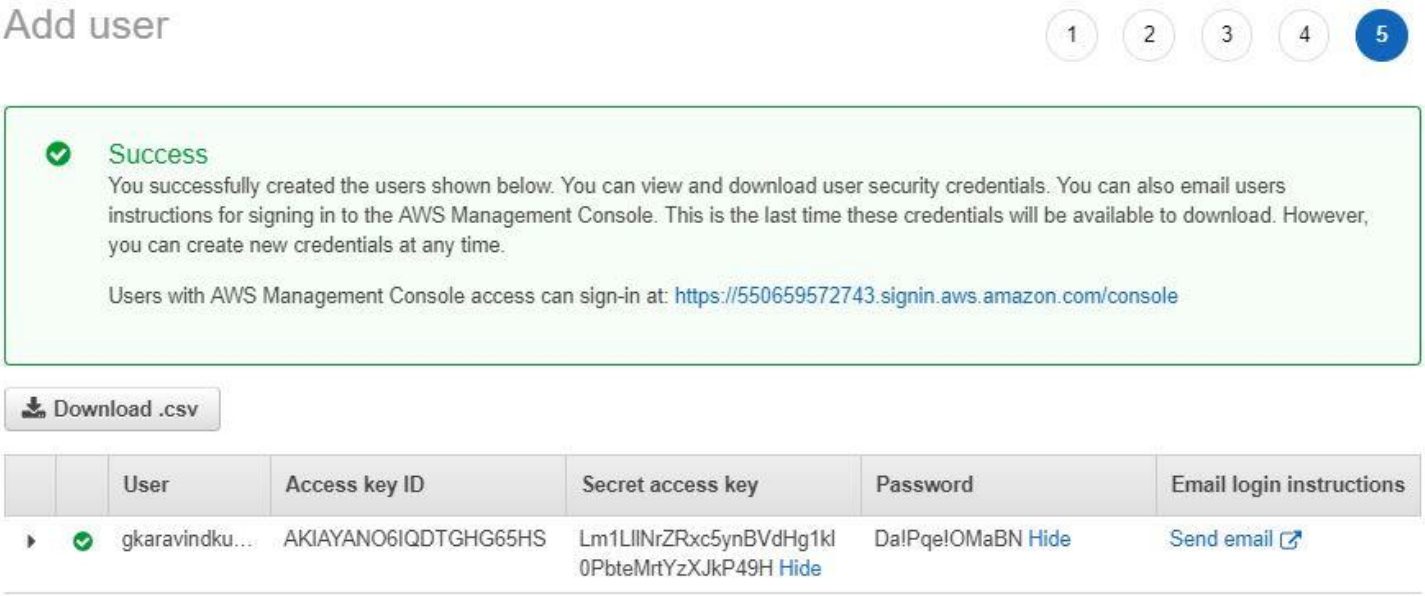
The new user will receive the following tag

Key	Value
Name	aravind

Cancel Previous Create user

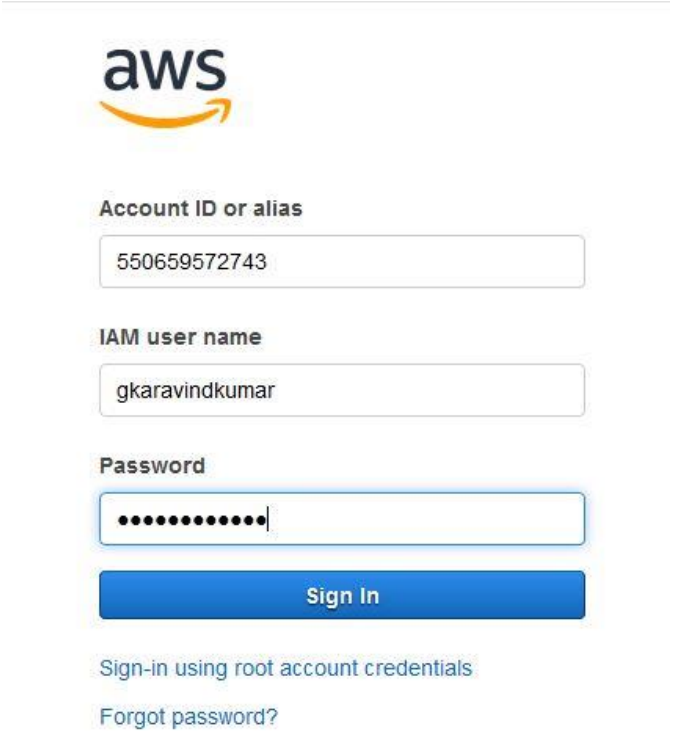
The user will be created and it shows the secret key and password only once you should copy it and you can't able to see it again



