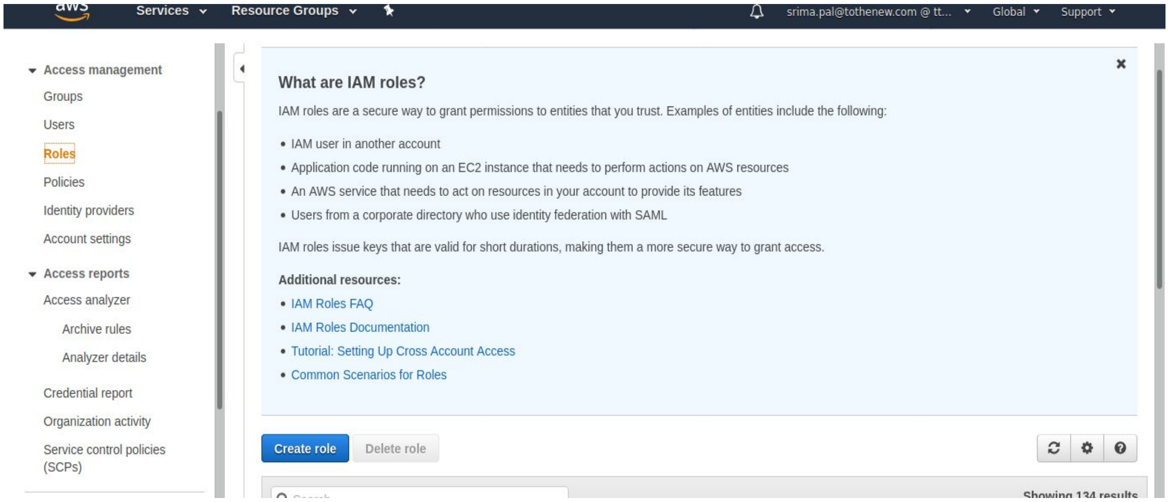
1. Create a Role with full access to S3

Go to IAM and select create role



What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

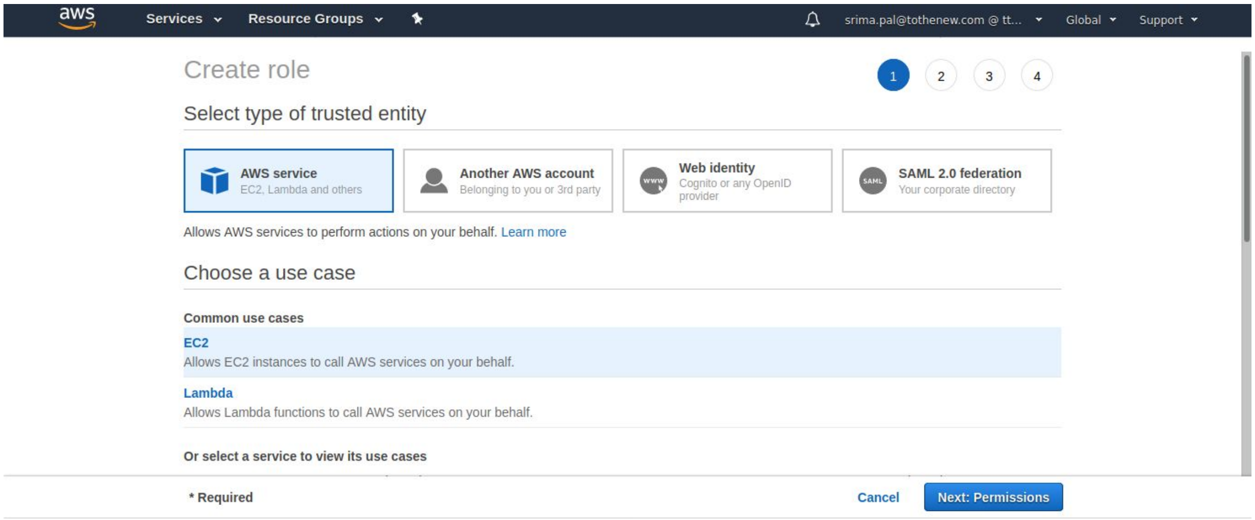
- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

Select the service you want to give access to s3



Create role

Select type of trusted entity

Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

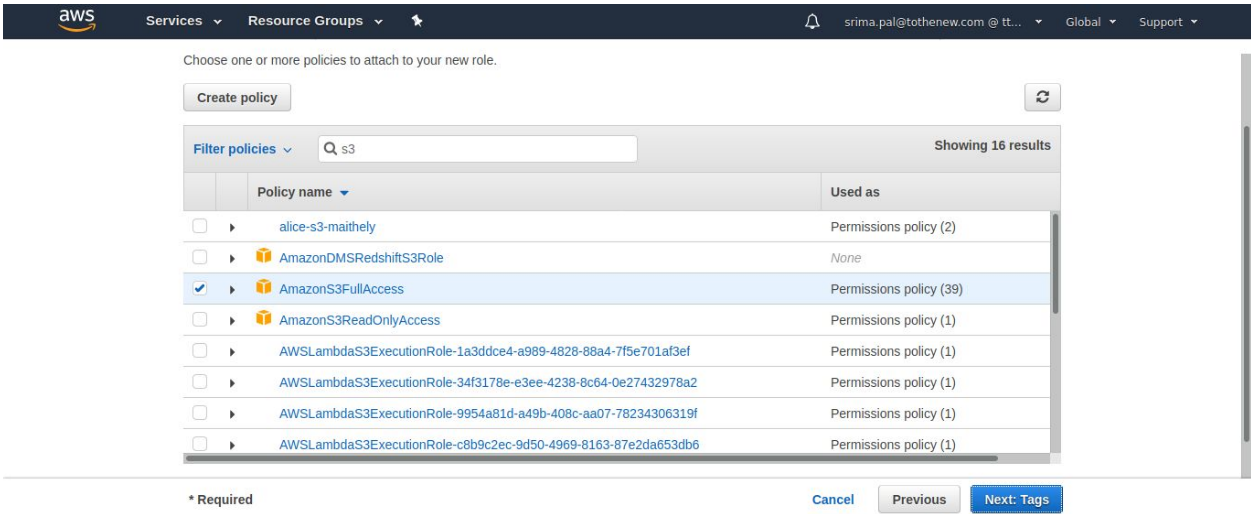
EC2
Allows EC2 instances to call AWS services on your behalf.

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

Or select a service to view its use cases

* Required

Select a policy with permission you want to give to ec2 (s3 full access)



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

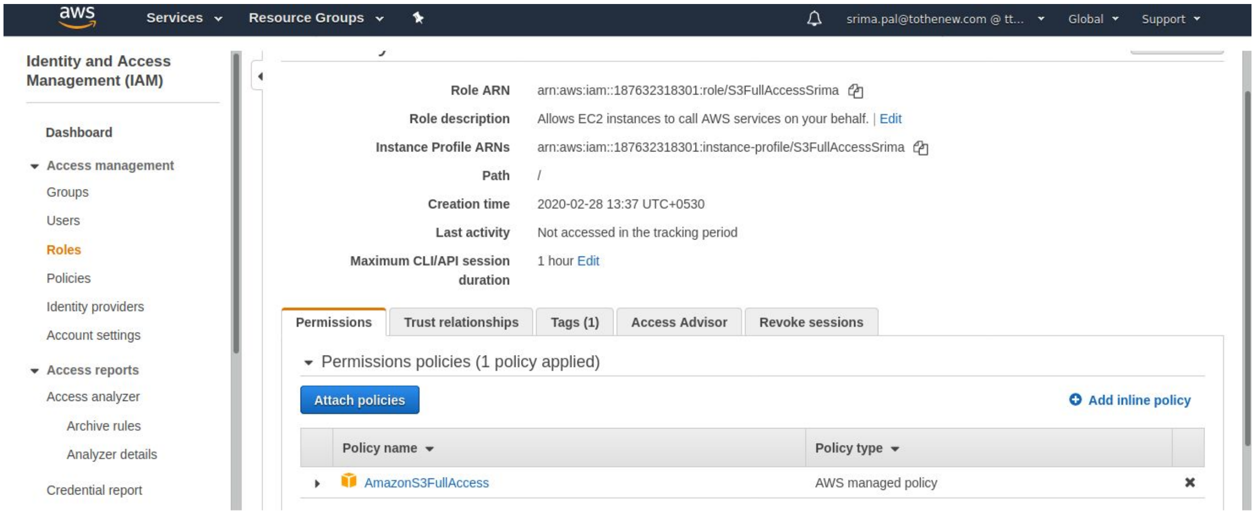
s3

Showing 16 results

		Policy name	Used as
□	▸	alice-s3-maithely	Permissions policy (2)
□	▸	AmazonDMSRedshiftS3Role	None
☑	▸	AmazonS3FullAccess	Permissions policy (39)
□	▸	AmazonS3ReadOnlyAccess	Permissions policy (1)
□	▸	AWSLambdaS3ExecutionRole-1a3ddce4-a989-4828-88a4-7f5e701af3ef	Permissions policy (1)
□	▸	AWSLambdaS3ExecutionRole-34f3178e-e3ee-4238-8c64-0e27432978a2	Permissions policy (1)
□	▸	AWSLambdaS3ExecutionRole-9954a81d-a49b-408c-aa07-78234306319f	Permissions policy (1)
□	▸	AWSLambdaS3ExecutionRole-c8b9c2ec-9d50-4969-8163-87e2da653db6	Permissions policy (1)

* Required

Create a role



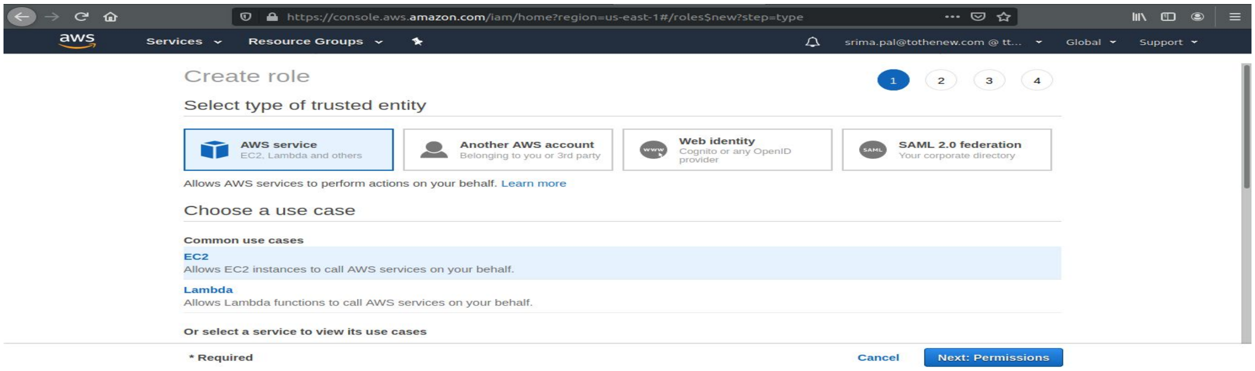
Role ARN	arn:aws:iam::187632318301:role/S3FullAccessSrima
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/S3FullAccessSrima
Path	/
Creation time	2020-02-28 13:37 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions policies (1 policy applied)

