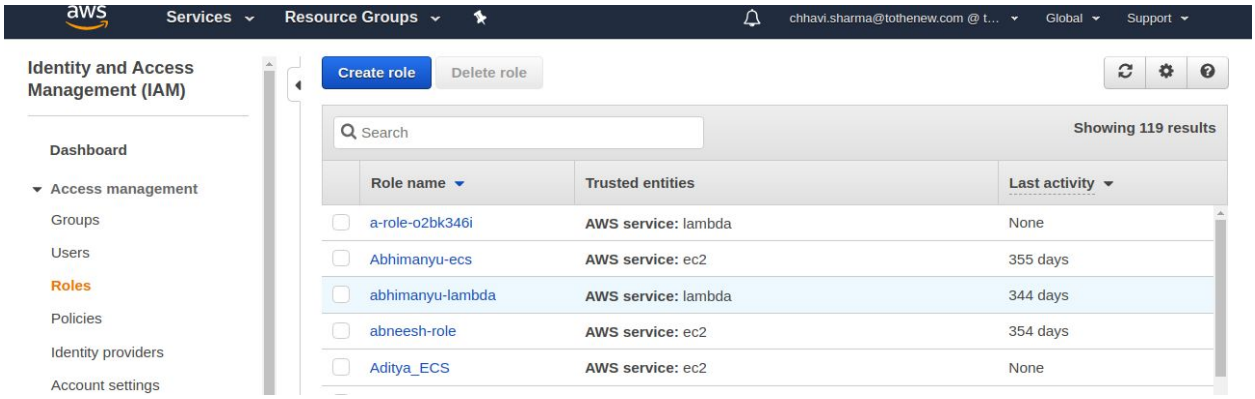
IAM and AWS CLI

Trainee Name : Chhavi Sharma
Newers ID : 4023
Mentor Name : Nishith Kulshrestha
College : UPES

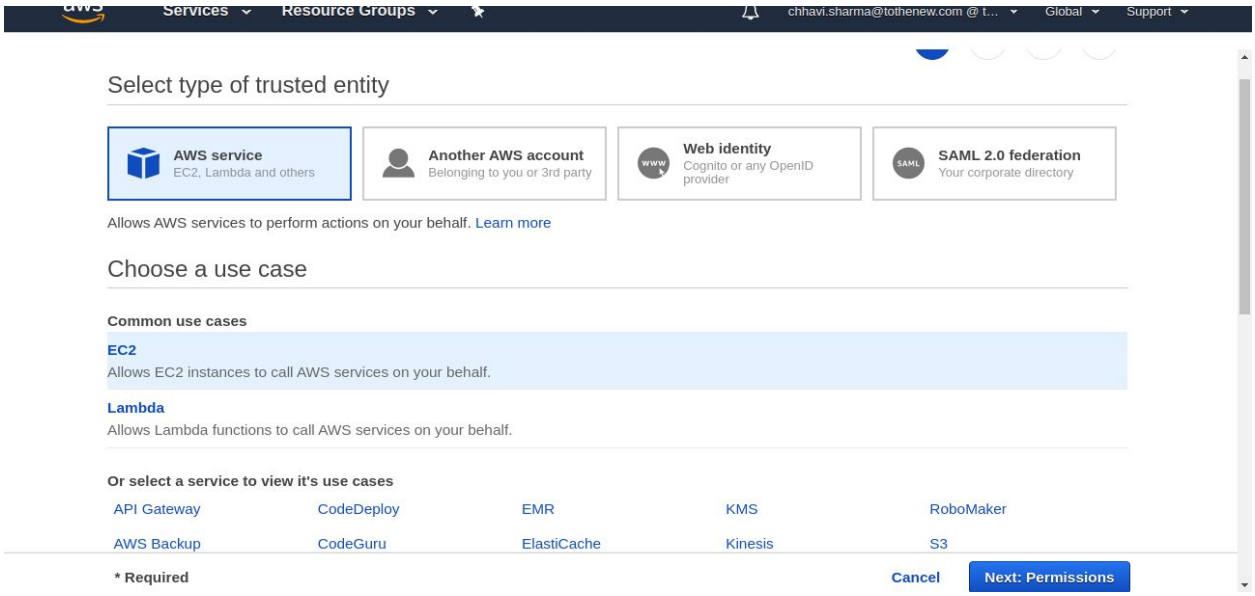
1. Create a Role with full access to S3

Ans. Go to the IAM dashboard. Select Roles from the side menu.

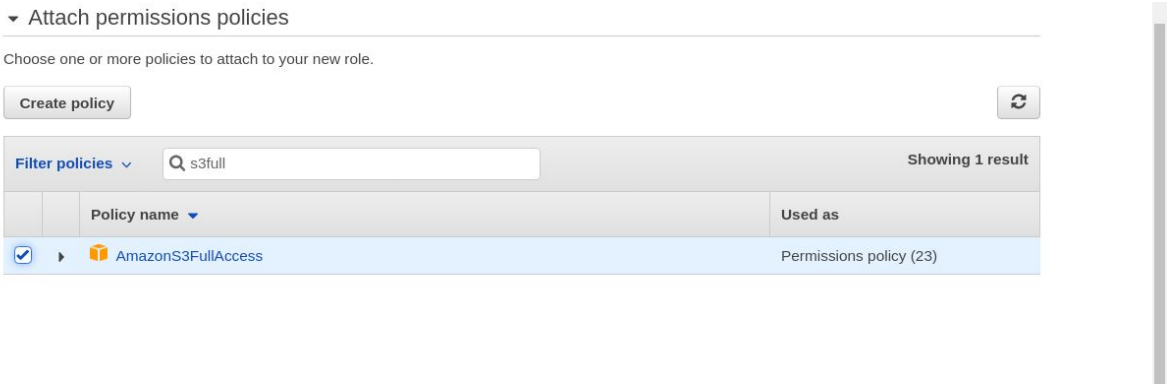


Click on create role.

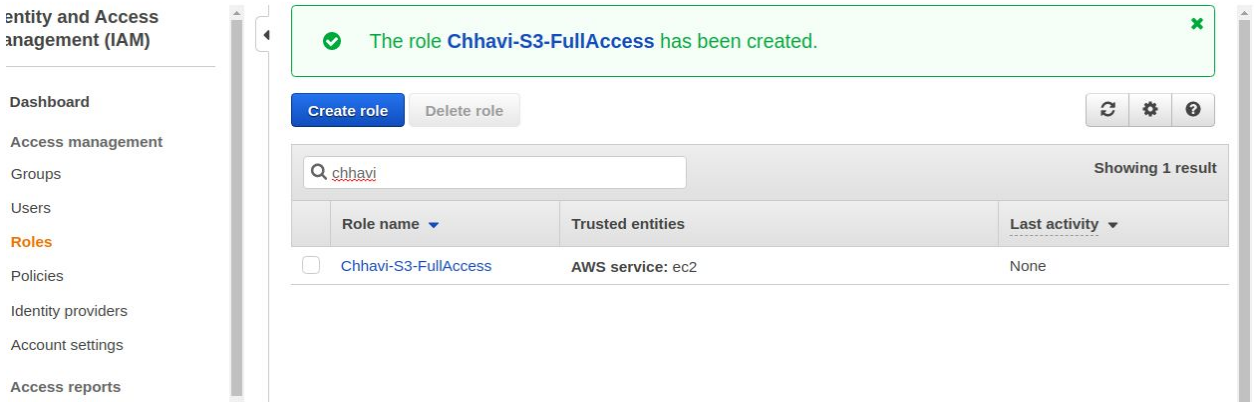
Select a use case.(here ec2)



Select permission : S3 full access



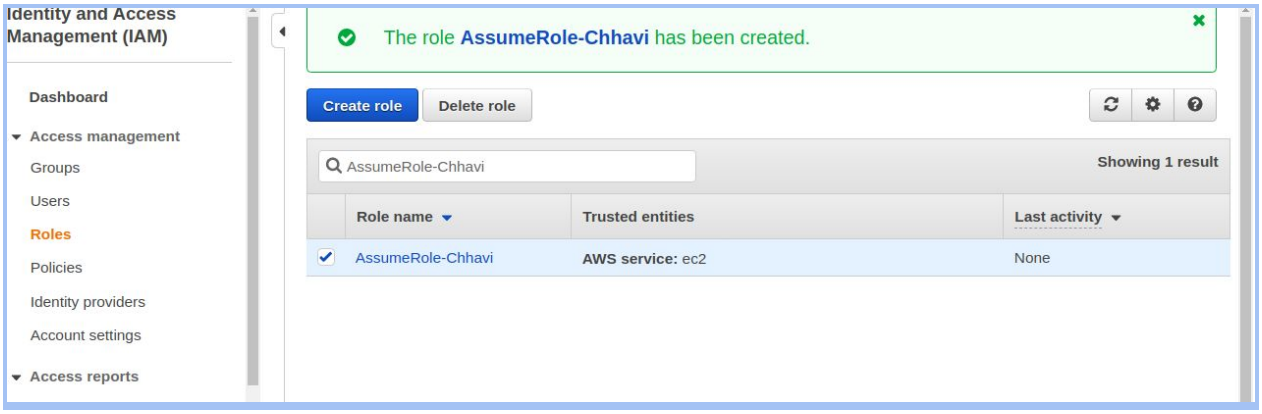
Role Created.



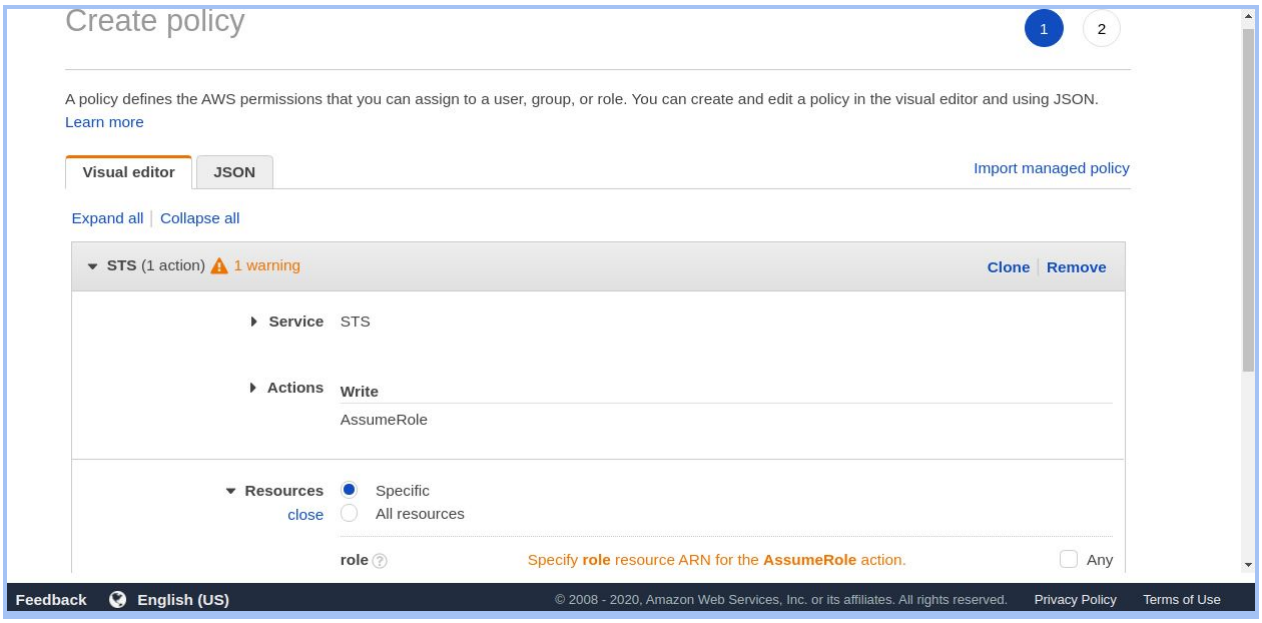
2. Create another which has the policy to assume the previous Role

Ans.

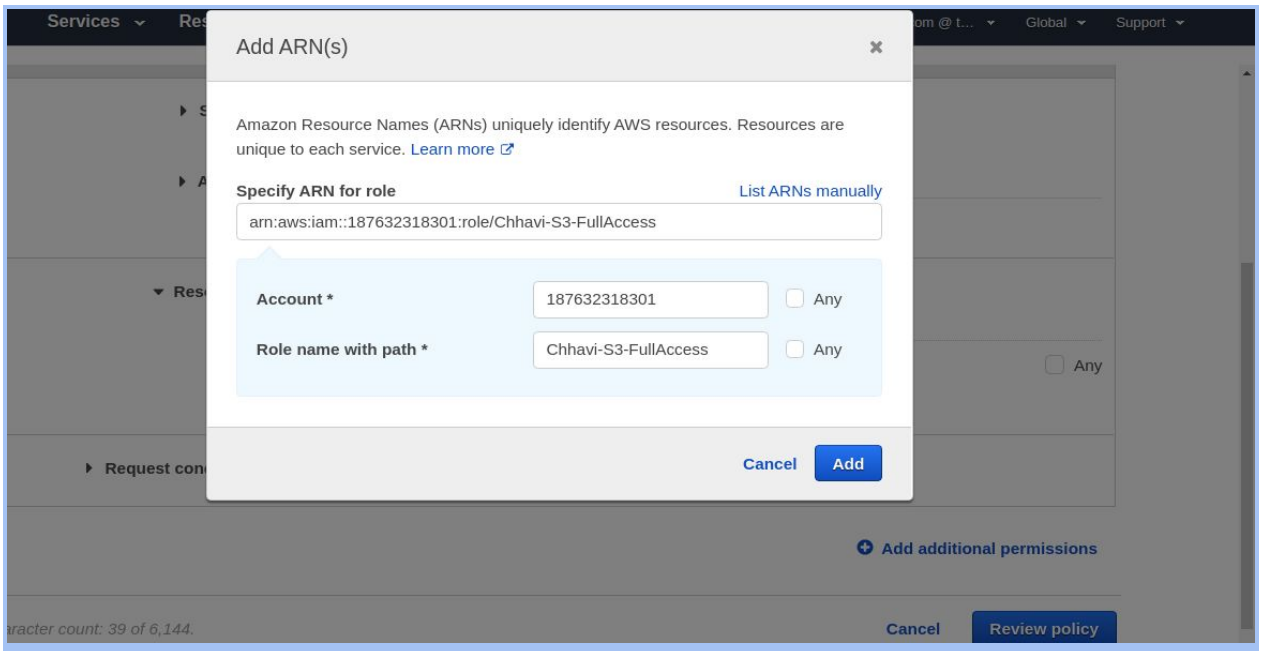
Step 1: Create a new role.