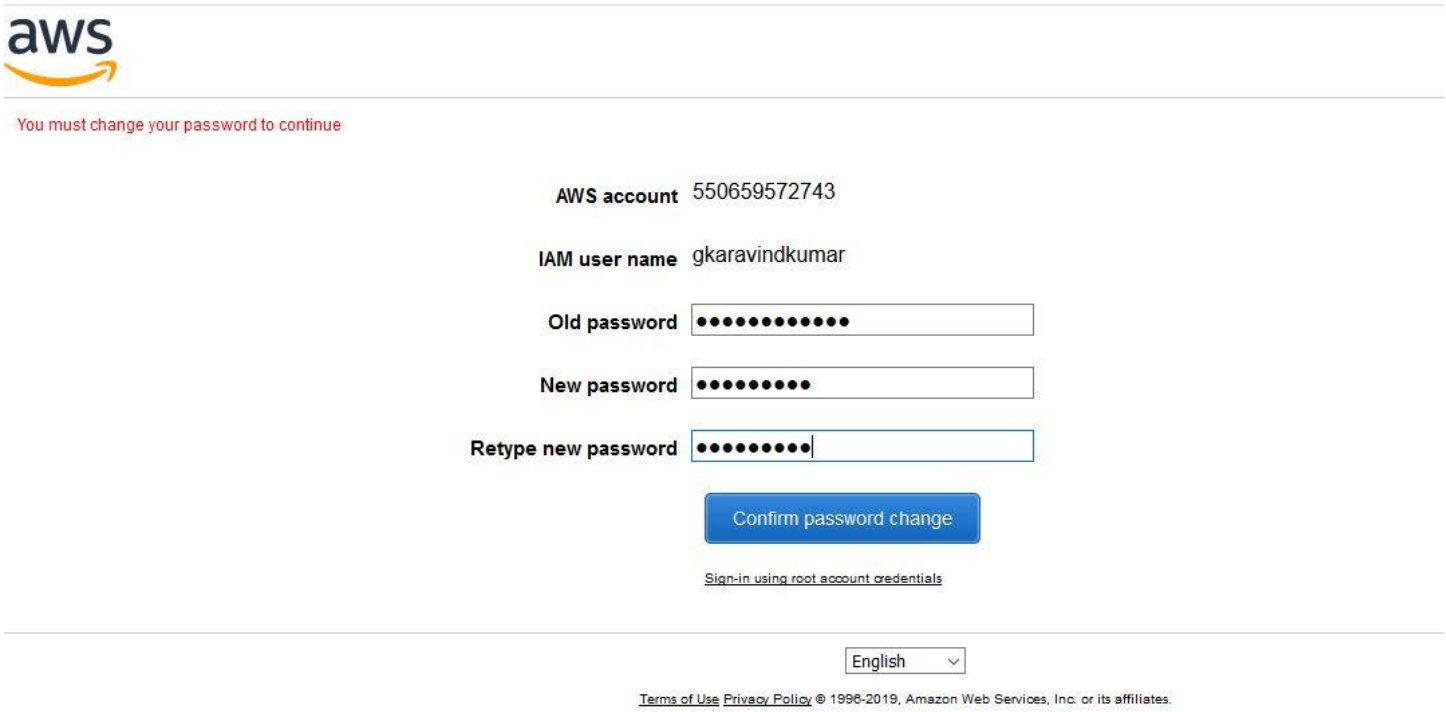


Now you User will be shown in the list

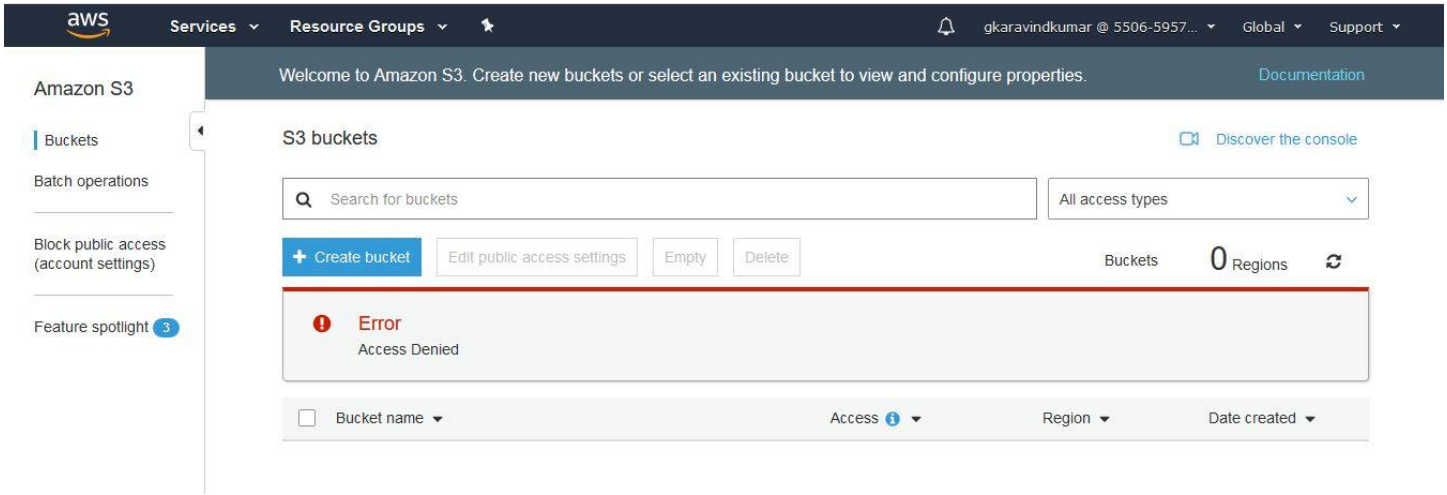
Step3: Check the user by login the console