	Policy name	Policy type	
▸	AmazonS3FullAccess	AWS managed policy	✖

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

Create a role with service EC2



Create role

Select type of trusted entity

Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

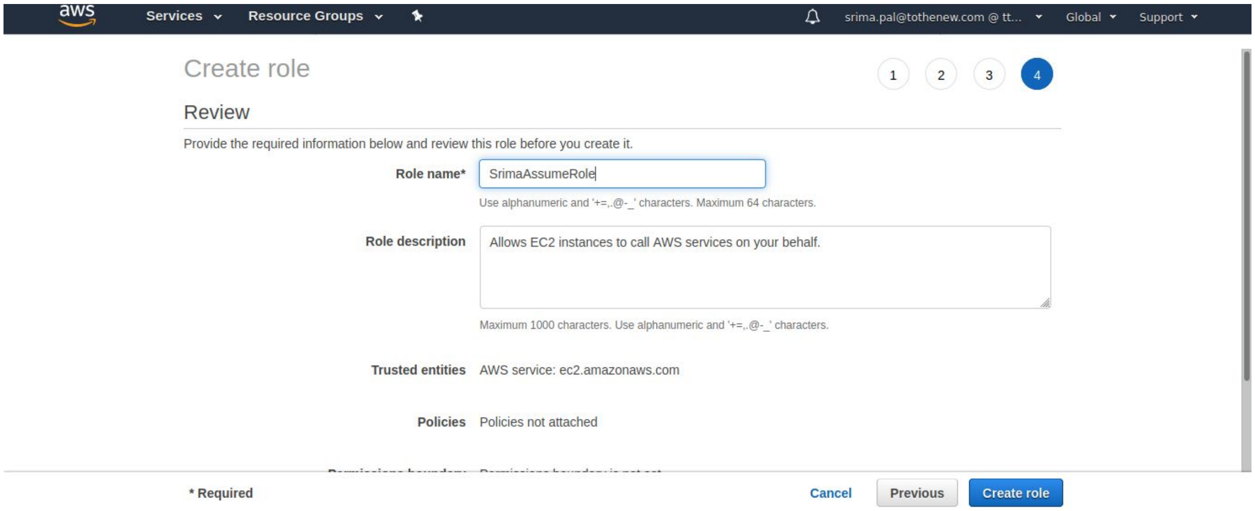
EC2
Allows EC2 instances to call AWS services on your behalf.

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

Or select a service to view its use cases

* Required

Create an assumed role with no attached policy



Create role

Review

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

Role name* SrimaAssumeRole

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

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

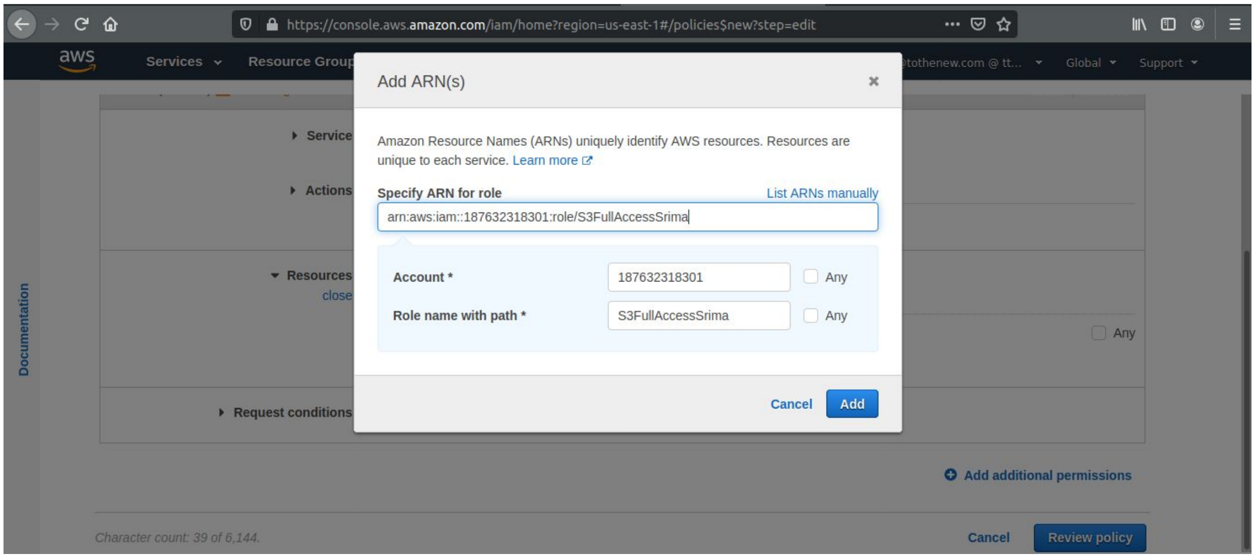
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies Policies not attached

* Required

Create a policy to attach with the above role



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for role — List ARNs manually

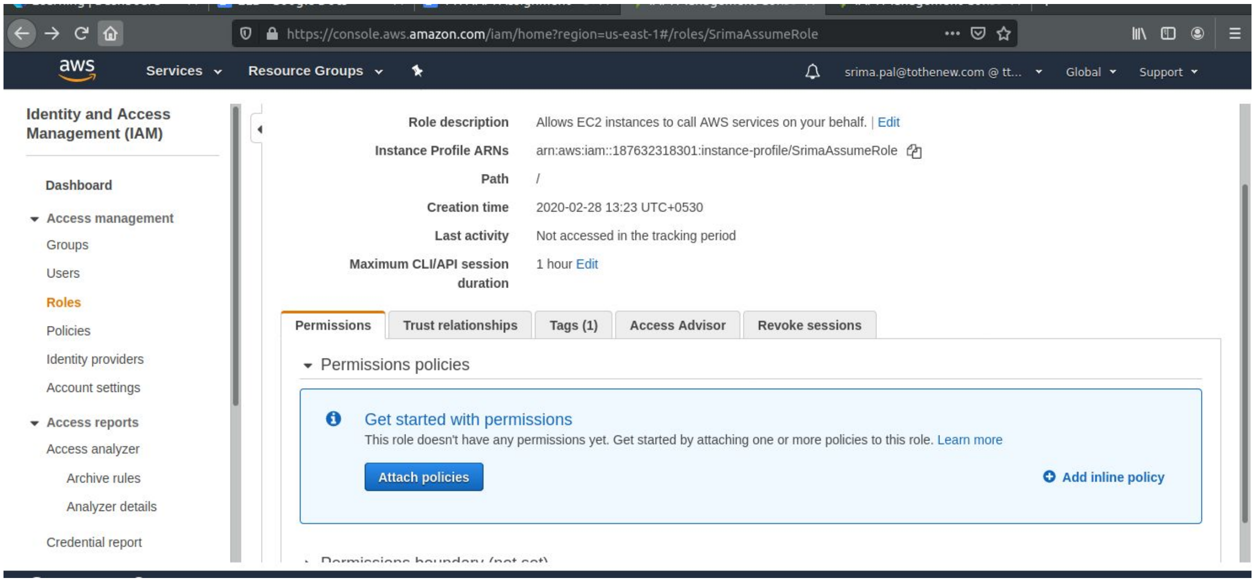
arn:aws:iam::187632318301:role/S3FullAccessSrima

Account *	187632318301	□ Any
Role name with path *	S3FullAccessSrima	□ Any

Cancel Add

Character count: 39 of 6,144.

Attach the created policy



Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/SrimaAssumeRole
Path	/
Creation time	2020-02-28 13:23 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

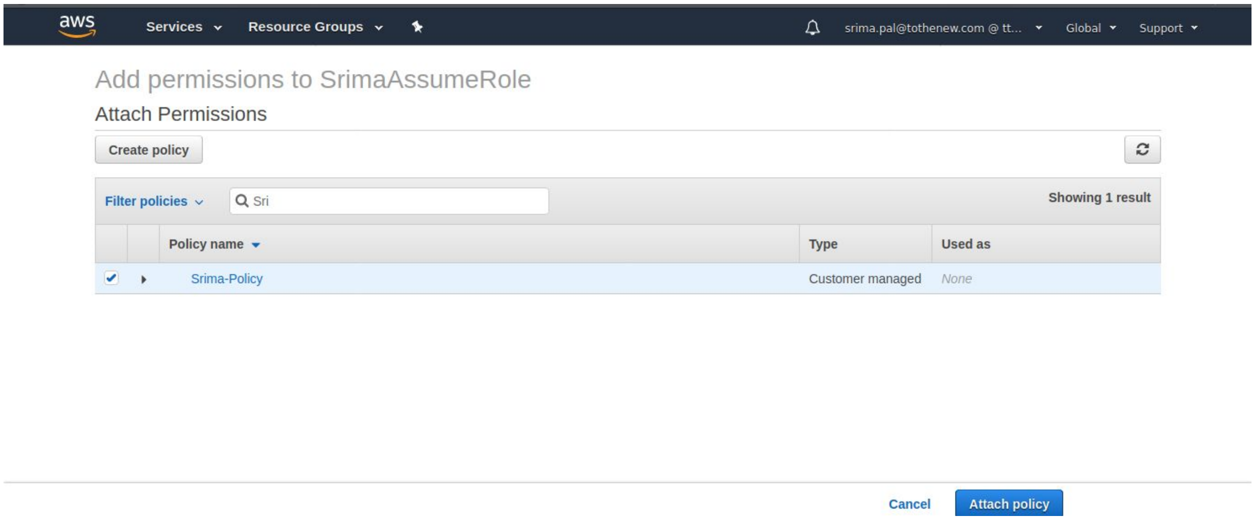
Permissions policies

Get started with permissions

This role doesn't have any permissions yet. Get started by attaching one or more policies to this role. Learn more

Attach policies Add inline policy

Permissions boundary (not set)