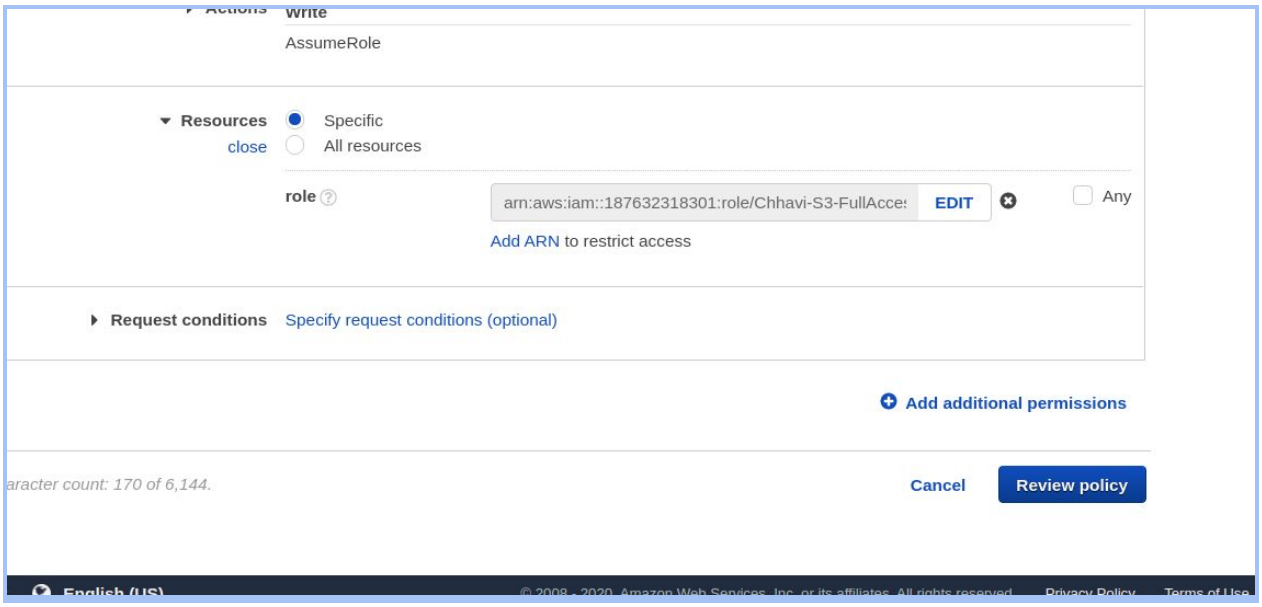


Step 2: Create a new policy.Select STS service.Select Assume role Action.

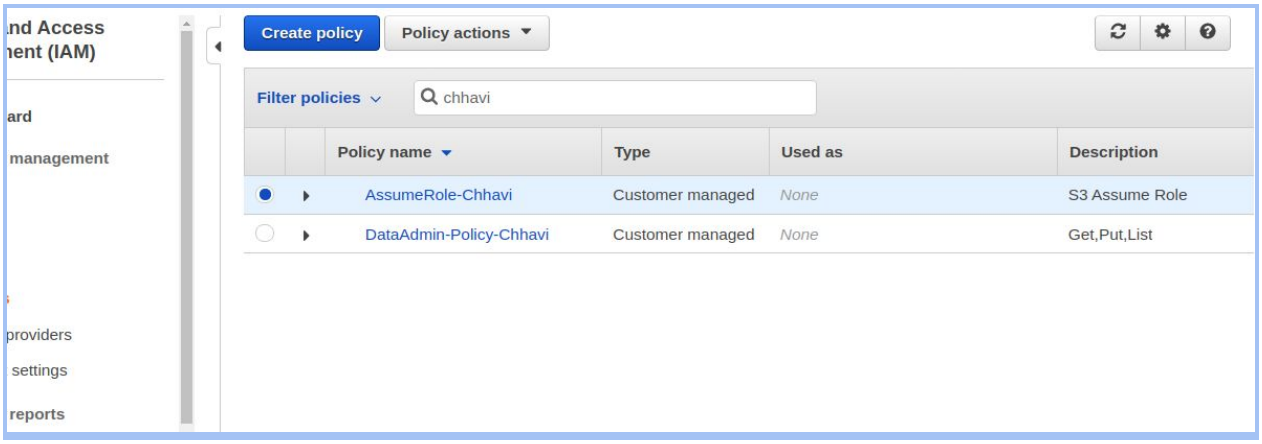


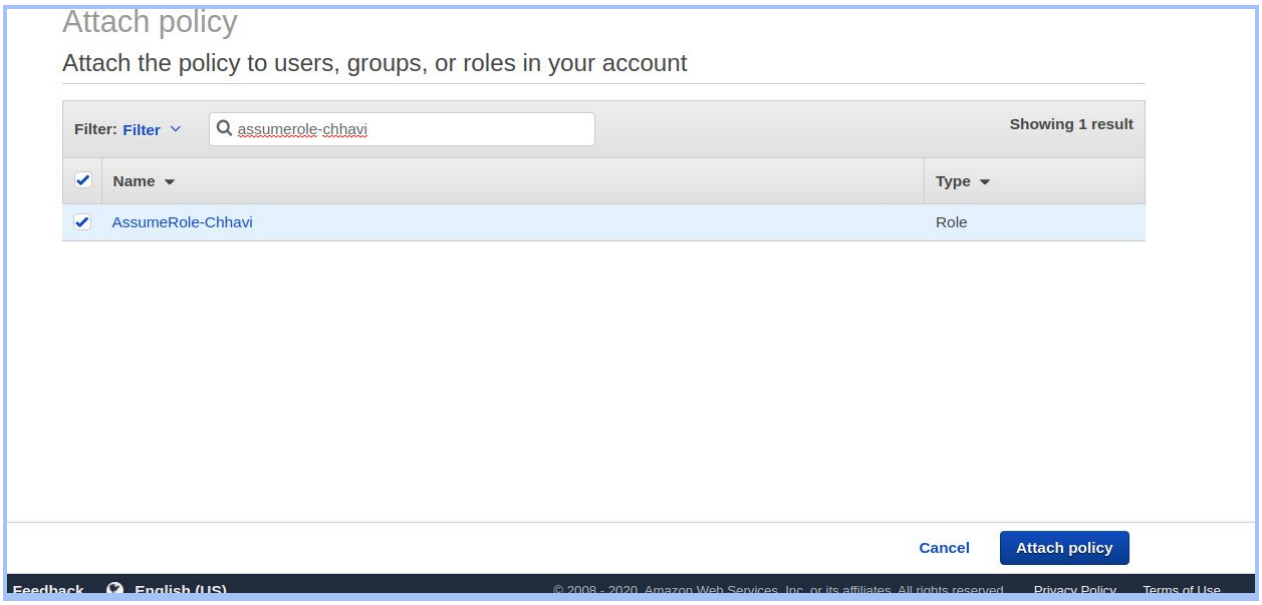
Step 3: Add previous policy's ARN



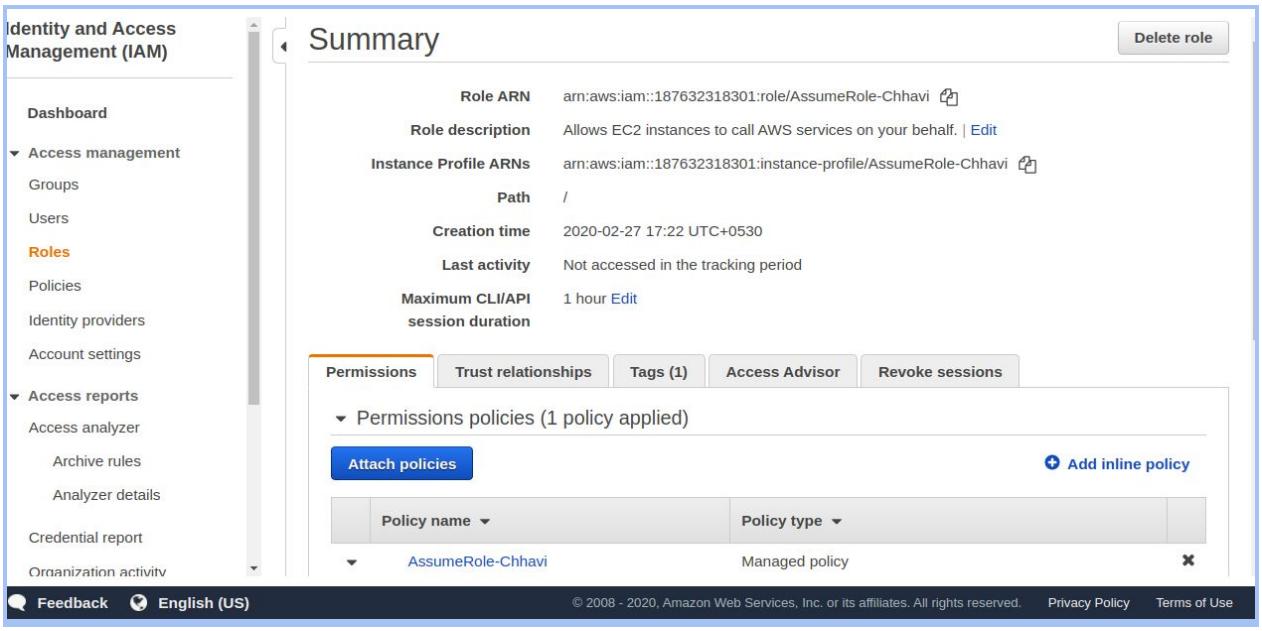


Step 4: Attach new policy to new role created.



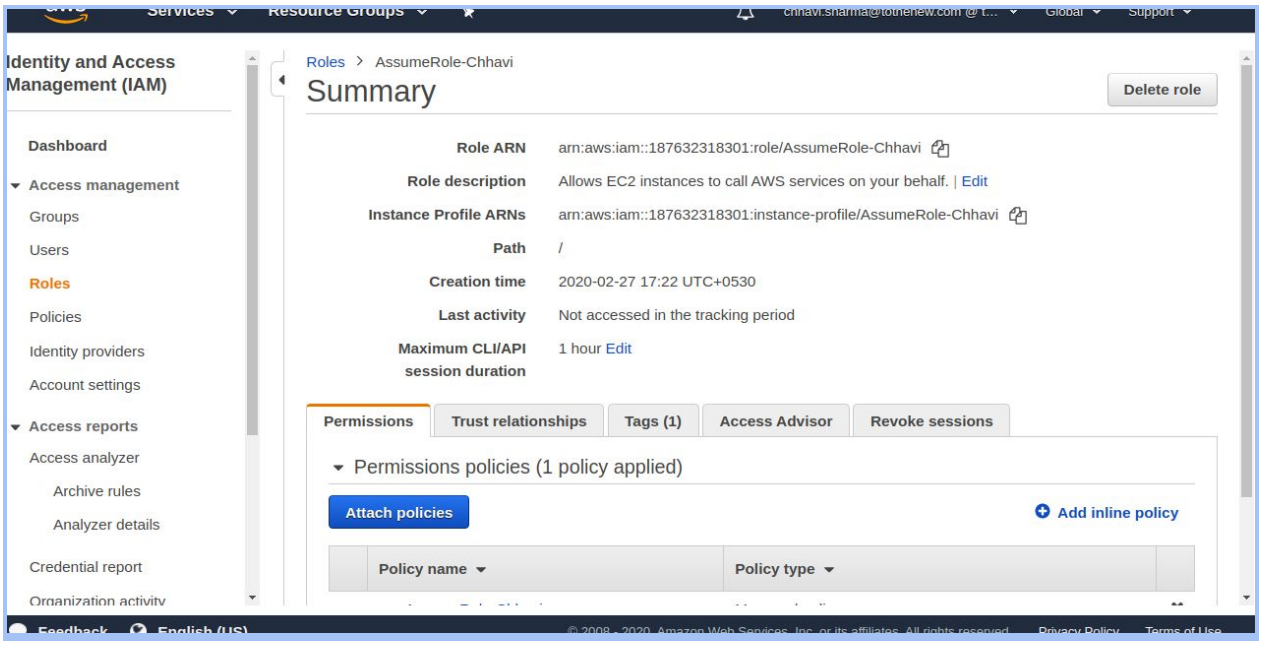


Step 5: Check New role's summary

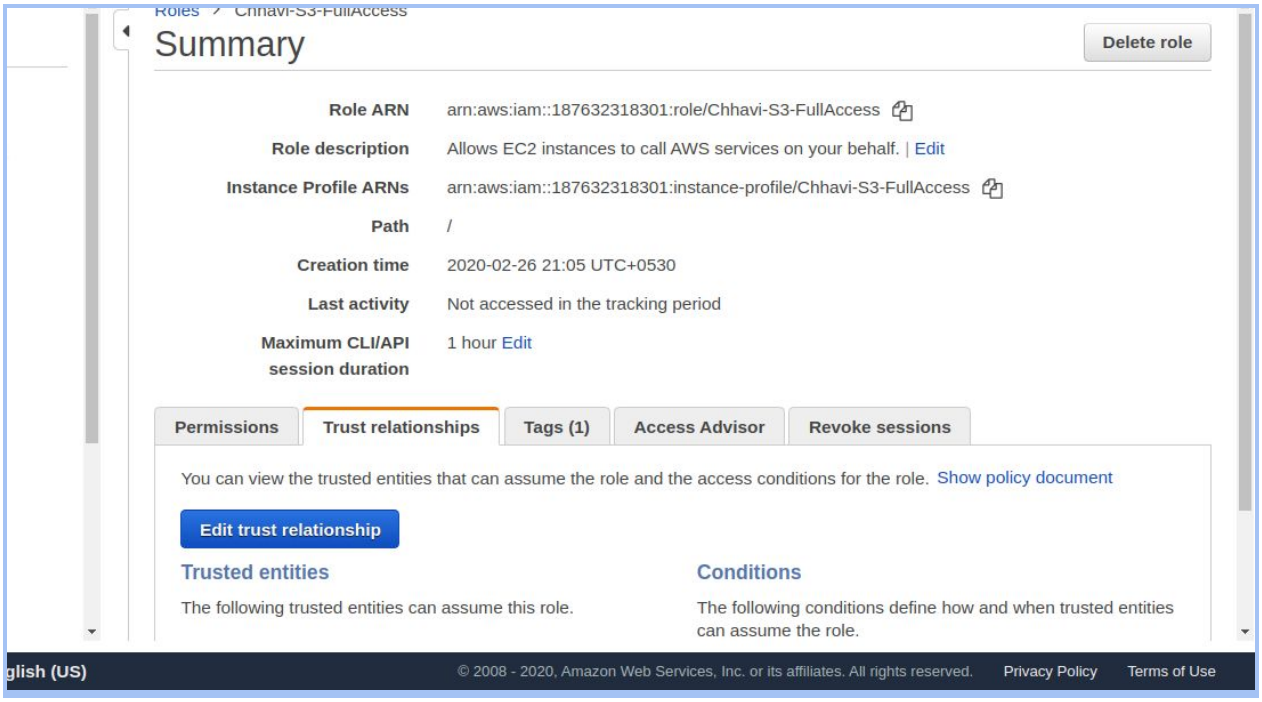


You can see the assumed role attached

Copy the ARN of assume role .



Goto Trust Relationship Tab in the previous policy.



Edit the Trust Relationship of the previous role created.Add the ARN of the assume role created.