It ask for password change if you selected this option while creating

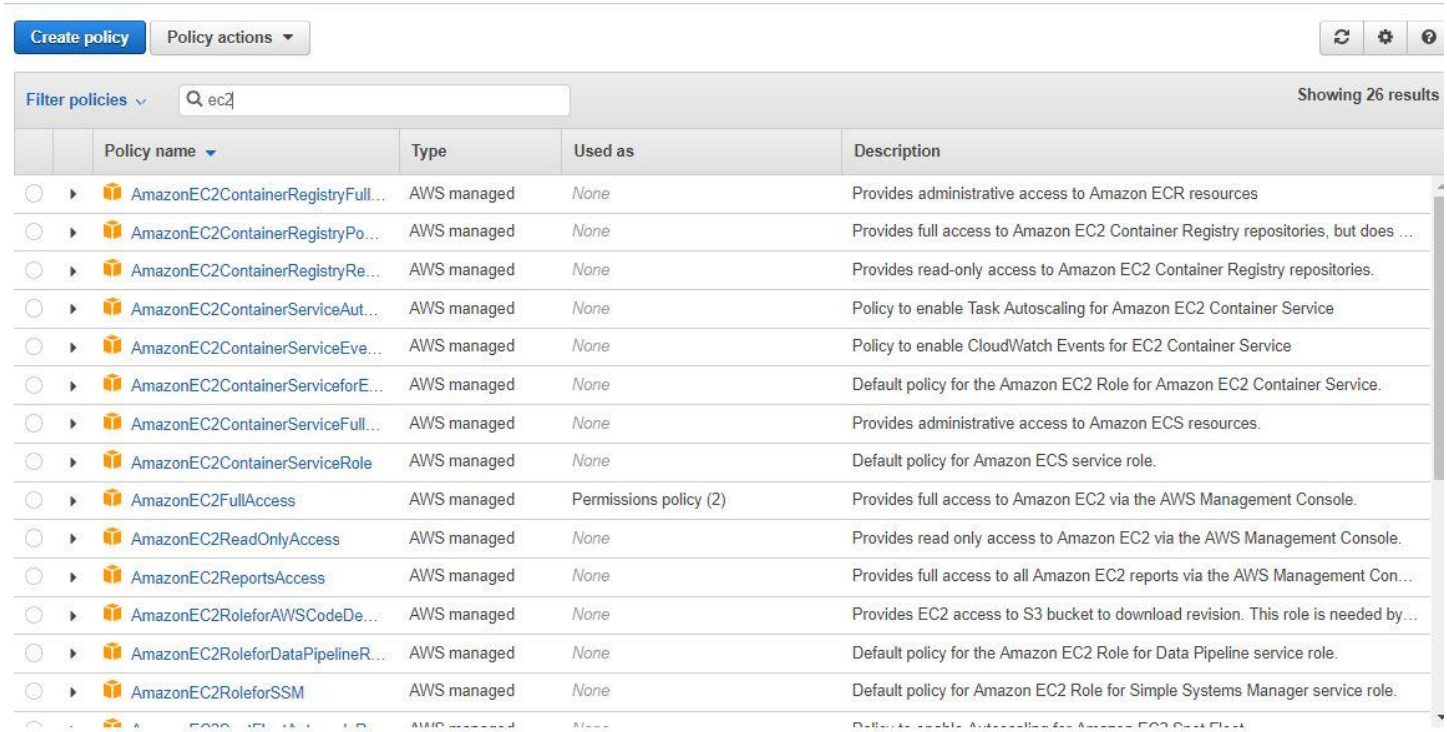


Check the permissions of the user it dot have rights to other services except EC2.



Policies

Step 4:Create a new policy and attaching it to a group. Goto policies > create Policy



You can use JASON script if you have or create policy in UI.