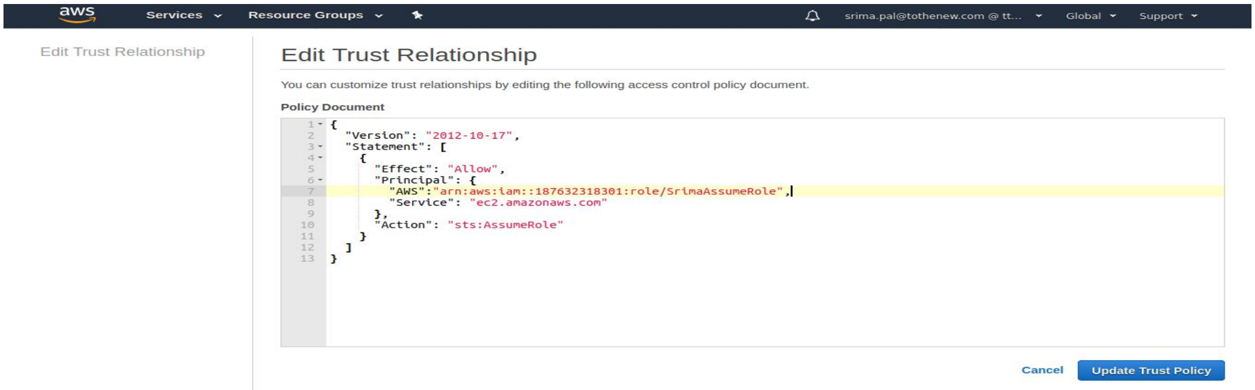
Add permissions to SrimaAssumeRole

Attach Permissions

Showing 1 result

	Policy name	Type	Used as
☑	Srima-Policy	Customer managed	None

Update trust relationship of S3fullaccess role



Edit Trust Relationship

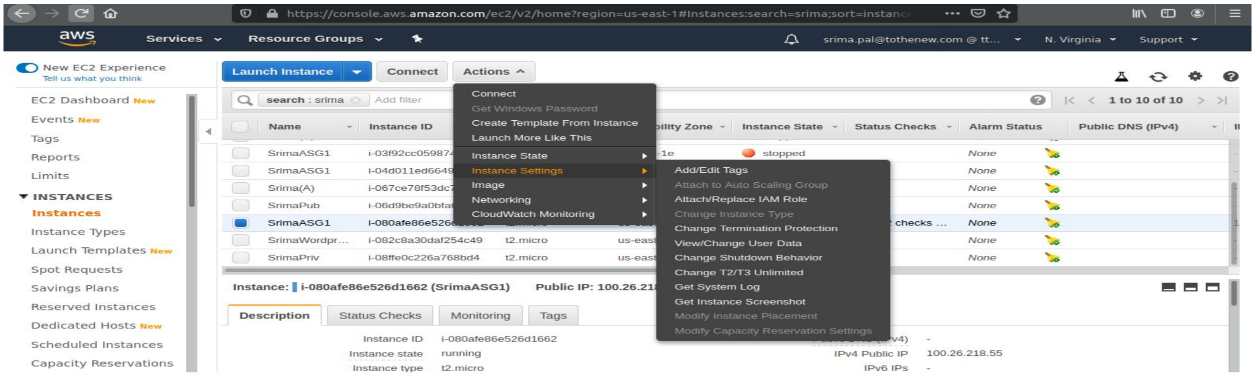
You can customize trust relationships by editing the following access control policy document.

Policy Document

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

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

Attach the assume role to the EC2 instance

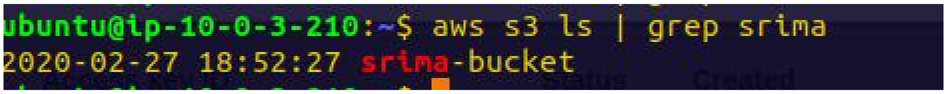


Name	Instance ID		bility Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
SrimaASG1	i-03f92cc059874		-1e	stopped		None	
SrimaASG1	i-04d011ed6649					None	
Srima(A)	i-067ce78f53dc7					None	
SrimaPub	i-06d9be9a0bfa					None	
SrimaASG1	i-080afe86e526				checks ...	None	
SrimaWordpr...	i-082c8a30daf254c49	t2.micro	us-east			None	
SrimaPriv	i-08ffe0c226a768bd4	t2.micro	us-east			None	

Instance: i-080afe86e526d1662 (SrimaASG1) Public IP: 100.26.21

Instance ID i-080afe86e526d1662
Instance state running
Instance type t2.micro

IPv4 Public IP 100.26.218.55
IPv6 IPs -



```
ubuntu@ip-10-0-3-210:~$ aws s3 ls | grep srima
2020-02-27 18:52:27 srima-bucket
```

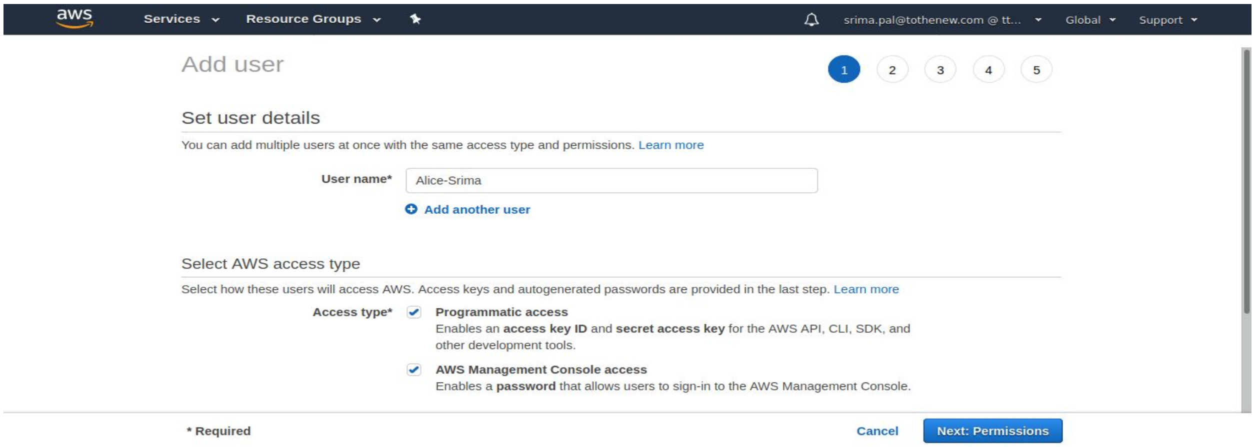
4. Create a group for "Data Administrator" where the user 'Alice' be a member of this group. This group will prepare the data for the analysis. So Provide the following access to the group.

Service: Amazon S3;

Action:

- **Get*,**
- **List*,**
- **Put*,**
- **ARN: Input and output Buckets (no conditions**

Create a user Alice



Add user

Set user details

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

User name* Alice-Srima

Select AWS access type

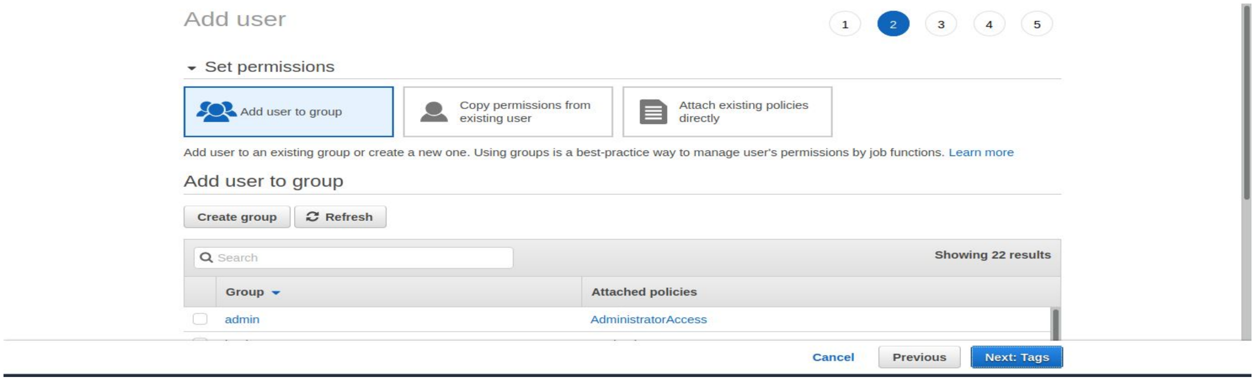
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

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.

* Required

Create a group for that user



Add user

Set permissions

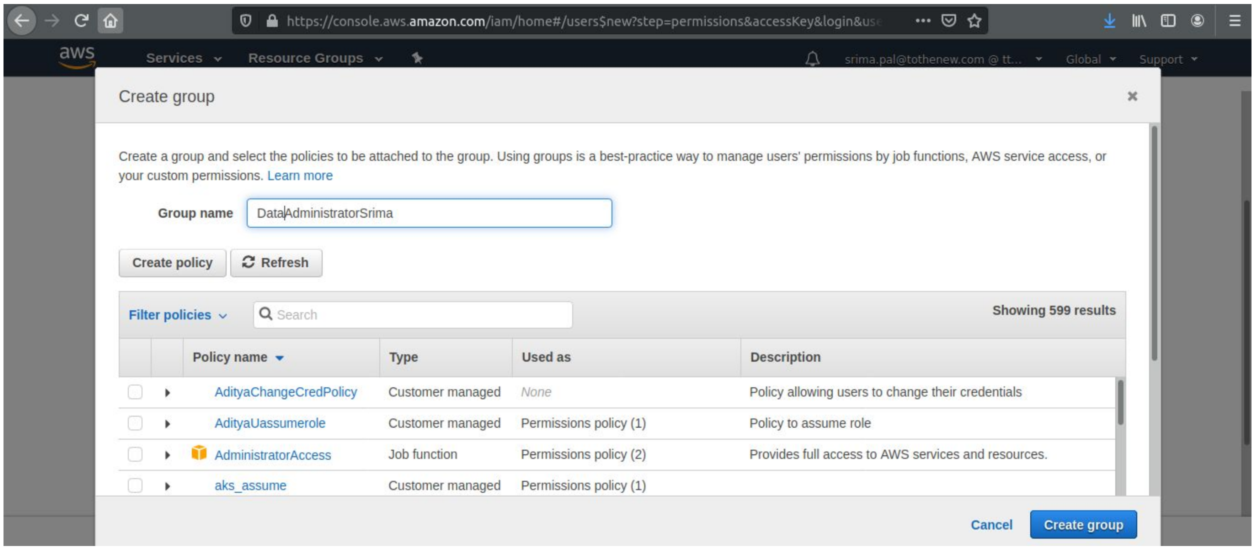
Add user to group
Copy permissions from existing user
Attach existing policies directly

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 22 results

	Group	Attached policies
□	admin	AdministratorAccess



https://console.aws.amazon.com/iam/home#/users$new?step=permissions&accessKey&login&use

Create group

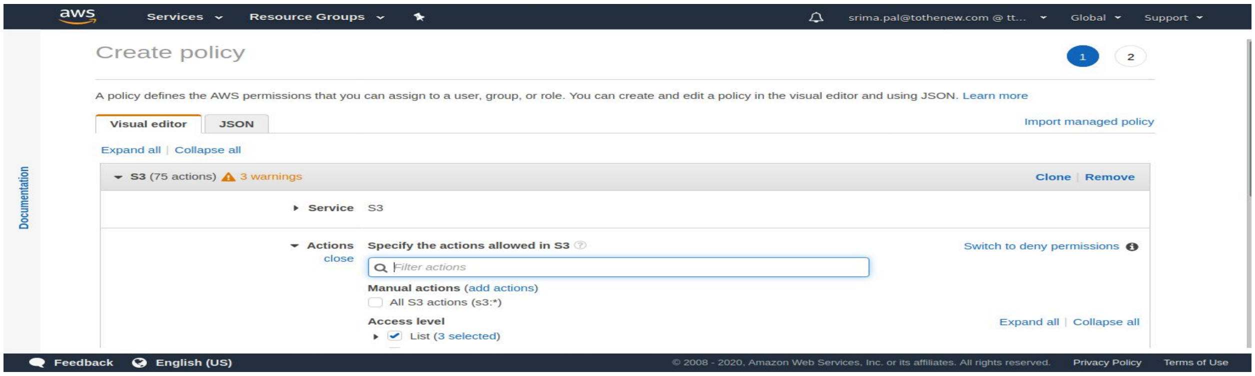
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: DataAdministratorSrima