Edit Trust Relationship

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS":"arn:aws:iam::187632318301:role/AssumeRole-Chhavi",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Cancel | Update Trust Policy

Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions | Trust relationships | Tags (1) | Access Advisor | Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

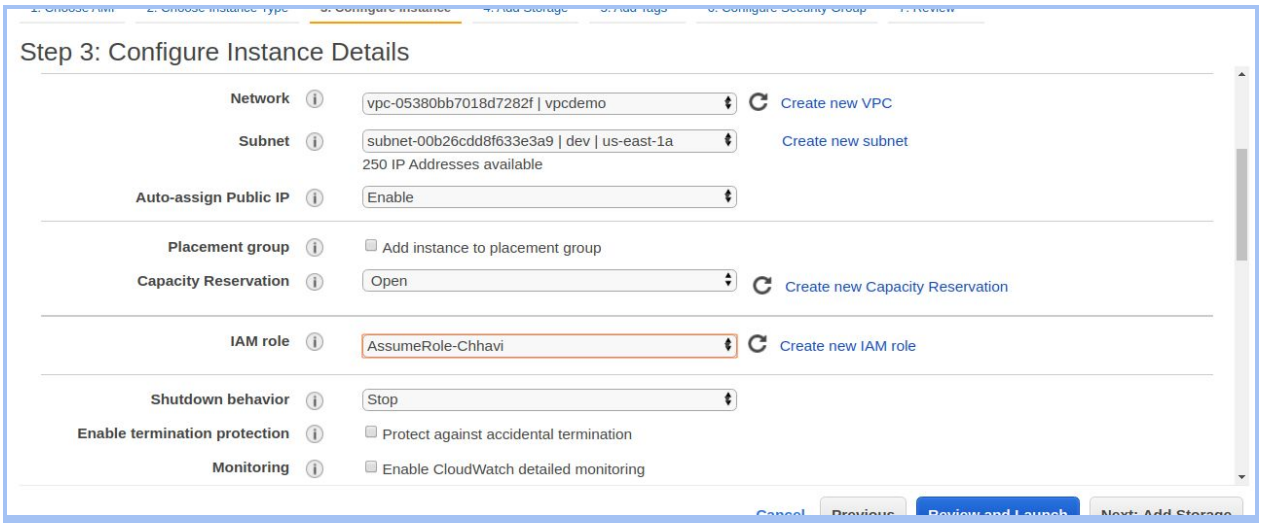
Trusted entities
arn:aws:iam::187632318301:role/AssumeRole-Chhavi
The identity provider(s) ec2.amazonaws.com

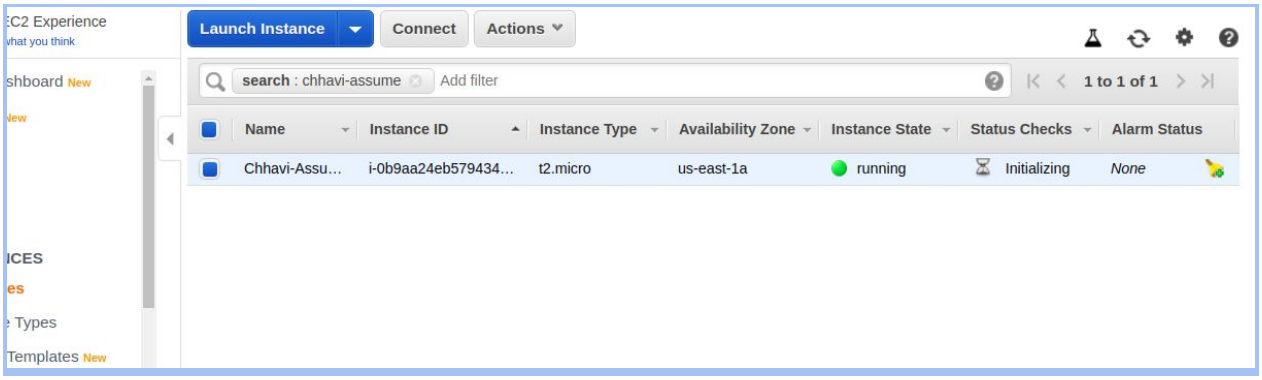
Conditions

The following conditions define how and when trusted entities can assume the role.

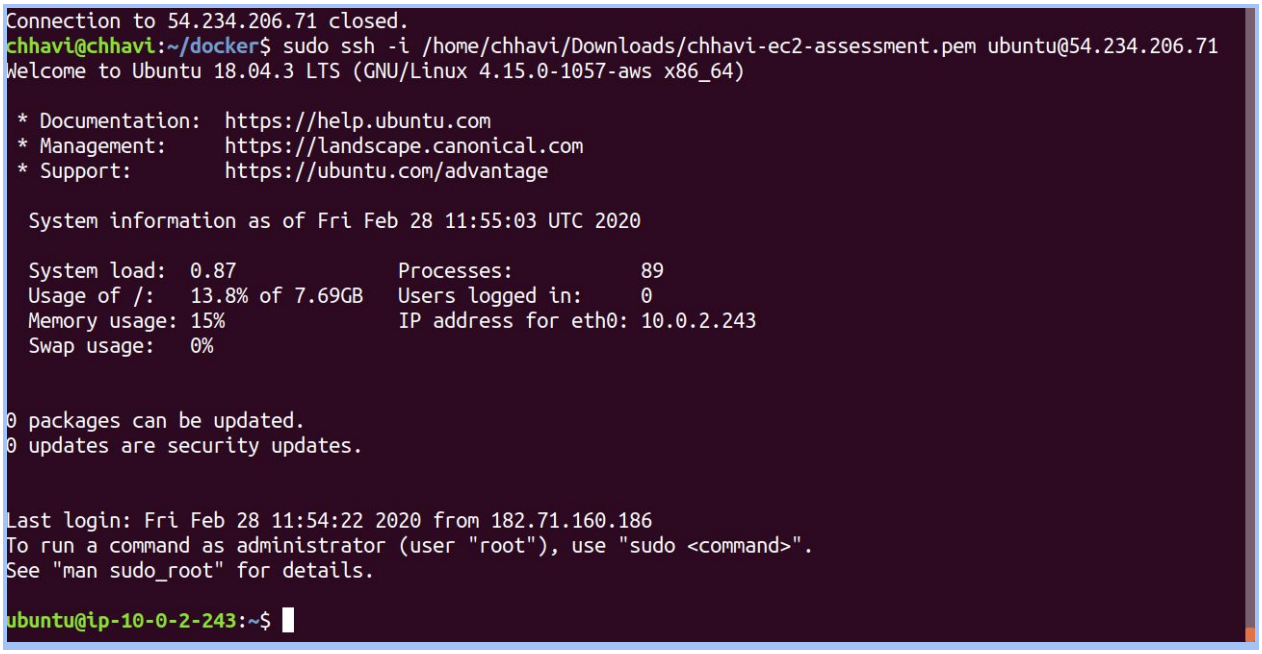
There are no conditions associated with this role.

Now create a new instance.Chhavi-AssumeRole-Instanceand attach AssumeRole-Chhavi to the instance in the configuration.





Ssh into the instance created.Install awscli.



```
Connection to 54.234.206.71 closed.
chhavi@chhavi:~/docker$ sudo ssh -i /home/chhavi/Downloads/chhavi-ec2-assessment.pem ubuntu@54.234.206.71
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Feb 28 11:55:03 UTC 2020

  System load:  0.87              Processes:           89
  Usage of /:   13.8% of 7.69GB   Users logged in:     0
  Memory usage: 15%               IP address for eth0: 10.0.2.243
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.


Last login: Fri Feb 28 11:54:22 2020 from 182.71.160.186
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-243:~$
```

Generate an sts token.

```
ubuntu@ip-10-0-2-243:~$ aws sts assume-role --role-arn arn:aws:iam::187632318301:role/Chhavi-S3-FullAccess
--role-session-name chhaviststoken
{
    "Credentials": {
        "AccessKeyId": "ASIASXL6B65OQRLQTPDF",
        "SecretAccessKey": "MPUnLCRcx9Na7qIJhxKXbNx2CcNSEKHjKFf7voZn",
        "SessionToken": "IQoJb3JpZ2luX2VjEA0aCXVzLWVhc3QtMSJGMEQCIH7HRcMylj4KgIBoCrD7bTO2wdn75KosptNtoJytor
q4AiBnYjhEGtHAQCBXY9NK+bEXu28KeT0D0SAU2ZjRwKdHdSreAQjV//////////8BEAIaDDE4NzYzMjMxODMwMSIMdPgJUWWVz5y7W4jpK
rIBPnWSPruSRlWQp/Vyp3/yeF74Qgff+yMY7ZhqC9r9K9/Grydrx1bM5gYwYt4PbZ9vRT7+LcsPwVR3e3+l964AaHBfL7qcq0UxZpwhR9qf
/hDfjd4FrcrCMFQ9R50JcbOyNWIB1VGQ4/8iqR8icGUTUUHPPrL6BjrhCEmq5SdN7bzzZb6q1uodWbPLi/1wh3jORVTun9OVEluvXpMyYqH
OU8rW+SoqFKtf8lUW6n1o29okgTC9iuTyBTrkASv8SDlp0T8vjRrVAEdwh7iWU+oCBTIO5UrDrl7UUbPSibwgHNeK6kxh1W1Qdxn8piuULG
C9IJFbJ04xHcmANlqSufaXQ+kpG3mGZbM2UEm5jWOmXKVOr/fxFWQxxlRh2ChWKBsPT8kQ+1mPIK8BvxEKgEpM1Sxs1ap27OzeVxEDAs9Oq
zKgB98A2+Cc02fNl8rOTvjgCjOv+4NYelqmYZJZnoB2QnzecE/Gc0EzOu6eLnxBQ5uqdAbzIEvwtrs87Spkj4ZzE0O+Hz8Q/0JUXJdZ2wxr
3ilQRYFwWtD8yJ7TY91niw==",
        "Expiration": "2020-02-28T13:19:09+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROASXL6B65O7H67PBCRZ:chhaviststoken",
        "Arn": "arn:aws:sts::187632318301:assumed-role/Chhavi-S3-FullAccess/chhaviststoken"
    }
}
ubuntu@ip-10-0-2-243:~$
```

Export access key id , secret access key and token.

```
ubuntu@ip-10-0-2-243:~$ export AWS_ACCESS_KEY_ID=ASIASXL6B65OQRLQTPDF
ubuntu@ip-10-0-2-243:~$ export AWS_SECRET_ACCESS_KEY=MPUnLCRcx9Na7qIJhxKXbNx2CcNSEKHjKFf7voZn
```

```
ubuntu@ip-10-0-2-243:~$ export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEA0aCXVzLWVhc3QtMSJGMEQCIH7HRcMylj4KgIBoCr
D7bTO2wdn75KosptNtoJytorq4AiBnYjhEGtHAQCBXY9NK+bEXu28KeT0D0SAU2ZjRwKdHdSreAQjV//////////8BEAIaDDE4NzYzMjMxO
DMwMSIMdPgJUWWVz5y7W4jpKrIBPnWSPruSRlWQp/Vyp3/yeF74Qgff+yMY7ZhqC9r9K9/Grydrx1bM5gYwYt4PbZ9vRT7+LcsPwVR3e3+l
964AaHBfL7qcq0UxZpwhR9qf/hDfjd4FrcrCMFQ9R50JcbOyNWIB1VGQ4/8iqR8icGUTUUHPPrL6BjrhCEmq5SdN7bzzZb6q1uodWbPLi/1
wh3jORVTun9OVEluvXpMyYqHOU8rW+SoqFKtf8lUW6n1o29okgTC9iuTyBTrkASv8SDlp0T8vjRrVAEdwh7iWU+oCBTIO5UrDrl7UUbPSib
wgHNeK6kxh1W1Qdxn8piuULGC9IJFbJ04xHcmANlqSufaXQ+kpG3mGZbM2UEm5jWOmXKVOr/fxFWQxxlRh2ChWKBsPT8kQ+1mPIK8BvxEKg
EpM1Sxs1ap27OzeVxEDAs9OqzKgB98A2+Cc02fNl8rOTvjgCjOv+4NYelqmYZJZnoB2QnzecE/Gc0EzOu6eLnxBQ5uqdAbzIEvwtrs87Spk
j4ZzE0O+Hz8Q/0JUXJdZ2wxr3ilQRYFwWtD8yJ7TY91niw==
```

Aws configure.

```
ubuntu@ip-10-0-2-243:~$ aws configure
AWS Access Key ID [None]: ASIASXL6B65OQRLQTPDF
AWS Secret Access Key [None]: MPUnLCRcx9Na7qIJhxKXbNx2CcNSEKHjKFf7voZn
Default region name [None]:
Default output format [None]:
```

Now write aws s3 ls.

```
ubuntu@ip-10-0-2-243:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-02-28 10:55:02 abhishek-bootcamp
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-02-26 16:26:29 akshaybuck1
2020-02-27 08:55:25 aman-khandelwal-1
2019-03-07 09:40:48 anmol-bootcamp19
2019-03-08 00:25:58 avcabc
2017-09-07 03:41:42 aws-codestar-us-east-1-187632318301
2017-09-07 04:23:01 aws-codestar-us-east-1-187632318301-codestartest2-app
2017-09-07 04:23:07 aws-codestar-us-east-1-187632318301-codestartest2-pipe
2017-09-07 03:41:48 aws-codestar-us-east-1-187632318301-codestarttest-pipe
2019-06-26 05:39:55 aws-lambda-trigger-ronozor
2020-02-28 03:56:49 ayush-public-bucket
2020-02-25 07:02:11 baban-123
2018-02-14 12:28:43 cf-templates-71mx96ojlvv5-us-east-1
2019-03-27 15:57:27 cfront1
2020-02-26 11:51:54 chirag-bucket-2
2020-02-26 11:46:43 chirag-bucket1
2019-03-27 20:34:52 cloudfront8
2020-02-25 10:59:18 copy-test-delete
```

3. Attach this to an instance and get an sts token.

Ans.

4. Create a group for "Data Administrator" where the user 'Alice' be a member of this group. This group will prepare the data for the analysis. So Provide the following access to the group.