Create policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

This policy validation failed and might have errors converting to Visual editor : Could not parse the policy: Statement is empty! For more information about the IAM policy grammar, see AWS IAM Policies

Visual editor | JSON | Import managed policy

Expand all | Collapse all

Select a service | Clone | Remove

Service Choose a service

Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

Add additional permissions

Select the service

Visual editor | JSON | Import managed policy

Expand all | Collapse all

Select a service | Clone | Remove

Service Select a service below | Enter service manually

close

ec2

EC2 | EC2 Auto Scaling | EC2 Messages

Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

Add additional permissions

Cancel | Review policy

Choose the Action

Service EC2

Actions List

DescribeAccountAttributes	DescribeImportImageTasks	DescribeSpotFleetRequestHistory
DescribeAddresses	DescribeImportSnapshotTasks	DescribeSpotFleetRequests
DescribeAggregateIdFormat	DescribeInstanceAttribute	DescribeSpotInstanceRequests
DescribeAvailabilityZones	DescribeInstanceCreditSpecifications	DescribeSpotPriceHistory
DescribeBundleTasks	DescribeInstances	DescribeStaleSecurityGroups
DescribeByoipCidrs	DescribeInstanceStatus	DescribeSubnets
DescribeCapacityReservations	DescribeInternetGateways	DescribeTransitGatewayAttachments
DescribeClassicLinkInstances	DescribeKeyPairs	DescribeTransitGatewayRouteTables
DescribeClientVpnAuthorizationRules	DescribeLaunchTemplates	DescribeTransitGateways
DescribeClientVpnConnections	DescribeLaunchTemplateVersions	DescribeTransitGatewayVpcAttachments
DescribeClientVpnEndpoints	DescribeMovingAddresses	DescribeVolumeAttribute
DescribeClientVpnRoutes	DescribeNatGateways	DescribeVolumes
DescribeClientVpnTargetNetworks	DescribeNetworkAcls	DescribeVolumeStatus
DescribeConversionTasks	DescribeNetworkInterfaceAttribute	DescribeVpcAttribute
DescribeCustomerGateways	DescribeNetworkInterfacePermissions	DescribeVpcClassicLink
DescribeDhcpOptions	DescribeNetworkInterfaces	DescribeVpcClassicLinkDnsSupport
DescribeEgressOnlyInternetGateways	DescribePlacementGroups	DescribeVpcEndpointConnectionNotifications
DescribeExportTasks	DescribePrefixLists	DescribeVpcEndpointConnections
DescribeFleetHistory	DescribePrincipalIdFormat	DescribeVpcEndpoints
DescribeFleetInstances	DescribePublicIpv4Pools	DescribeVpcEndpointServiceConfigurations
DescribeFleets	DescribeRegions	DescribeVpcEndpointServicePermissions
DescribeFlowLogs	DescribeReservedInstances	DescribeVpcEndpointServices
DescribeFpgaImageAttribute	DescribeReservedInstancesListings	DescribeVpcPeeringConnections
DescribeFpgaImages	DescribeReservedInstancesModifications	DescribeVpcs
DescribeHostReservationOfferings	DescribeReservedInstancesOfferings	DescribeVpnGateways
DescribeHostReservations	DescribeRouteTables	ExportClientVpnClientCertificateRevocationList

Set condition

Request conditions
close

- [ ] **MFA required**
  Requires users to authenticate with an MFA device to perform the specified actions
- [ ] **Source IP**
  Allow access to the specified actions only when the request comes from the specified IP address range.

Add condition

Edit request condition

Condition key	ec2:Region	
Qualifier	For any value in request	
Operator	StringEquals	If exists
Value	N.Virginia	

Add another condition value

Cancel Save changes

EC2 (107 actions) Clone | Remove

Service EC2

Actions Specify the actions allowed in EC2 Switch to deny permissions

close

Filter actions

Manual actions (add actions)

All EC2 actions (ec2:*)

Access level Expand all | Collapse all

List (95 selected)

Read (12 selected)

Tagging

Write

Resources All resources

Request conditions ec2:Region (StringEquals *N. Virginia*)

Add additional permissions

Cancel Review policy

Review and create Policy

Review policy

Name* Testpolicy

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

Description Providing access to North Virginia

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 177 services) Show remaining 176			
EC2	Full: List, Read	All resources	ec2:Region = N.Virginia

* Required

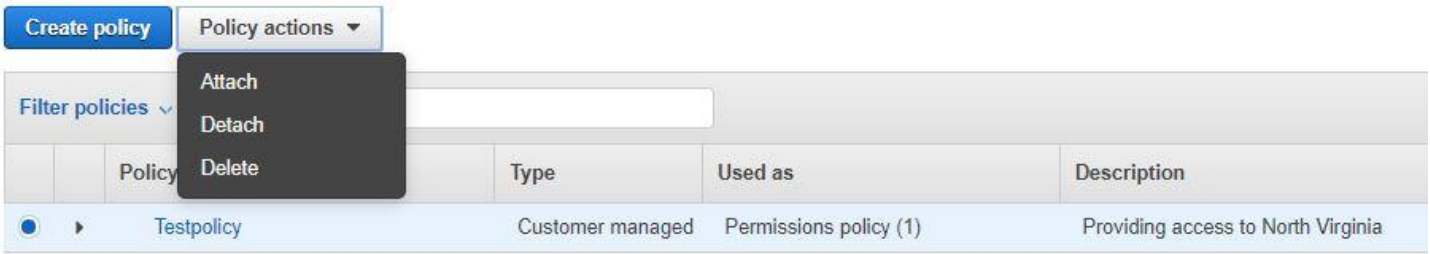
Cancel Previous Create policy

Testpolicy has been created.