Showing 599 results

		Policy name	Type	Used as	Description
□	▸	AdityaChangeCredPolicy	Customer managed	None	Policy allowing users to change their credentials
□	▸	AdityaUassumerole	Customer managed	Permissions policy (1)	Policy to assume role
□	▸	AdministratorAccess	Job function	Permissions policy (2)	Provides full access to AWS services and resources.
□	▸	aks_assume	Customer managed	Permissions policy (1)	

Create a policy for that group



aws
Services
Resource Groups
srima.pal@tothenew.com @ tt...
Global
Support
Documentation

Create policy

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
Expand all | Collapse all

S3 (75 actions) ⚠ 3 warnings

Service: S3

Actions (close) — Specify the actions allowed in S3

Switch to deny permissions
Filter actions

Manual actions (add actions)

□ All S3 actions (s3:*)

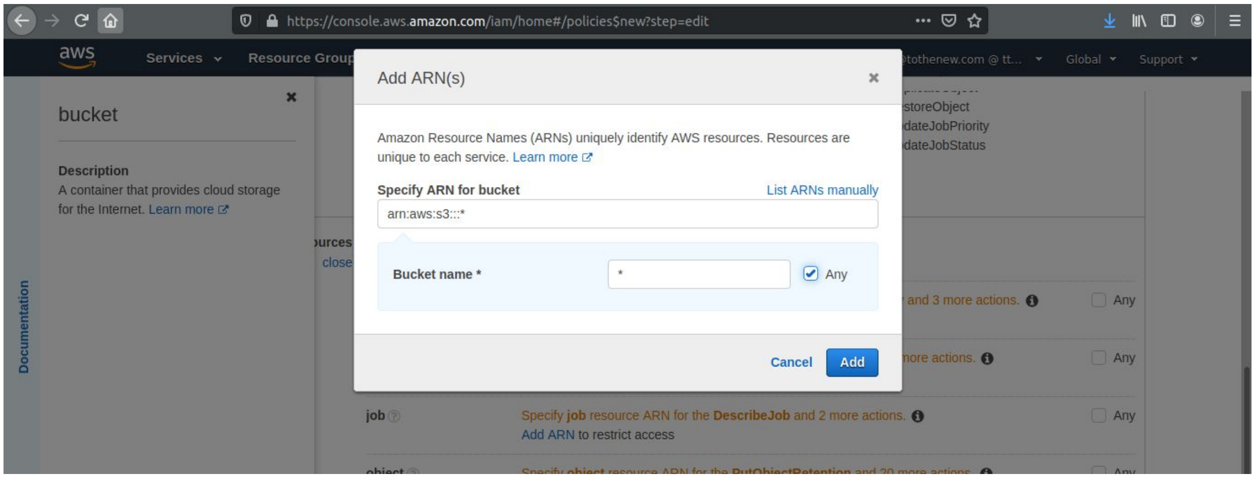
Access level

Expand all | Collapse all

☑ List (3 selected)

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

Specify ARN(All the ARN's)



https://console.aws.amazon.com/iam/home#/policies$new?step=edit

bucket

Description
A container that provides cloud storage for the Internet. Learn more

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

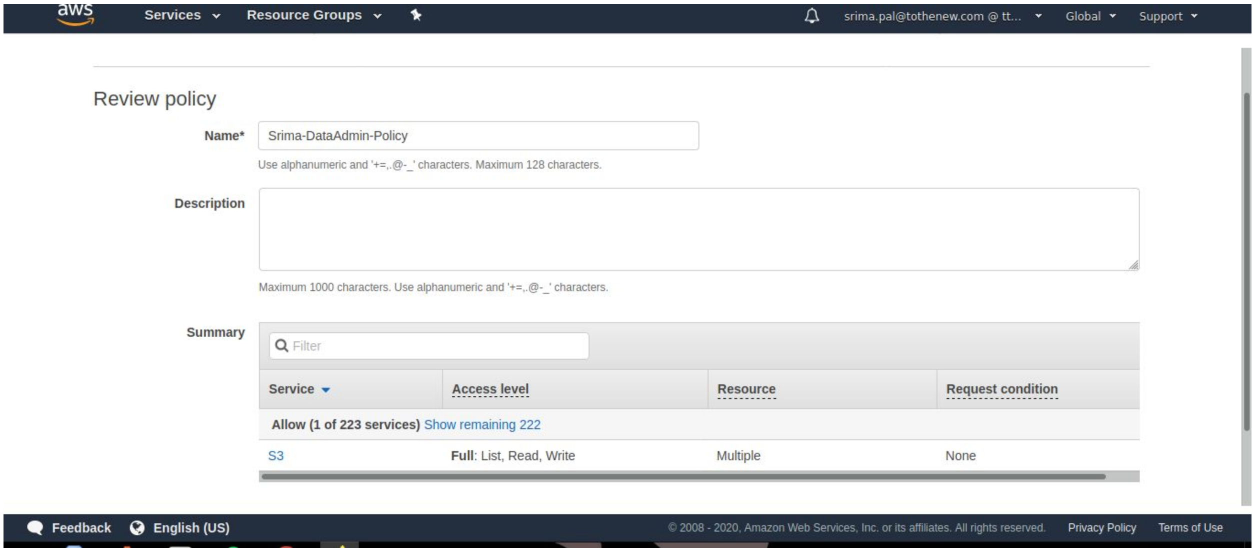
Specify ARN for bucket List ARNs manually

arn:aws:s3:::*

Bucket name * * ☑ Any

Cancel Add

job Specify job resource ARN for the DescribeJob and 2 more actions. Add ARN to restrict access □ Any



Review policy

Name* Srima-DataAdmin-Policy

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

Description

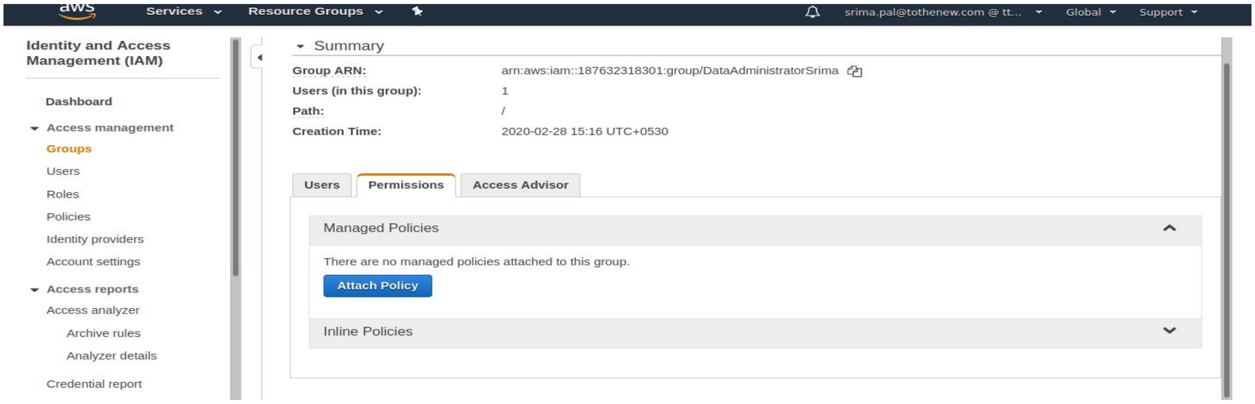
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 223 services) Show remaining 222			
S3	Full: List, Read, Write	Multiple	None

aws
Services
Resource Groups
srima.pal@tothenew.com @ tt...
Global
Support
Filter
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Attach a policy to the group



Summary

Group ARN:	arn:aws:iam::187632318301:group/DataAdministratorSrima
Users (in this group):	1
Path:	/
Creation Time:	2020-02-28 15:16 UTC+0530

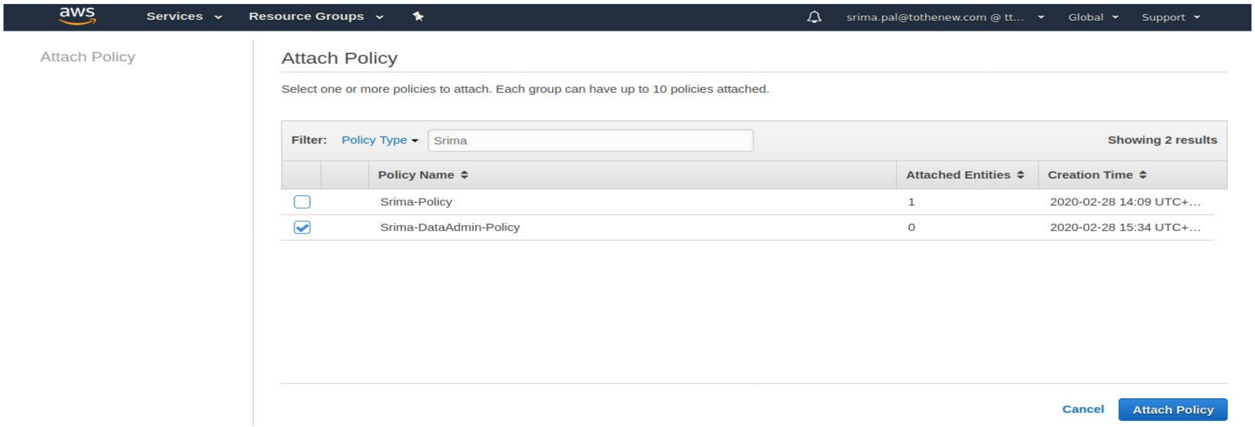
Users | Permissions | Access Advisor

Managed Policies

There are no managed policies attached to this group.

Attach Policy

Inline Policies



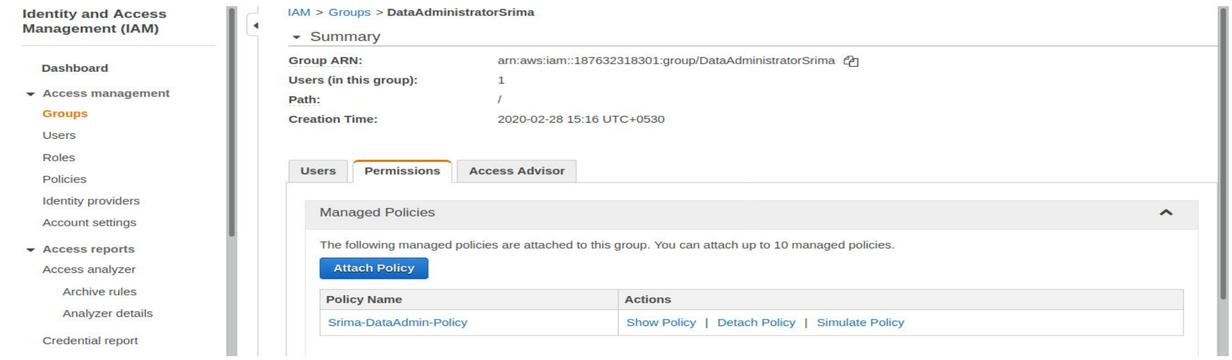
Attach Policy

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ Srima — Showing 2 results

	Policy Name	Attached Entities	Creation Time
□	Srima-Policy	1	2020-02-28 14:09 UTC+...
☑	Srima-DataAdmin-Policy	0	2020-02-28 15:34 UTC+...