Service: Amazon S3;

Action:

Get*,

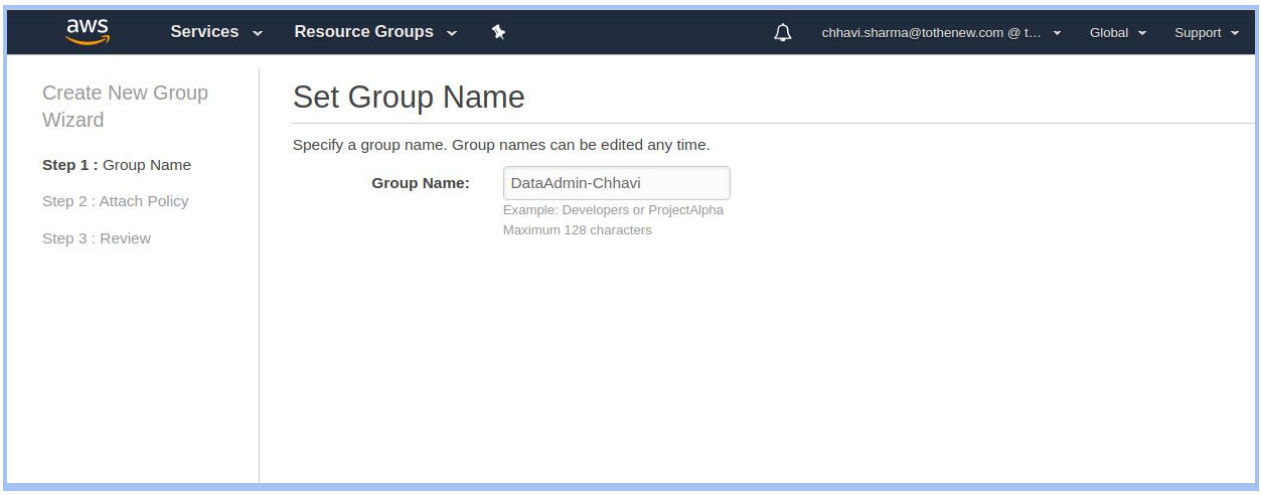
List*,

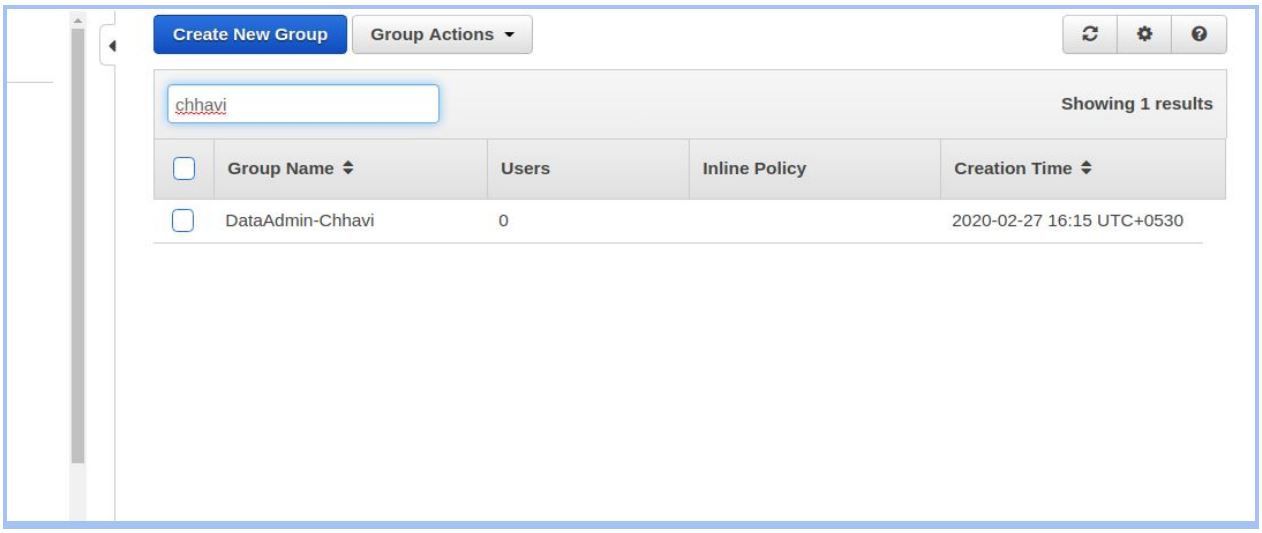
Put*,

ARN: Input and output Buckets (no conditions)

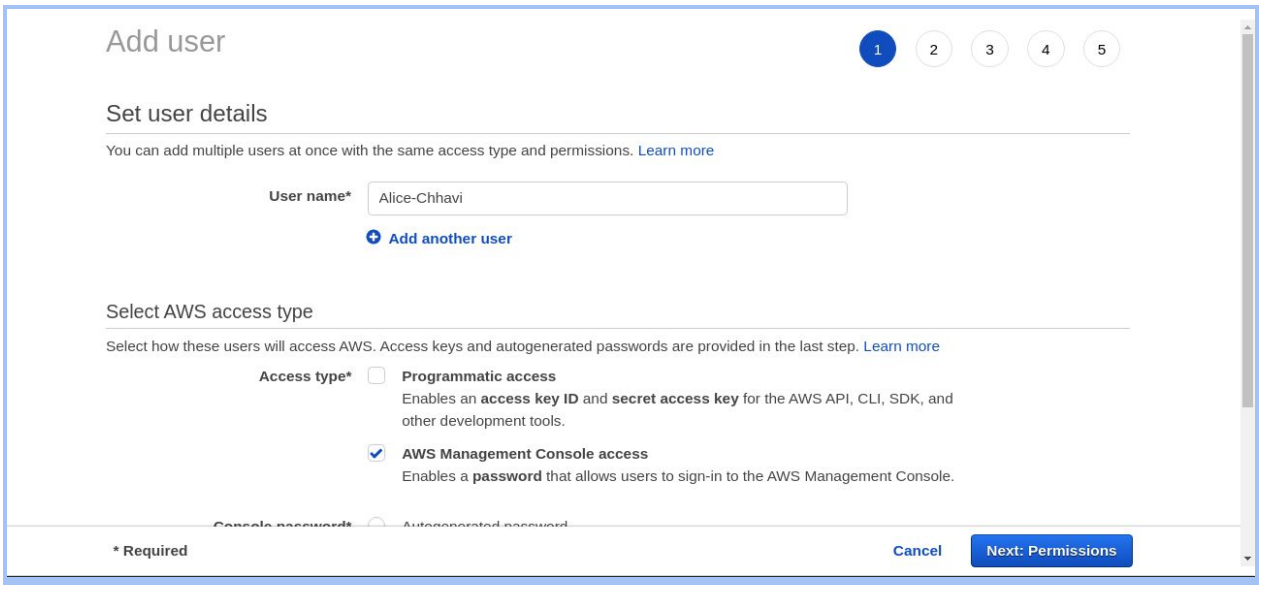
Ans.

Step 1: Create a Group : DataAdmin

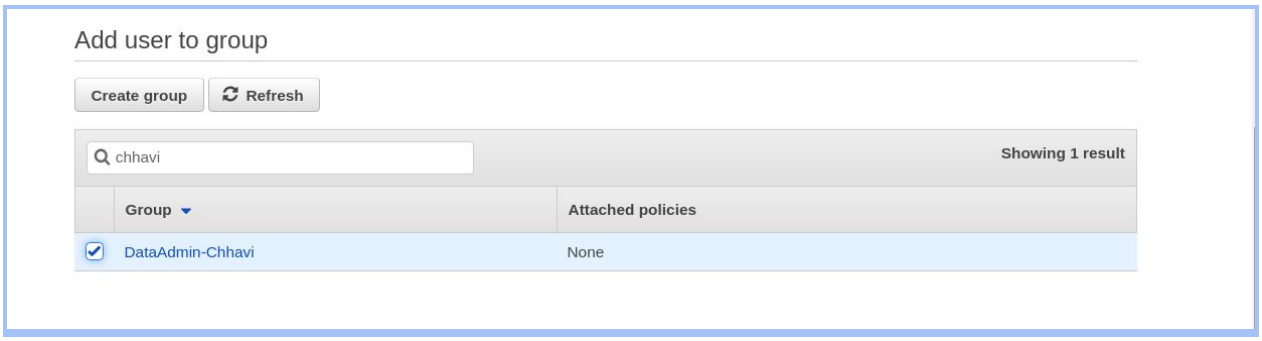




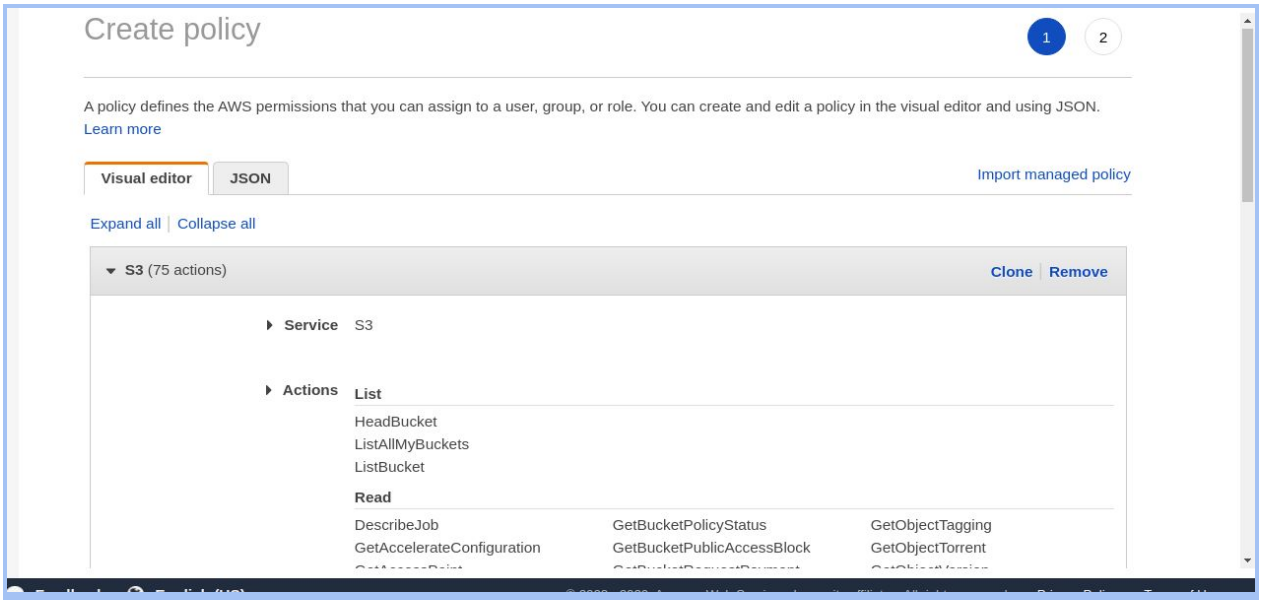
Step2: Create a user : Alice

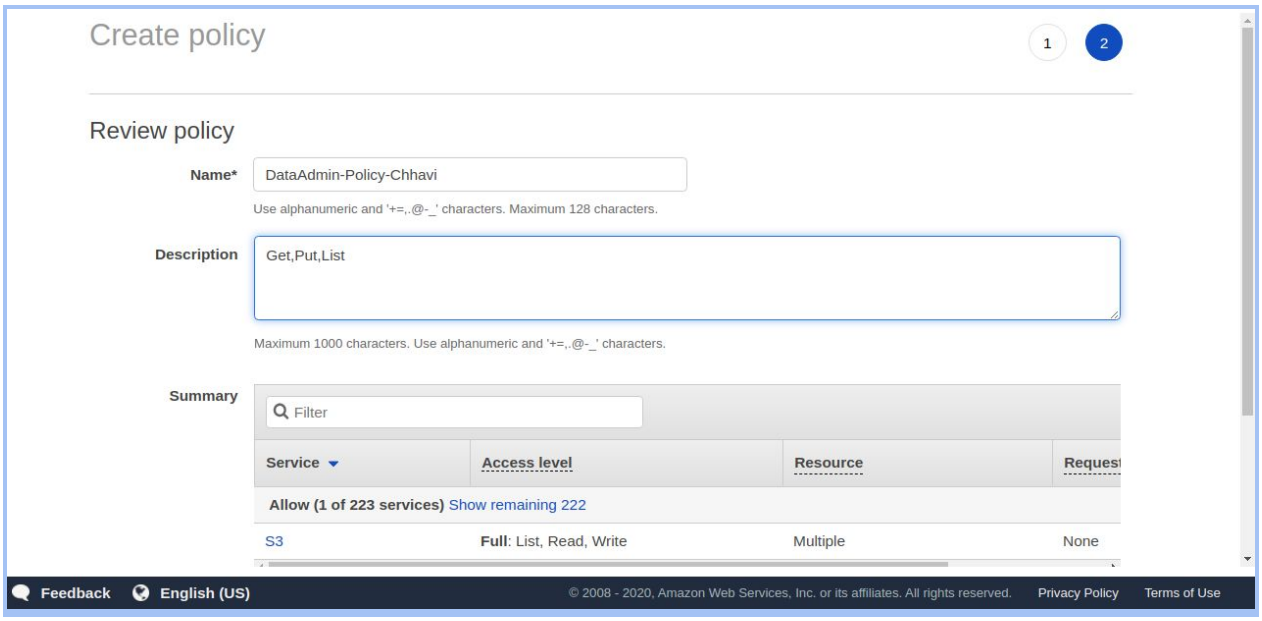


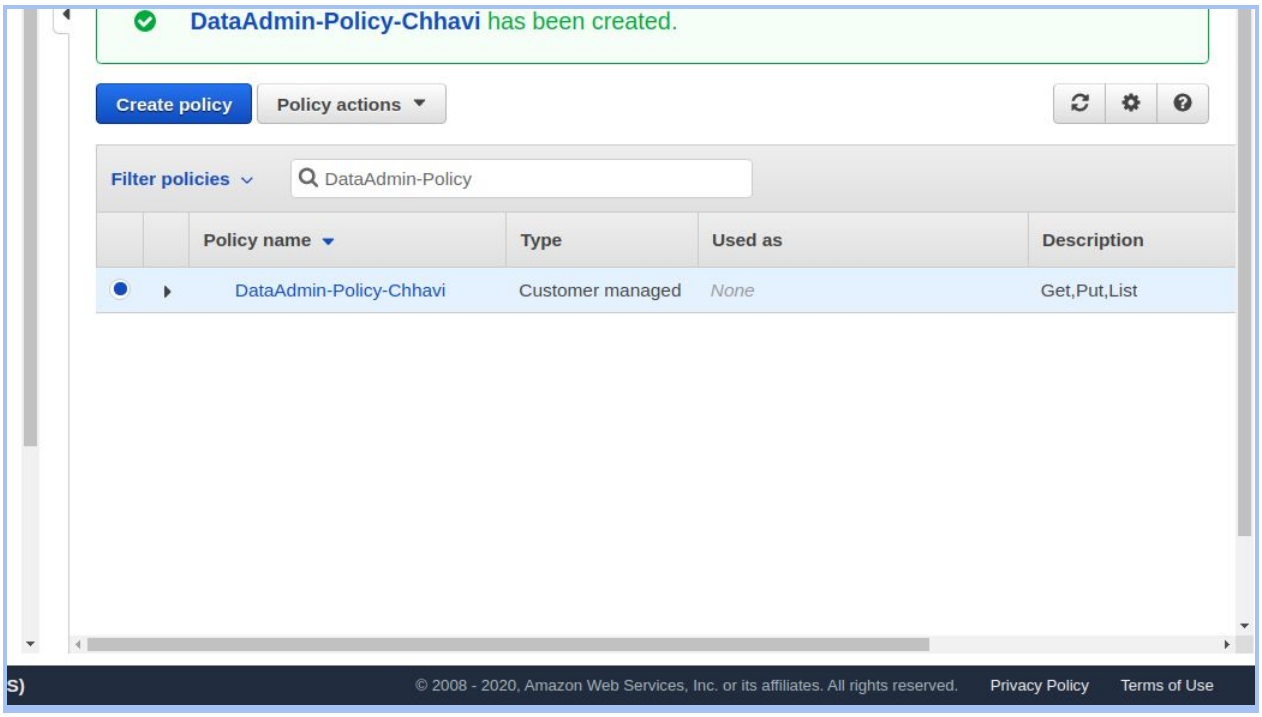
Step 3: Add user to Group



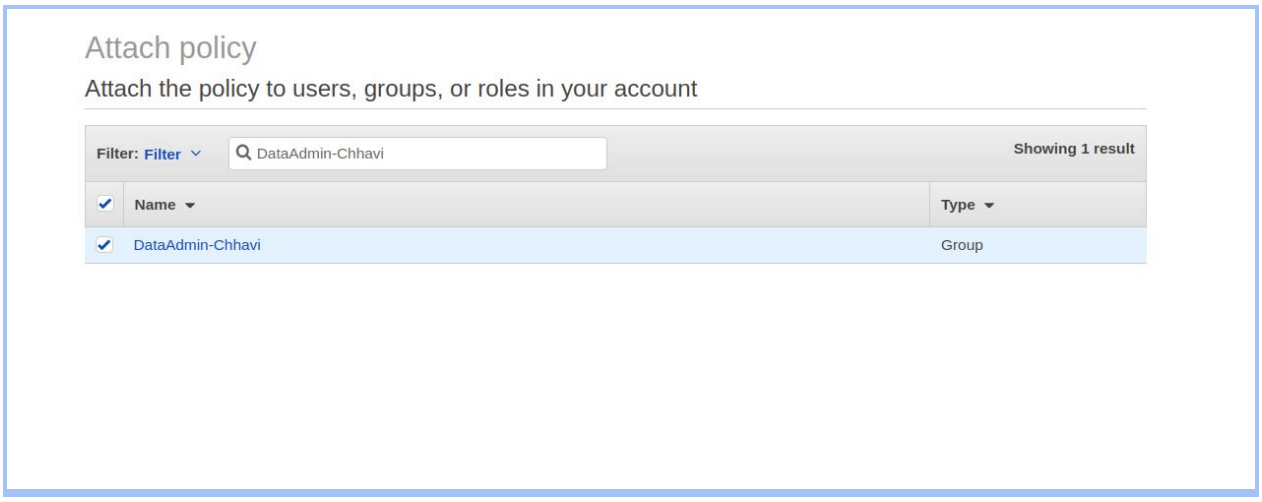
Step 4: Create a policy for Get*,List* and Put* S3.