Create policy Policy actions

Filter policies ec2 Showing 26 results

Policy name	Type	Used as	Description
AmazonEC2ContainerRegistryFu...	AWS managed	None	Provides administrative access to Amazon ECR resources
AmazonEC2ContainerRegistryPo...	AWS managed	None	Provides full access to Amazon EC2 Container Registry repositories, but doe...
AmazonEC2ContainerRegistryR...	AWS managed	None	Provides read-only access to Amazon EC2 Container Registry repositories.

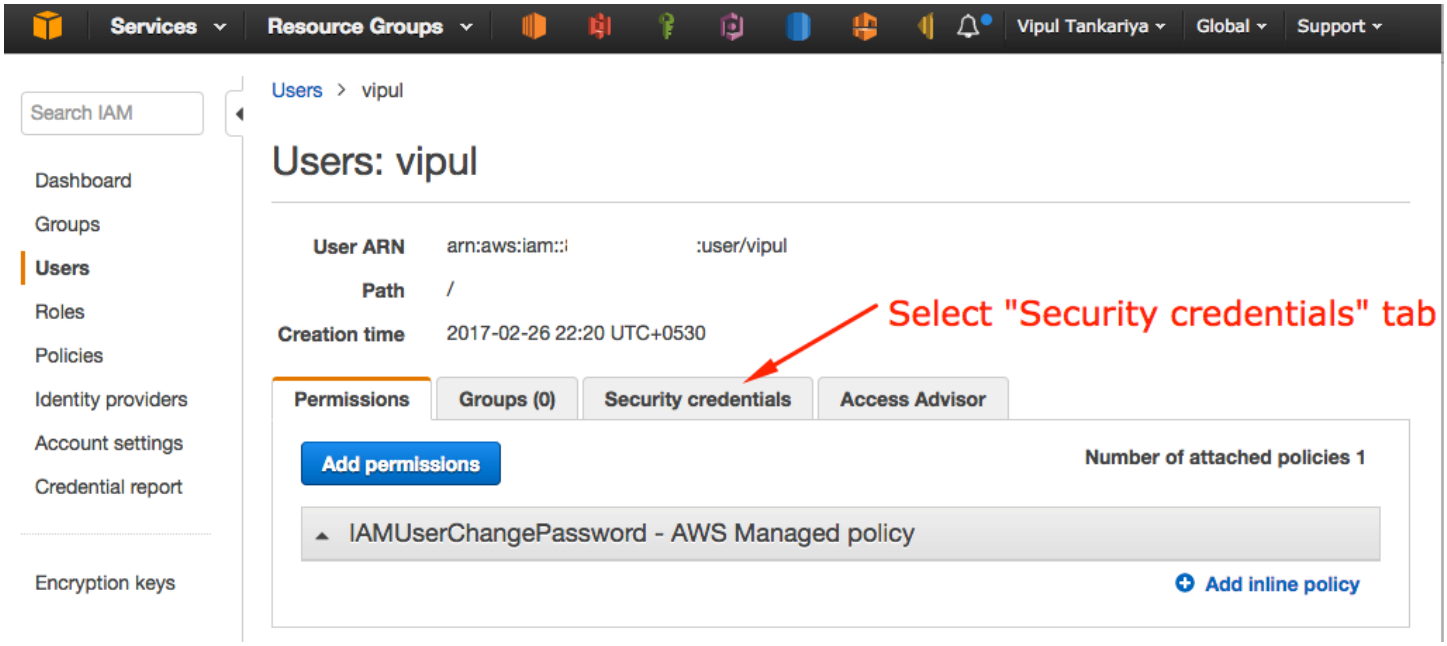


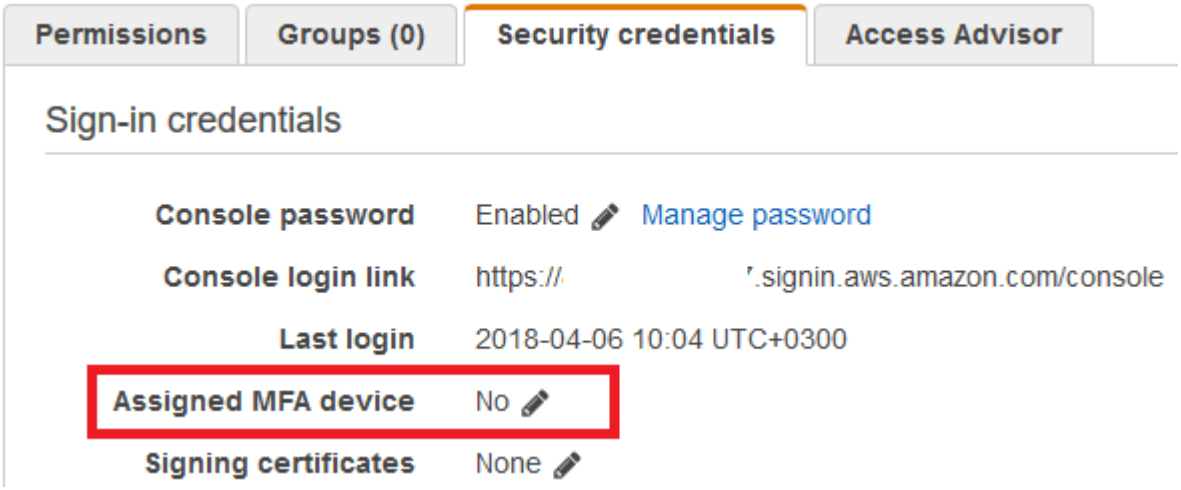
Use "**Attach**" to attach the policy to a group.