IAM > Groups > DataAdministratorSrima

Summary

Group ARN: arn:aws:iam::187632318301:group/DataAdministratorSrima

Users (in this group): 1

Path: /

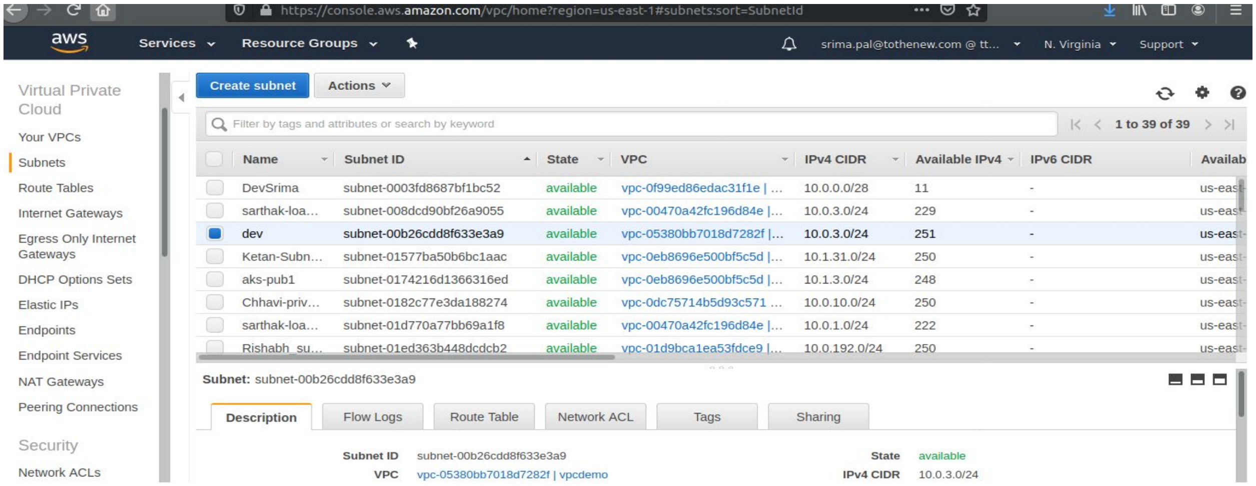
Creation Time: 2020-02-28 15:16 UTC+0530

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
Srima-DataAdmin-Policy	Show Policy | Detach Policy | Simulate Policy

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

Create a subnet dev and copy the subnet id



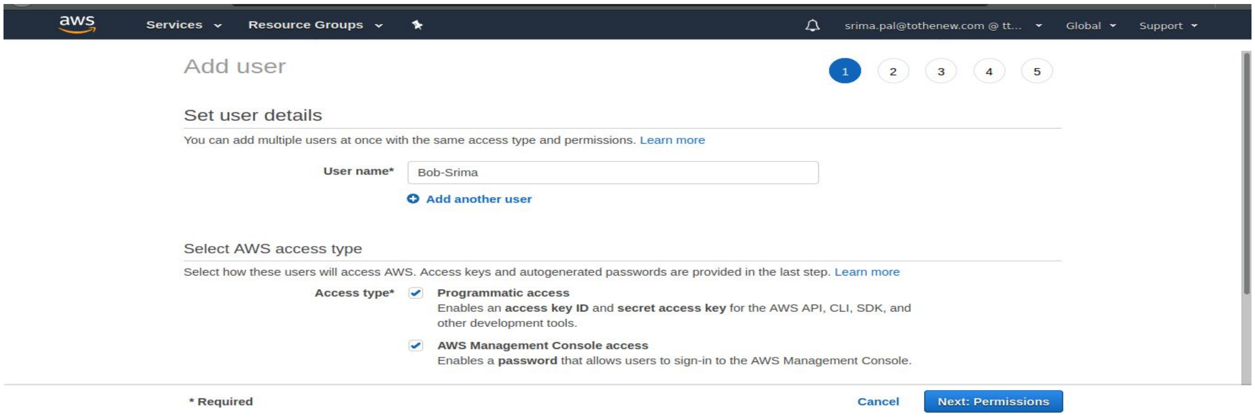
https://console.aws.amazon.com/vpc/home?region=us-east-1#subnets:sort=SubnetId

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availab
□	DevSrima	subnet-0003fd8687bf1bc52	available	vpc-0f99ed86edac31f1e | ...	10.0.0.0/28	11	-	us-eas
□	sarthak-loa...	subnet-008dcd90bf26a9055	available	vpc-00470a42fc196d84e |...	10.0.3.0/24	229	-	us-eas
☑	dev	subnet-00b26cdd8f633e3a9	available	vpc-05380bb7018d7282f |...	10.0.3.0/24	251	-	us-east-
□	Ketan-Subn...	subnet-01577ba50b6bc1aac	available	vpc-0eb8696e500bf5c5d |...	10.1.31.0/24	250	-	us-east-
□	aks-pub1	subnet-0174216d1366316ed	available	vpc-0eb8696e500bf5c5d |...	10.1.3.0/24	248	-	us-east-
□	Chhavi-priv...	subnet-0182c77e3da188274	available	vpc-0dc75714b5d93c571 ...	10.0.10.0/24	250	-	us-east-
□	sarthak-loa...	subnet-01d770a77bb69a1f8	available	vpc-00470a42fc196d84e |...	10.0.1.0/24	222	-	us-east-
□	Rishabh_su...	subnet-01ed363b448dcdcb2	available	vpc-01d9bca1ea53fdce9 |...	10.0.192.0/24	250	-	us-east-

Subnet: subnet-00b26cdd8f633e3a9

Subnet ID subnet-00b26cdd8f633e3a9 State available
VPC vpc-05380bb7018d7282f | vpcdemo IPv4 CIDR 10.0.3.0/24

Create a new user BOB



Add user

Set user details

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

User name* Bob-Srima

Add another user

Select AWS access type

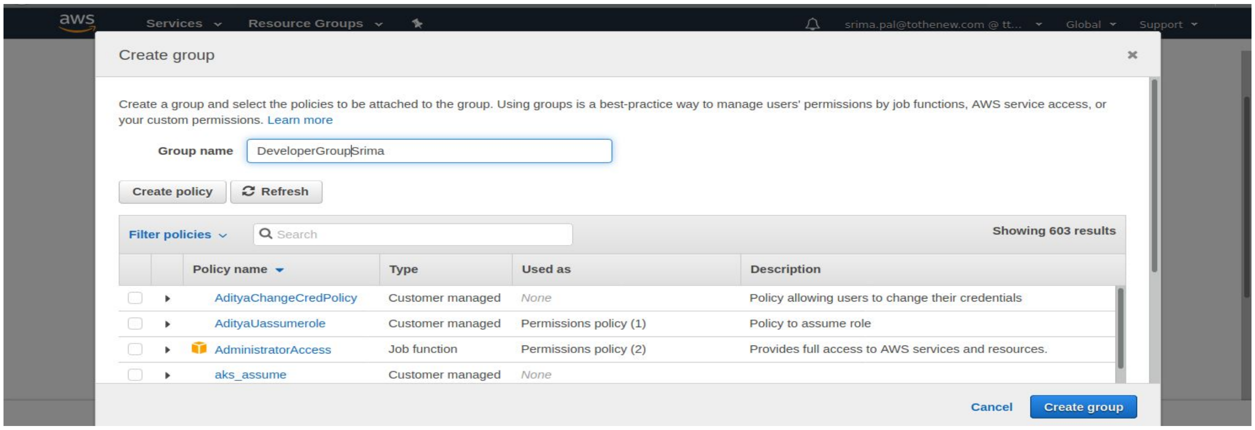
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

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.

* Required

Create a group



Create group

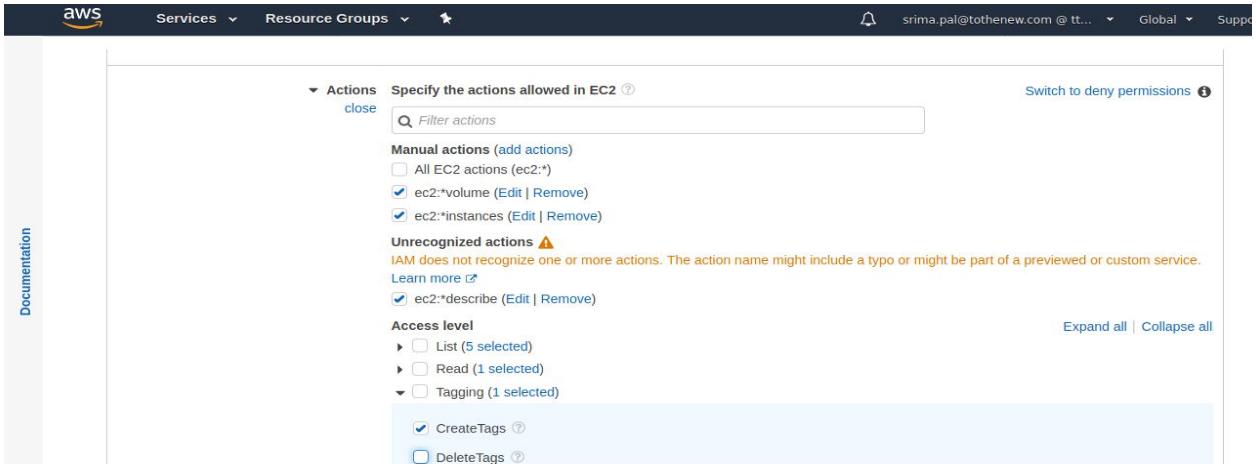
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name DeveloperGroupSrima

Showing 603 results

		Policy name	Type	Used as	Description
□	▸	AdityaChangeCredPolicy	Customer managed	None	Policy allowing users to change their credentials
□	▸	AdityaUassumerole	Customer managed	Permissions policy (1)	Policy to assume role
□	▸	AdministratorAccess	Job function	Permissions policy (2)	Provides full access to AWS services and resources.
□	▸	aks_assume	Customer managed	None	

Create a policy



Specify the actions allowed in EC2

Manual actions (add actions)

□ All EC2 actions (ec2:*)

☑ ec2:*volume (Edit | Remove)

☑ ec2:*instances (Edit | Remove)

Unrecognized actions ⚠

IAM does not recognize one or more actions. The action name might include a typo or might be part of a previewed or custom service. Learn more

☑ ec2:*describe (Edit | Remove)

Access level

▸ □ List (5 selected)

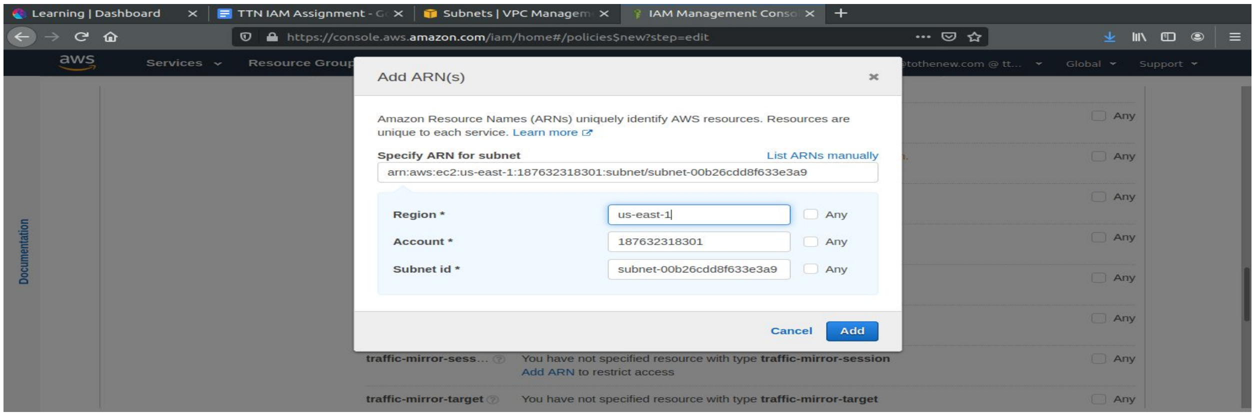
▸ □ Read (1 selected)