Step 5: Attach policy to group.



5. Create a group for the "Developer group " where the user 'bob ' is a member of this group. This group with Test Newly Developed Features for which they require access to EC2 instances. Provide the following access to this group:

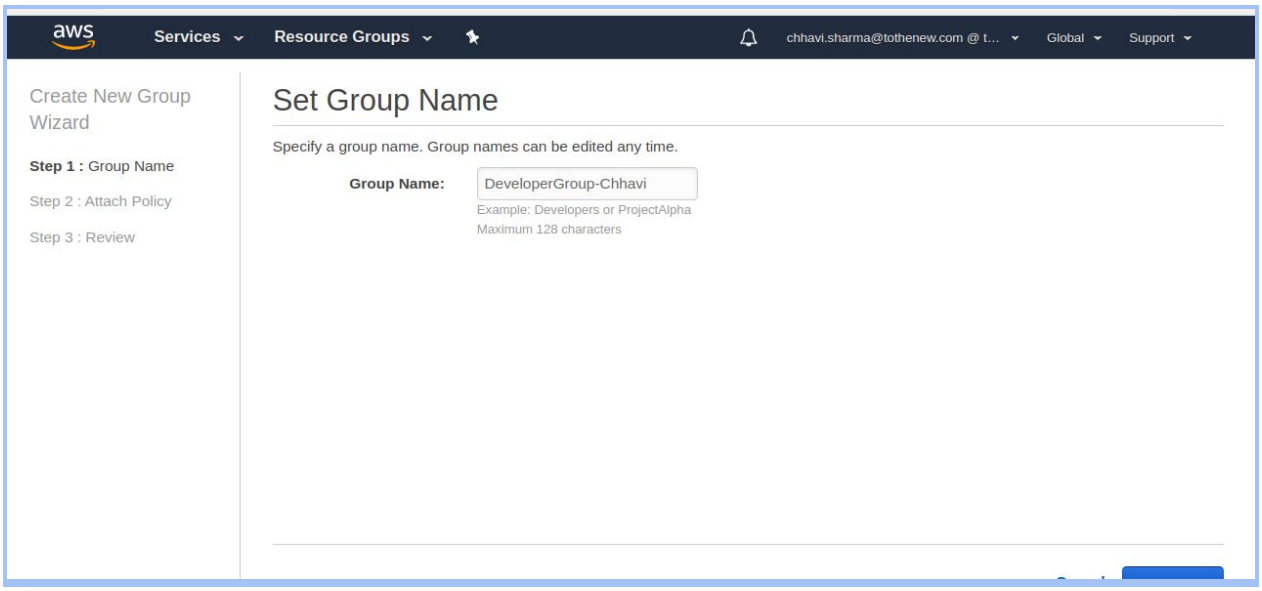
Service: Amazon EC2

Action: *Instances, *Volume, Describe*, CreateTags;

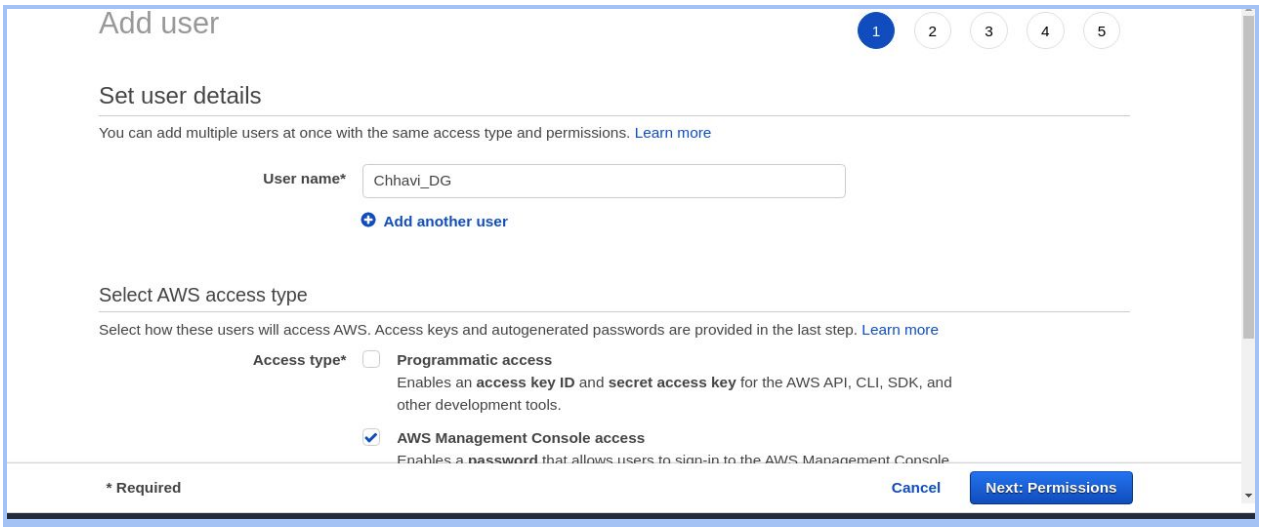
Condition: Dev Subnets only

Ans.

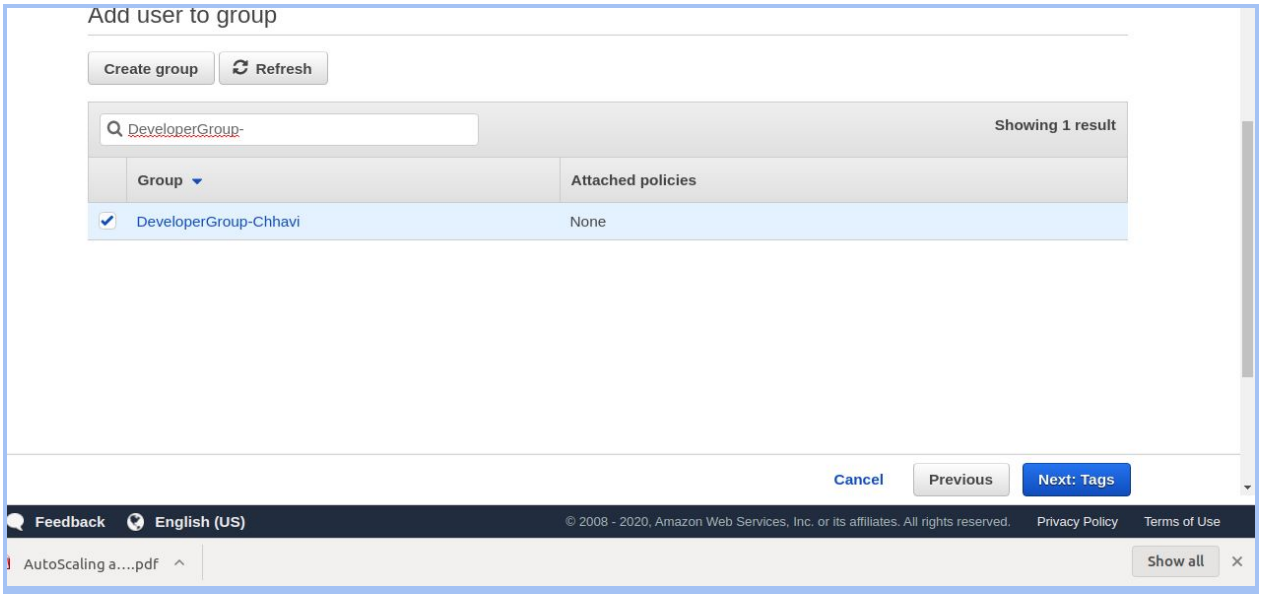
Step 1: Create a group - DeveloperGroup-Chhavi

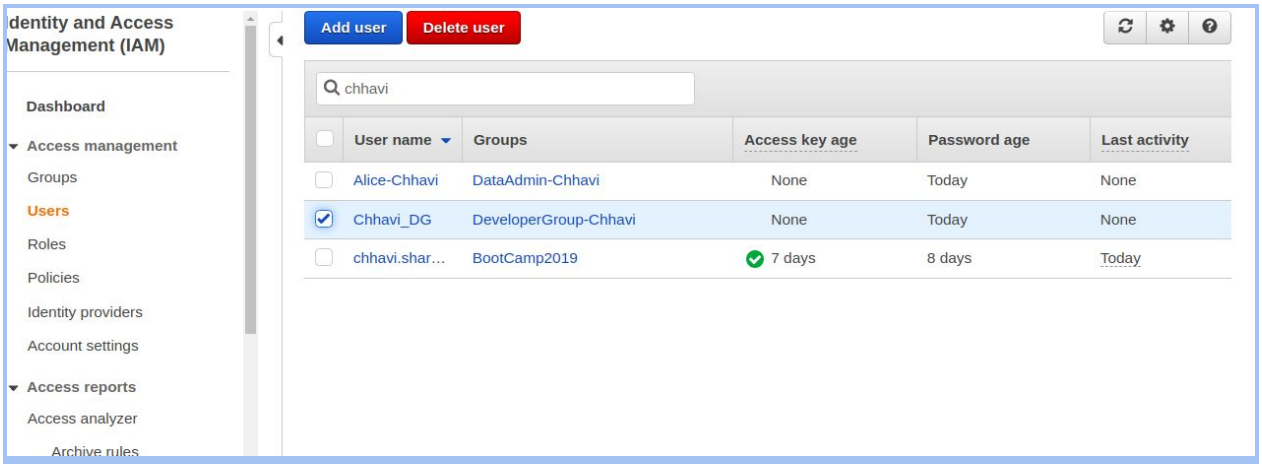


Step 2: Now add a User.

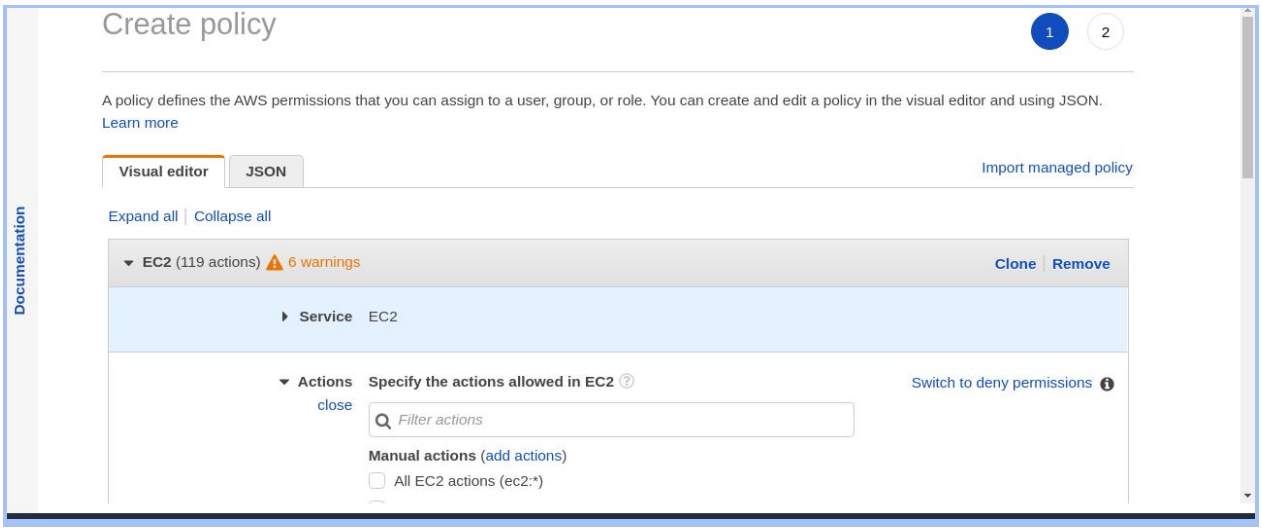


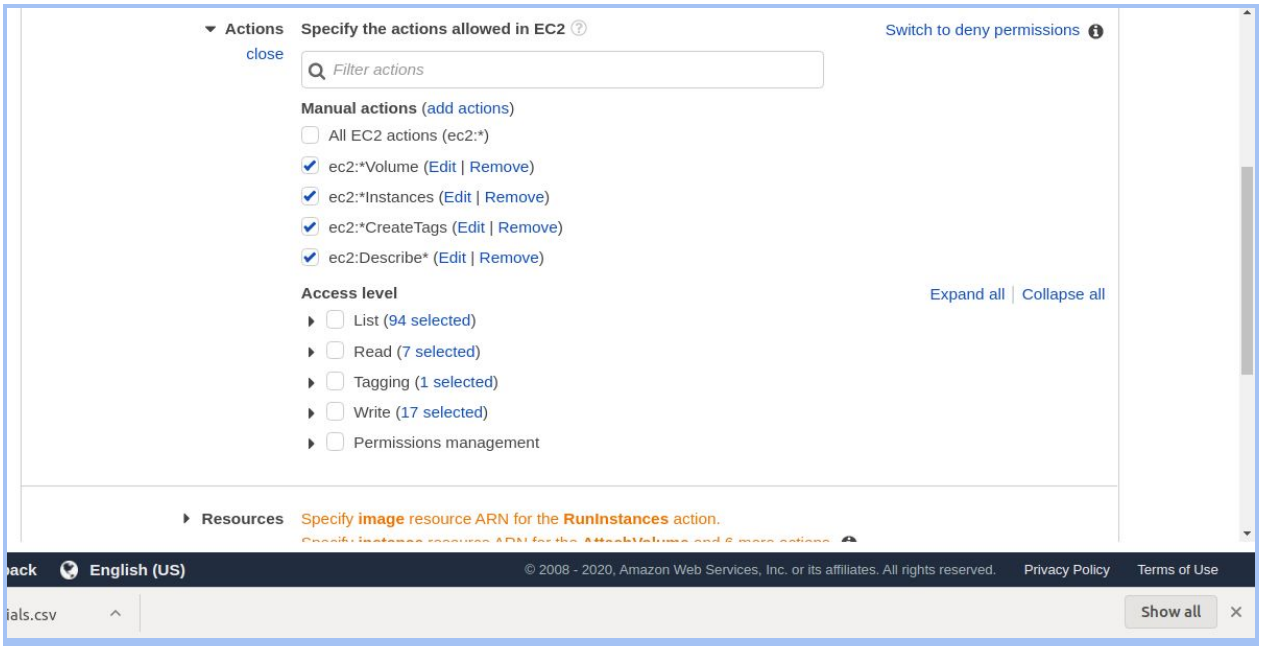
Step 3: Add the user to the group created above.