Adding MFA to a user

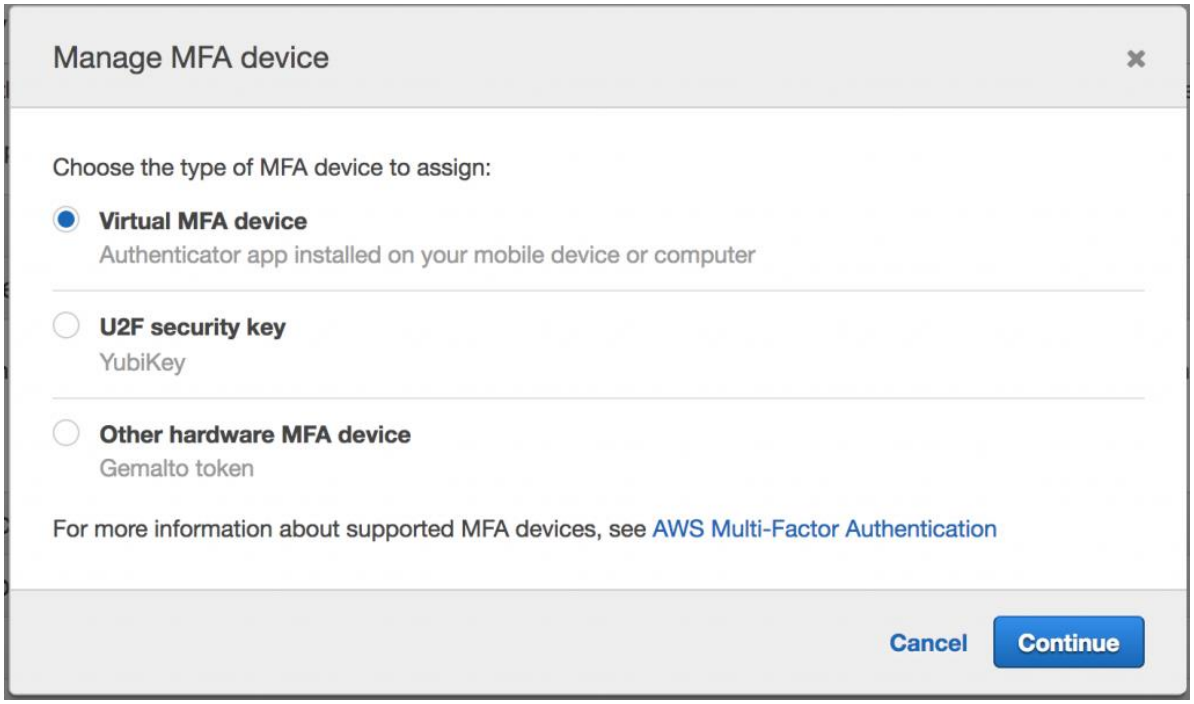
MFA is a additional authendication for user you can add mobile device of user to avoid hacking.