▾ □ Tagging (1 selected)

☑ CreateTags

□ DeleteTags

Attach subnet id where you want to grant the access



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for subnet — List ARNs manually

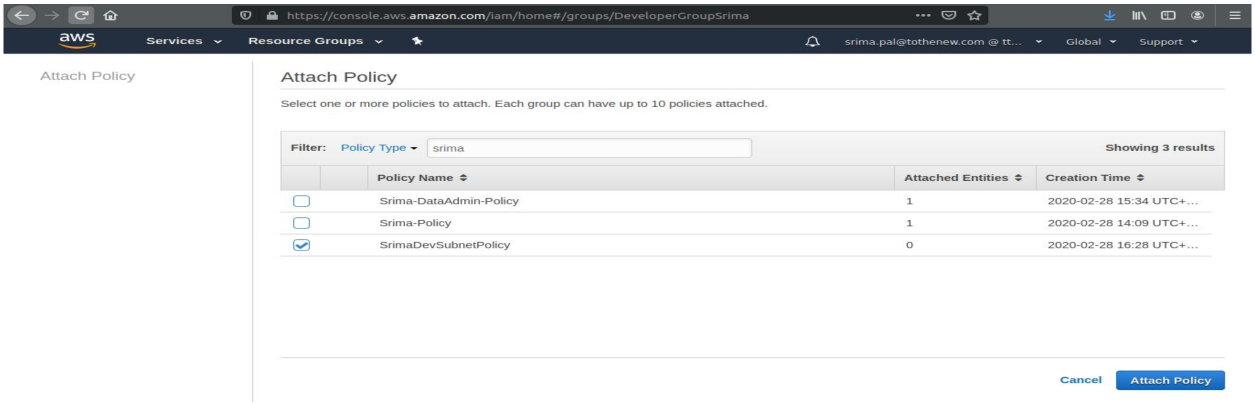
arn:aws:ec2:us-east-1:187632318301:subnet/subnet-00b26cdd8f633e3a9

Region *	us-east-1	□ Any
Account *	187632318301	□ Any
Subnet id *	subnet-00b26cdd8f633e3a9	□ Any

traffic-mirror-sess... You have not specified resource with type **traffic-mirror-session** Add ARN to restrict access □ Any

traffic-mirror-target You have not specified resource with type **traffic-mirror-target** □ Any

Attach policy to the group



https://console.aws.amazon.com/iam/home#/groups/DeveloperGroupSrima
aws
Services
Resource Groups
srima.pal@tothenew.com @ tt...
Global
Support
Attach Policy

Attach Policy

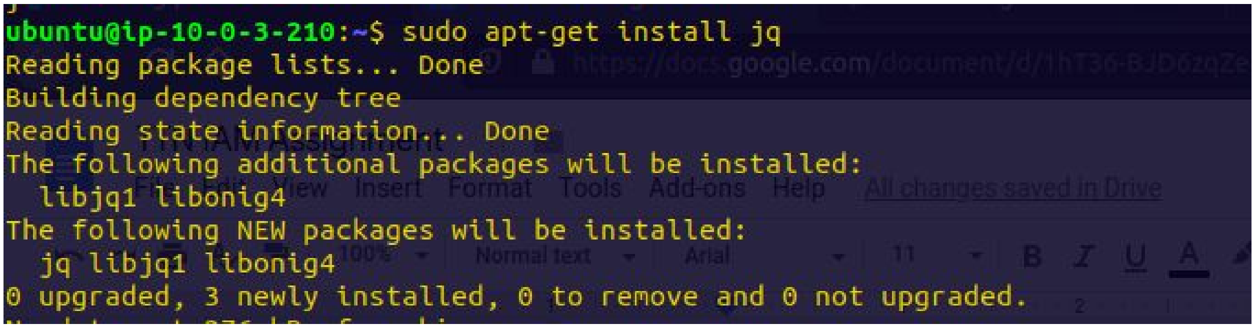
Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type srima — Showing 3 results

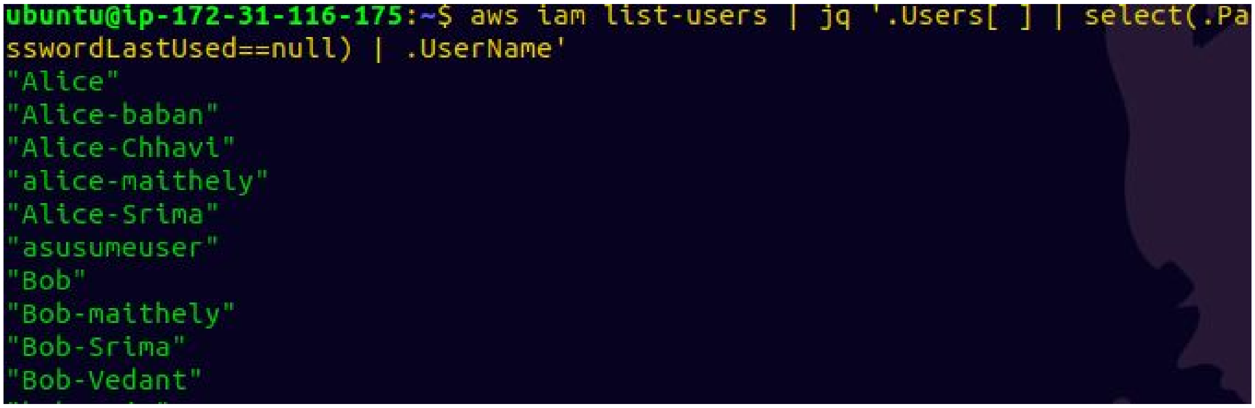
	Policy Name	Attached Entities	Creation Time
□	Srima-DataAdmin-Policy	1	2020-02-28 15:34 UTC+...
□	Srima-Policy	1	2020-02-28 14:09 UTC+...
☑	SrimaDevSubnetPolicy	0	2020-02-28 16:28 UTC+...

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

Download jq

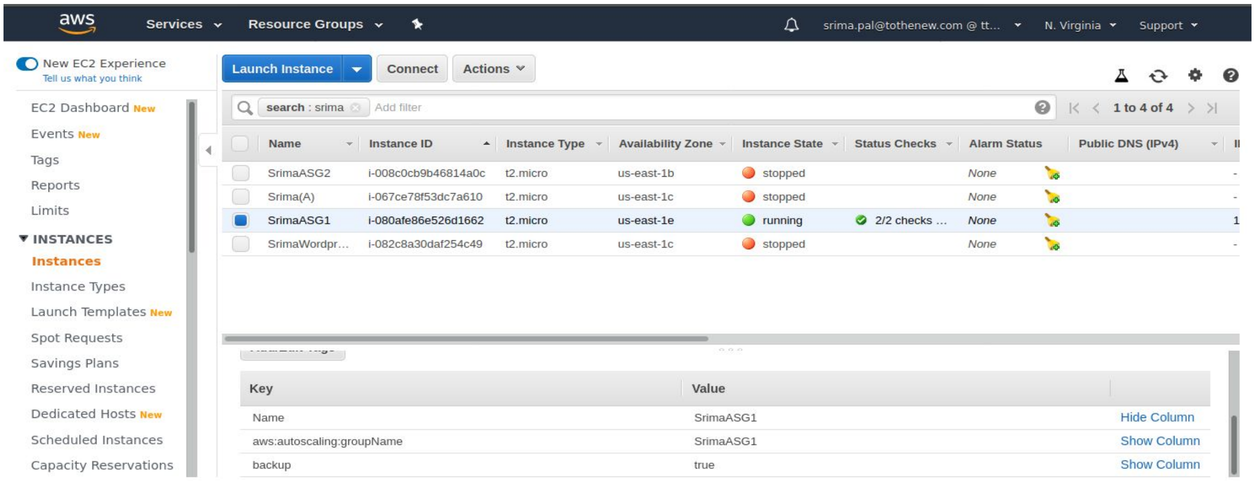


```
ubuntu@ip-10-0-3-210:~$ sudo apt-get install jq
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libjq1 libonig4
The following NEW packages will be installed:
  jq libjq1 libonig4
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
```



```
ubuntu@ip-172-31-116-175:~$ aws iam list-users | jq '.Users[ ] | select(.PasswordLastUsed==null) | .UserName'
"Alice"
"Alice-baban"
"Alice-Chhavi"
"alice-maithely"
"Alice-Srima"
"asusumeuser"
"Bob"
"Bob-maithely"
"Bob-Srima"
"Bob-Vedant"
```

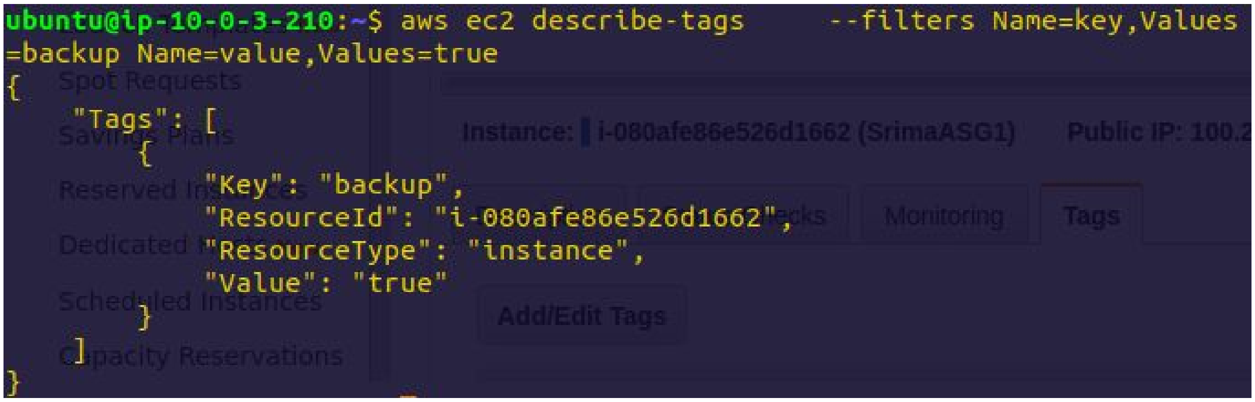
7. Identify all the instances having the tag key-value "backup=true" using AWS CLI.