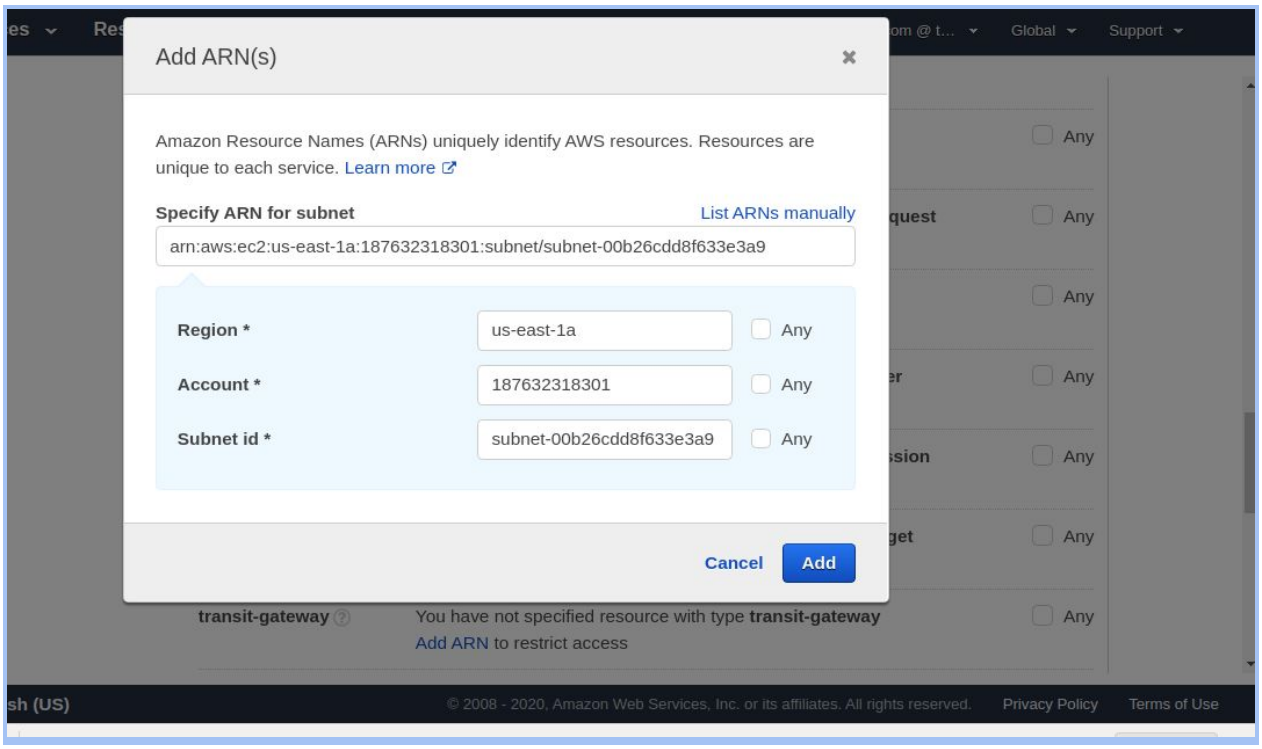


Step 4: Create a new policy for the Developer Group.

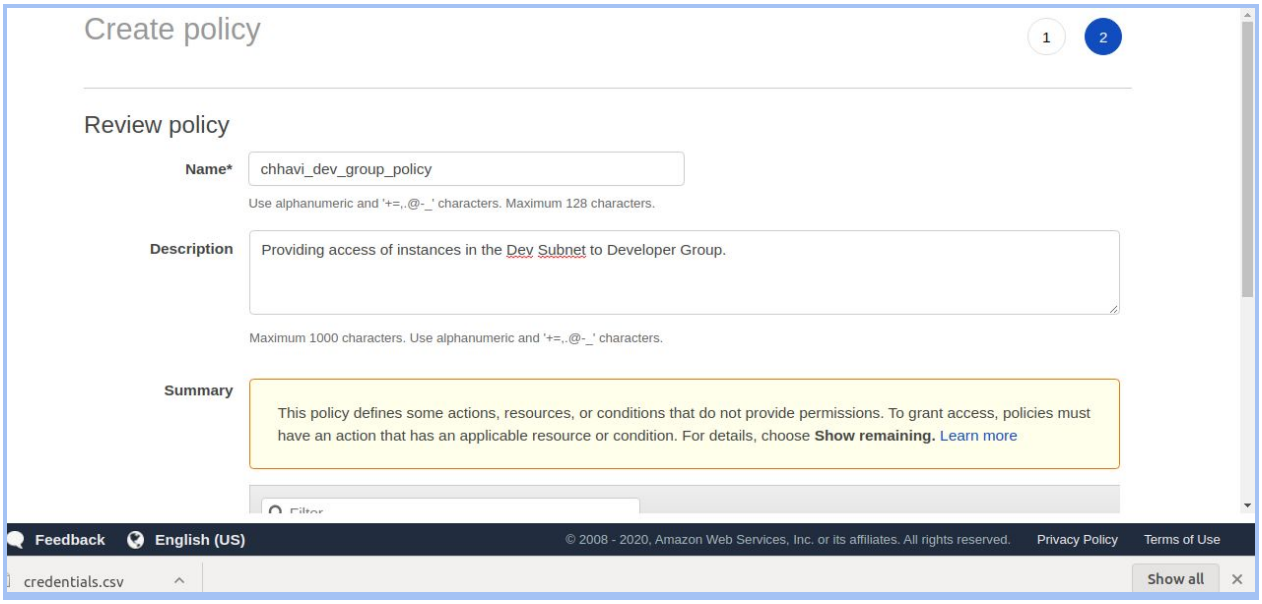




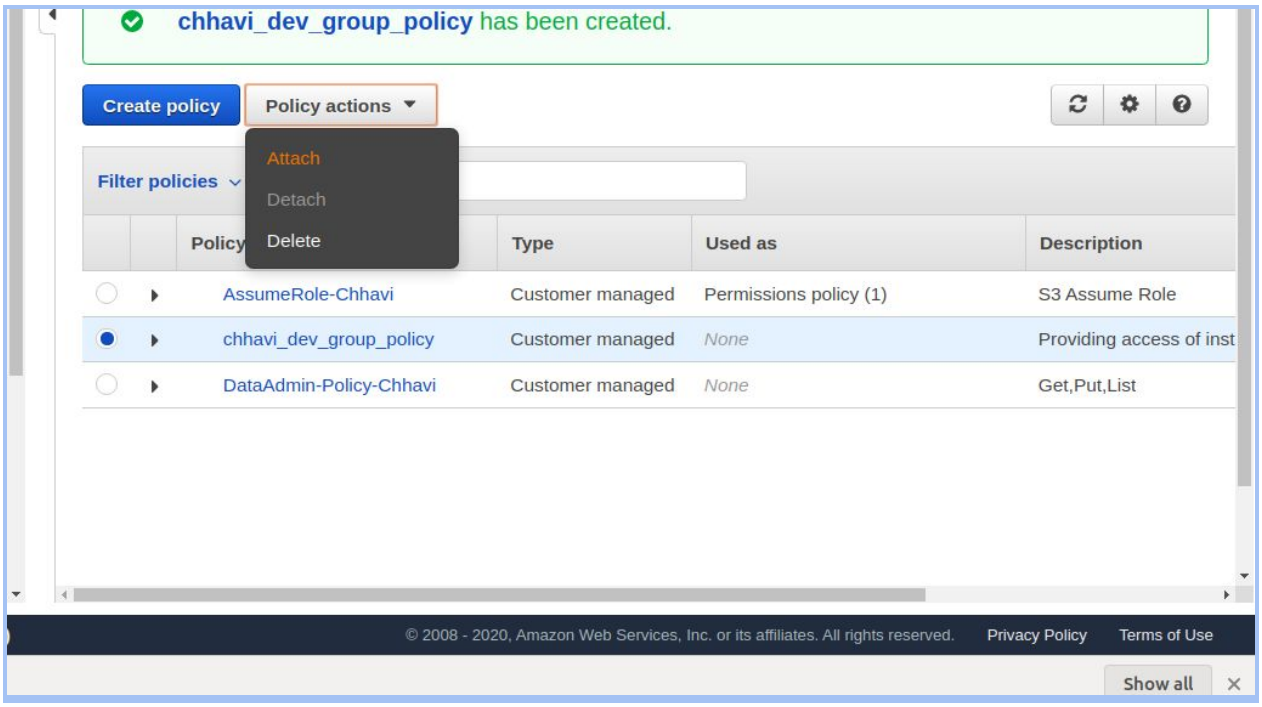
Add the ARN of the Subnet(dev subnet)

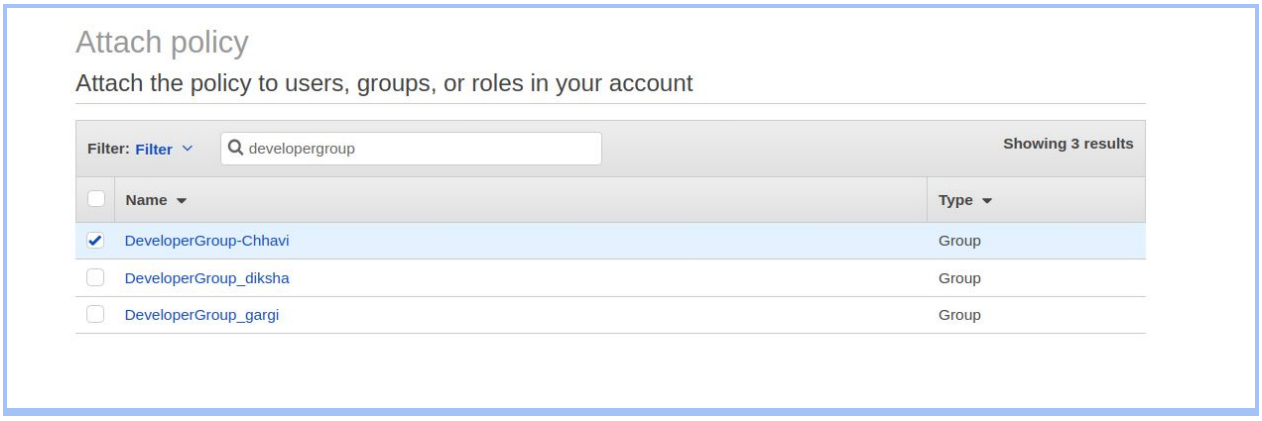


Review Policy

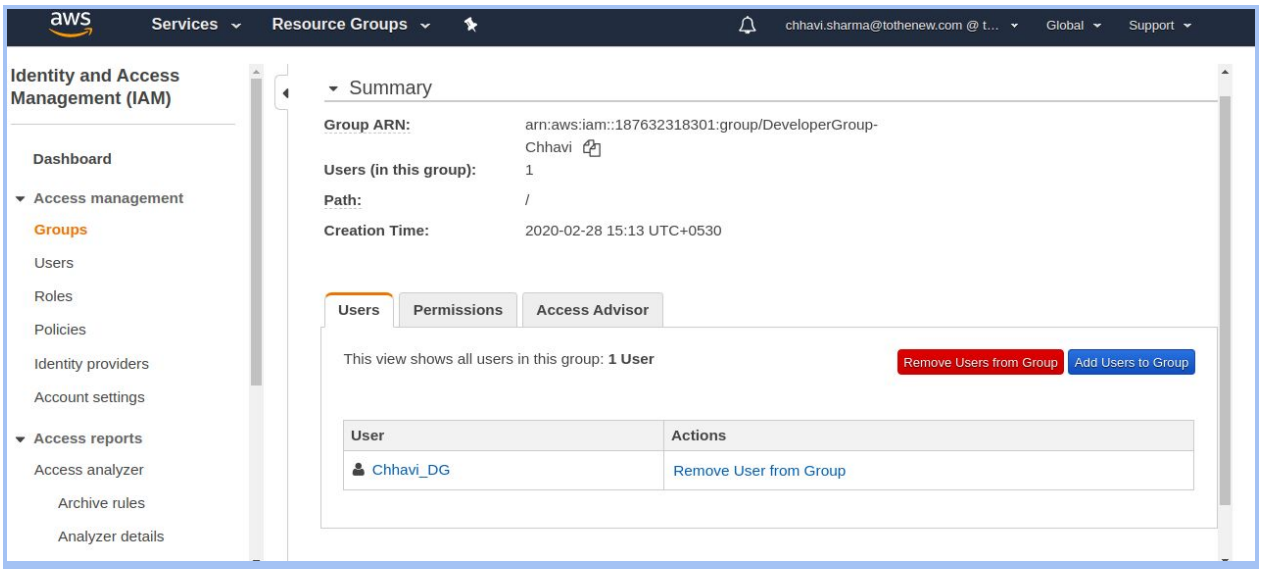


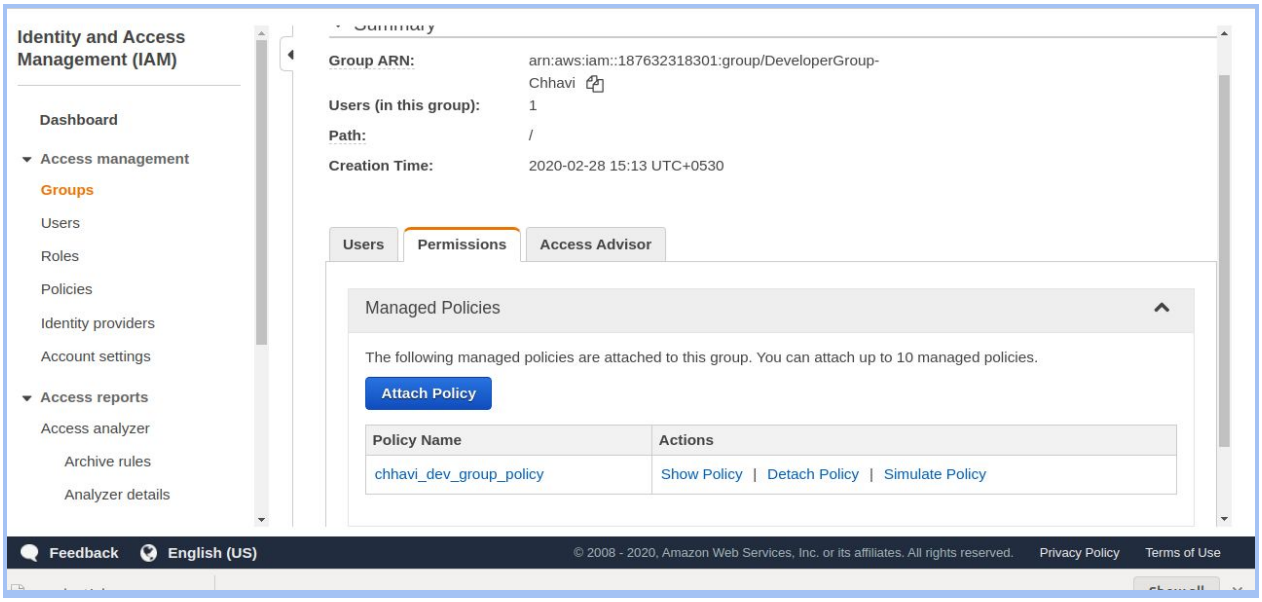
Step 5: Attach Policy to group (Developer Group)





Step 6: Check the group that it contains the user and the policy that you created





6. Identify the unused IAM users/credentials using AWS CLI.

Ans.