Go to user in the security credentials you find MFA



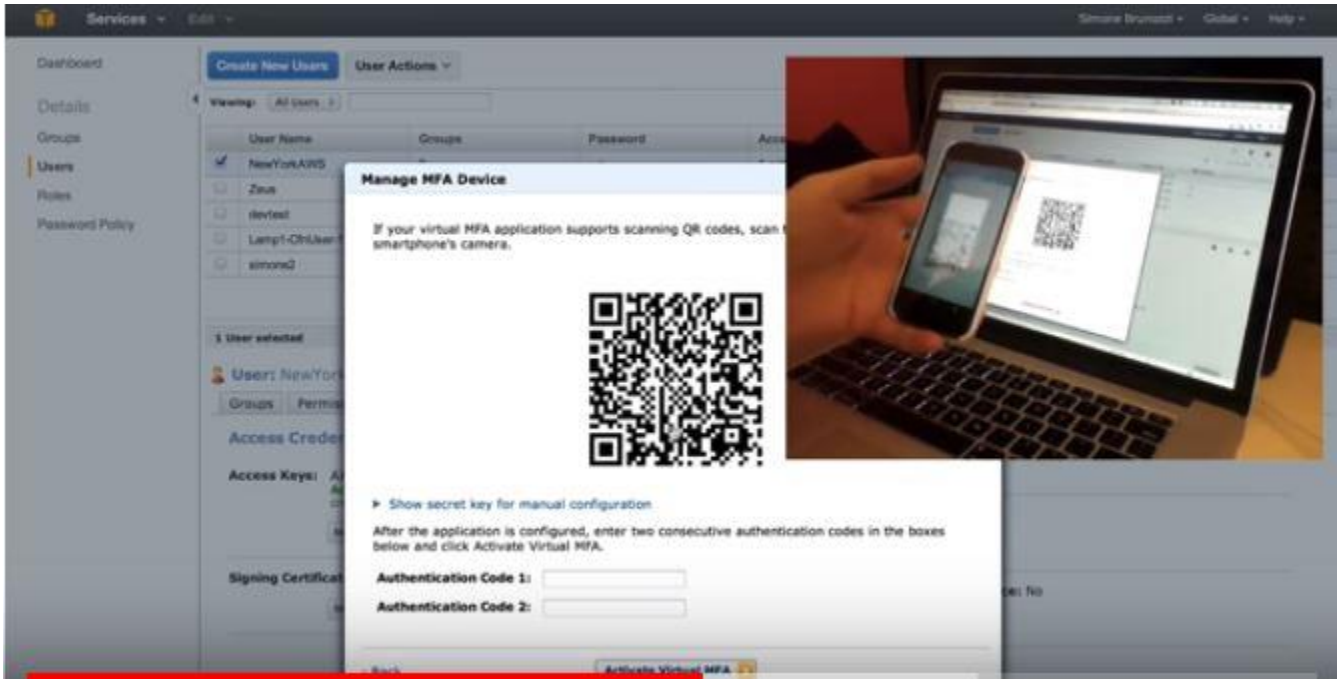


Edit “Assigned MFA device” and select “Virtual MFA device”

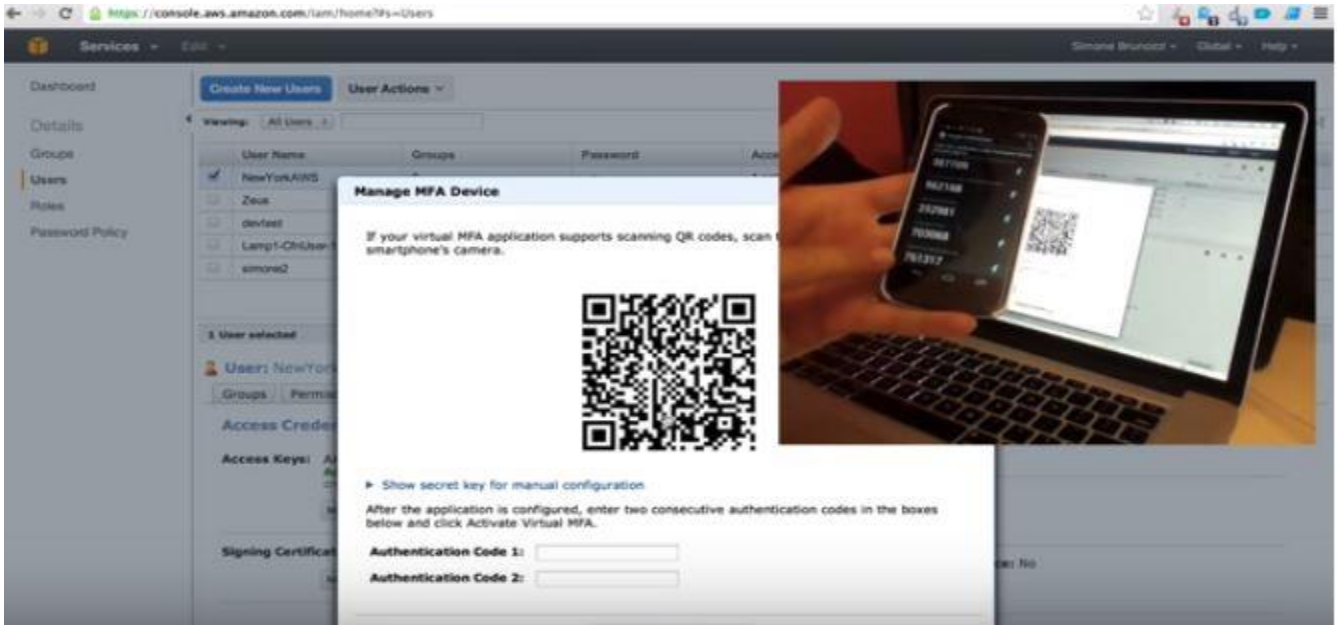


Install Google Authendicator in your mobile.

You will get a QR code scan using mobile.