search : srima   Add filter   1 to 4 of 4

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	I
SrimaASG2	i-008c0cb9b46814a0c	t2.micro	us-east-1b	stopped		None		-
Srima(A)	i-067ce78f53dc7a610	t2.micro	us-east-1c	stopped		None		-
SrimaASG1	i-080afe86e526d1662	t2.micro	us-east-1e	running	2/2 checks ...	None		1
SrimaWordpr...	i-082c8a30daf254c49	t2.micro	us-east-1c	stopped		None		-

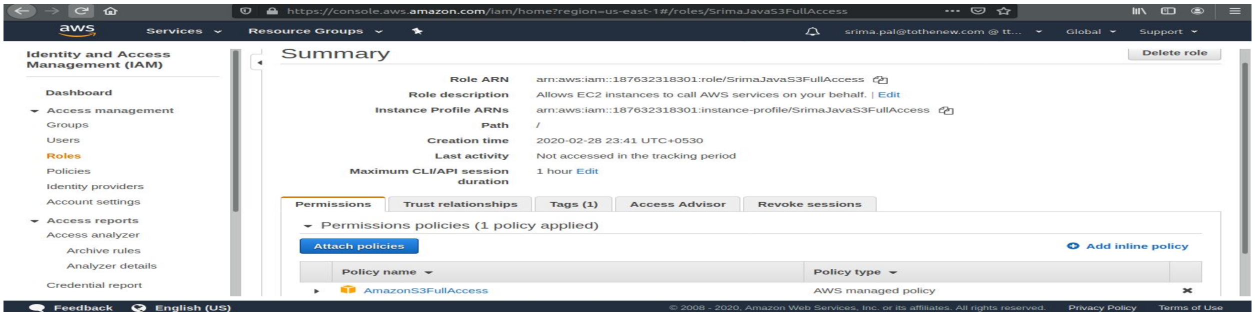
Key	Value	
Name	SrimaASG1	Hide Column
aws:autoscaling:groupName	SrimaASG1	Show Column
backup	true	Show Column



```
ubuntu@ip-10-0-3-210:~$ aws ec2 describe-tags    --filters Name=key,Values=backup Name=value,Values=true
{
    "Tags": [
        {
            "Key": "backup",
            "ResourceId": "i-080afe86e526d1662",
            "ResourceType": "instance",
            "Value": "true"
        }
    ]
}
```

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.

Create a role with s3 full access



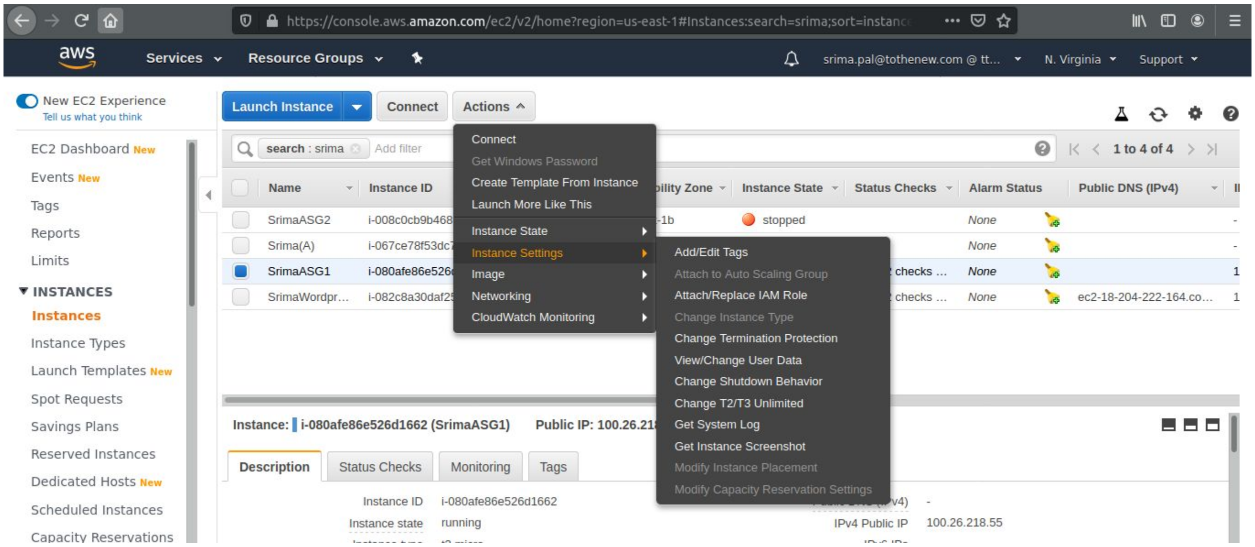
Summary

Role ARN	arn:aws:iam::187632318301:role/SrimaJavaS3FullAccess
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/SrimaJavaS3FullAccess
Path	/
Creation time	2020-02-28 23:41 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions policies (1 policy applied)

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy

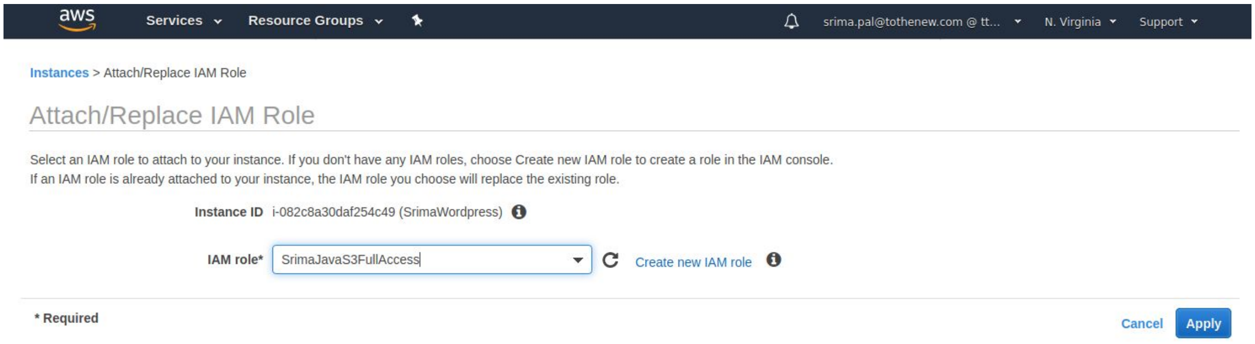
Attach the role to the EC2 instance



Name	Instance ID	...ility Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
SrimaASG2	i-008c0cb9b468	-1b	stopped		None	-
Srima(A)	i-067ce78f53dc7				None	-
SrimaASG1	i-080afe86e526			checks ...	None	
SrimaWordpr...	i-082c8a30daf25			checks ...	None	ec2-18-204-222-164.co...

Instance: i-080afe86e526d1662 (SrimaASG1) Public IP: 100.26.21

Instance ID i-080afe86e526d1662
Instance state running
IPv4 Public IP 100.26.218.55



Attach/Replace IAM Role

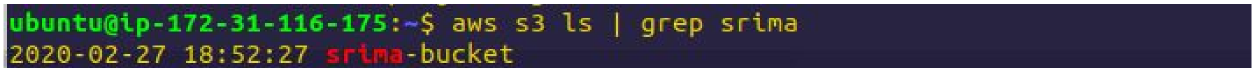
Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console.
If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-082c8a30daf254c49 (SrimaWordpress)

IAM role* SrimaJavaS3FullAccess

* Required

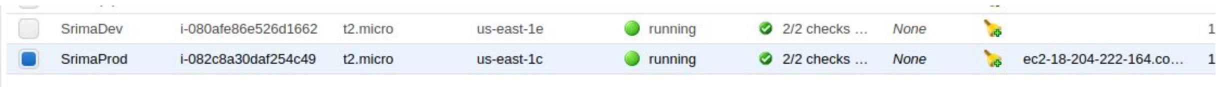
Able to access bucket without putting access keys



```
ubuntu@ip-172-31-116-175:~$ aws s3 ls | grep srima
2020-02-27 18:52:27 srima-bucket
```

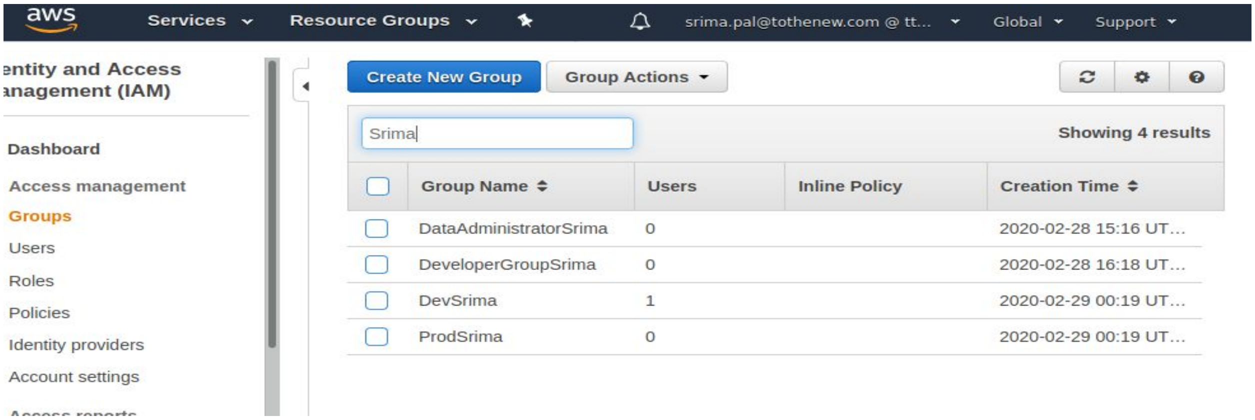
9. You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Define the tags on the test and production servers and add a condition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

Two instances, one dev and one production



☐	SrimaDev	i-080afe86e526d1662	t2.micro	us-east-1e	● running	✓ 2/2 checks ...	None			1
■	SrimaProd	i-082c8a30daf254c49	t2.micro	us-east-1c	● running	✓ 2/2 checks ...	None		ec2-18-204-222-164.co...	1

Create two groups , one for dev, one for prod

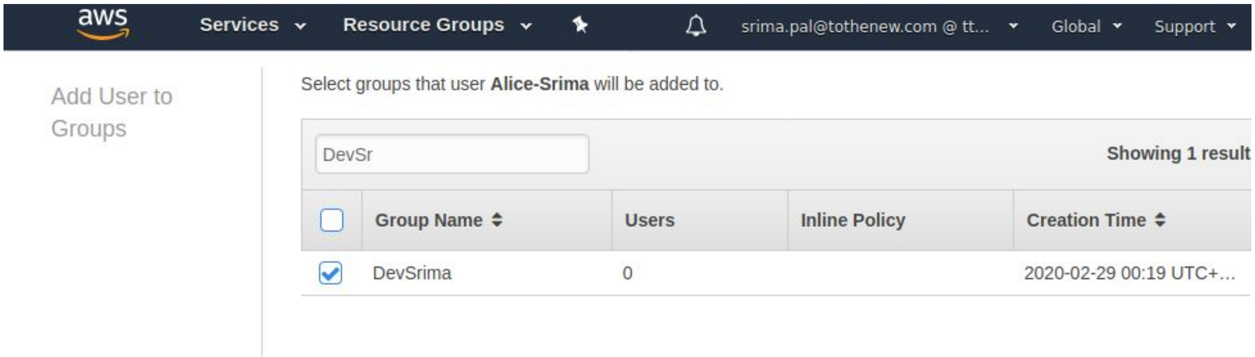


Srima

Showing 4 results

☐	Group Name	Users	Inline Policy	Creation Time
☐	DataAdministratorSrima	0		2020-02-28 15:16 UT...
☐	DeveloperGroupSrima	0		2020-02-28 16:18 UT...
☐	DevSrima	1		2020-02-29 00:19 UT...
☐	ProdSrima	0		2020-02-29 00:19 UT...