Step 1: Install jq.

jq is a lightweight and flexible command-line JSON processor.jq is like sed for JSON data - you can use it to slice and filter and map and transform structured data with the same ease that sed , awk , grep and friends let you play with text.

```
chhavi@chhavi:~$ sudo apt-get install jq
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libjq1 libonig4
The following NEW packages will be installed:
  jq libjq1 libonig4
0 upgraded, 3 newly installed, 0 to remove and 11 not upgraded.
Need to get 276 kB of archives.
After this operation, 930 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libonig4 amd64 6.7.0-1 [119 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libjq1 amd64 1.5+dfsg-2 [111 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 jq amd64 1.5+dfsg-2 [45.6 kB]

Fetched 276 kB in 8s (33.9 kB/s)

Selecting previously unselected package libonig4:amd64.
(Reading database ... 176040 files and directories currently installed.)
Preparing to unpack .../libonig4_6.7.0-1_amd64.deb ...
Unpacking libonig4:amd64 (6.7.0-1) ...
Selecting previously unselected package libjq1:amd64.
Preparing to unpack .../libjq1_1.5+dfsg-2_amd64.deb ...
Unpacking libjq1:amd64 (1.5+dfsg-2) ...
```

Step 2: list all users.

```
chhavi@chhavi:/etc/nginx/sites-available$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "abhishek.chauhan1@tothenew.com",
            "UserId": "AIDASXL6B65OQ4RMZ427Z",
            "Arn": "arn:aws:iam::187632318301:user/abhishek.chauhan1@tothenew.com",
            "CreateDate": "2020-02-19T11:03:23+00:00",
            "PasswordLastUsed": "2020-02-28T05:03:08+00:00"
        },
        {
            "Path": "/",
            "UserName": "aditya.upadhyay@tothenew.com",
            "UserId": "AIDASXL6B65OYD7UUCZUJ",
            "Arn": "arn:aws:iam::187632318301:user/aditya.upadhyay@tothenew.com",
            "CreateDate": "2020-02-19T11:03:25+00:00",
            "PasswordLastUsed": "2020-02-28T04:46:17+00:00"
        },
        {
            "Path": "/",
            "UserName": "akshay.shrivastava@tothenew.com",
            "UserId": "AIDASXL6B65OSGPOGZHFO",
            "Arn": "arn:aws:iam::187632318301:user/akshay.shrivastava@tothenew.com",
            "CreateDate": "2020-02-19T11:03:26+00:00",
```

Step 3: Use jq and filter the output .

```
chhavi@chhavi:~$ aws iam list-users | jq '.Users[] | select(.PasswordLastUsed==null) |.UserName'
"Alice"
"Alice-Chhavi"
"alice-maithely"
"Alice-Srima"
"asusumeuser"
"Bob"
"Bob-maithely"
"Bob-Vedant"
"bobpooja"
"Chhavi_DG"
"CloudCheckr"
"dikshaTomar"
"GargiIAM"
"Gargi_Alice"
"garima.dabral@tothenew.com"
"Graima"
"HAWK2.0-user"
"poojaalice"
"prod1-maithely"
"raghu.sharma@tothenew.com"
"s3pooja"
"Vedant-alice"
"vivek.yadav1@tothenew.com"
chhavi@chhavi:~$ Step 2:
```

7. Identify all the instances having the tag key-value "backup=true" using AWS CLI.

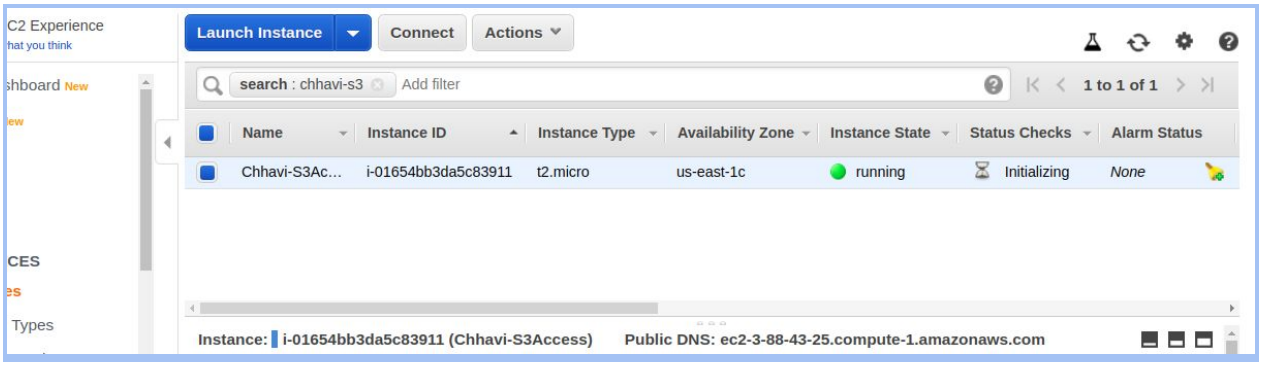
Ans.

```
chhavi@chhavi:~$ aws ec2 describe-instances --filters "Name=tag:backup,Values=true"
{
    "Reservations": []
}
```

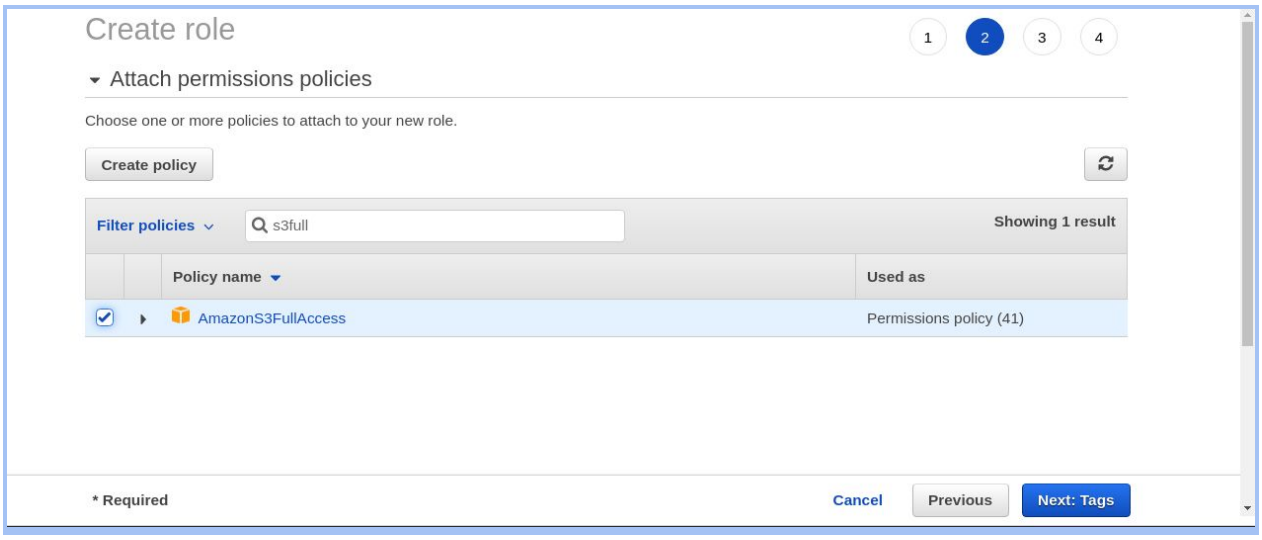
8. An EC2 Instance hosts a Java-based application that accesses an s3 bucket. This EC2 Instance is currently serving production users. Create the role and assign the role to EC2 instance.

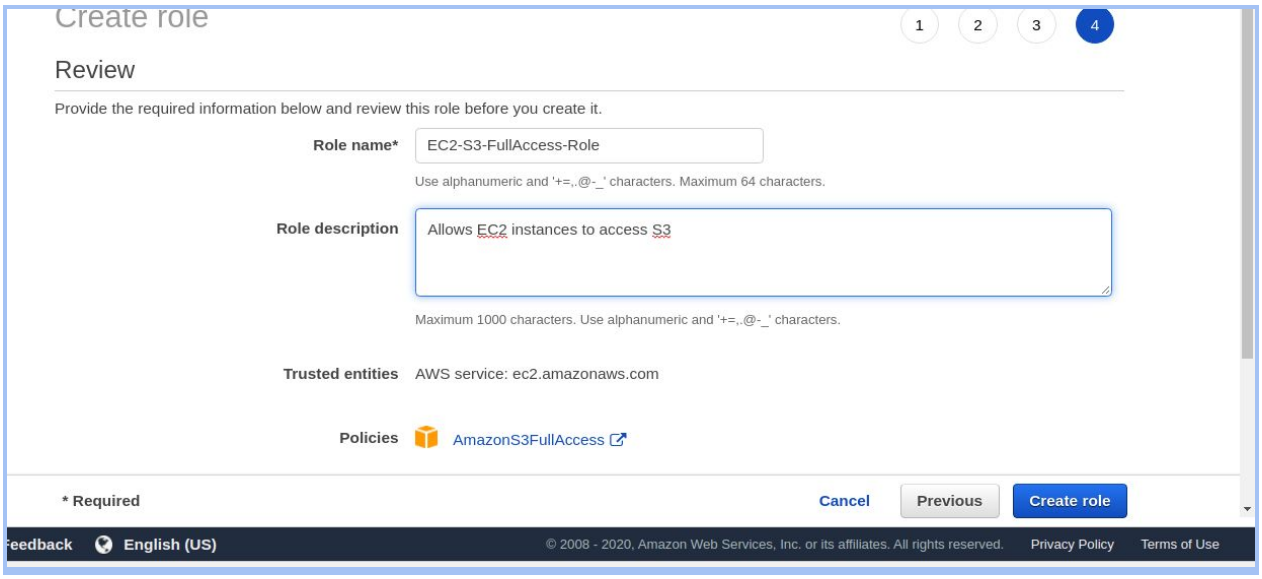
Ans.

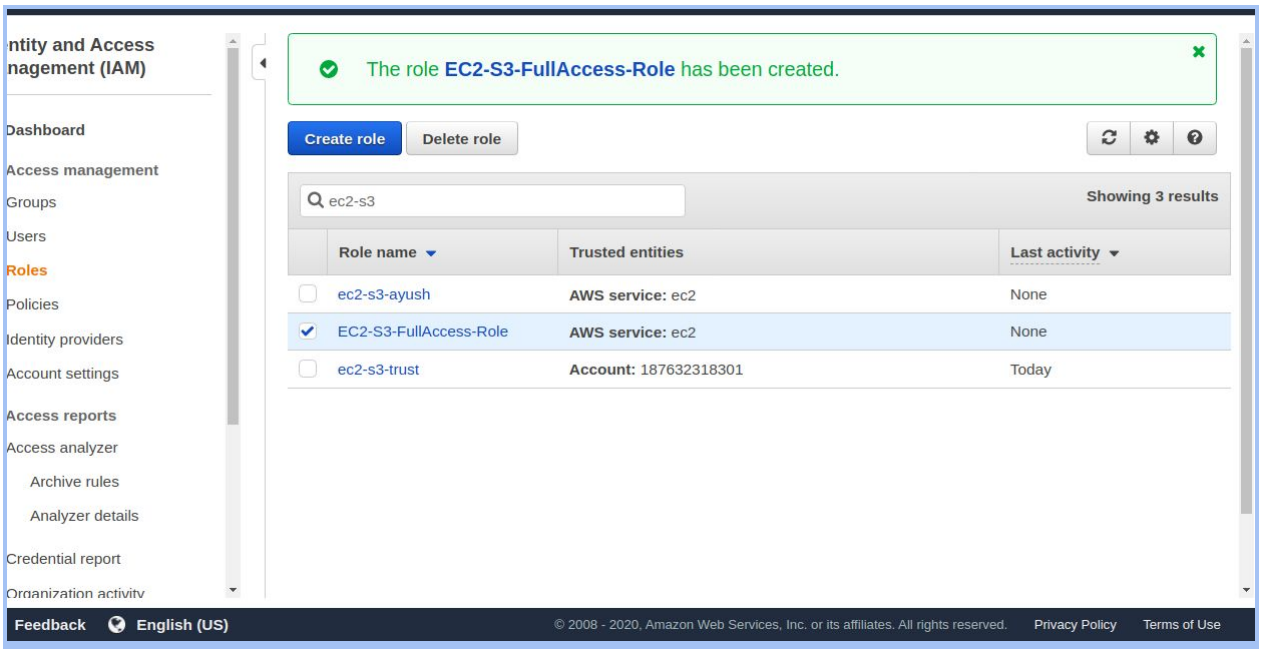
Step 1: Launch an EC2 Instance



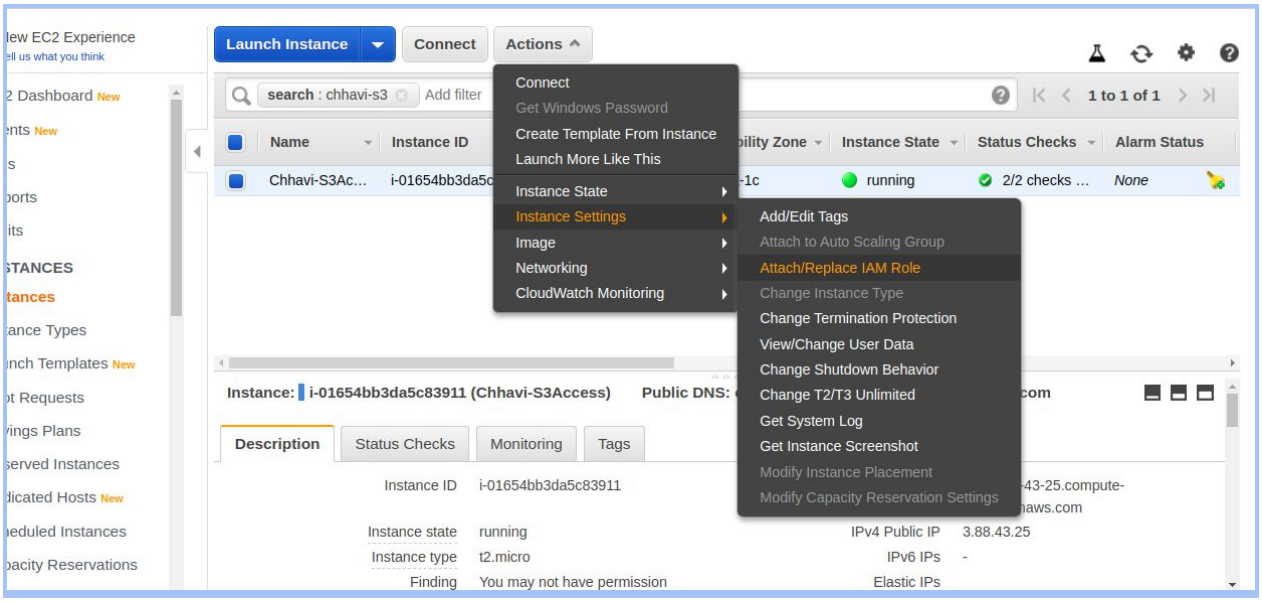
Step 2: Create a role for S3FullAccess.(Attach S3FullAccess policy to role)