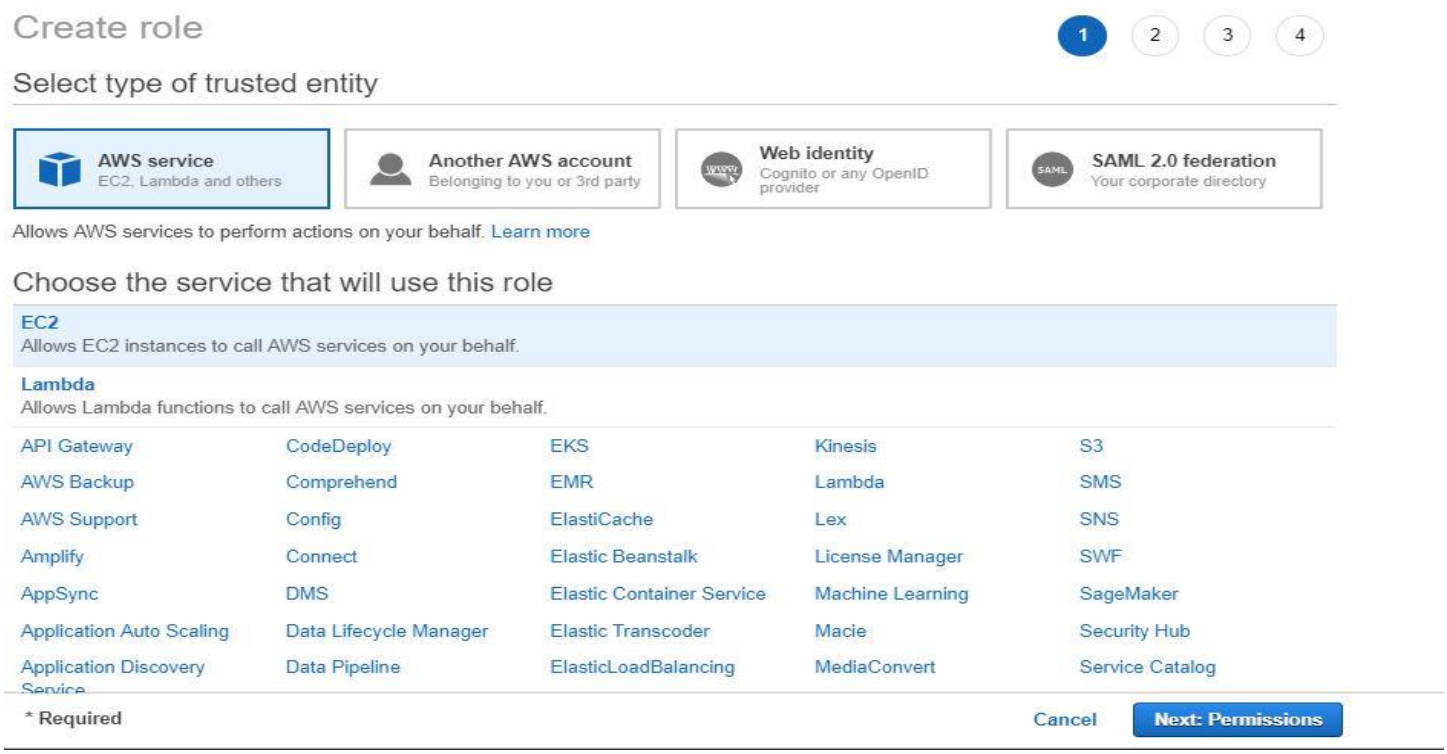
Once your code get scanned you will be getting code in your app enter that code your device will be added and you will be geeting this code automatically.



Then your code will be keep on changing user the current code to login while it through MFA authendication.

ROLES:

Create a role and Assign it to a EC2 instance Go to Roles and select service you are going to assign



Next Add permission to the selected service

Create role

1 2 3 4

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies s3full

Showing 1 result

	Policy name	Used as	Description
☑	AmazonS3FullAccess	None	Provides full access to all buckets via the...

Set permissions boundary

* Required

Cancel Previous Next: Tags

Next Add tags

Create role

1 2 3 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. 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 role. Learn more

Key	Value (optional)	Remove
name	full s3	✖
Add new key		

You can add 49 more tags.

Review the Role and create role

Review

Provide the required information below and review this role before you create it.

Role name* s3_test

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
name	full s3

* Required

Cancel | Previous | Create role

Assign a Role to the EC2 instance

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability
	d7b351d	t2.micro	us-east-1d
	1ed148	t2.micro	us-east-1d

Connect
Get Windows Password
Create Template From Instance
Launch More Like This
Instance State
Instance Settings
Image
Networking
CloudWatch Monitoring

Add/Edit Tags
Attach to Auto Scaling Group
Attach/Replace IAM Role
Change Instance Type
Change Termination Protection
View/Change User Data
Change Shutdown Behavior
Change T2/T3 Unlimited
Get System Log
Get Instance Screenshot
Modify Instance Placement
Modify Capacity Reservation Settings

Instance: i-02aac0ba44d7b351d (Ansib

Description | Status Checks | Mon

Instance ID i-02aa
Instance state stopp
Instance type t2.mic
Elastic IPs

Now this EC2 instance have full access to S3 bucket.

Try by creating different Roles

---------- END of the Document----------