Add Alice to dev group



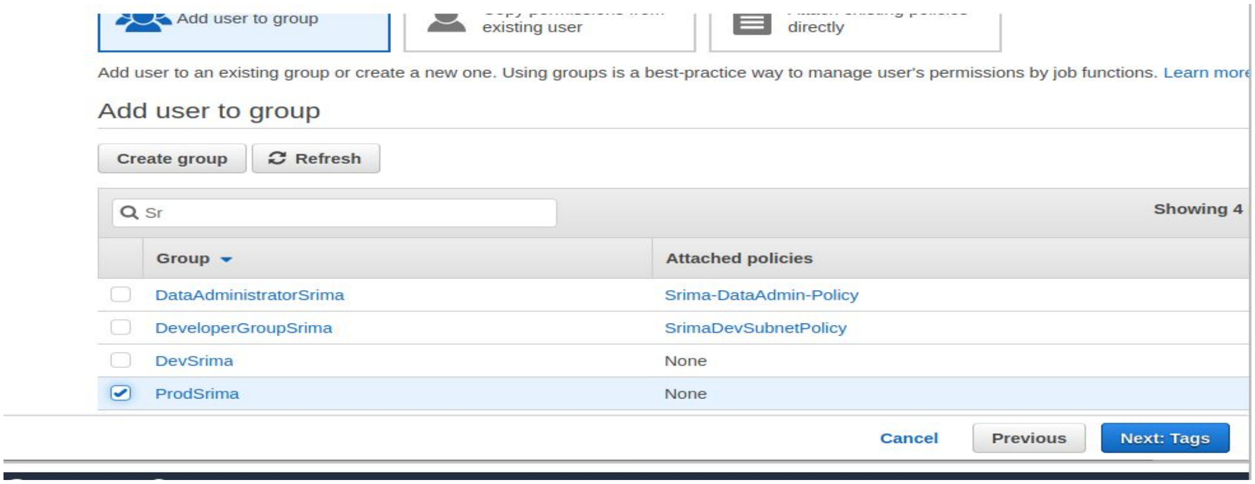
Select groups that user **Alice-Srima** will be added to.

DevSr

Showing 1 result

☐	Group Name	Users	Inline Policy	Creation Time
☑	DevSrima	0		2020-02-29 00:19 UTC+...

Add BOB to production group

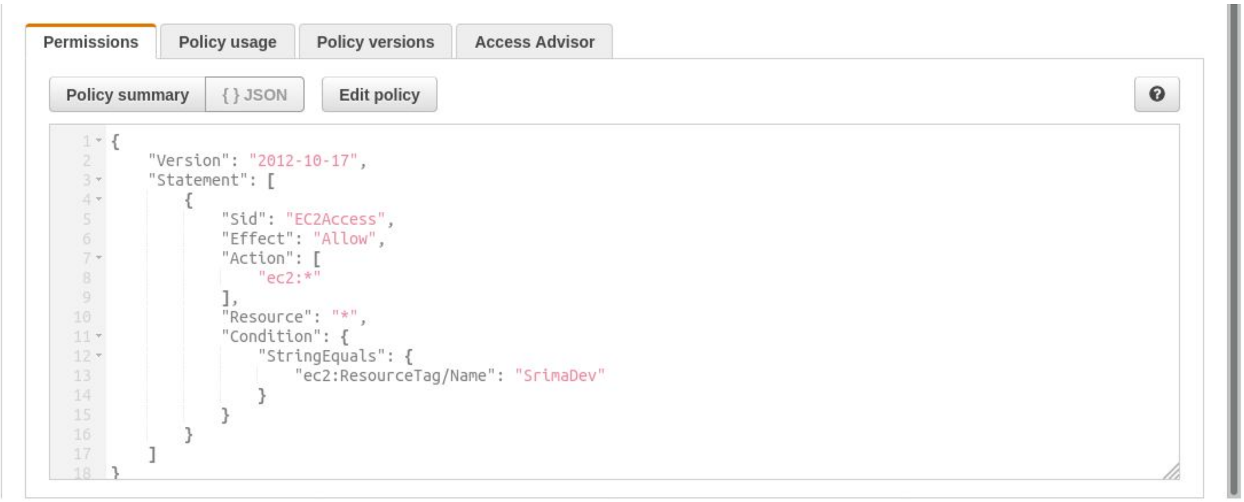


Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

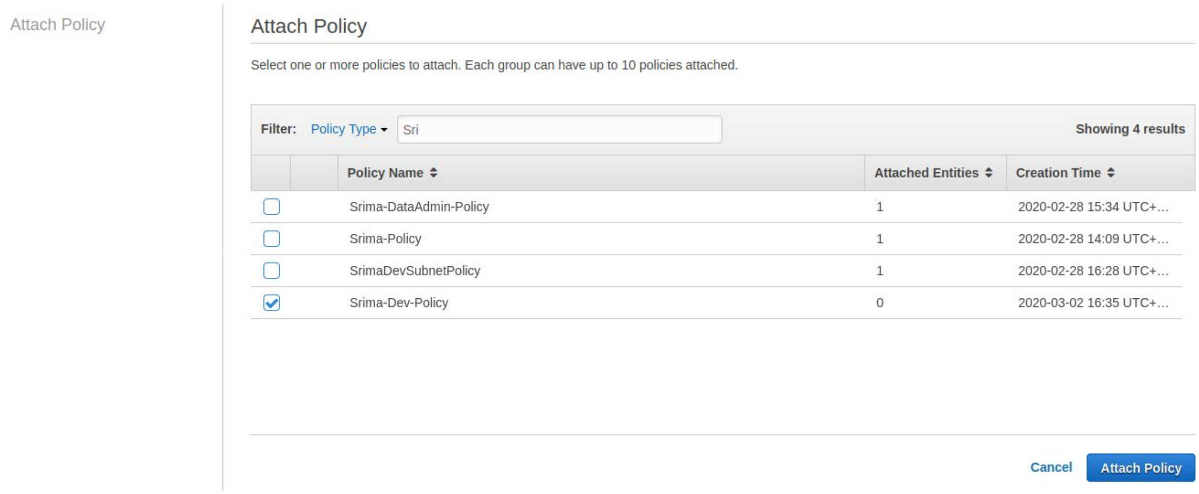
	Group	Attached policies
□	DataAdministratorSrima	Srima-DataAdmin-Policy
□	DeveloperGroupSrima	SrimaDevSubnetPolicy
□	DevSrima	None
☑	ProdSrima	None

Policy for SrimaDev



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Access",
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Name": "SrimaDev"
                }
            }
        }
    ]
}
```

Attach this to Dev group



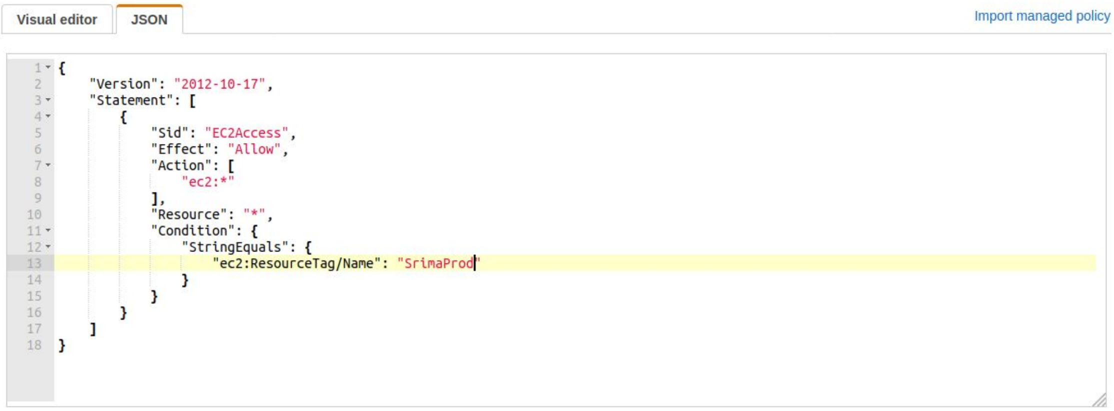
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ Sri Showing 4 results

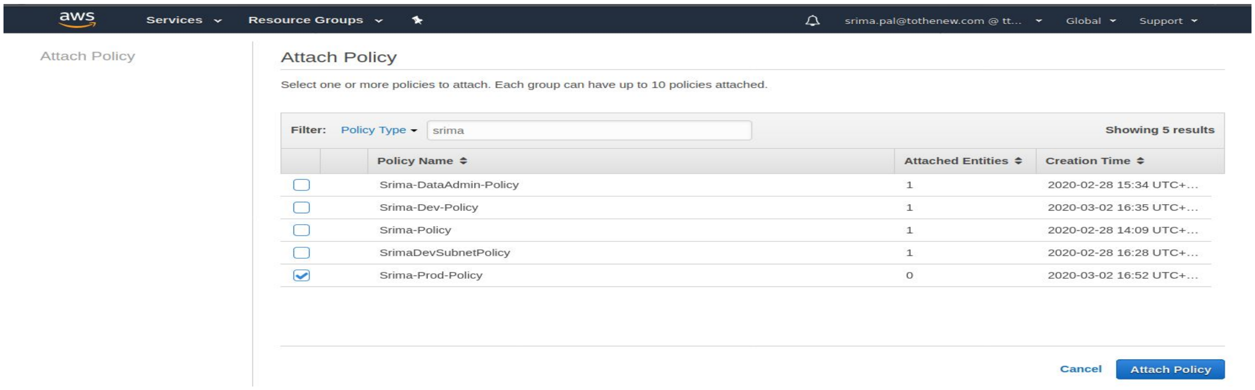
	Policy Name ⬍	Attached Entities ⬍	Creation Time ⬍
□	Srima-DataAdmin-Policy	1	2020-02-28 15:34 UTC+...
□	Srima-Policy	1	2020-02-28 14:09 UTC+...
□	SrimaDevSubnetPolicy	1	2020-02-28 16:28 UTC+...
☑	Srima-Dev-Policy	0	2020-03-02 16:35 UTC+...

Policy for SrimaProd



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Access",
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Name": "SrimaProd"
                }
            }
        }
    ]
}
```

Attach this to Srima Prod group



Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ srima Showing 5 results

	Policy Name ⬍	Attached Entities ⬍	Creation Time ⬍
□	Srima-DataAdmin-Policy	1	2020-02-28 15:34 UTC+...
□	Srima-Dev-Policy	1	2020-03-02 16:35 UTC+...
□	Srima-Policy	1	2020-02-28 14:09 UTC+...
□	SrimaDevSubnetPolicy	1	2020-02-28 16:28 UTC+...
☑	Srima-Prod-Policy	0	2020-03-02 16:52 UTC+...

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.

Create a policy