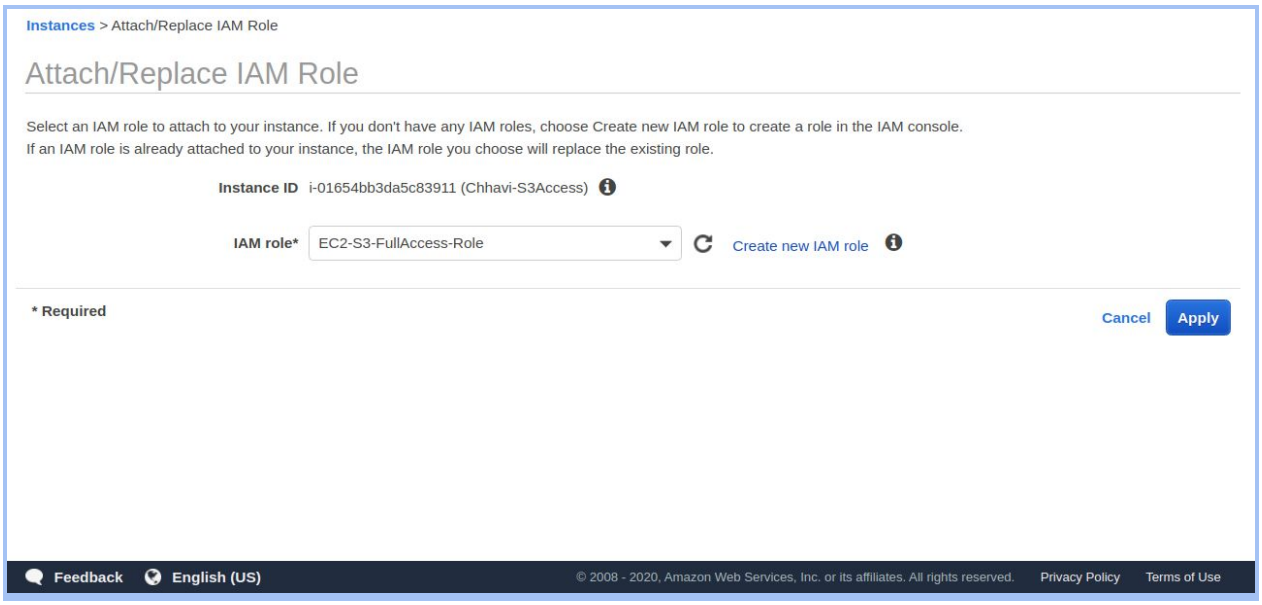

Create role
1
2
3
4
Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
Filter policies
s3full
Showing 1 result
Policy name
Used as
AmazonS3FullAccess
Permissions policy (41)
* Required
Cancel
Previous
Next: Tags


Create role
1
2
3
4
Review
Provide the required information below and review this role before you create it.
Role name*
EC2-S3-FullAccess-Role
Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.
Role description
Allows EC2 instances to access S3
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Trusted entities
AWS service: ec2.amazonaws.com
Policies
AmazonS3FullAccess
* Required
Cancel
Previous
Create role
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

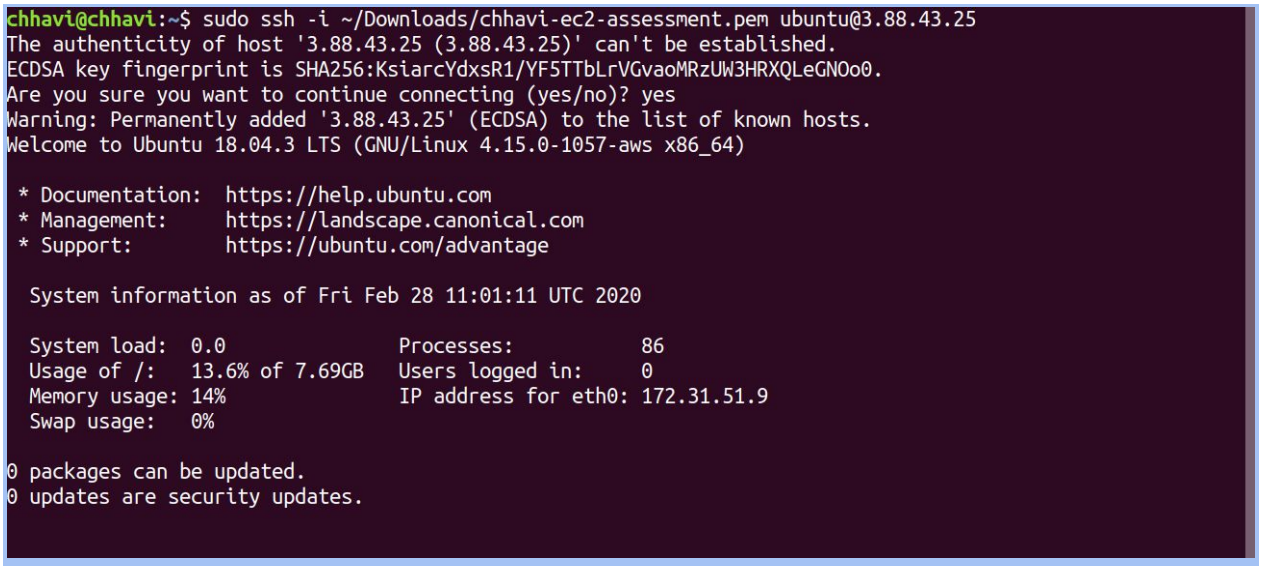


Step 3: Attach role to ec2 instances created





Step 4: ssh into the ec2 instance.



```
chhavi@chhavi:~$ sudo ssh -i ~/Downloads/chhavi-ec2-assessment.pem ubuntu@3.88.43.25
The authenticity of host '3.88.43.25 (3.88.43.25)' can't be established.
ECDSA key fingerprint is SHA256:KsiarcYdxsR1/YF5TTbLrVGvaoMRzUW3HRXQLeGNOo0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '3.88.43.25' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Feb 28 11:01:11 UTC 2020

  System load:  0.0               Processes:           86
  Usage of /:   13.6% of 7.69GB   Users logged in:     0
  Memory usage: 14%               IP address for eth0: 172.31.51.9
  Swap usage:   0%

0 packages can be updated.
0 updates are security updates.
```

Update and install awscli.Now write aws s3 ls.

```
ubuntu@ip-172-31-51-9:~$ aws s3 ls
2019-06-26 12:11:08 0testuser11
2018-04-20 16:59:22 187632318301-awsmacietrail-dataevent
2019-04-02 10:11:33 7testdemo
2019-03-11 04:51:59 abhimanyucftemplate
2020-02-28 10:55:02 abhishek-bootcamp
2019-03-04 06:55:23 abneesh1
2019-03-11 11:00:41 adityamun007
2020-02-26 16:26:29 akshaybuck1
2020-02-27 08:55:25 aman-khandelwal-1
2019-03-07 09:40:48 anmol-bootcamp19
2019-03-08 00:25:58 avcabc
2017-09-07 03:41:42 aws-codestar-us-east-1-187632318301
2017-09-07 04:23:01 aws-codestar-us-east-1-187632318301-codestartest2-app
2017-09-07 04:23:07 aws-codestar-us-east-1-187632318301-codestartest2-pipe
2017-09-07 03:41:48 aws-codestar-us-east-1-187632318301-codestarttest-pipe
2019-06-26 05:39:55 aws-lambda-trigger-ronozor
2020-02-28 03:56:49 ayush-public-bucket
2020-02-25 07:02:11 baban-123
2018-02-14 12:28:43 cf-templates-71mx96ojlvv5-us-east-1
2019-03-27 15:57:27 cfront1
2020-02-26 11:51:54 chirag-bucket-2
2020-02-26 11:46:43 chirag-bucket1
2019-03-27 20:34:52 cloudfront8
2020-02-25 10:59:18 copy-test-delete
```

9. You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Define the tags on the test and production servers and add a condition to the IAMPolicy which allows access to specific tags.

Ans.

Create two instances

Create two users

Production - chhaviprod

Development - chhavidev

User details

User names	chhaviprod and chhavidev
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes

Download .csv

		User	Access key ID	Secret access key	Email login instructions
▸	✓	chhaviprod	AKIASXL6B65O233OLB65	********* Show	Send email
▸	✓	chhavidev	AKIASXL6B65OSQ2NUSA3	********* Show	Send email

Close

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy

Policy for production

Visual editor JSON Import managed policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEquals": {
```

Character count: 328 of 6,144. Cancel Review policy

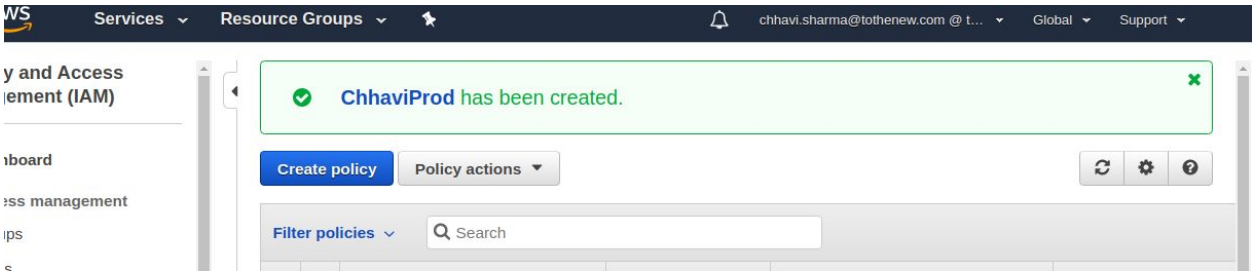
Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

credentials (1).csv chhavi-assig...pem Show all

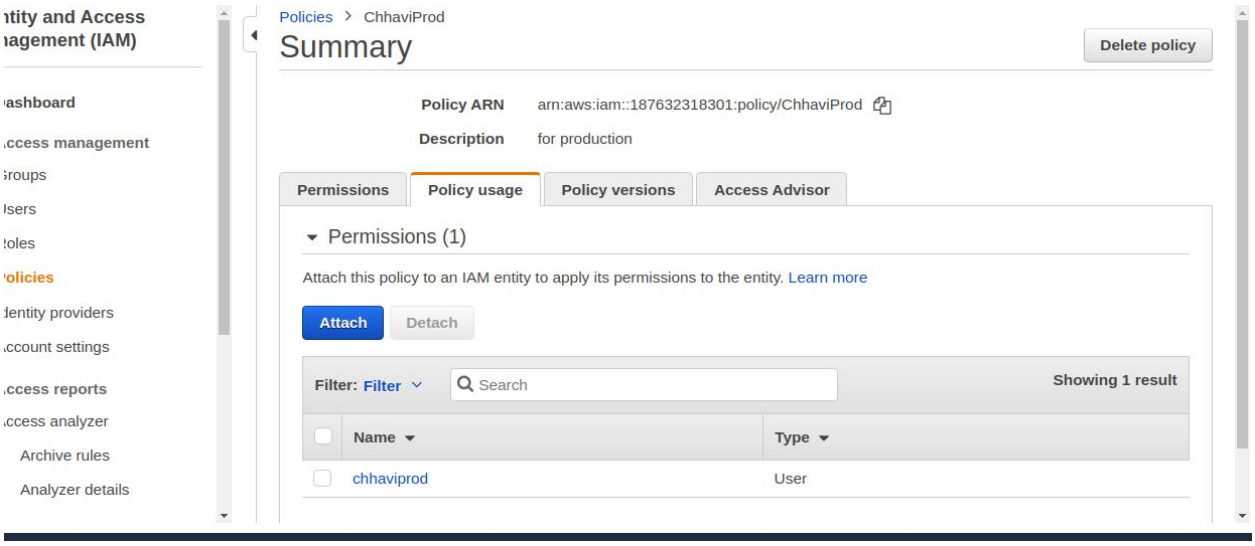
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor | JSON | Import managed policy

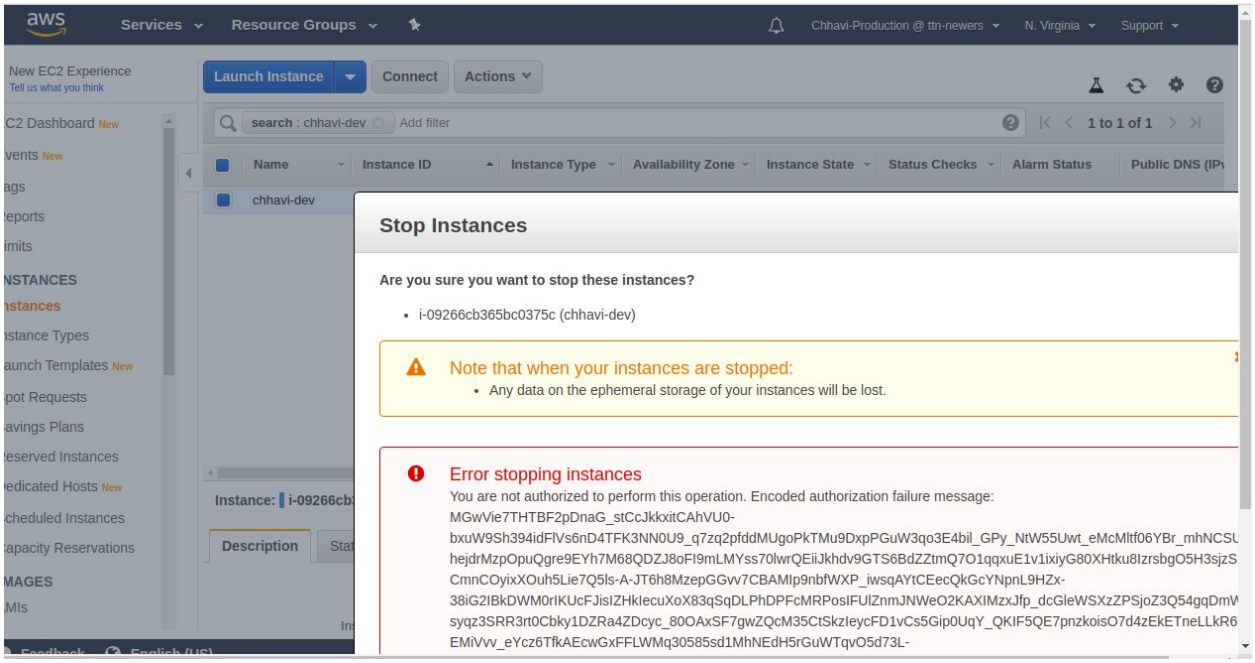
```
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Name": "chhavi-prod"
                }
            }
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
```



Attach to a user



Now login to the users account and try to start/stop an instances that belongs to chhavi-dev tag.You get the following error.



Incase of Development, just change the resource Resource tags.

10. Create a policy for allowing users to set or rotate their credentials, such as their console password, their programmatic access keys, and their MFA devices.

Ans.

Go to IAM -> Policy - >Create Policy

Visual editor | JSON | Import managed policy

```
13                "iam:ResyncMFADevice",
14                "iam:UpdateAccessKey",
15                "iam:CreateVirtualMFADevice",
16                "iam:ListMFADevices",
17                "iam:ChangePassword",
18                "iam:CreateAccessKey",
19                "iam:ListAccessKeys"
20            ],
21            "Resource": "arn:aws:iam::187632318301:user/${aws=username}"
22        },
23        {
24            "Sid": "VisualEditor1",
25            "Effect": "Allow",
26            "Action": "iam:ListVirtualMFADevices",
27            "Resource": "*"
28        }
29    ]
30 }
```